Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Επιθέσεις Πλευρικού Καναλιού στο Διαδίκτυο των Πραγμάτων

Ιωάννης Αθανασάκης

Διπλωματική Εργασία

Επιβλέπων: Δρ. Εμμανουήλ Θ. Μιχαηλίδης

Αιγάλεω, Ιανουάριος 2023

Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Επιθέσεις Πλευρικού Καναλιού στο Διαδίκτυο των Πραγμάτων

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	**Δρ. Εμμανουήλ Θ. Μιχαηλίδης**	**Ακαδημαϊκός Υπότροφος** Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής/ Εισηγητής – Επιβλέπων	Emmanouil Michailidis Digitally signed by Emmanouil Michailidis Date: 2023.01.29 15:32:49 +02'00'
2	**Δρ. Παναγιώτης Γιαννακόπουλος**	**Καθηγητής** Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής / Μέλος Εξεταστικής Επιτροπής	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.01.30 16:46:02 +02'00'
3	**Δρ. Παναγιώτης Ριζομυλιώτης**	**Επίκουρος Καθηγητής** Τμήμα Πληροφορικής και Τηλεματικής, Χαροκόπειο Πανεπιστήμιο / Μέλος Εξεταστικής επιτροπής	PANAGIOTIS RIZOMYLIOTIS PANAGIOTIS RIZOMYLIOTIS Feb 17 2023 11:00 AM

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος **Ιωάννης Αθανασάκης** του ΔΗΜΗΤΡΙΟΥ, με αριθμό μητρώου cscyb2003 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «**ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ»** του Τμήματος **Μηχανικών Πληροφορικής και Υπολογιστών** της Σχολής **Μηχανικών** του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

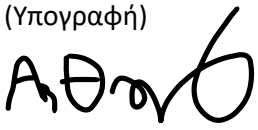
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Ιωάννης Αθανασάκης

27/1/2023

(Υπογραφή)



Αφιερώνεται εγκαρδίως στους πιο αξιόλογους και αγαπημένους ανθρώπους της οικουμένης,

Τους γονείς μου

Αφιερώνεται ως ελάχιστος φόρος τιμής σε έναν αδερφό που έφυγε νωρίς, «στα μακρινά ταξίδια…που έμειναν δίχως αύριο».

Στον Ένι Ζ.

«Στα ακροτελεύτια σύνορα και στην λεπτεπίλεπτη παρουσία σας εκεί»,

Στην δίδα Βλασία Π.

«Στις τρεις Μητέρες της ΠΑ που η στρατιωτική θητεία θα άξιζε μόνο και μόνο για τις συναντήσει κανείς στην ζωή του και να απολυθεί σοφότερος»,

Στις μητέρες του Λόχου, κκ. Μαρίνα, Αγλαΐα , Νίκη

« Στους συναδέλφους της υπηρεσίας και στο τμήμα της ΕΕ που θα ήθελα να υπηρετώ σε όλη μου την ζωή»,

Στους ανθρώπους της FRONTEX

"Στην δεσποινίδα που εσαεί θα συμβολίζει όλες τις πρωίες της Βαρσοβίας που κρατούσαν μέσα τους την ακροτελεύτια ελπίδα μιας άλλης εποχής»,

«Οι ευγενικοί άνθρωποι, κρύβουν μέσα τους παλιές πόλεις… κλεισμένες μέσα σε τείχη» (Χ. φ. Κ.),

Στην δίδα Anna Wrobel.

Ευχαριστίες

Στην μικρή αυτή ενότητα ο συγγραφέας θα επιθυμούσε να εκφράσει τον σεβασμό, την εκτίμηση και την εγκάρδια ευγνωμοσύνη του προς όλους όσους κρίνει ότι κάτι τέτοιο προσήκει.

Εν αρχής, ο συγγραφέας θα επιθυμούσε να ευχαριστήσει από βάθους καρδίας τους γονείς του, Δημήτρη και Ευδοκία, για την αμέριστη στήριξη, γνώση, και προπάντων αγάπη που του έχουν χαρίσει όλα αυτά τα χρόνια. Δίχως εκείνους το να φτάσει ο συγγραφέας μέχρι αυτό το σημείο στην ζωή του θα ήταν ανέφικτο, και γι' αυτό θα τους ευγνωμονεί αιωνίως.

Ακόμα ο συγγραφέας θα επιθυμούσε μέσα από αυτές τις λιγοστές γραμμές να αποτίνει έναν ελάχιστο φόρο τιμής σε άτομα που τον συνέδραμαν αμέριστα και που δεν είναι πια εδώ. Ο συγγραφέας απευθύνει μια ταπεινή γονυκλισία προς τους παππούδες του, Παύλο, Δέσποινα, Μαρία & Ιωάννη οι οποίοι μέσα από το παράδειγμα τους και την στάση ζωής τους κληροδότησαν στον ίδιο τον συγγραφέα κι στους γονείς του αξίες ζωής με βάσει τις οποίες δύνανται οι ίδιοι να πορευτούν στον βίο τους. Επίσης ο συγγραφέας επιθυμεί να κλείσει το γόνυ και στον παιδικό του φίλο, Ένι Ζ., που έφυγε νωρίς και του οποίου η φιλία και ο αμοιβαίος σεβασμός αποτελούν σήμερα ένα μετάλλιο τιμής για τον συγγραφέα. Οι αναμνήσεις αυτές θα συνθέτουν για πάντα ένα σημαίνον κομμάτι των μικρών αποσκευών στις ατελεύτητες λεωφόρους της επιστήμης, εκεί όπου πλανήθηκε με χάρη ο πιο χαρισματικός μαθηματικός νους ενός ναυπηγού που έμελλε ποτέ να γνωρίσει η επιστημονική κοινότητα.

Ολοκληρώνοντας την ελάχιστη αυτή παράθεση ο συγγραφέας θα επιθυμούσε ακόμα να ευχαριστήσει τα μέλη της τριμελούς επιτροπής, Δρ. Ε. Θ. Μιχαηλίδη (Επιβλέπων), Δρ. Π. Γιαννακόπουλο & Δρ. Π. Ριζομυλιώτη, για την κριτική καθοδήγηση και συμπαράσταση τους και τον καθένα ξεχωριστά για την γνώση που μετέδωσαν στον συγγραφέα και στους συμφοιτητές αυτού καθ' όλη την διάρκεια των μαθημάτων τους και του μεταπτυχιακού κύκλου σπουδών εν συνόλω, επιτρέποντας μας έτσι να πραγματοποιήσουμε τα πρώτα καθοριστικά βήματα στον ραγδαία εξελισσόμενο «κόσμο» της Κυβερνοασφάλειας.

Περιεχόμενα

Εισαγωγή 10

Μέρος 1ο 16

Θεωρητικό Πλαίσιο: Προβλήματα Ορισμών & Η Σημασία των Ταξινομήσεων των SCAs για τις Κρίσιμες Υποδομές (CI) 16

Κεφάλαιο 1ο : Ο ορισμός και η σημασία των επιθέσεων πλευρικού καναλιού για τις κρίσιμες υποδομές 17

Υπό-ενότητα 1.1: Το εννοιολογικό πλαίσιο περί του δίπολου διαδίκτυο των πραγμάτων (IoT) & επιθέσεις πλευρικού καναλιού (Side-channel Attacks, SCAs) 17

Υπό-ενότητα 1.2: Η σημασία των επιθέσεων πλευρικού καναλιού (SCAs) για τις κρίσιμες υποδομές ..23

Υπό-ενότητα 1.3: Η εννοιολογική αποσαφήνιση περί των επιθέσεων πλευρικού καναλιού (SCAs) 32

Κεφάλαιο 2ο : Η ιστορική αναδρομή και τα εγχειρήματα ταξινομήσεως των SCAs 48

Υπό-ενότητα 2.1: Ιστορική επισκόπηση περί των επιθέσεων πλευρικού καναλιού 48

Υπό-ενότητα 2.2: Σχετικά με τις κατηγοριοποιήσεις των επιθέσεων πλευρικού καναλιού 52

Μέρος 2ο 87

Περιπτώσεις SCAs κατά IoT συσκευών & Ενσωματωμένων Συστημάτων στις Κρίσιμες Υποδομές (CI) & Συστηματοποίηση Αντιμέτρων (Countermeasures) 87

Κεφάλαιο 3ο : Επιθέσεις Πλευρικού Καναλιού (SCAs) εναντίον Κρίσιμων Υποδομών (CI) 88

Υπό-ενότητα 3.1: Περί του ορισμού των κρίσιμων υποδομών (CIs) και των σχετικών παραδειγμάτων 88

Υπό-ενότητα 3.2: Επιθέσεις πλευρικού καναλιού στο Διαδίκτυο των Πραγμάτων (IoT) των κρίσιμων υποδομών, βιβλιογραφική ανασκόπηση 113

Κεφάλαιο 4ο : Ταξινομητικό εγχείρημα περί αντιμέτρων έναντι των Επιθέσεων Πλευρικού Καναλιού (SCAs) 186

Υπό-ενότητα 4.1: Συνοπτική Παρουσίαση Αντιμέτρων έναντι επιθέσεων πλευρικού καναλιού (SCAs), εγχείρημα περί της ταξινόμησης 187

Υπό-ενότητα 4.2: Η αξιοποίηση των SCAs ως αντιμέτρων καθαυτών 221

Υπό-ενότητα 4.3: Ενδεικτικές κατευθυντήριες (Indicative Guidelines) έναντι των SCAs για την προστασία των συσκευών του Διαδικτύου των Πραγμάτων (IoT) στις Κρίσιμες Υποδομές 223

Μέρος 3ο 229

ΣΥΜΠΕΡΑΣΜΑΤΑ 229

Συμπεράσματα 230

Βιβλιογραφία 242

Περίληψη

Αντικείμενο της ανά χείρας διπλωματικής εργασίας αποτελεί η μελέτη των επιθέσεων πλευρικού καναλιού (Side-Channel Attacks) κατά του Διαδικτύου των Πραγμάτων (Internet of Things , IoT) και των συσκευών που περιέρχονται κάτω από την ομπρέλα του όρου αυτού (ήτοι ευφυείς συσκευές, Smart Devices, και ενσωματωμένα συστήματα (Embedded Systems)) , και ταυτόχρονα εντός του ευρύτερου (αν και μόνο ακροθιγώς) πλαισίου των Κρίσιμων Υποδομών (Critical Infrastructure (CI)). Αξιοποιώντας αποκλειστικά την βιβλιογραφική προσέγγιση (αγγλόφωνη επιστημονική αρθρογραφία), η παρούσα διπλωματική εργασία διακρίνεται σε δύο μέρη, τα οποία περιλαμβάνουν αντίστοιχα από δύο κεφάλαια το καθένα. Το πρώτο μέρος αφιερώνεται αποκλειστικά στην συγκρότηση του θεωρητικού πλαισίου, όπου ο σημαίνων στόχος είναι αφενός η εννοιολογική αποσαφήνιση των στοιχείων που συνθέτουν τους αφετηριακούς ορισμούς του πονήματος αυτού (ήτοι του Διαδικτύου των Πραγμάτων, των εφαρμοσμένων συστημάτων και των επιθέσεων πλευρικού καναλιού), και αφετέρου η διερεύνηση των ταξινομητικών εγχειρημάτων που αφορούν στην παρουσίαση και ανάλυση των επιμέρους παραλλαγών που παρουσιάζουν οι επιθέσεις πλευρικού καναλιού στην βιβλιογραφία που μελετήθηκε.

Το δεύτερο μέρος της διπλωματικής εργασίας επικεντρώνει στην αρχικά στην εννοιολογική αποσαφήνιση των Κρίσιμων Υποδομών και σε παραδείγματα των τελευταίων που ενσωματώνουν συσκευές του Διαδικτύου των Πραγμάτων. Κατόπιν, και με βάσει την υπάρχουσα βιβλιογραφία, έγινε η παρουσίαση μεθοδολογιών επιθέσεως διαφόρων παραλλαγών με βάσει τις συσκευές IoT που θα μπορούσαν βρίσκονται ενσωματωμένες σε μια ενδεικτική πληθώρα Κρίσιμων Υποδομών (Νοσοκομεία, Αγροτικός Τομέας, Βιομηχανία κλπ).Το δεύτερο μέρος ολοκληρώνεται με την καταγραφή ενδεικτικών αντιμέτρων προς εφαρμογή επί των συσκευών IoT που μπορεί να απαντώνται στις Κρίσιμες Υποδομές, και τα οποία διαρθρώνονται επί ενός τετραμερούς σχήματος αξόνων, περιλαμβάνοντας ειδικότερα αντίμετρα Λογισμικού (Software), Υλικού (Hardware), περιβάλλοντος (Work Environment), καθώς και την συμβολή των ίδιων των επιθέσεων στην συγκρότηση αντιμέτρων (π.χ. anomaly detection).

Η κριτική συμβολή της διπλωματικής εργασίας αποτυπώνεται σε μια σειρά από συμπεράσματα που διατυπώνονται στο οικείο κεφάλαιο. Ειδικότερα, υφίσταται ένα κενό αναφορικά με την δυνατότητα εύληπτης ενσωμάτωσης νέας γνώσης διότι αναφύεται μια εννοιολογική σχετικότητα ομού μετά της απουσίας αποκλειστικών κατηγοριών κατά την ταξινόμηση των επιθέσεων. Δεύτερον, οι συσκευές IoT συγκεντρώνουν μια σειρά από ευπάθειες (περιορισμένη ισχύς, συνεχής λειτουργία, απουσία επιτήρησης κλπ) που τις καθιστά ιδιαίτερα

ευάλωτες έναντι των εν λόγω επιθέσεων. Τρίτον, παρατηρήθηκε επίσης πως οι επιθέσεις πλευρικού καναλιού αξιοποιούνται στην βιβλιογραφία μόνο παθητικά (passive) για συλλογή πληροφοριών, και συχνά εμφανίζονται να συνεπικουρούνται από έτερες επιθέσεις (π.χ. malware κλπ). Μελλοντικά η έρευνα μπορεί να κινηθεί στην κατεύθυνση, ενδεικτικά, είτε της επιθετικής χρήσης των επιθέσεων πλευρικού καναλιού (offensive), είτε του συνδυασμού διαφορετικών τέτοιων επιθέσεων για μεγιστοποίηση της αποτελεσματικότητας.

Λέξεις-κλειδιά: Επίθεση Πλευρικού Καναλιού, Κρίσιμες Υποδομές, Διαδίκτυο των Πραγμάτων, Ενσωματωμένα Συστήματα.

Abstract

This Dissertation investigates several types of Side-channel attacks (SCAs) in the Internet of Things (IoT) ecosystem, including IoT Devices, Embedded Systems, and IoT-based Critical Infrastructures (CI). Specifically, this Dissertation is divided into two parts, each consisting of two chapters. The first part focuses on the attempts to delineate definitions partaking to the subject at hand (i.e., IoT, Embedded Systems, Attack vectors, etc.) and also to present the various SCA-based Taxonomies found in many research articles. The second part of this Dissertation probes into the definition of CI as well as on the studying of various SCA-based schemes against IoT devices that can be in found in several different CIs (i.e., Healthcare Sector, Industries, Agricultural Sector, etc.). Additionally, the second part concludes with an additional listing of many different countermeasures clustered in a quadruple scheme incorporating Software-based countermeasures, Hardware-based countermeasures, Work Environment-related countermeasures, and lastly the use of SCAs as potential countermeasures (i.e., the use of electromagnetic emanations for anomaly detection, etc.).

Among the different concluding remarks the Dissertation has come up with, were the definitional and taxonomical ambiguity of SCAs and their variations. Also, it was observed that the IoT devices feature a number of vulnerabilities (e.g., limited resources, continuous functionality, lack of constant human supervision, etc.) that turn them into exemplary attack vectors for SCAs that attempt to extract information. Moreover, SCAs are treated as passive attack schemes merely for collecting information, while frequently being complemented by other attacks (e.g., malware, Insider threats, etc.) or having these other attacks complement them instead. Points for future research may include the utilization of SCAs in more offensive attack schemes that can damage systems and CIs, as well as conducting research in combinatory SCA schemes for maximizing gains.

Keywords: Side-channel Attack (SCA), Critical Infrastructure (CI), Internet of Things (IoT), Embedded Systems.

Εισαγωγή

Το αντικείμενο με το οποίο καταπιάνεται η παρούσα διπλωματική εργασία συνδέεται, έστω έμμεσα, με το ακόλουθο ερώτημα, τίνι τρόπω είναι εφικτό να ανακτηθεί ο ήχος μιας βιντεοσκόπησης χωρίς όμως ο επιτιθέμενος να έχει οποιαδήποτε πρόσβαση στο μικρόφωνο ή σε κάποια αποθηκευμένη ηχογράφηση καθ' οιοδήποτε στιγμή ;

Οι Davis et al. δίνουν μια πιθανή απάντηση στο παραπάνω ερώτημα καταδεικνύοντας πως οι δονήσεις που οι διάφοροι ήχοι (π.χ. διάφορες πηγές ήχων όπως η ανθρώπινη ομιλία κλπ) αναπαράγουν και που προσκρούουν (ενν. οι δονήσεις αυτές) πάνω σε αντικείμενα του περιβάλλοντος χώρου μπορούν να χρησιμεύσουν στην ανάκτηση του ήχου από ένα βίντεο (video) που να έχει ρυθμιστεί για αναπαραγωγή σε υψηλή ταχύτητα (high speed). Σε αυτή την περίπτωση οι συγγραφείς δείχνουν πως τα αντικείμενα του χώρου μπορούν, κατ' αναλογία, να χρησιμεύσουν ως ένα είδους μικρόφωνο καθώς οι δονήσεις που δημιουργούνται επ' αυτών, αν γίνει επεξεργασία τους, μπορούν να ανασυνθέσουν ήχους και ίσως ακόμα και το περιεχόμενο μιας συζητήσεως ανάμεσα σε ανθρώπους[1].

Το παραπάνω αποτελεί ένα μόνο παράδειγμα για το πώς μπορεί να σχεδιαστεί και να εκτελεστεί μια επίθεση πλευρικού καναλιού (Side-channel attack, εν συντομία SCA), αν και ομολογουμένως δεν πρόκειται για το τυπικότερο των δειγμάτων. Στο ευρύτερο πλαίσιο της κυβερνοασφάλειας οι επιθέσεις πλευρικού καναλιού αποτελούν μια αρκετά διευρυμένη κατηγορία επιθέσεων (όπως φαίνεται και από τις μεταβλητές που εμπλέκονται στο ως άνω παράδειγμα που παρατέθηκε) που εξαιτίας αυτής της ευρύτητας της καθιστά δυσχερές το εγχείρημα του ολόπλευρου ορισμού τους, καθώς επίσης και εκείνο της πλήρους καταγραφής όλων των πιθανών μεθοδολογιών εκτέλεσης τους[2](περισσότερα γι' αυτά τα δύο σημεία στα κεφάλαια που ακολουθούν).

---

[1] Χρησιμοποιείται ο όρος "*Visual Microphone"* για να περιγράψει την λειτουργία αυτή των αντικειμένων του περιβάλλοντος χώρου, ή ενδεχομένως ορθότερα αυτή την αλληλεπίδραση εκροής-περιβάλλοντος. Βλ. ενδεικτικά, Davis, A., & Rubinstein, M., & Wadhwa, N., & Mysore, G.J., & Durand, F., & Freeman, W.T.(2014). The Visual Microphone: Passive Recovery of Sound from Video. *ACM Transactions on Graphics, 33, 4, 79,*1-10,σ.9. doi: https://doi.org/10.1145/2601097.2601119. https://dl.acm.org/doi/10.1145/2601097.2601119 (τελευταία πρόσβαση 22/1/2022).

[2] Ένας ορισμός που μόνο σε γενικές γραμμές δίνει το περιεχόμενο του ακρωνύμιου SCA δίδεται από τον οργανισμό του NIST, όπου οι επιθέσεις πλευρικού καναλιού ορίζονται ως (η μετάφραση που ακολουθεί είναι του γράφοντος και σε κάποια σημεία αποδίδεται περισσότερο «ελεύθερα» το νόημα του αγγλικού κειμένου) «*μια επίθεση που καθίσταται εφικτή εξαιτίας της διαρροής πληροφοριών από ένα φυσικό κρυπτοσύστημα. Χαρακτηριστικά*

Η μελέτη αυτής της κατηγορίας επιθέσεων έχει μελετηθεί σε μεγάλο βαθμό από την διεθνή βιβλιογραφία, ειδικότερα από την δεκαετία του '90 και εντεύθεν[3], ενώ η ύπαρξη τους χρονολογείται , σε κάποιες περιπτώσεις, ήδη από το πρώτο μισό του 20ου αιώνος (για περισσότερες λεπτομέρειες ορά σχετικά το δεύτερο κεφάλαιο της διπλωματικής).

Η έμφαση στην διεθνή βιβλιογραφία δίνεται σε διάφορες πτυχές των SCAs όπως για παράδειγμα,

- ✓ στις μελέτες περίπτωσης για μια συγκεκριμένη υποκατηγορία και εν σχέση με ορισμένες συσκευές ή λογισμικό ως αποδέκτες της επιθέσεως[4],
- ✓ στις προσπάθειες ταξινόμησης (είτε συνολικά είτε για μεμονωμένες κατηγορίες αυτών σε κάθε διαφορετικό άρθρο) των SCAs γενικά[5],

---

τα οποία δύναται να εκμεταλλευθεί μια επίθεση πλευρικού καναλιού αποτελούν μεταξύ άλλων η χρονική διάρκεια/χρονομέτρηση στην εκτέλεση λειτουργιών, η κατανάλωση του ρεύματος, και οι ηλεκτρομαγνητικές και ακουστικές εκροές». χ.σ.(χ.χ.). Side-Channel Attack. *Glossary, Information Technology Laboratory Computer Security Center(CSRC),NIST.*https://csrc.nist.gov/glossary/term/side_channel_attack (τελευταία πρόσβαση 23/1/2022).

[3] Πρωτοπόρος στο εν λόγω εγχείρημα υπήρξε, μεταξύ άλλων, ο P. Kocher μελετώντας τις SCAs που αφορούσαν σε αναλύσεις ισχύος (SPA, Simple Power Analysis, DPA, Differential Power Analysis). Ορά ενδεικτικά το άρθρο του, μαζί με άλλους συγγραφείς, από τα τέλη της δεκαετίας του '90, Kocher, P., & Jaffe, J., & Jun, B.(1999). *Differential Power Analysis*. Paper presented at the 19th Annual International Cryptology Conference (Advances in Cryptology-CRYPTO'99). Santa Barbara, California, USA, August 15-19, 1-10, σ.1 κε. https://paulkocher.com/doc/DifferentialPowerAnalysis.pdf (τελευταία πρόσβαση 23/1/2022).

[4] Ορά ενδεικτικά και, Clark, S.S., & Ransford, B., & Rahmati, A., & Guineau, S., & Sorber, J., & Fu, K., & Xu, W.(2013). *WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices.* Paper presented at the 2013 USENIX Workshop on Health Information Technologies (HealthTech '13), Washington DC, USA, August 12, 1-11, σ.3 κε. https://www.usenix.org/conference/healthtech13/workshop-program/presentation/clark (τελευταία πρόσβαση 15/10/2021).

[5] Βλ. ενδεικτικά τα σχήματα στο, Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313, σ.298-305. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

- ✓ στην χρήση των SCAs ως αμυντικών μέσων (ήτοι αντίμετρα σε επίθεση, καίτοι οι προσπάθειες αυτές είναι μεμονωμένες και ελάχιστες ως τώρα) κα[6].

Αν και τα γενικότερα στοιχεία που συγκροτούν την κάθε επίθεση πλευρικού καναλιού θα αναλυθούν κατωτέρω, για την εισαγωγή της παρούσας διπλωματικής, αρκεί γενικά να αναφερθεί πως το ερευνητικό ενδιαφέρον που η κάθε μια τους παρουσιάζει επικεντρώνει κυρίως στο ότι όλες τους εκμεταλλεύονται τις εκροές (leakages, emanations) που προκύπτουν (ενν. παρατηρούνται, observation, measurement κλπ) ηθελημένα ή αθέλητα (intended, unintended) από την καθαυτό εφαρμογή του υλικού (hardware), χωρίς να επιτίθεται κατευθείαν στο υλικό ή σε κάποια εφαρμογή (όπως άλλες επιθέσεις), για να αποσπάσουν εν τέλει αυτό που επιθυμεί ο επιτιθέμενος αφήνοντας κυρίως ακέραιο τον στόχο[7]. Πράγματι παρουσιάζει ενδιαφέρον το γεγονός ότι η επίθεση γίνεται έμμεσα και όχι όπως συνηθίζεται με άμεσο τρόπο και συνήθως με την αναζήτηση ή δημιουργία κάποιας αδυναμίας.

Ένα δεύτερον ενδιαφέρον στοιχείο που παρακινεί στην μελέτη των SCAs για τους σκοπούς της παρούσας εργασίας είναι πως η τεχνολογική πρόοδος των τελευταίων δεκαετιών έχει διευκολύνει, αλλά και βελτιστοποιήσει, την εκτέλεση των SCAs, κάτι που παλαιότερα αποτελούσε δυσχερές εγχείρημα για την μεγάλη πλειοψηφία των δυνητικά επιτιθέμενων. Η μεγαλύτερη ευχέρεια στην επιτυχή εκτέλεση των SCAs μπορεί να οφείλεται, μεταξύ άλλων, στην πρόοδο στον εξοπλισμό για τις μετρήσεις, και επιπλέον στην πρόοδο που σημειώνεται στους αλγορίθμους μηχανικής μαθήσεως που συνδράμουν τον επιτιθέμενο στην λήψη και ανάλυση (μετατροπή σε κατανοητή μορφή) των εκροών[8].

Τρίτον, καθώς οι SCAs αξιοποιούν εκροές για να επιτεθούν εμμέσως προς ένα ή πολλούς στόχους, δεν θα ήταν καθόλου σπατάλη χρόνου η μελέτη τους υπό το πρίσμα των κρίσιμων υποδομών (Critical Infrastructures). Αυτό συμβαίνει διότι, αφενός οι κρίσιμες υποδομές δεν φαίνεται να έχουν μελετηθεί σε πολύ μεγάλο βαθμό από κοινού με τις SCAs, και επομένως υπάρχει ενδεχομένως ένα κενό στην βιβλιογραφική επισκόπηση όπου μελλοντικά νέα γνώση

---

[6] Επί παραδείγματι, για την χρησιμότητα κάποιων SCAs στο έργο του digital forensics, βλ. ενδεικτικά Sayakkara, A, & Le-Khac, N.A., & Scanlon, M.(2019). A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics. *Elsevier Digital Investigations,arXiv:1903.07703v1[cs.CR]*,1-13,σ.8-9 κε. https://arxiv.org/pdf/1903.07703.pdf (τελευταία πρόσβαση 12/10/2021).

[7]Wright,G.,&Gillis,A.S.(χ.χ.).Side-channel attack. *Techtarget.* https://www.techtarget.com/searchsecurity/definition/side-channel-attack (τελευταία πρόσβαση 23/1/2022).

[8] Ο.π.

μπορεί να παραχθεί και να ενσωματωθεί στην ήδη υπάρχουσα (και επομένως και σε ότι αφορά και στην κυβερνοασφάλεια εν σχέσει με τις υποδομές αυτές).

Αφετέρου, το μέγεθος, η περιπλοκότητα, και η σημασία των κρίσιμων υποδομών τόσο για την κοινωνία όσο και για την παγκόσμια οικονομία συνεπάγεται τον πολλαπλασιασμό των πιθανών εκροών από το υλικό, το λογισμικό, και τις ατομικές συσκευές που υπάρχουν και λειτουργούν εντός των εκάστοτε εγκαταστάσεων. Εύλογα οι ευκαιρίες για την επιτυχή εκτέλεση μιας SCA μπορούν να πολλαπλασιαστούν, και καθώς ο ENISA έχει σχετικά πρόσφατα χαρακτηρίσει την διαρροή (leakage) πληροφοριών ως μια σοβαρή κυβερνοαπειλή, πρέπει να διενεργηθεί η μελέτη τέτοιων απειλών πέρα από την μικροκλίμακα μιας συσκευής ή ενός προγράμματος λογισμικού(ή εναλλακτικά να επιχειρηθεί η μελέτη του πως οι απειλές σε ένα τέτοιο μίκρο-επίπεδο αντανακλούν στο ευρύτερο σκέλος της όποιας κρίσιμης υποδομής)[9].

Η ανά χείρας διπλωματική εργασία καλείται στα κεφάλαια που ακολουθούν να μελετήσει την σχέση των SCAs με τις κρίσιμες υποδομές (CI), υπό το πρίσμα των κάτωθι τριών ερευνητικών ερωτημάτων, ως εξής:

- Δεδομένου του μεγάλου αριθμού των εκροών και των πιθανών επιθέσεων SCAs, ποια η συμβολή των ορισμών και των υπαρχουσών σχημάτων ταξινόμησης σε ότι αφορά στην προσπάθεια αντιμετώπισης τους, και επίσης ποιες οι πιθανές αστοχίες τέτοιων εννοιολογικών/δομικών σχημάτων ;
- Τι συνεπάγονται οι SCAs για την εύρυθμη λειτουργία των συσκευών των κρίσιμων υποδομών όπως οι IoT συσκευές & τα ενσωματωμένα συστήματα, και ποια/-ες μεθοδολογία/-ες επιθέσεως αξιοποιούνται κατά των υποδομών αυτών (παραδείγματα στα οποία βρίσκουν εφαρμογή κάποιες επιθέσεις πλευρικού καναλιού επομένως) ;
- Ποια πιθανά αντίμετρα (countermeasures) υφίστανται και πως μπορούν, πιθανότατα, να ταξινομηθούν με βάσει τις ανάγκες για την προστασία των κρίσιμων υποδομών ;

Για την κατά το δυνατόν πληρέστερη πραγμάτευση του αντικειμένου της διπλωματικής, καθώς και για την όσο γίνεται ευκολότερη παρακολούθηση των επιχειρημάτων προς διατύπωση,

[9] χ.σ.(2019-2020). *From January 2019 to April 2020 Information leakage ENISA Threat Landscape.* Athens: ENISA European Union Agency for Cybersecurity,1-20,σ.11. Ανακτήθηκε από https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-information-leakage (τελευταία πρόσβαση 23/1/2022).

αλλά και του περιεχομένου αυτής, προτείνεται η διάρθρωση του πονήματος σε πέντε (5, συμπεριλαμβανομένων των τελικών συμπερασμάτων) κεφάλαια, ως ακολούθως:

- Κεφάλαιο 1ο : προτείνεται η συζήτηση περί των δυσκολιών ορισμού των επιθέσεων πλευρικού καναλιού και η ενδελεχής ανάλυση των στοιχείων που συγκροτούν τον ορισμό αυτών. Η διερεύνηση των δυσχερειών αυτών μπορεί να αναδείξει την σημασία που ενέχει ένας περιεκτικός ορισμός για την κατανόηση και δυνητικά επιτυχή αντιμετώπιση τέτοιων απειλών.
- Κεφάλαιο 2ο : προτείνεται η διερεύνηση τόσο της ιστορικής εξέλιξης των SCAs όσο και εκείνη ορισμένων σχημάτων ταξινομήσεως καθώς και οι δυσχέρειες που παρουσιάζονται στην προσπάθεια κατασκευής μιας τέτοιας δομής κατηγοριοποίησης (ή κατηγοριοποιήσεων). Διερευνάτε η (πρακτική) σημασία που ενέχει μια ταξινόμηση για την μελέτη των SCAs, καθώς επίσης και οι δυσχέρειες που παρατηρούνται σε ορισμένα από τα υπάρχοντα εγχειρήματα περί της ταξινόμησης προς άντληση γενικότερων συμπερασμάτων.
- Κεφάλαιο 3ο : στο κεφάλαιο αυτό θα διερευνηθούν, αφενός ο ορισμός της έννοιας κρίσιμες υποδομές συνοδευόμενος από ορισμένα παραδείγματα τέτοιων υποδομών, και αφετέρου πως οι SCAs απειλούν αυτές τις τελευταίες (μέθοδοι επιθέσεως κλπ). Στόχος εδώ είναι να αναδειχθούν οι πρακτικές διαστάσεις των επιθέσεων πλευρικού καναλιού επί των συσκευών που ενσωματώνουν οι διάφορες κρίσιμες υποδομές (IoT συσκευές, ενσωματωμένα συστήματα).
- Κεφάλαιο 4ο : στο συγκεκριμένο κεφάλαιο θα παρατεθούν και θα αναλυθούν, ταξινομητικά, μια σειρά από πιθανά και ήδη καταγεγραμμένα στην βιβλιογραφία αντίμετρα (countermeasures) έναντι των SCAs που απειλούν τις κρίσιμες υποδομές. Η στόχευση του κεφαλαίου επικεντρώνει στην προσπάθεια σύνδεσης των αντιμέτρων κατά των SCAs με συγκεκριμένες πτυχές των υποδομών (ήτοι IoT συσκευές και ενσωματωμένα συστήματα), έτσι ώστε να δημιουργηθεί (αν είναι εφικτό) μια ενδεικτική σειρά από κατευθυντήριες (guidelines) για την καλύτερη προστασία των υποδομών γενικά, αλλά και σε ότι αφορά τις συσκευές που αναφέρθηκαν [10].
- Συμπεράσματα: στο κεφάλαιο με το οποίο ολοκληρώνεται η ανά χείρας διπλωματική εργασία παρατίθενται αφενός τα συμπεράσματα στα οποία έφτασε η εν

[10] Το τελευταίο αυτό τμήμα προβλέπεται να αναφερθεί ακροθιγώς καθώς δεν επαρκεί ο χώρος για μια πλήρη ανάπτυξη.

λόγω έρευνα και αφετέρου ορισμένα σημεία προς μελλοντική διερεύνηση. Ακολούθως παρατίθεται και η συγκεντρωτική βιβλιογραφία (ξενόγλωσσα άρθρα κλπ) που αξιοποιήθηκε για την κατάρτιση και ολοκλήρωση της οικείας διπλωματικής εργασίας.

Μέρος 1ο

Θεωρητικό Πλαίσιο: Προβλήματα Ορισμών & Η Σημασία των Ταξινομήσεων των SCAs για τις Κρίσιμες Υποδομές (CI)

Κεφάλαιο 1ο : Ο ορισμός και η σημασία των επιθέσεων πλευρικού καναλιού για τις κρίσιμες υποδομές

Η συνεισφορά της ανά χείρας διπλωματικής εργασίας έγκειται στην μελέτη των SCAs εν σχέσει με τις κρίσιμες υποδομές, και πιο συγκεκριμένα σε ότι αφορά τις συσκευές IoT και τα ενσωματωμένα συστήματα που στην σημερινή συγκυρία υπάρχουν και επιτελούν λειτουργίες εντός μιας οποιασδήποτε από τις υποδομές αυτές (π.χ. τομέας υγειονομικής περίθαλψης, αγροτικός τομέας κλπ). Η ανάγκη της συμβολής αυτής απορρέει από το γεγονός ότι οι σύγχρονες υποδομές ενός οποιοδήποτε κράτους ανά την υφήλιο ενσωματώνουν, για να καταστούν εν τέλει οι ίδιες λειτουργικές, μια σειρά από συστήματα που τοποθετούνται υπό τον ευρύ ορισμό του διαδικτύου των πραγμάτων (Internet of Things), και τα οποία συστήματα και συσκευές αφορούν τόσο στο σκέλος της προσωπικής χρήσης από πλευράς προσωπικού (π.χ. κινητές, android ή iOS, συσκευές, wearables κλπ) όσο και σε εκείνο της καθαυτό εργασιακής τους λειτουργικότητας (π.χ. ιατρικά μηχανήματα, συσκευές που αξιοποιούνται σε αυτοματισμούς όπως στις περιπτώσεις φέρ' ειπείν των αυτόνομων οχημάτων, συσκευές που αξιοποιούνται για σκοπούς τηλεργασίας όπως Η/Υ κλπ).

Υπό-ενότητα 1.1: Το εννοιολογικό πλαίσιο περί του δίπολου διαδίκτυο των πραγμάτων (IoT) & επιθέσεις πλευρικού καναλιού (Side-channel Attacks, SCAs)

Αρχικά, κρίνεται ως ουσιαστικής σημασίας, το εγχείρημα αποσαφήνισης του ορισμού αφενός των IoT και αφετέρου των ενσωματωμένων συσκευών. Στόχος εδώ είναι η λειτουργική κατανόηση των εν λόγω ορισμών και επομένως η έμφαση θα δοθεί μόνο στα βασικά χαρακτηριστικά των ορισμών τους και στην συνοπτική παράθεση αυτών ως ακολούθως:

- ✓ Εκκινώντας από την έννοια του διαδικτύου των πραγμάτων (Internet of Things, όπου οι IoT devices τελούν σε σχέση γενικού-ειδικού αναφορικά με τον ορισμό που περιγράφεται εδώ), εδώ πρόκειται ουσιαστικά για έναν όρο-ομπρέλα ο οποίος συναποτελείτε από μια σειρά επίσης, αρκετά, γενικευτικών ορισμών όπως έξυπνες οικιακές συσκευές, φυσικές συσκευές, συσκευές που ενσωματώνουν αισθητήρες και ηλεκτρονικά κυκλώματα, αυτόνομα οχήματα κλπ[11].

[11] Shafiq, M., & Gu, Z., & Cheikhrouhou, O., & Alhakami, W., & Hamam, H.(2022). The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks.

✓ Το συνονθύλευμα των συσκευών αυτών , καίτοι διαφορετικών μεταξύ τους, ενέχει ένα κοινό σημείο αναφοράς σχετικά με την μεταξύ τους διασύνδεση (networked, connectivity κλπ). Η ολοένα αυξανόμενη συνδεσιμότητα τους επιτρέπει όχι μόνο την ανταλλαγή δεδομένων και την διαλειτουργικότητα (interoperability) εντός του πλαισίου των κρίσιμων υποδομών, αλλά και τον σχεδόν ταυτόχρονο πολλαπλασιασμό των πιθανών κυβερνοεπιθέσεων (cyberattacks) εναντίον τους, και κατ' επέκταση και ενάντια στις ίδιες τις υποδομές που τις ενσωματώνουν[12]. Τα βασικά αυτά χαρακτηριστικά του διαδικτύου των πραγμάτων κάνουν ώστε, τόσο οι χρήστες να επωφελούνται από την απομακρυσμένη λειτουργικότητα που το internet of Things προσφέρει, αλλά ταυτόχρονα και οι δυνάμει επιτιθέμενοι να εφευρίσκουν τρόπους ώστε να αξιοποιήσουν το remoteness υπέρ αυτών[13].

✓ Εν συντομία, καθώς η στόχευση του παρόντος πονήματος είναι πιο συγκεκριμένη, μπορεί να αναφερθεί πως μεταξύ άλλων υφίστανται τρεις κύριες κατηγορίες κυβερνοαπειλών (Ahmad et al.), ήτοι άρνηση υπηρεσιών ("*DoS, denial of service attacks*", availability), αλλοίωση περιεχομένου των δεδομένων ("*data manipulation*", integrity), μη εξουσιοδοτούμενη αποκάλυψη περιεχομένου ("*data manipulation*", confidentiality[14]).

✓ Η τυπική αρχιτεκτονική των κυβερνοεπιθέσεων έναντι του διαδικτύου των πραγμάτων περιλαμβάνει συνήθως την ανακάλυψη και επιλογή των συσκευών που θα γίνουν δέκτες της επιθέσεως (attack vectors) μέσα από μια διευρυμένη επιφάνεια πιθανής επιθέσεως (attack surface) λόγω και του σημαντικού βαθμού ενσωμάτωσης τους στις εγκαταστάσεις των κρίσιμων υποδομών. Δεύτερον, τον εντοπισμό πιθανών σημείων τρωτότητας (vulnerabilities) σε μια ή σε κάποιες από τις συσκευές του διαδικτύου των πραγμάτων που τίθενται σε λειτουργία (μια τέτοια ανακάλυψη σαφώς διευκολύνεται από την συνεχή, συνήθως, λειτουργία τέτοιων συσκευών εντός μιας υποδομής). Τρίτον, την δυνατότητα του επιτιθέμενου να συνδεθεί σε μια (ή διάφορες) από τις συσκευές αυτές, καθώς η λειτουργικότητα τους έγκειται σε μεγάλο βαθμό στην συνδεσιμότητα τους (connectivity), διαμέσου επισφαλών καναλιών ή πρωτοκόλλων επικοινωνίας, ώστε να

Wireless Communications and Mobile Computing, 2022, 1-12, σ.1. doi: The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks (hindawi.com). WCMC_8669348 1..12 (hindawi.com) (Τελευταία πρόσβαση 23/11/2022).

[12] Ο.π.

[13] Ο.π.,σ.2.

[14] Ο.π.

είναι σε θέση να στείλει εντολές προς το κακόβουλο λογισμικό που θα έχει εγκαταστήσει σε κάποια IoT συσκευή (-ές), εκμεταλλευόμενος τις όποιες τρωτότητες της, για να αποσπάσει εν τέλει τις πληροφορίες που αναζητά[15].

✓ Εκτός από τις καταγεγραμμένες τρωτότητες που επιτρέπουν στις συσκευές αυτές να γίνουν στόχος των επιτιθέμενων (δυσκολία στην προστασία τους, απουσία φιλικής προς τον χρήστη διεπαφής, δυσχέρεια στην συνεχή αναβάθμιση τους κλπ),ένα ακόμα στοιχείο που τις συνδέει συγκεκριμένα με τις SCAs, και επομένως αποτελεί τμήμα της συμβολής και της παρούσας διπλωματικής εργασίας(αν και το εν λόγω στοιχείο έχει βεβαίως αναφερθεί προηγουμένως και από την διεθνή βιβλιογραφία), είναι η χρήση των συσκευών αυτών ως ενδιάμεσων για να πληγούν έτερες συσκευές στόχοι (hopping όπως γίνεται πιο αναλυτικά λόγος και σε επόμενα κεφάλαια).Αυτό συμβάλλει σημαντικά στην ευελιξία που παρουσιάζουν οι SCAs έναντι τέτοιων στόχων (και) εντός των κρίσιμων υποδομών ευλόγως[16].

✓ Οι δυνατότητες διασύνδεσης και απομακρυσμένων λειτουργιών των IoT συσκευών όλο και περισσότερο εμπλέκουν (και) τις κρίσιμες υποδομές, στον βαθμό που τείνουν να αλληλοεπιδρούν όλο και περισσότερο με τα κυβερνό-φυσικά συστήματα (cyber-physical systems) που ευρίσκονται σε πολλές βιομηχανίες (π.χ. στον τομέα ιατρικής περιθάλψεως κλπ). Έτσι στην περίπτωση του επονομαζόμενου IIoT (Industrial Internet of Things) πέρα από την ύπαρξη πολλαπλών συσκευών, συστημάτων και αισθητήρων, αναφύεται επίσης το στοιχείο μιας αρχιτεκτονικής πολλαπλών επιπέδων (layers) υφίστανται πολλά πρωτόκολλα επικοινωνίας που επικοινωνούν με το επίπεδο του υλικού (hardware level) για την μεταφορά πληροφοριών, αλλά και αντιστρόφως υφίστανται πολλά πρωτόκολλα επικοινωνίας στο επίπεδο του δικτύου (network level) προς τα οποία αποστέλλει την επικοινωνία του το επίπεδο του υλικού[17]. Επομένως, εδώ ο λόγος γίνεται για την συνύπαρξη του υλικού με το ψηφιακό «*περιβάλλον*», και άρα οι όποιες απειλές επηρεάζουν τον ένα πόλο δύνανται όπως μεταφερθούν και στον έτερο

[15] Ο.π.

[16] Ο.π,σ.2-3.

[17] Jiang, W.(2022). Machine Learning Methods to Detect Voltage Glitch Attacks on IoT/IIoT Infrastructures. *Computational Intelligence and Neuroscience*, 22, 1-7, σ.1. doi: Machine Learning Methods to Detect Voltage Glitch Attacks on IoT/IIoT Infrastructures | Computational Intelligence and Neuroscience (acm.org). 6044071.pdf (hindawi.com) (Τελευταία πρόσβαση 23/11/2022).

(π.χ. software & physical SCAs, για την ταξινόμηση εν γένει ακολουθεί, στο επόμενο κεφάλαιο, ξεχωριστή ανάλυση[18]).

- ✓ Στο πλαίσιο της τέταρτης βιομηχανικής επαναστάσεως (Industry 4.0), και αυτό αντανακλά απευθείας στις κρίσιμες υποδομές και σε ότι ενσωματώνουν, εμφανίζεται και ενισχύεται η ετερογένεια των συστημάτων που συνυπάρχουν ενσωματωμένα (integration) στις εκάστοτε διαδικασίες παραγωγής (π.χ. πομποδέκτες που ενσωματώνουν με αναλογικό-ψηφιακό σήμα, συνδυαστικά κυκλώματα δυναμικής τροφοδοσίας κλπ). Αυτή η ετερογένεια της τέταρτης βιομηχανικής επαναστάσεως οδηγεί συνεπώς στην επαύξηση της επιφάνειας επιθέσεως για τις SCAs, στην ενίσχυση της δυνατότητας συνδυασμού των SCAs (η διπλωματική εργασία δεν θα επεκταθεί ιδιαίτερα σε αυτό το σκέλος), και επίσης στην επαύξηση της ευελιξίας των επιθέσεων αυτών, μέσα από την δυνατότητα του επιτιθέμενου να αξιοποιήσει διαφορετικές εκροές που είναι το απότοκο της ετερογένειας, της διαλειτουργικότητας και εν τέλει του συνδυασμού των συσκευών και λοιπών assets που τίθενται κάτω από την ομπρέλα του IoT[19].

  Αυτό αποτελεί και τμήμα της συμβολής της ανά χείρας διπλωματικής και αποκρυσταλλώνεται στην επόμενη ενότητα σε σειρά παραδειγμάτων, όπου αναλύονται οι SCAs έναντι των IoT συσκευών και των ενσωματωμένων συστημάτων με μια δυνάμει (ενδεχομένως μικρή με βάσει ότι επιτρέπει η υπάρχουσα βιβλιογραφία που συλλέχθηκε και μελετήθηκε) αναφορά σε εκάστοτε κρίσιμες υποδομές.

Καθώς το κύριο τμήμα της βιβλιογραφίας που μελετήθηκε διακρίνεται, κατά βάση, σε μελέτες που αφορούν σε IoT συσκευές (π.χ. android κινητά) και επίσης σε εφαρμοσμένα συστήματα, π.χ. SCADA systems κλπ. Αν και τα ενσωματωμένα συστήματα αποτελούν τμήμα του διαδικτύου των πραγμάτων, και επομένως οι ως άνω παρατηρήσεις για την συμβολή της διπλωματικής εργασίας ήδη περιλαμβάνουν μνεία και σε αυτά, αξίζει για λόγους αυτής της ίδιας της συμβολής να παρατεθούν ορισμένες παρατηρήσεις συγκεκριμένα για τα εν λόγω συστήματα (embedded systems):

- ✓ Ένας αρκετά γενικευτικός, αλλά εντούτοις πολύ περιεκτικός για του σκοπούς της παρούσας υπό-ενότητας, ορισμός για τα ενσωματωμένα συστήματα (embedded systems) είναι ο ακόλουθος, «*Ένα ενσωματωμένο σύστημα είναι ένα σύστημα υλικού και λογισμικού επί τι βάσει μικροεπεξεργαστών-ή μικροελεγκτών- σχεδιασμένο για*

[18] Ο.π.

[19] Ο.π.,σ.2.

να εκτελεί συγκεκριμένες λειτουργίες εντός του πλαισίου ενός ευρύτερου μηχανικού ή ηλεκτρονικού συστήματος (η μετάφραση είναι του συγγραφέως)[20]».

✓ Τα ενσωματωμένα συστήματα εν γένει παρουσιάζουν τις τρωτότητες που αναφέρθηκαν και ανωτέρω (απουσία διεπαφής φιλικής προς τον χρήστη, δυσχέρεια στην αναβάθμιση κλπ) αλλά και σε ότι αφορά το έτερο αντικείμενο αυτού του πονήματος (SCAs με έμφαση στο IoT και τα embedded systems) και την συμβολή αυτού, παρουσιάζουν ακόμα μια υψηλή συσχέτιση με τους περιβαλλοντικούς παράγοντες όπως η θερμοκρασία σε έναν χώρο εντός του οποίου λειτουργούν.

Γενικά, και αυτό φυσικά είναι μόνο μια πτυχή του ζητήματος, ενσωματωμένα συστήματα όπως smart chips ή FPGAs μπορούν να παρουσιάσουν αλλοιώσεις στην εύρυθμη λειτουργία τους αν υπερθερμανθούν (παραδείγματα σχετιζόμενα με τον περιβάλλοντα χώρο ακολουθούν σε επόμενο κεφάλαιο), με αποτέλεσμα οι SCAs και η σχέση τους με το IoT να πρέπει να μελετηθεί και σε συνδυασμό με την χωροθέτηση και τις συμπεριφοριστικές συνήθειες του ανθρώπινου δυναμικού εντός μιας οποιασδήποτε κρίσιμης υποδομής[21] (CI, τονίζεται εξαρχής ότι τέτοιες περιπτώσεις μόνο ακροθιγώς θίγονται στην παρούσα εργασία λόγω ελλείψεως αντίστοιχων, εκτεταμένων, ευρημάτων στην βιβλιογραφία που συγκεντρώθηκε και μελετήθηκε, οι συγκεκριμένοι παράγοντες παρόλ' αυτά ελήφθησαν υπόψη και για τις επιθέσεις και για τα αντίμετρα στα οικεία κεφάλαια).

✓ Η συνεισφορά της ανά χείρας διπλωματικής εργασίας έγκειται ακόμα στο ότι, και με βάσει βεβαίως τα προαναφερθέντα σημεία, επιχειρεί να αναδείξει μια διαρκώς αυξανόμενη τάση που ενυπάρχει στην διεθνή βιβλιογραφία για την συνδυαστική χρήση SCAs και βαθιάς μαθήσεως (Deep Learning), ούτως ώστε να διενεργηθεί μια κυβερνοεπίθεση έναντι των συσκευών του IoT. Σε ότι αφορά τα παραδείγματα των κρίσιμων υποδομών (που μόνο ελάχιστα θίγει η βιβλιογραφία που μελετήθηκε, αντίθετα το βάρος πέφτει στις μελέτες περιπτώσεως που περιλαμβάνουν κυρίως το IoT) ένας σχετικά διευρυμένος όγκος της βιβλιογραφίας αφιερώνεται σε template και

[20] χ.σ.(χ.χ.). Embedded System Definition. *HEAVY.AI*. What is an Embedded System? Definition and FAQs | HEAVY.AI (Τελευταία πρόσβαση 24/11/2022).

[21] Πρβλ. Hasnain, A., & Asfia, Y., & Khawaja, S.G.(2022). *Power profiling-based side-channel attacks on FPGA and Countermeasures: A survey*. Paper presented at the 2022 2nd International Conference on Digital Futures and Transformative Technologies (ICoDT2). Rawalpindi, Pakistan. May 24-26, 1-8, σ.1. doi: 10.1109/ICoDT255437.2022.9787473. FPGA-Based Remote Power Side-Channel Attacks (ieee.org))(Τελευταία πρόσβαση 23/11/2022).

microarchitectural SCAs που αφορούν στην εκπαίδευση μοντέλων με χρήση τεχνικών βαθιάς μάθησης, ώστε στην συνέχεια να διενεργηθεί επίθεση σε πτυχές του λογισμικού (π.χ. Virtual Machines, Embedded Neural Networks κλπ)[22].

Αυτή η τρίτη διαφαινόμενη τάση, δίπλα στις άλλες δύο που αφορούν σε μελέτες περιπτώσεως για ευφυείς συσκευές & εφαρμοσμένα συστήματα, σχετικά με την χρήση της βαθιάς μάθησης αναδεικνύει (σε σχέση με τις συσκευές του διαδικτύου των πραγμάτων που είναι ο κυρίως στόχος) δύο σημαίνοντα στοιχεία. Αφενός, αναδεικνύει την δυνατότητα, κυρίως από πλευράς επιτιθέμενου (αλλά όχι αποκλειστικά, αν ληφθεί υπόψη και η κατασκευή αντιμέτρων από την άλλη πλευρά), να απεμπλακεί εν μέρει η διαδικασία της λήψης μετρήσεων (π.χ. «*pre-process*») από τον ανθρώπινο παράγοντα και να εναποτεθεί στον Η/Υ μέσα από την χρήση της βαθιάς μάθησης (π.χ. ενίσχυση της τάσεως για remote και non-invasive SCAs). Αφετέρου, και αυτό χαρακτηρίζει και τις τρεις τάσεις στην βιβλιογραφία που μελετήθηκε, αναδεικνύετε η ροπή προς μια απουσία scalability, διότι οι μελέτες περιπτώσεως επικεντρώνουν, σε πολύ μεγάλο βαθμό, σε μεμονωμένες συσκευές και εφαρμογές λογισμικού, με αποτέλεσμα τα μεγέθη να μην είναι ακριβώς συγκρίσιμα μεταξύ τους (π.χ. διαφορετικοί κατασκευαστές συσκευών, άρα και διαφορετικά κατασκευαστικά χαρακτηριστικά συσκευής) και άρα ο προσπορισμός νέας γνώσης (περί των προκλήσεων, μεθοδολογιών, αντιμέτρων κλπ) να μην μπορεί να ενσωματωθεί με ευχέρεια[23]. Κατωτέρω ακολουθεί η αποσαφήνιση του ετέρου στοιχείου που αφορά στο υπό μελέτη ζήτημα, ήτοι των SCAs καθαυτών.

Σε ότι αφορά στο εγχείρημα περί της εννοιολογικής αποσαφήνισης των SCAs, οι διακηρυγμένοι στόχοι είναι δύο, ήτοι :

---

[22] Επί παραδείγματι οι Picek et al. Σημειώνουν τα εξής γραφόμενα για την ποσοτική πτυχή της τάσεως αυτής στην βιβλιογραφία, «*Η έλξη και η δημοτικότητα περί της χρήσεως της βαθιάς μαθήσεως στην ανάλυση πλευρικών καναλιών τα τελευταία χρόνια είναι οφθαλμοφανής, όπως φαίνεται και στο σχ.1. Πιο συγκεκριμένα, ανευρέθηκαν 183 άρθρα τα οποία διερευνούν την ανάλυση πλευρικών καναλιών (DL-SCA) επί τη βάσει της βαθιάς μαθήσεως τα τελευταία έξι χρόνια. Ξεκάθαρα, από το 2016 όταν και έκανε την εμφάνιση του το πρώτο άρθρο το οποίο προέβαινε σε χρήση βαθιάς μαθήσεως για την διενέργεια αναλύσεως πλευρικού καναλιού, ο εν λόγω τομέας κατέστη πολύ ελκυστικός.*» (Η μετάφραση είναι του συγγραφέως). Πρβλ. Picek, S., & Perin, G., & Mariot, L., & Wu, L., & Batina, L.(2021). SoK: Deep Learning-based Physical Side-channel Attacks. *ACM Computing Surveys,* 1-33, σ.2. doi: 10.1145/3569577. SoK: Deep Learning-based Physical Side-channel Analysis (acm.org) (Τελευταία πρόσβαση 24/11/2022).

[23] Ο.π.,σ.3.

- Η προσπάθεια αποσαφήνισης της σχέσης ανάμεσα στις επιθέσεις πλευρικού καναλιού και τις κρίσιμες υποδομές. Εν άλλοις λόγοις, ποιοι είναι οι βασικοί λόγοι για τους οποίους οι επιθέσεις πλευρικού καναλιού αποτελούν ένα σημαντικό ρίσκο για τις κρίσιμες υποδομές και το οποίο επομένως πρέπει να μελετηθεί και να ληφθεί σοβαρά υπόψη.
- Δεύτερον, η ενδελεχής και κατά το δυνατόν λεπτομερειακή προσπάθεια αποσαφήνισης του εννοιολογικού προσδιορισμού που αφορά στις επιθέσεις πλευρικού καναλιού. Η ανάδειξη των επιμέρους στοιχείων που συνθέτουν τον ορισμό (ή ορθότερα τους ορισμούς) των επιθέσεων πλευρικού καναλιού είναι το πρώτο και συνάμα πλέον απαραίτητο βήμα για την μετέπειτα πληρέστερη προσπάθεια ταξινόμησης των εκάστοτε επιθέσεων σε επιμέρους κατηγορίες ώστε να είναι δυνατό να διερευνηθεί (αν όχι όλο) το μεγαλύτερο φάσμα των απειλών που θα μπορούσαν, θεωρητικά και πρακτικά, να πλήξουν την λειτουργία των εκάστοτε κρίσιμων υποδομών (σε πρώτη γραμμή των συσκευών των σχετικών με το διαδίκτυο των πραγμάτων).

Υπό-ενότητα 1.2: Η σημασία των επιθέσεων πλευρικού καναλιού (SCAs) για τις κρίσιμες υποδομές

Αναφορικά με τον πρώτο στόχο θα πρέπει να αποσαφηνιστούν δύο επιμέρους σημεία. Αφενός, (α) γιατί η μεθοδολογία των επιθέσεων πλευρικού καναλιού (side-channel attack, SCAs) εν γένει θεωρείται τόσο απειλητική για τις κρίσιμε υποδομές ; εν άλλοις λόγοις γιατί ο επιτιθέμενος να θεωρεί ότι μια επίθεση πλευρικού καναλιού θα ήταν η καταλληλότερη επιλογή για να πλήξει μια οποιαδήποτε κρίσιμη υποδομή (compatibility) ; Αφετέρου, (β) ποιο είναι εκείνο το στοιχείο (ή εκείνα τα στοιχεία) που διαφοροποιούν κατά τι τις επιθέσεις πλευρικού καναλιού έναντι κρίσιμων υποδομών, από έτερες επιθέσεις διαφορετικής μεθοδολογίας (π.χ. DDoS, Malware attacks όπως το Triton Malware attack του 2017[24], brute force attacks κλπ.) κατά των ίδιων αυτών υποδομών (differentiation) ;

[24] Για μια συνοπτική παρουσίαση του εν λόγω Malware και των συνεπειών του για τις κρίσιμες υποδομές ορά και, Weinberg,A.(2021).Analysis of top 11 cyber-attacks on critical infrastructure. *FirstPoint*.https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/ (τελευταία πρόσβαση 2/11/2021).

Συνοπτικά οι κύριοι λόγοι για τους οποίους οφείλει κανείς να μελετήσει τις επιθέσεις πλευρικού καναλιού από κοινού με τις κρίσιμες υποδομές, αναφέρονται αμέσως κατωτέρω ως εξής :

- Εν πρώτοις, οι επιθέσεις πλευρικού καναλιού παρουσιάζουν μια , υπέρ το δέον, ευρεία επιφάνεια πιθανής επιθέσεως (attack surface[25]). Ενώ άλλες κυβερνοεπιθέσεις θα εστιάσουν μόνο σε ένα τμήμα του υπολογιστικού συστήματος, συνήθως αυτό είναι το λογισμικό (π.χ. σε περιπτώσεις ransomware, Man in the Middle attacks, DDoS, brute force attacks κλπ), οι επιθέσεις πλευρικού καναλιού μπορούν να λάβουν χώρα (ανάλογα με τις αδυναμίες του υπολογιστικού συστήματος και σε συνδυασμό με τις δυνατότητες του επιτιθέμενου) πρακτικά σε οποιαδήποτε συσκευή ή λογισμικό παράγει την οποιαδήποτε εκροή (leakage).

  Οι επιθέσεις πλευρικού καναλιού μπορούν είτε κατά τρόπο επιθετικό ή απλά παθητικό να εκμεταλλευτούν την οποιαδήποτε συσκευή και την οποιαδήποτε εκροή. Ο λόγος εδώ γίνεται για εκροές (leakage) που θα μπορούσαν να είναι είτε εκούσιες (intended) είτε ακούσιες (unintended) και που μεταξύ άλλων μπορούν να είναι οπτικές (optical), ηλεκτρομαγνητικές (electromagnetic), ακουστικές (acoustic), εκροές δονήσεων (vibrations) κλπ.[26]. Ενδιαφέρον παρουσιάζει το γεγονός ότι η έννοια της εκροής είναι ιδιαιτέρως εκτεταμένη, καθώς με την συνδρομή και της μηχανικής μαθήσεως[27] (που

---

[25] Ενδεικτικά ορά και, Bursztein, E., & Picod, J-M.(2020). *A Hacker's Guide to reducing side-channel attack surfaces using deep learning.* Paper presented at the Defcon 28 & Black Hat. USA, Virtual Event (originally intended to take place in Las Vegas),August,1-9,pp.1-68,σ.16-18. https://elie.net/talk/a-hacker-guide-to-side-channel-attack-surface-reduction-using-deep-learning/ (τελευταία πρόσβαση 2/11/2021).

[26] Ορά και Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.298-301. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer. https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[27] Ενδεικτικά παραθέτουμε το ακόλουθο άρθρο όπου με την χρήση κρυφών μοντέλων του Μαρκόφ (Hidden Markov models, HMMs) και του άμεσου μετασχηματισμού του Φουριέ (Short-time, Fast Fourier Transform, SFFT) μεταξύ άλλων επιχειρείτε η καταγραφή επί χάρτου των συνταγογραφήσεων που εκτυπώνει ένα μηχάνημα εκτύπωσης, για το εν λόγω πείραμα βλέπε και, Bakes, M., & Durmuth ,M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security

συνδράμει και την εξ αποστάσεως εκτέλεση μιας SCA), μια επίθεση πλευρικού καναλιού μπορεί να εκμεταλλευτεί και εκείνες τις εκροές που ευρίσκονται εκτός του αντιληπτικού φάσματος του ανθρώπου (π.χ. χαμηλά ακουστικά κύματα, ακτινοβολία, αποτυπώματα, ασύρματη φόρτιση κινητών κλπ.[28]).

Οι εν λόγω επιθέσεις μπορούν εντός κρίσιμων υποδομών να στοχεύσουν συσκευές διαφορετικών μεγεθών (ατομικό εξοπλισμό, εξοπλισμό εγκαταστάσεων όπως οι γεννήτριες, αν και ο βαθμός δυσκολίας ποικίλει) καθώς επίσης και διαφορετικών λειτουργιών (π.χ. lightweight devices, embedded systems κλπ.), επίσης μπορούν να στοχεύσουν επιμέρους τμήματα εξοπλισμού (π.χ. κάμερες, πληκτρολόγια κλπ.[29]) ομοίως μετά των συσκευών που μπορεί να έχουν ενσωματωθεί σε μέλη του ανθρωπίνου σώματος (π.χ. ενδεχομένως κάποιοι εργαζόμενοι στην κρίσιμη υποδομή να φέρουν βηματοδότη ή βαλβίδα για λήψη ινσουλίνης[30] κλπ.).

Symposium,DC,USA,August,11-13,pp.1-16,σ.6.https://www.researchgate.net/publication/221260462_Acoustic_Side-Channel_Attacks_on_Printers (τελευταία πρόσβαση 10/10/2021).

[28] Ενδεικτικά παραθέτουμε εδώ την υποπερίπτωση των smudge attacks, όπου με έναν επαυξημένο βαθμό δυσκολίας καθώς στην περίπτωση που αναφέρουμε απαιτούνται η εγγύτητα στην συσκευή καθώς και ο εξοπλισμός ο αποτελούμενος από θερμικές κάμερες φέρ' ειπείν, γίνεται να επιτευχθεί η συλλογή θερμικών ιχνών (thermal traces) από οθόνες αφής (είτε κινητού είτε ενδεχομένως και από κάποιο πίνακα ελέγχου) ώστε με τον τρόπο αυτό να εξαχθούν στοιχεία για τα ψηφιακά πλήκτρα που πατήθηκαν (όπως γίνεται με τον κωδικό κλειδώματος στις οθόνες αφής των κινητών συσκευών). Η περίπτωση αυτή περιλαμβάνει την μελέτη εκροής θερμότητας που δεν είναι άμεσα αντιληπτή δια γυμνού οφθαλμού, και επίσης καταδεικνύει και την ευελιξία των SCAs, αφού το ίδιο αυτό τμήμα μιας συσκευής (εν προκειμένω η οθόνη) μπορεί να «προσβληθεί» με τουλάχιστον τρείς τρόπους (ήτοι optical attack, electromagnetic attack, smudge attack), όπου η εκροή είναι αντιληπτή στις ανθρώπινες αισθήσεις μόνο στην πρώτη εκ των τριών αυτών παραδειγμάτων. Για μια λεπτομερέστερη καταγραφή αυτού του υπό-τύπου SCA (smudge attack) ορά , μεταξύ άλλων και, Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,*20, 1,465-488 (1-24),σ.8-9. doi : 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[29] Ο.π.,σ.302-305.

[30] Ενδεικτικά παραθέτουμε το ακόλουθο άρθρο για τον κίνδυνο που ελλοχεύει για τις ιατρικές συσκευές και την κρίσιμη υποδομή των υγειονομικών μονάδων εν γένει εξαιτίας των επιθέσεων πλευρικού καναλιού. Pycroft, L., & Aziz, T.Z.(2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices,15:6,* 403-406,σ.404.https://www.tandfonline.com/doi/pdf/10.1080/17434440.2018.1483235?needAccess=true (τελευταία πρόσβαση 12/10/2021).

Η επιφάνεια επιθέσεως διευρύνεται έτι περαιτέρω αφενός επειδή οι επιθέσεις πλευρικού καναλιού μπορούν αξιοποιήσουν συνδυασμένες εκροές (π.χ. ακουστικές και εκροές ρεύματος), και αφετέρου επειδή μπορούν κάλλιστα να συνδυαστούν και με άλλες απειλές (π.χ. insider threat για να διευκολυνθεί η λήψη μετρήσεων), ενώ ο συνδυασμός αυτός διευκολύνεται λόγω και του μειωμένου κόστους σε ότι αφορά στον εξοπλισμό (αν και αυτή η συνθήκη δεν πληρείται εις άπασες τις περιπτώσεις[31]).

➢ Εν δευτέροις, οι επιθέσεις πλευρικού καναλιού διαθέτουν μια εκτεταμένη και ιδιαίτερα ευέλικτη αλυσίδα επίθεσης (cyber kill-chain[32]) σε ότι αφορά στον

[31] Παραμένει ένα εκ ων διαχρονικότερων παραδειγμάτων η κλασσική πλέον περίπτωση του Wim van Eck ο οποίος κατάφερε με έναν πολύ φτηνό εξοπλισμό της τάξεως των 15 δολαρίων να προχωρήσει σε επιτυχή εξαγωγή μετρήσεων ηλεκτρομαγνητικής εκροής, για μια πολύ συνοπτική καταγραφή της ιστορικής καταγραφής των SCAs ορά και Liu, Z., & Samwel, N., & Weissbart, L., & Zhao, Z. & Lauret, D., & Batina, L., & Larson, M.(2020). Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. *arXiv: 2011.09877v1 [cs.CR]*,pp.1-15,σ.2. https://arxiv.org/abs/2011.09877 (τελευταία πρόσβαση 10/10/2021).

[32] Η παραδοσιακή αντίληψη για την αλυσίδα επίθεσης, όπως έχει προσαρμοστεί από την στρατιωτική ορολογία, περιλαμβάνει τα εξής πέντε στάδια: Reconnaissance(αναγνώριση), Vulnerability Search(αναζήτηση τρωτότητας), Attack Vector Detection(εντοπισμός του σημείου επίθεσης), Attack(επίθεση), Trace Removal(αφαίρεση ίχνους). Για μια σύντομη επεξήγηση του κάθε σταδίου ορά , μεταξύ άλλων και, Staddon, E., & Loscri, V., & Mitton, N.(2021). Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Applied Sciences,2021,11,7228,* pp.1-39,σ.5-6. doi: https://doi.org/10.3390/app11167228. Applied Sciences | Free Full-Text | Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey (mdpi.com) (τελευταία πρόσβαση 16/9/2021). Αν και ο χώρος δεν επαρκεί για μια εις βάθος ανάλυση, μπορεί ίσως να ειπωθεί πως οι επιθέσεις πλευρικού καναλιού ίσως και να τροποποιούν κατά τι το σχήμα αυτό για διάφορους λόγους, όπως το ότι εκμεταλλεύονται εκροές και άρα δεν χρειάζεται να υπάρχει πάντα το πέμπτο στάδιο (Trace Removal). Επίσης, όπως θα ειπωθεί και παρακάτω, οι επιθέσεις πλευρικού καναλιού εστιάζουν σε εκροές από τον τρόπο εφαρμογής (ήτοι implementation) και επομένως δεν χρειάζεται να εκμεταλλευτούν απαραιτήτως κάποια αδυναμία (vulnerability), οπότε από την αναγνώριση μπορούν να περάσουν πιο άμεσα στην επίθεση. Τέλος, μπορεί να αναφερθεί ακόμα το γεγονός ότι, αφενός οι attack vectors μπορούν να είναι πολλοί και να αξιοποιούνται ταυτόχρονα, και αφετέρου πως οι συσκευές μπορούν να χρησιμοποιούνται σε συνδυαστικές επιθέσεις όπου ανάμεσα στον vector και την καθαυτό επίθεση (attack) να παρεμβάλλεται, μέσω μιας SCA, και ένα ακόμα στάδιο reconnaissance που θα αξιοποιεί μια συσκευή για να προσβληθεί και μια άλλη (για ένα παράδειγμα ορά την υποσημείωση 17 και το αντίστοιχο άρθρο που εκεί παραθέτουμε ως ενδεικτική πηγή βιβλιογραφίας). Αυτό, μεταξύ άλλων, σημαίνει πως ο ένας attack vector μπορεί να λειτουργήσει ως όχημα για την ενίσχυση μιας υπάρχουσας εκροής και μέσω αυτής της ενισχύσεως να γίνει η μετάβαση στον επόμενο attack vector. Πρβλ. Liu, Z., & Samwel, N., & Weissbart, L., & Zhao, Z. & Lauret, D., & Batina, L., & Larson, M.(2020). *Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel*. A paper presented at The Network and Distributed System Security

σχεδιασμό και στην εκτέλεση του κάθε ξεχωριστού υπό-τύπου επιθέσεως. Η ευελιξία[33] αφορά στην εναλλαγή ανάμεσα στην εγγύτητα και στην απόσταση που μπορεί να διατηρήσει ο επιτιθέμενος, αλλαχού, εν σχέση με την συσκευή στην οποία επιθυμεί να επιτεθεί. Το εύρος επιλογών και σχεδιασμού είναι ως εκ τούτου αρκετά διευρυμένο εν σχέση και με τις άλλες επιθέσεις[34].

Αν για παράδειγμα λάβουμε υπόψη μια και μόνη εκροή (π.χ. κατανάλωση ρεύματος), υπάρχουν περισσότεροι του ενός τρόπου για να την εκμεταλλευτούν οι επιθέσεις πλευρικού καναλιού. Στο συγκεκριμένο παράδειγμα, είτε ο επιτιθέμενος θα επιχειρήσει να μετρήσει (simple power analysis, differential power analysis) την κατανάλωση ρεύματος μιας συσκευής φέρ' ειπείν (ενός κινητού), είτε θα μπορούσε κάλλιστα να μετρήσει την παροχή ρεύματος από μια πηγή φόρτισης (π.χ. wireless hub) στην οποία προσφάτως είχε συνδεθεί η εν λόγω συσκευή[35]. Επομένως η αλυσίδα επιθέσεως και η ευελιξία αυτής σε μεγάλο βαθμό σχετίζονται όχι με την ασφάλεια την

Symposium (NDSS) 2021. Virtual venue. 21-25 February,1-15,σ.2. https://arxiv.org/abs/2011.09877 (τελευταία πρόσβαση 10/10/2021).

[33] Ενδεικτικά ορισμένα πιθανοί στόχοι των SCAs περιλαμβάνουν τα πρωτόκολλα κρυπτογραφίας, τις διάφορες συσκευές, τα εφαρμοσμένα συστήματα, τα πρωτόγονα (primitives), τα ενθέματα κα. Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.307. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[34] Για ένα τέτοιο παράδειγμα προσαρμοστικότητας/ευελιξίας ορά και Phan, Q-S., & Bang, L., & Pasareanu, C.S., & Malacaria, P., & Bultan, T.(2017). *Synthesis of Adaptive Side-Channel Attacks.* Paper presented at the 2017 IEEE 30th Computer Security Foundations Symposium (CSF). Santa Barbara,CA,USA, August,21-25,pp.1-15,σ.2 κε. https://eprint.iacr.org/2017/401.pdf (τελευταία πρόσβαση 16/9/2021).

[35]Ορά και Pycroft, L., & Aziz, T.Z.(2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices,15:6,* 403-406,σ.8 κε.https://www.tandfonline.com/doi/pdf/10.1080/17434440.2018.1483235?needAccess=true (τελευταία πρόσβαση 12/10/2021).

σχετική με μια υποδομή ή ένα κρυπτοσύστημα[36], αλλά αντίθετα με τον τρόπο που όλα αυτά εφαρμόζονται και με το αν η εφαρμογή αυτή είναι η ορθή (implementation[37][38]).

- Εν τρίτοις, οι επιθέσεις πλευρικού καναλιού παρουσιάζουν έναν εκτεταμένο πολυμορφισμό. Αν στην παραδεδεγμένη αντίληψη για τις κυβερνοεπιθέσεις πρέπει να υφίσταται μια αδυναμία (vulnerability) που οι κυβερνοεπιθέσεις αυτές θα εκμεταλλευτούν για να πλήξουν μια υποδομή ή ένα απλό πληροφοριακό σύστημα, στην

---

[36] Πράγματι, μεταξύ άλλων πραγμάτων, ορισμένες διαφορές εν σχέση με άλλες επιθέσεις, έχουν να κάνουν και με το ότι οι άλλες επιθέσεις (πλην των SCAs, ορά και τις ακόλουθες δύο υποσημειώσεις) συνήθως (αν και η γενίκευση πρέπει να αποφευχθεί) προϋποθέτουν την εκμετάλλευση κάποιας τρωτότητας, ή/και επιδιώκουν την επαύξηση προνομίων, ή/και χρειάζεται να χρησιμοποιήσουν κάποια κακόβουλη εφαρμογή ή και κάποια ιστοσελίδα για να εκτελεστούν. Αντίθετα, οι επιθέσεις πλευρικού καναλιού δεν χρειάζονται , απαραίτητα, καμία από τις τρεις αυτές προϋποθέσεις για να εκτελεστούν επιτυχώς, οπότε αυτό αναδεικνύει και την δυνατότητα ευελιξίας που οι SCAs δύνανται να διαθέτουν. Για μια σύντομη συγκριτική παράθεση ορά και Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1 ,1-24(465-488),σ.5-6. doi: 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[37] Η ορθή εφαρμογή (ήτοι implementation) εύλογα ανάγεται σε ένα ευρύτερο επίπεδο συζητήσεως, καθότι η ίδια η έννοια της περί του ορθού εφαρμογής εξαρτάται από πλήθος μεταβλητών που επηρεάζουν την ίδια την ασφάλεια των κρίσιμων υποδομών εν γένει. Πρόκειται για την συσχέτιση μεταξύ ασφάλειας και , εν πολλοίς, λειτουργικότητας των συστημάτων και των εφαρμογών, που με την σειρά της υπόκειται και καθορίζεται από πλήθος μεταβλητών όπως η ύπαρξη προτύπων (standards) στην εκάστοτε βιομηχανία κατασκευαστών, στην ακαδημαϊκή και όχι μόνο συμφωνία περί ορισμών και θεωρητικών σχημάτων (π.χ. τι ορίζεται ως security, αν υπάρχουν ή μπορεί να συγκροτηθούν ασφαλείς γλώσσες προγραμματισμού, information-theoretic security έναντι της computational security κλπ), στις προθεσμίες που τίθενται για την κατασκευή και παράδοση του υλικού ή την έκδοση ενός πακέτου λογισμικού, το κόστος παραγωγής κλπ. Ενδεικτικά για τις δυσκολίες σε ότι αφορά την ορθή εφαρμογή αλγορίθμων κρυπτογράφησης για την μείωση των πιθανοτήτων επιτυχούς εκτέλεσης μια επιθέσεως πλευρικού καναλιού, ορά μεταξύ άλλων και για πιθανά αντίμετρα (countermeasures), Socha, P., & Novotny, M.(2020). *Towards High-Level Synthesis of Polymorphic Side-Channel Countermeasures.* Paper presented at the 2020 23rd Euromicro Conference on Digital System Design(DSD). Slovenia, Kranj. August,26-28, 1-7, σ.2. doi:10.1109/DSD51259.2020.00040 https://ieeexplore.ieee.org/document/9217858/authors#authors (τελευταία πρόσβαση 3/11/2021). Όπως επίσης και, Zhang, L., & Hu, W., & Ardeshiricham, A., & Tai, Y., & Blackstone, J., & Mu, D., & Kastner, R.(2018). *Examining the Consequences of High-Level Synthesis Optimizations on Power Side-Channel.* Paper presented at the 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE). Dresden, Germany. March, 19-23,1-4,σ.1. doi: 10.23919/DATE.2018.8342189. https://ieeexplore.ieee.org/document/8342189/authors#authors (τελευταία πρόσβαση 4/11/2021).

[38] Ορά και Lake, J.(2021). What is a side-channel attack and how do they work ? *comparitech*. https://www.comparitech.com/blog/information-security/side-channel-attack/ (τελευταία πρόσβαση 3/11/2021).

περίπτωση των επιθέσεων πλευρικού καναλιού η αδυναμία μπορεί να υφίσταται αλλά μπορεί και μια τέτοια συνθήκη (τουλάχιστον αφετηριακά) να μην είναι απαραίτητη.

Ούτως ειπείν, τα συστήματα εντός των κρισίμων υποδομών θα παράγουν κάποιου είδους εκροή ως φυσική απόρροια της ίδιας τους της λειτουργίας (π.χ. ένας οποιοσδήποτε υπολογιστής θα παράγει κάποια ακουστική εκροή, είτε κάποια ηλεκτρομαγνητική εκροή, είτε κάποια εκροή θερμότητας, είτε κάποια οπτική εκροή σχετική με την εκπομπή φωτεινότητας και ούτω καθεξής). Επομένως, και χωρίς να αποκλείονται οι λανθάνουσες εκροές (unintended leakages[39]) που θα αποτελούσαν καθαυτές μια αδυναμία (vulnerability), οι επιθέσεις πλευρικού καναλιού δεν μπορούν να προληφθούν εξ' ολοκλήρου μέσα από την εξάλειψη αδυναμιών[40] ενός τμήματος είτε του υπολογιστικού συστήματος είτε της κρίσιμης υποδομής (ή εν τω συνόλω αυτής[41]). Αντίθετα, ο

[39] Αν και θα αναπτυχθεί εκτενώς και κατωτέρω, οι έννοιες αυτές χρήζουν περαιτέρω αποσαφηνίσεως, καθότι στην προκειμένη περίπτωση ο όρος unintended/ακούσιος δεν προσδιορίζει επιθετικά μόνο τον όρο εκροή/πληροφορία, αλλά σε τουλάχιστον μια περίπτωση χρησιμοποιήθηκε για να περιγράψει λειτουργικά χαρακτηριστικά συσκευής που τείνουν εις ορισμένες περιπτώσεις να συμπεριφέρονται κατά τρόπο "ακούσιο", δηλαδή όταν μπορούν να χρησιμοποιηθούν από τον επιτιθέμενο με τρόπο τέτοιο που να τον ενισχύσουν στην εκτέλεση μιας επιθέσεως πλευρικού καναλιού, ενδεικτικά παραθέτουμε την κάτωθι αποστροφή από το άρθρο των Marquardt et al "*Όλο και περισσότερο οι κινητές συσκευές τείνουν να εξοπλίζονται με μια ευρεία γκάμα αισθητήρων υψηλής αποκρίσεως. Από τις κάμερες και την λειτουργία GPS μέχρι τα τριαξονικά επιταχυνσιόμετρα, οι εφαρμογές που τρέχουν σε αυτές τις συσκευές βρίσκονται εις θέση να αλληλοεπιδράσουν με το περιβάλλον τους με μια πληθώρα διαφορετικών τρόπων. Όλος ατυχώς, κάποιες εφαρμογές μπορεί να είναι εις θέσην να χρησιμοποιήσουν τέτοιους αισθητήρες για να επιτηρήσουν τον περιβάλλοντα χώρο τους κατά τρόπο μη επιδιωκόμενο/ακούσιο (unintended)"* (η μετάφραση είναι του ίδιου του συγγραφέα). Ορά σχετικά Marquardt, P., & Verma, A., & Carter, H., & Traynor, P.(2011).*(sp) iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers* . Paper presented at the proceedings of the 18th ACM Conference on Computer and Communications Security, CSS 2011. Chicago, Illinois ,USA. October, 17-21,2011,σ.1.DOI:10.1145/2046707.2046771. (sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers | Request PDF (researchgate.net) (τελευταία πρόσβαση 05/01/2021).

[40] Στο σημείο αυτό δέον όπως αναλογιστούμε περισσότερο τις επιθέσεις πλευρικού καναλιού που λαμβάνουν χώρα στο υλικό (hardware), και λιγότερο ίσως εκείνες που θα στοχεύουν στο λογισμικό (software), ώστε να είναι περισσότερο κατανοητό το εν λόγω σημείο. Σε κάθε περίπτωση όμως η συνδυαστική στόχευση και των δύο δεν δύναται να αποκλειστεί εις καμία περίπτωση.

[41] Ενδεχομένως το σημείο αυτό είναι περισσότερο περίπλοκο, καθώς οι SCAs σε έναν βαθμό προκαλούνται από την εφαρμογή (implementation) του υλικού όπως έχει ήδη αναφερθεί. Τα μέτρα που λαμβάνονται γενικά για την πρόληψη επιθέσεων πρέπει να λάβουν υπόψη την σχέση ασφάλειας και επιδόσεως (security έναντι performance). Όπως δείχνει, φέρ' ειπείν, η περίπτωση των microarchitectural attacks όσο περισσότερο βελτιώνεται η επίδοση (π.χ. multithreading) τόσο αυξάνουν οι πηγές των εκροών και άρα η επιφάνεια επιθέσεως των SCAs.

πολυμορφισμός τους σχεδόν επιβάλλει την προστασία του οικείου περιβάλλοντος[42][43] εντός του οποίου λειτουργεί ένα οποιοδήποτε σύστημα ομού μετά της ανάγκης για εξάλειψη των όποιων αδυναμιών μπορεί να εμφανίζει ένα υπολογιστικό σύστημα ή ένα τμήμα μιας κρίσιμης υποδομής.

Αυτή η παρατήρηση δείχνει επίσης, όπως θα καταδειχθεί και κατωτέρω, πως οι εκροές δεν είναι πάντα unintended αλλά μπορεί κάλλιστα να δημιουργούνται επί σκοπού κατά μια έννοια, καθότι οι βελτιώσεις που αυξάνουν τις εκροές (leakages) είναι ως εκ τούτου ηθελημένες. Για ένα τέτοιο παράδειγμα (microarchitectural attacks) βλ. σχετικά, Lou, X., & Zhang, T., & Jiang, J., Zhang, Y.(2021). A Survey of Microarchitectural Side-channel Vulnerabilities, Attacks, and Defenses in Cryptography. *ACM Computing Surveys, 54(6),* 1-37,σ.1. doi: 10.1145/3456629. https://arxiv.org/pdf/2103.14244.pdf (τελευταία πρόσβαση 29/11/2021).

[42] Ένα παραδεδεγμένο αντίμετρο (countermeasure) για την προστασία έναντι των SCAs που στοχεύουν στις ηλεκτρομαγνητικές εκροές είναι να υπάρχει κάποιας μορφής masking. Ήτοι, μια προσπάθεια αποτροπής του επιτιθέμενου από το να μπορέσει να αποσπάσει ο τελευταίος ακριβείς μετρήσεις για την τάση κατανάλωσης ρεύματος ενός υπολογιστικού συστήματος, μέσω του masking επιχειρείτε να διαρραγεί η συσχέτιση ανάμεσα στις παρατηρήσεις που προκύπτουν από τις μετρήσεις και τις μέσες τιμές (intermediate values) που οι μετρήσεις προσπαθούν να ανακαλύψουν, αυτό επιτυγχάνεται μέσα από κατάτμηση των ευαίσθητων τιμών σε μικρότερα μέρη (shares). Για μια συνοπτική περιγραφή ορά και Courousse, D., & Barry, Th., & Robisson, B., & Jaillon, P., & Potin, O., & Lanet, J.-J.(2016). *Runtime Code Polymorphism as a Protection Against Side Channel Attacks.* Paper presented at the 10th IFIP WG 11.2 International Conference on Information Security Theory and Practice (WISTP 2016).Greece,Heraklion.September,26-27,1-16,σ..doi:10.1007/978-3-319-45931-8_9.https://www.researchgate.net/publication/308278270_Runtime_Code_Polymorphism_as_a_Protection_Against_Side_Channel_Attacks (τελευταία πρόσβαση 3/11/2021).

[43] Εδώ πρέπει να επισημανθεί πως η χωρική διάσταση της έννοιας του περιβάλλοντος δεν περιορίζεται μόνο στην χωροθέτηση των υλικών στοιχείων και του προσωπικού της οποιασδήποτε κρίσιμης υποδομής (π.χ. στρατιωτικές βάσεις, φράγματα, νοσοκομεία κλπ), αλλά αντιθέτως φρονούμε πως μπορεί να επεκτείνεται και στην λειτουργικότητα των επιμέρους τμημάτων που συνθέτουν τις μηχανές και τα υπολογιστικά συστήματα (π.χ. ένα μικροτσίπ). Έτσι για παράδειγμα ένας τρόπος προστασίας κατά επιθέσεων πλευρικού καναλιού είναι (και) το εγχείρημα μετατοπίσεως της διαρροής πληροφοριών τόσο χρονικά όσο και χωρικά (ήτοι τεχνική hiding). Σε αυτή την περίπτωση η χωρική διάσταση αφορά σε μετατόπιση της δραστηριότητας που λαμβάνει χώρα εντός ενός μικροτσιπ (hardware, λογικά εδώ μπορούμε να φανταστούμε την λειτουργία ενός embedded συστήματος κλπ) όπως συμβαίνει κατά το run-time ενός δείγματος κώδικα (code script). Για μια περιεκτική αναφορά πάνω στην χωρική διάσταση όπως αναφέρθηκε ανωτέρω, αλλά και σε ότι αφορά την τεχνική hiding, παραθέτουμε μεταξύ άλλων και το ακόλουθο άρθρο, Courousse, D., & Barry, Th., & Robisson, B., & Jaillon, P., & Potin, O., & Lanet, J.-J.(2016). *Runtime Code Polymorphism as a Protection Against Side Channel Attacks.* Paper presented at the 10th IFIP WG 11.2 International Conference on Information Security Theory and Practice (WISTP 2016). Greece, Heraklion. September,26-27,1-16,σ.2.doi:10.1007/978-3-319-45931-8_9. https://www.researchgate.net/publication/308278270_Runtime_Code_Polymorphism_as_a_Protection_Against_Side_Channel_Attacks (τελευταία πρόσβαση 3/11/2021).

Τούτου δοθέντος, ο πολυμορφισμός των επιθέσεων πλευρικού καναλιού ενέχει (εν αντιθέσει με άλλες επιθέσεις) το επιπλέον στοιχείο της αξιοποίησης τρίτων συσκευών που βρίσκονται πλησίον έτερης συσκευής, ώστε να πλήξουν αυτή την τελευταία (devices in vicinity[44]). Αν και άλλες επιθέσεις μπορούν να πραγματοποιήσουν κάτι το αντίστοιχο (π.χ. ένας οποιοδήποτε μολυσμένο αρχείο ή κινητό κομμάτι κώδικα που εν συνεχεία θα μεταφορτωθεί από την μια συσκευή στην άλλη), εντούτοις οι επιθέσεις πλευρικού καναλιού παρουσιάζουν δύο επιπρόσθετα πλεονεκτήματα ως προς το σχήμα επιθέσεως αυτό.

Πρώτον, μπορούν να εκμεταλλευτούν την ύπαρξη πολλαπλών συσκευών, χωρίς οι συσκευές αυτές να έρθουν σε, ενσύρματη ή ασύρματη, επαφή μεταξύ τους[45] (π.χ.

---

[44] Αναφερόμαστε στο ζήτημα αυτό και κατωτέρω, αλλά και εδώ η έννοια vicinity μπορεί να είναι ολίγον διφορούμενη, συνήθως αναφέρεται στην εγγύτητα υπολογιστικού συστήματος-επιτιθέμενου, όμως φρονούμε πως μπορεί σε κάποιες περιπτώσεις να αναφέρεται κάλλιστα και στην εγγύτητα συσκευών μεταξύ τους ή στην εγγύτητα μεταξύ συσκευής και δικτύου. Επί παραδείγματι, οι Ali et al επιχείρησαν να καταδείξουν πως ο συνδυασμός κίνησης και ηχητικής εκροής από την πίεση των πλήκτρων σε ένα πληκτρολόγιο δύναται όπως προκαλέσει παρεμβολές (distortion) στην εκπομπή των σημάτων του ασύρματου δικτύου (Wi-Fi) εντός του οποίου βρίσκεται το υπολογιστικό σύστημα μετά του πληκτρολογίου αυτού. Ali et al στο Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1, 465-488 (1-24),σ.11. doi:10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021). Τέλος δε να σημειωθεί πως, όπως θα καταδειχθεί και κατωτέρω, η τεχνολογική πρόοδος (π.χ. ασύρματα δίκτυα, IoT συσκευές κλπ.) φέρνει και νεοπαγή χαρακτηριστικά και ζητήματα ασφαλείας, όπως είναι η αλληλεξάρτηση των εκάστοτε συσκευών (interdependence), και επομένως η έννοια vicinity (αν και δεν αναφέρεται στο παρακάτω άρθρο) μπορεί κάλλιστα να επεκταθεί και να συμπεριλάβει την έννοια interdependence. Για τον όρο interdependence ως μια εκ των αρχών επί της ασφάλειας των IoT συσκευών ορά και, Staddon, E., & Loscri, V., & Mitton, N.(2021). Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Applied Sciences,2021,11,7228,* pp.1-39,σ.7. doi: https://doi.org/10.3390/app11167228. Applied Sciences | Free Full-Text | Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey (mdpi.com) (τελευταία πρόσβαση 16/9/2021).

[45] Όχι μόνο μπορεί να υπάρχει απουσία διασύνδεσης, αλλά οι συσκευές που θα δεχθούν την επίθεση πλευρικού καναλιού μπορούν κάλλιστα να έχουν και πολύ διαφορετικά μεταξύ τους τεχνικά στοιχεία, κάτι που μας υπενθυμίζει εκ νέου το μεγάλος εύρος της επιφανείας επιθέσεως που ενέχουν οι SCAs. Στο παράδειγμα που επιλέγουμε να παραθέσουμε, αρκεί να αντικαταστήσουμε το μικρόφωνο με μια κινητή συσκευή (π.χ. android, Apple κλπ.) που θα υπάρχει πλησίον ενός, κατά τ' άλλα, πεπαλαιωμένου εκτυπωτή, για να καταστεί εφικτό ο επιτιθέμενος να διενεργήσει μια επίθεση πλευρικού καναλιού που θα εκμεταλλευτεί το ενσωματωμένο μικρόφωνο του κινητού, ώστε κατόπιν να καταγράψει την ηχητική εκροή του εκτυπωτή, και εν συνεχεία με την χρήση της μηχανικής μάθησης (με ένα trained model) να είναι εις θέση να ανασυγκροτήσει (κατά το μάλλον ή ήττον) το κείμενο που εκτυπώθηκε, και έτσι να αντλήσει τις πληροφορίες που επιθυμεί. Ορά το ακόλουθο παράδειγμα (όπου υπενθυμίζεται

χωρίς να ανταλλάξουν κάποιο αρχείο, ή χωρίς αυτές να βρίσκονται απαραιτήτως εντός δικτύου κλπ). Δεύτερον, οι επιθέσεις αυτές δύνανται να στοχεύσουν και έτσι να εκμεταλλευτούν όχι την διασύνδεση των επιμέρους τμημάτων μιας υποδομής ή ενός υπολογιστικού συστήματος, αλλά αντίθετα τις διαφορετικές εκροές των πλέον διαφορετικών συσκευών που θα ευρίσκονται εντός μιας εύλογης απόστασης μεταξύ των[46].

Υπό-ενότητα 1.3: Η εννοιολογική αποσαφήνιση περί των επιθέσεων πλευρικού καναλιού (SCAs)

Στο δεύτερο μέρος με το οποίο ολοκληρώνεται το πρώτο κεφάλαιο του ανά χείρας πονήματος καλούμαστε όπως προσδιορίσουμε εννοιολογικός το περιεχόμενο του ορισμού περί των επιθέσεων πλευρικού καναλιού και των υπό- περιπτώσεων στις οποίες αυτές μπορούν να διακριθούν (ήδη ονομαστικά έχει γίνει λόγος για κάποιες υποκατηγορίες όπως optical attacks, electromagnetic attacks, smudge attacks, acoustic attacks κλπ.). Το δεύτερο τμήμα του πρώτου κεφαλαίου προχωρά σε ένα τέτοιο εγχείρημα για δύο κυρίως λόγους:

- Αφενός, διότι η πληθώρα των επιθέσεων πλευρικού καναλιού (και στο σημείο αυτό δεν ενδιαφέρει θα λέγαμε τόσο η δυσκολία στην εκτέλεση κάποιων εξ αυτών, άρα η πιθανότητα επιτυχίας αυτών) καθιστά, κατά κάποιο τρόπο, δυσχερή την

ότι η πειραματική συνθήκη χρησιμοποιεί ένα μικρόφωνο για την καταγραφή της ακουστικής εκροής και ουχί τηλεφωνική συσκευή) στο, Bakes, M., & Durmuth ,M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security Symposium,DC,USA,August,11-13,1-16,σ.9-10. https://www.researchgate.net/publication/221260462_Acoustic_Side-Channel_Attacks_on_Printers (τελευταία πρόσβαση 10/10/2021).

[46] Ενδεχομένως εδώ να αξιοποιηθεί το εξής απλό παράδειγμα συνδυαστικής εκροής (correlation), όπου η σε κάθε περίπτωση διαφορετική τάση του ρεύματος (voltage, αναλόγως και των διεργασιών που λαμβάνουν χώρα) οδηγεί (και) στην παραγωγή διαφορετικών, σε ένταση, ακουστικών εκροών. Ορά και Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton,St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer,2021,10.1007/s41635-021-00112-6.hal-03176249,*1-24,σ.5.https://hal.archives-ouvertes.fr/hal03176249/document (τελευταία πρόσβαση 15/10/2021).

αντίληψη του ποια πτυχή[47] συζητείται κάθε φορά που αναφέρεται ο όρος «επίθεση πλευρικού καναλιού[4849]». Εξαιτίας αυτής της αδυναμίας στην σύλληψη όλων των

[47] Δεδομένης και της εν γένει απουσίας consensus περί της ορολογίας και ενδεχομένως και της ταξινομήσεως των απειλών και επιθέσεων σε ότι αφορά τον κλάδο της κυβερνοασφάλειας γενικά. Εν γένει, παρατηρείται πως ο κάθε ξεχωριστός συγγραφέας ή η κάθε ξεχωριστή ομάς αυτών τείνει να χρησιμοποιεί , επί παραδείγματι, διαφορετικά μοντέλα ταξινόμησης των εκάστοτε απειλών και επιθέσεων έναντι των υπολογιστικών συστημάτων ή/και των κρίσιμων υποδομών, κάτι που αντανακλά μεταξύ άλλων την υποκειμενική οπτική αλλά και την εκάστοτε χρονική και τοπική συγκυρία αναπόφευκτα (π.χ. οι IoT συσκευές είναι συγκριτικά πιο πρόσφατες τεχνολογικές καινοτομίες εν σχέση με τους Η/Υ κλπ.), με αποτέλεσμα από το ένα άρθρο στο άλλο να παρατηρούνται διαφοροποιήσεις. Η συγκεκριμένη παρατήρηση διατυπώνεται, μεταξύ άλλων, και στο ακόλουθο άρθρο, Staddon, E., & Loscri, V., & Mitton, N.(2021). Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Applied Sciences,2021,11,7228,* pp.1-39,σ.4 & 8. doi: https://doi.org/10.3390/app11167228. Applied Sciences | Free Full-Text | Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey (mdpi.com) (τελευταία πρόσβαση 16/9/2021). Για ένα εγχείρημα προς την παγίωση και καταγραφή των διαφόρων ορισμών στον κλάδο της κυβερνοασφάλειας, ορά και, χ.σ.(χ.χ.). Cybersecurity Glossary Explore Terms: A Glossary of Common Cybersecurity Terminology. *NICCS National Initiative For Cybersecurity Careers and Studies.* https://niccs.cisa.gov/about-niccs/cybersecurity-glossary (τελευταία πρόσβαση 7/11/2021).

[48] Χαρακτηριστικό παράδειγμα (διότι οι συγκριτικές παραθέσεις θα μπορούσαν να επεκταθούν και σε έτερες θεματικές) ίσως να αποτελεί η ίδια η έννοια της «εκροής» (leakage), καθώς αυτή η τελευταία μπορεί να είναι είτε προϊόν της ίδιας της λειτουργίας του εκάστοτε συστήματος (άρα intended), ή θα μπορούσε κάλλιστα να είναι προϊόν της δυσλειτουργίας ενός συστήματος (επομένως unintended). Στο ακόλουθο άρθρο που παρατίθεται για παράδειγμα αυτή η διάκριση δεν, φαίνεται, να λαμβάνει χώρα, καθώς το χωρίο έχει ως ακολούθως (η μετάφραση είναι του συγγραφέα) «*Οι επιθέσεις πλευρικού καναλιού (SCA) εισήχθησαν από τον Paul Kocher [20]. Εκμεταλλεύονται την διαρροή πληροφοριών πλευρικού καναλιού, συμπεριλαμβανομένης της κατανάλωσης ενεργείας και του χρόνου εκτελέσεως [ενν. από τις διεργασίες] των [μίκρο] τσιπ στα κρυπτοσυστήματα που εφαρμόζονται στο υλικό»* . Πρβλ. AlDosari, F.(2017). Security and Privacy Challenges in Cyber-Physical Systems. *Journal of Information Security,8,*285-295,σ.290. https://www.scirp.org/pdf/jis_2017101216204555.pdf (τελευταία πρόσβαση 12/10/2021). Ενώ αλλού γίνεται αντίστοιχος λόγος ως εξής (η μετάφραση καθώς και η έμφαση είναι του συγγραφέα), «*στην κρυπτανάλυση, ο όρος επίθεση πλευρικού καναλιού αναφέρεται σε επίθεση για την εξαγωγή ευαίσθητων πληροφοριών, όπως οι πληροφορίες για το μυστικό κλειδί, μέσω της παρατηρήσεως των σχετικών με την εφαρμογή [ενν. του κρυπτοσυστήματος] γεγονότων και/ή σημάτων που ΔΕΝ ΕΙΝΑΙ μέρος της συμπεριφοράς [της σχετικής] με τις εισόδους/εξόδους του αλγόριθμου.* Πρβλ. Khan, H.A., & Alam, M., & Zajic, A., & Prvulovic, M.(2018). *Detailed Tracking of Program Control Flow Using Analog Side-Channel Signals: A Promise for IoT Malware Detection and a Threat for Many Cryptographic Implementations.* Paper presented at the Cyber Sensing 2018, SPIE Defense + Security (SPIE). Orlando, Florida, USA, April 15-19, 1-14,σ.1. https://cpb-us-w2.wpmucdn.com/sites.gatech.edu/dist/4/463/files/2018/05/main.pdf (τελευταία πρόσβαση 28/10/2021). (Εδώ αν και δεν χρησιμοποιείται ο προσδιορισμός unintended, εντούτοις μάλλον εννοείται, ή σε κάθε περίπτωση δεν εννοούνται οι ηθελημένες, κανονικές, εκροές ήτοι intended κλπ). Αν και η διαφορά φαντάζει ελάσσονα, και τωόντι

επιμέρους πτυχών του ορισμού[50], γίνεται ακανθώδες το εγχείρημα αποτυπώσεως όλων των πιθανών απειλών που θα μπορούσαν οι SCAs να ενέχουν για τις κρίσιμες υποδομές εν γένει.

μπορεί να είναι τέτοια ορισμένες φορές, εντούτοις δύναται όπως δημιουργήσει συγχύσεις ένθεν και ένθεν, για παράδειγμα πρέπει να σχεδιαστούν τα αντίμετρα κατά των SCAs, όπως θα μπορούσε να συμβεί και σε μια υποθετική περίπτωση (στο άρθρο που παραθέτουμε κατωτέρω υφίσταται πειραματική συνθήκη σχετικά με τον έλεγχο των επιπέδων ασύρματης φόρτισης, αν και το παράδειγμα που δίνουμε εδώ δεν είναι απαραίτητο να συντρέχει για να υπάρξει μη ηθελημένη εκροή) όπου η εκροή από ασύρματη φόρτιση είναι επαυξημένη όσο περισσότερο φορτισμένη είναι η συσκευή (εδώ ο όρος unintended θα μπορούσε να χρησιμοποιηθεί για να δηλώσει την τάση, οι χρήστες να ξεχνούν το κινητό τους πλησίον της πηγής φόρτισης ακόμα και όταν το τελευταίο έχει φορτιστεί πλήρως, οπότε εδώ ο όρος unintended αφορά ίσως περισσότερο στον ανθρώπινο παράγοντα παρά στην εκροή καθαυτή, και αυτό πρέπει να διευκρινίζεται όπως και το ότι η μη πλήρης φόρτιση έχει μικρότερη εκροή, άρα είναι δυνάμει ένα αντίμετρο). Πρβλ.Cour, A.S.L., & Afridi, K.K., & Suh, G.E.(2021). Wireless Charging Power Side-Channel Attacks. *A arXiv:2105.12266v2 [cs.CR]*,1-13,σ.2. https://arxiv.org/pdf/2105.12266.pdf (τελευταία πρόσβαση 11/10/2021). Τέλος δε, μπορεί να υφίστανται και περιπτώσεις στις οποίες η SCA να μην εκμεταλλεύεται μια εκροή, δηλαδή εκείνη να μην είναι προϋφιστάμενη, αλλά αντίθετα να την δημιουργεί αυτή η πρώτη, βλ. το έργο των Kinugawa et al στο ακόλουθο άρθρο, Liu, Z., & Samwel, N., & Weissbart, L., & Zhao, Z. & Lauret, D., & Batina, L., & Larson, M.(2020). Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. *arXiv: 2011.09877v1 [cs.CR]*,1-15,σ.2. https://arxiv.org/abs/2011.09877 (τελευταία πρόσβαση 10/10/2021).

[49] Για την καλύτερη επίρρωση της προηγούμενης υποσημείωσης (υπ' αριθμόν 34) και σε ότι αφορά την χρήση του όρου intended leakage, παραθέτουμε ενδεικτικά και το ακόλουθο άρθρο των Real και Salvador, όπου ο συγκεκριμένος όρος διατυπώνεται (εν μέρει το επιχείρημα αυτό παρατίθεται και στην επόμενη υποσημείωση από άλλη όμως πηγή και η διευκρίνιση που εμείς παραθέτουμε στην επόμενη σημείωση είναι περισσότερο εννοιολογική) σε σχέση με την βελτίωση (optimization) των αισθητήρων (sensors) που οι συσκευές χρησιμοποιούν (σημειωτέων το εν λόγω άρθρο κάνει λόγο τόσο για τις unintended όσο και για τις intended διαρροές, ενώ όπως έχει ήδη αναφερθεί άλλα άρθρα δεν προχωρούν στην αυτή διάκριση) . Γι' αυτό ορά, Real, M.M., & Salvador, R.(2021). Physical Side-Channel Attacks on Embedded Neural Networks: A Survey. *Applied Science,11,6790,*1-25. doi:https://doi.org/10.3390/app11156790.(PDF) Physical Side-Channel Attacks on Embedded Neural Networks: A Survey (researchgate.net) (τελευταία πρόσβαση 16/9/2021).

[50] Σε συνέχεια (και) της προηγούμενης υποσημείωσης, πρέπει να αναφερθεί πως ενδεχόμενα ούτε ο όρος intended leakage (ηθελημένη διαρροή) είναι αρκούντως κατανοητός. Αντίθετα, είναι αρκετά γενικευτικός, ώστε περιλαμβάνει πέρα από την έννοια της διαρροής λόγω της εφαρμογής (implementation) και την διαρροή που αφορά σε πληροφορίες που οι ίδιες οι εταιρείες αποδεσμεύουν για διάφορους λόγους (π.χ. transparency). Εδώ η έννοια της διαρροής δεν φαντάζει ως ορθή, καθώς η δημοσιοποίηση δεν γίνεται (τουλάχιστον όχι πάντα) με αθέμιτα μέσα ή σκοπό, αλλά η έννοια της ηθελημένης πράξης (intended) υφίσταται για τον ανθρώπινο παράγοντα σε αυτό ο συγκείμενο (βέβαια και η έννοια της εφαρμογής περιλαμβάνει, εν μέρει, τον άνθρωπο που δημιουργεί ένα τμήμα του υπολογιστικού συστήματος ή το script του αλγόριθμου κρυπτογράφησης). Αν δεν αξιοποιηθεί κάποιος άλλος

- Αφετέρου, διότι η εννοιολογική αποσαφήνιση θα μπορέσει να διευκολύνει το εγχείρημα περί της ταξινομήσεως των επιμέρους υποκατηγοριών στις οποίες η διεθνής βιβλιογραφία διακρίνει τις επιθέσεις πλευρικού καναλιού. Με τον τρόπο αυτό το ανά χείρας πόνημα καθίσταται ευκολότερο στην ανάγνωση και επομένως και στην κατανόηση του.

Στην υπό-ενότητα αυτή γίνεται, κατ΄ επέκταση, η αποσαφήνιση δύο βασικών σημείων. Κατά πρώτον, των διαφόρων πτυχών με τις οποίες καταπιάνονται οι εκάστοτε ορισμοί περί του τι συνιστά μια επίθεση πλευρικού καναλιού (SCA), ώστε να γίνει κατανοητό σε τι ακριβώς διαφέρουν. Κατά δεύτερον, θα επιχειρηθεί η αποσαφήνιση των διαφόρων επιμέρους ορισμών (π.χ. εκροές, συσκευές κλπ.) που εντάσσονται στους ευρύτερους ορισμούς-ομπρέλα περί της επιθέσεως πλευρικού καναλιού (SCA).

όρος στην θέση του συγκεκριμένου ορισμού, τότε θα πρέπει η βιβλιογραφική ανασκόπηση να αποσαφηνίσει τον όρο intended leakage, διότι όπως φαίνεται και στο ακόλουθο άρθρο (για SCAs έναντι κινητών συσκευών), οι επιθέσεις πλευρικού καναλιού μπορούν να λάβουν υπόψη τους τέτοιες πληροφορίες αν όχι για να εκτελεστούν οι επιθέσεις αυτές, τότε για να εξαχθούν ακόμα πιο ευαίσθητες πληροφορίες. Ορά και, Spreitzer, R., & Moonsamy, V., & Korak, T., &Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1, 465-488 (1-24),σ.5. doi : 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021). Σημειώνεται ακόμα πως πέρα από την σχετικότητα που εμφανίζεται στην εναλλαγή των όρων emission/leakage/emanation κλπ, και πέρα από την διάκριση ανάμεσα σε ηθελημένες (intended) και αθέλητες (unintended) που προσδιορίζει τις εκροές, μπορεί επίσης να παρατηρηθεί ο προσδιορισμός έμμεση (indirect) και, δια της ατόπου απαγωγής, άμεση (direct) εκροή κλπ. Σε αυτή την τελευταία περίπτωση αναφέρουμε ενδεικτικά την καταγραφή «*indirect emissions*» (έμμεσες εκροές) που σημειώνουν οι Camurati et al. για να υποδείξουν την έμμεση αύξηση των εκροών των διαφόρων στοιχείων ενός RT (radio transceiver, π.χ. συσκευή Wi-fi) εξαιτίας της λειτουργίας των αρμονικών ταλαντώσεων (modulated harmonics) του ρολογιού σε μια τέτοια συσκευή. Επομένως, φαίνεται πως αξιοποιούνται αλλαχού τα δίπολα των όρων έμμεσος/άμεσος(indirect/direct, τον δεύτερο όρο επίσης τον παραθέτουν οι ίδιοι συγγραφείς αναφερόμενοι στους Agrawal et al. Με αναφορά στις ηλεκτρομαγνητικές εκροές που προκύπτουν από ταχεία μετάβαση από την μια ψηφιακή κατάσταση στην άλλη κατά την πειραματική συνθήκη έναντι του αλγορίθμου DES) και το αντίστοιχο μη ηθελημένος/ηθελημένος (intended/unintended), ενδεχομένως να υφίσταται και ζήτημα ενδιάμεσων μεταβλητών (latent variables), αν και δεν έχει διερευνηθεί αν οι όροι αυτοί είναι ταυτόσημοι ή μη. Πρβλ. Camurati, G., & Poeplau, S., & Muench, M., & Hayes, T., & Francillon, A.(2018). *Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers*. Paper presented at the 25th ACM Conference on Computer and Communications Security. Toronto, Canada. October, 15-19, 1-14,σ.7,11. doi: http://dx.doi.org/10.1145/3243734.3243802. https://www.eurecom.fr/en/publication/5625 (τελευταία πρόσβαση 8/2/2022).

Διευκρινίζεται εδώ ότι οι υποκατηγορίες των επιθέσεων πλευρικού καναλιού δεν θα αναφερθούν στο παρών κεφάλαιο, καθότι αποτελούν ξεχωριστό αντικείμενο του αμέσως επόμενου κεφαλαίου που καταπιάνεται με την ταξινόμηση των υποκατηγοριών αυτών.

Από το τμήμα της επιστημονικής βιβλιογραφίας που έχει ως τα τώρα μελετηθεί (διευκρινίζεται πως δεν γίνεται να καλυφθούν όλα τα άρθρα με την σχετική θεματολογία, παρά μόνο ένα αντιπροσωπευτικό δείγμα για τις ανάγκες της παρούσας υπό-ενότητας) μπορούν να παρατεθούν κατά τρόπο συγκριτικό οι ακόλουθες εννοιολογικές παρατηρήσεις και διευκρινήσεις ως εξής :

- Αρχικά, πρέπει να διευκρινιστεί πως η εμβάθυνση στην περί της εννοιολογικής διασαφήνισης συζήτηση εξαρτάται, μεταξύ άλλων, και από τον τρόπο που δομείται το κάθε επιστημονικό άρθρο, ενώ πρέπει να ληφθεί υπόψη και ο στόχος που οι εκάστοτε συγγραφείς θέτουν κάθε φορά. Υπό το πρίσμα αυτό η έκταση που θα λάβει ο ορισμός περί των επιθέσεων πλευρικού καναλιού, όπως επίσης και η εμβάθυνση σε αυτόν και στις διάφορες πτυχές του, θα εξαρτηθεί από ένα εύρος παραγόντων σχετικών με την δομή του εκάστοτε επιστημονικού πονήματος, όπως το αν το εκάστοτε άρθρο επικεντρώνει μόνο στις επιθέσεις πλευρικού καναλιού ή αν αντίθετα επεκτείνεται σε ευρύτερες θεματικές (π.χ. απειλές έναντι IoT ή κινητών συσκευών εν γένει[51]), επίσης από το αν το εκάστοτε πόνημα θα αποκλειστικά στον στόχο του ορισμού και της ταξινομήσεως των επιθέσεων πλευρικού καναλιού[52] ή αν

[51] Για παράδειγμα, Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1, 465-488 (1-24), σ.3 κε.doi : 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[52] Συμπληρωματικά προς την υποσημείωση υπ' αριθμόν 36, πέρα από τον ορισμό της διαρροής πρέπει να σημειωθεί πως και ο όρος side-channel (πλευρικό κανάλι) σε αρκετές περιπτώσεις δεν αναλύεται πέρα από την διατύπωση του στο πλαίσιο ορισμού της συγκεκριμένης επίθεσης γενικά. Επίσης, παρατηρείται μια σχετική απουσία σε ορισμένα άρθρα (εν αντιθέσει με αυτό που παραθέτουμε στην παρούσα υποσημείωση) της αποσαφήνισης σχετικά με το αν πρόκειται για ορισμούς που θέτουν οι ίδιοι οι συγγραφείς για τις ανάγκες του άρθρου τους χωρίς να είναι απαραίτητα απόλυτα γενικευτικοί ή αν συμβαίνει το αντίθετο (σε αρκετά άρθρα σε αυτή την δεύτερη περίπτωση παρατίθενται αναφορές στην εν γένει βιβλιογραφία σε ξεχωριστή υπό-ενότητα, όπως με το άρθρο στην αμέσως προηγούμενη υποσημείωση για παράδειγμα). Σε ότι αφορά τον όρο «κανάλι» οι Biswas et al. αναφέρονται σε timing channels, και κατ' επέκταση σε κανάλια κρυπτογραφημένης επικοινωνίας για ασφαλή ανταλλαγή πληροφοριών ανάμεσα στους χρήστες. Παράλληλα με τον ορισμό του όρου «κανάλι» γίνεται και παραπέρα διάκριση σε φανερά (overt) και κρυφά (covert) κανάλια, και εδώ ο όρος διαρροή προσδιορίζει το μη ασφαλές κανάλι επικοινωνίας και όχι το υλικό, και επομένως υπάρχει διάκριση ανάμεσα στην διαρροή και τον όρο «κανάλι».

Biswas, A.K., & Ghosal, D., & Nagaraja, Sh.(2016). A Survey of Timing Channels and Countermeasures. *ACM Computing Surveys (CSUR),0,0,*1-39,σ.3 κε. doi: 10.1145/3023872. http://personal.strath.ac.uk/shishir.nagaraja/papers/timing-survey.pdf (τελευταία πρόσβαση 24/12/2021). Επιπροσθέτως, δεν φαίνεται να υπάρχει απόλυτη συμφωνία για το αν ο προσδιορισμός που συνοδεύει τον όρο κανάλι (π.χ. covert channel κλπ) μπορεί να εντάσσεται στις SCAs, ή αν πρόκειται για ξεχωριστή περίπτωση που δεν μπορεί να ενταχθεί σε αυτές τις τελευταίες. Φέρ' ειπείν οι Montasari et al. διαχωρίζουν τα πλευρικά από τα εν κρυπτό κανάλια (covert) και τα πραγματεύονται ως ξεχωριστά στο άρθρο τους για τις Timing-Based Side Channel Attacks, βλ. ενδεικτικά Montasari, R., & Hosseinian-Far, A., & Hill, R., & Montaseri, F., & Sharma, M., & Shabbir, Sh.(2018). Are Timing-Based Side-Channel Attacks Feasible in Shared, Modern Computing Hardware ?. *International Journal of Organizational and Collective Intelligence,8,2,*32-59,σ.33, 36. doi: 10.4018/IJOCI.2018040103.https://pure.hud.ac.uk/ws/portalfiles/portal/13423218/Are_Timing_Based_Side_Channel_Attacks_Feasible_in_Shared_Modern_Computing_Hardware_.pdf (τελευταία πρόσβαση 24/12/2021). Ακόμα, οι Townley et al. στην συζήτηση περί της αρχιτεκτονικής και λειτουργίας του SMT (simultaneous multithreading) κάνουν επίσης μια συνοπτική και χωρίς έτερες διευκρινήσεις διάκριση ανάμεσε σε covert και side channels. Ήτοι, στην εξήγηση τους για το πώς δύο νήματα (Spy s & Victim v) διαγκωνίζονται για τους πόρους εντός του SMT (resources RES) σημειώνουν το εξής για το πώς μέσω του τρόπου λειτουργίας και του διαμοιρασμού αυτών των πόρων μπορούν να εμφανιστούν είτε covert είτε side channels, (η μετάφραση είναι του συγγραφέα όπως αναφέρθηκε και αλλού) « *Κατά συνέπεια, οι τρεις οδηγίες από το s* (ενν. το Spy s νήμα) *χρειάζονται περισσότερο χρόνο για να εκτελεστούν. Εάν οι διαφοροποιούμενες φάσεις του v* (ενν. το victim v νήμα) *βασίζονται σε ευαίσθητα δεδομένα , το s μπορεί ν ανακτήσει τα δεδομένα αυτά μετρώντας κατ' επανάληψη την καθυστέρηση που εμφανίζεται κατά την εκτέλεση. Η μέθοδος αυτή μπορεί να γίνει η βάση για ένα εν κρυπτό κανάλι* (covert channel)*, στο οποίο ένα συνωμοτικό victim* (ενν. μάλλον το νήμα που ανήκει στον επιτιθέμενο) *επί τούτου εναλλάσσεται μεταξύ μιας φιλονικούς και μιας μη φιλονικούς συμπεριφοράς* (ενν. το νήμα το οποίο εναλλάξ ανταγωνίζεται για πόρους του SMT και κατόπιν απέχει από τον ανταγωνισμό αυτό, και σε αυτές τις εναλλαγές ο επιτιθέμενος κάνει τις μετρήσεις του για να υποκλέψει πληροφορίες) *για να υπεξαιρέσει ευαίσθητα δεδομένα, ή να γίνει η βάση για ένα πλευρικό κανάλι* (ενν. side channel) *, στο οποίο ένα λησμονημένο victim* (ενν. νήμα) *μπορεί να διαρρέει πληροφορίες, όπως επί παραδείγματι ένα κλειδί κρυπτογράφησης, μέσα από περιστασιακές διαφοροποιήσεις σε ότι αφορά στην συμπεριφορά εκτέλεσης* (ενν. η συμπεριφορά του νήματος κλπ). Πρβλ. Townley, D., & Ponomarev, D.(2019). *SMT-COP: Defeating Side-Channel Attacks on Execution Units in SMT Processors.* Paper presented at the 2019 28th International Conference on Parallel Architectures and Compilation Techniques (PACT). Seattle, WA, USA. September,23-26,43-54(1-12),σ.3.doi:10.1109/PACT.2019.00012.
http://www.cs.binghamton.edu/~dima/pact19.pdf (τελευταία πρόσβαση 8/2/2022). Περαιτέρω, οι Maiti et al προχωρούν και εκείνοι στο άρθρο τους σε διάκριση ανάμεσα σε εν κρυπτό και πλευρικά κανάλια. Συγκεκριμένα η αρχιτεκτονική της επιθέσεως τους που αφορά σε SCA , σε συνδυασμό με malware(malicious application), που θα στοχεύει μια κινητή συσκευή (συλλογή πληροφοριών για το τι πληκτρολογείτε επί αυτής) με την συνδρομή ενός smartwatch (ο φορέας του Malware) που θα είναι στον καρπό του θύματος που πληκτρολογεί. Στην προκειμένη περίπτωση " *Η κακόβουλη εφαρμογή μπορεί κάλλιστα να διατηρεί ένα εν κρυπτό κανάλι επικοινωνίας (επί λεξεί covert communication channel) ανάμεσα στην ίδια και τον επιτιθέμενο, και όπου θα ανεβάζει κατά περιοδικά διαστήματα τα συλλεχθέντα δεδομένα κίνησης από τον καρπό (ενν. του έξυπνου ρολογιού του θύματος) σε κάποιον διακομιστή*

αντίθετα θα περιέχει και κάποιας μορφής μελέτη περιπτώσεως (case-study[53]). Τέλος δε, και από το αν η συνδυασμένη μελέτη των SCAs με κάποια μελέτη περιπτώσεως

(server) που θα ελέγχεται από τον επιτιθέμενο διαμέσου του καναλιού αυτού" (η μετάφραση είναι του συγγραφέα). Εδώ, οι δύο όροι που προσδιορίζουν την έννοια κανάλι είναι και πάλι σαφώς διακριτή, και προστίθενται τα στοιχεία αφενός της συνδυαστικής χρήσης της SCA, και αφετέρου το στοιχείο της χρήσης του εν κρυπτό καναλιού ως υποβοηθητικού στην κύρια επίθεση του πλευρικού καναλιού, όπου σαφώς προσδιορίζεται η ταύτιση εν κρυπτό καναλιού και επικοινωνίας (με διακομιστή), δηλαδή ο ρόλος είναι σαφώς παθητικός με την έννοια της απλής μεταφοράς, ενώ το πλευρικό κανάλι είναι κι αυτό παθητικό αλλά με την έννοια της μετάβασης από το έξυπνο ρολόι στην έξυπνη συσκευή για απόσπαση των πληροφοριών της εκροής (emanation κλπ). Βλ. χαρακτηριστικά, Maiti, A., & Jadiwala, M., & He, J., & Bilogrevic, I.(2018). Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches. *IEEE Transcactions on Mobile Computing* PP(99),1-16,σ.3. DOI:10.1109/TMC.2018.2794984. (PDF) Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches (researchgate.net) (τελευταία πρόσβαση 23/03/2022). Ενώ σε έτερη πηγή οι Cheng et al. Διατυπώνουν τους επιθετικούς προσδιορισμούς active (ενεργητικό) και passive (παθητικό) τόσο για να αναφερθούν στην χρήση/φύση των ακουστικών SCAs όσο και για να διακρίνουν το δικό τους σχήμα επίθεσης (*SonarSnoop*) από έτερα εγχειρήματα στην υπάρχουσα βιβλιογραφία. Η εν λόγω διάκριση, που αφορά στον τρόπο αξιοποίησης της επίθεσης έναντι κινητής συσκευής Android, κατά τους συγγραφείς προκύπτει από το ότι ο όρος passive αναφέρεται σε επιθέσεις όπου οι ακουστικές εκροές προκύπτουν ως λανθάνουσες από την ίδια την συσκευή του θύματος, ενώ στο δικό τους σχήμα ο όρος active χρησιμοποιείται για να καταδείξει τον ενεργητικό ρόλο του επιτιθέμενου ο οποίος προκαλεί (induce) τα ακουστικά σήματα/ακουστικές εκροές, πιο συγκεκριμένα " *Όλες οι ως τα τώρα γνωστές ακουστικές επιθέσεις πλευρικού καναλιού,[...], είναι παθητικές [passive], εννοώντας με αυτό ότι τα ακουστικά σήματα στο πλευρικό κανάλι δημιουργούνται από το θύμα αλλά υφαρπάζονται [eavesdropped] από τον επιτιθέμενο. Εν αντιθέσει, η δική μας προσέγγιση είναι αυτή ενός ενεργητικού [active] πλευρικού καναλιού, εννοώντας με αυτό ότι τα ακουστικά σήματα στο πλευρικό κανάλι προκαλούνται [are induced] από τον ίδιο τον επιτιθέμενο*" (η μετάφραση είναι του συγγραφέα). Και εδώ φαίνεται να διαφοροποιείται η νοηματοδότηση του όρου "πλευρικό κανάλι", καθώς χρησιμοποιείται αφενός ως διακριτός όρος από την εκροή και αφετέρου συσχετίζει την εκροή με τον ρόλο του επιτιθέμενου για να προχωρήσει σε ορισμό του καναλιού ως ενεργητικό ή παθητικό με βάσει αν η εκροή υπάρχει καθαυτή ή αν ο επιτιθέμενος παίζει κάποιο ρόλο στην ύπαρξη της, και εδώ το δίπολο ενεργητικό/παθητικό πρέπει σαφώς να διαχωριστεί από εκείνο της επιθετικής/παθητικής (offensive/passive) χρήσης που γίνεται σε άλλα άρθρα και που αφορά περισσότερο στην συσκευή (vector) και αν αυτή καταστρέφεται ή απλώς αποσπώνται πληροφορίες από εκείνη, διότι οι Cheng et al. φαίνεται να διακρίνουν με βάσει τον ενεργό/παθητικό ρόλο του επιτιθέμενου και όχι μόνο της οποιασδήποτε συσκευής. Ορά ενδεικτικά, Cheng, P., & Bagci, I.E., & Roedig, U., & Yan, J. (2018). SonarSnoop: Active Acoustic Side-Channel Attacks. *International Journal of Information Security,* 19, 213-228(1-13)(2020),σ.1. DOI: https://doi.org/10.1007/s10207-019-00449-8. https://arxiv.org/pdf/1808.10250.pdf (τελευταία πρόσβαση 07/09/2022).

[53] Βλ. ενδεικτικά το ακόλουθο άρθρο, Bakes, M., & Durmuth ,M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security Symposium,DC,USA,August,11-13,1-16,σ.4κε.

θα εστιάσει σε περιπτώσεις που θα αφορούν σε υλικό (hardware όπως για παράδειγμα εκτυπωτές, ιατρικές συσκευές κλπ) ή αν θα κάνουν λόγο για κάποια εφαρμογή που θα αφορά περισσότερο στο λογισμικό (software, συγγραφή κώδικα κλπ[54]).

Πέρα από την έκταση που κάθε φορά αφιερώνεται στα χωρία τα σχετικά με τον ορισμό, και τα οποία ευλόγως είναι εκτενέστερα όταν ο στόχος είναι μόνο ο ορισμός ή η ταξινόμηση των SCAs ενώ αντίθετα είναι συντομότερα όταν πρέπει να αναλυθεί και άλλη θεματική, υφίστανται επιπλέον και άλλες διαφοροποιήσεις που μόνο εν τάχει θα αναφερθούν εδώ (και οι οποίες αφορούν κυρίως το τμήμα της βιβλιογραφίας που έχει μελετηθεί, και δεν επεκτείνονται ενδεχομένως στο σύνολο αυτής απαραίτητα). Διαφοροποιήσεις επομένως παρατηρούνται σε πτυχές όπως η ανάλυση της ορολογίας της σχετικής με τις SCAs[55], μελετών-περιπτώσεως (case-studies[56]), καθώς επίσης και σε ότι αφορά στις προτάσεις σχετικών αντιμέτρων (countermeasures[57]) που το εκάστοτε πόνημα παραθέτει μεταξύ άλλων (και οι οποίες

---

https://www.researchgate.net/publication/221260462_Acoustic_Side-Channel_Attacks_on_Printers(τελευταία πρόσβαση 10/10/2021).

[54] Ενδεικτικά παραθέτουμε εδώ το ακόλουθο άρθρο, Courousse, D., & Barry, Th., & Robisson, B., & Jaillon, P., & Potin, O., & Lanet, J.-J.(2016). *Runtime Code Polymorphism as a Protection Against Side Channel Attacks.* Paper presented at the 10th IFIP WG 11.2 International Conference on Information Security Theory and Practice (WISTP 2016). Greece, Heraklion. September, 26-27, 1-16,σ.3 κε. doi: 10.1007/978-3-319-45931-8_9. https://www.researchgate.net/publication/308278270_Runtime_Code_Polymorphism_as_a_Protection_Against_Side_Channel_Attacks (τελευταία πρόσβαση 3/11/2021).

[55] Ορά και τις σχετικές παραθέσεις στις υποσημειώσεις υπ' αριθμόν 32 & 33, καθώς και την συζήτηση κατωτέρω.

[56] Ορά ενδεικτικά το άρθρο που παρατίθεται στην υποσημείωση υπ' αριθμόν 33.

[57] Αν και τα αντίμετρα θα αναλυθούν εκτενέστερα σε κατοπινό κεφάλαιο της ανά χείρας εργασίας, στο σημείο αυτό αξίζει να αναφερθεί πως υφίστανται διαφοροποιήσεις (και) σε συνάρτηση με το αν ένα άρθρο αξιοποιεί μια μελέτη περιπτώσεως , οπόταν και τα αντίμετρα θα είναι πιο προσαρμοσμένα στην περίπτωση αυτή, ορά την περίπτωση αντιμέτρων του ακόλουθου άρθρου που παρατίθεται, Bakes, M., & Durmuth ,M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security Symposium,DC,USA,August,11-13,pp.1-16,σ.11-12.
https://www.researchgate.net/publication/221260462_Acoustic_Side-Channel_Attacks_on_Printers (τελευταία πρόσβαση 10/10/2021). Ή αν το άρθρο επιχειρεί μια γενικότερη επισκόπηση περί της ταξινομήσεως μιας συγκεκριμένης υποκατηγορίας επιθέσεων πλευρικού καναλιού, όπου κατ' επέκταση η συζήτηση για τα αντίμετρα θα είναι ίσως πιο εκτεταμένη και θα καλύπτει ενδεχομένως μεγαλύτερο εύρος υποπεριπτώσεων, ορά ενδεικτικά και το ακόλουθο άρθρο, Lyu, Y., & Mishra, P..(2017). A Survey of Side-Channel Attacks on Caches and Countermeasures. *Journal of Hardware and Systems Security,*2,33-50(2018), σ.44 κε.

πτυχές εύλογα οδηγούν και σε διαφορετική διάταξη των ενοτήτων στις οποίες διαρθρώνεται το εκάστοτε επιστημονικό άρθρο).

- Δεύτερον, αν και έχει αναφερθεί με την ευρύτερη έννοια και ανωτέρω, υφίστανται διαφοροποιήσεις σε ότι αφορά την κατηγοριοποίηση των υποκατηγοριών των επιθέσεων πλευρικού καναλιού. Έχει παρατηρηθεί υπό του γράφοντος, αν και ενδεχομένως να υφίστανται περισσότερες υποπεριπτώσεις, πως οι παραλλαγές στο εκάστοτε εγχείρημα κατηγοριοποίησης οφείλονται είτε στον βαθμό εγγύτητας του επιτιθέμενου προς την συσκευή κατά της οποίας επιθυμεί να επιτεθεί, είτε στο ίδιο το αντικείμενο της επιθέσεως ανεξαρτήτως αν πρόκειται για υλικό, λογισμικό, κρίσιμη υποδομή ή κάποιου είδους δίκτυο[58].

- Τρίτον, ενδεχομένως υφίσταται ακόμα μια διαφοροποίηση σε ότι αφορά την μελέτη των επιθέσεων πλευρικού καναλιού υπό το πρίσμα του τριπτύχου της CIA (Confidentiality, Integrity, Availability) και το ποιο από τα τρία στοιχεία οι επιθέσεις αυτές δύνανται να προσβάλλουν. Εμφανίζεται μια μονομέρεια στο σημείο αυτό ενδεχομένως, καθώς σε κάποιες περιπτώσεις δίνεται μεγαλύτερη έμφαση στην τυπολογία των SCAs ως παθητικών επιθέσεων (passive attacks) οπότε η ανάλυση γίνεται περισσότερο υπό την οπτική της προσβολής της εμπιστευτικότητας (confidentiality), ενώ το υπολογιστικό σύστημα θεωρείται πως παραμένει ακέραιο[59]. Σε άλλες όμως περιπτώσεις όπου μελετάτε , επί παραδείγματι, μια συσκευή που

---

doi:https://doi.org/10.1007/s41635-017-0025-y. https://esl.cise.ufl.edu/Publications/hass18.pdf (τελευταία πρόσβαση 22/11/2021).

[58] Συνήθως η περιγραφή η σχετική με την εγγύτητα εκφράζεται με όρους όπως local, vicinity, remote, όπως φαίνεται και στην ταξινόμηση που επιχειρείται στο ακόλουθο άρθρο, βλ. σχετικά Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1,465-488 (1-24), σ.7. doi:10.1109/COMST.2017.2779824.https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[59] Ένα παράδειγμα άρθρου στο οποίο ο ορισμός των SCAs συνδέεται με το στοιχείο της εμπιστευτικότητας της πληροφορίας δίδεται στην εισαγωγή του ακόλουθου πονήματος, ενδεικτικά βλ., Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.283. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311),.Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

δέχεται την επίθεση πλευρικού καναλιού, τότε ενδέχεται να μελετηθεί η επιθετική φύση των επιθέσεων αυτών (π.χ. χειραγώγηση της τάσης του ρεύματος ή χειραγώγηση ιατρικής συσκευής), και επομένως να εμφανιστεί κι εδώ μια μονομέρεια ανάλογα και με τις επιλογές του εκάστοτε συγγραφέα (π.χ. αν υφίσταται use-case που μελετά ορισμένες εφαρμογές ή συσκευές ή αν επιχειρείτε μια ταξινόμηση (και) των SCAs με βάσει διάφορους θεματικούς άξονες[60]).

- Τέταρτον, οι περιγραφικοί όροι που χρησιμοποιούνται στους ορισμούς περί των επιθέσεων πλευρικού καναλιού[61] (π.χ. εγγύτητα, εκροή, ακόμα ίσως και η

[60] Ορισμένα παραδείγματα περί της επιθετικής (ήτοι offensive) εφαρμογής των SCAs δίδονται και στο άρθρο που ακολουθεί, ορά και Pycroft, L., & Aziz, T.Z.(2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices,15:6,* 403-406,σ.404. https://www.tandfonline.com/doi/pdf/10.1080/17434440.2018.1483235?needAccess=true (τελευταία πρόσβαση 12/10/2021). Επίσης, ένα χαρακτηριστικό παράδειγμα σε ότι αφορά τους περιορισμούς που υφίστανται οι κατηγοριοποιήσεις, όπου ένας περιορισμός αναφύεται όταν η κατηγοριοποίηση εκκινεί από το εύρος του αντίκτυπου που έχει μια επίθεση σε ένα σύστημα (μη εξαιρουμένης και της πιο επιθετικής πτυχής των SCAs,αλλά ο λόγος δεν γίνεται αποκλειστικά γι' αυτές στο ακόλουθο άρθρο) ορά και, Staddon, E., & Loscri, V., & Mitton, N.(2021). Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Applied Sciences,2021,11,7228,*1-39,σ.20 κε.doi: https://doi.org/10.3390/app11167228. Applied Sciences | Free Full-Text | Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey (mdpi.com) (τελευταία πρόσβαση 16/9/2021).

[61] Ενδεχομένως αξίζει να σημειωθεί πως ακόμα και ο όρος επίθεση δεν απαντάται (αν και κυρίως χρησιμοποιείται) πάντοτε σε ότι αφορά στην εννοιολογική συζήτηση για τις SCAs, επί παραδείγματι υπάρχει η περίπτωση κατά την οποία ο όρος που χρησιμοποιείται είναι εκείνος της αναλύσεως (analysis) και της τεχνικής (technique) και ουχί εκείνος που δηλώνει επίθεση (attack), επίσης στο ίδιο άρθρο χρησιμοποιείται ο όρος "*template attack*" για να περιγράψει μια εκάστη των SCAs (συνήθως ο εν λόγω όρος δεν ενέχει θέση συνώνυμου, αλλά περιγράφεται όπως και στο άρθρο που παρατίθεται ως υποκατηγορία των SCAs). Αν και ο όρος επίθεση είναι αυτός που ξεκάθαρα επικρατεί, εντούτοις η σποραδική εμφάνιση άλλων εννοιών (όπως ανάλυση, τεχνική κλπ.) ενδεχομένως να αξίζει αναφοράς (αν και στο συγκεκριμένο χωρίο του άρθρου που θα παραθέσουμε δεν υφίσταται τέτοια μνεία ακριβώς) διότι δυνητικά τα πλευρικά κανάλια μπορούν να χρησιμοποιηθούν και από τις κυανές ομάδες (blue teams). Βλ. ενδεικτικά, Liu, Z., & Samwel, N., & Weissbart, L., & Zhao, Z. & Lauret, D., & Batina, L., & Larson, M.(2020). *Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel*. A paper presented at The Network and Distributed System Security Symposium (NDSS) 2021. Virtual Venue. 21-25 February,1-15,σ.3. https://arxiv.org/abs/2011.09877 (τελευταία πρόσβαση 10/10/2021).

έννοια συσκευή κλπ.) είναι κάποιες φορές αρκούντως γενικευτικοί και δεν εξειδικεύουν ενδεχομένως σε όλες τις περιπτώσεις κατάλληλα. Επί παραδείγματι :

1. Ο όρος εγγύτητα, ή οι επιμέρους όροι που δηλώνουν εγγύτητα/απόσταση μέσα στα συμφραζόμενα, δεν ορίζουν ακριβώς την θέση που πρέπει να έχει ο επιτιθέμενος σε κάθε διαφορετικό τύπο επιθέσεως πλευρικού καναλιού, ή ορθότερα δεν γίνεται ξεκάθαρο με αυτούς τους όρους αν σημασία έχει μόνο το δίπολο εγγύτητα/απόσταση για τον επιτιθέμενο ή αν πρέπει να επεκταθεί η σημασία αυτή και σε άλλους παράγοντες. Ξεκάθαρα, η εγγύτητα αποτελεί αντικείμενο της εκάστοτε πραγματείας ως ένα βαθμό. Γενικά, σε ένα τμήμα της βιβλιογραφίας παρατηρείτε ένας δυϊσμός, η έννοια της εγγύτητας/απόστασης είτε θα αφορά στον επιτιθέμενο και το πόσο κοντά ή μακριά βρίσκεται σε σχέση με τον στόχο (εδώ εννοείται η κλασσική διάκριση σε invasive, semi-invasive, none-invasive παραλλαγών[62]). Είτε θα αφορά στην χωροθέτηση διαφόρων αντικειμένων πλησίον του στόχου, όπως επί παραδείγματι αντανακλάσεις επί αντανακλάσεων[63]. Έτσι παρουσιάζεται μια μικρή δυσχέρεια στον ορισμό της απόστασης ή της εγγύτητας αλλά και σε ότι αφορά ενδεχομένως τον αριθμό και την συσχέτιση των επιτιθέμενων και των αντικειμένων που δέχονται την επίθεση[64].

[62] Για μια αναφορά σε κριτήρια των εκάστοτε ταξινομήσεων ορά μεταξύ άλλων και Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311), σ.306.Cham:Springer. https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[63] Χαρακτηριστικά αναφέρεται για το πόνημα των Backes et al, ορά και Liu, Z., & Samwel, N., & Weissbart, L., & Zhao, Z. & Lauret, D., & Batina, L., & Larson, M.(2020). *Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel*. A paper presented at The Network and Distributed System Security Symposium 2021. Virtual venue. 21-25 February,1-15,σ.2. https://arxiv.org/abs/2011.09877 (τελευταία πρόσβαση 10/10/2021).

[64] Ο.π.

2. Ο όρος εκροή στο τμήμα της βιβλιογραφίας που αξιοποιήθηκε περιγράφεται, εν γένει, με τους όρους leakage[65], emanation[66] και emission[67][68]. Εδώ αναφύεται μια σχετική διαφοροποίηση ανάμεσα στους τρεις αγγλόφωνους όρους, καθώς μπορεί να παρατηρηθεί ότι δεν υφίσταται λεπτομερειακή διάκριση ανάμεσα τους, ενώ κυρίως χρησιμοποιείται ο όρος leakage για να περιγραφούν οι εκροές. Συχνάκις εννοείται ή υποδηλώνεται η έννοια της αθέλητης εκροής (unintended leakage πρβλ. υποσημείωση υπ' αριθμόν 32) χωρίς συχνά να γίνεται μια ξεκάθαρη διάκριση όπως έχει προαναφερθεί (πρβλ. υποσημειώσεις υπ' αριθμόν 32 & 33). Αξίζει ωστόσο να επισημανθεί μια μικρή διαφορά που παρατηρήθηκε στο συγκεκριμένο τμήμα της βιβλιογραφίας. Ενώ τα περισσότερα άρθρα κάνουν διάκριση ανάμεσα σε intrusive και none-intrusive SCAs, εντούτοις εκείνο των Lavaud et al πέρα από μια τέτοια διάκριση, προχωρά και στην εδραίωση μιας

---

[65] Χαρακτηριστικά αναφέρεται ο όρος leakage στο ακόλουθο άρθρο, όπου και ο τελευταίος χρησιμοποιείται για να καταδείξει τόσο τις SCAs που βασίζονται σε διαρροές software όσο και εκείνες που αφορούν στο hardware, ενώ ταυτόχρονα δεν υφίσταται σαφής διάκριση ανάμεσα σε ηθελημένη (intended) και μη ηθελημένη εκροή (unintended), αν και η δεύτερη εννοείται με την έκφραση (η μετάφραση είναι του γράφοντος) «*...είναι το αποτέλεσμα ενός ή περισσότερων φυσικών φαινομένων που κάνουν ώστε η πληροφορία να αποκλίνει από το ενδεδειγμένο μονοπάτι για να φτάσει σε έτερο μη ηθελημένο».* Βλ. Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton,St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer,2021,10.1007/s41635-021-00112-6 . hal-03176249,*1-24,σ.1. https://hal.archives-ouvertes.fr/hal-03176249/document (τελευταία πρόσβαση 15/10/2021).

[66] Χαρακτηριστικά στο αμέσως προηγούμενο άρθρο ο όρος emanation χρησιμοποιείται αλλαχού με τον όρο leakage, ο τελευταίος χρησιμοποιείται για να μιλήσει για τις διαρροές γενικά ενώ ο πρώτος για να τονίσει την διάκριση/ταξινόμηση των SCAs ανάμεσα επιθέσεις που στοχεύουν το λογισμικό και εκείνες που προϋποθέτουν ειδικό εξοπλισμό για να στοχεύουν κυρίως το υλικό (για αυτές τις δεύτερες χρησιμοποιείται ο όρος emanation). Βλ. Ενδεικτικά, ο.π.,σ.1.

[67] Εν προκειμένω για pipeline emission, Siemens(χ.χ.). Side-channel attacks. *Tech Design Forum.* https://www.techdesignforums.com/practice/guides/side-channel-analysis-attacks/ (τελευταία πρόσβαση 24/11/2021).

[68] Αξίζει επίσης να σημειωθεί πως σε μια περίπτωση παρατηρήθηκε και η χρήση του όρου «*non-functional behaviors"* (μη λειτουργικές συμπεριφορές) για να περιγράψει τα είδη των εκροών (ηλεκτρομαγνητικές και άλλες) τις οποίες έτεροι συγγραφείς είχαν περιγράψει με τους άλλους όρους που ανεφέρθησαν στην οικεία παράγραφο. Ορά Lyu, Y., & Mishra, P.(2017). A Survey of Side-Channel Attacks on Caches and Countermeasures. *Journal of Hardware and Systems Security,*2,33-50(2018),σ.1.doi:https://doi.org/10.1007/s41635-017-0025-y.https://esl.cise.ufl.edu/Publications/hass18.pdf (τελευταία πρόσβαση 22/11/2021).

διάκρισης ανάμεσα στην εκροή ως απόδοση πληροφορίας και στην εκροή ως ένα «*πλήρως ελεγχόμενο μέσο επικοινωνίας*» ("*fully controllable communication medium*[69][70]"). Έτσι τίθεται και η διάκριση ανάμεσα σε μια παθητική και σε μια πιο επιθετική εκροή, ενώ συνήθως η εκροή αντιμετωπίζεται ως ουδέτερη (ήτοι απόρροια της εφαρμογής ενός συστήματος ή ενός αλγόριθμου κρυπτογραφίας κλπ) και οι τύποι των SCAs μελετιούνται ως επιθετικά ή παθητικά σχήματα (intrusive ή none intrusive κλπ).

3. Η έννοια της συσκευής αν και αρκετά ακριβόλογη, εντούτοις δεν αναδεικνύει πάντοτε το εύρος των σχετικών attack vectors τους οποίους οι SCAs δύνανται να πλήξουν[71]. Η προσπάθεια αποσαφήνισης του είδους της

---

[69] Ορά Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton,St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer,2021,10.1007/s41635-021-00112-6 . hal-03176249,*1-24,σ.2. https://hal.archives-ouvertes.fr/hal-03176249/document (τελευταία πρόσβαση 15/10/2021).

[70] Επιπροσθέτως, σε έτερο άρθρο των Knechtel και Sinanoglu αυτή την φορά, εμφανίζεται επίσης μια κάπως διαφοροποιημένη εκδοχή του όρου εκροή που ενδεχομένως ομοιάζει με την προαναφερθείσα. Χρησιμοποιείται ο όρος «*physical interactions*" (φυσικές αλληλεπιδράσεις) για να περιγραφούν οι εκροές των συσκευών, οπότε και εδώ εμφανίζεται μια παραλλαγή διότι η εκροή δεν νοείται καθαυτή αλλά σε συνάφεια με τον περιβάλλοντα χώρο. Ακόμα στο συγκεκριμένο άρθρο, όπως και σε εκείνο των Lavaud et al, τονίζεται ξανά η χρήση της εκροής (για τις Thermal SCAs) ως μέσου για την αλληλοδιαδοχή δύο διαφορετικών τύπων SCAs (ήτοι thermal & power SCAs) σε ότι αφορά την επιφάνεια επιθέσεως (συγκεκριμένα η εκροή ως μέσο αλληλοδιαδοχής περιγράφεται στο εν λόγω άρθρο με τον όρο "*proxy*"). Βλ. ενδεικτικά, Knechtel, J., & Sinanoglu, O.(2017). *On mitigation of side-channel attacks in 3D ICs: Decorrelating thermal patterns from power and activity.* Paper presented at the 2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC), 2017. Austin, TX, USA, June, 18-22, 1-6,σ.1.doi:10.1145/3061639.3062293 .https://dl.acm.org/doi/pdf/10.1145/3061639.3062293?casa_token=nY_J0HkLqiUAAAAA:QX3FpVcsY0AWRdq_xbssryCEIRlfZdyT6gV6CmS5ofawQbRgQ0C-fTvrxX0K1UOZ5EFgLjp8__Co2A (τελευταία πρόσβαση 22/11/2021).

[71] Σχετικά πιο πρόσφατα η σχέση SCA-συσκευής έχει μελετηθεί κι υπό το πρίσμα της δυνατότητας προστασίας τέτοιων συσκευών, ορά και Khan, H.A., & Alam, M., & Zajic, A., & Prvulovic, M.(2018). *Detailed Tracking of Program Control Flow Using Analog Side-Channel Signals: A Promise for IoT Malware Detection and a Threat for Many Cryptographic Implementations.* Paper presented at the Cyber Sensing 2018, SPIE Defense + Security (SPIE). Orlando, Florida, USA, April 15-19, 1-14,σ.1. https://cpb-us-w2.wpmucdn.com/sites.gatech.edu/dist/4/463/files/2018/05/main.pdf(τελευταία πρόσβαση 28/10/2021).

συσκευής που μπορεί να δεχτεί μια επίθεση πλευρικού καναλιού είναι σημαντική, καθώς όπως μπορεί να καταδείξει ίδια η ιστορική μελέτη των συγκεκριμένων επιθέσεων, σχεδόν προοδευτικά, η επιφάνεια των επιθέσεων διευρύνεται.

Υπό αυτό το πρίσμα ο όρος συσκευή έχει, τουλάχιστον, διττή σημασία, αφενός εννοείται ο εξοπλισμός (equipment) που σε αρκετές περιπτώσεις απαιτείται για την διενέργεια μιας SCA, και αφετέρου εννοείται η συσκευή στόχος (έννοια επομένως σχετική με την επιφάνεια επιθέσεως και εκείνη του attack vector). Στην πρώτη περίπτωση, και ανάλογα με τον στόχο του επιτιθέμενου, η συσκευή με την έννοια του εξοπλισμού (π.χ. oscilloscope) μπορεί να ποικίλλει σε χρηματική αξία και περιπλοκότητα. Επιπροσθέτως, λαμβάνεται υπόψη και η παράμετρος λοιπών τεχνικών γνώσεων σε άλλες επιστήμες (π.χ. γνώσεις περί των χημικών ενώσεων για τις περιπτώσεις εκείνες που απαιτείται decapsulation πριν μπορέσει ο επιτιθέμενος να λάβει τις μετρήσεις που χρειάζεται[72]).

Στην δεύτερη περίπτωση ο λόγος γίνεται για συσκευές ή υπό την ευρύτερη έννοια συστήματα που δέχονται την επίθεση, εδώ υφίσταται μια αρκετά μεγάλη ποικιλομορφία. Ανάλογα με τις περιπτώσεις που οι εκάστοτε συγγραφείς μελετούν ο όρος συσκευή (ή άλλοι συναφείς όροι όπως ο όρος σύστημα) χρησιμοποιείται για να περιγράψει συσκευές όπως ενσωματωμένα συστήματα (embedded systems[73]), κινητές συσκευές (mobile devices[74]),

---

[72] Standaert, F-X. (2010). Introduction to Side-Channel Attacks.Στο I.M.R. Verbauwhede (Επιμ.), *Secure Integrated Circuits and Systems* (σ.27-42),σ.27. Leuven: Springer Link. https://www.researchgate.net/publication/225852558_Introduction_to_Side-Channel_Attacks(τελευταία πρόσβαση 26/11/2021).

[73] Βλ. Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1, 465-488 (1-24),σ.4 κε. doi: 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[74] Βλ. Clark, S.S., & Ransford, B., & Rahmati, A., & Guineau, S., & Sorber, J., & Fu, K., & Xu, W.(2013). *WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices.* Paper presented at the 2013 USENIX Workshop on Health Information Technologies (HealthTech '13), Washington DC, USA, August 12, 1-11, σ.2-3. https://www.usenix.org/conference/healthtech13/workshop-program/presentation/clark (τελευταία πρόσβαση 15/10/2021).

ενσωματωμένα κυκλώματα (integrated circuits, ICs[75]), αυτοκινούμενα οχήματα (automobiles[76]) κα.

Ο λόγος εδώ γίνεται μόνο για το υλικό, καθώς η μεγαλύτερη συνάφεια στην βιβλιογραφία παρατηρείται σε σχέση με τέτοιους attack vectors, όμως η παράθεση αρκεί για να καταδείξει αφενός το εύρος της επιφάνειας επιθέσεως, και αφετέρου την πολυπλοκότητα στην οποία δύναται να φτάσει μια επίθεση πλευρικού καναλιού, εν μέρει η δυσκολία παράθεσης ενός ακριβούς ορισμού οφείλεται και στους δύο αυτούς παράγοντες.

Συμπερασματικά, οι επιθέσεις πλευρικού καναλιού αποτελούν μια ιδιαίτερα εύρωστη απειλή για τις κρίσιμες υποδομές καθώς , σε αντίθεση με άλλα επιθετικά σχήματα, η αιτία του ρίσκου απορρέει από την εφαρμογή των συστημάτων στις κρίσιμες υποδομές παρά από τις αδυναμίες αυτών (ενν. των εκάστοτε πληροφοριακών συστημάτων κλπ). Η φύση αυτή της απειλής, ήτοι η εφαρμογή, είναι (τουλάχιστον) διττή. Αφενός, η απειλή μεγεθύνεται από την λανθασμένη εφαρμογή (π.χ. ενός αλγόριθμου κρυπτογραφίας κλπ) που είτε δεν είναι εύκολο προβλεφθεί εξαρχής καθώς υφίσταται χάσμα ανάμεσα σε κατασκευαστές και χρήστες συσκευών και συστημάτων[77] (μεταξύ άλλων), είτε δεν είναι πάντα εφικτό να εφαρμοστούν (αποτελεσματικά ως προς την εφαρμογή τους) αντίμετρα εξαιτίας της ίδιας της φύσης ορισμένων

---

[75] Βλ. Knechtel, J., & Sinanoglu, O.(2017). *On mitigation of side-channel attacks in 3D ICs: Decorrelating thermal patterns from power and activity.* Paper presented at the 2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC), 2017. Austin, TX, USA, June, 18-22, 1-6, σ.1.doi:10.1145/3061639.3062293 .https://dl.acm.org/doi/pdf/10.1145/3061639.3062293?casa_token=nY_J0HkLqiUAAAAA:QX3FpVcsY0AWRdq_xbssryCEIRlfZdyT6gV6CmS5ofawQbRgQ0C-fTvrxX0K1UOZ5EFgLjp8__Co2A (τελευταία πρόσβαση 22/11/2021).

[76] Βλ. Saeedi, E., & Kong, Y.(2014). Side-channel Vulnerabilities of Automobiles. *Transaction on IoT and Cloud Computing,2(2),*1-8,σ.3. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.680.3844&rep=rep1&type=pdf (τελευταία πρόσβαση 16/9/2021).

[77] Zhang, L., & Hu, W., & Ardeshiricham, A., & Tai, Y., & Blackstone, J., & Mu, D., & Kastner, R.(2018). *Examining the Consequences of High-Level Synthesis Optimizations on Power Side-Channel.* Paper presented at the 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE). Dresden, Germany. March, 19-23,1-4,σ.1. doi:10.23919/DATE.2018.8342189. https://ieeexplore.ieee.org/document/8342189/authors#authors (τελευταία πρόσβαση 4/11/2021).

συσκευών (π.χ. embedded systems[78]). Αφετέρου, οι επιθέσεις πλευρικού καναλιού (ή ορισμένες εξ αυτών) δεν χρειάζεται να βασιστούν σε αρκετές από τις προϋποθέσεις που βασίζονται άλλες επιθέσεις (π.χ. κάποιο κακόβουλο λογισμικό, backdoor κλπ) για να πετύχουν (ορά και υποσημείωση υπ' αριθμόν 22) κι έτσι ίσως υφίσταται μια μεγαλύτερη αμεσότητα στην εκτέλεση τους, ενώ ταυτόχρονα σε κάποιες περιπτώσεις υποβοηθούνται από την τεχνολογική πρόοδο των εκάστοτε συσκευών που μερικές φορές κάνει ώστε οι εκροές να αυξάνουν[79].

Μια επιπλέον αιτία που διευρύνει το μέγεθος της απειλής μιας επιθέσεως πλευρικού καναλιού για τις κρίσιμες υποδομές είναι οι διαφορές που παρατηρούνται τόσο σε ότι αφορά τον ορισμό όσο και στις ταξινομήσεις των συγκεκριμένων υποκατηγοριών της επιθέσεως αυτής. Πέρα και από το ευρύτερο θεωρητικό σκέλος, οι διαφοροποιήσεις στους ορισμούς και τις ταξινομήσεις (αυτές οι τελευταίες θα αναφερθούν στο επόμενο κεφάλαιο) αποτελούν, δυνητικά, τροχοπέδη τόσο στην συνολική καταγραφή των πιθανών attack vectors που οι επιτιθέμενοι θα θελήσουν να εκμεταλλευτούν, όσο και στην καταγραφή αποτελεσματικών στρατηγικών κυβερνοασφάλειας έναντι των επιθέσεων αυτών[80].

---

[78] Βλ. Clark, S.S., & Ransford, B., & Rahmati, A., & Guineau, S., & Sorber, J., & Fu, K., & Xu, W.(2013). *WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices.* Paper presented at the 2013 USENIX Workshop on Health Information Technologies (HealthTech '13), Washington DC, USA, August 12, 1-11, σ.2-3. https://www.usenix.org/conference/healthtech13/workshop-program/presentation/clark (τελευταία πρόσβαση 15/10/2021).

[79] Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton,St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer,2021,10.1007/s41635-021-00112-6 . hal-03176249,*1-24,σ.2. https://hal.archives-ouvertes.fr/hal-03176249/document (τελευταία πρόσβαση 15/10/2021).

[80] Για τα πλεονεκτήματα που ενέχει το περί της ταξινομήσεως εγχείρημα. βλ. ενδεικτικά και, Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.284. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

Κεφάλαιο 2ο : Η ιστορική αναδρομή και τα εγχειρήματα ταξινομήσεως των SCAs

Το παρόν κεφάλαιο, το οποίο και ολοκληρώνει το θεωρητικό πλαίσιο του ανά χείρας πονήματος, αφορά σε έναν διττό στόχο :

- Αφενός, θα επιχειρηθεί μια συνοπτική ιστορική αναδρομή στην εξελικτική πορεία των επιθέσεων πλευρικού καναλιού, ώστε να αναδειχθεί τόσο η ευελιξία που τις χαρακτηρίζει, όσο και η σχέση (κατά το δυνατόν) των εν λόγω επιθέσεων με τις κρίσιμες υποδομές.
- Αφετέρου, θα επιχειρηθεί μια προσπάθεια ταξινομήσεως των επιθέσεων πλευρικού καναλιού, όπου θα καταδειχθεί ο βαθμός δυσκολίας ενός τέτοιου εγχειρήματος, αλλά και θα καταγραφούν ορισμένες προσπάθειες ταξινομήσεως που η επιστημονική βιβλιογραφία έχει να επιδείξει.

Υπό-ενότητα 2.1: Ιστορική επισκόπηση περί των επιθέσεων πλευρικού καναλιού

Η συνοπτική αυτή ιστορική αναδρομή έχει ως στόχο, αφενός να καταδειχθεί η ποικιλομορφία των SCAs και αφετέρου να αναδειχθεί η συνεχώς αυξανόμενη επιφάνεια επιθέσεως (attack surface) που οι SCAs καλύπτουν σε σχέση με τις κρίσιμες υποδομές αλλά και ευρύτερα.

Παρά τις ποικίλες παραλλαγές και τους διάφορους συνδυασμούς που οι SCAs εμφανίζουν τα τελευταία χρόνια, η ύπαρξη τους είναι σαφώς αρχαιότερη των σύγχρονων υπολογιστικών συστημάτων καθώς επίσης και των σύγχρονων κρίσιμων υποδομών όπως αυτές νοούνται τη σήμερον. Οι πρώτες καταγραφές τέτοιων τύπων επιθέσεων αφορούσαν (όπως εν μέρει και σήμερα) το υλικό (hardware). Κατά γενική ομολογία οι πρώτες SCAs εμφανίζονται ακόμα από την εποχή του Πρώτου Παγκοσμίου Πολέμου και στην συνέχεια η εμφάνιση τους θα καταγραφεί και στην περίοδο του Ψυχρού Πολέμου[81], με ορισμένες καταγεγραμμένες περιπτώσεις εμφάνισης αυτών να είναι οι κάτωθι :

[81] Για ορισμένα άρθρα που παραθέτουν πληροφορίες ιστορικού περιεχομένου για κάποιες από τις πρώτες SCAs ορά και την βιβλιογραφία στο ακόλουθο άρθρο, Bakes, M., & Durmuth ,M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security

- Η μυστική υπηρεσία της CIA κατά την δεκαετία του ’50 κατάφερε επιτυχώς να αποκτήσει πρόσβαση σε μυστικές στρατιωτικές γραμμές επικοινωνίας αποκρυπτογραφώντας το κρυπτογραφημένο κείμενο στο Μοντέλο 131-B2 (Model 131-B2). Με την χρήση ενός oscilloscope καθίστατο εφικτό να εντοπιστούν τα πλήκτρα που είχαν πατηθεί σε ποσοστό 75% και όντας σε απόσταση περίπου ενός μιλίου από την συσκευή στόχο, η υπό μελέτη εκροή αφορούσε στο μήκος των ραδιοκυμάτων που εξέπεμπε η εν λόγω συσκευή[82].
- Οι σοβιετικές μυστικές υπηρεσίες περί τα μέσα του 20ου αιώνα φέρεται να εξέδωσαν και αν διακίνησαν μια σειρά έγγραφων οδηγιών για την μείωση των εκροών που θα μπορούσαν να οδηγήσουν σε επιτυχή εκτέλεση επίθεσης πλευρικού καναλιού[83].
- Ίσως η γνωστότερη περίπτωση SCA στην ψυχροπολεμική περίοδο αφορά στην ανάπτυξη από πλευράς της αμερικανικής αντικατασκοπείας του συστήματος κανόνων TEMPEST[84]. Στα μέσα της δεκαετίας του ’80 ο van Eck καταφέρνει να φέρει σε πέρας μια πειραματική συνθήκη κατά την οποία ο επιτιθέμενος δύναται να αντλήσει πληροφορίες από τις εκροές της οθόνης ενός υπολογιστή. Η συγκεκριμένη προσπάθεια αποτέλεσε μια σημαντική καμπή καθώς με την επίδειξη μιας τέτοιας εφαρμογής κατέστη κατανοητό πως αυτή είναι εφικτή, ακόμα και όταν ένας επιτιθέμενος δεν διαθέτει πόρους αντίστοιχους με εκείνους μιας εθνικής κυβερνήσεως (ή κάποιου άλλου κρατικού φορέα), και χωρίς παράλληλα να διαθέτει κάποιου είδους πρόσβαση σε διαβαθμισμένα έγγραφα (καθώς κατά γενική ομολογία το TEMPEST ήταν εν πολλοίς προνόμιο μυστικών υπηρεσιών στον Ψυχρό Πόλεμο[85]).

Symposium,DC,USA,August,11-13,1-16,σ.3. https://www.researchgate.net/publication/221260462_Acoustic_Side-Channel_Attacks_on_Printers (τελευταία πρόσβαση 10/10/2021).

[82] Fow, E-G.(2019). A Brief Peek Into the Fascinating World of Side Channel Attacks. *Start it up.*https://medium.com/swlh/a-brief-peek-into-the-fascinating-world-of-side-channel-attacks-809f96eabea1 (τελευταία πρόσβαση 11/10/2021).

[83] Ο.π.

[84] Ο.π.

[85] Liu, Z., & Samwel, N., & Weissbart, L., & Zhao, Z. & Lauret, D., & Batina, L., & Larson, M.(2020). *Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel*. A paper presented at The Network and Distributed System Security Symposium 9NDSS) 2021. Virtual Venue. 21-25 February,1-15,σ.2. https://arxiv.org/abs/2011.09877 (τελευταία πρόσβαση 10/10/2021).

Αυτό που αξίζει να επισημανθεί για την ιστορική πορεία των SCAs είναι πως παρά την μακροχρόνια ύπαρξη τους διατηρούν ορισμένα από τα αρχικά χαρακτηριστικά τους (όπως το ότι ορισμένες από τις εκροές που παράγουν πληροφορία παραμένουν ίδιες, ήτοι η θερμότητα, ο ηλεκτρισμός, και εν μέρει η ακουστική εκροή[86][87]), και επίσης παρουσιάζουν μια διαχρονικότητα (εν μέρει) και σε ότι αφορά στην εφαρμογή αντιμέτρων για την αντιμετώπιση τους (π.χ.shielding, χαμηλή τάση του ρεύματος και λειτουργία σε κάποιο προστατευμένο/απομονωμένο περιβάλλον[88]).

Με την σταδιακή πρόοδο της τεχνολογίας οι SCAs , σε ότι αφορά τα υπολογιστικά συστήματα πλέον, παρουσιάζουν ορισμένες διαφοροποιήσεις στο πέρασμα των ετών :

- Εν γένει, την δεκαετία του ’90 η έμφαση δίδονταν κυρίως στις SCAs που προϋπέθεταν την εγγύτητα του επιτιθέμενου με την συσκευή (π.χ. Kocher[89]). Οι βασικές πηγές εκροής τις οποίες και εκμεταλλεύονταν οι επιθέσεις πλευρικού καναλιού είχαν να κάνουν κυρίως με την ενεργειακή κατανάλωση (power consumption), την χρονομέτρηση των εκάστοτε διαδικασιών εκτέλεσης όπως οι

[86] Μια χαρακτηριστική περίπτωση είναι εκείνη κατά την οποία οι βρετανικές μυστικές υπηρεσίες εκμεταλλεύτηκαν ακουστικές εκροές για να κατασκοπεύσουν την αιγυπτιακή πρεσβεία στα μέσα της δεκαετίας του ’50. Ορά και Bakes, M., & Durmuth ,M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security Symposium,DC,USA,August,11-13,1-16,σ.3. https://www.researchgate.net/publication/221260462_Acoustic_Side-Channel_Attacks_on_Printers (τελευταία πρόσβαση 10/10/2021).

[87] Fow, E-G.(2019). A Brief Peek Into the Fascinating World of Side Channel Attacks. *Start it up.*https://medium.com/swlh/a-brief-peek-into-the-fascinating-world-of-side-channel-attacks-809f96eabea1 (τελευταία πρόσβαση 11/10/2021).

[88] Ο.π.

[89] Ενδεικτικά ο Cocher δημοσίευσε αρθρογραφία σχετικά με την timing analysis (1995) , οι Cocher et al ένα χρόνο αργότερα δημοσίευσαν αρθρογραφία για την power analysis (απλή και διαφορική, ήτοι simple & differential power analysis) έναν χρόνο μετά (1996), ενώ στις αρχές της δεκαετίας του 2000 οι Quisquater, Samyde και Gandolfi et al δημοσίευσαν αρθρογραφία σχετική με τις ηλεκτρομαγνητικές επιθέσεις ως υποκατηγορίας των SCAs. Επιπροσθέτως, οι Boneh, DeMillo και Lipton δημοσίευσαν επίσης το 1996 αρθρογραφία για την υποκατηγορία των fault injection επιθέσεων, την ίδια χρονιά οι Biham και Shamir διερεύνησαν την διαφορική (differential) fault analysis, ενώ μερικά χρόνια αργότερα (2002) ο Skorobogatov και Anderson δημοσίευσαν αρθρογραφία η οποία επικεντρωνόταν σε optical fault SCAs. Βλ. χ.σ.(χ.χ.). Lehrstuhl fur Eingegettete Sicherheit. *Ruhr-Universitat Bochum.* https://www.emsec.ruhr-uni-bochum.de/research/projects/sclounge/ (τελευταία πρόσβαση 5/12/2021).

αλγόριθμοι κρυπτογραφήσεως (timing), και επίσης οι ηλεκτρομαγνητικές εκροές (electromagnetic emanations[90]).

- Στην δεκαετία του 2000 η εμφάνιση και σταδιακή εδραίωση του Cloud οδήγησε την έρευνα στην μελέτη των απομακρυσμένων SCAs, κάποιες εκ των οποίων διαμεσολαβούνταν από την χρήση κακόβουλου λογισμικού που διευκόλυνε την εκτέλεση μιας επιθέσεως πλευρικού καναλιού. Κατά την περίοδο αυτή μελετιούνται και έτεροι τύποι επιθέσεων πλευρικού καναλιού που εύλογα εστιάζουν περισσότερο στο λογισμικό και δεν απαιτούν απαραιτήτως να υπάρχει εγγύτητα επιτιθέμενου-συσκευής, δύο τέτοια παραδείγματα αποτελούν οι επιθέσεις εναντίον της cache memory (π.χ. cache-timing attacks[91]) όπως επίσης και οι επιθέσεις που επιχειρούν να προξενήσουν υπερχείλιση (π.χ. DRAM row buffer attacks[92]).
- Την τελευταία δεκαετία, ένα τμήμα της βιβλιογραφίας, ασχολήθηκε επισταμένα με τις επιθέσεις πλευρικού καναλιού κατά έξυπνων κινητών (smart phones, lightweight devices κλπ) και οι οποίες εκμεταλλεύονταν την εκτεταμένη εφαρμογή και χρήση αισθητήρων (sensors) και εφαρμοσμένων χαρακτηριστικών (embedded features[93]) που αξιοποιούνται στο πλαίσιο της δημιουργίας, εγκατάστασης, και χρήσης διαφόρων εφαρμογών (applications[94]) , καθώς επίσης και την κατανάλωση ρεύματος από το σύστημα αρχείων (proc filesystem) για την ανάκτηση πληροφοριών σχετικά με τους χρήστες των συσκευών αυτών[95].

Μέσα από αυτή την σχετικά συνοπτική ιστορική αναδρομή καθίσταται αντιληπτό πως οι SCAs συν τω χρόνο παραμένουν μια ενεργή απειλή χωρίς απαραίτητα να παραλλάζουν ιδιαίτερα τον αρχικό σχεδιασμό τους (π.χ. σε ότι αφορά το σύνολο των εκροών που μπορούν να εκμεταλλευτούν). Από την άλλη μεριά η τεχνολογική πρόοδος όχι μόνο αυξάνει την επιφάνεια πιθανής επιθέσεως (π.χ. αισθητήρες κλπ) αλλά και αναδεικνύει νέους παράγοντες

---

[90] Spreitzer, R., & Moonsamy, V., & Korak, T., &Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1,465-488 (1-24), σ.1. doi : 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[91] Ο.π.

[92] Ο.π.

[93] Ο.π.

[94] Ο.π.

[95] Ο.π.

διακινδύνευσης (risk) που δυσχεραίνουν το εγχείρημα χαρτογράφησης και εντοπισμού μιας SCA , καθώς από τις απειλές που πάλαι ποτέ μπορούσαν να υλοποιηθούν μόνο από τα κράτη φτάνουμε στον 21ο αιώνα σε SCAs που δύνανται να εκτελεστούν με χαμηλό κόστος και από δυνάμει επιτιθέμενους που δεν έχουν απαραίτητα πρόσβαση σε κρατικούς πόρους. Καθώς μεταξύ άλλων οι κρίσιμες υποδομές ενσωματώνουν πλήθος συσκευών και εφαρμογών που δεν είναι καταρχήν στοιχεία των υποδομών αυτών, και άρα δημιουργούν δυσκολίες σε ότι αφορά τα προαπαιτούμενα για την προστασία όλων των ετερογενών στοιχείων αυτών (ενσωματωμένα συστήματα, κινητές συσκευές, ατομικοί εξοπλισμοί, προσωπικές συσκευές κλπ).

Τούτου δοθέντος, η σύντομη ιστορική παράθεση χρησιμεύει στο να αναδείξει τις δυσχέρειες στην (κατά το δυνατόν) πλήρη και ολοκληρωμένη κατηγοριοποίηση των SCAs, ώστε αυτή η τελευταία να μπορέσει να χρησιμεύσει ως κατευθυντήριος γραμμή για την εφαρμογή των κατάλληλων αντιμέτρων (μεταξύ άλλων). Τις δυσχέρειες ενός ή διαφόρων εγχειρημάτων κατηγοριοποιήσεως των SCAs (και) εν σχέση με τις κρίσιμες υποδομές θα επιχειρήσουμε να καταδείξουμε στην υπό-ενότητα που ακολουθεί.

Υπό-ενότητα 2.2: Σχετικά με τις κατηγοριοποιήσεις των επιθέσεων πλευρικού καναλιού

Η παρούσα υπό-ενότητα αφιερώνεται στην ανάλυση των δύο ακόλουθων προβληματικών:

- Εν πρώτοις, η προβληματική που αφορά στην καταγραφή των δυσχερειών που αναφύονται κατά την προσπάθεια συγκρότησης μιας περιεκτικής κατηγοριοποίησης των SCAs. Η δυσχέρεια αφορά ιδιαίτερα στα κριτήρια με βάσει τα οποία καταρτίζεται μια τέτοια κατηγοριοποίηση σε ότι αφορά (και) τις επιθέσεις πλευρικού καναλιού.
- Εν δευτέροις, η προβληματική που σχετίζεται με την εν γένει σημασία που ενέχει το εγχείρημα περί της ορθής και περιεκτικής κατηγοριοποιήσεως για το ζήτημα των κρίσιμων υποδομών. Ήτοι, πως ακριβώς η ασφάλεια των κρίσιμων υποδομών ενισχύεται από μια τέτοια καταγραφή, και επίσης πως οι σχετικές αδυναμίες μιας τέτοιας καταγραφής μπορούν να λειτουργήσουν ενισχυτικά σε ότι αφορά στην επιτυχή διενέργεια μιας ή πολλών επιθέσεων πλευρικού καναλιού κατά μιας ή περισσότερων κρίσιμων υποδομών.

Η πληθώρα των επιθέσεων πλευρικού καναλιού (είτε αυτές ερευνώνται κατά μονάς είτε συνδυαστικά) έχει εύλογα οδηγήσει στην παραγωγή μιας εκτενούς βιβλιογραφίας η οποία και πραγματεύεται το ζήτημα της κατηγοριοποίησης ή των κατηγοριοποιήσεων, είτε υπό το πρίσμα μιας ευρύτερης επισκόπησης[96] είτε υπό την προοπτική μιας συγκεκριμένης υποκατηγορίας των SCAs κάθε φορά[97]. Ανεξάρτητα όμως από το πώς διαρθρώνεται ένα άρθρο το οποίο θα αφορά στην προσπάθεια κατηγοριοποίησης των SCAs, η προσπάθεια περιεκτικής κατηγοριοποίησης πολλές φορές προσκρούει στο ότι οι κατηγοριοποιήσεις αυτές δομούνται γύρω από έναν μεμονωμένο θεματικό άξονα. Πράγματι, πολλές κατηγοριοποιήσεις οργανώνονται γύρω από μια μεταβλητή ή θεματική, όπως φέρ' ειπείν:

- Ο βαθμός διείσδυσης (invasiveness): Αφορά στον βαθμό διείσδυσης στον οποίο πρέπει να φτάσει μια SCAs για να καταστεί η εκτέλεση της επιτυχής (π.χ. depackaging[98][99]).

---

[96] Ενδεικτικά βλ., Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313, σ.285 κε. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer. https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[97] Όπως οι Microarchitectural Attacks επί παραδείγματι, Lou, X., & Zhang, T., & Jiang, J., Zhang, Y.(2021). A Survey of Microarchitectural Side-channel Vulnerabilities, Attacks, and Defenses in Cryptography. *ACM Computing Surveys, 54(6),* 1-37, σ.6 κε. doi: 10.1145/3456629. https://arxiv.org/pdf/2103.14244.pdf (τελευταία πρόσβαση 29/11/2021).

[98] Ενδεικτικά βλ., Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.306. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies*(σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[99] Για μια τέτοια περίπτωση ορά το σχήμα στο ακόλουθο άρθρο, Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices.

❖ Προσαρμοστικότητα (Adaptability): αφορά στο κατά πόσο μια επίθεση μπορεί να προσαρμοστεί σε πολλές διαφορετικές περιπτώσεις-μελέτης (π.χ. από το ένα λογισμικό στο άλλο κλπ[100]).

❖ Απόδοση (Performance): Κυρίως αφορά στην ταχύτητα με την οποία μπορεί να εκτελεστεί μια SCA, λαμβάνοντας υπόψη και τις απαιτούμενες για την κάθε επίθεση, κάθε φορά, προϋποθέσεις (π.χ. εξοπλισμός[101][102]).

❖ Βαθμός περιπλοκότητας(Complexity): Σε αυτή την μεταβλητή το ενδιαφέρον επικεντρώνει στην πολυπλοκότητα που προϋποθέτει η επιτυχής εκτέλεση μιας οποιασδήποτε SCA (π.χ. σε πόσους τομείς πρέπει να εκτείνεται το γνωστικό υπόβαθρο του επιτιθέμενου σε ότι αφορά στην invasive SCAs επί παραδείγματι[103]).

Η εργασία των Tsalis et al προσπαθεί να προτείνει μια συνδυαστική κατηγοριοποίηση όπως η ανωτέρω, παρόλα αυτά οι περισσότερες κατηγοριοποιήσεις όπως τονίζουν και οι ίδιοι αυτοί συγγραφείς στο πόνημα τους παρουσιάζουν ορισμένους περιορισμούς, οι οποίοι και σαφώς τις οδηγούν στο να επικεντρώνουν σε μια (ή ορισμένες) μόνο θεματικές. Οι περιορισμοί αυτοί συνοψίζονται κατωτέρω ως εξής:

---

*IEEE Communications Surveys & Tutorials, vol. XX,No. Z,Month YYYY,*1-24(465-488),σ.2. doi :10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[100] Ο.π.

[101] Ο.π.

[102] Σχετικά με την εν λόγω μεταβλητή ένα παράδειγμα που αφορά σε microarchitectural SCAs παρατίθεται και στο ακόλουθο άρθρο μεταξύ άλλων, Lou, X., & Zhang, T., & Jiang, J., Zhang, Y.(2021). A Survey of Microarchitectural Side-channel Vulnerabilities, Attacks, and Defenses in Cryptography. *ACM Computing Surveys, 54(6),* 1-37,σ.23. doi: 10.1145/3456629. https://arxiv.org/pdf/2103.14244.pdf (τελευταία πρόσβαση 29/11/2021).

[102] Ο.π.

- Αρχικά, οι διαφορετικές κατηγοριοποιήσεις επιχειρούν πολλές φορές να επιτύχουν διαφορετικούς σκοπούς ανάλογα με την θεματική και τι επιδιώκεται μέσα από την διερεύνηση αυτής[104][105][106].

- Δεύτερον, οι διάφορες κατηγοριοποιήσεις , βάσει και των στόχων που έχουν τεθεί, μπορεί αρκετές φορές να ενέχουν μια διαφορετική (ως προς την μεταξύ τους σύγκριση[107]) δομή που να δυσχεραίνει το εγχείρημα την

---

[104] Ο.π.,σ.284.

[105] Αν για παράδειγμα ο στόχος είναι μια σύνοψη, όπως στο Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.284 κε. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham :Springer. https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021). ή αν ο στόχος είναι να προταθούν/διερευνηθούν (και) κάποια αντίμετρα, όπως στο Lou, X., & Zhang, T., & Jiang, J., Zhang, Y.(2021). A Survey of Microarchitectural Side-channel Vulnerabilities, Attacks, and Defenses in Cryptography. *ACM Computing Surveys, 54(6),* 1-37,σ.16 κε. doi: 10.1145/3456629. https://arxiv.org/pdf/2103.14244.pdf (τελευταία πρόσβαση 29/11/2021).

[106] Σε αυτό συμβάλλει και το γεγονός ότι η προσοχή που εδόθη στις επιθέσεις πλευρικού καναλιού δεν κατανέμεται ισομερώς σε όλες τις υποκατηγορίες (επί παραδείγματι μια σειρά άρθρων ασχολείται κάπως περισσότερο με ηλεκτρομαγνητικές επιθέσεις, electromagnetic, και επιθέσεις ανάλυσης ισχύος, power analysis, απ' ότι με άλλες μορφές). Στο άρθρο που εδώ παραθέτουμε ο λόγος γίνεται εν γένει για κυβερνοεπιθέσεις, Staddon, E., & Loscri, V., & Mitton, N.(2021). Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Applied Sciences,2021,11,7228,* 1-39, σ.20. doi: https://doi.org/10.3390/app11167228. Applied Sciences | Free Full-Text | Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey (mdpi.com) (τελευταία πρόσβαση 16/9/2021).

[107] Ειδικότερα αυτό μπορεί να παρατηρηθεί σε επιστημονικά πονήματα που περιλαμβάνουν εκτέλεση επιθέσεως πλευρικού καναλιού σε πειραματική συνθήκη, για παράδειγμα στο άρθρο των Steiner et al για τις εκροές κατά την ομιλία μέσω κινητού τηλεφώνου που σχετίζονται με τις κινήσεις του προσώπου κατά την άρθρωση και το πώς μέσω των αισθητήρων του κινητού που εντοπίζουν αυτές τις κινήσεις μπορεί να υπάρξει εκροή που με την βοήθεια της μηχανικής μάθησης να ανασυγκροτεί το περιεχόμενο της ομιλίας. Στην δομή του συγκεκριμένου άρθρου περιλαμβάνετε και μια ενότητα για τις διαφορές που υφίστανται ανάμεσα στην δική τους πειραματική συνθήκη και στην αρθρογραφία με παραπλήσια θεματολογία, όπως σε ότι αφορά την τοποθέτηση του κινητού κατά την ομιλία, και επίσης σε ότι αφορά στο attack vector που αξιοποιείται (κίνηση στόματος/ομιλία έναντι αισθητήρων κίνησης που μελετάται σε παραπλήσια αρθρογραφία). Για μια λεπτομερέστερη καταγραφή αυτών και άλλων διαφορών ορά το ακόλουθο άρθρο, Steiner, I.G., & LeFevre, Z., & Serwadda,A.(2020). Smartphone Speech Privacy Concerns from Side-Channel Attacks on Facial Biomechanics. *Computers & Security,vol.100,*1-

ομοιογένειας ή της συγκρισιμότητας[108][109](επί παραδείγματι σε κάποια άρθρα μπορεί να υπάρχουν αλληλοεπικαλύψεις κατηγοριών SCAs[110], ή ενδεχομένως να χρησιμοποιούνται διαφορετικές ονομασίες για την μια και την αυτή κατηγορία επιθέσεως πλευρικού καναλιού[111]).

16,σ.5.doi:10.1016/j.cose.2020.102110. https://www.researchgate.net/publication/345906717_Smartphone_Speech_Privacy_Concerns_from_Side-Channel_Attacks_on_Facial_Biomechanics (τελευταία πρόσβαση 14/12/2021).

[108] Ο.π.

[109] Για παράδειγμα σε ένα άρθρο ο χώρος μπορεί να αφιερώνεται, εν μέρει, στην διαφορά ανάμεσα στις SCAs και σε άλλες επιθέσεις, π.χ. Spreitzer, R., & Moonsamy, V., & Korak, T., &Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1,465-488 (1-24),σ.4. doi : 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021). ενώ σε έτερο άρθρο ο χώρος (έστω εν μέρει) μπορεί να αφιερώνεται στο εγχείρημα μιας εξαντλητικής κατηγοριοποίησης μιας υποκατηγορίας SCA και των αντιμέτρων που προτείνονται, π.χ. Lyu, Y., & Mishra, P..(2017). A Survey of Side-Channel Attacks on Caches and Countermeasures. *Journal of Hardware and Systems Security,*2,33-50(2018), σ.35 κε.doi:https://doi.org/10.1007/s41635-017-0025-y. https://esl.cise.ufl.edu/Publications/hass18.pdf (τελευταία πρόσβαση 22/11/2021).

[110] Για μια παρατήρηση που αφορά στην χρήση περισσότερων της μιας υποκατηγορίας, που όμως αναφέρονται στις κυβερνοεπιθέσεις γενικά, ορά και το ακόλουθο άρθρο, Staddon, E., & Loscri, V., & Mitton, N.(2021). Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Applied Sciences,2021,11,7228,*1-39,σ.20.doi: https://doi.org/10.3390/app11167228. Applied Sciences | Free Full-Text | Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey (mdpi.com) (τελευταία πρόσβαση 16/9/2021).

[111] Για παράδειγμα οι cache SCAs αναφέρονται ως τέτοιες στο ακόλουθο άρθρο, Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham :Springer. https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021). Ενώ σε έτερο άρθρο που αφορά σε παράθεση και περιγραφή μόνο των cache SCAs εκεί χρησιμοποιείται ο γενικότερος περιγραφικός όρος Microarchitectural, βλ. ενδεικτικά Lou, X., & Zhang, T., & Jiang, J., Zhang, Y.(2021). A Survey of Microarchitectural Side-channel Vulnerabilities, Attacks, and Defenses in Cryptography. *ACM Computing Surveys, 54(6),* 1-37,σ.6 κε. doi: 10.1145/3456629. https://arxiv.org/pdf/2103.14244.pdf (τελευταία πρόσβαση 29/11/2021).

❖ Τρίτον, ο εκάστοτε συγγραφέας ή συγγραφική ομάδα (όπως προαναφέρθηκε) εισάγουν την δική τους υποκειμενική οπτική (ήτοι πολλαπλές προσεγγίσεις) στο εκάστοτε πόνημα, με αποτέλεσμα τα επιστημονικά αυτά πονήματα να μην είναι εύκολα συγκρίσιμα μεταξύ τους ή να μην υφίσταται μια «συνέχεια» από το ένα άρθρο στο επόμενο κλπ[112].

Έχοντας διατρέξει συνοπτικά τους περιορισμούς που αφορούν στα εκάστοτε εγχειρήματα περί της κατηγοριοποίησης των επιθέσεων πλευρικού καναλιού, καλούμαστε πλέον να προχωρήσουμε σε μια συνοπτική παράθεση των επιμέρους υποκατηγοριών[113] που συνθέτουν το σύνολο (ή έστω την κρίσιμη πλειοψηφία) των επιθέσεων πλευρικού καναλιού[114][115].

[112] Ο.π.

[113] Τονίζεται ξανά εδώ ότι ο αριθμός των υποκατηγοριών μπορεί να ποικίλει ανά άρθρο, π.χ. οι Montasari et al. Αναφέρονται στις μικροαρχιτεκτονικές (microarchitectural) επιθέσεις ως έχουσες 13 υποκατηγορίες, στις οποίες μεταξύ άλλων τοποθετούν τόσο τις timing όσο και τις electromagnetic αλλά και τις cache SCAs, οι οποίες στην ακόλουθη κατηγοριοποίηση του κυρίως κειμένου του ανά χείρας πονήματος αντιμετωπίζονται ως υποκατηγορίες των SCAs γενικά, έτσι φαίνεται και πάλι πως οι ταξινομήσεις μπορούν να ποικίλουν και ως προς το πώς ορίζονται οι υποκατηγορίες μιας υποκατηγορίας των SCAs, δηλαδή σε ότι αφορά στην σχέση γενικού (όρου ομπρέλα)-ειδικού (υποτύπων) και σε ότι αφορά στο υποκειμενικό στοιχείο της σχεδίασης του εκάστοτε άρθρου, εύλογα η παρατήρηση αυτή περιπλέκει τόσο το θεωρητικό όσο και το πρακτικό σκέλος της εμπειρικής σημασίας του όποιου εγχειρήματος ταξινόμησης. Ενδεικτικά παραθέτουμε τις 13 υποκατηγορίες που ονομαστικά αναφέρουν οι παραπάνω συγγραφείς ότι έχουν εντοπίσει στην διεθνή βιβλιογραφία (μέχρι το 2018) στο δικό τους πόνημα, «*Acoustic Cryptanalysis Attack, Branch-Prediction Attack, Cold Boot Attack, Cache Attack, Differential Fault Analysis Attack, DMA Attack, Electromagnetic Attack, Fault-Attacks, Lucky-Thirteen Attack, Pass the Hash Attack, Power-Analysis Attack, Tempest Attack, and Timing Attack*». Montasari, R., & Hosseinian-Far, A., & Hill, R., & Montaseri, F., & Sharma, M., & Shabbir, Sh.(2018). Are Timing-Based Side-Channel Attacks Feasible in Shared, Modern Computing Hardware ?. *International Journal of Organizational and Collective Intelligence,8,2,*32-59,σ.. doi: 10.4018/IJOCI.2018040103. https://pure.hud.ac.uk/ws/portalfiles/portal/13423218/Are_Timing_Based_Side_Channel_Attacks_Feasible_in_Shared_Modern_Computing_Hardware_.pdf (τελευταία πρόσβαση 24/12/2021).

[114] Οι μεταφράσεις των αγγλόφωνων όρων που ακολουθούν είναι του συγγραφέως.

[115] Για τους σκοπούς της παράθεσης που ακολουθεί λαμβάνεται υπόψη η προαναφερθείσα κατηγοριοποίηση, και επιπλέον για λόγους πληρότητας της ανάλυσης μας προσθέτουμε όπου χρειάζεται και συμπληρωματικές πληροφορίες για τις επιμέρους SCAs από έτερες βιβλιογραφικές πηγές.

Ακουστικές επιθέσεις πλευρικού καναλιού (Acoustic Attacks):

Πρόκειται για επιθέσεις που στόχο έχουν να εκμεταλλευτούν τις ακουστικές εκροές ώστε να μπορέσουν οι επιτιθέμενοι που τις αξιοποιούν να λάβουν πληροφορίες σχετικά με την λειτουργία ενός υπολογιστικού συστήματος (π.χ. να αποκρυπτογραφήσουν τμήμα ή το σύνολο ενός ciphertext που παράγει ένας αλγόριθμος κρυπτογραφίας[116]). Επί παραδείγματι, οι Schwarzl et al. εξέτασαν την δυνατότητα εξαγωγής πληροφοριών μέσα από συσχετίσεις ανάμεσα στον χρόνο αποσυμπίεσης αρχείων (decompression time) και σε διάφορα άλλα χαρακτηριστικά των αρχείων αυτών (π.χ. εντροπία, σχετική θέση και ευθυγράμμιση των δεδομένων του αρχείου προς αποσυμπίεση κλπ[117]). Για τον σκοπό αυτό χρησιμοποιείται κατά την πειραματική συνθήκη ο αλγόριθμος *Comprezzor* ο οποίος με την λειτουργία του ως fuzzer παρατηρεί και καταγράφει την χρονική διάρκεια που απαιτείται για να αποσυμπιεστούν τα bits ώστε να καθίσταται εφικτή μια επίθεση είτε τύπου dictionary είτε bytewise[118]. Για παράδειγμα όταν υφίστανται δεδομένα που για κάποιο λόγο δεν μπορούν να συμπιεστούν (incompressible) , σε αυτές τις περιπτώσεις εύλογα η αποσυμπίεση για το συγκεκριμένο bit είναι ταχύτερες εν σχέση με ένα bit που έχει προηγουμένως συμπιεστεί[119].

[116] Σαν υποκατηγορία επιθέσεων πλευρικού καναλιού οι ακουστικές επιθέσεις δεν λαμβάνουν μέχρι πρότινος την μερίδα του λέοντος σε ότι αφορά την βιβλιογραφική παραγωγή και ανασκόπηση, εν αντιθέσει με άλλες κατηγορίες που ακολουθούν κατωτέρω (π.χ. electromagnetic attacks). Βλ. ενδεικτικά και Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[117] Schwarzl, M., & Borrello, P., & Saileshwar, G., & Muller, H., Schwarz, M., & Gruss, D.(2021). Practical Timing Side Channel Attacks on Memory Compression. *Arxiv:2111.08404v1 [cs.CR]*,1-18,σ.1. https://arxiv.org/abs/2111.08404 (τελευταία πρόσβαση 24/12/2021).

[118] Ο.π.,σ.6.

[119] Ο.π.,σ.7.

Επιθέσεις πλευρικού καναλιού κατά προσωρινής μνήμης (Cache-based Attacks):

Υποκατηγορία επιθέσεων πλευρικού καναλιού που ως στόχο της έχει τμήματα της μνήμης cache, ο επιτιθέμενος μεταξύ άλλων προχωρά σε καταγραφή του χρόνου (π.χ. delays) που χρειάζεται για να εκτελεστούν οι οδηγίες προς την μνήμη cache και με τον τρόπο αυτό δύναται να εξάγει χρήσιμες πληροφορίες[120]. Εν άλλοις λόγοις, ο επιτιθέμενος μετρά την χρονική καθυστέρηση που παρατηρείται κατά την πρόσβαση σε δεδομένα που είναι αποθηκευμένα στα ιεραρχημένα επίπεδα μνήμης του υπολογιστικού συστήματος, ούτως ώστε να κατανοήσει τον τρόπο με τον οποίο το εκάστοτε υπολογιστικό σύστημα οργανώνει την πρόσβαση στην μνήμη γενικά ("*memory access pattern*[121]").Η υποκατηγορία αυτή δύναται όπως διακριθεί στις ακόλουθες επιθέσεις έναντι της cached memory, ήτοι:

- Evict + Time: ο επιτιθέμενος μετρά τον χρόνο που απαιτείται για να εκτελεστεί μια λειτουργία του υπολογιστικού συστήματος[122]. Η συγκεκριμένη επίθεση αποτελείται από τρία βήματα, πρώτον ο επιτιθέμενος ενεργοποιεί μια διαδικασία (π.χ. κρυπτογράφηση), δεύτερον, ο επιτιθέμενος γεμίζει ένα τμήμα του cache με τα δικά του δεδομένα για να αφήσει εκτός εκείνα του στόχου του (evict), τρίτον η αρχική λειτουργία ενεργοποιείται εκ νέου ώστε ο επιτιθέμενος να παρατηρήσει τις χρονικές αποκλίσεις ανάμεσα στο πρώτο και το τρίτο βήμα[123].

---

[120] Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[121] Lyu, Y., & Mishra, P..(2017). A Survey of Side-Channel Attacks on Caches and Countermeasures. *Journal of Hardware and Systems Security,*2,33-50(2018), σ. 34-35. doi: https://doi.org/10.1007/s41635-017-0025-y. https://esl.cise.ufl.edu/Publications/hass18.pdf (τελευταία πρόσβαση 22/11/2021).

[122] Ο.π.,σ.39.

[123] Ο.π.

- Prime + Probe: Λειτουργεί αντιστρόφως σε σχέση με την προηγούμενη επίθεση, ο επιτιθέμενος αρχικά φορτώνει τα δικά του δεδομένα σε ένα τμήμα της cache μνήμης, κατόπιν ο υπολογιστής στόχος φορτώνει κι εκείνος δεδομένα στην προσπάθεια του να εκτελέσει μια δική του λειτουργία[124]. Στο τρίτο βήμα ο επιτιθέμενος αποκτά ξανά πρόσβαση στα δικά του δεδομένα από το πρώτο βήμα, και αν (με βάση την χρονική μέτρηση που πρέπει να κάνει) η φόρτωση των δεδομένων διαρκεί επί μακρό τότε ο υπολογιστής στόχος έχει και αυτός καταγράψει τα δεδομένα του στην ίδια διαδρομή με τον επιτιθέμενο (ήτοι ίδιο cache mapping[125]), με αποτέλεσμα να γίνει έξωση των δεδομένων του τελευταίου και γι' αυτό η φόρτωση διαρκεί περισσότερο (cache miss[126]). Σε αντίθετη περίπτωση η διαδικασία κρατά σαφώς λιγότερο (cache hit[127]).
- Flush + Reload: Και αυτή η επίθεση περιλαμβάνει τρία βήματα και επί της ουσίας παραλλάσει την αμέσως προηγούμενη (Prime+Probe[128]). Αρχικά, ο επιτιθέμενος αφαιρεί (flush) μια γραμμή μνήμης από το cache. Στην συνέχεια αναμένει ο υπολογιστής στόχος να φορτώσει στο cache τα δεδομένα για κάποια λειτουργία που θέλει να εκτελέσει, και τέλος ο επιτιθέμενος μετρά τον χρόνο που χρειάζεται για την επαναφόρτιση της γραμμής μνήμης που είχε αφαιρεθεί στο πρώτο βήμα[129]. Ανάλογα με το αν ο στόχος προχωρά σε επαναφόρτιση των δεδομένων πριν ή μετά την εκτέλεση τότε και ο χρόνος για την εκτέλεση των λειτουργιών θα διαφοροποιηθεί ανάλογα, έτσι ο επιτιθέμενος θα λάβει τις κατάλληλες μετρήσεις για να αποτυπώσει το ακριβές μονοπάτι εκτέλεσης λειτουργιών στην μνήμη cache του υπολογιστή στόχου[130].

[124] Ο.π.

[125] Ο.π.

[126] Ο.π.

[127] Ο.π.

[128] Ο.π.,σ.40.

[129] Ο.π.,σ.39.

[130] Ο.π.

Ηλεκτροακουστικές επιθέσεις πλευρικού καναλιού (Electroacoustic Attacks):

Οι ηλεκτροακουστικές επιθέσεις δεν παρουσιάζονται συχνά στην βιβλιογραφία που μελετήθηκε (μόνο μια φορά παρατηρήθηκε η συγκεκριμένη ονομασία, σε αντίθεση με τις ηλεκτρομαγνητικές επιθέσεις που αναφέρονται κατωτέρω). Εντούτοις, η σπανιότητα της υποκατηγορίας αυτής χρησιμεύει στο να καταδείξει δύο ενδιαφέροντα στοιχεία. Πρώτον, λειτουργεί ως παράδειγμα για το πώς οι SCAs μπορούν να λειτουργήσουν ως αντίμετρα. Δεύτερον, αποτελεί ένα κατατοπιστικό παράδειγμα του πως οι SCAs δύνανται να πλήξουν την ακεραιότητα του περιεχομένου της πληροφορίας (integrity, κατωτέρω αναφέρεται και μια σχετική ταξινόμηση με βάσει τις SCAs και το CIA). Τα δύο αυτά στοιχεία συνοψίζονται στο άρθρο των Vincent et al., όπου μια κεραία PZT τοποθετείται στην παραγωγή εξαρτημάτων (στο πλαίσιο του SHM, structural health monitoring), ώστε να αντληθεί και ελεγχθεί η υπογραφή ηλεκτρικής εμπέδησης/αντίστασης (impedance signature). Με τον τρόπο αυτό είναι εφικτό να ελεγχθούν εν τέλει τυχόν παρεμβάσεις ή/και αλλοιώσεις στα εξαρτήματα που παράχθηκαν, με τον τρόπο αυτό μπορεί μέσω μιας SCA να ελεγχθεί και το integrity[131].

Ηλεκτρομαγνητικές επιθέσεις πλευρικού καναλιού (Electromagnetic Attacks):

Σε αυτό τον τύπο επιθέσεως πλευρικού καναλιού ο επιτιθέμενος παρατηρεί και καταγράφει τις ηλεκτρομαγνητικές εκροές με στόχο να κατανοήσει τις αιτιακές σχέσεις ανάμεσα στην εκροή και την εργασία που το υπολογιστικό σύστημα εκτελεί κάθε φορά[132]. Οι εν λόγω επιθέσεις παρουσιάζουν ορισμένες ομοιότητες και με τις επιθέσεις ανάλυσης

[131] Ορά Vincent et al. στο Tsalis et al. ο.π.,σ.288.

[132]. Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos (Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

ισχύος (power analysis SCAs), και γενικά μπορούν να διακριθούν όπως και οι τελευταίες σε δύο κυρίως υποκατηγορίες[133]:

- Απλή ηλεκτρομαγνητική ανάλυση (SEMA): στην υποκατηγορία αυτή ο επιτιθέμενος παρατηρεί επισταμένως είτε την χρονική διάρκεια της ηλεκτρομαγνητικής εκροής (time-domain) είτε μετατρέπει την ηλεκτρομαγνητική εκροή σε συχνότητα (frequency-domain) για να παρατηρήσει το λεγόμενο frequency pattern και από εκεί να αντλήσει πληροφορίες[134].
- Διαφορική ηλεκτρομαγνητική ανάλυση (DEMA): εδώ ο επιτιθέμενος λαμβάνει έναν μεγάλο αριθμό από ηλεκτρομαγνητικές εκροές και στόχος του είναι να βρει τις διαφοροποιήσεις ανάμεσα σε αυτό τον μεγάλο αριθμό εκροών, π.χ. σε ορισμένες περιπτώσεις μια αύξηση των εκροών σημαίνει ότι ο επεξεργαστής εκτελεί μια λειτουργία κρυπτογράφησης κλπ[135].

Επιθέσεις πλευρικού καναλιού εκμεταλλευόμενες σφάλματα (Fault Attacks):

Σε αυτή την υποκατηγορία ανήκουν εκείνες οι επιθέσεις πλευρικού καναλιού για την εκτέλεση των οποίων ο επιτιθέμενος χρειάζεται να εκμεταλλευθεί την ύπαρξη σφαλμάτων (faults) κατά την εκτέλεση κάποιου κρυπταλγόριθμου στην συσκευή στόχο[136]. Πρόκειται κυρίως για υποκατηγορία που επικεντρώνει κυρίως τόσο σε επεμβατικές μορφές SCA(invasive forms) που απαιτούν γνώσεις decapsulation για παράδειγμα, όσο και σε

---

[133] Sayakkara, A, & Le-Khac, N.A., & Scanlon, M.(2019). A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics. *Elsevier Digital Investigations,arXiv:1903.07703v1[cs.CR]*,1-13,σ.6. https://arxiv.org/pdf/1903.07703.pdf (τελευταία πρόσβαση 12/10/2021).

[134] Ο.π.

[135] Ο.π.

[136] Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.286. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

περιπτώσεις όπου οι SCAs μπορούν να χρησιμοποιηθούν επιθετικά (offensive, ήτοι να προκαλέσουν ζημιά στην λειτουργία της συσκευής στόχου). Οι Riviere et al. επί παραδείγματι αξιοποίησαν μια επίθεση σφάλματος (συγκεκριμένα ηλεκτρομαγνητικού σφάλματος, Electromagnetic Fault Injection, EMFI), για να μπορέσουν να υπερκεράσουν ορισμένες οδηγίες που περιλαμβάνονται σε μικροελεγκτές ARM (ARM microcontrollers[137]).

Επιθέσεις πλευρικού καναλιού κατά μνήμης (Memory Attacks):

Πρόκειται κατά κύριο λόγο για παραλλαγή της προαναφερθείσας cache-based attack, με βασική διαφορά το ότι ο επιτιθέμενος έχει ως στόχο κάποιο άρθρωμα (π.χ. λειτουργίες read ή write) μνήμης (memory module)[138]. Η υποκατηγορία αυτή , σε ένα τμήμα της βιβλιογραφίας, φέρει κοινά σημεία με τις επιθέσεις ανάλυσης ισχύος (power analysis) και επίσης με τις ηλεκτρομαγνητικές επιθέσεις (electromagnetic attacks). Σε ορισμένες περιπτώσεις ίσως είναι εφικτό να τεθεί ο ισχυρισμός πως οι επιθέσεις κατά μνήμης δεν είναι ξεχωριστές από τις άλλες δύο υποκατηγορίες, αλλά περισσότερο φαίνεται ως αν οι πρώτες να είναι μια επιθετική εφαρμογή (π.χ. μια fault injection attack[139]) των άλλων δύο (ή πως υπάρχει μια αλληλοεπικάλυψη μεταξύ των δύο αυτών κατηγοριών, και πως και πάλι είναι δύσκολο να ταξινομηθούν κατά μονάς ή ιδεοτυπικά).

Επί παραδείγματι, οι Khan et al. χρησιμοποίησαν σε πειραματική συνθήκη NVM chips (Non-Volatile Memories) και μέσα από την χρήση μιας Differential Power Analysis

---

[137] Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1,465-488 (1-24),σ.9. doi:10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[138] Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[139]Khan & Gosh, πρβλ. Khan, M.N.I., & Bashin, Sh., & Liu, B., & Yuan, A., & Chattopadhyay, A., & Ghosh, S.(2021). Comprehensive Study of Side-Channel Attack on Emerging Non-Volatile Memories. *Journal of Low Power Electronics and Applications, 2021, 11(4),38*,1-18,σ.2 . doi: https://doi.org/10.3390/jlpea11040038. https://www.mdpi.com/2079-9268/11/4/38 (τελευταία πρόσβαση 15/1/2022).

SCA έλαβαν τις μετρήσεις της τάσης του ρεύματος για να αποσπάσουν το μυστικό κλειδί από το chip(παρατήρησαν πως ανάλογα με το αν πρόκειται για διεργασία write ή read υπάρχει πτώση στην τάση του ρεύματος ανάλογα με το ποια από τις δύο διεργασίες εκτελείται κάθε φορά και αυτό αποτελεί πηγή διαρροής[140]).

Οπτικές επιθέσεις πλευρικού καναλιού (Optical Attacks):

Κατηγορία επιθέσεων που αφορά σε εξαγωγή πληροφοριών μέσα από την μελέτη διαρροών οπτικής φύσεως (visual), όπως για παράδειγμα αντανακλάσεων της οθόνης πάνω σε αντικείμενα πλησίον αυτής, καθώς επίσης και μέσα από την καταγραφή της οπτικής ακτινοβολίας (optical radiation) που προκύπτει από διάφορες οθόνες, τύπου LED επί παραδείγματι[141]. Όπως και σε άλλες υποπεριπτώσεις οι οπτικές επιθέσεις μπορούν αξιοποιηθούν σε διαφορετικούς συνδυασμούς και επομένως να ταξινομηθούν ως παθητικές ή επιθετικές (π.χ. optical fault injection[142]).

Το γεγονός πως οι οπτικές επιθέσεις (όπως και άλλες SCAs) δεν απαντώνται πάντοτε ιδεοτυπικά (δηλαδή κατά μονάς και χωρίς να συνδυάζονται με άλλες κατηγορίες ταξινόμησης) μας επαναφέρει , εν μέρει, στην δυσκολία ορισμού που αναπτύχθηκε στο προηγούμενο κεφάλαιο. Ενώ η έννοια «οπτικές» ως προσδιορισμός στις επιθέσεις παρουσιάζεται ως αρκούντως κατανοητή, εντούτοις ο όρος συγχέει (και αυτό φαίνεται αντίστροφα στις εμπειρικές συνθήκες) διαφορετικά πτυχές και άλλους επιμέρους ορισμούς.

Διότι ο όρος «οπτικός» , αν αναλυθεί προσεκτικά, εμπεριέχει μέσα του τρία (τουλάχιστον) στοιχεία που εκ πρώτης όψεως δεν φαίνεται ότι συγχέονται, αυτά είναι εκείνα

---

[140] Ο.π.,σ.15.

[141] Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[142] Spreitzer, R., & Moonsamy, V., & Korak, T., &Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20,1,1-24(465-488),σ.10.doi:10.1109/COMST.2017.2779824.https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

του φωτισμού (καθαυτό εκροή), της οθόνης (συσκευή που εκπέμπει την εκροή, π.χ. LED) και της αντανάκλασης (ενδεχομένως κάποιο αντικείμενο που βρίσκεται σε απόσταση, και βοηθά σε μα συνδυασμένη εκτέλεση της επίθεσης, όπως τα γυαλιά μυωπίας, άρα ο λόγος αφορά το vicinity). Όμως τα επιμέρους αυτά στοιχεία (είτε οι επιμέρους περιπτώσεις τα περιλαμβάνουν είτε όχι) δεν είναι τα μόνα που περιλαμβάνονται στον ορισμό, καθώς οι Loughry et al. με τον όρο LED προσδιορίζουν και λαμπτήρες συσκευών (π.χ. routers, κάρτες δικτύων, συσκευές φαξ, συσκευές μόντεμ κλπ) και όχι μόνο οθόνες H/Y[143].

Σε αυτό το παράδειγμα, και αφήνοντας κατά μέρος ζητήματα ορισμών, η οπτική εκροή μπορεί δυνητικά να αναφέρεται σε διαφορετικές περιπτώσεις καθώς και να απαιτούνται διαφορετικά εργαλεία (όχι ίσως για την συλλογή αλλά) για την παραπέρα ανάλυση της. Οι Loughry et al. πρότειναν στην μελέτη τους να παρατηρηθούν οι λαμπτήρες συσκευών που επιτρέπουν την διέλευση πακέτων δεδομένων (π.χ. οι λυχνίες σε routers) και έτσι να καταστεί εφικτή η παρακολούθηση και ανακατασκευή της ροής δεδομένων(“*error-free reconstruction*”[144]).

Στο παράδειγμα που μόλις αναφέραμε η οπτική εκροή δεν έχει σχέση με την αντανάκλαση την οποία ενδεχόμενα μπορεί να συλλάβει το ανθρώπινο μάτι (τονίζεται πως και οι εκροές της οθόνης μπορούν να ληφθούν και με άλλους τρόπους επίσης μη δεκτικούς μιας άμεσης αντιληπτικής ικανότητας από την πλευρά του ανθρώπινου ματιού), αλλά αντίθετα σχετίζεται με την ταχύτητα και την φωτεινότητα στην σήμανση που παράγει ο λαμπτήρας της συσκευής (όταν αναβοσβήνει), και άρα θα απαιτούνται και οι υπολογιστικές τεχνικές για την ανάλυση της.

<u>Επιθέσεις πλευρικού καναλιού μέσω ανάλυσης ισχύος (Power Analysis Attacks):</u>

Πρόκειται για επίθεση πλευρικού καναλιού που εκμεταλλεύεται τις διακυμάνσεις στην τροφοδοσία του ρεύματος για να εκτελεστεί επιτυχώς. Οι δύο παραλλαγές στις οποίες απαντάται η εν λόγω επίθεση έχουν ως ακολούθως[145]:

---

[143] Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton,St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer,2021,10.1007/s41635-021-00112-6 . hal-03176249,*1-24,σ.6. https://hal.archives-ouvertes.fr/hal-03176249/document (τελευταία πρόσβαση 15/10/2021).

[144] Ο.π.,σ.6-7.

[145] Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M.

- Απλή ανάλυση ρεύματος (Simple Power Analysis[146]): η μέτρηση της τροφοδοσίας γίνεται με σκοπό να ανακαλύψει ο επιτιθέμενος ποια λειτουργία στο υπολογιστικό σύστημα εκτελείται καθ' εκάστη στιγμή[147].
- Διαφορική ανάλυση ρεύματος (Differential Power Analysis[148]): σε αυτή την περίπτωση απαιτείται από την πλευρά του επιτιθέμενου η χρήση στατιστικών αναλύσεων διότι ο τελευταίος προσπαθεί να μαντέψει, όχι μόνο τις τιμές εισόδου και εξόδου, αλλά επίσης και τις ενδιάμεσες[149].

Επιθέσεις πλευρικού καναλιού κατά αισθητήρων (Sensor-based Attacks):

Υποκατηγορία επιθέσεων πλευρικού καναλιού, ιδιαιτέρως διευρυμένη στην επιστημονική βιβλιογραφία, που εκμεταλλεύεται εκροές (ακουστικές, οπτικές, κίνησης κλπ) που προκύπτουν από τους αισθητήρες (sensors) κατά κύριο λόγο κινητών τηλεφώνων. Η υποκατηγορία αυτή απαντάται και σε συνδυασμό με χρήση κακόβουλου λογισμικού[150] που χρησιμοποιείται συνδυαστικά με την εκροή από τους αισθητήρες, ενώ μια βασική παράμετρος που συνάδει και με την επιτυχή εκτέλεση της επίθεσης αφορά στην δυνατότητα πρόσβασης στους αισθητήρες χωρίς προηγούμενη έγκριση από το λειτουργικό (permission[151]).

Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[146] Ο.π.

[147] Ο.π.

[148] Ο.π.

[149] Ο.π.

[150] Ορά και το ακόλουθο άρθρο, Steiner, I.G., & LeFevre, Z., & Serwadda,A.(2020). Smartphone Speech Privacy Concerns from Side-Channel Attacks on Facial Biomechanics. *Computers &Security,vol.100,*1-16,σ.5.doi:10.1016/j.cose.2020.102110. https://www.researchgate.net/publication/345906717_Smartphone_Speech_Privacy_Concerns_from_Side-Channel_Attacks_on_Facial_Biomechanics (τελευταία πρόσβαση 14/12/2021).

[151] Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.285. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications*

Εδώ η ταξινόμηση υποχρεωτικά περιλαμβάνει και το υλικό και την εκροή (leakage κλπ), ενώ υπονοείται πως μπορεί (όπως και στις άλλες κατηγορίες) να εμφανιστεί συνδυαστικά η επίθεση πλευρικού καναλιού καθώς υπάρχει ποικιλία αισθητήρων σε μια συσκευή, όπως αναφέρουμε και κατωτέρω οι ταξινομήσεις εμφανίζουν αυτό το πρόβλημα, ήτοι το να εμπλέκονται πολλές διαφορετικές μεταβλητές σε αναλύσεις που βασίζονται μόνο σε μια εξ' αυτών. Ορισμένα παραδείγματα επιθέσεων πλευρικού καναλιού που επιτίθενται κατά αισθητήρων είναι και τα ακόλουθα (τα κάτωθεν παραδείγματα επιβεβαιώνουν και το ότι είναι δυσχερές να αποτυπωθούν κατά μονάς υποκατηγορίες επιθέσεων εντελώς ξέχωρες από συνδυαστικούς τύπους επιθέσεων):

- Επίθεση κατά του αισθητήρα πληκτρολογίου αφής (Keyloggers[152]): Όπως και στις ακόλουθες περιπτώσεις οι αισθητήρες δεν προαπαιτούν κάποια έγκριση για να αποκτήσει πρόσβαση στην χρήση τους ο επιτιθέμενος (permission), ενώ σε ένα σενάριο μιας τέτοιας πιθανής επιθέσεως μπορεί να χρησιμέψει και η φωτεινότητα της οθόνης (light emanation), και άρα αυτή μπορεί να είναι δυνάμει συνδυαστική[153]. Σε ότι αφορά τις καθαυτό παραλλαγές υπάρχουν επιθέσεις που σχεδιαστικά εστιάζουν στις συσχετίσεις ανάμεσα σε έναν αισθητήρα (π.χ. GPS ή επιταχυνσιόμετρο) και στην επιλογή των πλήκτρων που λαμβάνει χώρα στην οθόνη αφής[154]. Επίσης είναι καθόλα εφικτό να συνδυαστεί ο αισθητήρας φωτεινότητας (π.χ. μιας κινητής συσκευής) με το επιταχυνσιόμετρο ώστε ο επιτιθέμενος να μπορέσει να αντιληφθεί τι πληκτρολογείτε στην οθόνη αφής από τον τρόπο που μπορεί να αυξομειώνεται η φωτεινότητα κάθε φορά που η συσκευή αλλάζει θέση η περιστρέφεται[155].

Infrastructure Security and Resilience Theories, Methods, Tools and Technologies (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[152] Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1, 465-488 (1-24),σ.13. doi : 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[153] Ο.π.

[154] Βλ. Cai & Chen ο.π.

[155] Βλ. Spreitzer ο.π.

- Επίθεση που εκμεταλλεύεται τις προσωποποιημένες επιλογές/συμπεριφορές του χρήστη της συσκευής για να εκτελεστεί (Fingerprinting[156]): Έχει παρατηρηθεί πως οι αστοχίες στην κατασκευή αισθητήρων σε συνδυασμό (και) με την χρήση της γλώσσας Javascript δύνανται όπως επιτρέψουν στον επιτιθέμενο να προχωρήσει σε fingerprinting της συσκευής στόχου (όπως και σε προαναφερθέντα σημεία η επίθεση και εδώ μπορεί να λάβει χώρα συνδυαστικά με εκμετάλλευση τόσο του λογισμικού όσο και του υλικού[157]). Ενδεικτικά, σε μια διαφορετική περίπτωση, οι Kurtz et al. σε πειραματική συνθήκη χρησιμοποίησαν έναν συνδυασμό ομάδων δεδομένων και μηχανικής μάθησης υπό επίβλεψη (supervised learning) για να αποτυπώσουν έγκυρους συσχετισμούς (μέσω εφαρμογών λογισμικού για ακρόαση μουσικής κλπ, δημιουργίας και φόρτωσης cookies) σε ότι αφορά στις προσωποποιημένες επιλογές μιας συσκευής και κατ' επέκταση να επιτύχουν στο fingerprinting του χρήστη και της συσκευής αυτού[158].

- Επίθεση με αξιοποίηση του αισθητήρα αναγνώρισης φωνής (Speech Recognition[159]): Στην υποπερίπτωση αυτή αξίζει όπως σημειωθεί ότι για την εκτέλεση μιας επιθέσεως πλευρικού καναλιού κατά ενός τέτοιου αισθητήρα μπορεί κάλλιστα να αξιοποιηθεί (και) ο περιβάλλοντας χώρος[160]. Οι Michalevsky et al. επί παραδείγματι κατέγραψαν ακουστικές εκροές στον περίγυρο του τηλεφώνου κάνοντας χρήση του γυροσκοπικού αισθητήρα. Εδώ υπάρχουν δύο σημαντικά σημεία, αφενός αξιοποιούνται εκροές που δεν προέρχονται από την συσκευή καθαυτή (αυτό επισημάνθηκε και στο προηγούμενο κεφάλαιο), και αφετέρου η χρήση ενός αισθητήρα ίσως καθιστά εφικτή την υπερκέραση των περιορισμών που μπορεί να υφίστανται για τον αισθητήρα που εκπέμπει την επιθυμητή εκροή

---

[156] Ο.π.

[157] Για περισσότερες λεπτομέρειες που ο εδώ χώρος δεν επιτρέπει την παράθεση τους, βλ. τους Bojinov et al., Dey et al. Και Kurtz et al. μεταξύ άλλων, ο.π.

[158] Για την ανασκόπηση της πειραματικής συνθήκης που αναφέρθηκε ορά, Kurtz, A., & Gascon, H., & Becker, T., & Rieck, K., & Freiling, F.(2016). *Fingerprinting Mobile Devices Using Personalized Configurations.* Paper presented at the 2016 Proceedings on Privacy Enhancing Technologies. Darmstadt, Germany. July, 19-22, 1-17,σ.12 κε. doi: 10.1515/popets-2015-0027. (PDF) Fingerprinting Mobile Devices Using Personalized Configurations (researchgate.net) (τελευταία πρόσβαση 4/1/2022).

[159] Ο.π.,σ.14.

[160] Ο.π.

(υπενθυμίζεται ότι η πρόσβαση στο μικρόφωνο προϋποθέτει την άδεια από πλευράς του χρήστη[161]).

Επιθέσεις πλευρικού καναλιού κατά υποδείγματος (Template Attacks):

Πρόκειται για υποκατηγορία στην οποία εντάσσονται οι περιπτώσεις των SCAs για τις οποίες ο επιτιθέμενος έχει πρόσβαση σε μια αντίστοιχη πειραματική συσκευή με παρόμοια χαρακτηριστικά με εκείνη στην οποία επιθυμεί να επιτεθεί[162]. Οι επιθέσεις αυτές έχουν εκτελεστεί (και) υπό πειραματική συνθήκη υπό τους δύο εξής (και αντίστροφους μεταξύ τους) τρόπους, ήτοι :

- Εκτέλεση από την αρχική φάση (initial stage): Οι Chari et al. πρότειναν τρία βήματα για την εκτέλεση της επίθεσης, ο επιτιθέμενος αρχικά δημιουργεί ένα δικό του template το οποίο να ομοιάζει με εκείνο του στόχου του, στην συνέχεια λαμβάνει ορισμένες μετρήσεις από το template του στόχου και κατόπιν τις συγκρίνει με εκείνες από το δικό του template για να είναι σε θέση να δει αν τα δύο αυτά templates ταιριάζουν (template matching), σε κάθε περίπτωση μια τέτοια επίθεση προετοιμάζει το template πριν ληφθούν τα οποιαδήποτε δείγματα από την συσκευή ή το λογισμικό στόχο[163].
- Αντίστροφη εκτέλεση (*backward*[164]): Οι Aldaya et al. Πρότειναν ουσιαστικά την αντιστροφή της προηγούμενης επίθεσης, ήτοι η επίθεση να βασίζεται λήψη μετρήσεων στην πρώτη φάση, ώστε στην συνέχεια να γίνει σύγκριση με τις αντίστοιχες του template, η συγκεκριμένη πρόταση επιπλέον αποδεικνύει πως η χρήση τεχνικών τυχαιοποίησης ενός αλγόριθμου σε ότι αφορά στην αρχική του φάση

[161] Ο.π.

[162] Ο.π., σ.286.

[163] Aldaya, A.C., & Brumley, B.B.(2021). Online Template Attacks:Revisited. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(3),*28-59(1-32),σ.1-2. doi: https://doi.org/10.46586/tches.v2021.i3.28-59.https://tches.iacr.org/index.php/TCHES/article/view/8967 (τελευταία πρόσβαση 4/1/2022).

[164] Ο.π.,σ.24.

δεν αποτρέπει απαραίτητα της εκροές και κατ' επέκταση δεν αποτελεί πανάκεια για ορισμένες SCAs[165].

Επιθέσεις πλευρικού καναλιού κατόπιν χρονομέτρησης (Timing Attacks):

Πρόκειται για εκδήλωση επιθέσεως αφότου ο επιτιθέμενος έχει διεξάγει (κατά το δυνατόν) ακριβείς μετρήσεις κατά τον χρόνο εκτέλεσης ενός αλγορίθμου κρυπτογράφησης, εύλογα το ζητούμενο είναι ο επιτιθέμενος να διακρίνει και να εκμεταλλευθεί την χρονική διαφορά που υφίσταται ανάμεσα στις εκάστοτε εκτελέσιμες διεργασίες[166] (π.χ. ποια η χρονομετρική διαφορά ανάμεσα στην παραγωγή ενός 0 και ενός 1 ώστε μέσω αυτής της διάκρισης ο επιτιθέμενος να μπορεί να μαντέψει το εκάστοτε bit κάθε φορά). Πρόκειται για υποκατηγορία SCA που χρονολογείται από το 1973 και που υπό το πρίσμα αυτό τοποθετείται δίπλα στις ηλεκτρομαγνητικές (electromagnetic) και τις επιθέσεις ανάλυσης ισχύος (power analysis) σε ότι αφορά την διαχρονικότητα της[167].

Οι Montasari et al. ασχολούνται στην έρευνα τους με δύο είδη της συγκεκριμένης υποκατηγορίας, αφενός τις επιθέσεις που λαμβάνουν χώρα εντός δικτύου (''*TBSCA in a network''*[168]), και εκείνες που λαμβάνουν χώρα εντός ενός και μόνο υπολογιστικού συστήματος (''*TBSCA in a PC platform''*[169]). Οι TBSCAs ομοιάζουν ως προς την εκροή που εκμεταλλεύονται με τις cache-based SCAs, με μια βασική διαφορά ότι οι πρώτες εκτελούνται και εν τη απουσία cache channels, δηλαδή εδώ ο λόγος γίνεται για τις χρονομετρήσεις γενικά, που δεν αφορούν επομένως αποκλειστικά την προσωρινή μνήμη (cache-memory[170]).

Με την σειρά του αυτό σημαίνει πως μέσα από την εκτέλεση μιας TBSCA ο επιτιθέμενος μπορεί (όπως καταγράψαμε και σε μια άλλη περίπτωση που αφορούσε τις template επιθέσεις) να επιτεθεί με την αντίστροφη φορά απ' εκείνη των cache-based SCAs.

---

[165] Ο.π.,σ.5,24.

[166] Ο.π.,σ.285.

[167] Ο όρος ανήκει στον Lampson, βλ. ενδεικτικά Montasari, R., & Hosseinian-Far, A., & Hill, R., & Montaseri, F., & Sharma, M., & Shabbir, Sh.(2018). Are Timing-Based Side-Channel Attacks Feasible in Shared, Modern Computing Hardware ?. *International Journal of Organizational and CollectiveIntelligence,8,2,*32-59,σ.36.doi:10.4018/IJOCI.2018040103. https://pure.hud.ac.uk/ws/portalfiles/portal/13423218/Are_Timing_Based_Side_Channel_Attacks_Feasible_in_Shared_Modern_Computing_Hardware_.pdf (τελευταία πρόσβαση 24/12/2021).

[168] Ο.π.

[169] Ο.π.

[170] Ο.π.,σ.37.

Ήτοι, ο επιτιθέμενος (αν επιπρόσθετα η λειτουργία του συστήματος στόχου του είναι καθόλα γνωστή[171]) μπορεί μέσω των μετρήσεων (αν αυτές είναι ακριβείς) να ξεκινήσει από τις εξόδους (outputs) για να βρει τις εισόδους (inputs[172]), ενώ στις cache-based SCAs συμβαίνει το αντίστροφο (πρέπει να δοκιμάσει δικές του εισόδους ο επιτιθέμενος για να βρει εκείνες του στόχου, όπως στην παραλλαγή flush+reload κλπ).

Στην παραπάνω ταξινόμηση διατυπώθηκε ένας τρόπος συστηματικής καταγραφής στην βιβλιογραφική ανασκόπηση (που έκαναν οι Tsalis et al.) που αξιοποιήθηκε με βάσει δύο (κυρίως, διότι θα μπορούσαν να υπάρχουν και άλλες μεταβλητές που όμως δεν είναι οι κυριότερες στο συγκεκριμένο εγχείρημα ταξινόμησης, υπάρχει δηλαδή μια διαφορά, κατά περίπτωση, στην αλυσίδα αιτιότητας αν μπορούμε να το θέσουμε έτσι) κυρίως στοιχεία (πλαισιωμένο βέβαια από τις προαναφερθείσες μεταβλητές, όπως η προσαρμοστικότητα, η δυνατότητα διείσδυσης κλπ), ήτοι εκείνο του τύπου/-ων (ή υποκατηγορίας) στο/-ους οποίο/-ους δύναται/-νται να διακριθούν οι εκάστοτε επιθέσεις πλευρικού καναλιού με βάσει τον τύπο της διαρροής (leakage), και εκείνο της συσκευής (π.χ. αισθητήρας) ή του λογισμικού (π.χ. μνήμη) από το οποίο προέρχεται η διαρροή.

Όπως όμως έχει λεχθεί και προηγουμένως (αλλά και σε κατά τόπους υποσημειώσεις του προηγούμενου κεφαλαίου, και εδώ θα αναφερθούν συγκεντρωτικά για τον σχηματισμό μιας κατά το δυνατόν πληρέστερης εικόνας) μπορούν να υπάρξουν διαφορετικές ταξινομήσεις επί τι βάση έτερων στοιχείων (κατά μονάς ή συνδυαστικά) που εύλογα οδηγούν και σε διαφορετικές διαρθρώσεις των εγχειρημάτων ταξινόμησης, κατωτέρω παρουσιάζονται συνοπτικά ορισμένα τέτοια παραδείγματα για την πληρότητα (κατά το δυνατόν) του κεφαλαίου αυτού, χωρίς όμως ο χώρος να επαρκεί για μια εξαντλητική παράθεση, καθότι υπενθυμίζεται πως ο κύριος στόχος είναι η ανάδειξη των δυσχερειών περί την ταξινόμηση σε ότι αφορά (και) τις κρίσιμες υποδομές, και ουχί η ταξινόμηση καθαυτή απομονωμένη από οποιαδήποτε επιστημονική στόχευση. Τούτου δοθέντος, έτερα σχήματα ταξινόμησης δυνητικά περιλαμβάνουν:

- <u>Ταξινομήσεις που αφορούν σε συνδυαστικές επιθέσεις πλευρικού καναλιού (combined side-channel attacks[173]):</u>

[171] Όπως αναφέρεται εν παρόδω μεταξύ άλλων και στους Ge et al., Murray et al. Schafer et al. στην βιβλιογραφική ανασκόπηση των Montasari et al. ο.π.

[172] Βλ. περιπτώσεις των Vetiillard & Ferrari, το άρθρο του Cocher, που αναφέρονται εν παρόδω στην βιβλιογραφική ανασκόπηση των Montasari et al. ο.π.

[173] Αξίζει στο σημείο αυτό να τονιστεί εκ νέου (όπως και στο προηγούμενο κεφάλαιο) η , εν μέρει, απουσία συμφωνίας στην χρήση συγκεκριμένων ορισμών, και αντ΄ αυτού ορισμένες φορές χρησιμοποιούνται διαφορετικοί

Αναφορικά με τις συνδυαστικές επιθέσεις αξίζει να σημειωθούν οι εξής δύο παρατηρήσεις. Κατά πρώτον, η τεχνολογική πρόοδος φαίνεται να επιτρέπει ,όχι μόνο την εμφάνιση νέων επιθέσεων, αλλά ταυτοχρόνως φαίνεται και να διευκολύνει τον συγκερασμό των ήδη υπαρχουσών επιθέσεων σε νέες SCAs(δηλαδή οι νέες επιθέσεις να προκύπτουν ως συνδυασμοί προϋφιστάμενων επιθέσεων πλευρικού καναλιού). Επί παραδείγματι, στις συσκευές με αισθητήρες (π.χ. smart phones κλπ), είναι πιθανός ο συνδυασμός μιας απομακρυσμένης (software based) επίθεσης που θα αξιοποιεί τους αισθητήρες (physical properties) ώστε μέσα από την χρήση ενός νευρωνικού δικτύου να είναι εφικτό να εντοπιστούν οι είσοδοι στον αισθητήρα της οθόνης αφής(swipe input[174]).

ορισμοί που νοούνται ως συνώνυμοι αλλά ενδεχομένως να κρύβουν κάποιες διαφοροποιήσεις που δεν αναδεικνύονται ενδεχομένως ορισμένες φορές. Επί παραδείγματι, οι Knechtel et al. στο ακόλουθο άρθρο τους για τις SCAs & τα 3D ICs, χρησιμοποιούν τον όρο «*proxy*» για να περιγράψουν τον συνδυασμό των thermal SCAs & power analysis SCAs. Τουλάχιστον για τον συγγραφέα του ανά χείρας πονήματος, δεν είναι ξεκάθαρο αν ο εν λόγω όρος «*proxy*» μπορεί να χρησιμοποιηθεί αλλαχού με τον όρο «συνδυαστικός» ή αν θα μπορούσε να γίνει λόγος για κάποια διαφορά σε ότι αφορά στην μεθοδολογία εκτέλεσης της επίθεσης. Ήτοι, αν οι δύο επιθέσεις νοούνται ως αυτοτελής στον συνδυασμό τους, ή αν μεθοδολογικά πρόκειται για μια προσέγγιση που κάνει ώστε οι thermal SCAs να είναι απλώς το μέσο για τις power SCAs, και άρα οι πρώτες να μην διατηρούν την αυτοτέλεια τους και να είναι απλό όχημα για την εκτέλεση των δεύτερων, ή αν πρόκειται , γενικά μιλώντας, για μετατροπή της μιας εκροής σε άλλη ή αν διατηρούνται ως ξεχωριστές εκροές. Πάντως, στην ως άνω κατηγοριοποίηση διατηρούμε την αντίληψη πως οι εκροές και οι επιθέσεις διατηρούν την αυτοτέλεια τους ακόμα και αν συνδυάζονται, το ζήτημα είναι ενδεχομένως και μεθοδολογικό και ζήτημα ενδελεχούς εννοιολογικής αποσαφήνισης και χρήζει περαιτέρω διερεύνησης που εδώ δεν επαρκεί ο χώρος για να γίνει. Ορά ενδεικτικά, Knechtel, J., & Sinanoglu, O.(2017). *On mitigation of side-channel attacks in 3D ICs: Decorrelating thermal patterns from power and activity.* Paper presented at the 2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC), 2017. Austin, TX, USA, June, 18-22,1-6,σ.1.doi:10.1145/3061639.3062293 .https://dl.acm.org/doi/pdf/10.1145/3061639.3062293?casa_token=nY_J0HkLqiUAAAAA:QX3FpVcsY0AWRdq_xbssryCEIRlfZdyT6gV6CmS5ofawQbRgQ0C-fTvrxX0K1UOZ5EFgLjp8__Co2A (τελευταία πρόσβαση 22/11/2021).

[174] Βλ. Simon et al. στο Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20,1, 465-488 (1-24),σ.16. doi:10.1109/COMST.2017.2779824.https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021). Παρόμοια διάκριση διατυπώνουν και οι Alahmadi et al., διαχωρίζοντας τις SCAs σε φυσικές (physical) και λειτουργικές (functional). Οι μεν πρώτες αφορούν "*στην μετρήσιμη ποσότητα που είναι το υπό-προϊόν της εφαρμογής* (ενν. κάποιας συσκευής π.χ. IoT κλπ)" (η μετάφραση είναι του συγγραφέως όπως και κατωτέρω), δηλαδή κάνουν αναφορά στα physical properties της οικείας παραγράφου, και σε αυτές οι συγγραφείς περιλαμβάνουν τύπους επιθέσεων όπως οι ακουστικές, οι επιθέσεις ανάλυσης ισχύος, οι θερμικές, οι οπτικές κλπ.

Κατά δεύτερον, πρέπει ακόμα να παρατηρηθεί πως οι SCAs όσο ευέλικτες και αν είναι, και όσους συνδυασμούς και αν παρουσιάζουν (με τα μέχρι τώρα δεδομένα), παρουσιάζουν και αυτές περιορισμούς. Αφενός, δεν εμφανίζονται όλες οι επιθέσεις ή οι συνδυασμοί τους με την ίδια συχνότητα, και αφετέρου δεν είναι το ίδιο εφικτή όλοι οι πιθανοί συνδυασμοί τουλάχιστον προς ώρας. Για παράδειγμα, οι Spreitzer et al. παρατηρούν πως δεν είναι προς ώρας εφικτή μια συνδυαστική επίθεση λογισμικού και fault injection έναντι κάποιας συσκευής (ήτοι η fault injection SCA μπορεί να εκτελεστεί κυρίως με φυσική πρόσβαση του επιτιθέμενου σε μια συσκευή, π.χ. decapsulation κλπ[175]). Περαιτέρω, για λόγους περιορισμού του χώρου (και επειδή , έστω και εμμέσως όπως έχουμε δείξει και στις οπτικές επιθέσεις μεταξύ άλλων, έχει ήδη γίνει μια μικρή αναφορά σε συνδυαστικές επιθέσεις) θα αναφερθούν ορισμένα παραδείγματα συνδυαστικής επίθεσης εδώ, το οποίο θα συνδυάζει για τους σκοπούς τις επιθέσεως δύο εκροές(ενώ υπενθυμίζεται πως οι συνδυασμοί μπορεί να αφορούν και SCAs με έτερες επιθέσεις, π.χ. insider threats, αλλά η ανάλυση τους δεν εμπίπτει στους στόχους του κεφαλαίου αυτού):

- Συνδυασμός ήχου + τάση του ρεύματος (sound+voltage): οι συσκευές κατά την εκτέλεση διεργασιών προχωρούν σε κάποια αυξομείωση της τάσης του ρεύματος, η οποία με την σειρά της συσχετίζεται με την παραγωγή θορύβου (sound) που λογικά αυξομειώνεται σε σχέση με την αντίστοιχη τάση του ρεύματος που αξιοποιείται[176].

Οι δε δεύτερες "*βασίζονται στην εσωτερική λειτουργική εφαρμογή και στην λειτουργία του συστήματος υπολογισμού* (ενν. *computing*) *που μπορεί να οδηγήσει σε διαρροή δεδομένων*", σε αυτή την υποκατηγορία εμπίπτουν επιθέσεις όπως architectural attacks, template attacks, και γενικά όποια παραλλαγή απαιτεί στόχευση σχεδόν αποκλειστικά λογισμικού και λήψη μετρήσεων από την CPU/GPU κλπ. Ορά ενδεικτικά,Alahmadi, A.D., & Rehman, S.U., & Alhazmi, H.S., & Glynn, D.G., & Shoaib, H., & Sole, P.(2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. Sensors 2022, 22, 3520, 1-14, σ.6. DOI: Sensors | Free Full-Text | Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture (mdpi.com) . Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture - PMC (nih.gov) (Τελευταία πρόσβαση 29/9/2022).

[175] Ο.π.

[176] Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton,St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and*

- Συνδυασμός ακουστικού σήματος + κατανάλωση ρεύματος(acoustic signal(s) + power consumption): οι Zhou et al. πρότειναν ένα σχήμα επιθέσεως πλευρικού καναλιού, όπου ο επιτιθέμενος παρατηρεί (μέσω των procfs) την κατανάλωση του ρεύματος της συσκευής για να εντοπίσει αν το μικρόφωνο της συσκευής είναι ενεργό (π.χ. για λήψη οδηγιών από εφαρμογή GPS), και έτσι μέσα από την κατανάλωση ρεύματος που απαιτεί η λειτουργία του μικροφώνου να καταστεί εφικτό να μετρηθεί το μήκος της πρότασης που το μικρόφωνο αναπαράγει (π.χ. για να κατευθύνει τον οδηγό του οχήματος). Μέσα από τον προσδιορισμό του μήκους της πρότασης, ενδεχόμενα, είναι εφικτό να εντοπιστεί η διαδρομή που ο οδηγός ακολουθεί (driving fingerprinting), δεδομένου και του ότι οι προτάσεις που η εφαρμογή σχηματίζει είναι στερεοτυπικές και θα έχουν ορισμένο μέγεθος για κάθε ξεχωριστή εντολή κατεύθυνσης[177].
- Συνδυασμός οπτικής διαρροής + θερμότητας (finger touch+ heat traces): οι Zhang et al. διερεύνησαν την δυνατότητα λήψης πληροφοριών μέσα από την συσχέτιση της θερμότητας που αφήνει το δακτυλικό αποτύπωμα πάνω σε μια οθόνη αφής με την δυνατότητα των θερμικών καμερών να εντοπίζουν και να απεικονίζουν τις θερμικές εκροές (άρα εδώ πρόκειται και για οπτική απεικόνιση/εκροή, αφού πρέπει να αξιοποιηθούν τεχνολογίες απεικόνισης όπως μια κάμερα[178]).
- Συνδυασμός λειτουργίας μνήμης + θερμότητας (memory + temperature variation): οι Muller & Spreitzenbarth με την χρήση του εργαλείου FROST (forensics) επιχειρούν την απόσπαση του μυστικού κλειδιού από την μνήμη RAM μιας συσκευής Android (γνωστή ως cold-boot attack), βασιζόμενοι στην συσχέτιση ανάμεσα στην διατήρηση δεδομένων σε μια μνήμη RAM και στην μείωση της θερμοκρασίας που

*Systems Security, Springer,2021,10.1007/s41635-021-00112-6.hal-03176249,*1-24,σ.4. https://hal.archives-ouvertes.fr/hal-03176249/document (τελευταία πρόσβαση 15/10/2021).

[177] Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, 1,465-488 (1-24),σ.14.doi: 10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[178] Ο.π.,σ.9.

επέρχεται μετά την απενεργοποίηση μιας συσκευής. Η συσχέτιση αυτή προκύπτει από το ότι τα δεδομένα μπορούν να διατηρηθούν σε μια RAM για ένα ορισμένο διάστημα μετά την απενεργοποίηση της συσκευής ακριβώς λόγω της χαμηλής θερμοκρασίας που προκύπτει εξαιτίας της απενεργοποίησης αυτής (και που επομένως επιτρέπει στον επιτιθέμενο να ανακτήσει, βλ. boot up, τα δεδομένα της πρότερης κατάστασης πριν την απενεργοποίηση[179]).

❖ Ταξινόμηση με βάσει τον attack vector (υλικό ή λογισμικό που γίνεται αποδέκτης ή που μεσολαβεί για την εκτέλεση της επίθεσης, σημειωτέων ο attack vector έχει εν μέρει αξιοποιηθεί όταν για παράδειγμα έγινε λόγος για τους αισθητήρες ανωτέρω):

➢ cross-VM Attacks: πρόκειται για τις ίδιες παραλλαγές με τις άνωθεν τρεις (εκεί όπου ο λόγος γίνεται για cache-based SCAs), μόνο που σε αυτή την υποπερίπτωση εξετάζονται υπό το πρίσμα του multitenancy (ο επιτιθέμενος και ο στόχος βρίσκονται στο ίδιο περιβάλλον εντός μιας εικονικής μηχανής[180]). Η συνύπαρξη αυτή μπορεί να αφορά είτε σε ένα εικονικό περιβάλλον ενός υπολογιστή, είτε σε ένα περιβάλλον Cloud. Περαιτέρω, υφίσταται ακόμα το σενάριο κατά το οποίο ο επιτιθέμενος επιχειρεί να περάσει από την μια εικονική μηχανή στην άλλη (cross-VM attacks).

Επί παραδείγματι, οι Chen et al. προτείνουν μια επίθεση που θα προβαίνει σε παρατήρηση της συσχέτισης κατανάλωσης ρεύματος και εκτέλεσης λειτουργιών ανάμεσα στο υλικό του πυρήνα (core) και εκείνο του uncore σε ένα περιβάλλον με πολλές εικονικές μηχανές όπως το Cloud[181]. Η λογική πίσω από την επίθεση βασίζεται στην

[179] Ο.π.,σ.10.

[180]Montasari, R., & Hosseinian-Far, A., & Hill, R., & Montaseri, F., & Sharma, M., & Shabbir, Sh.(2018). Are Timing-Based Side-Channel Attacks Feasible in Shared, Modern Computing Hardware ?. *International Journal of Organizational and Collective Intelligence,8,2,*32-59,σ.41.doi: 10.4018/IJOCI.2018040103.https://pure.hud.ac.uk/ws/portalfiles/portal/13423218/Are_Timing_Based_Side_Channel_Attacks_Feasible_in_Shared_Modern_Computing_Hardware_.pdf (τελευταία πρόσβαση 24/12/2021).

[181]Ειρήσθω εν παρόδω, το επιθετικό σχήμα που προτείνεται εδώ αφορά σε συσχετίσεις που προκύπτουν από ένα συγκεκαλυμμένο κανάλι εκροής (covert channel), όπως φαίνεται και από τον τίτλο του άρθρου, κάτι που έχει συζητηθεί στην περίπτωση των ορισμών (εκεί όπου γίνεται λόγος για covert & overt κανάλια, και κατ' επέκταση

παρατήρηση πως η κατανάλωση ρεύματος από την πλευρά του uncore τελεί σε εξάρτηση από τις λειτουργίες που εκτελούν οι πυρήνες, εν άλλοις λόγοις ο φόρτος εργασίας των πυρήνων καθορίζει το αν θα ενεργοποιείται ο uncore ή όχι (προφανώς σε διαστήματα αδράνειας ο uncore απενεργοποιείται[182]).

Από την συσχέτιση αυτών των δύο προκύπτει πως ένας επιτιθέμενος με πρόσβαση (cross-VM) έστω και σε έναν πυρήνα μπορεί να μελετήσει την τροφοδοσία του uncore για να αντλήσει πληροφορίες για τον φόρτο εργασίας (workload pattern) και τις λειτουργίες που εκτελούνται από τους πυρήνες εντός του διαμοιρασμένου συστήματος (shared machine, cloud κλπ) καθώς υπάρχει αλληλεξάρτηση ανάμεσα στα δύο τμήματα του υλικού (interdependency[183]).

- Επιθέσεις πλευρικού καναλιού κατά ενσωματωμένων συστημάτων (embedded devices): οι Clark et al. αναφέρουν στο άρθρο τους την , συνήθη για το παράδειγμα των SCAs, περίπτωση των ενσωματωμένων συστημάτων στον τομέα της Υγείας, που όμοια με τα αντίστοιχα ενσωματωμένα συστήματα σε άλλους τομείς εμφανίζουν δυσκολίες σε ότι αφορά στην εγκατάσταση λογισμικού προστασίας και στον εν γένει έλεγχο τους σε ότι αφορά παραβιάσεις[184] (forensics). Στο εν λόγω άρθρο η επίθεση λειτουργεί

για το τι σημαίνει κανάλι) στο προηγούμενο κεφάλαιο και που καταδεικνύεται και εδώ, καθώς οι συγγραφείς επιλέγουν να προσδιορίσουν την φύση του καναλιού εδώ. Βλ. ενδεικτικά, Chen, P., & Li, L., & Yang, Zh.(2021). *Cross-VM and Cross-Processor Covert Channels Exploiting Processor Idle Power Management.* Paper presented at the USENIX Security '21 30th USENIX Security Symposium. Vancouver, BC, Canada, August, 11-13, 733-750(1-19),σ.1. https://www.usenix.org/conference/usenixsecurity21/presentation/chen-paizhuo (τελευταία πρόσβαση 21/1/2022).

[182] Ο.π.

[183] Ο.π.

[184] Clark, S.S., & Ransford, B., & Rahmati, A., & Guineau, S., & Sorber, J., & Fu, K., & Xu, W.(2013). *WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices.* Paper presented at the 2013 USENIX Workshop on Health Information Technologies (HealthTech '13), Washington DC, USA, August 12, 1-11, σ.10. https://www.usenix.org/conference/healthtech13/workshop-program/presentation/clark (τελευταία πρόσβαση 15/10/2021).

συνδυαστικά με την εγκατάσταση ενός κακόβουλου λογισμικού σε ένα σύστημα SCADA. (Supervisory Control and Data Acquisition device[185]).

Στο εν λόγω άρθρο παρουσιάζει ενδεχομένως (και σε σχέση με το προηγούμενο κεφάλαιο) ενδιαφέρον η διάκριση που κάνουν οι συγγραφείς ανάμεσα σε μη ηθελημένα πλευρικά κανάλια (εδώ undesirable, ενώ σε άλλα άρθρα χρησιμοποιείται περισσότερο ο όρος unintended για να προσδιορίσουν την πληροφορία) και σε constructive πληροφορίες[186].

Με βάση αυτή την διάκριση αναδεικνύεται και μια διαφορά ανάμεσα σε εφαρμοσμένα και μη συστήματα, καθώς στα πρώτα αποκρύπτεται σχεδόν το σύνολο του OS(σε αντίθεση π.χ. με τις κινητές συσκευές και την προσβασιμότητα στο procfs) καθώς οι ιατρικές συσκευές εκτελούν ρητά ορισμένες λειτουργίες, αλλά ο όρος constructive information κάνει αναφορά στην δυνατότητα ύπαρξης κάποιας διαρροής (π.χ. κατανάλωση ρεύματος) που να επιτρέπει στον επιτιθέμενο να αντλήσει πληροφορίες για το σύνολο του λειτουργούντος συστήματος («*systemwide power consumption that scales closely with their workloads*[187]»).

- Επιθέσεις πλευρικού καναλιού κατά κινητών (mobile) & IoT (διαδίκτυο των πραγμάτων) συσκευών : οι εν λόγω vectors , εν μέρει, θέτουν το αντίστροφο ζήτημα σε σχέση με τις περισσότερες άλλες ταξινομήσεις αυτού του κεφαλαίου, καθώς αυτές οι συσκευές (mobile, IoT, wearables) προσφέρουν αρκετές ευκαιρίες για συνδυαστικές επιθέσεις (π.χ. cross-platform attacks), ώστε μια ταξινόμηση που θα τις διερευνά ξεχωριστά να μην δίνει μια πλήρη εικόνα[188]. Διευκρινίζεται, ότι η άνωθεν ταξινόμηση συνδυαστικών

[185] Ο.π,σ.3.

[186] Ο.π.

[187] Ο.π.

[188] Ορά ενδεικτικά, Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials, vol. XX,No. Z,Month YYYY,*1-24(465-488),σ.19.doi:10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

SCAs αφορούσε συνδυασμό εκροών, εδώ σε αυτή την υποκατηγορία οι συνδυαστικές επιθέσεις διερευνώνται υπό το πρίσμα του συνδυασμού πρωτίστως των attack vectors και ενδεχομένως δευτερευόντως των συνδυαστικών εκροών από τους αισθητήρες ή κάποιο software[189].

Οι κινητές συσκευές ευνοούν τις συνδυαστικές επιθέσεις λόγω των πολλών αισθητήρων με τους οποίους είναι εξοπλισμένες. Και εδώ όπως και πριν, υπάρχουν δίπλα στους vectors εγγύτητα (φυσική παρουσία ή απόσταση) του επιτιθέμενου και οι επιλογές μεταξύ υλικού και λογισμικού για την εκτέλεση ορισμένων επιθέσεων μεταξύ άλλων. Αν απομονώσουμε τους συνδυασμούς των vectors τότε υπάρχουν ,μεταξύ άλλων, δύο ενδιαφέροντες συνδυασμοί.

- Αφενός, ο συνδυασμός Android συσκευής και ενός (ή κάποιων) wearable(s) ο οποίος διευρύνει το πεδίο της επίθεσης και επιπλέον καταδεικνύει πως μια μοναδική εκροή, συγκεκριμένα ο ήχος που δεν αντιλαμβάνεται το ανθρώπινο αυτί (inaudible sounds) και που συνδέουν τις συσκευές (μέσω γυροσκόπιού), μπορεί να αξιοποιηθεί για επίθεση προς πολλές συσκευές (στα περισσότερα παραδείγματα που παραθέτουμε η αναλογία είναι μια εκροή προς μια συσκευή κλπ[190]).
- Αφετέρου, το παράδειγμα της cross-platform επίθεσης που καθίσταται εφικτό διότι πολλές εφαρμογές για android συσκευές έχουν προδιαγραφές για λειτουργία σε πολλές πλατφόρμες, έτσι ο attack vector πολλαπλασιάζεται μέσα από τον συνδυασμό αισθητήρων και software (ομοίως και σε ότι αφορά τις IoT συσκευές επομένως)[191].

❖ <u>Ταξινόμηση επί τη βάσει της διακρίσεως ανάμεσα σε επιθετικές (offensive) και παθητικές (passive) SCAs</u>: οι Spreitzer et al. προχωρούν σε αυτή την διάκριση στην περίπτωση του δικού τους άρθρου, το οποίο προχωρά σε αυτή την

[189] Ο.π.,σ.2.

[190] Πρβλ. Farshteindiker et al. για την σύνδεση των hardware implants στο Spreitzer et al. ο.π.,σ.19.

[191] Ο.π.

διάκριση με βάση την εγγύτητα ή την απόσταση που διατηρεί ο επιτιθέμενος εν σχέση με την συσκευή[192]. Περαιτέρω, οι συγγραφείς υιοθετούν ένα σχήμα ταξινόμησης που έχει τέσσερις υποκατηγορίες, δηλαδή οι παθητικές και επιθετικές μορφές παραπέρα διαιρούνται σε επιθέσεις που αξιοποιούν είτε φυσικές (physical) είτε λογικές (logical) ιδιότητες (properties). Εδώ υπάρχουν τέσσερις ομαδοποιήσεις, που η κάθε μια με την σειρά της καταγράφει τις μεμονωμένες επιθέσεις.

Αντίθετα οι Tsalis et al. δεν αξιοποιούν ομαδοποιήσεις κάτω από τον όρο ομπρέλα του SCA και προχωρούν απευθείας στην ξεχωριστή καταγραφή επιθέσεων. Οι Spreitzer et al. φαίνεται να αξιοποιούν ένα διμεταβλητό σχήμα (βαθμός εγγύτητας επιτιθέμενου, χαρακτηριστικά της συσκευής στόχου) για τις ομαδοποιήσεις τους, κάτι που τονίζει το ζήτημα ύπαρξης ενδιάμεσων μεταβλητών που μπορεί, λόγω της πληθώρας των SCAs, να παραληφθεί κατά λάθος από τους συγγραφείς κατά την κατάρτιση μιας ταξινόμησης.

Επί παραδείγματι, η ταξινόμηση που εδώ αναλύεται διακρίνει ενσωματώνει εντός της διάκρισης σε passive & offensive, εμμέσως, και την διάκριση των SCAs σε εκείνες που στοχεύουν στο λογισμικό και σε εκείνες που στοχεύουν στο υλικό, αλλά όπως θα φανεί αυτή η τελευταία νοείται ως υποκατηγορία (physical-logical properties[193]) της πρώτης υποκατηγορίας (passive-offensive[194]), και επομένως εδώ παρουσιάζεται και διαφοροποίηση σε ότι αφορά στον τρόπο δόμησης της ταξινόμησης, αλλά και στην ονοματοδοσία αφού για ίδιες έννοιες μπορεί να χρησιμοποιούνται συνώνυμοι όροι (όχι δηλαδή μόνο στο περιεχόμενο της κάθε υποκατηγορίας). Κατωτέρω παρουσιάζονται οι τέσσερις ομαδοποιήσεις και ορισμένα χαρακτηριστικά τους[195]:

- Στις passive επιθέσεις η εγγύτητα δεν θεωρείται απαραίτητη συνθήκη, κυρίως η έννοια συνδέεται από τους συγγραφείς με την παραβίαση μη ασφαλών αλγορίθμων κρυπτογραφίας. Υπό την κατηγορία των passive επιθέσεων οι συγγραφείς εντάσσουν επιθέσεις που στην προηγούμενη ταξινόμηση που παρουσιάσαμε αποτελούσαν διακριτές

[192] Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20, *1,*465-488 (1-24),σ.8 κε. doi:10.1109/COMST.2017.2779824.https://arxiv.org/pdf/1611.03748.pdf(τελευταία πρόσβαση 16/9/2021).

[193] Ο.π,σ.7.

[194] Ο.π.,σ.8-9.

[195] Ορά σχετικό σχήμα ο.π.,σ.7.

υποκατηγορίες, όπως επιθέσεις ανάλυσης ισχύος (Power Analysis Attacks), ηλεκτρομαγνητικές (electromagnetic Analysis Attacks), καθώς και επιθέσεις με χρήση αισθητήρων (π.χ. Hand/Device Movements[196]).

- Αντίθετα, στις offensive επιθέσεις ο επιτιθέμενος ,θεωρούν οι συγγραφείς, πως πρέπει να βρίσκεται σε επαφή με την συσκευή στην οποία επιδιώκει να επιτεθεί. Σε αυτή την υποκατηγορία εντάσσονται με βάσει τους συγγραφείς οι επιθέσεις σφάλματος (Optical και Laser Fault Injection Attacks), επιθέσεις με βάσει την ανάλυση της θερμοκρασίας (Temperature Variation) κα[197].
- Φυσικές ιδιότητες (Physical properties): πρόκειται ουσιαστικά για τις εκροές που προκύπτουν από το υλικό (hardware), όπως οι ηλεκτρομαγνητικές εκροές ή η κατανάλωση ρεύματος[198].
- Λογικές ιδιότητες (Logical properties): πρόκειται επί τις ουσίας για τα χαρακτηριστικά που αναφέρονται στο λογισμικό (software) μιας συσκευής, εδώ χαρακτηριστικά αναφέρονται εκείνες οι στατιστικές και οι μετρήσεις που αφορούν στην δεδομένα που συγκροτούν την προσωποποιημένη λειτουργία μιας συσκευής (π.χ. data-usage statistics[199]).

❖ <u>Ταξινόμηση με βάσει την διάκριση των SCAs ανάλογα με το αν η διαρροή (leakage,emanation) είναι ηθελημένη ή μη</u>: η συγκεκριμένη προσπάθεια ταξινόμησης προσθέτει το επιπλέον στοιχείο της διαρροής υπό την μορφή πληροφορίας αποτυπωμένης σε μια αναφορά ή σε ένα επίσημο έγγραφο που εκδίδει ένας οργανισμός. Σε αυτή την περίπτωση η διαρροή είναι περισσότερο ταυτόσημη με την πληροφορία, ενώ η αθέλητη διαρροή προέρχεται από ηλεκτρονικές συσκευές και μπορεί να ενέχει διαφορετικά επίπεδα σε ότι αφορά την ανθρώπινη κατανόηση αυτής, και άρα να μην είναι πάντα ταυτόσημη με την άμεσα διαθέσιμη πληροφορία (π.χ. μπορεί να χρειάζεται

[196] Ο.π,σ.8.

[197] Ο.π.,σ.8.

[198] Ο.π.,σ.7.

[199] Ο.π.

κάποιο μοντέλο μηχανικής μάθησης για τον σκοπό αυτό). Παραδείγματα εκροών των δύο τύπων παρατίθενται ακολούθως:

- Μη ηθελημένες εκροές(unintended information leaks[200]): όσες εκροές δεν αποτελούν μέρος του αρχικού σχεδιασμού ενός συστήματος (κατανάλωση ρεύματος, χρόνος εκτέλεσης μιας λειτουργίας κλπ[201]).
- Ηθελημένες εκροές (information published on purpose[202]): πρόκειται είτε για πληροφορίες που υπάρχουν διαθέσιμες εντός του λειτουργικού (π.χ. OS) είτε για εκείνες που οι κατασκευαστές εκδίδουν οικεία βουλήσει (π.χ. πληροφορίες για δεδομένα, αισθητήρες κλπ[203]). Ειδικά αυτή η κατηγορία προσεγγίζει αρκετά την ταξινόμηση με βάσει την εγγύτητα του επιτιθέμενου, διότι ο τελευταίος μπορεί να αξιοποιήσει τις δημοσιευμένες εκροές για να εκτελέσει , μεταξύ άλλων, μια επίθεση πλευρικού καναλιού κατά λογισμικού (όπως στην προηγούμενη ταξινόμηση[204]). Πέρα και από τον συνδυασμό ανάμεσα σε αυτές τις ταξινομήσεις, χρήζει μνείας επίσης το ότι οι ηθελημένες εκροές αυξάνουν σταδιακά απ' αφορμή την παραπέρα εξέλιξη των λειτουργικών των συσκευών Android, καθώς και την αντίστοιχη (προαναφερθείσα) των πλατφορμών και συσκευών (IoT όπως αναφέρθηκε ανωτέρω στην ταξινόμηση των attack vectors[205]).

❖ Ταξινόμηση με βάσει τα χαρακτηριστικά του επιτιθέμενου (attacker): οι Biswas et al. παραθέτουν στο άρθρο τους τρεις πιθανούς τύπους επιτιθέμενου ως ακολούθως[206] :

---

[200] Ο.π.,σ.5.

[201] Ο.π.

[202] Ο.π.

[203] Ο.π.

[204] Ο.π.,σ.6.

[205] Ο.π.

[206] Με αναφορά στις επιθέσεις πλευρικού καναλιού που αξιοποιούν timing channels στην προκειμένη περίπτωση, βλ. Biswas, A.K., & Ghosal, D., & Nagaraja, Sh.(2016). A Survey of Timing Channels and Countermeasures. *ACM Computing Surveys (CSUR),0,0,*1-39,σ.18. doi: 10.1145/3023872. http://personal.strath.ac.uk/shishir.nagaraja/papers/timing-survey.pdf (τελευταία πρόσβαση 24/12/2021).

- Ο απομονωμένος επιτιθέμενος (isolated attacker[207]): σε αυτή την παραλλαγή ο επιτιθέμενος γνωρίζει μόνο την ροή δεδομένων που έχει υδατογραφηθεί για να εντοπίσει χρονικές συσχετίσεις που θα τον βοηθήσουν να αποκρυπτογραφήσει την κρυπτογραφημένη επικοινωνία ενός timing channel[208].
- Η μερικώς εγνωσμένη επίθεση ροής (partially known flow attack[209]): σε αυτή την παραλλαγή ο επιτιθέμενος διαθέτει πρόσβαση τόσο σε μια μη πλήρη αρχική ροή όσο και σε εκείνη που έχει υδατογραφηθεί , και στην συνέχεια προσπαθεί μέσα από την εξαγωγή πληροφοριών για την υδατογραφημένη ροή να εξάγει πληροφορίες για την αρχική ροή συμπληρώνοντας την δεύτερη με την χρήση της πρώτης[210].
- Η πλήρως εγνωσμένη επίθεση ροής (fully known flow attack[211]): εδώ ο επιτιθέμενος έχει πρόσβαση τόσο στην πλήρη αρχική ροή όσο και στην υδατογραφημένη ροή και εν συνεχεία τις συγκρίνει για να εξάγει πληροφορίες[212].

❖ Ταξινόμηση με βάσει τα χαρακτηριστικά στοιχεία (elements) της πληροφορίας (Confidentiality, Integrity, Availability): μια τέτοια ταξινόμηση δεν απαντάται συχνά στην βιβλιογραφία που μελετήθηκε για τις ανάγκες του κεφαλαίου αυτού. Όμως, στον βαθμό που αρκετά παραδείγματα σχετιζόμενα με SCAs αφορούσαν την παραβίαση αλγορίθμων κρυπτογράφησης, μπορούν να γίνουν οι κάτωθι παρατηρήσεις αναφορικά με το κάθε επιμέρους στοιχείο:

- Confidentiality: απαντάται συχνότερα από τα άλλα δύο στοιχεία, στον βαθμό μάλιστα που αρκετές δημοσιεύσεις πρωτίστως εξετάζουν (αν και όχι εξ' ολοκλήρου) τις SCAs υπό το πρίσμα της απόσπασης μυστικών κλειδιών χωρίς να υφίσταται παραβίαση (όπως για παράδειγμα με μια επίθεση rainbow table) καθαυτή του αλγόριθμου ή κάποια ζημιά στο σύστημα στόχο (υπό αυτή την έννοια μια τέτοια ταξινόμηση με βάσει τα στοιχεία της πληροφορίας λαμβάνει χώρα στην πιο πάνω ταξινόμηση των Spreitzer et al. που διακρίνει τις SCAs σε passive & offensive SCAs).

[207] Ο.π.

[208] Ο.π.

[209] Ο.π.

[210] Ο.π.

[211] Ο.π.,σ.19.

[212] Ο.π.

Χαρακτηριστικά παραδείγματα που απαντούν στην βιβλιογραφία, και που αναφέρθηκαν ανωτέρω, αποτελούν οι ηλεκτρομαγνητικές επιθέσεις (electromagnetic attacks) και εκείνες με χρήση χρονομέτρησης(timing attacks). Η βασική ιδέα παραμένει η εξαγωγή πληροφοριών σχετικά με τις δραστηριότητες ρουτίνας των συσκευών που επιτρέπουν την εξαγωγή μυστικών (workload pattern[213]).

- Integrity & Availability: οι SCAs έχουν εδώ μια πιο επιθετική μορφή, αν και η βιβλιογραφία που μελετήθηκε επικεντρώνει περισσότερο στο confidentiality. Χαρακτηριστικό παράδειγμα αποτελεί η αντιστροφή των δυαδικών ψηφίων (bit flipping) σε τμήματα μνήμης (DRAM) που δεν προαπαιτούν πρόσβαση βάσει προνομίων (unprivileged memory access[214]).

Μια τέτοια περίπτωση αποτελεί η επίθεση RAMBleed, όπου μέσω hammering των δυαδικών ψηφίων στις σειρές της μνήμης μιας συσκευής, αλλάζουν τόσο τα bits που ο επιτιθέμενος στοχεύει, όσο και τα bits που βρίσκονται πλησίον αυτών (π.χ. τα true bits τείνουν να αλλάζουν σε 1 όταν τα bits άνωθεν και κάτωθεν τους είναι 0 κλπ), διευκολύνοντας τον επιτιθέμενο στην ανεύρεση του μυστικού κλειδιού ακόμα και όταν ως αντίμετρο χρησιμοποιείται κώδικας διόρθωσης σφαλμάτων (error-correcting code[215]).

Μια ακόμα περίπτωση επισημάνθηκε ανωτέρω στην αναφορά στην υποκατηγορία της ηλεκτροακουστικής επίθεσης πλευρικού καναλιού. Όσον αφορά το availability, ίσως δυνητικά να μπορεί να

---

[213] Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.295-297. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (τελευταία πρόσβαση 16/9/2021).

[214] Goodin, D.(2019). Researchers use Rowhammer bit flips to steal 2048-bit crypto key. *Arstechnica.* https://arstechnica.com/information-technology/2019/06/researchers-use-rowhammer-bitflips-to-steal-2048-bit-crypto-key/ (τελευταία πρόσβαση 22/1/2022).

[215] Ο.π.

συνδυαστεί μια SCA με κάποια άλλη επίθεση, όπως μια DDoS(Distributed Denial of Service attack, επίθεση άρνησης παροχής υπηρεσιών[216]).

Συμπερασματικά, και εδώ η αναφορά γίνεται εν σχέση με το δεύτερο σημείο στο οποίο έγινε αναφορά στην αρχή της υπό-ενότητας (2.2) του παρόντος κεφαλαίου, τα εγχειρήματα περί της ταξινομήσεως των SCAs , αυτή την φορά όχι ιδωμένα κατά μονάς, αλλά σε σχέση με την σημασία και χρησιμότητα τους για την προστασία των κρισίμων υποδομών, έχουν (ενν. για τις υποδομές αυτές) τους ακόλουθους στόχους να προς επίτευξη:

- Εν πρώτοις, τα εγχειρήματα ταξινομήσεως αφορούν, μεταξύ άλλων, στην δυνατότητα τους να λειτουργήσουν ευρετικά (heuristically). Η ευρετική λειτουργία μιας ταξινόμησης σε ότι αφορά στην προστασία των κρισίμων υποδομών συνεπάγεται ότι δημιουργείται μια συνεκτική δομή και σύνδεση ανάμεσα σε ένα πλήθος από έννοιες, ορισμούς, τύπους επιθέσεων, εκροών, τύπους επιτιθέμενων, συσκευών στόχων κλπ, που πλέον δεν είναι ασύνδετες. Αλλά αντίθετα, εντάσσονται σε μια δομή που διευκολύνει , κατά το δυνατόν, τον εντοπισμό και ταχύτερη αντιμετώπιση μιας τέτοιας επίθεσης όταν εμφανιστεί και απειλήσει μια κρίσιμη υποδομή (π.χ. χρήση statistics). Επιπροσθέτως, η συνεκτική δομή των ταξινομήσεων επιτρέπει την ευκολότερη ενσωμάτωση νέας γνώσης σχετικά είτε με καινοφανείς SCAs είτε με συνδυαστικές επιθέσεις πλευρικού καναλιού (συγκριτικό πλαίσιο, comparison), και επομένως την ταχύτερη απόκριση στις νέες απειλές[217].
- Εν δευτέροις, οι πολλαπλές ταξινομήσεις καταλήγουν να ενέχουν κάποιες φορές αλληλοεπικαλύψεις (ενώ σε άλλες περιπτώσεις αντίθετα παρατηρούνται διαφοροποιήσεις στις ταξινομήσεις και τις μεθόδους ταξινόμησης, χρήση ορισμών που είναι συνώνυμοι αλλά όχι ταυτόσημοι ίσως, εν γένει μια απουσία ομοιογένειας στην προσέγγιση των ταξινομήσεων, χωρίς αυτό να είναι πάντα αρνητικό, καθώς ευνοεί ορισμένες φορές την πολυμέρεια ως προς τις SCAs εν γένει).

[216] Ενδεχομένως μια τέτοια, μεταξύ άλλων, τάση να αναδυθεί ή να υπάρχει ήδη ως ενδεχόμενο. Ορά ενδεικτικά και, Kleinman, L.(2020). Organizations Must Develop Zero Trust to Defend Against DDoS Attacks. Here's Why. *Securing the Digital World.* https://www.securid.com/en-us/blog/organizations-must-develop-zero-trust-to-defend-against-ddos-attacks/ (τελευταία πρόσβαση 22/1/2022).

[217] Για την σημασία των ταξινομήσεων και των μεθοδολογιών ορά ενδεικτικά και , Tsalis et al. ο.π.,σ.284.

Αυτές οι τελευταίες , πέρα από το να αναδεικνύουν και ορισμένες διαστάσεις συνέργειας ανάμεσα σε SCAs, επίσης καταδεικνύουν ότι το κάθε ξεχωριστό στοιχείο σε κάθε ταξινόμηση μπορεί να περιλαμβάνει εντός του και άλλα στοιχεία, που δεν διευκολύνουν την μελέτη του κάθε στοιχείου σε απομόνωση (καμιά φορά και συνδυαστικά ακόμα).

Αντίθετα, τα στοιχεία αυτά αλληλοδιαπλέκονται και δεν βοηθούν στην καταγραφή όλων των πιθανών περιπτώσεων πάντα. Αυτές οι ενδιάμεσες μεταβλητές, αν μπορούν να αποκληθούν έτσι, πρέπει αν είναι εφικτό να διακριθούν και να λαμβάνονται υπόψη. Αφενός, γιατί οι ορισμοί πρέπει να είναι ξεκάθαροι για να χρησιμεύουν σε μια ταξινόμηση. Και αφετέρου, διότι εξαιτίας του η μεθοδολογία της επίθεσης μπορεί να παραλλάσει, ενώ ο ορισμός να μένει ο ίδιος, και έτσι η ταξινόμηση να μην μπορεί να συνεισφέρει στην ενσωμάτωση νέας γνώσης στις υπάρχουσες δομές ταξινόμησης, και έτσι να μην σχεδιάζονται τα κατάλληλα αντίμετρα[218].

- Εν τρίτοις, οι ταξινομήσεις δύνανται όπως συνδράμουν στον σχεδιασμό και την λήψη αντιμέτρων (τα οποία θα αναλυθούν περαιτέρω σε κατοπινό κεφάλαιο του ανά χείρας πονήματος). Εδώ υπάρχει ένα στοιχείο που είναι ευρύτερο σε σχέση με την απλή αντιστοίχιση ενός αντίμετρου με μια επίθεση πλευρικού καναλιού, πρόκειται για την διεύρυνση της αντίληψης σχετικά με τα αντίμετρα και με το τι είναι ικανές να πλήξουν οι SCAs. Με αυτό εννοείται πως οι ταξινομήσεις αναδεικνύουν διαστάσεις πέρα από την στενή (stricto sensu) έννοια του επιτιθέμενου ή του ορισμού μιας οποιασδήποτε SCA. Αυτές οι διαστάσεις αφορούν περισσότερο στην ευρετική αντίληψη για τον συνδυασμό ξεχωριστών στοιχείων όταν λαμβάνει χώρα μια επίθεση, και αυτός ο συνδυασμός δέον όπως αποτυπώνεται και στον σχεδιασμό αντίμετρων.

Επί παραδείγματι, αυτή η διεύρυνση στην αντίληψη περί των SCAs αποτυπώνεται στην προσοχή που πρέπει να δοθεί όχι μόνο στις συσκευές, αλλά και στο περιβάλλον (ενν. ο περιβάλλοντας χώρος, environment) εντός του οποίου αυτές

---

[218] Στο σημείο αυτό αρκεί να αξιοποιήσουμε την περίπτωση της οπτικής εκροής, που αναφέρθηκε ανωτέρω. Ενώ η οπτική εκροή σαν ορισμός μένει ίδιος, υπάρχουν εντός του ορισμού αυτού, αφενός η μέθοδος της αντανάκλασης από αντικείμενα πλησίον μιας οθόνης. Και αφετέρου, η οπτική εκροή με την μέθοδο της παρατήρησης των λαμπτήρων LED σε ένα router για να καταγραφεί η μετάδοση των πακέτων δεδομένων (workload pattern). Βλ. ενδεικτικά, Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton,St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer,2021,10.1007/s41635-021-00112-6.hal-03176249,*1-24,σ.6.https://hal.archives-ouvertes.fr/hal-03176249/document (τελευταία πρόσβαση 15/10/2021).

τοποθετούνται και λειτουργούν[219]. Η έννοια του περιβάλλοντος εξειδικεύεται περαιτέρω τόσο στα αντικείμενα και το που αυτά τοποθετούνται χωρικά (και προφανώς και σε ότι αφορά τον συνδυασμό των εκροών τους), όσο επίσης και το πώς κινούνται αλλά και πως χρησιμοποιούν τις συσκευές που ενέχουν εκροές οι άνθρωποι που μπορεί να βρίσκονται στον ίδιο χώρο με αυτές[220][221]. Οι πειραματικές συνθήκες και τα εγχειρήματα ταξινόμησης πρέπει να συνεχίζουν να λαμβάνουν υπόψη τους αυτές , τις όχι αυστηρά συνδεόμενες με την τεχνική πτυχή, παραμέτρους όχι μόνο για τον σχεδιασμό αντιμέτρων, αλλά και για την κατάρτιση τυχόν συστάσεων και οδηγών καλών πρακτικών για το προσωπικό που εργάζεται εντός των κρίσιμων υποδομών.

[219] Χαρακτηριστικά στο παράδειγμα των Davis et al. όπου και μελετάτε η αλληλεπίδραση, μεταξύ άλλων, ανάμεσα στις εκροές και στα αντικείμενα του περιβάλλοντος, υπάρχουν και αντικείμενα (π.χ. σακούλα με potato chips) που δεν ανήκουν καθόλου στο εύρος των ηλεκτρονικών συσκευών (π.χ. Android συσκευές, υπολογιστές, κυκλώματα κλπ) και που ορισμένες φορές δύσκολα περιλαμβάνονται σε ορισμένες αναλύσεις, παρά το ότι συνδυαστικά μπορούν να αποδειχθούν πηγές κινδύνου (π.χ. κόλλες αναφοράς, τοίχοι, σακούλες με πατατάκια). Ακόμα και διαισθητικά είναι δύσκολο να λαμβάνει ο καθένας υπόψη τέτοιες περιπτώσεις και εδώ φαίνεται πάλι η αναγκαιότητα σχεδιασμού αξιοποιήσιμων ταξινομήσεων. Ορά ενδεικτικά τις εικόνες του σχήματος στο ακόλουθο άρθρο, Davis, A., & Rubinstein, M., & Wadhwa, N., & Mysore, G.J., & Durand, F., & Freeman, W.T.(2014). The Visual Microphone: Passive Recovery of Sound from Video. *ACM Transactions on Graphics, 33, 4, 79,*1-10,σ.1. doi: https://doi.org/10.1145/2601097.2601119. https://dl.acm.org/doi/10.1145/2601097.2601119 (τελευταία πρόσβαση 22/1/2022).

[220] Εδώ αρκούμαστε, για λόγους οικονομίας χώρου, στο παράδειγμα των αντανακλάσεων επάνω σε αντικείμενα που βρίσκονται, για παράδειγμα, κοντά σε μια οθόνη ή ακόμα και των σκιών επάνω σε αντικείμενα όπως οι τοίχοι. Βλ. ενδεικτικά, Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials, vol. XX,No. Z,Month YYYY,*1-24(465-488),σ.9. doi:10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (τελευταία πρόσβαση 16/9/2021).

[221] Για την σημασία του τρόπου χρήσης των συσκευών και επίσης για την σημασία της εγγύτητας ή της στάσης του σώματος (και το πώς ο επιτιθέμενος μπορεί να την εκμεταλλευθεί και με την χρήση αλγορίθμων μηχανικής μαθήσεως) βλ. ενδεικτικά, Steiner, I.G., & LeFevre, Z., & Serwadda,A.(2020). Smartphone Speech Privacy Concerns from Side-Channel Attacks on Facial Biomechanics. *Computers & Security,vol.100,*1-16,σ.11.doi: 10.1016/j.cose.2020.102110.https://www.researchgate.net/publication/345906717_Smartphone_Speech_Privacy_Concerns_from_Side-Channel_Attacks_on_Facial_Biomechanics (τελευταία πρόσβαση 14/12/2021).

Μέρος 2ο

Περιπτώσεις SCAs κατά IoT συσκευών & Ενσωματωμένων Συστημάτων στις Κρίσιμες Υποδομές (CI) & Συστηματοποίηση Αντιμέτρων (Countermeasures)

Κεφάλαιο 3ο : Επιθέσεις Πλευρικού Καναλιού (SCAs) εναντίον Κρίσιμων Υποδομών (CI)

Στο πρώτο κεφάλαιο του δευτέρου μέρους του ανά χείρας πονήματος ορίζουμε τους κάτωθι δύο στόχους ως εξής :

- Αρχικά, πρέπει να οριστεί το γενικό συγκείμενο (context) του παρόντος κεφαλαίου μέσα από την παράθεση του ορισμού και των κυριότερων χαρακτηριστικών που αφορούν στις κρίσιμες υποδομές (critical infrastructures, CI). Ακολούθως θα παρατεθούν ορισμένα παραδείγματα κρίσιμων υποδομών, ώστε μέσα από την παράθεση ορισμού και παραδειγμάτων να οριοθετηθεί σαφώς το αντικείμενο του δευτέρου μέρους της διπλωματικής, και αφετέρου να καταστεί σαφές ποια είναι εκείνα τα αγαθά (εύρος των assets) που οι επιθέσεις πλευρικού καναλιού δύνανται να απειλήσουν.
- Το δεύτερο μέρος με το οποίο και ολοκληρώνεται το παρόν κεφάλαιο αφορά στην μελέτη των κρίσιμων υποδομών υπό το πρίσμα των SCAs αυτή την φορά. Εδώ η στόχευση αφορά στην παράθεση στοιχείων για την μεθοδολογία των σχετικών επιθέσεων έναντι κάποιας υποδομής, και επιπλέον στις επιμέρους πτυχές και εκροές (leakage,emanations) των υποδομών που αποτελούν δυνητικά το πρωταρχικό σημείο εκμετάλλευσης ή τον τελικό στόχο μιας ή διαφόρων επιθέσεων πλευρικού καναλιού. Με βάσει την υπάρχουσα βιβλιογραφία που μελετήθηκε, η διπλωματική εργασία θα εστιάσει, σε αυτό το σημείο, περισσότερο στις περιπτώσεις των IoT συσκευών, των ενσωματωμένων συστημάτων και σε μικρότερο βαθμό σε πτυχές του λογισμικού (neural networks, αλγόριθμοι κρυπτογράφησης κλπ), καθώς η βιβλιογραφία περιορίζεται κατά βάση σε αυτές τις θεματικές και επίσης γιατί πρέπει να υφίσταται μια εστίαση του ανά χείρας πονήματος σε ένα θέμα τόσο εκτενές όσο οι κρίσιμες υποδομές.

Υπό-ενότητα 3.1: Περί του ορισμού των κρίσιμων υποδομών (CIs) και των σχετικών παραδειγμάτων

Σε ότι αφορά σε έναν συνεκτικό και περιεκτικό ορισμό των κρίσιμων υποδομών (critical infrastructure, CIs) δυνάμεθα όπως παραθέσουμε τα κάτωθι στοιχεία (elements) τα σχετικά με έναν τέτοιο ορισμό:

- Αρχικά, οι εννοιολογικοί προσδιορισμοί που το κάθε επιστημονικό άρθρο ή επίσημη αναφορά παραθέτουν σχετικά με τις κρίσιμες υποδομές καταδεικνύουν , μέσα από τις όποιες διαφορές τους, το εύρος και την πολυπλοκότητα αυτών των τελευταίων. Εδώ αναφύονται κατά βάση δύο σημεία προβληματισμού (μια αντινομία κατά βάση), αφενός όλες εκείνες τις περιπτώσεις που ο ορισμός δεν θα συμπεριλάβει για διάφορους λόγους (π.χ. μεθοδολογία, σκοπός του ορισμού κλπ), αφετέρου όλες οι περιπτώσεις που θα περιληφθούν και που μπορεί να αυξήσουν υπέρμετρα το εύρος, φτάνοντας στο σημείο ο ορισμός κρίσιμες υποδομές να σημαίνει τα πάντα και γι' αυτό τίποτα, άρα να μην είναι λειτουργικός λόγω εύρους ενώ πριν δεν ήταν λειτουργικός λόγω στενότητας[222]. Επιπροσθέτως, η συζήτηση περί στενότητας και ευρύτητας των ορισμών συνδέεται και αναδεικνύει παράλληλα και την σχετική συζήτηση για την ρευστή (fluidity) εννοιολόγηση των επιμέρους στοιχείων των ορισμών, με αποτέλεσμα κάποια από τα στοιχεία αυτά να ορίζονται αλλαχού και να μην υπάρχει έτσι μια ολοκληρωμένη και σταθερή αποσαφήνιση των εκάστοτε νοημάτων.

Επί παραδείγματι, οι Izuakor & White παρατηρούν πως υφίσταται μια ορισμένη δυσκολία στην διάκριση ανάμεσα στον ορισμό του θύματος (victim) σε περιπτώσεις που πλήττεται μια υποδομή και σε εκείνο του μέσου (vector[223]) που θα επιχειρήσει να πλήξει αυτή την τελευταία. Ειδικότερα, αναφέρεται το παράδειγμα του αγροτικού/επισιτιστικού τομέα, όπου αν μια αγελάδα μολυνθεί με κάποιον ιό τότε μπορεί εξίσου να θεωρηθεί το θύμα (victim) μιας επίθεσης κατά κρίσιμης υποδομής (bioterrorism), όσο και μέσο για την εκτέλεση μιας επίθεσης (vector, δηλαδή το ζώο ως ξενιστής του συγκεκριμένου ιού κλπ[224]).

---

[222] Πρβλ. Fjader & Riedman στο Heino, O., & Takala, A., & Jukarainen, P., & Kalalahti, J., & Kekki, T., & Verho,P.(2018). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability 2019, 11(3), 838,*1-18, σ.4.doi: https://doi.org/10.3390/su11030838. https://www.mdpi.com/2071-1050/11/3/838 (τελευταία πρόσβαση 30/1/2022).

[223] Izuakor,C. & White, R.(2017). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Paper presented at the 10th Conference on Critical Infrastructure Protection (ICCIP). Arlington, VA, USA.March,10-13,27-41,σ.38.doi:10.1504/IJCIS.2017.083634. https://www.researchgate.net/publication/309613559_Critical_Infrastructure_Asset_Identification_Policy_Methodology_and_Gap_Analysis (τελευταία πρόσβαση 22/1/2022).

[224] Ο.π.

Ειδικότερα, σε ότι αφορά το εύρος των διαφόρων ορισμών πρέπει να ειπωθεί πως υφίστανται περιπτώσεις όπου οι ορισμοί (τουλάχιστον αφετηριακά) διατηρούν μια κάποια στενότητα, και επομένως οριοθετούν τα assets των κρισίμων υποδομών stricto sensu[225]. Επί παραδείγματι, τόσο η ΕΕ όσο και οι ΗΠΑ σε ορισμούς που έδιναν στις αρχές της δεκαετίας του '00 περί των κρισίμων υποδομών εμφάνιζαν μια σχετική στενότητα στο τρόπο με τον οποίο τις όριζαν[226]. Αφενός, η ΕΕ ξεκίνησε με ένα στενότερο ορισμό των assets που ουσιαστικά περιλάμβανε τους δύο τομείς της ενέργειας και των μεταφορών ενώ επικέντρωνε περισσότερο σε τρομοκρατικής φύσεως απειλές, πριν προχωρήσει σε διεύρυνση αυτής της λίστας σε κατοπινά έτη[227]. Αφετέρου, οι ΗΠΑ διεύρυναν τον δικό τους ορισμό για να συμπεριλάβουν και ανθρωπογενείς καταστροφές ιδίως με αφορμή τον τυφώνα Κατρίνα[228].

Επιπλέον, το εύρος του ορισμού δύναται να ποικίλει και σε ότι αφορά και στο πεδίο εφαρμογής, για παράδειγμα η ΕΕ δίνει ιδιαίτερη έμφαση στην διασυνοριακή διάσταση των κρίσιμων υποδομών, οπότε και η διάσταση του εύρους εκτείνεται ίσως και πέρα από τον αντίστοιχο ορισμό που ένας κράτος έχει για τις υποδομές αυτές. Σε αυτό

---

[225] Χαρακτηριστικό παράδειγμα αποτελεί η ΕΕ η οποία όταν και εξέδωσε την Directive 2008/114/EC για να ορίσει τις κρίσιμες υποδομές ουσιαστικά επικεντρώθηκε σχεδόν αποκλειστικά σε δύο τομείς ήτοι τον ενεργειακό και εκείνο των μεταφορών, πρβλ. Anglmayer, I.(2021). *European critical infrastructure Revision of Directive 2008/114/EC*(PE 662.604). Brussels: European Parliamentary Research Service,σ.1.Ανακτήθηκε από: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)662604 (τελευταία πρόσβαση 27/1/2022).

[226] Ο.π.

[227]Για παράδειγμα πέντε χρόνια μετά η ΕΕ προσπαθώντας να εγκαινιάσει μια νέα προσέγγιση στο ευρωπαϊκό πρόγραμμα για την προστασία των κρισίμων υποδομών (EPCIP) όπου και εστίασε σε τέσσερις πανευρωπαϊκές υποδομές, ήτοι το Eurocontrol (ευρωπαϊκός οργανισμός αεροναυτιλίας), το Galileo (ευρωπαϊκό πρόγραμμα ραδιοπλοήγησης και προσδιορισμού θέσης μέσω δορυφόρου), τον ευρωπαϊκό οργανισμό μεταφοράς ηλεκτρικής ενέργειας, και το ευρωπαϊκό δίκτυο μεταφοράς φυσικού αερίου. Περαιτέρω, το 2017 προστέθηκαν και οι κυβερνοαπειλές/κυβερνοεπιθέσεις στα συστήματα ελέγχου των βιομηχανιών (ψήφισμα 3ης του Οκτωβρίου 2017) Ο.π.,σ.5,8.

[228] Izuakor,C. & White, R.(2017). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Paper presented at the 10th Conference on Critical Infrastructure Protection (ICCIP). Arlington, VA, USA. March,10-13, 27-41, σ.28. doi: 10.1504/IJCIS.2017.083634. https://www.researchgate.net/publication/309613559_Critical_Infrastructure_Asset_Identification_Policy_Methodology_and_Gap_Analysis (τελευταία πρόσβαση 22/1/2022).

το παράδειγμα φαίνεται ότι το εύρος του ορισμού κάλλιστα μπορεί να μικρύνει αν και οι χώρες της ΕΕ είναι περισσότερες, εντούτοις όταν η διασυνοριακή διάσταση τίθεται, τότε υπάρχουν υποδομές που λειτουργούν μόνο εντός των ξεχωριστών κρατών, και άλλες που εκτείνονται εκτός συνόρων[229]. Περαιτέρω, μπορεί ο όρος κρίσιμες να χρησιμοποιείτε αλλαχού με τον όρο στρατηγικός[230]. Τέλος δε, παρατηρείται πως στο πέρασμα των ετών δύναται να υπάρξει μια διεύρυνση ενδεχομένως της λίστας των απειλών έναντι των κρίσιμων υποδομών, και πως σε ότι αφορά τις απειλές μπορεί ενδεχόμενα να ποικίλλει κάπως η σχετική βαρύτητα που δίδεται σε αυτές[231].

Όλων τούτων δοθέντων παρατίθενται ακολούθως οι σχετικοί περί των κρίσιμων υποδομών, ως εξής :

- Κρίσιμος/κρισιμότητα (critical/criticality): κατά βάση η κρισιμότητα ορίζεται με δύο αλληλένδετους τρόπους (δύο βασικές πτυχές). Αφενός, από την θέση ενός asset εντός ενός ευρύτερου πλαισίου αποτελούμενου από assets (δικτυοκεντρική

[229] Anglmayer, I.(2021). *European critical infrastructure Revision of Directive 2008/114/EC*(PE 662.604). Brussels: European Parliamentary Research Service,σ.3. Ανακτήθηκε από: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)662604 (τελευταία πρόσβαση 27/1/2022).

[230] Ορά επί παραδείγματι τον τίτλο της ακόλουθης αναφοράς προς το ευρωκοινοβούλιο, αν και ο εν γένει ο όρος κρίσιμες υποδομές είναι εκείνος που επικρατεί. Tessari, P. & Muti, K.(2021). *Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations* (PE 653.637).Brussels: Requested by the INGE committee European Parliament,σ.1 κε. Ανακτήθηκε από: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf (τελευταία πρόσβαση 30/1/2022).

[231] Επί παραδείγματι, το σχέδιο για την προστασία των εθνικών κρισίμων υποδομών (NIPP) των ΗΠΑ στην αρχή έδινε καταρχήν σχεδόν απόλυτη βαρύτητα στην ανάλυση ρίσκου με στόχο την προστασία των υποδομών από τρομοκρατικές επιθέσεις (υπό την σκιά και των επιθέσεων της 9/11), η στόχευση αυτή στα χρόνια που ακολούθησαν το αρχικό αυτό σχέδιο (2006) διευρύνθηκε. Πρβλ. Izuakor,C. & White, R.(2017). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Paper presented at the 10th Conference on Critical Infrastructure Protection (ICCIP). Arlington, VA, USA. March,10-13, 27-41, σ.28.doi:10.1504/IJCIS.2017.083634. https://www.researchgate.net/publication/309613559_Critical_Infrastructure_Asset_Identification_Policy_Methodology_and_Gap_Analysis (τελευταία πρόσβαση 22/1/2022).

προσέγγιση), κάτι που συνεπάγεται το ότι η συσχέτιση μεταξύ των assets θα κρίνει την κρισιμότητα τους ή μη[232].

Αφετέρου, με βάσει τα ίδια τα χαρακτηριστικά που φέρει ένα asset, για παράδειγμα οι οικονομικές επιπτώσεις που μπορεί να προκληθούν λόγω της ζημίας αυτού ή η πιθανότητα απώλειας ζωής ενός τμήματος του πληθυσμού εξαιτίας της αδυναμίας λειτουργίας ενός asset[233].

Ειδικότερα για το δεύτερο αυτό σημείο ο Metzger επισημαίνει πως είναι ευρύτερο του πρώτου καθώς καλείται να λάβει υπόψη και άλλες πτυχές της κρισιμότητας των assets και ενδεχομένως μη τεχνικά τους χαρακτηριστικά (πρόκειται για μια προσέγγιση ,με βάσει τα κριτήρια, ήτοι criteria-based[234]).

- Κρίσιμες υποδομές (Critical Infrastructure(s),CIs), 1ος ενδεικτικός ορισμός: Ενδεικτικά παραθέτουμε κάποιους ορισμούς που έχουν δοθεί για τις κρίσιμες υποδομές. Στην περίπτωση των ΗΠΑ οι κρίσιμες υποδομές ορίζονται από το «*σχέδιο για την προστασία των υποδομών του 2013*» («*US National Infrastructure Protection Plan 2013*») ως ακολούθως : «*συστήματα και περιουσιακά στοιχεία που είτε μέσω της φυσικής τους ή εικονικής τους υποστάσεως, είναι τόσο ζωτικά για τις ΗΠΑ που η αποτελμάτωση ή καταστροφή τέτοιων συστημάτων και περιουσιακών στοιχείων θα επιφέρει δυνάμει μια αποδυνάμωση της ασφάλειας (ενν. το security), της εθνικής οικονομίας, της εθνικής δημόσιας υγείας ή της ασφάλειας (ενν. το safety), ή ενός συνδυασμού των παραπάνω ζητημάτων*[235]».
- Κρίσιμες υποδομές (Critical Infrastructure(s),CIs),2ος ενδεικτικός ορισμός: στην δε περίπτωση

[232] Ο.π.,σ.32.

[233] Ο.π.

[234] Ο.π.,σ.33.

[235] Heino, O., & Takala, A., & Jukarainen, P., & Kalalahti, J., & Kekki, T., & Verho,P.(2018). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability 2019, 11(3), 838,*1-18, σ.4.doi: https://doi.org/10.3390/su11030838. https://www.mdpi.com/2071-1050/11/3/838 (τελευταία πρόσβαση 30/1/2022).

της ΕΕ, που δεν αποτελεί κυρίαρχο κράτος, ο ορισμός που είχε δοθεί αρχικά το 2008 (διευρύνθηκε βεβαίως σε κατοπινά έτη) όριζε τις κρίσιμες υποδομές ως εξής «*ένα περιουσιακό στοιχείο, ένα σύστημα ή μέρος αυτού, ευρισκόμενο στο έδαφος των κρατών-μελών, το οποίο είναι στοιχειώδες για την διατήρηση των ζωτικών κοινωνικών λειτουργιών, για την υγεία, την ασφάλεια, την οικονομία ή την κοινωνική ευημερία των ανθρώπων, και του οποίου η διακοπή της λειτουργίας του ή η καταστροφή αυτού θα είχε δυνάμει μια σημαντική επίπτωση σε ένα κράτος-μέλος ως αποτέλεσμα της αποτυχίας σε ότι αφορά στην διατήρηση αυτών των λειτουργιών*[236]».

- Κρίσιμες υποδομές (Critical Infrastructure(s), CIs)3ος ενδεικτικός ορισμός: το κράτος της Αυστραλίας παραθέτει τον ακόλουθο ορισμό περί των κρισίμων υποδομών ως εξής «*υλικές εγκαταστάσεις, αλυσίδες προμηθειών, τεχνολογίες πληροφορικής και δίκτυα επικοινωνιών, τα οποία σε περίπτωση που καταστραφούν, υποβαθμιστούν ή καταστούν μη διαθέσιμα για μια εκτεταμένη χρονική περίοδο, θα επηρέαζαν σημαντικά την κοινωνική ή οικονομική ευημερία του έθνους, ή θα επηρέαζαν την ικανότητα της Αυστραλίας να οργανώσει την εθνική της άμυνα και να διασφαλίσει την εθνική της ασφάλεια*[237]».
- Περιουσιακό στοιχείο κρισίμων υποδομών (Critical Infrastructure Asset): η παρούσα έρευνα δεν εντόπισε κάποιον ιδιαίτερο ορισμό για το asset, αντίθετα το τελευταίο εμμέσως ορίζεται μέσα από τον ευρύτερο ορισμό που δίδεται για

[236] Udeanu, G.(2015). *A New Approach To The European Programme For Critical Infrastructure Protection.* Paper presented at the 21st International Conference The Knowledge-Based Organization, Conference Proceedings 1 Management and Military Sciences, 21, 1, 2015, 135-142,σ.135. doi: https://doi.org/10.1515/kbo-2015-0022. https://sciendo.com/article/10.1515/kbo-2015-0022 (τελευταία πρόσβαση 24/01/2022).

[237] Izuakor, C. & White, R.(2017). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Paper presented at the 10th Conference on Critical Infrastructure Protection (ICCIP). Arlington, VA, USA. March,10-13, 27-41, σ.30. doi: 10.1504/IJCIS.2017.083634. https://www.researchgate.net/publication/309613559_Critical_Infrastructure_Asset_Identification_Policy_Methodology_and_Gap_Analysis (τελευταία πρόσβαση 22/1/2022).

τις κρίσιμες υποδομές εν γένει. Ο όρος asset περισσότερο χρησιμοποιείται όταν ο αντίστοιχος όρος κρίσιμη υποδομή εξειδικεύεται περαιτέρω σε ένα ευρύ φάσμα παραδειγμάτων από διάφορους τομείς που εντάσσονται στο πεδίο του εν λόγω ορισμού. Τέτοια παραδείγματα αποτελούν ο ενεργειακός τομέας, η αμυντική βιομηχανία, ο τομέας της υγείας, εκείνος ων μεταφορών κλπ, υπό αυτή την έννοια ο όρος asset ή χρησιμοποιείται αλλαχού με τον όρο τομέας (sector), ή θα υπονοεί μέρος ή το σύνολο των τεχνικών μέσων και εμμέσως και του προσωπικού[238].

- Αν και ο χώρος στην παρούσα υπό-ενότητα δεν επαρκεί για έτερες παραθέσεις ενδεικτικών ορισμών, εντούτοις οι τρεις προαναφερθέντες αρκούν για να καταδείξουν όσα αναφέρθηκαν ανωτέρω. Και εδώ διακρίνεται μια αρκετά μεγάλη ευρύτητα και σχετικότητα των ορισμών, επίσης διακρίνεται μια διαπλοκή των επιμέρους στοιχείων που ο εκάστοτε ορισμός δεν αποτυπώνει ιδιαιτέρως ξεκάθαρα (π.χ. σχέση του κοινωνικού με το τεχνικό στοιχείο, η έμφαση είναι κυρίως το δεύτερο κλπ), τέλος δε υφίσταται μια σχετικότητα στην χρήση των επιμέρους στοιχείων που συνθέτουν τον ορισμό, καθώς στην περίπτωση της ΕΕ οι επιπτώσεις αναφέρονται σε κράτη-μέλη κυρίως ενώ στις άλλες δύο αναφέρονται περισσότερο στην κοινωνία των πολιτών, ενώ ταυτόχρονα η σχέση μέσου επίθεσης-πιθανού στόχου δείχνεται μονοσήμαντα (π.χ. δεν καταδεικνύεται πως , μέσω της αλληλεπίδρασης, μια υποδομή εκτός από στόχος θα μπορούσε δυνάμει να είναι και vector για την στόχευση μιας άλλης υποδομής κλπ).

- Δεύτερο στοιχείο, που συνδέεται με τον ορισμό, αφορά στην ύπαρξη μιας σχετικής και οσοδήποτε αναλυτικής (στάδια κλπ) μεθοδολογίας (methodology). Η

[238] Πρβλ. χ.σ.(χ.χ.). Changes to better protect critical infrastructure. *Australian Government Department of Home Affairs, Cyber and Infrastructure Security Centre.* Ανακτήθηκε από: https://www.cisc.gov.au/changes/changes-to-current-regulation/regulatory-obligations (τελευταία πρόσβαση 2/2/2022).

μεθοδολογία αυτή μπορεί να διαφέρει από την μια αναφορά στην άλλη σε ότι αφορά τις παραμέτρους που τίθενται, αλλά η βασική στόχευση είναι η αναγνώριση των κρισίμων υποδομών και η αποτίμηση των μέτρων προστασίας που έχουν ληφθεί γι' αυτές. Αναφορικά με την αναγνώριση των assets των κρισίμων υποδομών οι Izuakor & White (για να αναφέρουμε ορισμένα ενδεικτικά παραδείγματα) εντοπίζουν τρεις προσεγγίσεις, ήτοι εκείνη που βασίζεται στην λειτουργία (function-based), την δικτυοκεντρική (network-based), και την βασιζόμενη στην λογική (logic-based[239]). Οι δύο πρώτες κινούνται ενδεχομένως σε ευρύτερο επίπεδο αφαίρεσης και αναφέρονται από τους συγγραφείς ως συστημικές προσεγγίσεις (systematic) , ενώ η τελευταία αναφέρεται ως μη συστηματική (unsystematic) καθότι φέρεται να είναι πιο κοντά στο ατομικό επίπεδο. Οι τρεις αυτές προσεγγίσεις ενδεικτικά αφορούν σε :

- Λειτουργική προσέγγιση (function-based approach): βασικό κριτήριο εδώ αποτελεί η λειτουργία που ένα asset ή διάφορα assets των υποδομών επιτελούν. Έχοντας ορίσει τις λειτουργίες που είναι σημαντικές για την επίτευξη του σκοπού της εκάστοτε υποδομής, τότε με βάσει το αν ένα asset επιτελεί ή υποβοηθά τις λειτουργίες αυτές θα οριστεί ως κρίσιμο για την υποδομή[240].
- Δικτυοκεντρική προσέγγιση (network-based approach): τα assets κρίνονται ως κρίσιμα με βάσει τις συσχετίσεις που έχουν με άλλα τμήματα των υποδομών, έτσι δημιουργείται ουσιαστικά μια χαρτογράφηση και με βάσει αυτή προσδιορίζεται η σημασία του asset για την υποδομή[241].
- Λογική προσέγγιση (logic-based approach): τα assets προσδιορίζονται ως κρίσιμα ή μη για την υποδομή με βάσει

[239] Izuakor,C. & White, R.(2017). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Paper presented at the 10th Conference on Critical Infrastructure Protection (ICCIP). Arlington, VA, USA.March,10-13,27-41,σ.32.doi:10.1504/IJCIS.2017.083634. https://www.researchgate.net/publication/309613559_Critical_Infrastructure_Asset_Identification_Policy_Methodology_and_Gap_Analysis (τελευταία πρόσβαση 22/1/2022).

[240] Ο.π.

[241] Ο.π.

λογικά κριτήρια που ορίζουν οι κάθε φορά αξιολογητές της εκάστοτε υποδομής[242].

Πέρα όμως και από τις διαφορετικές θεωρητικές προσεγγίσεις που αναφέρθηκαν ανωτέρω, η μεθοδολογία δείχνει να διαφοροποιείται και σε ότι αφορά στην κατάρτιση του σχεδιασμού των βημάτων που οι εκάστοτε οργανισμοί διενεργούν για να προσδιορίσουν τις κρίσιμες υποδομές (πρακτικό σκέλος που αφορά στους κατά περίπτωση οργανισμούς). Αξίζει να σταθούμε στις δύο χαρακτηριστικές περιπτώσεις αφενός των ΗΠΑ και αφετέρου της ΕΕ.

Στην περίπτωση των ΗΠΑ δύο βασικά σχέδια κυβερνητικών φορέων, ήτοι το εθνικό πρόγραμμα προτεραιοποίησης των κρισίμων υποδομών (National Critical Infrastructure Prioritization Program, NCIPP) του Department of Homeland Security και αμυντικό πρόγραμμα κρισίμων υποδομών (Defense Critical Infrastructure Program, DCIP) του υπουργείου Εθνικής Αμύνης (U.S. Department of Defense) διαφοροποιούνται ως προς τα εξής στοιχεία[243]:

- Ως προς τον αριθμό των βημάτων, το πρώτο σχέδιο απαιτεί τέσσερα κριτήρια για τον εντοπισμό του ελάχιστου ορίου συνεπειών («*consequence category threshold*[244]») και κατόπιν το κατώφλι αυτό διακρίνεται στα επίπεδα 1 και 2, όπου το asset επιπέδου 1 έχει μεγαλύτερη προτεραιότητα. Αντίθετα το δεύτερο σχέδιο έχει εννέα βήματα για την πρώτη φάση και πέντε κριτήρια για την αναγνώριση των assets κατόπιν[245].
- Ως προς τους εμπλεκόμενους δρώντες που συνδιαμορφώνουν τις λίστες των κρισίμων υποδομών. Στην πρώτη περίπτωση συμμετέχουν υπηρεσίες εθνικής ασφάλειας (homeland security) και έτερες υπηρεσίες σε ομοσπονδιακό επίπεδο. Ενώ στην δεύτερη οι mission owners[246].

[242] Ο.π.

[243] Ο.π.,σ.33-34.

[244] Ο.π.,σ.34.

[245] Ο.π.

[246] Ο.π.

- Τέλος, το πρώτο σχέδιο δίνει προτεραιότητα στις υποδομές αφού πρώτα αναγνωρίσει ποιες είναι αυτές, ενώ το δεύτερο κινείται αντιστρόφως, καθώς δίνει προτεραιότητα όχι με βάσει την αναγνώριση ενός asset ως κρίσιμου αλλά με βάσει τους στόχους της κάθε αποστολής (π.χ. τις δυνατότητες που η εκάστοτε αποστολή θα χρειαστεί να αξιοποιήσει, capability requirements)[247].

Από την άλλη η ΕΕ ως υπερεθνικός οργανισμός διαθέτει κι εκείνη το δικό της σχέδιο για την προστασία κρισίμων υποδομών (ευρωπαϊκό πρόγραμμα για την προστασία των κρισίμων υποδομών, European Programme on Critical Infrastructure Protection, EPCIP). Το σχέδιο περιλαμβάνει 4 βήματα σε ότι αφορά την αξιολόγηση των κρισίμων υποδομών. Λόγω και του μεγέθους αλλά και της περιπλοκότητας του εν λόγω οργανισμού, ο κάθε τομέας δραστηριότητας έχει δικά του κριτήρια για την αναγνώριση των assets που θεωρηθούν ως κρίσιμα[248]. Το κατώφλι της ελάχιστης βαθμολογίας ορίζεται από τα κράτη-μέλη, κατόπιν το asset ή η υποδομή αξιολογείται με βάσει κριτήρια που αφορούν στις διασυνοριακές επιπτώσεις (cross-border) που αυτή η υποδομή δύναται να έχει[249].

Κατόπιν η ίδια υποδομή αξιολογείται και με βάσει έτερα κριτήρια (cross-cutting criteria) όπως οι ενδεχόμενες απώλειες, οικονομικές απώλειες και ο αντίκτυπος στο ηθικό των πολιτών κλπ (και σε αντιστοιχία με βάσει το κάθε φορά εύλογα χειρότερο σενάριο[250]). Ολοκληρώνοντας η κάθε υποδομή πρέπει να πληροί αφενός και τα τέσσερα κριτήρια (ήτοι να διέλθει και των τεσσάρων βημάτων) και αφετέρου να αναγνωρίζεται ως κρίσιμη και από το κράτος-μέλος εντός του οποίου ευρίσκεται, επομένως οι δύο αυτές συνισταμένες (4 κριτήρια και αποδοχή από το κράτος-μέλος) πρέπει να λειτουργούν σωρευτικά για να χαρακτηριστούν ως τέτοιες οι εκάστοτε κρίσιμες υποδομές[251].

Εν κατακλείδι, οι δύο συγγραφείς παραθέτουν δύο είδη κριτηρίων που οι εκάστοτε μεθοδολογίες (ή έστω ορισμένες εξ αυτών) δύναται να αξιοποιήσουν για την αναγνώριση των κρίσιμων υποδομών, αφενός τα ποιοτικά και αφετέρου τα ποσοτικά

[247] Ο.π.

[248] Ο.π.,σ.35.

[249] Ο.π.

[250] Ο.π.

[251] Ο.π.

κριτήρια[252]. Αναφορικά με τα ποιοτικά κριτήρια, αυτά μπορεί να περιλαμβάνουν (με παράδειγμα αναφοράς το σχέδιο για τις κρίσιμες υποδομές του αμερικανικού Homeland Security):

- Ολιστική προσέγγιση (completeness): το κριτήριο πληρείται όταν έχουν εξεταστεί όλα τα assets ενός τομέα που δυνητικά θα μπορούσαν να ανήκουν στην κατηγορία των κρίσιμων υποδομών[253].
- Αναπαραγωγισιμότητα (Reproducibility): τα κριτήρια που χρησιμοποιούνται είναι απλά και ομοιόμορφα για να επιτρέπονται έτσι οι συγκρίσεις ανάμεσα στις σχετικές με το ρίσκο βαθμολογίες που έχουν δοθεί[254].
- Καταγραφή/αρχειοθέτηση (Documentation): συγκέντρωση και καταγραφή των πληροφοριών που αξιοποιήθηκαν στην εκτίμηση ρίσκου για ένα οποιοδήποτε asset[255].
- Δυνατότητα υπεράσπισης (Defensibility): αφορά στην δυνατότητα υπεράσπισης (απόδειξης) της επιστημονικής μεθόδου ή των επιστημονικών μεθόδων που αποτέλεσαν την βάση της αξιολόγησης, κυρίως δε στην δυνατότητα να αποδειχθεί πως δεν έχουν λάβει χώρα σημαντικά λάθη ή παραλήψεις κατά την διαδικασία εφαρμογής της εκάστοτε μεθοδολογίας[256].

- Οι κρίσιμες υποδομές στον βαθμό που αναπτύσσονται επιφέρουν μια ταυτόχρονη επαύξηση της αλληλεξάρτησης(interdependency), που με την σειρά της συνδράμει την ανάπτυξη των υποδομών[257], και αυτό αποτελεί το τρίτο κατά σειρά στοιχείο. Πέρα και από την από κοινού ανάπτυξη τους, οι κρίσιμες υποδομές

[252] Ο.π.,σ.30.

[253] Ο.π.

[254] Ο.π.

[255] Ο.π.

[256] Ο.π.,σ.31.

[257] Udeanu, G.(2015). *A New Approach To The European Programme For Critical Infrastructure Protection.* Paper presented at the 21st International Conference The Knowledge-Based Organization, Conference Proceedings 1 Management and Military Sciences, 21, 1, 2015, 135-142,σ.136. doi: https://doi.org/10.1515/kbo-2015-0022. https://sciendo.com/article/10.1515/kbo-2015-0022 (τελευταία πρόσβαση 24/1/2022).

αλληλεξαρτώνται και σε ότι αφορά την διακοπή της λειτουργίας τους (disruption), με αποτέλεσμα η ζημία σε μια εξ' αυτών εύλογα να επιδρά και στις υπόλοιπες με ανάλογες λίγο έως πολύ συνέπειες[258][259]. Επί παραδείγματι στην περίπτωση της ΕΕ η αλληλεξάρτηση αναφορικά με τις κρίσιμες υποδομές εκφράζεται στις παρακάτω τέσσερις (4) συσχετίσεις :

- Στην αλληλεξάρτηση ανάμεσα στις διάφορες υποδομές (π.χ. δορυφορικό σύστημα Galileo,ευρωπαϊκό Δίκτυο των Διαχειριστών Συστημάτων Μεταφοράς Ηλεκτρικής Ενέργειας, Ευρωπαϊκό Δίκτυο Διαχειριστών Συστημάτων Μεταφοράς Φυσικού Αερίου κλπ[260]).
- Στην αλληλεξάρτηση ανάμεσα σε υποδομές και στα κράτη-μέλη (διασυνοριακή αλληλεξάρτηση, cross-border[261]).
- Στην αλληλεξάρτηση μεταξύ υποδομών και ευρωενωσιακών οργάνων, ήτοι την ΕΕ (σε επίπεδο ευρωπαϊκής συνεργασίας για την ενίσχυση της συνεργασίας προς ενίσχυση προστασίας υποδομών[262]).
- Στην αλληλεξάρτηση μεταξύ υποδομών, ΕΕ και τρίτων χωρών μη μελών (ενίσχυση υποδομών και μεταφοράς τεχνογνωσίας σε τρίτες χώρες, και εκτός της ευρωπαϊκής ηπείρου[263]).

---

[258] Για ορισμένα συνοπτικά παραδείγματα (π.χ. σχέση δορυφορικών συστημάτων και οικονομίας/ασφάλειας) βλ. Udeanu, G. ο.π.,σ.140.

[259] Είτε και αντιστρόφως, καθώς η αύξηση της αλληλεξάρτησης μπορεί να βελτιώσει την διαλειτουργικότητα των υποδομών αυτών, και άρα να μειώσει την πιθανότητα αλληλοεπικαλυπτόμενων αποτυχιών («*cascading failures*»), οπότε και εδώ όπως και ανωτέρω φαίνεται να υπάρχει μια ταυτολογία όπου η ίδια αιτία οδηγείς και σε εκ διαμέτρου αντίθετα αποτελέσματα και άρα μειώνει την όποια λειτουργική χρήση ενός ορισμού ή μιας ταξινόμησης. Πρβλ. Heino, O., & Takala, A., & Jukarainen, P., & Kalalahti, J., & Kekki, T., & Verho,P.(2018). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability 2019, 11(3), 838,*1-18, σ.6.doi: https://doi.org/10.3390/su11030838. https://www.mdpi.com/2071-1050/11/3/838 (τελευταία πρόσβαση 30/1/2022).

[260] Udeanu, G.(2015). *A New Approach To The European Programme For Critical Infrastructure Protection.* Paper presented at the 21st International Conference The Knowledge-Based Organization, Conference Proceedings 1 Management and Military Sciences, 21, 1, 2015, 135-142,σ.136. doi: https://doi.org/10.1515/kbo-2015-0022. https://sciendo.com/article/10.1515/kbo-2015-0022 (τελευταία πρόσβαση 24/1/2022).

[261] Ο.π.

[262] Ο.π.

[263] Ο.π.,σ.138.

Τα ποσοτικά κριτήρια που αναφέρουν οι δύο συγγραφείς από την άλλη περιλαμβάνουν τα κάτωθι[264]:

- Σκοπός (Scope): αναφέρεται στο εύρος της έρευνας επί τις ουσίας, ο σκοπός μπορεί να είναι είτε η συστηματική διερεύνηση (systematic) του συνόλου των assets και των συνδεόμενων με αυτά στοιχείων, είτε η μη-συστηματική διερεύνηση (unsystematic) που θα επικεντρώνει σε ένα ή ορισμένα μόνο assets και άρα δεν θα εξαντλεί το σύνολο των πιθανών επιλογών[265].
- Προσέγγιση (Approach): εξειδικεύει τον σκοπό που αναφέρεται ακριβώς ανωτέρω. Οι προσεγγίσεις εν γένει διακρίνονται σε λειτουργικές (function-based), δικτυοκεντρικές (network-based) και επίσης σε λογικές (logic-based) προσεγγίσεις, και οι τρεις αναφέρθηκαν κάπως πιο ενδεικτικά ανωτέρω εκεί όπου έγινε λόγος για τις πτυχές τις αφορούσες στον ορισμό των κρισίμων υποδομών[266].
- Εφαρμογή (Application): πρόκειται για εφαρμογή των επιλεγμένων κριτηρίων και τρόπων βαθμολόγησης του εκάστοτε asset με βάσει τις συγκεκριμένες μεθόδους (scoring matrices κλπ) που έχουν επιλεγεί ως τμήμα της μεθοδολογίας[267].

- Τέταρτον, η αλληλεξάρτηση επί της ουσίας λειτουργεί προς δύο κατευθύνσεις, αφενός προς την κατεύθυνση της διαντίδρασης της μιας υποδομής με την άλλη που είναι ως ένα βαθμό εμφανής και σχετικά εύκολα γίνεται αντιληπτή (εκ των προτέρων και σχεδιαστικά επομένως), αφετέρου η αλληλεξάρτηση προκύπτει και από «*λανθάνουσες μεταβλητές*» («*latent variable*[268]») στον βαθμό που υφίστανται παράγοντες

---

[264] Izuakor,C. & White, R.(2017). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Paper presented at the 10th Conference on Critical Infrastructure Protection (ICCIP). Arlington, VA, USA. March,10-13,27-41,σ.32.doi:10.1504/IJCIS.2017.083634. https://www.researchgate.net/publication/309613559_Critical_Infrastructure_Asset_Identification_Policy_Methodology_and_Gap_Analysis (τελευταία πρόσβαση 22/1/2022).

[265] Ο.π.,σ.32.

[266] Ο.π.

[267] Ο.π.

[268] Heino, O., & Takala, A., & Jukarainen, P., & Kalalahti, J., & Kekki, T., & Verho,P.(2018). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability 2019, 11(3), 838,*1-18,

που δεν είναι εξαρχής εμφανείς στην μελέτη των υποδομών, και που όμως μπορούν να αποτελέσουν σημεία τρωτότητας αλλά και λόγω αυτής της τρωτότητας να αναδείξουν εκ των υστέρων αλληλεξαρτήσεις/αλληλοσυσχετίσεις που εξ' αρχής δεν ήταν αντιληπτές[269].

- Μεταβαίνοντας στην θεματική που αφορά στην προστασία των εκάστοτε υποδομών πρέπει αρχικά να επισημανθεί πως μια επαρκής αντιμετώπιση της οποιασδήποτε απειλής για την απρόσκοπτη λειτουργία των υποδομών (disruption) αναδεικνύει σε έναν βαθμό και το ζήτημα μια δικτυοκεντρικής προσέγγισης (network-approach[270]). Καθώς η αλληλεξάρτηση θα αυξάνει την συνεργασία φορέων και προσωπικού που μέχρι πρότινος μπορεί να δρούσαν απομονωμένα, θα αυξάνεται αφενός η ανάγκη για μια αλλαγή στον τρόπο σκέψης των δρώντων αυτών.

Ήτοι, μια στροφή προς έναν πιο δικτυοκεντρικό τρόπο σκέψης που θα κάνει ώστε οι δρώντες να λαμβάνουν υπόψη τα οφέλη της ετοιμότητας (preparedness) ως τμήμα ενός προδραστικού τρόπου σκέψης που θα είναι προσανατολισμένος στην συνεργασία (δικτυοκεντρικός) με άλλους φορείς και θα αποσκοπεί σε μη χειροπιαστά/άμεσα (π.χ. return of investment) οφέλη που εκ πρώτης μπορεί να μην διαφαίνονται (η ετοιμότητα και η προδραστικότητα δεν έχουν εκ πρώτης όψεως οικονομικό όφελος, αλλά η διασφάλιση τους συνάμα διασφαλίζει και την λειτουργικότητα των υποδομών κλπ[271]).

Και αφετέρου θα γίνεται πιο επιτακτική η ανάγκη ο τρόπος σκέψης αυτός να καλλιεργείται στους συμβαλλόμενους δρώντες μέσα σε ένα πλαίσιο ενισχυτικό προς την συνεργασία μεταξύ διαφορετικών φορέων και προς την παραγωγή νέων νοηματοδοτήσεων (γλώσσας, ορολογίας, κουλτούρας στην συνεργασία κλπ) ανάμεσα στους φορείς, έτσι ώστε να διασφαλίζεται η ανθεκτικότητα (resilience) των υποδομών μέσα από την υπερκέραση των παραδεδεγμένων ορίων σκέψης και δράσης, προς μια συνεργασία προσαρμοσμένη στις ανάγκες των αλληλεξαρτώμενων υποδομών[272].

- Ο βασικός στόχος για την απρόσκοπτη λειτουργία των SCAs συνήθως περιγράφεται είτε με τον όρο προστασία (protection) είτε με εκείνον της αντοχής

σ.6.doi: https://doi.org/10.3390/su11030838.https://www.mdpi.com/2071-1050/11/3/838 (τελευταία πρόσβαση 30/1/2022).

[269] Ο.π.,σ.3.

[270] Ο.π.,σ.14.

[271] Ο.π..σ.13.

[272] Ο.π.

(resilience). Ο όρος resilience έχει ερμηνευτικά μια διττή σημασία, αφενός χρησιμοποιείται για να καταδείξει την διαλειτουργικότητα (interoperability) των κρισίμων υποδομών καθώς η ζημία σε μια εξ αυτών μπορεί να επιδράσει αρνητικά σε διεργασίες που διενεργούνται σε έτερες υποδομές. Αφετέρου, η αντοχή μιας υποδομής, πέρα και από την δυνατότητα της να αναδιοργανώνεται και να συνεχίζει την λειτουργία της ακόμα και όταν μια απειλή εναντίον της περατωθεί , σημαίνει επίσης και την δυνατότητα της να ανταπεξέρχεται (εν συνόλω ή εν μέρει) απέναντι σε μη γνωστές ή μη καταγεγραμμένες απειλές ή αδυναμίες εντός εύλογου χρονικού διαστήματος (επί παραδείγματι έναντι «*λανθανουσών τρωτοτήτων*», «*latent vulnerabilities*» ή έναντι της επίδρασης που δυνητικά ασκούν οι «*λανθάνουσες μεταβλητές*», «*latent variables*[273]»).

Έχοντας αναλύσει ορισμένες βασικές πτυχές της εννοιολόγησης περί των κρισίμων υποδομών, παραθέτουμε στην συνέχεια ορισμένα χαρακτηριστικά παραδείγματα τέτοιων υποδομών , ώστε να καταδειχθεί ενδεικτικά το εύρος των εφαρμοσμένων συστημάτων και του διαδικτύου των πραγμάτων αλλά και μεγάλου εύρους των λειτουργιών των τελευταίων, που οι εγκαταστάσεις αυτές περικλείουν εντός των τειχών τους[274] :

- Κυβερνητικές εγκαταστάσεις : αναφορικά με τις κυβερνητικές εγκαταστάσεις αξίζει μεταξύ άλλων να αναφερθούν δύο σημεία. Πρώτον, υπό τον όρο αυτό εννοούνται αφενός οι κτιριακές εγκαταστάσεις και το προσωπικό και αφετέρου τα επιμέρους κυβερνοσυστήματα (cyber systems) που είναι εγκατεστημένα στα κτίρια αυτά (για παράδειγμα CCTV, σημεία ελέγχου εισόδου, αυτοματοποιημένα συστήματα για επιτέλεση διαφόρων λειτουργιών κλπ) που εύλογα παράγουν εκροές όπως έχουμε αναφέρει για τον εν γένει εξοπλισμό σε προηγούμενα κεφάλαια[275].

---

[273] Ο.π.,σ.6.

[274] Οι ενδεικτικές αυτές παραθέσεις προέρχονται σε μεγάλο βαθμό (αν και μόνο ενδεικτικές περιπτώσεις παρατίθενται εδώ, και ο κατάλογος δεν είναι εξαντλητικός) από χ.σ.(χ.χ.). The 16 Sectors of Critical Infrastructure Cybersecurity. *Cipher insights Blog.* https://cipher.com/blog/the-16-sectors-of-critical-infrastructure-cybersecurity/ (τελευταία πρόσβαση 15/1/2022).

[275] χ.σ.(2015). *Government Facilities Sector-Specific Plan an annex to the NIPP 2013.* Washington: Homeland Security GSA,σ.5. Ανακτήθηκε από: https://www.cisa.gov/publication/nipp-ssp-government-facilities-2015 (τελευταία πρόσβαση 6/2/2022).

Δεύτερον, η λειτουργία και το ιδιοκτησιακό καθεστώς των κτιριακών εγκαταστάσεων αναδεικνύουν διάφορες αλληλεξαρτήσεις (interdependencies), καθώς είναι εφικτό για παράδειγμα μια κυβέρνηση είτε να νοικιάζει από έναν ιδιωτικό φορέα είτε να επιτρέπει η ίδια σε τρίτους να αξιοποιούν κτιριακές της εγκαταστάσεις (leasing[276]). Ενδεικτικά οι αλληλεξαρτήσεις που δημιουργούντα δύνανται να αφορούν στο φυσικό/υλικό επίπεδο (physical interdependencies) όπου δύο τουλάχιστον διαφορετικές κτιριακές εγκαταστάσεις χρησιμοποιούν η μια την υπηρεσία που παράγει η άλλη (input-output). Στο επίπεδο της κυβερνοασφάλειας (cyber interdependencies) και εδώ κυρίως εννοούνται οι ανταλλαγές πληροφοριών και η διασύνδεση των εκάστοτε πληροφοριακών συστημάτων των εγκαταστάσεων αυτών[277].

Στο γεωγραφικό επίπεδο (geographical interdependencies) όπου μπορούν να επηρεαστούν εγκαταστάσεις ειδικά αν βρίσκονται σε γεωγραφική εγγύτητα (στις δύο προηγούμενες περιπτώσεις η εγγύτητα δεν είναι αναγκαίο να πληρείται ως προϋπόθεση[278]). Τέλος, στο λογικό επίπεδο (logical interdependencies), όπου εδώ η αλληλεξάρτηση εννοείται ως γενικότερη έννοια για να συμπεριλάβει οποιεσδήποτε περιπτώσεις οι προηγούμενες τρεις εν μπορούν να συλλάβουν (π.χ. insider threat ενδεχομένως[279]). Εύλογα οι αλληλεξαρτήσεις αυτές συντείνουν στην ενίσχυση επιτυχούς εκτέλεσης των SCAs καθώς, μεταξύ άλλων, δύνανται να συνδράμουν τόσο στον πολλαπλασιασμό και την ένταση των εκροών όσο και την δυνατότητα συνδυασμού μεταξύ τους.

- Τομέας της Υγείας: Εν μέρει έχουν συζητηθεί διάφορες πτυχές περί των νοσοκομειακών εγκαταστάσεων και μηχανημάτων, εδώ αρκεί να αναφερθεί ότι εκ των βασικών στοιχείων για την ανάλυση πρέπει να θεωρείται η διαλειτουργικότητα των επιμέρους συστημάτων (interoperability), η αλληλεξάρτηση με άλλους τομείς (π.χ. εγκαταστάσεις ηλεκτρισμού, παροχή νερού, θέρμανσης κλπ), καθώς και η πολυμορφία

[276] Ο.π.

[277] Ο.π.,σ.6.

[278] Ο.π.,σ.7.

[279] Ο.π.

στις δραστηριότητες των εγκαταστάσεων αυτών (ιατρικά μηχανήματα, υπολογιστικά συστήματα, συσκευές ιδιωτών κλπ[280]).

Λαμβάνοντας υπόψη αυτές τις τρεις παραμέτρους, η προστασία τέτοιων υποδομών από SCAs (μεταξύ άλλων) καθίσταται δυσχερής, διότι ένα μέρος της υποδομής του νοσοκομείου φυσιολογικά είναι προσβάσιμο στο ευρύ κοινό (publicly accessible) άρα συνακόλουθα και οι πρόσβαση στις εκροές[281]. Επίσης, οι συγκεκριμένες υποδομές λόγω του ότι χρησιμοποιούν ένα ευρύ φάσμα συσκευών που καθιστούν δύσκολο τον σχεδιασμό αποτελεσματικών αντιμέτρων. Ακόμα, ο τομέας της Υγείας διαθέτει εγκαταστάσεις σε ευρύ εθνικό και υπερεθνικό φάσμα, κάτι που δυσχεραίνει τις καίριες επεμβάσεις και τους εν γένει σχεδιασμούς ιδίως όταν οι επιθέσεις πλευρικού καναλιού είναι ταυτόχρονες ή συνδυαστικές[282].

Τέλος δε, το γεγονός ότι οι υποδομές αυτές (όπως και οι άλλες) προϋποθέτουν εργατικό δυναμικό με μια διαφοροποιημένη στάθμη δεξιοτήτων, με αποτέλεσμα η εκπαίδευση και αντικατάσταση τους σε ότι αφορά (και) τις SCAs να είναι δυσχερείς καθώς εμπλέκονται όπως καταδείχθηκε πολλές μεταβλητές και το πλήρες εύρος για τις επιθέσεις αυτές δεν είναι εύκολο να γίνει αντιληπτό[283].

- Εργοστασιακές Εγκαταστάσεις: δεδομένου του εύρους της αλληλεξάρτησης ανάμεσα σε δευτερογενείς βιομηχανίες (παραγωγές εξαρτημάτων, τμημάτων εξοπλισμών, γραμμές συναρμολόγησης κλπ) οι συγκεκριμένες υποδομές αφενός απειλούνται από διακοπή στην αλυσίδα προμηθειών (supply chain disruption) με αποτέλεσμα να ζημιωθούν και πολλοί άλλοι τομείς βιομηχανικοί ή τριτογενείς (π.χ. χρηματοπιστωτικός τομέας κλπ), και αφετέρου από αδυναμία λειτουργίας σε παγκόσμιο

[280] χ.σ.(2016). *Healthcare and Public Health Sector-Specific Plan.* Washington: Homeland Security ,σ.4. Ανακτήθηκε από: https://www.cisa.gov/publication/nipp-ssp-healthcare-public-health-2015 (τελευταία πρόσβαση 6/2/2022).

[281] Ο.π.,σ.13.

[282] Ο.π.

[283] Ο.π.

επίπεδο καθώς λόγω της παγκοσμιοποίησης οι βιομηχανίες όλο και περισσότερο συνδέουν τις χώρες μεταξύ τους[284].

Οι SCAs μπορούν ενδεχομένως σε ορισμένα σενάρια είτε να λειτουργήσουν επιθετικά καταστρέφοντας την αλυσίδα προμηθειών και την αλληλεξάρτηση (ενδεχομένως δυσχερές σενάριο, αλλά θα άξιζε να τεθεί το ερώτημα αν τέτοιες επιθέσεις θα μπορούσαν να δράσουν αλυσιδωτά, ήτοι ανάμεσα σε πολλές εργοστασιακές μονάδες και όχι μόνο σε μια) είτε να δράσουν στην κατεύθυνση της υποκλοπής πληροφοριών (passive form, για παράδειγμα κλοπή πνευματικής ιδιοκτησίας) μέσα από την μελέτη εκροών[285].

- Οδικά Δίκτυα: πέρα από ορισμένες πτυχές που αναφέρθηκαν και ανωτέρω η κρίσιμη υποδομή των οδικών δικτύων απειλείται μεταξύ άλλων τόσο λόγω παλαιότητας των υποδομών μεταφορών (π.χ. δρόμοι) όσο και λόγω της κλιματικής αλλαγής και των συνεπειών αυτής (π.χ. οι συνέπειες που μπορεί να έχει η άνοδος της στάθμης της θάλασσας για το οδικό δίκτυο πλησίον των ακτών κλπ[286]). Ειδικότερα οι SCAs δύνανται να αποτελέσουν απειλή κυρίως για τα αυτοματοποιημένα οχήματα και τα συστήματα αυτών, καθώς η αλληλεξάρτηση των δικτύων που συνδράμουν στην αυτοματοποίηση προσφέρει απομακρυσμένη πρόσβαση σε πλήθος οχημάτων και χρηστών,

---

[284] Γενικά οι απειλές δεν προέρχονται μόνο από κυβερνοεπιθέσεις, μπορεί να περιλαμβάνουν φυσικές καταστροφές, τρομοκρατία, πολιτικές αναταραχές κλπ, πρβλ. χ.σ.(2015). *Critical Manufacturing Sector-Specific Plan An Annex to the NIPP 2013.* Washington: Homeland Security,σ.5. Ανακτήθηκε από: https://www.cisa.gov/publication/nipp-ssp-critical-manufacturing-2015 (τελευταία πρόσβαση 6/2/2022).

[285] Οι Azriel et al. έχουν αναλύσει μια παρεμφερή πειραματική συνθήκη σχετική με κλοπή πνευματικής ιδιοκτησίας (IP Theft) όπου το πλευρικό κανάλι (scan-based side channel) λειτουργεί αμυντικά (blue team). Στο άρθρο τους προτείνουν την συνδυαστική χρήση συναρτήσεων μπουλιανού τύπου και γραφημάτων (μηχανική μάθηση) ώστε έχοντας μερική γνώση του σχεδιασμού της IP να είναι εφικτό με την χρήση αυτού του scan να λάβει χώρα ένα reverse engineering και η πατέντα να ανακτηθεί πλήρως. Πρβλ. Azriel, L., & Ginosar, R., & Gueron, S., & Mendelson, A.(2017). Using Scan Side Channel to Detect IP Theft. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25, 12,*3268-3280 (1-13), σ.12. https://webee.technion.ac.il/~ran/papers/AzreilTVLSI2017.pdf (τελευταία πρόσβαση 7/2/2022).

[286] χ.σ.(2015). *Transportation Systems Sector-Specific Plan.* Washington: Homeland Security United States Department of Transportation,σ.7. Ανακτήθηκε από: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf (τελευταία πρόσβαση 7/2/2022).

διευκολύνοντας έτσι την ευκολότερη πρόσβαση από πλευράς των επιτιθέμενων[287].

- Διαδίκτυο: Πέρα από την ατομική χρήση του διαδικτύου και την επιρροή που αυτή ασκεί στην καθημερινή ζωή των ανθρώπων, το διαδίκτυο συνδέεται εύλογα με τις κρίσιμες υποδομές και στο σημείο όπου συναντάται με την βιομηχανία και τις ανάγκες αυτής (industrial Internet of Things, IIoT[288]). Αρκετές τρωτότητες έχουν ήδη αναφερθεί στο πρώτο κεφάλαιο της διπλωματικής (είτε έχουν σχέση με τις SCAs είτε όχι), αφορούν ενδεικτικά σε αστοχίες υλικού, λανθασμένες εφαρμογές αλγόριθμων, υψηλή αλληλεξάρτηση μεταξύ των συσκευών IoT, υψηλός βαθμός διαφοροποίησης ανάμεσα στους κατασκευαστές, σχετική ανυπαρξία φιλικής προς τον χρήστη διεπαφής, ανάδυση νέων τεχνολογιών που κάνουν να αναφύονται νέες προκλήσεις ασφαλείας κλπ[289].

Ειδικότερα σε ότι αφορά το IIoT (ως βιομηχανικό σύνολο εδώ), τα ενσωματωμένα συστήματα (ICs) στις βιομηχανίες, παρουσιάζουν αδυναμίες όπως η έλλειψη χαρακτηριστικών ασφαλείας καθώς δεν υφίσταται μια εκτεταμένη δυνατότητα διεπαφής ή ευελιξία στην αναβάθμιση τέτοιων συστημάτων που βασίζονται κυρίως στο υλικό (hardware). Επιπλέον, το κόστος για την έρευνα και δημιουργία ασφαλέστερων συστημάτων και ακόμα και αντιμέτρων θεωρείται κοστοβόρα για τις βιομηχανίες ενώ οι αλλαγές στα εκάστοτε συστήματα συνεπάγονται και υψηλό αρχικό κόστος επένδυσης για τους ιδιοκτήτες και τις κυβερνήσεις. Περαιτέρω, διευκρινίζεται ότι οι συσκευές IoT χαρακτηρίζονται οι ίδιες τόσο από τεχνικές όσο και μη τεχνικές τρωτότητες[290].

Οι πρώτες αφορούν σε αδυναμίες που μπορεί να σχετίζονται με εφαρμογές ή και σε πιο απλές αδυναμίες όπως εκείνες που εμφανίζονται

---

[287] Ο.π.,σ.11.

[288] Simmon, T.(2017). Critical Infrastructure and the Internet of Things. *Global Commission on Internet Governance Paper Series GCIG,46,*1-11,σ.7. https://www.cigionline.org/publications/critical-infrastructure-and-internet-things-0/ (τελευταία πρόσβαση 7/2/2022).

[289] Ο.π.

[290] Ο.π.

σε βασικά πρωτόκολλα του διαδικτύου (TCP,HTTP κλπ) που υφίστανται ακόμα ως λειτουργικά μέρη του διαδικτύου. Οι δεύτερες αφορούν σε ζητήματα ελλιπούς εκπαίδευσης προσωπικού και σε αστοχίες σε ότι αφορά στις διαδικασίες λειτουργίας μιας εργοστασιακής (ή έτερης) μονάδας καθώς και στους κανονισμούς που αφορούν στο προσωπικό (εγχειρίδια ασφαλούς χρήσης κλπ[291]).

- Χρηματοπιστωτικός Τομέας: ως κρίσιμη υποδομή ο χρηματοπιστωτικός τομέας μπορεί να βρεθεί στο επίκεντρο απειλών όπως οι περιβαλλοντικές καταστροφές, οι τρομοκρατικές ενέργειες και εύλογα οι κυβερνοαπειλές[292].

Ο χρηματοπιστωτικός τομέας παρουσιάζει όπως και οι υπόλοιποι έναν υψηλό βαθμό αλληλεξάρτησης με έτερους τομείς, και έπεται ότι πρέπει να υφίσταται αφενός μια καλή κατανόηση των αλληλεξαρτήσεων που δημιουργούνται μεταξύ αυτού του τομέα και του κυβερνοχώρου (cyber dependencies, πλατφόρμες, e-banking, POS κλπ) και αφετέρου ότι πρέπει να δίδεται έμφαση (και) στον έλεγχο των προσώπων που σχετίζονται με τέτοιες αλληλεξαρτώμενες υποδομές (ιδιοκτήτες, υπάλληλοι κλπ) για την πιστοποίηση αυτών των τελευταίων και την πρόσβαση τους σε διαβαθμισμένες πληροφορίες (π.χ. στις ΗΠΑ υπάρχει πρόβλεψη, μέσω του EO 13636 παρ.9, για ένα πρόγραμμα clearance για άτομα από τον ιδιωτικό τομέα, DHS Private Sector Clearance Program[293]).

- Δίκτυα Τηλεπικοινωνιών: Για την συγκεκριμένη υποδομή και σε σχέση με τις SCAs ισχύει ότι παρατέθηκε στο δεύτερο κεφάλαιο στην συζήτηση για τις ταξινομήσεις των επιθέσεων πλευρικού καναλιού. Οι τηλεπικοινωνίες παρουσιάζουν μεγάλο βαθμό αλληλεξάρτησης και μπορούν να απειληθούν από διάφορους παράγοντες (όπως φυσικές καταστροφές, διακοπές στην αλυσίδα προμηθειών, πολιτικές αναταραχές

[291] Ο.π.

[292] χ.σ.(2015). *Financial Services Sector-Specific Plan 2015.* Washington: The Department of Treasury, US Department of Homeland Security,σ.8.Ανακτήθηκε από: https://www.cisa.gov/publication/nipp-ssp-financial-services-2015 (τελευταία πρόσβαση 7/2/2022).

[293] Ο.π.,σ.9.

κλπ[294]). Σε ότι αφορά στις κυβερνοαπειλές (SCAs κλπ) εδώ μεταξύ άλλων καταγράφονται οι απειλές έναντι του τρίπτυχου CIA , οι εκ των ένδον απειλές, το DDoD, καθώς οι απειλές έναντι του μη χρησιμοποιούμενου χώρου στις βάσεις δεδομένων (white space frequency database κλπ[295]). Για ένα σχετικό παράδειγμα συνδυασμού SCA και τηλεπικοινωνιών παραπέμπουμε στο δεύτερο κεφάλαιο (οπτικές επιθέσεις) και στην υποσημείωση υπ' αριθμόν 130.

- Αμυντική Βιομηχανία: επί παραδείγματι σε αυτή την κρίσιμη υποδομή, όπως και σε πολλές άλλες φυσικά, τα assets που πρέπει να προστατευθούν αφορούν μεταξύ άλλων και στην προστασία του προσωπικού σε συνθήκες πανδημίας (π.χ. COVID-19 κλπ). Αυτή η πτυχή αναδεικνύει ζητήματα αντιθέσεων και ανάμεσα σε ορισμούς οργανισμών και σε ότι αφορά στην συνεργασία ανάμεσα σε δημόσιους φορείς (π.χ. Υπουργείο Αμύνης κλπ) και κατά περίπτωση ιδιώτες παρόχους υπηρεσιών (contractors[296]).
- Τομείς Παραγωγής Ενέργειας: αξίζει να τονιστεί πως παρά το ότι η αλληλεξάρτηση διατηρείται και εδώ όπως και στα υπόλοιπα παραδείγματα, εντούτοις οι κλάδοι παραγωγής ενέργειας (όπως και ο βιομηχανικός κλάδος εν γένει) χαρακτηρίζονται από μια μεγαλύτερη ίσως ετερογένεια σε σχέση και με άλλες υποδομές, επομένως τα αντίμετρα αλλά και η έννοια της απειλής και του ρίσκου εδώ ενδέχεται να διαφοροποιηθούν σημαντικά. Οι απειλές παραμένουν οι ίδιες όπως και πριν, ήτοι φυσικές καταστροφές, τρομοκρατία, πολιτικές αναταραχές κλπ[297].

---

[294] χ.σ.(2015). *Communications Sector-Specific Plan An Annex to the NIPP 2013.* Washington: Homeland Security,σ.7.Ανακτήθηκε από:https://www.cisa.gov/publication/nipp-ssp-communications-2015(τελευταία πρόσβαση 7/2/2022).

[295] Ο.π.

[296] χ.σ.(2020). The DIB as critical infrastructure during COVID-19. *NDIA.* https://www.ndia.org/policy/recent-posts/2020/6/11/the-dib-as-critical-infrastructure-during-covid19 (τελευταία πρόσβαση 5/2/2022).

[297] χ.σ.(2015). *Energy Sector-Specific Plan.* Washington: Homeland Security,σ.3-6. Ανακτήθηκε από: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf (τελευταία πρόσβαση 7/2/2022).

Γι' αυτούς τους λόγους τονίζεται ιδιαίτερα και ένα σημείο που αναφέρθηκε ανωτέρω, ήτοι η ανάγκη για συνεργασία, επικοινωνία ανάμεσα στους εταίρους, και ο διαμοιρασμός καλών πρακτικών μεταξύ άλλων για την αντιμετώπιση των εκάστοτε προκλήσεων[298] (η πολυμορφία των SCAs επίσης επιβεβαιώνει κάτι τέτοιο, καθώς έχει δειχθεί πως η ίδια υποκατηγορία ή επίθεση μπορεί να εκτελεστεί με διαφορετικό τρόπο ανάλογα το περιβάλλον ή την συσκευή).

- Δίκτυα Υδροδοτήσεως: εντός του εύρους των διαχειριστικών εργασιών των σχετικών με το πόσιμο ή μη ύδωρ η κρίσιμη υποδομή των δικτύων υδροδοτήσεως αξιοποιεί μεταξύ άλλων και μια σειρά από αισθητήρες όπως επίσης και αυτοματοποιημένων συστημάτων (SCADA κλπ[299]).

Οι εγκαταστάσεις δεν περιλαμβάνουν μόνο αυτά τα συστήματα, αλλά όπως έχει καταδειχθεί στα δύο προηγούμενα κεφάλαια οι SCAs μπορούν να χρησιμοποιήσουν ως vectors τέτοια συστήματα και να εκμεταλλευτούν αν μη τι άλλο δύο καίρια σημεία, αφενός το ότι είναι δυσχερής η επικοινωνία με τα SCADA από την πλευρά του ανθρώπινου παράγοντα (π.χ. management), και αφετέρου ότι υφίστανται περιπτώσεις όπου τέτοια συστήματα επηρεάζονται είτε από ελλείψεις πόρων είτε λόγω της παλαιότητας τους, με αποτέλεσμα να μην υπάρχει ομοιομορφία στην στρατηγική και τα αντίμετρα που πρέπει να εφαρμοστούν[300][301].

- Τομείς Επισιτισμού και γεωργικής παραγωγής εν γένει: σε γενικές γραμμές και σε ότι αφορά την κυβερνοασφάλεια και τις SCAs ο εν λόγω τομέας έχει αρκετά κοινά με τα δίκτυα υδροδοτήσεως. Ήτοι, η ύπαρξη αρκετών συστημάτων SCADA και ICs (εκτός από την επιρροή

---

[298] Ο.π.,σ.4.

[299] χ.σ.(2015). *Water and Wastewater Systems Sector-Specific Plan.* Washington: Homeland Security, United States Environmental Protection Agency,σ.7-8. Ανακτήθηκε από: https://www.cisa.gov/publication/nipp-ssp-water-2015 (τελευταία πρόσβαση 7/2/2022).

[300] Ο.π.,σ.10.

[301] Για τον κύκλο ζωής των SCADA και τα συνδεόμενα με αυτόν ζητήματα, πρβλ. Gupta, M.S.(χ.χ.). Need for SCADA Migration Plan Increases with New Functionality. *ARC Advisory Group.* https://www.arcweb.com/industry-best-practices/need-scada-migration-plan-increases-new-functionality (τελευταία πρόσβαση 7/2/2022).

των φυσικών φαινομένων κλπ) που οδηγεί σε ανάδειξη ζητημάτων τρωτότητας λόγω απουσίας διεπαφής, δυσχέρειας στην προστασία και αναβάθμιση, και επίσης λόγω της επαυξημένης δυνατότητας απομακρυσμένου ελέγχου[302] (επομένως ισχύει ότι και σε σχέση με το προηγούμενο σημείο για τις SCAs κλπ).

Ολοκληρώνοντας την εν λόγω υπό-ενότητα θα επιχειρήσουμε να παραθέσουμε ορισμένα σημεία, τα οποία δυνητικά θα μπορούσαν να παρουσιάσουν μια ορισμένη συμβατότητα ανάμεσα στα στοιχεία που συνθέτουν το εννοιολογικό πλαίσιο των υποδομών αφενός, και σε ορισμένα από εκείνα που διαπιστώθηκε πως ενυπάρχουν στην αντίστοιχη προσπάθεια περί του ορισμού και των ταξινομήσεων των SCAs. Η καταγραφή αυτών των συμπτώσεων ενδεχομένως να συνδράμει στην εναργέστερη κατανόηση της σχέσης ανάμεσα στις SCAs (πιο συγκεκριμένα τα assets τους που αφορούν σε internet of Things) και τις CIs, στο για ποιους λόγους επομένως οι SCAs συνιστούν μια απειλή τέτοιου μεγέθους που θα ταίριαζε να μελετηθεί από κοινού με τις υποδομές. Ενδεικτικά οι τρεις (3) αυτοί λόγοι έχουν ως ακολούθως :

- ✓ Αρχικά, τόσο οι κρίσιμες υποδομές όσο και οι επιθέσεις πλευρικού καναλιού αντιμετωπίζουν δυσχέρειες σε ότι αφορά στις διαδικασίες ορισμού και ταξινόμησης είτε των επιθέσεων είτε των assets που αποτελούν κρίσιμες υποδομές. Οι δυσχέρειες αυτές εν γένει οφείλονται σε παράγοντες όπως ενδιάμεσες μεταβλητές που δεν λαμβάνονται συχνά υπόψη, η σχετικότητα των επιμέρους στοιχείων των ορισμών (π.χ. vector-victim κλπ), καθώς επίσης και η αξιοποίηση διαφορετικών ομάδων κριτηρίων τόσο για τον χαρακτηρισμό των κρίσιμων υποδομών όσο και για τις ταξινομήσεις των SCAs. Όλα αυτά συντείνουν στο να είναι οι ορισμοί και οι εκάστοτε ταξινομήσεις λιγότερο προσανατολισμένες στην δράση (actionable) και συνάμα περισσότερο ταυτολογικές, ενώ ταυτόχρονα γίνεται πιο δυσχερές να αναδειχθεί το πλήρες εύρος ορισμών και ταξινομήσεων ώστε να δοθεί έτσι μια πλήρης εποπτεία της συσχέτισης των CIs και των SCAs.
- ✓ Δεύτερον, οι κρίσιμες υποδομές και οι επιθέσεις πλευρικού καναλιού παρουσιάζουν αμφότερες μια ευρεία ετερογένεια. Από αυτό έπεται ότι οι παράγοντες που

[302] χ.σ.(2015). *Food and Agriculture Sector-Specific Plan.* Washington: Food and Drug Administration, USDA, Homeland Security,σ.6-7.Ανακτήθηκε από:https://www.cisa.gov/publication/nipp-ssp-food-ag-2015 (τελευταία πρόσβαση 7/2/2022).

δυσχεραίνουν συχνά την προστασία των υποδομών στον αντίποδα μπορούν κάλλιστε να διευκολύνουν την επιτυχή διενέργεια μιας ή διαφόρων επιθέσεων πλευρικού καναλιού. Οι κρίσιμες υποδομές όπως έχει δειχθεί από την ανωτέρω ανάλυση διακρίνονται:

- Από ένα μεγάλο εύρος από vectors,
- από ένα ανθρώπινο δυναμικό διαφοροποιημένων ειδικοτήτων και γνωστικών πεδίων,
- από ένα υψηλό επίπεδο μιας διαφοροποιημένης αλληλεξάρτησης,
- από ένα υψηλό επίπεδο διαλειτουργικότητας (interoperability),
- από εξοπλισμό διαφορετικών προδιαγραφών (παλαιότητα, πολυπλοκότητα κλπ),
- και επίσης από μια διαφοροποιημένη κλίμακα λειτουργίας αυτών (εθνικές, διασυνοριακές και παγκόσμιες υποδομές, με αναφορά και στην συνεργατική τους αλληλεξάρτηση εδώ).

Υπό αυτό το πρίσμα οι SCAs αξίζει να μελετηθούν από κοινού με τις κρίσιμες υποδομές (IoT devices, embedded systems) διότι οι ίδιες διακρίνονται:

- από την ευχέρεια με την οποία μπορούν να λειτουργούν συνδυαστικά και να αξιοποιούν τις εκροές σε συνδυασμούς, κάτι που σημαίνει πως μπορούν εύλογα να εκμεταλλευτούν την ανάγκη των υποδομών για διαλειτουργικότητα και αλληλεξάρτηση,
- από την σχετική ευχέρεια με την οποία μπορούν αξιοποιηθούν απέναντι σε τεχνολογίες διαφορετικών προδιαγραφών, χρόνου κατασκευής και λειτουργίας, ειδικά όταν υποστηρίζονται από αλγορίθμους μηχανικής μαθήσεως για την ανάλυση των εκροών (επί παραδείγματι οι SCAs μπορούν να λειτουργήσουν και απέναντι σε ενσωματωμένα συστήματα, κυκλώματα, υπολογιστές, αισθητήρες, λογισμικό, IoTs κλπ, και οι κρίσιμες υποδομές μαζί και το προσωπικό που εργάζεται εκεί έχουν τέτοιες συσκευές στις εγκαταστάσεις τους).
- Τέλος δε, από την δυνατότητα τους να ευεργετούνται από τον περιβάλλοντα χώρο και από την ύπαρξη και κίνηση του ανθρώπινου δυναμικού μέσα σε αυτόν. Οι κρίσιμες υποδομές χωροθετούνται σε διαφορετικά περιβάλλοντα και οι άνθρωποι που εργάζονται εντός αυτών

είτε φέρουν αντικείμενα που ευνοούν την παραγωγή εκροών ή την πρόσκρουση/αντανάκλαση αυτών πάνω στα αντικείμενα αυτά (π.χ. γυαλιά, ρούχα, αξεσουάρ κλπ) είτε οι ίδιοι με κάποιον τρόπο μπορούν να λειτουργήσουν ως κομιστές εκροών (π.χ. ομιλία, ανθρώπινες σκιές κλπ). Από την άλλη η χωροθέτηση των υποδομών, είτε εντός του φυσικού χώρου είτε περισσότερο με την έννοια της αλληλουχίας που τα πληροφοριακά συστήματα επιτρέπουν, ίσως οδηγήσει σε αύξηση είτε των εκροών (ευλόγως) είτε σε αύξηση της ευχέρειας στον συνδυασμό διαφορετικών SCAs μέσα από την αύξηση του συνδυασμού εκροών.

✓ Τρίτον, η ενασχόληση πολλών διαφορετικών φορέων στο ευρύτερο πλαίσιο της λειτουργίας των κρισίμων υποδομών, καθώς επίσης και η διαφοροποίηση που παρατηρείται εντός του ανθρωπίνου δυναμικού που απασχολείται σε αυτές, κάνει ώστε να αναφύονται κενά σε ότι αφορά την προστασία τους από τις SCAs (μεταξύ άλλων). Αυτό εύλογα συμβαίνει είτε γιατί οι εμπλεκόμενοι προέρχονται από διαφορετικά γνωστικά πεδία και άρα δεν γνωρίζουν σε βάθος τα ζητήματα τα σχετικά με την κυβερνοασφάλεια και τις κυβερνοαπειλές και επομένως η μεταξύ τους επικοινωνία δυσχεραίνεται εξαιτίας (και) αυτού του παράγοντα. Είτε διότι η ανάγκη τους να συνεργαστούν (εξαιτίας της αλληλεξάρτησης των υποδομών) δεν υποβοηθάτε συχνά από στεγανά στον τρόπο σκέψης, καθώς η συνεργασία τους απαιτεί (και) την παραγωγή νοηματοδοτήσεων και τρόπων σκέψης ενταγμένων σε ένα πλαίσιο συνεργασίας και αλληλεξάρτησης.

Επομένως, οι SCAs (και όχι μόνο αυτές φυσικά) είτε δεν θα αντιμετωπίζονται αποτελεσματικά λόγω κενών στις γνώσεις του προσωπικού (απουσία πρόληψης, αδυναμίες στον σχεδιασμό αντιμέτρων), είτε δεν θα αντιμετωπίζονται/προλαμβάνονται λόγω απουσίας ενός τρόπου σκέψης που να είναι τόσο ευέλικτος και πολύπλευρος όσο και εκείνες. Επί παραδείγματι, αν ο στόχος είναι το continuity δηλαδή η συνέχιση λειτουργίας μιας υποδομής κάτω από οποιεσδήποτε συνθήκες, τότε ο τρόπος σκέψης αυτός δεν φαίνεται να λαμβάνει υπόψη το ότι πολλές SCAs κατά κόρον λειτουργούν παθητικά υποκλέπτοντας πληροφορίες ενώ αφήνουν το σύστημα άθικτο, και πως αυτό συμβαίνει εξαιτίας του ίδιου του τρόπου λειτουργίας της υποδομής και όχι λόγω κάποιας αστοχίας απαραίτητα.

Από την άλλη, η γνώση απλά και μόνο του παθητικού (passive) τρόπου λειτουργίας των SCAs, μπορεί να οδηγήσει σε παράλειψη του τρόπου σκέψης που αφορά στο πως οι SCAs δύνανται να λειτουργήσουν επιθετικά (offensively), καταστρέφοντας μόνες ή σε συνδυασμό με έτερες επιθέσεις όλη την υποδομή ή τμήμα αυτής (που δεν διαφέρει πολύ λόγω του υψηλού βαθμού αλληλεξάρτησης κλπ). Τέτοιες μονομέρειες στον τρόπο σκέψης ίσως να μην συλλάβουν εγκαίρως , για παράδειγμα, είτε το πώς συνδυάζονται οι εκροές διαφορετικών υποδομών είτε το πώς μη αμιγώς τεχνικοί παράγοντες (άνθρωποι, περιβάλλοντας χώρος) δύνανται να συνδράμουν μια επίθεση πλευρικού καναλιού κατά μιας ή πολλών υποδομών.

Υπό-ενότητα 3.2: Επιθέσεις πλευρικού καναλιού στο Διαδίκτυο των Πραγμάτων (IoT) των κρίσιμων υποδομών, βιβλιογραφική ανασκόπηση

Στο δεύτερο μέρος με το οποίο και κλείνει το παρών κεφάλαιο η στόχευση αφορά στον συγκερασμό υποδομών και επιθέσεων, ήτοι στην από κοινού μελέτη τους, αφού ως τώρα είχαν μελετηθεί στο παρών πόνημα μονάχα κατά μονάς. Η συγκεκριμένη στόχευση αναλύεται περαιτέρω στα κάτωθι δύο σημεία, που εύλογα αλληλεξαρτώνται, ήτοι:

- Πρώτον, θα επιχειρηθεί η διερεύνηση ενός τμήματος της υπάρχουσας βιβλιογραφίας, ώστε να καταστεί εφικτό να καταδειχθούν πρακτικά οι τρόποι (ορά μέθοδοι/μεθοδολογία) με τους οποίους οι SCAs δύνανται να απειλήσουν τις κρίσιμες υποδομές.
- Δεύτερον, θα επιχειρηθεί η καταγραφή διαφόρων πτυχών που δεν εμφανίζουν άμεση συνάφεια ανάμεσα σε SCAs-CIs, και που όμως μπορούν έστω έμμεσα να συσχετιστούν με τις απειλές κατά κρίσιμων υποδομών τις σχετιζόμενες με SCAs.

Αρχικά, πρέπει να παρατηρηθεί πως σε ότι αφορά στο τμήμα της βιβλιογραφίας που μελετήθηκε οι SCAs μόνο σπάνια μελετήθηκαν (είτε σε πειραματική συνθήκη είτε υπό μια καθαρά θεωρητική έννοια) υπό το πρίσμα όσον αφορούν τις κρίσιμες υποδομές. Αυτό είναι ένα κενό το οποίο παρατηρείται σε ένα τμήμα της βιβλιογραφίας και το οποίο διασταυρώνεται με ένα έτερο κενό που αφορά στο τι ακριβώς μελετάτε όταν οι SCAs λαμβάνονται υπόψη από κοινού μετά των κρίσιμων υποδομών.

Σε αυτή την δεύτερη περίπτωση παρατηρείται ένα κενό (το δεύτερο κατά σειρά) που έχει να κάνει με το ποιες από τις υποδομές μελετιούνται σε σχέση με τις SCAs όταν μια τέτοια μελέτη λαμβάνει χώρα στο πλαίσιο κάποιας σχετικής αρθρογραφίας. Εν άλλοις λόγοις, τα δύο αυτά κενά συντείνουν στο ότι η ανάλυση τείνει να γίνει κάπως μονόπλευρη, διότι μια εκάστη άρθρων δεν μελετούν τις SCAs σε επίπεδο που να αντιστοιχεί σε εκείνο των κρίσιμων υποδομών (στην ολότητα τους δηλαδή), παρά κυρίως επικεντρώνουν σε μια κατά τι μικρότερη κλίμακα ανάλυσης (π.χ. πειραματικές συνθήκες με χρήση μεμονωμένων κυκλωμάτων, επεξεργαστών, αλγορίθμων κρυπτογράφησης, συσκευών όπως κινητά όπως δείξαμε στα δύο προηγούμενα κεφάλαια κλπ).

Εν γένει, αν θα έπρεπε να κατηγοριοποιηθούν οι βιβλιογραφικές αναφορές που έχουν εντοπιστεί στο πλαίσιο εκπόνησης της ανά χείρας διπλωματικής, τότε η ομαδοποίηση θα είχε ενδεχομένως ως ακολούθως (υπενθυμίζεται ότι η έμφαση στα κατωτέρω παραδείγματα δίδεται στο επίπεδο λειτουργίας ενσωματωμένων συστημάτων & συσκευών IoT, επιθέσεις επί των οποίων καταγράφονται ποικιλοτρόπως κατωτέρω στα παραδείγματα που ακολουθούν):

- SCAs & Υγειονομικός τομέας (ιατρικός και μη εξοπλισμός κλπ),
- SCAs & Αυτοκινούμενα οχήματα/Οδικά δίκτυα,
- SCAs & Διαδίκτυο,
- SCAs & Ενσωματωμένα Συστήματα (βιομηχανικός εξοπλισμός κλπ),
- SCAs & Αγροτικός τομέας,
- SCAs & Χρηματοπιστωτικός τομέας.

Η έμφαση δίνεται στην βιβλιογραφική ανασκόπηση για να καταδειχθεί σε σχέση με ποιες από εκείνες τις μεταβλητές, που αναφέρθηκαν στο δεύτερο κεφάλαιο όταν ο λόγος γινόταν για τις ταξινομήσεις (υλικό, λογισμικό, vectors, υποκατηγορία SCA κλπ), εξετάζονται από κοινού οι επιθέσεις πλευρικού καναλιού.

<u>SCAs & Υγειονομικός Τομέας:</u>

Ο συγκεκριμένος συνδυασμός αφορά σε πτυχές (με βάση την βιβλιογραφία που μελετήθηκε ωσαύτως) όπως η χρήση των ιατρικών συσκευών/μηχανημάτων, η αξιοποίηση εξοπλισμού γραφείου για ιατρική/διοικητική χρήση, επίσης η συσχέτιση μεταξύ επιθέσεων πλευρικού καναλιού αφενός και ατομικών συσκευών προς ιατρική χρήση αφετέρου, και ακόμα στην χρήση ατομικών συσκευών ασθενών/προσωπικού/επισκεπτών που δεν έχει κατ' ανάγκη

συνάφεια με τον ιατρικό τομέα (ή έστω έχει έμμεση σχέση) αλλά που η συνάφεια αυτή αφορά στην γεωγραφική εγγύτητα με την κρίσιμη (υγειονομική) υποδομή. Τονίζεται και εδώ όπως και στην προηγούμενη ενότητα πως το προσωπικό των υγειονομικών υποδομών προέρχεται από ένα εξαιρετικά διαφοροποιημένο υπόβαθρο, και πως η πολλαπλότητα των εκροών (leakages) θα μπορούσε να είναι γόνιμο έδαφος για συνδυαστικές επιθέσεις δυνητικά.

Η πλειοψηφία των επιθέσεων είναι κατά κύριο λόγο παθητικής φύσεως (passive forms) και κατ' εξαίρεση επιθετικής (offensive forms) , έπεται ότι οι δεύτερες είναι πιο δύσκολο να εκτελεστούν. Καθώς η λογική της παρούσας υπό-ενότητας είναι να ταξινομηθούν οι SCAs με βάσει τις εκάστοτε υποδομές, έπεται από αυτό ότι η παρακολούθηση του εγχειρήματος θα καθίσταται ευκολότερη αν για την κάθε υποδομή μελετηθούν χωριστά τα εκάστοτε assets (ή vectors) που συναποτελούν την κάθε ξεχωριστή υποδομή (η βιβλιογραφία που έχει μελετηθεί για τους σκοπούς της ανά χείρας διπλωματικής ευνοεί τον συγκεκριμένο τρόπο ταξινόμησης και συνεπακόλουθα ανάλυσης). Με βάσει την συγκεκριμένη ταξινομητική λογική επομένως παρατίθενται οι ακόλουθες διαπιστώσεις ως εξής:

- Ιατρικός εξοπλισμός (medical equipment/machinery): πρόκειται για την κύρια κατηγορία των assets στην οποία επικεντρώνει η απειλή των επιθέσεων πλευρικού καναλιού. Οι μεθοδολογίες των εκάστοτε SCAs εμφανίζουν μια σχετική ποικιλομορφία. Σε ότι αφορά στον εξοπλισμό στόχο, τουλάχιστον στην συγκεκριμένη υποκατηγορία, αυτός αποτελείται κατά κύριο λόγο, αν όχι εξ' ολοκλήρου, από ενσωματωμένα συστήματα (embedded systems) που αφορούν σε ιατρικές λειτουργίες. Δυνάμεθα να διακρίνουμε δύο κατηγορίες εφαρμοσμένων συστημάτων, αφενός αυτά που αποτελούνται μόνο από το υλικό (hardware), και αφετέρου εκείνα που διαθέτουν κάποιου είδους λειτουργικό σύστημα (OS), το οποίο όμως δεν είναι τόσο εύκολα προσβάσιμο όσο στους συμβατικούς υπολογιστές (για παράδειγμα τα pharmaceutical compounders[303]). Εν γένει, ορισμένα προβλήματα που αναφύονται (και εν μέρει έχουν αναφερθεί και σε προηγούμενες σελίδες) αφορούν σε απουσία παρέμβασης από την πλευρά των κατασκευαστών, σε αδυναμία παρέμβασης από την πλευρά των χρηστών (απουσία

[303] Clark, S.S., & Ransford, B., & Rahmati, A., & Guineau, S., & Sorber, J., & Fu, K., & Xu, W.(2013). *WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices.* Paper presented at the 2013 USENIX Workshop on Health Information Technologies (HealthTech '13), Washington DC, USA, August 12, 1-11, σ.1,3. https://www.usenix.org/conference/healthtech13/workshop-program/presentation/clark (τελευταία πρόσβαση 15/10/2021).

διεπαφής κλπ), και επίσης στην απουσία φιλικών προς τον χρήστη χαρακτηριστικών σε ότι αφορά την εμπορική χρήση τέτοιων μηχανημάτων[304]. Αποτέλεσμα όλων των παραπάνω είναι τόσο η αδυναμία εγκατάστασης λογισμικού για την προστασία τέτοιων συστημάτων, όσο και η αδυναμία των NIDS να εντοπίσουν ζητήματα ασφαλείας στα συστήματα αυτά[305].

Χαρακτηριστικό παράδειγμα αποτελεί η πειραματική συνθήκη των Clark et al. όπου με την συνδρομή της μηχανικής μάθησης κατασκεύασαν ένα malware (*WattsUpDoc*) για να λαμβάνουν μετρήσεις σχετικά με την κατανάλωση ενός ενσωματωμένου συστήματος . Η εν λόγω πειραματική συνθήκη καταδεικνύει πως σε ενσωματωμένα συστήματα με ορισμένο αριθμό λειτουργιών (ή και μονολειτουργικά ακόμα) η κατανάλωση ενέργειας παρουσιάζει ομοιομορφία που είναι σχετικά εύκολο να μετρηθεί[306].

- Εξατομικευμένες ιατρικές συσκευές (implantable medical devices etc): Πιο επιθετικές μορφές SCAs δύνανται να περιλαμβάνουν σε ότι αφορά τις ατομικές ιατρικές συσκευές (εμφυτεύματα κλπ) απομύζηση της μπαταρίας μιας ιατρικής συσκευής ή απορρύθμιση της δοσολογίας ορισμένων συσκευών (ή έτερων ρυθμίσεων τους) με στόχο να επηρεαστούν οι καρδιακοί παλμοί ή τα επίπεδα ινσουλίνης. Μεταξύ άλλων αυτό που εδώ διακυβεύεται είναι αφενός η υποκλοπή ευαίσθητων και προσωπικών δεδομένων, και αφετέρου η δυνατότητα πρόσβασης σε κάποιας μορφής θεραπεία δυνάμει[307]. Τονίζοντας εκ νέου την σχετικότητα των ορισμών σε ότι αφορά τις SCAs, μπορούμε ίσως να διαπιστώσουμε πως στις περιπτώσεις αυτής της , δυνάμει, υποκατηγορίας φαίνεται εφικτό η έννοια vector να μην είναι αποκλειστικά η συσκευή, αλλά και ο τύπος ασθενείας τον οποίο να είναι σε θέση να εκμεταλλευτεί ο επιτιθέμενος[308].

---

[304] Ο.π.,σ.2.

[305] Ο.π.,σ.1.

[306] Ο.π.,σ.2.

[307] Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices,15:6,*403-406,σ.404.https://www.tandfonline.com/doi/pdf/10.1080/17434440.2018.1483235?needAccess=true (τελευταία πρόσβαση 12/10/2021).

[308]Ο.π.

Επιπροσθέτως, οι ιατρικές αυτές συσκευές παρουσιάζουν ορισμένα ακόμα βασικά σημεία τρωτότητας. Εν πρώτοις, υφίσταται το ζήτημα της ευελιξίας στον σχεδιασμό της επίθεσης και της δυνατότητος εκπόνησης κάποιας συνδυαστικής επιθέσεως πλευρικού καναλιού (συνδυασμός ξεχωριστών επιθέσεων ή και συνδυασμός εκροών δυνητικά). Αυτό διότι αν η συσκευή τίθεται σε λειτουργία και εκτός της νοσοκομειακής μονάδος τότε ο επιτιθέμενος θα ηδύνατο να εκτελέσει την SCA απομακρυσμένα (none-invasive), ενώ αν η συσκευή τελεί υπό την προϋπόθεση της δικτυοκεντρικής λειτουργίας (networked Medical Device) τότε ο επιτιθέμενος δυνητικά έχει πρόσβαση και στο δίκτυο του νοσοκομείου αν μπορεί να έχει πρόσβαση στην συσκευή, κι έτσι να εκδηλώσει ενδεχόμενα και συνδυαστική επίθεση (π.χ. αν υπάρχει και κάποια εκ των ένδον απειλή, ήτοι insider threat) ή να συνδυάσει διαφορετικές εκροές[309].

Εν δευτέροις, η εκδήλωση μιας SCA επιθετικής φύσεως (offensive form) χαρακτηρίζεται ως εξαιρετικά δυσχερής και μια τέτοια επιτυχής παραλλαγή (σε μη πειραματική συνθήκη) ενδεχομένως να μην έχει καταγραφεί από την βιβλιογραφία τουλάχιστον σε ότι αφορά τις ατομικές ιατρικές συσκευές. Η προβληματική όμως αναφύεται και εδώ, αφενός μια τέτοια ενδεχόμενη επίθεση φαντάζει εξαιρετικά δύσκολη λόγω της πολυπλοκότητας και των γνώσεων από διαφορετικά επιστημονικά πεδία (ιατρική, πληροφορική κλπ) που θα πρέπει να κομίζει ο επιτιθέμενος θέτοντας όμως και το ζήτημα της πολυεπιστημονικότητας για το προσωπικό που θα επιφορτιστεί με την προστασία του νοσοκομείου[310].

Αφετέρου, οι περισσότερες από αυτές τις συσκευές παρουσιάζουν αδυναμίες αντίστοιχες με τα ενσωματωμένα συστήματα, κυρίως ως προς το ότι και οι δύο διακρίνονται από απουσία μιας φιλικής προς τον χρήστη διεπαφής, και επίσης ως προς το ότι δεν υφίσταται κάποιος αποτελεσματικός τρόπος για την καταγραφή των logs σε αυτές τις συσκευές , με αποτέλεσμα να καθίστατο κάπως παρακινδυνευμένο να λεχθεί αν έχουν υπάρξει επιτυχείς ή μη τέτοιες επιθέσεις καθώς και ο έλεγχος περί αυτών είναι ελλιπείς υπό μια έννοια[311].

- Εξοπλισμός γραφείου (μη ιατρικός κατά βάση, π.χ. printers κλπ): εδώ η αναφορά γίνεται σε σχέση με μηχανήματα που αξιοποιούνται κυρίως στο διοικητικό

[309] Ο.π.,σ.403.

[310] Ο.π.,σ.404.

[311] Ο.π.

σκέλος ή από τους ιατρούς για χρήση σχετική με την ιατρική πληροφορική, επομένως εδώ από κοινού μελετάτε η συσκευή και ο ανθρώπινος παράγοντας (υπό την έννοια της αντιστροφής στην σχέση αιτίου-αιτιατού που αναφέρθηκε και ανωτέρω, και με ότι αυτό συνεπάγεται για ελλιπή γνώση σε θέματα κυβερνοασφάλειας και επιθέσεων πλευρικού καναλιού, όπως αναφέρθηκαν και σε προηγούμενες ενότητες). Οι Backes et al. διερεύνησαν σε πειραματική συνθήκη την αξιοποίηση ενός αλγορίθμου μηχανικής μάθησης για την ανασυγκρότηση κειμένου έχοντας ως βάση την ηχητική καταγραφή από έναν πεπαλαιωμένο εκτυπωτή μελάνης που οι ιατροί χρησιμοποιούν για την εκτύπωση συνταγών[312].

Με την αξιοποίηση της μηχανικής μάθησης επιχείρησαν να πετύχουν την αναπαραγωγή του κειμένου μέσα από την έμφαση στην ανάλυση υψηλών συχνοτήτων, την ομοιόμορφη κατανομή τους στο εύρος συχνοτήτων και επίσης μέσα από την εφαρμογή αλγορίθμων εξομάλυνσης για την μείωση των θορύβων, των προερχόμενων από το εξωτερικό περιβάλλον που δύνανται να επηρεάσουν την απόδοση του αλγορίθμου[313]. Σε ότι αφορά τον αλγόριθμο μηχανικής μάθησης αυτός εκπαιδεύεται για αναγνώριση λέξεων και όχι γραμμάτων, ενώ παράλληλα το μοντέλο Hidden Markov για βελτίωση του αλγορίθμου σε ότι αφορά στην αναγνώριση φωνής, ώστε ο τελευταίος να μπορεί ευκολότερα να αναγνωρίσει τις λέξεις που αποτυπώνει στο χαρτί ο εκτυπωτής και οι οποίες στην προκειμένη περίπτωση είναι στην αγγλική[314].

SCAs & Αυτοκινούμενα οχήματα/οδικά δίκτυα:

Και στην συγκεκριμένη υποπερίπτωση ισχύει μια πολυμέρεια αντίστοιχη με εκείνη της προηγούμενης υποπερίπτωσης. Στο τμήμα της βιβλιογραφίας που μελετήθηκε οι SCAs αναλύονταν στην σχέση τους με τα τρία ακόλουθα στοιχεία , ήτοι τους αλγορίθμους κρυπτογράφησης, τα ίδια τα αυτόνομα οχήματα, και επίσης σε ότι αφορά την πλατφόρμα υλικού

[312] Bakes, M., & Durmuth ,M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security Symposium,DC,USA,August,11-13,pp.1-16,σ.1. https://www.researchgate.net/publication/221260462_Acoustic_Side-Channel_Attacks_on_Printers(τελευταία πρόσβαση 10/10/2021).

[313] Ο.π.,σ.2.

[314] Ο.π.

που αξιοποιεί ένα αυτόνομο όχημα (περισσότερο στην περίπτωση αυτή γίνεται αναφορά σε έναν συνδυασμό λογισμικού/υλικού για την εκτέλεση της επιθέσεως).

- Αλγόριθμοι κρυπτογράφησης: αντικειμενικός στόχος μιας SCA είναι να υπονομεύσει την ασφάλεια της λειτουργίας των αυτοκινούμενων οχημάτων μέσα από την απόσπαση του μυστικού κλειδιού από πλευράς επιτιθέμενου. Αναλυτικότερα, οι Jain et al. στο επιστημονικό του άρθρο διερευνούν την πιθανότητα υποκλοπής του μυστικού κλειδιού μέσα από επίθεση πλευρικού καναλιού (πρόκειται όπως θα δειχθεί για παραδείγματα υποκατηγοριών όπως οι SCAs ανάλυσης ισχύος και οι επιθέσεις χρονομέτρησης) την οποία ο επιτιθέμενος διενεργεί έναντι του CAN bus (Controller Area Network[315]). Στην συνθήκη που πραγματεύονται οι εν λόγω συγγραφείς ο δυνάμει επιτιθέμενος χρησιμοποιεί ένα ταλαντοσκόπιο (oscilloscope, ή εναλλακτικά με την συνδυαστική χρήση ενός A/D controller και ενός έτερου CAN bus για προσομοίωση μιας template attack[316]). Περαιτέρω ο επιτιθέμενος αξιοποιεί την επίθεση πλευρικού καναλιού μόνο με παθητικό τρόπο (passive) και λαμβάνει μετρήσεις από συνολικά 16 nodes.

  Αντικειμενικός στόχος ου επιτιθέμενου είναι λαμβάνοντας μετρήσεις από το CAN bus να καταφέρει να κλέψει το μυστικό κλειδί που δημιουργεί το πρωτόκολλο κρυπτογραφίας pnS-TwoParty[317].

  Το μυστικό κλειδί εύλογα αποσπάται όταν ο επιτιθέμενος , μέσω των μετρήσεων, αποκτήσει επαρκή γνώση (στο δυαδικό σύστημα 0/1) περί του ποιο node είναι εκείνο που μεταδίδει το κυρίαρχο bit κάθε φορά (ήτοι το bit0 το οποίο αφορά στην εντολή για την κίνηση του οχήματος, το bit1 επομένως δεν πραγματοποιεί κάποια ενέργεια[318]). Ο επιτιθέμενος θα συνεχίσει να καταγράφει τις μετρήσεις μέχρι να έχει βρει όλα τα κυρίαρχα bits (σε κάθε ζεύγος nodes που επικοινωνούν, αν το ένα bit είναι μηδέν, εύλογα το άλλο node θα έχει το bit1 κλπ), και κατ' επέκταση θα έχει επιτυχώς αποσπάσει το κλειδί[319](σε αυτό το πρωτόκολλο τα ECUs που επικοινωνούν είναι πάντα δύο, οπότε ο επιτιθέμενος διευκολύνεται στο ότι δεν χρειάζεται να αναγνωρίσει τα nodes καθαυτά,

---

[315] Jain, S., & Wang, Q., & Arafin, M.T., & Guajardo, J.(2018). *Probing Attacks on Physical Layer Key Agreement for Automotive Controller Area Networks.* Paper presented at the ESCAR Europe 2017. Aachen, Deutschland. November,7-8,1-12,σ.1. https://arxiv.org/pdf/1810.07305.pdf (τελευταία πρόσβαση 16/9/2021).

[316] Ο.π.,σ.3.

[317] Ο.π.,σ.4.

[318] Ο.π.

[319] Ο.π.

παρά μόνο να είναι σε θέση κάθε φορά να ξεχωρίζει το dominant από το recessive bit για να βρει το κλειδί[320]).

Το συγκεκριμένο είδος δικτύου (CAN bus) δύναται όπως επιτρέψει τον εντοπισμό των διαφορετικών bits που ανταλλάσσουν τα nodes, με την διενέργεια μιας SCA ή και με έτερες επιθέσεις, καθότι διαθέτει τα ακόλουθα τρία χαρακτηριστικά:

- Πρώτον, υπάρχουν χαρακτηριστικά σταθερών καταστάσεων (steady state characteristics), τα οποία οφείλονται στο ότι ένα bus CAN μπορεί να λειτουργήσει ως πλατφόρμα για διαφορετικές συσκευές. Εύλογα, οι τελευταίες αυτές ενέχουν διαφορετικά μοτίβα κατανάλωσης ενέργειας, και άρα είναι πιο εύκολο αφού συνυπάρχουν, και αφού τα μοντέλα αυτά διατηρούνται, για τον επιτιθέμενο που διενεργεί μια SCA να παρατηρήσει τις εκάστοτε διαφορές μεταξύ τους, και αυτές να αποτελέσουν έτσι μια μορφή (μη ηθελημένης) διαρροής[321].

  Επίσης, η διαφορά στα κυκλώματα των οδηγών (driver circuits), αυτό συμβαίνει διότι οι διαφορετικοί κατασκευαστές των εκάστοτε κυκλωμάτων δημιουργούν αυτά τα τελευταία με πολύ διαφορετικά πρότυπα, και άρα εκείνα ενέχουν διαφορετική κατανάλωση (voltage), με αποτέλεσμα ο επιτιθέμενος να επωφελείται και από αυτή την δυνάμει μη ηθελημένη διαρροή[322]. Το ίδιο ισχύσει και σε ότι αφορά στην κατανάλωση ισχύος κατά την διαλειτουργικότητα μεταξύ των nodes σε ένα bus CAN[323]. Τέλος δε, υφίσταται και μια ακόμα διαφοροποίηση σε ότι αφορά στην φυσική χωροθέτηση (physical location) των τμημάτων που συγκροτούν το δίκτυο (π.χ. στην διαφορετική θέση των πομποδεκτών, μέγεθος καλωδίων κλπ), και η οποία οδηγεί στην δημιουργία αντιστάσεων, που με την σειρά της παράγει μετρήσιμες διαφοροποιήσεις για τον επιτιθέμενο.

- Δεύτερον, μεταβατικά χαρακτηριστικά (transient characteristics), που αφορούν στην ποιότητα μετάδοσης του σήματος που αλλοιώνεται καθώς μεταφέρεται από το ένα node στο άλλο, αυτές τις διαφοροποιήσεις μπορεί ο επιτιθέμενος να τις εκμεταλλευτεί για να εντοπίσει το node που μεταδίδει το bit,

[320] Ο.π.,σ.6.

[321] Ο.π..σ.4.

[322] Ο.π.

[323] Ο.π.,σ.5.

καθώς τυπικά υφίσταται καθυστέρηση όταν μεταδίδεται το sample bit ώστε το δίκτυο να βεβαιωθεί πως έχουν ελαχιστοποιηθεί οι όποιες αλλοιώσεις[324].

- Τρίτον, χαρακτηριστικά χρονικής φύσεως (timing characteristics), που αφορούν στις χρονικές καθυστερήσεις που προκύπτουν από την χρήση καλωδίων που χρησιμοποιούνται στην συνδεσμολογία του bus CAN (twisted pair[325]). Οι χρονοκαθυστερήσεις προκύπτουν εξαιτίας δύο παραγόντων εδώ, αφενός από την καθυστέρηση στον ρυθμό εξάπλωσης που βιώνουν ο αποστολέας και ο παρατηρητής, και αφετέρου λόγω του συγχρονισμού ανάμεσα στους αποστολείς (transceivers). Αυτές τις διαφορές μπορεί να παρατηρήσει ο επιτιθέμενος για να λάβει ακριβείς μετρήσεις[326].

- Ειδικότερα στην περίπτωση του πρωτοκόλλου pns-TwoParty εντός του δικτύου bus CAN (PnS-CAN, στην περίπτωση της πειραματικής συνθήκης των δύο συγγραφέων) υφίστανται δύο χαρακτηριστικά τα οποία δύναται να αξιοποιήσει ο επιτιθέμενος κατά την εκτέλεση μιας SCA. Πρώτον, ο επιτιθέμενος διευκολύνεται στην χρονομέτρηση από το γεγονός ότι στην αρχική φάση της επικοινωνίας τα δύο (μόνο) nodes μεταδίδουν πληροφορίες ακολουθιακά, ήτοι το πρώτο μεταδίδει το header ενώ το δεύτερο συγχρονίζεται σε σχέση με το πρώτο. Έτσι, αφού υπάρχει μόνο ένα node που μεταδίδει κάθε φορά (στην αρχική φάση, initializing) τότε ο επιτιθέμενος διευκολύνεται στο να μετρήσει επακριβώς τον χρόνο συντονισμού του δεύτερου node[327].

Δεύτερον, υφίσταται μια εξάρτηση ανάμεσα στα τυχαία bits και σε εκείνα που είναι αντεστραμμένα (inverted bits) κατά την διαδικασία ανταλλαγής της πληροφορίας, και επομένως ο επιτιθέμενος μπορεί να την αξιοποιήσει για να μαντέψει σωστά ορισμένα εξ αυτών των bits κατά την διενέργεια ακολουθιακών μεταδόσεων στο δίκτυο[328].

- Αυτόνομα οχήματα καθαυτά (autonomous vehicles): οι Luo et al. Επί παραδείγματι παρουσίασαν στο άρθρο τους μια περίπτωση όπου μέσω μιας cache SCA ο επιτιθέμενος θα μπορούσε να λάβει πληροφορίες για την φυσική

[324] Ο.π.

[325] Ο.π.

[326] Ο.π.

[327] Ο.π.,σ.7.

[328] Ο.π.

κατάσταση του οχήματος (physical state) παρατηρώντας τις συσχετίσεις ανάμεσα στην κατάσταση που βρίσκεται κάθε φορά το όχημα και τα μοτίβα πρόσβασης στην μνήμη cache από πλευράς του λογισμικού που ελέγχει το εν λόγω όχημα[329]. Οι συγγραφείς αξιοποιούν τον αλγόριθμο μηχανικής μάθησης random forest για την πρόβλεψη των κινήσεων και της τοποθεσίας του οχήματος και σε ότι αφορά τις cache SCAs αξιοποιούν την περίπτωση της επιθέσεως Prime + Probe[330]. Ιδιαίτερο ενδιαφέρον παρουσιάζει το ότι η εν λόγω επίθεση δεν σκοπεύει ενάντια σε κάποια εφαρμογή αλγορίθμου κρυπτογράφησης όπως έτερες περιπτώσεις στην βιβλιογραφία, αλλά αντίθετα με την χρήση μιας τέτοιας SCA, μικροαρχιτεκτονικού τύπου (microarchitectural), εξάγονται πληροφορίες για την πορεία του αυτοκινήτου χωρίς προηγούμενη γνώση παραμέτρων (όπως συμβαίνει σε άλλες πειραματικές συνθήκες) η εμβέλεια του σήματος που φτάνει στο όχημα[331].

- Πλατφόρμα υλικού του αυτόνομου οχήματος (platform): γενικά παρατηρείται η τάση μείωσης του κόστους στην κατασκευή των VANETs μέσα (και) από τον διαμοιρασμό πόρων του υλικού από πλευράς διαφόρων εφαρμογών λογισμικού, ήτοι η μη ύπαρξη ή μη σωστή εφαρμογή της τεχνικής του sandboxing[332]. Δεύτερον, το λογισμικό που συνήθως χρησιμοποιείται για τα VANETs (π.χ. Jackal UGV) τυγχάνει ευρείας εφαρμογή, κάτι που ενδεχομένως συνεπάγεται ευκολότερο προσπορισμό γνώσεως από πλευράς του επιτιθέμενου[333] (π.χ. μέσω ηθελημένης εκροής όπως η δημοσίευση στοιχείων για το εν λόγω λογισμικό κλπ). Επιπροσθέτως, σε ότι αφορά στα VANETs παρατηρείται επίσης η ροπή προς μια ανοικτού τύπου αρχιτεκτονική στην υλοποίηση του λογισμικού προς εφαρμογή στα αυτοκινούμενα οχήματα αυτά, όπως για παράδειγμα η δυνατότητα να μπορεί ο οδηγός του οχήματος να κατεβάζει και να εγκαθιστά εφαρμογές τρίτων (infotainment κλπ). Αυτό έχει ως

[329] Luo, M., & Myers, A.C., & Suh, G.E.(2020). *Stealthy Tracking of Autonomous Vehicles with Cache Side Channels.* Paper presented at the 29th USENIX Security Symposium. Virtual Event, August, 12-14,1-18(859-876),σ.1.sec20-luo.pdf (usenix.org) (Τελευταία πρόσβαση 14/12/2021).

[330] Ο.π.,σ.2.

[331] Ο.π.,σ.15.

[332] Ο.π.,σ.14.

[333] Ο.π.

αποτέλεσμα, δυνητικά να διευρύνετε η επιφάνεια επιθέσεως (όπως έχει αναφερθεί και ανωτέρω σε έτερο κεφάλαιο[334]).

SCAs & Το Διαδίκτυο (IoT συσκευές):

Πρόκειται για την μεγαλύτερη, ενδεχομένως, κατηγορία στην βιβλιογραφική ανασκόπηση της ανά χείρας διπλωματικής εργασίας εν σχέση με τις επιθέσεις πλευρικού καναλιού. Η έκταση της συγκεκριμένης θεματικής έγκειται κυρίως σε δύο στοιχεία, αφενός στην σημασία του διαδικτύου για τις κρίσιμες υποδομές και την κοινωνία εν συνόλω, και αφετέρου στο γεγονός ότι οι διάφορες συσκευές που αξιοποιούν έστω και εν μέρει την λειτουργία του διαδικτύου μπορούν κάλλιστα να αποτελούν τμήμα της εργασιακής καθημερινότητας εντός μιας κρίσιμης υποδομής (αλλά και εκτός αυτής, όπως οι αρκετά συχνές τη σήμερον περιπτώσεις τηλεργασίας κλπ), λαμβάνοντας υπόψη και περιστάσεις κατά τις οποίες οι συσκευές αυτές δεν χρησιμοποιούνται απαραίτητα για σκοπούς σχετικούς με την καθαυτό λειτουργία της εκάστοτε κρίσιμης υποδομής(π.χ. κατά τις ώρες περάτωσης ενός εργασιακού διαλείμματος[335][336]).

[334] Ο.π.

[335] Ενδεχομένως η χρήση αυτών να διενεργείται και παρά τις περί του αντιθέτου συστάσεις που λαμβάνουν χώρα εντός μιας κρίσιμης υποδομής και για την προστασία αυτών από ,ηθελημένα και μη, λάθη του ανθρώπινου παράγοντος.

[336] Εδώ επανερχόμαστε εκ των πραγμάτων και σε μια θεματική στην οποία έγινε αναφορά ανωτέρω, οι ποικιλομορφία των συσκευών IoT, αναδεικνύει πέρα από την τεχνική, και την μη τεχνική πλευρά στις επιθέσεις πλευρικού καναλιού. Εδώ θα μπορούσε να γίνει εκ νέου αναφορά στην εργασιακή κουλτούρα εντός του οργανισμού, ακόμα και σε πρακτικές και συνήθειες του ανθρώπινου δυναμικού, που θα μπορούσαν να εμμένουν ακόμα και αν ο κανονισμός μιας κρίσιμης υποδομής ρητά ορίζει άλλως. Εδώ εν συντομία θα μπορούσαν να καταγραφούν περιπτώσεις συνηθειών όπως η τοποθέτηση του κινητού πλησίον του υπολογιστή εργασίας, περιπτώσεις χωροθέτησης αντικειμένων και ύπαρξης εξοπλισμού (για παράδειγμα το υλικό πάνω στο οποίο βρίσκεται ένας υπολογιστής μπορεί να διευκολύνει ή να δυσχεραίνει αντίστοιχα την πρόσληψη μιας εκροής) που μπορούν δυνάμει να διευκολύνουν έναν επιτιθέμενο, με κάποια γνώση αυτών των παραμέτρων. Ενδεικτικά ορά και, Marquardt, P., & Verma, A., & Carter, H., Traynor, P.(2011). *(sp) iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers.* Paper presented at the proceedings of the 18th ACM Conference on Computer and Communications Security, CSS 2011. Chicago, Illinois, USA. October, 17-21,2011,σ.9-10. DOI:10.1145/2046707.2046771.(sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers | Request PDF (researchgate.net) (τελευταία πρόσβαση 05/01/2022).

Δοθέντων των δύο ως άνω σημείων η συγκεκριμένη υποκατηγορία απειλών έναντι της συγκεκριμένης υποδομής μπορεί να διακριθεί, για το τμήμα της βιβλιογραφίας που μελετήθηκε, περαιτέρω σε τρεις υποομάδες ως ακολούθως:

- Εν πρώτοις, η υποομάδα απειλών που αφορά στην στόχευση και τη συνακόλουθη παραβίαση αλγορίθμων κρυπτογραφίας που αξιοποιούν οι συσκευές IoT. Πρόκειται εύλογα για το τμήμα εκείνο της αρθρογραφίας που απαντάται ενδεχομένως συχνότερα στην διεθνή βιβλιογραφία και αφορά συνήθως περιπτώσεις μελέτης σχετικές με την υποκατηγορία SCA την σχετική με επιθέσεις ανάλυσης ισχύος (π.χ. DPA κλπ).
- Εν δευτέροις, η υποομάδα η σχετική με τις απειλές που προκύπτουν από την διασύνδεση των συσκευών IoT. Ειδικότερα, η σύνδεση τους με έτερο υλικό (hardware) όπως οι βάσεις φόρτισης επί παραδείγματι. Και επίσης, οι απειλές που προκύπτουν από την ύπαρξη/χρήση αισθητήρων στις IoT συσκευές (π.χ. εκείνων που φέρουν τα smartphones) για έτερες συσκευές υλικού (π.χ. σκληροί δίσκοι).
- Εν τρίτοις, η υποομάδα απειλών που απορρέουν από τον περιβάλλοντα χώρο εντός του οποίου υφίστανται και λειτουργούν οι εκάστοτε IoT συσκευές. Υπό μια έννοια, πρόκειται για την αντιστροφή της προηγούμενης περίπτωσης, καθώς εδώ εννοούνται οι εκροές που προέρχονται όχι από την IoT συσκευή αλλά οι εκροές που προέρχονται από έτερα αντικείμενα στον περιβάλλοντα χώρο και μπορούν να αποτελέσουν το μέσο για την εκτέλεση μιας SCA, ενώ στην προηγούμενη παράγραφο η IoT συσκευή είναι το μέσο για την εκτέλεση της αυτής επιθέσεως με την εκροή να μεταφέρει την επίθεση προς έτερο στόχο.

Εν γένει, μπορεί να λεχθεί πως σε ότι αφορά στην σχέση των κρίσιμων υποδομών και των συσκευών IoT δύνανται όπως αναδειχθούν ορισμένες αντιθέσεις που κάνουν ώστε οι συσκευές αυτές να αποτελούν δυνάμει στόχο των επιθέσεων πλευρικού καναλιού.

Αφενός, η χρήση των συσκευών χαρακτηρίζεται από μικρή σχετικά κατανάλωση πόρων εν σχέση με τους πόρους που απαιτούν οι κρίσιμες υποδομές, άρα και ο σχεδιασμός αντιμέτρων ασφαλείας εύλογα κινείται σε διαφορετικά επίπεδα για τις δύο αυτές οντότητες[337]. Αφετέρου, η

[337]Gunathilake, N.A., & Al Dubai, A., & Buchanan, W.J., & Lo, O.(2020). *Electromagnetic Analysis of an Ultra-Lightweight Cipher:PRESENT*. Paper presented at the 10th International Conference on Information Technology Convergence and Services(ITCSE 2021). Syndey, Australia. June, 26-27,(185-205),σ.200. Format guide for AIRCC (arxiv.org) (τελευταία πρόσβαση 17/5/2022).

διαφορά στην υπολογιστική ισχύ ανάμεσα σε κρίσιμες υποδομές και συσκευές IoT έρχεται σε αντίθεση και με το μέγεθος των δεδομένων που οι δύο τους καλούνται να επεξεργαστούν.

Τούτου δοθέντος, δύναται να λεχθεί πως οι αλγόριθμοι κρυπτογράφησης (και γενικά η αρχιτεκτονική ασφαλείας αυτών των συσκευών) έχουν μικρότερη ισχύ εν σχέση με εκείνους των άλλων υπολογιστικών συστημάτων εντός των κρίσιμων υποδομών (επί παραδείγματι μικρότερο μέγεθος κλειδιού, αντίστοιχα μικρότερο μέγεθος του κάθε block δεδομένων, όπως και λιγότεροι γύροι για την κρυπτογράφηση των δεδομένων αυτών[338]).

Σταχυολογώντας περαιτέρω τα ευρήματα της βιβλιογραφίας που συλλέχθηκε και μελετήθηκε, και που όμως δεν συναρτά το δίπολο SCAs-IoT με την ανάλυση των συνεπειών για τις κρίσιμες υποδομές ευθέως με αποτέλεσμα το εγχείρημα σύνδεσης ανάμεσα στα δύο στοιχεία να καθίσταται δυσχερές, οδηγούμαστε στην διατύπωση των ακόλουθων παρατηρήσεων :

- Σε ότι αφορά την πρώτη υποομάδα απειλών, χαρακτηριστικά παραδείγματα εδώ αποτελούν οι εκάστοτε επιθέσεις ανάλυσης ισχύος, οι ηλεκτρομαγνητικές επιθέσεις, οι επιθέσεις χρονομέτρησης και ούτω καθεξής. Πρέπει να σημειωθεί πως αν και οι κρυπταλγόριθμοι που χρησιμοποιούνται σε lightweight συσκευές εν γένει θεωρούνται ως πιο αδύναμοι έναντι εκείνων που χρησιμοποιούνται σε συσκευές μεγαλύτερης υπολογιστικής ισχύος, εντούτοις η θεώρηση αυτή δεν επιβεβαιώνεται στην ολότητα της πάντα[339]. Εν γένει, η αρχιτεκτονική των IoT συσκευών προσφέρει εύφορο έδαφος στις επιθέσεις πλευρικού καναλιού, καθόσον οι συσκευές αυτές έχουν χαμηλότερης ισχύος επεξεργαστές και οι επιθέσεις αυτές έναντι των κρυπταλγόριθμων τους τοποθετούνται εγγύτερα στο επίπεδο της μνήμης CPU[340].

Εδώ αρκεί ενδεικτικά να αναφερθούν τρία παραδείγματα για να καταδειχθούν οι επιμέρους πτυχές της απειλής των SCAs στην συγκεκριμένη υποομάδα. Πρώτον, το παράδειγμα της πρόσβασης του επιτιθέμενου σε φακέλους αρχείων του συστήματος android που δεν απαιτούν προηγούμενη εξουσιοδότηση (privileges), ώστε με την διενέργεια μιας SCA

---

[338] Ο.π.,σ.185.

[339] Ορά επί παραδείγματι τα ευρήματα του ακόλουθου άρθρου, Heuser, A., & Picek, S., & Guilley, S., & Mentens, N.(2017). Side-Channel Analysis of Lightweight Chipers: Does Lightweight Equal Easy ? *Lecture Notes in Computer Science, 10155:*91-104,σ.12. DOI:10.1007/978-3-319-62024-4_7. (PDF) Side-Channel Analysis of Lightweight Ciphers: Does Lightweight Equal Easy? (researchgate.net) (τελευταία πρόσβαση 20/5/2022).

[340] Πρβλ. Jha, A.(2020). IoT Security-Part 19 (101-Introduction to Side Channel Attacks(SCA)). *Payatu.* IoT Security - Part 19 (101 - Introduction to Side Channel Attacks (SCA)) (payatu.com) (τελευταία πρόσβαση 20/5/2022).

(ενδεχομένως και υποβοηθούμενης από κάποιο malware που θα έχει προηγουμένως εγκατασταθεί στην κινητή συσκευή) ο επιτιθέμενος να αποσπάσει πληροφορίες σχετικές με τις προτιμήσεις του χρήστη (π.χ. ποιες ιστοσελίδες επισκέπτεται, εδώ κυρίως γίνεται λόγος για software-based SCA χωρίς φυσική πρόσβαση σε συσκευή κλπ).

Οι Jana και Shmatikov σε μια πειραματική συνθήκη αξιοποίησαν τον φάκελο /proc/<pid>/statm για να εντοπίσουν το μέγεθος της εφαρμογής που λειτουργεί σε μια συσκευή (μέσω της pid), και κατόπιν δημιουργώντας attack signatures μελετούν την σχέση ανάμεσα στην εφαρμογή που λειτουργεί (π.χ. ένας φυλλομετρητής) και στις αλλαγές στην κατανάλωση μνήμης, ώστε με την χρήση του δείκτη Jaccard (Jaccard index) να μελετήσουν τα αποτυπώματα στην μνήμη, και να είναι σε θέση να βρουν ποιες ιστοσελίδες επισκέφτηκε ο χρήστης[341].

Στο δεύτερο παράδειγμα, που εδώ αφορά στους κρυπταλγόριθμους σε κινητές συσκευές (lightweight devices κλπ) και την πιθανότητα διενέργειας μιας SCA κατά αυτών, οι Selvam et al. μελετούν την περίπτωση μιας SCA κατά των αλγορίθμων PRINCE και RECTANGLE[342]. Καθώς οι αλγόριθμοι κρυπτογράφησης τείνουν να είναι λιγότερο ισχυροί σε lightweight συσκευές, οι συγγραφείς αξιοποιούν μια επίθεση πλευρικού καναλιού κατηγορίας διαφορικής ανάλυσης ισχύος (DPA) για να ελέγξουν την ασφάλεια των ως άνω αλγόριθμων[343]. Για τον αλγόριθμο PRINCE η DPA κατέδειξε ότι τα peaks του εν λόγω αλγόριθμου ομοιάζουν αρκετά ως προς το αποτύπωμα της ισχύος τους, και κατ' επέκταση αν ο επιτιθέμενος καταφέρει να εντοπίσει το σημαντικότερο bit (τα δύο bits των nibble στοιχείων σε κάθε στήλη αρκούν κατά τους συγγραφείς για να αποκαλύψουν ολόκληρο το κλειδί μεγέθους 64 bits) σε μια δωδεκάδα

[341] θα μπορούσε μια τέτοια συνθήκη να είναι πιθανή σε περιπτώσεις που ένας υπάλληλος χρησιμοποιεί των φυλλομετρητή σε εταιρικό κινητό android για να εισέλθει για παράδειγμα στην ιστοσελίδα ή το intranet της κρίσιμης υποδομής. Ορά σχετικά με αυτή την συνθήκη (που δεν λαμβάνει όμως υπόψη της την περίπτωση της απειλής των SCAs κατά κρίσιμων υποδομών), Alqazzaz, A., & Alrashdi, I., & Alharthi, R., & Aloufi, E., & Zohdy, M.A.(2018).*An Insight into Android Sid-Channel Attacks*. Paper presented at the 2018 International Conference on Computational Science and Computational Intelligence (CSCI). Tangerang, Indonesia. September 07-08, 2018, 776-780,σ. 778-779. DOI: 10.1109/CSCI46756.2018.00156.An Insight into Android Side-Channel Attacks | IEEE Conference Publication | IEEE Xplore (τελευταία πρόσβαση 24/11/2021).

[342] Selvam, R., & Shanmugam, D., & Annadurai, S.(2015). *Side Channel Attacks: Vulnerability Analysis of PRINCE and RECTANGLE using DPA.* Paper presented at the Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. Singapore, Republic of Singapore. 14 March- 14 April, 2015, 1-15,σ.1. [PDF] Side Channel Attacks: Vulnerability Analysis of PRINCE and RECTANGLE using DPA | Semantic Scholar (τελευταία πρόσβαση 12/11/2021).

[343] Ο.π.

αυτών (12-bit) τότε με αυτό το κλειδί μπορεί με αρκετά καλή στατιστική πιθανότητα να μαντέψει και τα υπόλοιπα bits[344].

Για τον αλγόριθμο RECTANGLE η DPA καταδεικνύει ότι η SCA αυτή ακολουθεί την λογική της κατάτμησης των bits του κλειδιού με αποτέλεσμα η πολυπλοκότητα εύρεσης των σωστών δυαδικών ψηφίων να βαίνει μειούμενη, έτσι με την DPA πραγματοποιείται η σύγκριση μιας υποθετικής κατανάλωσης ισχύος ως προς την πραγματική κατανάλωση ισχύος με στόχο να εντοπιστεί η ενδιάμεση υποθετική τιμή (intermediate hypothetical value) και πολύ κοντά σε αυτή θα ευρίσκεται και η ορθή, πραγματική, τιμή για το κλειδί στο peak της κατανάλωσης ισχύος[345].

Το τρίτο παράδειγμα αφορά στο έργο των Spreitzer et al. όπου μεταξύ άλλων αναφέρεται η περίπτωση της εισαγωγής fault injection διαμέσου power ή clock glitching. Σε αυτή την περίπτωση, που όμως απαιτεί και κάποια τροποποίηση του υλικού επί της κινητής συσκευής για να καταστεί εφικτή και άρα είναι δυσκολότερη ίσως στην εφαρμογή και μάλλον απαιτεί την ύπαρξη κάποιας εκ των έσω απειλής (insider κλπ) με κατάλληλες γνώσεις, η δυνατότητα του επιτιθέμενου να αυξομειώσει την τάση στην τροφοδοσία ρεύματος της συσκευής κάνει ώστε να παρεισφρήσει ένα fault injection στην συσκευή (π.χ. android) και με τον τρόπο αυτό να μπορούν να υπερκεραστούν οδηγίες προς τα τμήματα της συσκευής ή να αλλοιωθούν καταλλήλως ώστε να έχει ο επιτιθέμενος πρόσβαση στις πληροφορίες που θέλει (CPU κλπ[346]).

Εν παρόδω αναφέρουμε ακόμα και μια ενδιάμεση περίπτωση, αυτή της diferential fault injection SCA (*DfAs*), η οποία και ενσωματώνει στοιχεία που προσομοιάζουν στις template/microarchitectural επιθέσεις για να προσβάλλει αλγορίθμους (επομένως και εκείνους που προστατεύουν συσκευές IoT). Η εν λόγω παραλλαγή λειτουργεί σε ένα συγκριτικό πλαίσιο,

---

[344] Ο.π.,σ.9.

[345] Ο.π.,σ.10,12-13.

[346]Παραδείγματα αντίστοιχης λογικής (όχι πάντα για συσκευές android και όχι σε σχέση με κρίσιμες υποδομές καθαυτές) σε ότι αφορά τις συγκεκριμένες SCAs ενδεικτικά αναφέρονται σε άρθρα των O' Flynn για fault injection που θα παρακάμπτει οδηγίες του συστήματος, των Ordas et al. για μια ηλεκτρομαγνητική fault injection που αξιοποιείται ενάντια στον αλγόριθμο AES ενός επεξεργαστή ARM (πρόκειται για εφαρμογή του AES σε υλικό), και των Riviere et al. που επίσης χρησιμοποίησαν μια ηλεκτρομαγνητική fault injection για να υπερκεράσουν οδηγίες σε έναν ARM επεξεργαστή (αξίζει να σημειωθεί πως οι συγκεκριμένοι επεξεργαστές βρίσκουν σχετικά ευρεία εφαρμογή σε κινητές συσκευές οπότε είναι σχετικά αυτά τα παραδείγματα με την παρούσα υπό-ενότητα), για την αρθρογραφία αυτή ορά σχετικά το άρθρο, Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangrad, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,* 20,1,465-488 (1-24),σ.9. DOI:10.1109/COMST.2017.2779824.[1611.03748] Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices (arxiv.org) (τελευταία πρόσβαση 16/9/2021).

καθώς ο επιτιθέμενος παρατηρεί την εκτέλεση του αλγόριθμου (π.χ. AES) κατά την συνθήκη όπου υφίσταται η παρεμβολή ενός fault, και επίσης και κατά την συνθήκη εκείνη που ο αλγόριθμος λειτουργεί κανονικά. Στόχος του επιτιθέμενου είναι να συγκρίνει κατόπιν τις δύο αυτές λειτουργικές καταστάσεις και να εξάγει συμπεράσματα για το ποιες χρήσιμες πληροφορίες μπορεί (μέσω της σύγκρισης) να αποκαλυφθούν[347].

- Σε ότι αφορά στην δεύτερη, τι τάξει, υποομάδα εδώ η συσκευή IoT καταφανώς λειτουργεί σαν μέσο για την εκτέλεση ή την επαύξηση της εμβέλειας μιας SCA. Εν γένει, οι απειλές σε αυτή την κατηγοριοποίηση προϋποθέτουν αφενός την εκμετάλλευση των κενών ασφαλείας στην αρχιτεκτονική των φορητών συσκευών (π.χ. android κινητά κλπ) και αφετέρου την εγγύτητα τους με άλλες συσκευές υλικού (π.χ. H/Y, laptop κλπ). Επί παραδείγματι, οι Biedermann, Katzenbeiser και Szefer, εξετάζουν σε άρθρο τους μια πειραματική συνθήκη όπου η SCA η οποία και θα αξιοποιεί τους αισθητήρες μαγνητικού πεδίου (Magnet Field Sensors) των κινητών android, μέσω εγκατάστασης σε αυτών ενός malware, ώστε να λαμβάνει μέσω της επίθεσης αυτής πληροφορίες από την λειτουργία των σκληρών δίσκων παρακείμενων υπολογιστών[348]. Έχοντας πρόσβαση στις μετρήσεις από τον συγκεκριμένο αισθητήρα ο επιτιθέμενος, μεταξύ άλλων, μπορεί να αντλήσει πληροφορίες για το ποια εικονική μηχανή τρέχει σε ποιόν σκληρό δίσκο, ποιος server φιλοξενεί μια συγκεκριμένη ιστοσελίδα, καθώς επίσης και ποιοι φάκελοι μπορεί να έχουν προσωρινά στην κρυφή μνήμη (cached files[349]).

Η λογική πίσω από την συγκεκριμένη SCA βασίζεται σε πολλαπλές μετρήσεις, όπου το κινητό τηλέφωνο χρησιμεύει για παράδειγμα στη λήψη αρχείων από έναν διακομιστή, ώστε μέσα από τις μετρήσεις των μαγνητικών πεδίων του τελευταίου, να καταστεί εμφανές αν τα τμήματα των δεδομένων αντιστοιχούν σε ποιόν από τους διακομιστές αυτούς, με αποτέλεσμα να μπορεί

---

[347] Πρβλ. Potestad-Ordonez, F.E., & Tena-Sanchez, E., & Acosta-Jimenez, A.J., & Jimenez-Fernandez, C.J., & Chaves, R.(2022). Hardware Countermeasures Benchmarking against Fault Attacks. *Applied Sciences*, 2022, 12(5), 2443, 1-20, σ.5. doi:https://doi.org/10.3390/app12052443. Applied Sciences | Free Full-Text | Hardware Countermeasures Benchmarking against Fault Attacks (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

[348] Biedermann, S., & Katzenbeisser, S., & Szefer, J.(2015). *Hard Drive Side-Channel Attacks using Smartphone Magnetic Field Sensors.* Paper presented at FC 2015: Financial Cryptography and Data Security, Lecture Notes in Computer Science(), vol.8975.San Juan, Puerto Rico, January 30, 2015,σ.1.DOI:https://doi.org/10.1007/978-3-662-47854-7_30. [PDF] Hard Drive Side-Channel Attacks Using Smartphone Magnetic Field Sensors | Semantic Scholar (τελευταία πρόσβαση 24/06/2022).

[349] Ο.π.,σ.6-7.

να προσδιοριστεί σε ποιόν από όλους αυτούς βρίσκεται , επί παραδείγματι, ένας φάκελος ή μια ιστοσελίδα κλπ[350]. Περαιτέρω, υφίσταται και η περίπτωση των La Cour et al που εντός πειραματικής συνθήκης μελέτησαν την περίπτωση διενέργειας SCA (πρόκειται για ανάλυση ισχύος, power SCA) κατά την φάση ασύρματης (wireless) φορτίσεως κινητών συσκευών για την άντληση πληροφοριών σχετικά με τις ιστοσελίδες που ο χρήστης επισκέπτεται κατά την διαδικασία της φόρτισης[351], εύλογα οι κρίσιμες υποδομές μπορεί να διαθέτουν σημεία φόρτισης και μια τέτοια επίθεση να καταγράψει πληροφορίες που προβάλλονται είτε σε προσωπικές συσκευές είτε σε εκείνες που η ίδια η υποδομή διαθέτει στο προσωπικό της (π.χ. εταιρικό κινητό τηλέφωνο κλπ).

Η συγκεκριμένη πειραματική συνθήκη παρουσιάζει δύο ενδιαφέροντα σημεία, αφενός μπορεί να οδηγήσει σε διαρροή πληροφοριών ακόμα και με μικρό σχετικά δείγμα καταγραφής (2.5’’), και αφετέρου η διαρροή πληροφοριών αυτή αυξάνει σχετικά όταν η μπαταρία είναι σε χαμηλότερα επίπεδα φόρτισης εν συγκρίσει με περιπτώσεις ενσύρματης φόρτισης[352]. Εν αντιθέσει με το προηγούμενο παράδειγμα εδώ απαιτείται μια εγγύτητα με την βάση φόρτισης για να ληφθούν οι μετρήσεις, αλλά στον αντίποδα δεν απαιτείται κάποιου είδους λογισμικό (malware κλπ) για να υπάρξει πρόσβαση στην βάση αυτή, καθώς δεν προϋποτίθεται λήψη ή επαύξηση προνομίων από την πλευρά της κινητής συσκευής[353].

Πρόκειται για μια πειραματική συνθήκη με χρήση του αλγορίθμου CNN (Convolutional Neural Network), όπου η συλλογή μετρήσεων ισχύος από τον ασύρματο φορτιστή χρησιμοποιείται στην δημιουργία ενός μοντέλου που θα είναι σε θέση να εντοπίζει σε ποιες ιστοσελίδες έχει πρόσβαση ο χρήστης μιας κινητής συσκευής, η ακρίβεια του μοντέλου σε τέτοιες πειραματικές συνθήκες ευλόγως επηρεάζεται από το επίπεδο φορτίσεως, και εντοπίστηκαν ακριβέστερες μετρήσεις σε περιπτώσεις χαμηλής (περί το 30%) και σχεδόν περατωμένης φορτίσεως (περί το 90%[354]). Η πειραματική συνθήκη ευρέθη να επηρεάζεται ελάχιστα από την ύπαρξη θορύβου (noise) κατά την συλλογή των μετρήσεων, ενώ η διάρκεια της λήψεως δείγματος επηρέαζε σαφώς την ακρίβεια του μοντέλου (για σύντομες μετρήσεις των

---

[350] Ο.π.,σ.7.

[351] Cour, A.S.L., & Afridi, K.K., & Suh, G.E.(2021). Wireless Charging Power Side-Channel Attacks. A arxiv:2105.12266v2[cs.CR],1-13,σ.1. Wireless Charging Power Side-Channel Attacks (archive.org) (τελευταία πρόσβαση 11/10/2021).

[352] Ο.π.,σ.12.

[353] Ο.π.

[354] Ο.π.,σ.6 & 10.

2,5'' η ακρίβεια μειωνόταν τωόντι, διότι η πλειοψηφία των ιστοσελίδων απαιτούν μεγαλύτερους χρόνους φόρτωσης του περιεχομένου τους[355]).

Έτερο παράδειγμα εγγύτητας συσκευών που δυνάμεθα να αναφέρουμε εδώ αφορά στην χρήση επιταχυνσιόμετρου (accelerometer) κινητής συσκευής για την λήψη πληροφοριών σχετικά με το τι πληκτρολογείτε σε ένα πληκτρολόγιο υπολογιστή πλησίον της εν λόγω κινητής συσκευής[356]. Η αρχιτεκτονική της πειραματικής συνθήκης παραμένει η ίδια όπως και σε προηγούμενες περιπτώσεις, ήτοι ο επιτιθέμενος έχει πρόσβαση σε μια κινητή συσκευή πλησίον του πληκτρολογίου με την μεσολάβηση ενός malware, κατόπιν ο επιτιθέμενος δημιουργεί ένα λεξικό για να εκπαιδεύσει το μοντέλο μάθησης του (neural network) και έπειτα με βάσει το μοντέλο αυτό να είναι σε θέση να εξάγει συσχετίσεις για τα ζεύγη πλήκτρων που ο χρήστης επιλέγει να πληκτρολογήσει (συγκεκριμένα οι μεταβλητές που χρησιμοποιούνται είναι εκείνες της τοποθέτησης των πλήκτρων στο πληκτρολόγιο, δηλαδή αν βρίσκονται δεξιά ή αριστερά κλπ, και της αποστάσεως ανάμεσα στα πλήκτρα που πληκτρολογούνται[357]).

Η πειραματική συνθήκη λαμβάνει τα δεδομένα από το επιταχυνσιόμετρο στο οποίο έχει πρόσβαση ο επιτιθέμενος, μετά τα ανεβάζει σε έναν διακομιστή, και κατόπιν τα δεδομένα κατηγοριοποιούνται ανάλογα αν αφορούν στην τοποθέτηση (δεξιά-αριστερά) ή στην απόσταση (feature extraction[358]). Μετά ο αλγόριθμος δημιουργεί κατατάξεις των πλήκτρων που πατήθηκαν, και δίνει σε αυτά ταμπέλες με βάσει την εκπαίδευση που έχει λάβει ο αλγόριθμος νευρωνικού δικτύου για να ξεχωρίζει τα κουμπιά ανάλογα με την απόσταση και αν βρίσκονται δεξιά ή αριστερά του πληκτρολογίου[359]. Τέλος, ακολουθεί η φάση κατά την οποία ο αλγόριθμος βαθμολογεί την κάθε λέξη με βάσει το μέγεθος της (n-1), ώστε κατόπιν αυτή να αντιστοιχηθεί με την όμοια της από το λεξικό που ο επιτιθέμενος έχει δημιουργήσει[360]. Στο πείραμα των ερευνητών τα ποσοστά αυξομειώνονταν ανάλογα με το εύρος των λέξεων (π.χ. το ποσοστό

---

[355] Ο.π.,σ.8.

[356] Marquardt, P., & Verma, A., & Carter, H., & Traynor, P.(2011).*(sp) iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers.* Paper presented at the proceedings of the 18th ACM Conference on Computer and Communications Security ,CSS 2011. Chicago, Illinois,USA. October 17-21,2011,σ.1. DOI:10.1145/2046707.2046771. (sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers | Request PDF (researchgate.net) (τελευταία πρόσβαση 05/01/2022).

[357] Ο.π.,σ.1 & 4.

[358] Ο.π.,σ.6.

[359] Ο.π.

[360] Ο.π.

μειωνόταν για λέξεις των δύο ή τριών γραμμάτων[361]). Ενώ, διατυπώθηκε παράλληλα και η αντίληψη πως η επίθεση θα μπορούσε να λειτουργήσει με καλύτερα ποσοστά αν ο επιτιθέμενος είχε έστω μερική γνώση του εννοιολογικού πλαισίου εντός του οποίου εντάσσονταν οι λέξεις που πληκτρολογήθηκαν[362] (δυνάμει εδώ η SCA θα μπορούσε να εξεταστεί συνδυαστικά και με την ύπαρξη μιας εκ των ένδον απειλής).

Στο συγκεκριμένο άρθρο καταγράφονται ακόμα και ορισμένες παράμετροι που δυνητικά μειώνουν την απόδοση του αλγόριθμου μηχανικής μάθησης, και που εδώ θα αναφερθούν μόνο ονομαστικά, διότι δυνητικά θα μπορούσαν να αποτελέσουν αντίμετρα και η όλη συλλογιστική αφορά στο επόμενο κεφάλαιο. Οι προκλήσεις αυτές ήσαν τρεις, ήτοι η τοποθέτηση (orientation) της κινητής συσκευής σε σχέση με το πληκτρολόγιο, δεδομένου ότι ο αισθητήρας είναι το επιταχυνσιόμετρο επηρεάζει τον τρόπο με τον οποίο σχεδιάζονται οι άξονες με βάσει τους οποίους το μοντέλο μηχανικής μάθησης θα αντιλαμβάνεται την τοποθέτηση (δεξιά/αριστερά), κι αυτό διότι οι άξονες αλλάζουν ανάλογα με το αν για παράδειγμα το κινητό τοποθετείται κάθετα ή οριζόντια[363]. Δεύτερον, στον βαθμό που η εκροή που καταγράφεται είναι οι δονήσεις, τότε πρέπει να ληφθεί υπόψη και η ύπαρξη θορύβου που προκαλείται από έτερες δονήσεις, άσχετες με την πληκτρολόγηση, και που όμως υπάρχουν στον οικείο χώρο[364]. Τρίτον, η επιφάνεια πάνω στην οποία βρίσκεται το πληκτρολόγιο, ανάλογα με αυτή δυσχεραίνεται ή διευκολύνεται η δυνατότητα του επιταχυνσιόμετρου να αντιληφθεί όλες τις δονήσεις, και επομένως να καταγράψει εμμέσως όλα τα "χτυπήματα" στο πληκτρολόγιο[365].

- Αναφορικά με την τρίτη υποομάδα απειλών που σχετίζονται με το δίπολο κρίσιμες υποδομές/κινητές συσκευές εδώ ορισμένα ενδεικτικά παραδείγματα αφορούν σε αντανακλάσεις αντανακλάσεων όπως ερευνούν οι Xu et al. Σε αυτό το παράδειγμα οι ερευνητές επιχειρούν να ανασυγκροτήσουν το περιεχόμενο μιας οθόνης κινητής συσκευής, μέσω της επεξεργασίας εικόνων που έχουν τραβηχτεί δια της τεθλασμένης, δηλαδή μέσω αντανακλάσεων επάνω σε διάφορα αντικείμενα που εν τέλει αντανακλούν επάνω στον βολβό του ματιού του χρήστη (π.χ. μέσω της επιφάνειας μιας τοστιέρας ή ενός καθρέπτη που είναι έτσι τοποθετημένα ώστε να αντανακλούν τα γυαλιά ηλίου ή τον βολβό του ματιού του χρήστη κλπ), και κατόπιν με την χρήση αλγορίθμων να καθίσταται

[361] Ο.π.,σ.7.

[362] Ο.π.,σ.9.

[363] Ο.π.,σ.9.

[364] Ο.π.,σ.9-10.

[365] Ο.π.

εφικτή η επεξεργασία των εικόνων που έχουν καταγραφεί και αντανακλούν το περιεχόμενο της οθόνης πάνω στον βολβό[366].

- Περαιτέρω, υφίσταται το παράδειγμα της εκτέλεσης επιθέσεως πλευρικού καναλιού διαμέσου της αξιοποιήσεως της ακουστικής ηχούς (echoes). Σε αυτή την περίπτωση οι Cheng et al. αναλύουν μια συνθήκη όπου κάποια συσκευή εγγραφής ήχου έχει τοποθετηθεί στο ίδιο περιβάλλον με μια κινητή συσκευή android (ώστε αυτή η τελευταία να λειτουργεί εν είδει συστήματος σόναρ, sonar system) και η οποία είναι σε θέση να καταγράψει ηχητικές εκροές που απορρέουν από την τελευταία και που δεν γίνονται αντιληπτές από το ακουστικό φάσμα του ανθρώπινου αυτιού (inaudible acoustic signals).

Κατόπιν, το επιθετικό σχήμα με την ονομασία *Sonarsnoop*, θα αξιοποιηθεί στην κατεύθυνση του εντοπισμού του μοτίβου ξεκλειδώματος της συσκευής από τον χρήστη (phone unlock pattern). Η λογική που υπαγορεύει η ως άνω επίθεση προκύπτει αρχικά από την παρατήρηση ότι τα αντικείμενα στον περιβάλλοντα χώρο της κινητής συσκευής αντανακλούν επάνω τους μια σειρά ακουστικών σημάτων, μη αντιληπτών από ανθρώπινα ώτα, που αποτελούν εκροές της κινητής συσκευής (OFDM sound signals[367]).

Τα μικρόφωνα που ο επιτιθέμενος έχει τοποθετήσει στον χώρο λαμβάνουν, αφενός τα σήματα αυτά και αφετέρου τις αντανακλάσεις τους από τα αντικείμενα στα οποία έχουν προσκρούσει. Κατόπιν ο επιτιθέμενος αξιοποιεί την *μήτρα προφίλ ηχούς* (*echo profile matrix*) στην οποία εισάγονται οι διαφορετικές καταγραφές των ηχητικών σημάτων από πολλαπλά μικρόφωνα, ώστε μέσω του συνδυασμού των καταγραφών να εντοπιστεί το μοτίβο της κίνησης των δακτύλων του χρήστη για το ξεκλείδωμα της οθόνης[368].

Εδώ η ανάλυση των καταγραφών είναι εφικτή διότι ο βασικός κανόνας της αντανάκλασης των ηχητικών εκροών είναι πως ο χρόνος άφιξης του ήχου από την συσκευή στα

---

[366] Heinly, J., & White, A.M., & Frahm, J.-M.(2013).*Seeing double: Reconstructing obscured typed input from repeated compromising reflections*. Paper presented at the CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. Berlin, Germany. November 4-8, 2013,1063-1074, σ.1066 & 1070. DOI:https://doi.org/10.1145/2508859.2516709. Seeing double | Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (τελευταία πρόσβαση 10/09/2021).

[367] Cheng, P., & Bagci, I.E., & Roedig, U., & Yan, J.(2018). SonarSnoop: Active Acoustic Side-Channel Attacks. *International Journal of Information Security,*19,213-228(1-13)(2020),σ.1-2.DOI: https://doi.org/10.1007/s10207-019-00449-8. SonarSnoop: Active Acoustic Side-Channel Attacks (arxiv.org) (τελευταία πρόσβαση 07/09/2022).

[368] ο.π.,σ.3.

αντικείμενα του χώρου θα είναι ίδιος, εκτός και αν κάποιο αντικείμενο (εν προκειμένω το δάκτυλο του χρήστη) κινείται οπότε και οι χρόνοι εκκίνησης και άφιξης θα διαφοροποιηθούν ανάλογα, με αποτέλεσμα αν συνδυαστούν αποτελεσματικά να δίνουν το προαναφερθέν μοτίβο[369].

Όπως γίνεται εύκολα αντιληπτό οι επιθέσεις πλευρικού καναλιού δεν εξαντλούνται μόνο σε περιπτώσεις που αφορούν κινητές συσκευές (ήτοι κινητά τηλέφωνα), πριν ολοκληρωθεί η παρούσα υπό-ενότητα θα παρουσιαστούν εν συντομία ορισμένες έτερες περιπτώσεις που αφορούν σε παραδείγματα συνδυασμού χρήσης διαδικτύου, έξυπνων συσκευών, και SCA απειλών. Ενδεικτικά, ορισμένες τέτοιες περιπτώσεις είναι και οι κάτωθι :

- Αναφορικά με τις καρπιαίες έξυπνες συσκευές (wearable smart devices, ήτοι smart watches) οι Maiti et al. διερευνούν την περίπτωση χρήσης των αισθητήρων των ευφυών ρολογιών για να αποσπάσουν, φέρ' ειπείν, κωδικούς ξεκλειδώματος μιας παρακείμενης κινητής συσκευής android (επομένως εδώ ο λόγος γίνεται για hopping). Οι συγγραφείς αξιοποιούν, όπως γίνεται και σε προηγούμενα παραδείγματα none-invasive SCAs, έναν συνδυασμό μηχανικής μάθησης (εξαρτημένης σε αυτή την περίπτωση) και του αισθητήρα κίνησης του ευφυούς ρολογιού[370].

Η πειραματική συνθήκη ξεκινά με τον επιτιθέμενο να αποκτά πρόσβαση στους αισθητήρες του ευφυούς ρολογιού (accelerometer, gyroscope κλπ) μέσω ενός κακόβουλου λογισμικού που θα εγκαθίσταται στο τελευταίο, κατόπιν τα στοιχεία από τους αισθητήρες θα μεταφέρονται σε κάποιον εξυπηρετητή που ο επιτιθέμενος θα έχει πρόσβαση[371]. Με τις πληροφορίες από τον εξυπηρετητή ο επιτιθέμενος εκπαιδεύει το μοντέλο του (data collection, feature extraction, learning phase για δημιουργία κατατάξεων, classifiers) σε διαφορετικές

---

[369] Το μοντέλο της επίθεσης αυτής διακρίνεται σε τέσσερα στάδια, το στάδιο δημιουργίας (*Signal Generation*) του σήματος από την android συσκευή, το στάδιο της συλλογής (*Data Collection*) των δεδομένων μέσω μικροφώνων, το στάδιο επεξεργασίας του σήματος (*Signal processing*) για την δημιουργία των προφίλ της ηχούς (με συνδυαστική χρήση των στοιχείων των σχετικών με την κατεύθυνση της κίνησης, *movement direction,* και την απόσταση που διανύει η κάθε κίνηση, *movement distance*) και την συνακόλουθη αφαίρεση των πάσης φύσεως θορύβων, και τέλος το στάδιο λήψης της απόφασης (*Decision Making*) όπου με βάσει τα στοιχεία του προηγούμενου σταδίου επιχειρείται το επιτυχές ξεκλείδωμα της οθόνης της συσκευής android. Ο.π,σ.3 & 5.

[370] Maiti, A., & Jadliwala, M., & He, J., & Bilogrevic, I.(2017). Side-Channel Inference Attacks on Mobile Keypads using Smartwatches. *IEEE Transactions on Mobile Computing* PP (99),1-16,σ.1. DOI:10.1109/TMC.2018.2794984. (PDF) Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches (researchgate.net) (τελευταία πρόσβαση 23/03/2022).

[371] Ο.π.,σ.3.

συνθήκες κατά την πληκτρολόγηση (ήτοι πληκτρολόγηση με τα δύο χέρια, με το ένα χέρι στο οποίο είναι τοποθετημένο και το smartwatch κλπ) και στην συνέχεια συγκρίνει τα classifiers σε διάφορες περιπτώσεις (π.χ. τα διαφορετικά δεδομένα του ενός και μόνο χρήστη, τα δεδομένα ενός χρήστη έναντι άλλων χρηστών κλπ[372]).

Ενδιαφέρον στην πειραματική αυτή συνθήκη έχει το γεγονός ότι οι συγγραφεί συγκρίνουν και με δεδομένα όπου η επίθεση εκτελείται άνευ αξιοποίησης του smartwatch, όπου σε αυτή την περίπτωση παρατηρείται ότι υπάρχει αυξομείωση στην ακρίβεια εντοπισμού ορισμένων κουμπιών του πληκτρολογίου, το οποίο οι συγγραφείς αποδίδουν στην μεταβλητή της απόστασης ανάμεσα στον δείκτη του χρήστη, στο κινητό και το smartwatch που επιβάλλει ο χρήστης να κάνει επιπλέον κινήσεις όταν πληκτρολογεί[373]. Εύλογα το hopping που λαμβάνει χώρα εδώ θα μπορούσε να αξιοποιηθεί για να υποκλαπούν δεδομένα αν για παράδειγμα ο χρήστης πληκτρολογεί σε εταιρικό τηλέφωνο που δίνει πρόσβαση σε στοιχεία της κρίσιμης υποδομής (π.χ. ηλεκτρονικά μηνύματα, αν και το άρθρο δεν κάνει νύξη σε αυτά ή στις κρίσιμες υποδομές γενικά).

- Αναφορικά με την συνάθροιση των έξυπνων συσκευών εντός κατοικίας (ήτοι smart homes) οι Abrishamchi et al. στο άρθρο τους κάνουν μια συνοπτική παρουσίαση των εκροών που εμφανίζουν οι συσκευές ενός smart home και ορισμένων τρόπων επιθέσεως που μπορούν να εφαρμόσουν οι επιτιθέμενοι. Οι συγγραφείς στο τμήμα της βιβλιογραφίας που μελετούν επικεντρώνουν όχι στην ανταλλαγή πληροφοριών ανάμεσα στις συσκευές, αλλά τουναντίον εστιάζουν σε μεταβλητές όπως η σχετική τους θέση μέσα στον χώρο, το είδος της δραστηριότητας που επιτελούν και η ταυτοποίηση των προδιαγραφών τους (*identities*[374]).

Περαιτέρω, το άρθρο τους διαρθρώνει τις SCAs σε τέσσερα επίπεδα (infrastructure layer, ambient condition management layer, application layer και security layer) και εξετάζει την σχετική για το καθένα βιβλιογραφία, χωρίς όμως να προχωρά και πάλι (όπως πολλοί άλλοι συγγραφείς) σε κάποιου είδους σύνθεση στο μάκρο-επίπεδο (δηλαδή για την ευφυή κατοικία

---

[372] Ο.π.,σ.3-4.

[373] Ο.π.,σ.8.

[374] Abrishamchi, M.A.N., & Abdullah, A.H., & Cheok, A.D., & Bielawski, K.S. (2017). *Side Channel Attacks on Smart Home Systems: A short Overview.* Paper presented at the IECON 2017- 43RD Annual Conference of the IEEE Industrial Electronics Society. Beijing, China. October 29-November 1, 2017, 4926-4932,σ.1. DOI: 10.1109/IECON.2017.8217429. [PDF] Side channel attacks on smart home systems: A short overview | Semantic Scholar (τελευταία πρόσβαση 12/12/2021).

συνολικά κλπ) και η έμφαση δίνεται στις επιμέρους συσκευές και επίσης στο επίπεδο του λογισμικού (network κλπ[375]).

Στο επίπεδο της εφαρμογής (application layer) περιλαμβάνονται και σκιαγραφούνται αφενός οι επιθέσεις που στοχεύουν φυσική δραστηριότητα της κάθε συσκευής (ήτοι φωτεινότητα και αντανάκλαση αυτής από την οθόνη στις γύρω διαφανείς επιφάνειες, επικοινωνία με φωνητικές εντολές και αξιοποίηση της μείωσης των πακέτων δεδομένων, traffic packets, για τον εντοπισμό μοτίβων μέσω αναγνώρισης χαρακτηριστικών της φωνής, αξιοποίηση των μικροφώνων αυτών των συσκευών για εντοπισμό της κίνησης των δακτύλων πάνω σε οθόνες αφής ή/και αξιοποίηση των ψηφιακών βοηθών, όπως η Alexa, για την διαρροή πληροφοριών εξαιτίας της μόνιμης δυνατότητας για αποστολή φωνητικών εντολών κλπ[376]). Αφετέρου, οι επιθέσεις που στοχεύουν στην ανάλυση της κίνησης των πακέτων δεδομένων με χρήση της μηχανικής μάθησης ώστε να κάνει ο επιτιθέμενος σειρά συσχετίσεων (στόχευση κατ' επέκταση του network traffic, του firmware κλπ[377]).

Στο επίπεδο του Ambient Condition Management Layer η έμφαση δίδεται κυρίως σε επιθέσεις που επιχειρούν να δώσουν τον έλεγχο μιας ευφυής συσκευής (προσπέλαση του firmware στο Google's Nest για να επιχειρηθεί κατόπιν κάποιο hopping σε έτερες συσκευές του δικτύου, χρήση δικτύου μικρής κατανάλωσης ισχύος, για προσπέλαση ελέγχων ασφαλείας), κινούμενες σε λογικές injection ίσως, και από την άλλη σε επιθέσεις που μπορούν για παράδειγμα να εστιάσουν στην διασπάθιση φωτεινότητας των VLC (visual light communication) ώστε με αυτό τον τρόπο να αποκρυπτογραφήσουν τα μηνύματα των πακέτων[378].

---

[375] Ο.π.,σ.5 κε.

[376] Χαρακτηριστικά παραδείγματα που οι συγγραφείς αναφέρουν είναι η τεχνική VAD (voice activity detection) με την οποία οι Backes et al. σχεδιάζουν SCA που θα συνδυάζει την επιτυχή συσχέτιση των φωνητικών εντολών με την κυκλοφορία των πακέτων που περιέχουν πληροφορίες φωνητικών εντολών (voice traffic loads), και το άρθρο των Bachy et al. που καταφέρνουν να τροποποιήσουν το firmware ευφυιών τηλεοράσεων μέσω της μη ορθής χρήσης των διεπαφών JTAG (JTAG interfaces), που οδηγούν σε δυνητική πρόσβαση στο bootloader όταν επιχειρείται μέσω των JTAGs να γίνει αποσφαλμάτωση των CPUs, οι συγγραφείς χρησιμοποίησαν διάφορες τεχνικές ανάλυσης firmware στην συνθήκη τους (η μια εξ αυτών είναι η αποσφαλμάτωση του JTAG, η άλλη η φυσική πρόσβαση, και τέλος η ανάλυση των ενημερώσεων των firmware), βλ. στο ο.π.,σ.6-7.

[377] Βλ. ενδεικτικά τα άρθρα των Rutkin και Gray αντίστοιχα και στο ο.π.

[378] Πρόκειται για τα παραδείγματα των Hernandez et al. για το Google's Nest που και με την διαμεσολάβηση της χρήσης κακόβουλου λογισμικού είναι εφικτό να γίνει hopping και σε έτερες συσκευές, το *ZLL (Zigbee Light Link*) των Morgner et al. που προορίζεται για χρήση ευφυιών συστημάτων φωτισμού, και το *VLC*

Στο επίπεδο ασφαλείας (Security Layer) δίνεται εκ νέου το παράδειγμα της ανάλυσης traffic για κλειστά συστήματα παρακολούθησης με την ροή δεδομένων να αυξομειώνεται ανάλογα με τις δραστηριότητες (κίνηση από το ένα δωμάτιο στο άλλο, στέγνωμα μαλλιών κλπ) που καταγράφονται[379]. Στο επίπεδο της υποδομής (Infrastructure Layer) κυρίως παρουσιάστηκαν επιθέσεις χρονομέτρησης, μέτρησης ισχύος, και σε συνδυασμό με μοντέλα μηχανικής μάθησης (π.χ. Markov) για εύρεση συσχετίσεων[380]. Οι επιθέσεις εδώ κυρίως μελετούν την κατανάλωση ισχύος από τις δραστηριότητες εντός του σπιτιού και από την λειτουργία συσκευών (π.χ. φορητών υπολογιστών, ή από πρίζες) και από τις χρόνο-αναλύσεις της επικοινωνίας και ανταλλαγής πακέτων μεταξύ των ευφυιών συσκευών[381].

Εν γένει, για τα smart homes φαίνεται πως μπορούμε να συμπεράνουμε πως δύνανται να απειλήσουν τις κρίσιμες υποδομές όχι μόνο μέσω των πολλών εκροών, αλλά και διότι λόγω του μικρότερου μεγέθους ενός διαμερίσματος εν σχέσει με μια εγκατάσταση CI ίσως είναι ευκολότερο να εκτελεστεί ένα hopping από μια συσκευή σε άλλη (π.χ. από οικιακή ευφυή συσκευή σε κάποια εταιρική), και διότι οι ευφυείς συσκευές καταγράφουν κινήσεις και συνήθειες καθιστώντας ίσως ευκολότερη την εκπαίδευση μοντέλων μηχανικής μάθησης (Markov, ZLL κλπ) και αυξάνοντας την πιθανότητα επιτυχών συσχετίσεων (correlations) για διαρροή πληροφοριών (πακέτα μηνυμάτων/πληροφοριών, κωδικοί ξεκλειδώματος οθόνης, περιεχόμενο smart TV, PIN λογαριασμών κλπ).

- Περαιτέρω, σε ότι αφορά στην περίπτωση του περιβάλλοντος Cloud (που αξιοποιούν οι κρίσιμες υποδομές) εδώ υφίσταται μια σειρά στοιχείων που καθιστούν το έδαφος πρόσφορο για μια SCA, όπως η φυσική συνύπαρξη της εικονικής μηχανής με , πέραν αυτής, υπολογιστικό σύστημα, και το multitenancy (συνύπαρξη πολλαπλών χρηστών στο ίδιο περιβάλλον, co-residency κλπ[382]). Σε συμπλήρωση των cache-based

(*vulnerability of visual light communication*) των Classen et al. που αξιοποιεί την διάχυση φωτεινότητας (εκροή φωτεινότητας, στο ο.π.,σ.6.

[379] Εδώ το παράδειγμα ανήκει στην μελέτη των Li et al. στο ο.π.

[380] Ο.π.,σ.7.

[381] Παραδείγματα όπως των Tang & Ono με το μοντέλο τους LHMM (*layered hidden Markov model*), των Conti et al. με την ονομασία *MTPlug* για την παρακολούθηση της μέτρησης ισχύος, και επίσης των Srinivasan et al. με τίτλο *FATS* (*fingerprint and timing-based snooping*) που χρησιμοποιήθηκε στο timestamping της ασύρματης επικοινωνίας μεταξύ ευφυιών συσκευών στο ο.π.

[382] Younis, Y.A., & Kilayat, K., & Merabti, M.(2014). *Cache-Side Channel Attacks in Cloud Computing*. Paper presented at the 2nd International Conference on Cloud Security Management (ICCSM 2014). Cranfield ,

SCAs που παρατέθηκαν στο προηγούμενο κεφάλαιο, παρατίθενται από τους Younis et al. Ορισμένοι τύποι ακόμα, που εδώ θα αναφερθούν μόνο εν παρόδω. Οι Time-driven SCAs (Evict and Time Attack), όπου ο επιτιθέμενος κάνει εκκένωση (evict) ενός σετ μνήμης cache εγγράφοντας εκεί τα δικά του δεδομένα, και σε περίπτωση που ο χρήστης χρησιμοποιήσει το συγκεκριμένο σετ τότε ο χρόνος κρυπτογράφησης θα είναι προσαυξημένος, κι έτσι ο επιτιθέμενος θα γνωρίζει πληροφορίες για το μυστικό κλειδί, καθώς η τιμή του τελευταίου θα επηρεάζει τον χρόνο εκτέλεσης της κρυπτογράφησης[383].

Οι Trace-driven SCAs, συνήθως βασίζονται σε μετρήσεις ηλεκτρονικών εκροών, και ο επιτιθέμενος παρακολουθεί τα hits και misses του χρήστη σε ένα cache set , ώστε μέσω αυτών των παρατηρήσεων να λάβει πληροφορίες για τις δραστηριότητες του τελευταίου στο εν λόγω set[384] (περισσότερο αφορά στην μνήμη CPU). Περαιτέρω, οι Giechaskiel et al. διερευνούν σε άρθρο τους την περίπτωση επιθέσεως πλευρικού καναλιού έναντι των Cloud data center όπου ο χρήστης μπορεί να λειτουργήσει απομονωμένα (ήτοι single tenant όπου ο διαθέσιμος χώρος στο Cloud είναι διαθέσιμος σε έναν και μόνο χρήστη που τον έχει νοικιάσει για ιδίους σκοπούς[385]). Οι συγγραφείς παραθέτουν και μελετούν τρεις διακριτές υπό-περιπτώσεις επιθέσεως πλευρικού καναλιού στην μελέτη περίπτωσης των Cloud based FPGAs (Field Programmable Gate Arrays) ως ακολούθως :

→ Πρώτον, η περίπτωση όπου ο επιτιθέμενος δύναται να μειώσει το την ευρυζωνικότητα (bandwidth) μέσω πρόκλησης ασυμφωνίας (contention) στο PCIe

---

United Kingdom. October 23-24, 1-11, σ.9. DOI: 10.13140/2.1.4666.7206. (PDF) Cache Side-Channel Attacks in Cloud Computing (researchgate.net) (τελευταία πρόσβαση 24/12/2021).

[383] Ο.π.,σ.7.

[384] Ο.π.

[385] Η υποπερίπτωση αυτή μας ενδιαφέρει και παρατίθεται εδώ αντί του προηγούμενου κεφαλαίου με τις ταξινομήσεις, διότι αφενός πολλές εταιρείες (επομένως κρίσιμες υποδομές) ανήκουν στους παρόχους πόρων, όπως είναι οι δημόσια διαθέσιμες συστοιχίες προγραμματιζόμενων πυλών (FPGAs), σε περιβάλλον Cloud, όπως επί παραδείγματι οι Alibaba, Amazon Web Services (AWS), Baidu, Huawei και άλλες. Και αφετέρου, διότι μια τέτοια επίθεση πλευρικού καναλιού μπορεί να διασπάσει την απομόνωση του χρήστη σε περιβάλλον VM/Cloud κι έτσι να θέσει εν κινδύνω όσους εργαζόμενους, και τα δεδομένα τους, εργάζονται απομακρυσμένα χρησιμοποιώντας τους εικονικούς χώρους που προσφέρουν τα κέντρα δεδομένων (data centres, που είναι και τα ίδια κρίσιμες υποδομές τουτέστιν). Giechaskiel, I., & Tian, S., & Szefer, J.(2022). Cross-VM Covert- and Side-Channel Attacks in Cloud FPGAs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS),* 32, 1-29,σ.1-2 & 26. DOI:https://doi.org/10.1145/3534972Cross-VM Covert- and Side-Channel Attacks in Cloud FPGAs | ACM Transactions on Reconfigurable Technology and Systems (τελευταία πρόσβαση 22/08/2022).

(υλικό διαύλου Η/Υ[386]). Οι συγγραφείς χρησιμοποιούν το σενάριο της ευρυζωνικότητας με δύο διακριτούς τρόπους, αφενός για να εκμαιεύσουν πληροφορίες για τις δραστηριότητες του εκάστοτε χρήστη ενόσω βρίσκεται σε περιβάλλον VM/Cloud (passive τύπος επίθεσης) και αφετέρου για να μειώσουν δυνάμει την λειτουργικότητα του ίδιου του περιβάλλοντος για τον έτερο χρήστη (αυτή η μορφή επίθεσης είναι περισσότερη active, προφανώς βέβαια όχι offensive, καθώς οι πόροι μειώνονται αλλά δεν επέρχεται κάποια ζημία στο περιβάλλον VM/Cloud). Για την πρώτη περίπτωση οι συγγραφείς δημιουργούν ένα εν κρυπτό κανάλι (covert channel) με το να οδηγούν σε κορεσμό (saturating) τον σύνδεσμο PCIe που ενώνει τον διακομιστή με το FPGA, κατόπιν ο επιτιθέμενος πρέπει να βρίσκεται στο ίδιο NUMA node με εκείνο του χρήστη τον οποίο θέλει να παρακολουθήσει (αυτό ελέγχεται μέσα από την αποστολή στιγμιότυπων και την σύναψη χειραψιών με ετέρους χρήστες κλπ[387]).

Ανάλογα με το μέγεθος των πακέτων δεδομένων που μπορούν να μεταφερθούν μέσω της ευρυζωνικότητας (καθότι μεγέθη κάτω των 4kB φαίνεται να επηρεάζουν την ακρίβεια της πειραματικής συνθήκης, μιας και ο θόρυβος κατά την μεταφορά αυξάνει σημαντικά φέρ' ειπείν, ενώ και τα σημαντικά μεγαλύτερα μεγέθη είναι επίσης επιρρεπή στον θόρυβο διότι πραγματοποιούν πολλές μικρές μεταφορές που δεν μπορούν εύκολα να παρατηρηθούν) η πειραματική συνθήκη έχει μεγαλύτερα ή μικρότερα ποσοστά ακρίβειας[388].

Δεδομένων όλων των παραπάνω, ο επιτιθέμενος μπορεί είτε να λάβει πληροφορίες για την επεξεργασία αρχείων, εδώ πρόκειται για βίντεο και συγκεκριμένα για πληροφορίες που αφορούν παραμέτρους των οπτικοακουστικών αρχείων και πληροφορίες για το αν ο χρήστης προχωρά σε μια μετατροπή (converting) της ποιότητας του εν λόγω αρχείου[389]. Παρατηρήθηκε πως υπάρχει πτώση της ταχύτητας μεταφοράς της ευρυζωνικότητας όταν γίνεται μετατροπή ενός τέτοιου αρχείου και ότι περαιτέρω ο χρόνος διάρκειας του εν λόγω αρχείου αναμένεται να είναι μικρότερος από εκείνον ενός ετέρου αρχείου αν συγκριθούν η ποιότητα ανάλυσης (resolution) και ο χρόνος εναλλαγής των καρέ (frame rate) ανάμεσα στα δύο αυτά (δηλαδή το αρχείο με την μεγαλύτερη διάρκεια θα υπερτερεί και στα δύο αυτά σημεία[390]).

[386] Ο.π.

[387] Ο.π.,σ.7-8.

[388] Ο.π.,σ.10-12.

[389] Ο.π.,σ.14 & 16.

[390] Ο.π.,σ.16.

Ακόμα, ο επιτιθέμενος δύναται να εντοπίσει, διαμέσου της μέτρησης του PCIe traffic, την έναρξη στιγμιοτύπων (instance initialization), καθώς η μέτρηση αυξομειώνεται ανάμεσα στην στιγμή που ο χρήστης αιτείται ενός στιγμιότυπου και εκείνη κατά την οποία αυτό ενεργοποιείται, ενώ όταν το στιγμιότυπο δεν βρίσκεται στο ίδιο VM με αυτό του χρήστη και του επιτιθέμενου τότε το PCIe bandwidth μένει σταθερό[391]. Το δεύτερο σημείο της πρώτης υποπερίπτωσης αφορά στην δυνατότητα του επιτιθέμενου να μειώσει την επίδοση των εφαρμογών που λειτουργούν στις εικονικές μηχανές που βρίσκονται να συνυπάρχουν ο επιτιθέμενος και ο χρήστης[392] (ιδιαίτερα χρήσιμο για μελέτη ιδίως υπό συνθήκες τηλεργασίας και μετάβασης λειτουργιών των κρίσιμων υποδομών online).

Γενικά παρατηρήθηκε ότι όσο πιο μεγάλο είναι το στιγμιότυπο (instance) που έχει δημιουργήσει ο χρήστης και στο οποίο λειτουργούν οι εφαρμογές που έχει επιλέξει, τόσο μεγαλύτερη θα είναι η χρονοτριβή της FPGA εξαιτίας της μείωσης της ευρυζωνικότητας λόγω του PCIe contention[393]. Εύλογα, οι δύο υπο-περιπτώσεις συνδυάζονται καθώς η χρονοτριβή στην εκτέλεση μιας εφαρμογής (ή εφαρμογών) δίνει περισσότερο χρόνο στον επιτιθέμενο να παρατηρήσει τον χρήστη και να αποσπάσει ακόμα περισσότερες πληροφορίες για τις δραστηριότητες του τελευταίου στο Cloud[394].

→ Δεύτερον, η επίθεση που στοχεύει στην υποδαύλιση ανταγωνισμού για τους πόρους της μνήμης μη τυχαίας προσπέλασης (NVMe, Non-Volatile Memory Express) των δίσκων SSD οι οποίοι πόροι γίνονται διαθέσιμοι για προσπέλαση από τα στιγμιότυπα F1 εντός του διαύλου PCIe bus[395].Το contention αυτό χρησιμοποιείται με δύο τρόπους από τους συγγραφείς, είτε ως ανταγωνισμός του ενός δίσκου προς τον άλλο (SSD to SSD contention) είτε ως ανταγωνισμός ανάμεσα σε δίσκο SSD και των συστοιχιών προγραμματιζόμενων πυλών (FPGAs). Στην πρώτη περίπτωση ο επιτιθέμενος χρησιμοποιεί τις εντολές hdparm (με το όρισμα -t) και stress για να διαβάσει το δίσκο SSD και να μπορέσει να αναγνωρίσει αν το bit είναι 1 ή 0, καθώς στην περίπτωση του 1 η εντολή stress χρειάζεται 7'' ενός στην περίπτωση του 0 δεν

[391] Ο.π.,σ.17.

[392] Ο.π.,σ.19.

[393] Ο.π.,σ.20.

[394] Ο.π.

[395] Ο.π.

μεταδίδεται κάτι (idleness). Επίσης, οι ίδιες τεχνικές μπορούν να επιβραδύνουν (μέσω contention) την επίδοση των προγραμμάτων που εκτελούνται σε έτερα στιγμιότυπα[396].

Για την περίπτωση του FPGA-to-SSD contention ο επιτιθέμενος χρησιμοποιεί το PCIe ως stressor για να μειώσει τον ρυθμό κυκλοφορίας των δεδομένων της ευρυζωνικότητας και συνακόλουθα την ευρυθμία του SSD δίσκου, αυτό γίνεται όταν σε οποιοδήποτε στιγμιότυπο που έχει δημιουργηθεί ο επιτιθέμενος εκτελεί τις εντολές hdparm και stress για ορισμένο χρονικό διάστημα (στην πειραματική συνθήκη για 3' και 30'' αντίστοιχα) για τα στιγμιότυπα receiver (δέκτης) και transmitter (πομπός) αντίστοιχα, ενώ ταυτόχρονα η FPGA-based PCIe λειτουργεί σε ορισμένη στιγμή σαν stressor μεταδίδοντας το bit 1 για 30'' συνέχεια[397]. Έτσι το bandwidth καταλήγει να μειώνεται και μαζί του η επίδοση του SSD.

→ Τρίτον, εδώ το υπόδειγμα επίθεσης αφορά στις κοινές θερμικές υπογραφές (common thermal signatures) τις οποίες λαμβάνει ο επιτιθέμενος παρατηρώντας τους ρυθμούς decay (decay rates) των αρθρωμάτων (modules) της δυναμικής μνήμης RAM (DRAM, Dynamic RAM) της κάθε ξεχωριστής συστοιχίας προγραμματιζόμενων πυλών (FPGAs[398]).Οι συγγραφείς αξιοποιούν την υπερθέρμανση των DRAMs σε κάθε ξεχωριστή FPGA (καθώς η πρόσβαση στην κεντρική DRAM της υποδομής του Cloud δεν είναι εφικτή, αυτό στο οποίο ένας επιτιθέμενος μπορεί ευκολότερα να έχει πρόσβαση είναι η emulated DRAM που διαθέτει προς αξιοποίηση η κάθε FPGA) απενεργοποιώντας την λειτουργία ανανέωσης τους (refresh), προς δύο την κατεύθυνση που επιτρέπει στον επιτιθέμενο να εντοπίσει τις σχετικές θέσεις των FPGAs, ακόμα και όταν οι χρήστες τους τελούν σε απομόνωση[399].

Σχετικά με το DRAM decay, όταν οι DRAMs εκκινούν την λειτουργεία κάποιου αρθρώματος τότε τα μισά από τα κελιά τους (cells) φορτίζονται για να αποθηκευτούν εκεί οι τιμές που θα περάσει ο χρήστης στο άρθρωμα. Όταν η λειτουργία refresh απενεργοποιηθεί κάποια από τα κελιά θα χάσουν το φορτίο τους, και το bit που τους αντιστοιχεί θα αντιστραφεί (από 0 σε 1 ή αντιστρόφως), κατά τον χρόνο στον οποίο επέρχεται το decay ο επιτιθέμενος μπορεί να βρει ορισμένες συσχετίσεις διότι τα στιγμιότυπα που ευρίσκονται στον ίδιο διακομιστή θα έχουν σχετικά παρόμοιο ρυθμό decay, λόγω και της συσχέτισης σε ότι αφορά την

[396] Ο.π.,σ.21-22.

[397] Ο.π.,σ.22-23.

[398] Ο.π.

[399] Ο.π.,σ.24.

θερμοκρασία στην οποία θα έχουν ανέρθει εξαιτίας της μη ανανέωσης, ενώ εκείνα που θα βρίσκονται σε διαφορετικούς διακομιστές θα παρουσιάζουν ουσιώδεις διαφορές. Κατά τον τρόπο αυτό η τοποθεσία των στιγμιότυπων είναι ευκολότερα αναγνωρίσιμη ακόμα κι αν ανήκουν σε διαφορετικά NUMA νήματα, αλλά βρίσκονται πάντα στον ίδιο διακομιστή[400] .

Επιπροσθέτως, η τελευταία περίπτωση του συγκεκριμένου παραδείγματος (thermal signatures) συνδυάζεται και με τις δύο άλλες (PCIe contention), καθώς ο επιτιθέμενος με την χρήση του contention μπορεί να εντοπίσει περιπτώσεις "συγκατοίκησης" (co-location) εντοπίζοντας το NUMA νήμα στο οποίο βρίσκεται κάποια FPGA, ενώ η μέθοδος DRAM decay θα εντοπίσει συσχετίσεις εντός ενός και του ίδιου διακομιστή, άρα το ποσοστό της επιτυχίας της SCA μπορεί συνδυαστικά να αυξηθεί περαιτέρω[401].

- Τέλος δε, μπορούμε να αναφέρουμε και την VoIP λειτουργία κλήσης μέσω της χρήσης του λογισμικού Skype, καθώς η τηλεργασία (όπως και η συνύπαρξη των εργαζομένων στις εγκαταστάσεις μιας κρίσιμης υποδομής) απαιτεί εκ προοιμίου την δυνατότητα επικοινωνίας και αυτό αυξάνει τις εκροές, ενώ ταυτόχρονα πρέπει να παρατηρηθεί ότι τα παραδείγματα της υπό-ενότητας αυτής δεν έχουν προς ώρας μελετήσει την πτυχή της διαμεσολαβούμενης επικοινωνίας (δηλαδή τον συνδυασμό internet-based application,όπως το skype κλπ, και την συμμετοχική χρήση αυτής από έναν αριθμό εργαζομένων, διότι τα περισσότερα παραδείγματα αφορούν την κατά μόνας χρήση IoT συσκευών ή εφαρμογών, με παρέμβαση σε κάποιες περιπτώσεις του επιτιθέμενου ως eavesdropper).

Οι Compagno et al. σε άρθρο τους μελετούν την περίπτωση εκτέλεσης SCA, όπου ο επιτιθέμενος στην πειραματική τους συνθήκη έχει ελάχιστη έως καθόλου πρόσβαση στην φωνητική εκροή από την κλήση VoIP (σε προγράμματα όπως το Skype ή το Google Hangouts) και αντιθέτως επιχειρεί με την χρήση μηχανικής μάθησης να ανασυντάξει το plaintext από την ακουστική εκροή των πλήκτρων του πληκτρολογίου (εξ' ου και η ονομασία της επίθεσης ως "*Skype & Type Attack*[402]".

---

[400]Αυτό σημαίνει ότι ο επιτιθέμενος προχωρά σε μια profile attack (SCA) καθώς οι συγγραφείς ισχυρίζονται ότι εκκινώντας από τις θερμικές υπογραφές ο επιτιθέμενος μπορεί να σκιαγραφήσει το προφίλ ολόκληρου του διακομιστή (π.χ. τι προγράμματα εκτελούνται κλπ).Ο.π.

[401] Ο.π.,σ.26.

[402] Compagno, A., & Conti, M., & Lain, D., & Tsudik, G.(2017). *Don't Skype & Type ! Acoustic Eavesdropping in Voice-Over-I*P. Paper presented at the Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. Abu Dhabi, UAE. April 2-6, 1-13, σ.4. DOI: 10.1145/3052973.3053005.

Όπως και σε προηγούμενα παραδείγματα, ο επιτιθέμενος χρησιμοποιεί την μηχανική μάθηση για να εκπαιδεύσει το μοντέλο του (κατά βάση τα είδη δεδομένων για τους classifiers είναι δύο ειδών, είτε τους ήχους των πλήκτρων που ο επιτιθέμενος κατάφερε να συλλέξει, είτε την καταγραφεί όλων των ήχων όλων των πλήκτρων από το πληκτρολόγιο στόχο), και κατόπιν σχεδιάζει το προφίλ του σεναρίου επίθεσης (Model Profiling Scenario), όπου μεταξύ άλλων προτείνεται (και) μια εναλλακτική σεναρίου που περιλαμβάνει συνδυαστική χρήση social engineering, καθώς ορισμένα γράμματα του αγγλικού αλφαβήτου έμειναν εκτός του μοντέλου λόγω της περιορισμένης εμφάνισης τους(small training set), θέτοντας έτσι την πτυχή της μερικής γνώσης του εκάστοτε κειμένου από πλευράς επιτιθέμενου (π.χ. αν είναι insider κλπ[403]).

Η συγκεκριμένη πειραματική συνθήκη, αν και όμοια με άλλες που αναφέρθηκαν πρωτύτερα αποσκοπεί στην ανασύνταξη λέξεων κειμένου και κωδικών από τους ήχους ενός πληκτρολογίου, θέτει επιπλέον την πτυχή του θορύβου του προερχόμενου από κάποιο multitasking (ήτοι ο χρήστης να πληκτρολογεί και να ομιλεί ταυτόχρονα) ως επιπλέον παράμετρο περιορισμού/δυσκολίας.

Οι συγγραφείς επανέλαβαν την πειραματική τους συνθήκη, περιλαμβάνοντας σε αυτήν φωνές διαφορετικής έντασης, και παρατήρησαν πως η δραστική μείωση της ακρίβειας του αλγόριθμου συμβαίνει με ήχους άνω των 20 dB(Decibel) για να τείνει προς την τυχαιότητα, ενώ πρέπει να ληφθεί υπόψη και η ηχητική ένταση που προκύπτει από το μικρόφωνο μέσω του οποίου θα καταγράφεται ο ήχος του πληκτρολογίου[404]. Οι συγγραφείς θέτουν με τον τρόπο αυτό (και) την μεταβλητή της ανθρώπινης συνήθειας (π.χ. ομιλία και πληκτρολόγηση ταυτόχρονα), πέρα και από εκείνη της χωροθέτησης των άψυχων αντικειμένων εντός ενός οικιακού ή περιβάλλοντος εργασίας που έχει τονιστεί και σε προηγούμενη αρθρογραφία.

SCAs & Ενσωματωμένα Συστήματα:

Η παρούσα υπό-ενότητα αντιμετωπίζει αφενός την έλλειψη ενός σχετικά μεγάλου όγκου βιβλιογραφίας όπως ο αντίστοιχος στις δύο προηγούμενες υπό-ενότητες, και αφετέρου (όπως και σε έτερες περιπτώσεις) το ότι η εστίαση γίνεται στο μίκρο-επίπεδο των εκάστοτε attack

[1609.09359] Don't Skype & Type! Acoustic Eavesdropping in Voice-Over-IP (arxiv.org) (τελευταία πρόσβαση 13/10/2021).

[403] Ο.π.,σ.5.

[404] Ο.π.,σ.10.

vectors (πειραματικές συνθήκες που επικεντρώνουν σε μια συγκεκριμένη συσκευή) και όχι σε εκείνο της κρίσιμης υποδομής συνολικά (π.χ. βιομηχανία).

Όπως και στην ως άνω περίπτωση των IoT συσκευών, τα εφαρμοσμένα συστήματα αποτελούν έννοια ομπρέλα για ένα σύνολο συσκευών των πλέον διαφορετικών λειτουργιών και εφαρμογών που δυσχεραίνει το οποιοδήποτε ταξινομητικό εγχείρημα επιχειρεί να λειτουργήσει εξαντλητικά, τέτοιες περιπτώσεις εφαρμοσμένων συστημάτων μπορούν σε πρώτη γραμμή να διακριθούν με βάσει τις συσκευές στις οποίες ενσωματώνονται, έτσι υφίστανται κατηγορίες όπως τα κινητά ενσωματωμένα συστήματα (mobile embedded systems) όπως εκείνα που διαθέτουν ψηφιακές κάμερες και κινητά, τα δικτυωμένα εφαρμοσμένα συστήματα (networked embedded systems) τα παράγουν εξόδους για έτερα συστήματα όπως συστήματα point-of-sale και οικιακής ασφάλειας, τα απομονωμένα εφαρμοσμένα συστήματα (standalone embedded systems) τα οποία έχουν πολύ συγκεκριμένες λειτουργίες και δεν συνδέονται με έτερα συστήματα (π.χ. αριθμομηχανές, ψηφιακά ρολόγια κλπ), και επίσης τα ενσωματωμένα συστήματα σε πραγματικό χρόνο (Real-time embedded systems) τα οποία παράγουν εξόδους/λειτουργίες σε προκαθορισμένο χρόνο όπως είναι τα συστήματα ελέγχου της κίνησης οχημάτων[405].

Η διάκριση των ενσωματωμένων συστημάτων γίνεται ακόμα και επί τη βάσει της αρχιτεκτονικής τους ή και των απαιτήσεων για την λειτουργικότητα τους. Έτσι εδώ μπορούν να παρατεθούν χαρακτηριστικές περιπτώσεις όπως τα συστήματα ενσωματωμένα σε τσιπ (SoC, Systems on a chip) που ενυπάρχουν σε μικρές το δέμας καταναλωτικές συσκευές, όπως smartphones, αισθητήρες IoT συσκευών, γυροσκόπια κλπ και τα οποία είναι ετερογενή ως προς το εύρος των συστημάτων που βρίσκονται ενσωματωμένα σε ένα μόνο τσιπ (π.χ. I/O logic control, μετατροπέας σήματος από αναλογικό σε ψηφιακό κλπ).

Ακόμα, τα ενσωματωμένα κυκλώματα για χρήση σε συγκεκριμένες εφαρμογές (ASICs, application-specific integrated circuits όπως είναι και τα ίδια τα SoCs βασικά) τα οποία ενσωματώνονται σε συσκευές IoT και εκτελούν συγκεκριμένες λειτουργίες ή πρωτόκολλα[406]. Η αναφορά για την ομαδοποίηση εφαρμοσμένων συστημάτων (ατομικά παραδείγματα περιλαμβάνουν ακόμα sim cards, smart cards, ATM, κυκλώματα, μηχανήματα γραμμών παραγωγής, ιατρικός εξοπλισμός κλπ) θα φανεί χρήσιμη και κατωτέρω, διότι η ετερογένεια, η πολυλειτουργικότητα τους και τα πλεονεκτήματα τους (π.χ. χαμηλό κόστος και μαζικότητα

[405] Lulka, J.(2022). 5 embedded systems terms IoT Admins must know. *TechTarget, IoTAgenda.* 5 embedded system terms IoT admins must know (techtarget.com) (Τελευταία πρόσβαση 27/9/2022).

[406] Ο.π.

παραγωγής[407]) ανοίγουν προοπτικές σε πιθανές SCAs και ακόμα και σε πιθανές νέες τεχνικές και συνδυασμούς αυτών των τελευταίων, ενώ μπορούν να δυσχεράνουν λόγω αρχιτεκτονικής (όπως θα αναφερθεί κατωτέρω) την ορθή σχεδίαση αντιμέτρων.

Η αρχιτεκτονική των συγκεκριμένων attack vectors συμβάλλει ως στοιχείο στην παραπέρα μελέτη της δυνατότητας επιτυχούς διενέργειας μιας SCA για μια σειρά λόγων που οι Lyu & Mishra αναφέρουν ως εξής και σε σχέση με τις cache SCAs που μελέτησαν εκείνοι (λόγοι τους οποίους οι συγγραφείς επεκτείνουν από κοινού σε ενσωματωμένα συστήματα και IoT συσκευές, επομένως μελλοντικά θα μπορούσαν και θα έπρεπε να μελετηθούν συνδυαστικά):

- Συνήθως τα ενσωματωμένα συστήματα (όπως έχει αναφερθεί και προηγουμένως) έχουν σχετικά λίγες λειτουργίες να επιτελέσουν και υποστηρίζουν μικρό εύρος εφαρμογών (applications). Αποτέλεσμα αυτού είναι για παράδειγμα η απουσία ορισμένων οδηγιών (instructions) σε επεξεργαστές ARM φέρ' ειπείν, όπου η οδηγία clflush απουσιάζει και δεν μπορεί έτσι να αφαιρεθεί κάποιο τμήμα μνήμης από διαφορετικά επίπεδα του cache[408].
- Δεύτερον, τα μεγέθη και τα επίπεδα στα οποία διακρίνεται η cache memory είναι συνήθως μικρότερα για τις IoT συσκευές και τα ενσωματωμένα συστήματα, απ' ότι για τους επεξεργαστές x86 για παράδειγμα[409].
- Τρίτον, τα πρωτόκολλα σε αυτά τα συστήματα και σε ότι αφορά την μνήμη cache δεν καταγράφονται επαρκώς (π.χ. πρωτόκολλα cache coherence), ή καταγράφονται κατά τρόπο που δεν επιτρέπει εύκολη πρόσβαση[410].
- Τέταρτον, τα πρωτόκολλα κρυπτογράφησης παρουσιάζουν σαφής διαφορές σε σχέση με τα αντίστοιχα συστημάτων και επεξεργαστών μεγαλύτερων δυνατοτήτων (π.χ. το μέγεθος του πίνακα lookup κλπ[411]).

Εδώ φαίνεται και πάλι το στοιχείο της ετερογένειας, από την μια πλευρά ο επιτιθέμενος μπορεί να δυσκολευτεί ενώ από την άλλη δυσχεραίνει το έργο της προστασίας έναντι των SCAs,

---

[407] Ο.π.

[408] Lyu, Y., & Mishra, P.(2017). A Survey of Side-Channel Attacks on Caches and Countermeasures. *Journal of Hardware and Systems Security,*2, 33-50 (2018), σ.43. DOI: A Survey of Side-Channel Attacks on Caches and Countermeasures | SpringerLink . A Survey of Side-Channel Attacks on Caches and Countermeasures (ufl.edu) (τελευταία πρόσβαση 22/11/2021).

[409] Ο.π.

[410] Ο.π.

[411] Ο.π.

καθότι δεν επιτρέπει μια ομοιογενή αντίδραση με βάσει τις παραμέτρους της αρχιτεκτονικής, και η κάθε ταξινόμηση πρέπει να λαμβάνει υπόψη της και επιπλέον ορίζουσες για να καταρτήσει μια στρατηγική αντιμέτρων.

Επί τη βάσει της συλλεχθήσας ως τα τώρα βιβλιογραφίας (που αποτελεί μόνο δείγμα του συνόλου αυτής) οι επιθέσεις πλευρικού καναλιού έναντι των ενσωματωμένων συστημάτων διακρίνονται, καταρχήν, σε δύο ευκρινή τμήματα για τους σκοπούς της παρούσης ανάλυσης :

- Οι επιθέσεις έναντι των ενσωματωμένων συστημάτων (embedded systems) καθαυτών, ανεξάρτητα που ευρίσκονται αυτά ενσωματωμένα[412].
- Οι επιθέσεις που στοχεύουν το ενσωματωμένο λογισμικό (embedded software), και που σε ότι αφορά την βιβλιογραφία αποτελούν ένα μικρότερο τμήμα αυτής έναντι της προηγούμενης κατηγορίας αυτής της υπό-ενότητας.

Σχετικά με το πρώτο δίπολο (embedded systems/SCAs) υφίστανται μια σειρά από τρωτότητες που καθιστούν το έδαφος ιδιαίτερα πρόσφορο για τέτοιες επιθέσεις. Κυριότερες εξ' αυτών είναι το κόστος αντικατάστασης τέτοιων συστημάτων, η δυσκολία στον οποιονδήποτε έλεγχο αυτών που προκύπτει από τις ελάχιστες δυνατότητες διεπαφής (interface), το γεγονός πως το λογισμικό (ή οι πλατφόρμες λογισμικού, software platforms) που χρησιμοποιείται πολλές φορές σε τέτοια συστήματα δεν προέρχεται από έμπιστες πηγές (untrusted sources) για λόγους μείωσης του κόστους και μη συμβατότητας στο υλικό[413], και ακόμα το γεγονός ότι η πρόοδος της τεχνολογίας αυξάνει την πολυπλοκότητα τέτοιων συσκευών (ενσωμάτωση πυρήνων, IP από τρίτες εταιρείες για SoCs, περισσότερες δυνατότητες ρύθμισης παραμέτρων του υλικού κλπ) και συνακόλουθα πληθαίνει τα όποια ζητήματα ασφαλείας[414].

Παραλείποντας τμήματα στα οποία έχει ήδη πραγματοποιηθεί μνεία στα οικεία κεφάλαια, παραθέτουμε όπως κατωτέρω τις SCAs που σταχυολογήθηκαν για την παρούσα υπό-ενότητα :

---

[412] Εκτός από την περίπτωση του αντίστοιχου ιατρικού εξοπλισμού που έχει ήδη παρατεθεί στην οικεία υπό-ενότητα για τον ιατροφαρμακευτικό τομέα ανωτέρω.

[413] Brinkmann, R.(2019). Side-Channel Attacks on Embedded Processors. *EE|Times 50*, *Designlines.* Side-Channel Attacks on Embedded Processors - EETimes (τελευταία πρόσβαση 20/09/2021).

[414] Bossuet, L., & Benhani, E.M.(2021). Performing Cache Timing Attacks from the Reconfigurable Part of a Heterogeneous SoC- An Experimental Study. *Applied Sciences,* 11, n.14:6662,1-14,σ.1. DOI: https://doi.org/10.3390/app11146662. Applied Sciences | Free Full-Text | Performing Cache Timing Attacks from the Reconfigurable Part of a Heterogeneous SoC—An Experimental Study | HTML (mdpi.com) (τελευταία πρόσβαση 13/09/2022).

- Thermal SCAs: Οι Al Faruque et al. στην πειραματική τους συνθήκη αξιοποιούν έναν αλγόριθμο μηχανικής μάθησης και μια θερμική κάμερα για να εντοπίσουν τα κινούμενα τμήματα ενός τρισδιάστατου εκτυπωτή, καθώς επίσης και για να καταφέρουν να εντοπίσουν τόσο την κατεύθυνση της κίνησης των τμημάτων που σχεδιάζουν το κάθε αντικείμενο, όσο και την θερμοκρασία τους αλλά και την ταχύτητα με την οποία αυτά κινούνται[415]. Η λογική της επιθέσεως είναι πως ο εκτυπωτής των τρισδιάστατων αντικειμένων θα κινείται σε δύο άξονες (Y= η κίνηση που αποδίδει βάθος στα αντικείμενα που δημιουργούνται, X=η κίνηση της βάσης του τρισδιάστατου εκτυπωτή), ο εντοπισμός της κάθε κίνησης θα γίνεται μέσω των θερμικών καταγραφών της κάμερας, έτσι που η άνοδος της θερμοκρασίας θα σημαίνει ότι το μπεκ του εκτυπωτή (nozzle) πλησιάζει εγγύτερα στην κάμερα οπότε και η μέση τιμή θα είναι μεγαλύτερη (λόγω της αύξησης της θερμότητας (για κατώφλι τιμών 0 και 1, όπου 1 είναι για την αυξημένη θερμοκρασία και 0 για το αντίστροφο), αλλά και αντιστρόφως[416], έτσι ο επιτιθέμενος φτιάχνει έναν αλγόριθμο χαρτογράφησης (mapping algorithm) που αποτυπώνει τις ακριβείς κινήσεις του εκτυπωτή[417].

Οι συγγραφείς προτείνουν δύο διαφορετικά σενάρια επιθέσεως, που είναι συνήθη για τις περιπτώσεις αλγόριθμων μηχανικής μάθησης, την στατική προσέγγιση (dynamic approach), όπου δεν αξιοποιούνται κάποια σετ δεδομένων για εκπαίδευση του αλγόριθμου (με χρήση είτε μάθησης υπό επίβλεψη είτε χωρίς αυτή), και την αντίστοιχη δυναμική (dynamic approach), όπου συμβαίνει το αντίθετο, εύλογα στην στατική προσέγγιση ο επιτιθέμενος θα πρέπει να έχει περισσότερο ακριβείς μετρήσεις, ενώ στην έτερη περίπτωση θα υπάρχει μεγαλύτερο περιθώριο διότι υφίσταται μια πρότερη εικόνα μέσω του training set[418].

Ενδιαφέρον παρουσιάζει η παρατήρηση των συγγραφέων πως ανάμεσα στις μεταβλητές που μειώνουν την ακρίβεια του αλγόριθμου (π.χ. χαμηλή ανάλυση και χαμηλός ρυθμός αλλαγής των καρέ κλπ) περιλαμβάνεται και το γεγονός πως η κάμερα δεν παρέχει δυναμικό auto-focus,

---

[415] Faruque, M.A., & Chhetri, S.R., & Faezi,S., & Canedo,A.(2016). *Forensics of Thermal Side-Channel in Additive Manufacturing Systems*.Paper presented at the ICCPS '16: Proceedings of the 7th International Conference on Cyber-Physical Systems.Vienna,Austria.April 11-14,1-15,σ.12.DOI: 10.1109/ICCPS.2016.7479115. Poster Abstract: Thermal Side-Channel Forensics in Additive Manufacturing Systems (acm.org) (τελευταία πρόσβαση 12/09/2021).

[416] Ο.π.,σ.4-5.

[417] Ο.π.,σ.6.

[418] Ο.π., σ.7-8.

ενώ παράλληλα είναι στατική ευρισκόμενη σε ένα σημείο, με αποτέλεσμα να μην παρέχονται στοιχεία για το βάθος στην κίνηση του εκτυπωτή (δηλαδή προσαρμογή της κάμερας κάθε που ο εκτυπωτής κινείται εμπρός και πίσω[419]). Αυτό σημαίνει πως σε τέτοια ενσωματωμένα συστήματα ίσως να μην αρκεί απλώς η παρατήρηση, ως input για τον αλγόριθμο, αλλά να απαιτείται και η εστίαση στην έννοια της κίνησης (ως τμήματος του 3D) για την εκτέλεση ή την αποτροπή μιας SCA.

- Power Analysis SCAs: Αρχικά μπορεί να αναφερθεί εδώ ένα συνδυαστικό, σε σχέση με την προηγούμενη παράγραφο, σχήμα επίθεσης πλευρικού καναλιού έναντι τρισδιάστατων ενσωματωμένων κυκλωμάτων (3D ICs). Οι Knechtel et al. στην πειραματική τους συνθήκη επιδιώκουν την σύνδεση του θερμικού αποτυπώματος με το μοτίβο δραστηριότητας και παροχής ρεύματος στο εκάστοτε IC[420]. Οι συγγραφείς αναφέρουν πως η συσχέτιση των τριών αυτών στοιχείων μεταξύ τους επηρεάζεται κυρίως από την κατανομή της πυκνότητας ισχύος (power distribution density) και η αντίστοιχη κατανομή του TSV σιλικόνης (through-silicon via[421]). Παρατηρείται εδώ όπως και προηγούμενα (π.χ. στην περίπτωση των IoT συσκευών όπου το πληκτρολόγιο ήταν δίπλα στην κινητή συσκευή) πως η ανομοιομορφία της κατανομής ισχύος από το ένα die στο άλλο, ή και μέσα στο ίδιο το die, αλλά και η φύση του υλικού που χρησιμοποιείται στα TSVs (π.χ. χαλκός) επηρεάζουν τα επίπεδα συσχετίσεως και επομένως θέτουν εν αμφιβόλω τόσο την πειραματική συνθήκη, αλλά ταυτόχρονα δύνανται να είναι δυνητικά αντίμετρα[422].

Καθώς προϋποτίθεται ότι ο επιτιθέμενος έχει πρόσβαση σε κάποιο κύκλωμα και μπορεί να το παρατηρήσει, κατά πρώτον δίνει εισόδους (inputs) για να παρατηρήσει μοτίβα δραστηριότητας του κυκλώματος ώστε να κατανοήσει την θερμική συμπεριφορά αυτού

[419] Ο.π.,σ.10-11.

[420] Η υπόθεση εργασίας ενέχει ότι ο επιτιθέμενος έχει πρόσβαση στο κύκλωμα και ότι η επίθεση είναι non-invasive. Knechtel, J., & Sinanoglu, O.(2017). *On Mitigation of Side-Channel Attacks in 3D ICs: Decorrelating Thermal Patterns from Power and Activity*. Paper presented at the 2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC), 2017. Austin, TX,USA. June 18-22,1-6,σ.3. DOI: 10.1145/3061639.3062293. (PDF) On Mitigation of Side-Channel Attacks in 3D ICs: Decorrelating Thermal Patterns from Power and Activity (researchgate.net) (Τελευταία πρόσβαση 22/11/2021).

[421] Ο.π.,σ.2.

[422] Ο.π.

(*Thermal characterization of the 3D IC*[423]). Μια δεύτερη παραλλαγή που οι συγγραφείς προτείνουν είναι η δυνατότητα του επιτιθέμενου να παρατηρήσει τα θερμικά μοτίβα συγκεκριμένων αρθρωμάτων (*Localization and monitoring of modules*) , δηλαδή εν αντιθέσει με την πρώτη περίπτωση να γνωρίζει την συσχέτιση input-output και να κάνει πιο στοχευμένη την επίθεση του[424]. Η μεθοδολογία των συγγραφέων συνοψίζεται στην μέτρηση της ισχύος (voltage volume) και η βέλτιστη αποτελεσματικότητα παρουσιάζεται στις τάσεις που έχουν ομοιόμορφη κατανομή και στην μικρή τυπική απόκλιση ανάμεσα σε δείγματα διαφορετικών τάσεων ισχύος[425], ενώ η μεθοδολογία αυτή κατά τους συγγραφείς είναι κατά 30% φθηνότερη εν σχέση με άλλες (π.χ. *MILP formulations*[426]).

Αξιοσημείωτο είναι ακόμα το γεγονός πως η επίθεση είναι λιγότερο επιτυχής όσο πιο μεγάλο είναι το εκάστοτε κύκλωμα τόσο μικρότερες είναι οι συσχετίσεις, επομένως εδώ τίθεται ζήτημα επεκτασιμότητας (scalability) που φαίνεται να δημιουργεί μεγάλες διαφορές ανάμεσα στις μετρήσεις που θα λαμβάνονται, κι έτσι όταν η αρχιτεκτονική των dies του κυκλώματος τα τοποθετεί το ένα πάνω στο άλλο, οι υψηλές θερμικές συσχετίσεις του ενός, θα φέρνουν χαμηλότερες συσχετίσεις για το άλλο[427]. Επομένως, εδώ το μεγαλύτερο μέγεθος ενός ενσωματωμένου συστήματος (εν σχέση με το λειτουργικό, φέρ' ειπείν, μιας IoT συσκευής) μπορεί να διαδραματίσει ρόλο (και) αντιμέτρου σε μια περίπτωση κάποιας SCAs, και να πρέπει να ληφθεί υπόψη και από την πλευρά του επιτιθέμενου.

Τέλος, οι συγγραφείς αξιολογώντας την αποτελεσματικότητα του σχεδιασμού της επίθεσης παρατηρούν πως τα ευρήματα τους επηρεάζονται αφενός από την εισαγωγή dummy (εικονικών, ψευδών) TSVs για να αυξηθούν οι συσχετίσεις ισχύος, και αφετέρου από το πόσο εξονυχιστικά (εκείνοι και ο οποιοσδήποτε επιτιθέμενος) έχουν διερευνήσει τον τρισδιάστατο χώρο σχεδιασμού ενός τέτοιου κυκλώματος[428].

Εδώ επανέρχεται το ζήτημα της πρότερης γνώσης από πλευράς του επιτιθέμενου (ή της οικοδόμησης μιας τέτοιας γνώσης κατά τον σχεδιασμό και την εκτέλεση της επίθεσης), και επίσης συνίσταται η προσοχή στην ίδια την χρησιμότητα της SCA ως εργαλείο χαρτογράφησης κάποιου attack vector, που όπως και στο προηγούμενο παράδειγμα θερμικής επίθεσης, θέτει επί τάπητος όχι μόνο την γνώση του συστήματος, αλλά και την τρισδιάστατη αντίληψη περί χώρου

[423] Ο.π.,σ.4.

[424] Ο.π.

[425] Η τεχνική ονομάζεται *floorplanning centric voltage assignment*, Ο.π.

[426]Πρόκειται για διαχείριση της local και global κατανομής ισχύος Ο.π.

[427] Ο.π.,σ.5-6.

[428] Ο.π.,σ.6.

όχι γύρω από την συσκευή υπό επίθεση, αλλά εντός αυτής, κάτι που στο πόνημα μας δεν είχε προκύψει, ή έστω τονιστεί, ως τώρα ως πτυχή (ήτοι το 3D στοιχείο[429]).

- Electromagnetic SCAs: Οι Camurati et al. θέτουν με την σειρά τους επί τάπητος ένα ζήτημα αρχιτεκτονικής στο σχεδιασμό συστημάτων που μπορεί να προσφέρει εύφορο έδαφος σε εκτέλεση EM SCAs, το γεγονός ότι συσκευές όπως το WiFi και το Bluetooth διαθέτουν τόσο ψηφιακά όσο και αναλογικά τσιπάκια εντός του ίδιου περιβλήματος σιλικόνης, και με τον τρόπο αυτό το ενσωματωμένο σύστημα μπορεί δυνάμει να είναι το μέσο που θα μεταφέρει την SCA για να πλήξει κάποιον αλγόριθμο κρυπτογράφησης. Οι συγγραφείς αξιοποιώντας την ύπαρξη ενός πομποδέκτη ραδιοφώνου πλησίον μιας συσκευής που εκτελεί έναν αλγόριθμο κρυπτογράφησης επιχειρούν να ανασυγκροτήσουν το σήμα που εκπέμπεται ώστε μέσω των τεχνικών *Correlation Radio* (*CRA*) και *Template Radio Analysis* (*TRA*[430]) να αποσπάσουν το μυστικό κλειδί.

Οι συγγραφείς επιχειρούν να δείξουν, πειραματικά, πως ο επιτιθέμενος αποσπά το μυστικό κλειδί του AES εκμεταλλευόμενος την αναλογία σήματος και θορύβου (signal-to-noise Ratio, SNR) όπου το δεύτερο ενισχύει την δυνατότητα εντοπισμού του πρώτου όταν συνυπάρχουν αναλογικές και ψηφιακές εκπομπές[431]. Η λογική του πειράματος επομένως είναι η ευθυγράμμιση των λήψεων των εκάστοτε σημάτων (traces) με τον μέσο όρο του συνόλου των λήψεων (prototype trace[432]). Η εν λόγω συνθήκη βοηθά στην κατανόηση της συνδυαστικής λειτουργίας των εκροών, με το ψηφιακό σκέλος να λειτουργεί ως *aggressor* και το αναλογικό ως το θύμα (*victim*) για να συντελεστεί κάτι που προηγουμένως έχουμε αναφέρει σε άλλες περιπτώσεις (όχι και οι ίδιοι οι συγγραφείς όμως) ως hopping, καθώς οι τιμές 1 και 0 αλλάζουν

[429] Ακροθιγώς θίγεται και η δυνατότητα πιο ενεργής παρέμβασης του επιτιθέμενου (μέσω των dummy TSVs) στο πλαίσιο της SCA, χωρίς ακόμα να μπορεί να γίνει λόγος για εξ' ολοκλήρου επιθετική χρήση (offensive) αυτής, αλλά πάντως εγείρει το ερώτημα πως μια τέτοια πρακτική διαφοροποιείται από την offensive διάσταση, ή αν εν τέλει μπορεί να λειτουργήσει ως ένα βήμα προς αυτή την κατεύθυνση, εδώ δεν θα επεκταθούμε περαιτέρω.

[430] Camurati, G., & Poeplau, S., & Muench, M., & Hayes, T., & Francillon, A.(2018). *Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers.* Paper presented at the 25th ACM Conference on Computer and Communications Security. Toronto, Canada. October, 15-19,1-14, σ.1. doi: Screaming Channels | Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security . Screaming channels: When electromagnetic side channels meet radio transceivers | EURECOM(τελευταία πρόσβαση 8/2/2022).

[431] Ο.π.,σ.3.

[432] Ο.π.,σ.4.

κατά την λειτουργία του κυκλώματος, η αλλαγή αυτή αντικατοπτρίζει την αλλαγή στην τάση ρεύματος (current consumption, voltage activity κλπ) όταν το κύκλωμα εκτελεί κάποια λειτουργία όπως για παράδειγμα η λειτουργία του ρολογιού (clock signal), και ο επιτιθέμενος αξιοποιεί τα Hamming weight και Hamming distance για να βρει τις συσχετίσεις με βάσει τις αυξομειώσεις στην τάση[433].

Καθώς οι μετρήσεις των ηλεκτρομαγνητικών εκροών σε μια τέτοια επίθεση απαιτεί, όπως και σε προηγούμενο κεφάλαιο έχει ειπωθεί, αφαίρεση του περιβλήματος του κυκλώματος (depackaging) για να ληφθούν οι μετρήσεις αυτές, οι συγγραφείς προτείνουν και έτερο επιθετικό σχήμα (*screaming channels*, ορά υποσημείωση 50) το οποίο να είναι none-invasive και να αξιοποιεί όχι την αυξομείωση της τάσης αλλά την μεταβλητή του θορύβου ως propagator του σήματος, ως αποτέλεσμα του τρόπου λειτουργίας των μεικτών (αναλογικό και ψηφιακό σήμα) κυκλωμάτων[434]. Οι συγγραφείς παρατηρούν πως οι εκροές είναι εμφανείς όταν ο ενισχυτής ισχύος είναι ενεργοποιημένος (power amplifier) και επιβεβαιώνουν πως το *screaming channel* προκύπτει από την μετάβαση από το ψηφιακό στο αναλογικό τμήμα ενός κυκλώματος. Τα βέλτιστα αποτελέσματα για τον αλγόριθμο AES δίνονται όταν υπάρχουν χαμηλά επίπεδα θορύβου (noise) , ενώ οι template attacks που δοκιμάστηκαν σαφώς επηρεάζονταν ως προς τα αποτελέσματα τους από τον περιβάλλοντα χώρο[435]. Αξίζει δε να σημειωθεί πως η εν λόγω παραλλαγή ήταν πιο επιτυχής σε περιπτώσεις εφαρμογής του AES σε λογισμικό, παρά σε αντίστοιχες προσπάθειες για λήψη εκροών από εφαρμογή του AES σε υλικό (ήτοι σε περίπτωση κρυπτογράφησης για το επίπεδο ζεύξης δεδομένων[436]).

Καθώς η συγκεκριμένη πειραματική συνθήκη αξιοποιεί την κεραία για την λήψη των εκάστοτε εκροών οι συγγραφείς περαιτέρω πρότειναν την βελτίωση της επιθέσεως τους απλώς πολλαπλασιάζοντας τους πομποδέκτες και προσαρμόζοντας τους σε διαφορετικές συχνότητες για να ενισχυθεί ο αριθμός των εκροών που λαμβάνονται (SDR με διευρυμένη ευρυζωνικότητα, bandwidth, όλα αυτά για μελλοντική μελέτη). Ο πολλαπλασιασμός των μέσων αυτών θα μπορούσε να συνδράμει δυνητικά αφενός στην μείωση του θορύβου που ενυπάρχει στα εκάστοτε κυκλώματα, και αφετέρου στο noise coupling που θα μπορούσε να προκύψει και να ενισχυθεί

[433] Ο.π.,σ.5.

[434] Ο.π.,σ.7.

[435] Ο.π.,σ.8.

[436] Ο.π.,σ.9.

από συνδυασμένη χρήση SDRs κλπ, και έτσι να οδηγήσει στην βελτίωση του θορύβου ως aggressor για την ακριβέστερη καταγραφή του σήματος[437].

Σε αυτό το παράδειγμα καταδεικνύεται επομένως τόσο η χρησιμότητα της πολλαπλότητας των συσκευών καταγραφής (κατάτι ίσως και ρεαλιστικότερη εν σχέσει με την χρήση μιας και μόνο συσκευής σε έτερα παραδείγματα, δεδομένου ότι αν κάποιος επιχειρήσει να επιτεθεί σε κρίσιμες υποδομές θα μπορεί να διαθέσει ίσως και αντίστοιχους πόρους κλπ[438]) στρατηγικά τοποθετημένων εντός του περιβάλλοντος χώρου, όσο και του hopping όταν αυτό συνδυάζεται με την ετερογένεια (heterogeneity) στον κλάδο κατασκευής των ενσωματωμένων συστημάτων, κι εδώ αναδεικνύεται (αν και δεν μπορεί να μας απασχολήσει εν συνόλω λόγω του περιορισμένου χώρου της διπλωματικής εργασίας) εν μέρει η διάσταση της συνδυαστικότητας (έστω και έμμεσα εδώ) στις επιθέσεις πλευρικού καναλιού.

Πέρα όμως και από την παράμετρο της απόστασης σημαίνοντα ρόλο , σύμφωνα με τους Goller & Sigl, διαδραματίζει και το περίβλημα (shielding plate) που εσωκλείει μέσα του την ενσωματωμένη συσκευή. Στην περίπτωση αυτή τόσο η μεταβλητή της απόστασης όσο και ο λόγος ανάμεσα στην σηματική εκπομπή και τον θόρυβο δραστικά[439]. Οι συγγραφείς χρησιμοποιούν παρόμοια λογική στην πειραματική τους συνθήκη με την προηγούμενη περίπτωση, με την χρήση αλγορίθμου Square-and-Multiply όπου η ανάλυση των σηματικών δειγμάτων που έχουν ληφθεί γίνεται με βάσει τον μέσο όρο αυτών ώστε να εξαχθεί το μυστικό κλειδί (το 0 βγαίνει με ύψωση στο τετράγωνο, ενώ το 1 με ύψωση στο τετράγωνο και πολλαπλασιασμό[440]). Επιπροσθέτως, οι συγγραφείς αναφέρουν στο άρθρο τους την εναλλακτική στην χρήση κεραίας ραδιοφωνικού εξοπλισμού, όπου μπορεί να χρησιμοποιηθεί ένα DVB-T stick για την εκτέλεση μιας EM SCA, που όμως φεύ καταλήγει να μειώνει την ποιότητα της λήψης σήματος και την απόσταση, παρά το ότι το σύνολο του τεχνικού εξοπλισμού που απαιτείται είναι μικρότερο εν σχέσει με τους radio receivers, παρόλ' αυτά η παραλλαγή

---

[437] Ο.π.,σ.11.

[438] Ο.π., περί ρεαλιστικής πιθανότητας εφαρμογής της εν λόγω επιθέσεως, όχι όμως για κρίσιμη υποδομή,σ.9.

[439]Goller, G., & Sigl, G.(2015). *Side Channel Attacks on Smartphones and Embedded Devices Using Standard Radio Equipment*. Paper presented at the 6th International Workshop, COSADE 2015. Berlin, Gemrany.April,13-15, 1-16(255-270),σ.12.DOI:https://doi.org/10.1007/978-3-319-21476-4_17 . paper_S10_2.pdf (telecom-paristech.fr) (Τελευταία πρόσβαση 12/12/2021).

[440] Ο.π.,σ.9-10.

σημειώνεται για να αποτυπωθεί το εύρος των πιθανών επιλογών (και το ανάλογο κόστος) προς χρήση για την εκτέλεση της επιθέσεως έναντι κάποιου attack vector[441].

- Acoustic SCAs: οι Iijima et al. παρουσιάζουν στην πειραματική τους συνθήκη ένα παράδειγμα ακουστικής επιθέσεως πλευρικού καναλιού, υπό την ονομασία "*Audio Hotspot Attack*", όπου ο δυνάμει επιτιθέμενος είναι σε θέση να δώσει φωνητικές εντολές προς έναν βοηθό φωνητικών εντολών (GPS, Smart Homes voice assistance systems κλπ) αξιοποιώντας για τον σκοπό αυτό το υπερηχητικό ακουστικό φάσμα που ο χρήστης τέτοιων συσκευών δεν μπορεί να αντιληφθεί, αλλά που τέτοιες ευφυείς συσκευές μπορούν να καταγράψουν ("*inaudible malicious voice command attack*[442]").

Η εν λόγω επίθεση διαφοροποιείται από έτερες της προηγούμενης υπό-ενότητας ως προς το ότι, κι αυτό είναι ίσως το βασικότερο χαρακτηριστικό των SCAs εν γένει, δεν βασίζεται σε κάποια τρωτότητα ορμώμενη από την αρχιτεκτονική του σχεδιασμού μιας συσκευής ή εφαρμογής, αλλά αντίθετα εδράζεται σχεδόν εξ' ολοκλήρου στην μη γραμμικότητα (non-linearity) του φυσικού φαινομένου της μεταφοράς των ηχητικών κυμάτων σε ένα περιβάλλον όπου υφίσταται ατμοσφαιρικός αέρας (π.χ. περιβάλλον δωματίου κλπ[443]). Οι συγγραφείς περιγράφουν ένα επιθετικό σχήμα με δύο παραλλαγές, όπου ο επιτιθέμενος χρησιμοποιεί ένα παραμετρικό ηχείο (parametric loudspeaker) το οποίο ενσωματώνει υπερηχητικούς μετατροπείς (ultrasound transducers) για να μεταφέρει προς τους βοηθούς φωνητικών εντολών (voice assistants) μια σειρά από (κακόβουλες φωνητικές) εντολές που ο ίδιος έχει καταγράψει χρησιμοποιώντας μια υπηρεσία μετατροπής κειμένου σε φωνητικό μήνυμα (Amazon Polly[444] ή αντίστοιχα αν πρόκειται για ευφυείς βοηθούς με αναγνώριση φωνής τότε ο επιτιθέμενος θα μπορούσε να αξιοποιήσει και καταγεγραμμένες συνομιλίες όπου θα ακούγεται η φωνή του χρήστη των συσκευών αυτών ει δυνατόν[445]).

---

[441] Ο.π.,σ.13-14.

[442] Iijima, R., & Minami, S., & Zhou, Y., & Takehisa, T., & Takahashi, T., & Oikawa, Y., & Mori, T.(2021). Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams and its Feasibility. *IEEE Transactions on Emerging Topics in Computing,*vol.9,n.4,2004-2018,σ.2004.DOI: 10.1109/TETC.2019.2953041. Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams and its Feasibility | IEEE Journals & Magazine | IEEE Xplore (Τελευταία πρόσβαση 27/09/2022).

[443] Ο.π.,σ.2016.

[444] Ο.π.,σ.2005,2007-2008.

[445] Ο.π.,σ.2007.

Οι κακόβουλες εντολές του επιτιθέμενου μεταφέρονται μέσω ενός κινητού τηλεφώνου προς το parametric ηχείο και εν συνεχεία μέσω του ατμοσφαιρικού αέρα (μέσω ακτινών ήχου, sound beams) αυτές οι κακόβουλες εντολές να μεταφερθούν στις συσκευές βοηθούς , χωρίς να γίνονται όμως αντιληπτές από τον χρήστη τους καθότι δεν εμπίπτουν στο ακουστικό του φάσμα (αλλά οι συσκευές θα τις λάβουν διότι όταν οι ακτίνες ήχου συναντηθούν το υπερηχητικό φορτίο θα μετατραπεί σε ηχητικά κύματα, ήτοι AM sound waves), και να εκτελεστούν από τις τελευταίες (ενν. τις συσκευές) δίνοντας έτσι στον επιτιθέμενο είτε πληροφορίες είτε δυνητικά έναν μερικό έλεγχο επ' αυτών[446]. Οι δύο παραλλαγές της επιθέσεως είναι η γραμμική (*linear attack*) και η διασταυρούμενη (*cross attack*) που αξιοποιούν ένα ή δύο παραμετρικά ηχεία ταυτόχρονα για να εκτελεστούν[447].

Οι συγγραφείς δοκίμασαν το επιθετικό τους σχήμα σε διαφορετικά περιβάλλοντα (πειραματικά και μη) και επίσης έναντι διαφορετικών φωνητικών βοηθών (Google Home, Amazon Echo) και λαμβάνοντας υπόψη τους τις επιπτώσεις που μπορούν να έχουν έναντι μιας επιτυχούς εκτέλεσης μεταβλητές όπως η απόσταση, ο θόρυβος (είτε συνεχής θόρυβος, stationary, είτε διακοπτόμενος, nonstationary noise) το μέγεθος της πρότασης που σχηματίζει η κάθε εντολή, και το σημείο τοποθέτησης των ηχείων (ανάλογα αν υπάρχει κάποιο εμπόδιο που κάνει ώστε ο ήχος να προσκρούει και να διασπαθίζεται[448]). Οι εκάστοτε μεταβλητές επηρεάζουν εύλογα την επιτυχή εκτέλεση, καθώς σε μικρούς χώρους η επιτρεπτή απόσταση διαμορφώνεται στα 2-4 μέτρα, ενώ για μεγαλύτερους χώρους όπως οι διάδρομοι η απόσταση αυξάνει περί τα 10 μέτρα[449].

Ακόμα οι μικρότερες προτάσεις/εντολές γίνονται πιο εύκολα αντιληπτές από τους φωνητικούς βοηθούς απ' ότι οι σχετικά μεγαλύτερες[450]. Ενώ η μεταβλητή του θορύβου, στην περίπτωση που αυτός είναι μόνιμος (stationary), επηρεάζει λιγότερο όταν το δίπολο κακόβουλης εντολής-θορύβου είναι στο ίδιο επίπεδο έντασης, ενώ οι μικρότερες σε μέγεθος εντολές λειτουργούν καλύτερα. Ο μη στατικός/διακοπτόμενος θόρυβος (nostationary noise) επέτρεπε στην επίθεση να είναι περισσότερο επιτυχής όταν η διαφορά στα dB ανάμεσα στον συγκεκριμένο θόρυβο και την ένταση της εντολής ήταν περί τα -5 dB, ενώ η επίθεση αποτύγχανε σε κάποιες περιπτώσεις όπου τα επίπεδα εντάσεως των δύο ήταν περίπου ίδια[451].

---

[446] Ο.π.,σ.2005.

[447] Ο.π.,σ.2007.

[448] Ο.π.,σ.2009-2011,2013-2014.

[449] Ο.π.,σ.2016.

[450] Ο.π.,σ.2011.

[451] Ο.π.,σ.2010.

Αναφορικά με τις δύο παραλλαγές στην πρώτη, την γραμμική, το ηχείο τοποθετείται σε συμμετρική (ευθεία) απόσταση από την συσκευή στόχο, και η επίθεση εκτελείται όπως αναφέρθηκε ανωτέρω[452]. Στην δεύτερη παραλλαγή, *cross attack,* δύο παραμετρικά ηχεία τοποθετούνται κατά τέτοιο τρόπο ώστε οι ακτίνες ήχου τους να συναντηθούν σταυρωτά σε ένα κεντρικό σημείο εν τέλει. Σε αυτή την παραλλαγή το ηχητικό κύμα διασπάται, με την χρήση του λογισμικού MATLAB, σε carrier wave και σε κύμα sideband, με το κάθε παραμετρικό ηχείο να διαχέει αντίστοιχα το ένα από τα δύο, και τελικά τα δύο να συναντιούνται σε ένα συγκεκριμένο σημείο που θα σημάνει παράλληλα και το μέγιστο σημείο της ηχητικής πίεσης (*SPL of the audible sound*) των δύο ενωμένων πλέον μερών[453]. Η δεύτερη αυτή παραλλαγή , παρατηρούν οι συγγραφείς, είχε μεγαλύτερο ποσοστό επιτυχίας μόνο ως προς το σημείο που οι ηχητικές ακτίνες τέμνονταν, άρα το εύρος είναι ίσως πιο περιορισμένο σε σχέση με την πρώτη παραλλαγή, ενώ και πάλι οι μικρότερες προτάσεις εντολών είχαν μεγαλύτερη πιθανότητα επιτυχίας (π.χ. η εντολή ενεργοποίησης συσκευής είχε 100% επιτυχία και για τις δύο συσκευές φωνητικών εντολών της πειραματικής συνθήκης[454]).

Οι λοιποί περιορισμοί που αντιμετώπισε η πειραματική συνθήκη αφορούν περισσότερο την θεματική του επόμενου κεφαλαίου, εδώ εν παρόδω αναφέρονται αφενός στο ότι οι ευφυείς συσκευές που εδώ είναι attack vectors συνδέονται εύλογα με εξυπηρετητές (servers) και ακόμα πιο εύλογα αναβαθμίζονται τακτικά, είναι πιθανό να αλλοιωθεί έτσι η σχέση εισόδου (input) και εξόδου (output) σε ότι αφορά το δίπολο παραμετρικών ηχείων και φωνητικών βοηθών (π.χ. σε ότι αφορά το στοιχείο φωνητικής αναγνώρισης). Αφετέρου, ο περιβάλλοντας χώρος δεν βρίσκεται πάντα στον έλεγχο του επιτιθέμενου και επομένως τα οι ηχητικές ακτίνες μπορεί να παρεμποδίζονται και να αλλοιώνουν την επίθεση του λόγω αντικειμένων που παρεμβάλλονται ή που καθ' οιαδήποτε στιγμή τοποθετούνται κάπου ανάμεσα κλπ[455].

Οι αναφορές αυτές (από την ανάποδη) βοηθούν στην κατανόηση της λογικής των SCAs ως ανεξάρτητων από λοιπές τρωτότητες των attack vectors και ως ικανές να εκμεταλλευτούν περιβαλλοντικά στοιχεία (π.χ. ήχος) κατά τρόπο (π.χ. ultrasound, nonlinearity) που ένα αντίμετρο δεν μπορεί να περιορίσει αποτελεσματικά ή έστω χωρίς ιδιαίτερο κόστος[456], ακόμα δε περισσότερο (και σε ότι αφορά συγκεκριμένα τα εφαρμοσμένα συστήματα) τέτοιες SCAs

[452] Ο.π.,σ.2009.

[453] Ο.π.,σ.2011.

[454] Ο.π.

[455] Ο.π.,σ.2013-2014.

[456] Ο.π.,σ.2016.

κάνουν ώστε οι χρήστες/χειριστές των συστημάτων αυτών να υποχρεωθούν δυνάμει να προστατέψουν αυτοί οι ίδιοι τέτοιες συσκευές, με το να κληθούν να τροποποιήσουν την δική τους (ενν. Οι χρήστες) συμπεριφορά.

Με την επίδραση της τεχνολογικής προόδου όλο και περισσότερο τα εφαρμοσμένα συστήματα περνούν από το στάδιο όπου δρουν ως απομονωμένες συσκευές σε εκείνο όπου ,και με την συνδρομή κάποιου στοιχειώδους λογισμικού, θα μπορούν να δρουν εντός ενός δικτύου (*always-on networked*), με αποτέλεσμα η μετάβαση αυτή να κάνει ώστε να αναφύονται νέες απειλές, και να θέτει επί τάπητος το ζήτημα νέων πτυχών προστασίας όσο και της ταξινομητικής χαρτογραφήσεως έτερων απειλών σχετικών (και) με τις SCAs[457]. Αναφορικά λοιπόν με τις επιθέσεις πλευρικού καναλιού που στοχεύουν στο ενσωματωμένο λογισμικό (embedded software), με βάσει την μελέτη ενός τμήματος της υπάρχουσα βιβλιογραφίας, η υφιστάμενη κατάσταση έχει ως εξής:

- EM SCAs: σε ένα τμήμα της βιβλιογραφίας έχει επιχειρηθεί η μελέτη των ηλεκτρομαγνητικών εκροών για εξαγωγή πληροφοριών σχετικά με την λειτουργία των νευρωνικών δικτύων σε ενσωματωμένα συστήματα όπως μικροελεγκτές, FPGAs κλπ. Ενδεικτικά, οι Batina et al. χρησιμοποιούν τις ηλεκτρομαγνητικές εκροές για την ανάκτηση στοιχείων όπως οι παράμετροι των μυστικών κλειδιών, οι συναρτήσεις ενεργοποίησης (activation functions) και ο αριθμός των νευρώνων σε κάθε στρώμα του νευρωνικού δικτύου. Η λογική της συνθήκης τους αφορά σε μέτρηση του χρόνου που απαιτείται για την λειτουργία της συνάρτησης ενεργοποίησης οπόταν και γίνεται αντιληπτό ότι για τις ίδιες εισόδους ο χρόνος ενεργοποίησης διαφέρει και άρα αυτές μπορούν να διακριθούν μεταξύ τους[458].

Περαιτέρω, οι συγγραφείς χρησιμοποιούν το Hamming Weight (HW) των βαρών του νευρωνικού δικτύου για να παρατηρήσουν τις ηλεκτρομαγνητικές εκροές (EM signature) κάθε που γίνεται φόρτωση των βαρών αυτών για να μπορεί ο επιτιθέμενος να προχωρήσει σε

---

[457] Ambrose, J.A., & Ragel, R.G., & Jayasinghe, D., & Li, T., & Parameswaran, S.(2015). *Side Channel Attacks in Embedded Systems: A Tale of Hostilities and Deterrence*. Paper presented at the 16th Symposium on Quality Electronic Design. Santa Clara, SA, USA. March, 02-04, 1-9, σ.9. DOI:10.1109/ISQED.2015.7085468. (PDF) Side channel attacks in embedded systems: A tale of hostilities and deterrence (researchgate.net) (Τελευταία πρόσβαση 14/10/2021).

[458] Real, M.M., & Salvador, R.(2021). Physical Side-Channel Attacks on Embedded Networks: A Survey. *Applied Science, 11, 6790*, 1-25,σ.10. DOI: https://doi.org/10.3390/app11156790 . (PDF) Physical Side-Channel Attacks on Embedded Neural Networks: A Survey (researchgate.net) (Τελευταία πρόσβαση 16/9/2021).

μοντελοποίηση τους. Αυτό είναι εφικτό γιατί στους μικροελεγκτές το bit 0 φορτώνεται εκ των προτέρων (pre-charging) κάθε φορά που γίνεται φόρτωση οδηγίας για την ενεργοποίηση των μυστικών βαρών (*loading of pre-trained weights*[459]). Έτσι το επιθετικό σχήμα είναι ενδεχομένως σε θέση, για κάποιες διαστρωματώσεις του δικτύου του μικροελεγκτή, να επιτρέψει στον δυνάμει επιτιθέμενο να διακρίνει τις συναρτήσεις πολλαπλασιασμού και ενεργοποίησης για να μετρήσει με τον τρόπο αυτό τον αριθμό των νευρώνων[460].

Παρομοίως, οι Yoshida et al. αξιοποιούν μια επίθεση βασισμένη σε CEMA για να αποσπάσουν πληροφορίες για τα βάρη του μοντέλου MLP (που ενσωματώνεται όπως και στο επόμενο παράδειγμα σε ένα κύκλωμα FPGA) όταν αυτά αποκρυπτογραφούνται για να εισέλθουν στον επιταχυντή του νευρωνικού δικτύου (DNN, Deep Neural Network), οπότε ο επιτιθέμενος στέλνει μια σειρά από διάφορες εισόδους και παρατηρεί τις συσχετίσεις που γίνονται ανάμεσα στις ηλεκτρομαγνητικές εκροές και το HD του accumulator register[461]. Οι Yu et al. Χρησιμοποιούν παρόμοια (CEMA) τεχνική, με την διαφορά ότι αντιμετωπίζουν το δίκτυο ως μαύρο κουτί (black box), και καλούνται να ανασυγκροτήσουν την αρχιτεκτονική και τις παραμέτρους αυτού[462].

Η υπόθεση που κάνουν εδώ οι συγγραφείς είναι πως το μέγεθος της ηλεκτρομαγνητικής εκροής πρέπει να είναι αντίστοιχο των παραμέτρων του κάθε στρώματος στο νευρωνικό δίκτυο, και επομένως θα είναι ενδεικτικό τόσο των υπολογισμών που γίνονται σε κάθε στρώμα (layer) όσο και της χρονικής διάστασης στο εκάστοτε στρώμα[463]. Μόλις ολοκληρωθεί αυτή πρώτη αναγνωριστική φάση και ο επιτιθέμενος έχει γνώση των παραμέτρων του δικτύου, εισέρχεται στο δεύτερο στάδιο της επίθεσης όπου, όμοια με έτερα παραδείγματα μικροαρχιτεκτονικής (microarchitectural attacks), αξιοποιεί adversarial based μεθοδολογίες μάθησης για να δημιουργήσει ένα υπόδειγμα υποκατάστασης του πραγματικού δικτύου (substitute model), με χρήση ενός training dataset, ώστε να μπορεί να αποκτήσει πληροφορίες για το εύρος των αποφάσεων που το νευρωνικό δίκτυο λαμβάνει (decision boundaries[464]).

Έχοντας πλέον το υπόδειγμα του και γνώση των παραμέτρων του νευρωνικού δικτύου που μελετά, ο επιτιθέμενος τα συγκρίνει χρησιμοποιώντας τα ίδια ζεύγη εισόδων και για τα δύο ώστε συγκρίνοντας τον βαθμό ακριβείας ανάμεσα στα δύο να εξάγει συμπεράσματα για τον

[459] Ο.π.

[460] Ο.π.

[461] Ο.π.,σ.14.

[462] Ο.π.,σ.15.

[463] Ο.π.

[464] Ο.π.

πιθανό τύπο της αρχιτεκτονικής του δικτύου που παρακολουθεί[465]. Εκ νέου οι Batina et al. , και πάλι με αναφορά στους μικροελεγκτές, εκπονούν μια πειραματική συνθήκη όπου αξιοποίησαν αριθμούς κινητής υποδιαστολής ανάμεσα στα bits 1 & 0 της βάσης δεδομένων MNIST για να διενεργήσουν επίθεση έναντι ενός μικροελεγκτή τύπου ARM. Στο παράδειγμα αυτό οι συγγραφείς αξιοποιούν έναν συνδυασμό EM και DPA επιθέσεως για να καταγράψουν με ακρίβεια το αποτέλεσμα της συνάρτησης πολλαπλασιασμού που καταγράφετε στην μνήμη του μικροελεγκτή[466].

Έτσι στην πειραματική τους συνθήκη οι συγγραφείς χρησιμοποιούν την *οριζόντια ανάλυση ισχύος* (όπως αποκαλούν την τεχνική τους, *horizontal power analysis*), όπου η καταγραφή ενός δείγματος ηλεκτρομαγνητικής διαρροής κατατμίζεται σε i μικρότερα δείγματα (sub-traces) για να απομονωθούν και να μελετηθούν κατά μονάς ενώ τα βάρη (weights) του πρώτου στρώματος του δικτύου πολλαπλασιάζονται ένα προς ένα με την ίδια, κάθε φορά, είσοδο. Εν συνεχεία, η τιμή της εισόδου (input) συνάγεται από την χρήση μιας τεχνικής διαφορικής ανάλυσης ισχύος(DPA) από κοινού με την χρήση του συντελεστή συσχέτισης Pearson[467].

- Power Analysis SCAs: Οι Maji et al. στην περίπτωση των μικροελεγκτών επιχειρούν μια παρόμοια πειραματική συνθήκη με τις ανωτέρω, όπου ο επιτιθέμενος γνωρίζει τις μάκρο-παραμέτρους του δικτύου και αναζητεί τις αντίστοιχες μίκρο-παραμέτρους (grey box scenario[468]). Όπως συμβαίνει και ανωτέρω, ο δυνάμει επιτιθέμενος καλείται να χρησιμοποιήσει δείγματα από την κατανάλωση ισχύος για να ανακαλύψει πληροφορίες σχετικά με τους χρόνους εκτέλεσης των διαφόρων λειτουργιών του DNN[469]. Η λογική κι εδώ είναι ότι ο επιτιθέμενος χαρτογραφεί τον πολλαπλασιασμό των διαφόρων εισόδων (ουσιαστικά ο στόχος του είναι η ανεύρεση του mantissa bit που χρησιμοποιείται στην συνάρτηση ενεργοποίησης και που εμπεριέχει το bit υπογραφή και τον εκθέτη που χρησιμοποιούνται στην συνάρτηση πολλαπλασιασμού) που δίνει με τα μυστικά weights του δικτύου, και κατόπιν χρησιμοποιεί μια timing analysis για να εντοπίσει ποια συνάρτηση ενεργοποίησης καλείται κάθε φορά[470].

[465] Ο.π.

[466] Ο.π.,σ.16-17.

[467] Ο.π.,σ.17.

[468] Ο.π.,σ.13.

[469] Ο.π.

[470] Ο.π.

Οι Yoshida et al. στην δική τους πειραματική συνθήκη, έναντι ενός FPGA στο παράδειγμα αυτό (Xilinx Spartan3-A FPGA), εφαρμόζουν μια επιθετική τεχνική ονόματι *chain-CPA* με στόχο την μείωση του θορύβου και των ανακριβειών στις παρατηρήσεις τους που θα απορρέει από συσχετιστικές αναλύσεις ισχύος κατ' εξακολούθηση[471]. Η πειραματική τους συνθήκη αξιοποιεί (πρόκειται πάλι για gray-box scenario όπως και παραπάνω) ένα μοντέλο HD leakage όπου με την εφαρμογή της *chain-CPA* ο επιτιθέμενος θα μπορούσε με ακρίβεια να παρατηρήσει τις συσχετίσεις ανάμεσα στην κατανάλωση ισχύος (power signature) και τα αποτελέσματα των ενδιάμεσων συναρτήσεων που καλούνται εντός του χώρου (register) των συναρτήσεων πολλαπλασιασμού/συσσώρευσης (multiply-accumulate operation register[472]).

Περαιτέρω, και πάλι, στο πεδίο των νευρωνικών δικτύων για τα FPGA οι Wei et al. παρουσιάζουν ένα σχήμα επιθέσεως για την ανασυγκρότηση των pixels μιας εικόνας[473]. Το επιθετικό σχήμα που προτείνεται αξιοποιήθηκε με δύο παραλλαγές, μια ενεργητική (active) και μια έτερη πιο παθητική (passive[474]). Ο επιτιθέμενος στοχεύει την buffer line του υλικού όπου λαμβάνει χώρα αφενός η προσωρινή αποθήκευση των pixels και αφετέρου η συνέλιξη (convolution) τους από κοινού με κάποιες τιμές-φίλτρα (filter-values[475]). Στην παθητική εκδοχή της επιθέσεως τους, κάθε φορά που ένας κύκλος δημιουργίας pixels αρχίζει και ολοκληρώνεται, οι συγγραφείς παρατηρούν πως οι εκροές ισχύος κυμαίνονται μεταξύ των pixels που έχουν παρόμοιες τιμές, έτσι αν κάποια pixels παραμένουν ίδια κατά τις εναλλαγές κύκλων δραστηριότητας στο κύκλωμα, τότε μπορεί να υποτεθεί πως η κατανάλωση ισχύος γι' αυτά θα είναι μικρότερη εν σχέσει με εκείνα που εναλλάσσονται. Έτσι είναι εφικτό ο επιτιθέμενος να ανασυγκροτήσει το περίγραμμα της εικόνας, ή έστω να το ξεχωρίσει σε σχέση με τα pixels της σιλουέτας του κέντρου αυτής[476].

Στην πιο ενεργητική εκδοχή της εν λόγω CPA SCA ο επιτιθέμενος κινείται αντιστρόφως και επιχειρεί να ανεύρει τις τιμές για τα pixels του συνόλου της εικόνας που θέλει να ανασυγκροτήσει. Η λογική εδώ είναι πως για κάθε μια συγκεκριμένη περιοχή της εικόνας, στο convolution layer, τα pixels με ίδιες τιμές παράγονται από διαφορετικούς πυρήνες (kernels), και άρα αν μετρηθεί η κατανάλωση ισχύος των τελευταίων θα προσδιοριστούν και οι τιμές των

[471] Ο.π.,σ.16.

[472] Ο.π.,σ.15-16.

[473] Ο.π.,σ.17.

[474] Ο.π.,σ.17.

[475] Ο.π.,σ.17.

[476] Ο.π.,σ.18.

pixels που αυτοί παράγουν[477]. Πρακτικά ο επιτιθέμενος εδώ ακολουθεί μια λογική μικροαρχιτεκτονικής (microarchitectural SCA) και δημιουργεί ένα δικό του μοντέλο (template) ώστε μετά να μπορέσει να συγκρίνει τις τιμές αυτού με τον πραγματικό του στόχο (πρόκειται για αλγόριθμο με χρήση greedy heuristics, και χρήση εργαλείων μέτρησης για ακρίβεια pixel-level και ακρίβεια αναγνώρισης, recognition accuracy). Με αυτά τα εργαλεία μέτρησης ο επιτιθέμενος συγκρίνει αφενός την διαφορά ανάμεσα στην τιμή του pixel που έχει ο ίδιος βρει εν σχέσει με εκείνη της αρχικής εισόδου για το σωστό pixel (pixel-level accuracy), και αφετέρου να συγκρίνει αν το μοντέλο που έχει δημιουργηθεί και που έχει δεχθεί τις εισόδους έχει ή όχι το σωστό label[478].

Μια ακόμα παραλλαγή Power Analysis SCA που αξίζει να αναφερθεί, αφορά στην λήψη δειγμάτων κατανάλωσης ισχύος εξ' αποστάσεως (*Remote Power*) εντός κυκλωμάτων FPGA που χαρακτηρίζονται από multi-tenancy[479]. Οι Moini et al. παρουσιάζουν έναν επιθετικό σχήμα όπου ο επιτιθέμενος συνυπάρχει στο ίδιο FPGA με τον έτερο χρήστη και επομένως και οι δύο θέτουν σε λειτουργία διάφορα αρθρώματα (modules). Στόχος του επιτιθέμενου σε αυτή την συνθήκη είναι να συλλέξει δείγματα για την διακύμανση της ηλεκτρικής ισχύος στα κυκλώματα TDC (time-to-digital converter) μέσα από αισθητήρες που είναι ενσωματωμένοι επάνω σε ένα voltage chip (*custom built voltage on-chip sensors*).

Όπως και στο προηγούμενο παράδειγμα ο επιτιθέμενος στρέφει την προσοχή του στο buffer πρώτης γραμμής και πιο συγκεκριμένα στο πρώτο στρώμα (first layer) που προορίζεται για εισόδους με raw data. Αυτό που παρατηρεί ο επιτιθέμενος εν σχέσει με την διακύμανση της ισχύος είναι η καθυστέρηση που παρατηρείται (propagation delay) στην λειτουργία του TDC κυκλώματος ανάλογα αν παράγονται pixels για το περίγραμμα (background) ή την σιλουέτα στο κέντρο της εικόνας (foreground), δηλαδή η τάση των βολτ θα διαφέρει ανάλογα αν είναι pixels για το πρώτο ή το δεύτερο (background και foreground αντίστοιχα) . Κατόπιν ο επιτιθέμενος χρησιμοποιώντας HW (Hamming Weights) ,και φίλτρα για την αφαίρεση του θορύβου (noise), καταφέρνει να δημιουργήσει ένα κατώφλι (threshold) ως τον μέσο όρο των καθυστερήσεων στο TDC για να κατανοήσει ποιες καθυστερήσεις συσχετίζονται με τα background pixels και ποιες με τα foreground pixels[480].

[477] Ο.π.

[478] Ο.π.

[479] Ο.π.,σ.19.

[480] Ο.π.

- Cache (Timing) SCAs: έχει ήδη καταστεί σαφές ότι η ετερογένεια και η σταδιακή μετάβαση προς μια πολυλειτουργικότητα κάνουν ώστε τα εφαρμοσμένα συστήματα να καθίστανται όλο και περισσότερο ευάλωτα προς πάσης φύσεως SCAs, ειδικότερα σε αυτή την υποκατηγορία καλούμαστε να μελετήσουμε την δυνατότητα ενός επιτιθέμενου να εκμεταλλευτεί το σημείο σύνδεσης (εν μέρει και οι προηγούμενες παράγραφοι το έκαναν αυτό, εκεί όπου έγινε αναφορά στο line buffer του υλικού) ανάμεσα στο υλικό του εφαρμοσμένου συστήματος και στο λογισμικό που εκτελείται επ' αυτού (το επονομαζόμενο λογικό μέρος, logic part, logic gates κλπ[481]). Εμβαθύνοντας περαιτέρω οι Bossuet και Benhami στο άρθρο τους διερευνούν το σενάριο αξιοποίησης του στοιχείου διεπαφής AXI bus signal για τον επιτυχή σχεδιασμό μιας cache (timing) SCA εκμεταλλευόμενοι το cache coherency που το AXI προσφέρει για να λειτουργήσει σαν ενδιάμεσος κρίκος περάσματος από το υλικό του εφαρμοσμένου συστήματος στο λογικό τμήμα του SoC-FPGA[482].

Υπενθυμίζεται εν τάχει ότι σε μια cache SCA ο επιτιθέμενος αφενός αποσκοπεί στο να διακρίνει αν τα δεδομένα ή οι οδηγίες που αναζητά είναι όντως στο cache, επομένως να μπορεί να διακρίνει ανάμεσα στα hits και τα misses, και αφετέρου να μπορεί να προχωρήσει σε έξωση (evict) των εκάστοτε lines από την μνήμη cache[483]. Η αρχιτεκτονική των σύγχρονων SoC-FPGAs περιλαμβάνει μεταξύ άλλων μια θύρα cache coherency (ACP, accelerator coherency port) που αναλαμβάνει να συνδέσει τις διεπαφές (master interfaces) του υλικού του εφαρμοσμένου συστήματος με το σύστημα της μνήμης cache του λογικού τμήματος του εφαρμοσμένου συστήματος[484]. Στο πλαίσιο αυτής της αρχιτεκτονικής ο επιτιθέμενος ενδιαφέρεται και επικεντρώνει στο AxPort[1] το οποίο είναι ένα bit με βάσει το οποίο ο AXI bus ελέγχει την κατάσταση ασφαλείας (security status) των αιτημάτων που το master interface στέλνει προς το λογικό τμήμα του SoC και με βάσει το οποίο ο AXI bus απορρίπτει μη ασφαλή αιτήματα για να προστατεύσει τις IP. Στόχος του επιτιθέμενου είναι μέσω αυτού του security

[481] Bossuet, L., & Benhani, E.M.(2021). Performing Cache Timing Attacks from the Reconfigurable Part of a Heterogeneous SoC- An Experimental Study. *Applied Sciences*, 11, n.14:6662,1-14,σ.1.DOI: https://doi.org/10.3390/app11146662 . Applied Sciences | Free Full-Text | Performing Cache Timing Attacks from the Reconfigurable Part of a Heterogeneous SoC—An Experimental Study | HTML (mdpi.com) (Τελευταία πρόσβαση 13/09/2021).

[482] Ο.π..σ.13.

[483] Ο.π.,σ.2.

[484] Ο.π.,σ.3.

status bit να ελέγξει τον χρόνο πρόσβασης (access time) στην μνήμη cache και με τον τρόπο αυτό να διακρίνει τα misses και τα hits εντός αυτής[485].

Επί του πρακτέου ο επιτιθέμενος για να διακρίνει τα hits & misses αποστέλλει ένα αίτημα ανάγνωσης (read request) και κατόπιν μετρά τον χρόνο που χρειάζεται για να ολοκληρωθούν δύο χειραψίες , μια για το κανάλι read address και η έτερη για το κανάλι ανάγνωσης των δεδομένων (read data channel). Αντίστοιχα το evict των γραμμών cache λαμβάνει χώρα μέσω ενός write request προς την μνήμη cache L1 που αφαιρεί την γραμμή cache με την διεύθυνση του αιτήματος, αν τα δεδομένα για το εν λόγω αίτημα υπάρχουν εντός του L1 cache την δεδομένη στιγμή[486]. Οι συγγραφείς παρουσιάζουν κατόπιν τρεις επιθέσεις, ήτοι Flush+Reload, Time+Evict, και τέλος μια cache-based επίθεση βασιζόμενη στην ύπαρξη ενός εν κρυπτό καναλιού (cache-based covert channel attack).

Για τις δύο πρώτες επιθέσεις έχει γίνει λόγος στο προηγούμενο κεφάλαιο οπότε η μεθοδολογία τους δεν θα αναφερθεί εκτεταμένα εκ νέου εδώ. Στόχος των δύο επιθέσεων στην συγκεκριμένη πειραματική συνθήκη είναι ο κρυπταλγόριθμος AES-128, όπου καθώς η ενδιάμεση κατάσταση S1 (intermediate state S1) εξαρτάται από το plaintext p και το μυστικό κλειδί k, είναι εφικτό για τον επιτιθέμενο να ανακαλύψει το κλειδί αν έχει γνώση τόσο του byte Pi όσο και των πινάκων αντιστοίχισης (lookup tables) που αξιοποιούνται στην διαδικασία της κρυπτογράφησης. Σημειώνεται εν παρόδω ότι στην πειραματική συνθήκη το master interface έχει μολυνθεί με χρήση ενός hardware trojan ώστε ο επιτιθέμενος να είναι εις θέση να εκμεταλλευτεί καταλλήλως το cache coherency[487].

Και στις δύο επιθέσεις (Flush+Reload, Time+Evict) ακολουθείται και πάλι η λογική της profiling/microarchitectural προσέγγισης ώστε ο επιτιθέμενος να έχει υπολογίσει το κατώφλι (threshold) για την διάκριση ανάμεσα στα hit και miss, και επίσης (για την επίθεση Time+Evict) για την διάκριση ανάμεσα στην εκτέλεση του κρυπταλγόριθμου με ή χωρίς τον πίνακα αντιστοίχισης T_0. Στην περίπτωση της Flush +Reload αρχικά το master interface που έχει μολυνθεί με το hardware Trojan κάνει έξωση (evict) σε μια cache line που περιέχει κάποιο στοιχείο του πίνακα αντιστοίχισης T_0 , κατόπιν η ίδια διεπαφή εκκινεί την διαδικασία κρυπτογράφησης, και τέλος η διεπαφή λαμβάνει το ciphertext και μετά αποστέλλει αίτημα (read request) προς την διεύθυνση που έχει γίνει evict για να διαπιστώσει πόσοι ωρολογιακοί κύκλοι (clock cycles) συμπληρώθηκαν ανάμεσα στις χειραψίες των καναλιών read address και read data.

[485] Ο.π.,σ.6.

[486] Ο.π.,σ.8.

[487] Ο.π, σ.9.

Έχοντας διατυπώσει ένα κατώφλι στην αρχή ο επιτιθέμενος ελέγχει αν ο αριθμός των ωρολογιακών κυκλήσεων είναι κάτω ή πάνω από αυτό, σε περίπτωση που είναι κάτω από το κατώφλι, τότε το ciphertext εμπεριέχει στοιχεία του πίνακα αντιστοίχισης που έγιναν evicted στην αρχή από την master interface[488].

Στην επίθεση Evict+Time η μολυσμένη διεπαφή εκκινεί και πάλι την κρυπτογράφηση με τα στοιχεία του πίνακα αντιστοίχισης, και κατόπιν (κι εδώ υπάρχει διαφορά με την Flush+Reload) γίνεται η φόρτωση μόνο εκείνων της γραμμής cache μόνο με όσα στοιχεία λείπουν για να ολοκληρωθεί η κρυπτογράφηση. Τέλος, το master interface μετρά τον χρόνο από την έναρξη της διαδικασίας κρυπτογράφησης μέχρι την λήψη του ciphertext, και αν ο χρόνος αυτός είναι πάνω από το κατώφλι που έχει οριστεί τότε συνεπάγεται ότι το στοιχείο του πίνακα αντιστοίχισης που έχει γίνει evict έχει ταυτόχρονα χρησιμοποιηθεί και κατά την διαδικασία της κρυπτογράφησης[489].

Στην τελευταία τους παραλλαγή (cache based covert channel attack) οι συγγραφείς υποθέτουν πως υπάρχει ένα εν κρυπτώ κανάλι (covert channel) ανάμεσα σε μια διεργασία που χρησιμοποιεί λογισμικό για επίθεση Flush+Reload (spy process) και στην μολυσμένη με hardware Trojan διεπαφή του κυκλώματος Soc-FPGA. Η επικοινωνία ανάμεσα τους λαμβάνει χώρα σε μια διαμοιρασμένη διεύθυνση μνήμης (shared memory address) που είναι εντός της εξωτερικής μνήμης (external memory[490]).

Η διαδικασία κατάσκοπος μπορεί μόνο να διαβάσει την διεύθυνση αλλά η διεπαφή έχει δικαιώματα τόσο ανάγνωσης όσο και εγγραφής (writeable) επ' αυτής της διεύθυνσης. Η διαδικασία κατάσκοπος (spy process) χρησιμοποιεί έναν αλγόριθμο που εναλλάσσει την κατάσταση αδράνειας (sleep) με την εντολή για flushing της διαμοιρασμένης διεύθυνσης (shared address flushing), δηλαδή για κάθε λογικό 1 και 0 που θα στέλνει η spy process σε μια χρονική περίοδο (π.χ. Time 1), μετά θα δέχεται την εντολή sleep για την αμέσως επόμενη, και αλλαχού. Από την άλλη η διεπαφή μετρά τον χρόνο πρόσβασης στην διαμοιρασμένη διεύθυνση στέλνοντας συνεχή αιτήματα coherent read, και λαμβάνει ένα λογικό 0 ή 1 αν ο αριθμός των misses κατά την διαδικασία flushing είναι μικρός ή αντίστοιχα μεγάλος. Αντίστροφα, ο εντοπισμός ενός cache hit από την διεπαφή σημαίνει κιόλας την απαρχή μιας σειράς από cache misses, δηλαδή ο επιτιθέμενος θα είναι σε θέση να εντοπίσει την διαδοχή των 0 και 1 ανάλογα

[488] Ο.π.,σ.10.

[489] Ο.π.,σ.11.

[490] Ο.π.,σ.12.

το κατώφλι που θα φαίνεται από το λογικό 1 ή 0, και θα μπορεί μέσω της διάκρισης misses και hits να αποκωδικοποιήσει το εκάστοτε ciphertext[491].

Εν κατακλείδι, και σε ότι αφορά τα ενσωματωμένα συστήματα και ως προσθήκη στις τρωτότητες που ήδη έχουν αναφερθεί (απουσία φιλικής προς τον χρήστη διεπαφής, ετερογένεια στα στοιχεία της αρχιτεκτονικής κατασκευής και λειτουργίας των κλπ), μπορούμε να προσθέσουμε αφενός το ότι τα στοιχεία του περιβάλλοντος χώρου (π.χ. θερμότητα, ατμοσφαιρικός αέρας κλπ) δύνανται να υποβοηθήσουν την εκτέλεση των SCAs αυξάνοντας παράλληλα (ίσως μελλοντικά) το εύρος των συνδυασμών και της ευελιξίας του hopping των εκάστοτε επιθέσεων, χωρίς παράλληλα να είναι εύκολο να σχεδιαστούν αντίμετρα που θα περιορίζουν τα περιθώρια ευκαιριών που δίδουν ο χώρος και τα φυσικά φαινόμενα.

Ταυτόχρονα, και με αναφορά στο δίπολο λογισμικό/εφαρμοσμένο σύστημα, παρατηρείται πως ο σχεδιασμός των SCAs λαμβάνει σε αρκετά μεγάλο βαθμό υπόψη την συνδυαστικότητα επιθέσεων (SCA από κοινού με malware, Hardware Trojans κλπ) και επίσης (και εδώ υπόψη πρέπει να ληφθεί η παράμετρος του ανοικτού λογισμικού που ενσωματώνεται σε κυκλώματα κλπ, αν και δεν είναι πάντα ο κανόνας κάτι τέτοιο) την επαύξηση της δυνατότητας που έχουν οι επιτιθέμενοι σε ότι αφορά στην κατασκευή μοντέλων (pre-profiling,microarchticture κλπ) παρόμοιων με τα περιβάλλοντα λογισμικού που θέλουν να παραβιάσουν μέσω μιας SCA. Αυτό συνεπάγεται πως θα μπορούσαν να αυξήσουν την ακρίβεια της επιθέσεως των με το να εκπαιδεύουν τις τεχνικές επιθέσεων πλευρικού καναλιού τους (π.χ. thresholds, templates κλπ) με διάφορα μοντέλα, κι έτσι να καθίστανται γνώστες των συμπεριφορών των attack vectors, κι όπως κατέδειξε και το τελευταίο παράδειγμα, είτε να αυξάνουν την πιθανότητα καταγραφής των εκροών (leakages κλπ) είτε ακόμα και να μπορούν να σχεδιάσουν οι ίδιοι ένα λειτουργικό πλευρικό (π.χ. covert) κανάλι.

SCAs & Αγροτικός Τομέας:

Οι δύο τελευταίες υπό-περιπτώσεις κρίσιμων υποδομών που θα αναφερθούν υπό το πρίσμα της απειλής των SCAs διαφέρουν από τις προηγούμενες, σε ότι αφορά την υπάρχουσα βιβλιογραφία που μελετήθηκε, ως προς δύο στοιχεία κυρίως. Εν πρώτοις, ως προς το ότι το τμήμα της βιβλιογραφίας που τις αφορά είναι μικρότερο σε σχέση με όσες προηγήθηκαν μέχρι τώρα. Εν δευτέροις, το επίπεδο αφαιρετικής αναλύσεως που περιστρέφεται γύρω από αυτές,

[491] Ο.π.

είναι κατά τι, πιο διευρυμένο με αποτέλεσμα να καλύπτει την εκάστοτε κρίσιμη υποδομή (CI) ως σύνολο και όχι μόνο σε ότι αφορά μεμονωμένους attack vectors όπως ανωτέρω.

Το πεδίο στο οποίο γίνεται αναφορά στην συγκεκριμένη περίπτωση, και σε σχέση πάντα με κυβερνοαπειλές όπως οι SCAs, μπορεί να προσδιοριστεί ως *Γεωργία* ή *Καλλιέργεια ακριβείας* (*Precision Farming PF*, *Precision Agriculture PA*[492]). Πρόκειται επί της ουσίας για δύο αρκετά γενικευτικούς ορισμούς που χρησιμοποιούνται αλλαχού και που χρησιμοποιούνται για να περιγράψουν την ολοένα αυξανόμενη αξιοποίηση των πληροφοριακών τεχνολογιών (ICT) και των ευφυών συσκευών (IoT devices, κι εδώ περιλαμβάνονται επομένως και attack vectors, όπως οι αισθητήρες) στην κατεύθυνση της μειούμενης ανθρώπινης παρέμβασης σε ότι αφορά την διαχείριση των υποστηρικτικών προς την καλλιέργεια των χωραφιών στοιχείων (π.χ. ακριβέστερη χρήση λιπασμάτων, μεγαλύτερη ακρίβεια στην διαχείριση των υδάτινων πόρων για τις καλλιέργειες κλπ[493]).

Η σταδιακή μετάβαση μιας σειράς δραστηριοτήτων σχετικών με τον αγροτικό τομέα στο διαδίκτυο (ήτοι η ψηφιοποίηση, digitalization) οδηγεί σχεδόν αναπόδραστα στην αύξηση των δεδομένων των σχετικών με τις καλλιέργειες, στην ενίσχυση του αυτοματισμού, καθώς επίσης και στην επαύξηση της διασύνδεσης μεταξύ συσκευών καθώς και επιχειρήσεων μεταξύ άλλων πραγμάτων[494]. Η εξέλιξη αυτής του σύγχρονου αγροτικού τομέα συντείνει ακόμα στην δραστική αύξηση των απειλών για την κυβερνοασφάλεια όπως είναι η απώλεια δεδομένων και η απειλή έναντι της ακεραιότητας αυτών των τελευταίων[495]. Ενδεικτικά παραδείγματα τέτοιων απειλών για το τρίπτυχο CIA αποτυπώνονται σε ενδεχόμενες περιπτώσεις υποκλοπής δεδομένων (data theft) είτε από τους άμεσα εμπλεκόμενους αγρότες (stakeholders) είτε επειδή οι πλατφόρμες που διατηρούν τα δεδομένα αυτά δεν συμμορφώνονται με τα πρότυπα που υπάρχουν για την εμπιστευτικότητα των δεδομένων αυτών (confidentiality), και επίσης ενδεχόμενη μεταπώληση των εν λόγω δεδομένων που θα ζημίωνε τις επιχειρηματικές δραστηριότητες των αγροτών κοκ[496].

---

[492] Demestichas, K., & Peppes, N., & Alexakis, T.(2020). Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors,* 20(22), 6458,1-17,σ.3. DOI: Sensors | Free Full-Text | Survey on Security Threats in Agricultural IoT and Smart Farming (mdpi.com) . (PDF) Survey on Security Threats in Agricultural IoT and Smart Farming | ResearchGate (Τελευταία πρόσβαση 8/2/2022).

[493] Ο.π.

[494] Ο.π.,σ.3-4.

[495] Ο.π.,σ.4.

[496] Ο.π.,σ.5.

Καθώς το ζήτημα της βελτίωσης των καλλιέργειας βρίσκεται στο επίκεντρο της ψηφιακής μετάβασης του αγροτικού τομέα, προκύπτει από την διαπίστωση αυτή και το ενδεχόμενο ύπαρξης επιπτώσεων σε ότι αφορά τον επισιτισμό του πληθυσμού που θα απορρέουν απευθείας από την επιτυχή διενέργεια κυβερνοεπιθέσεων, συμπεριλαμβανομένων και των SCAs ομολογουμένως. Επί παραδείγματι, και με αναφορά στην ακεραιότητα των δεδομένων (Integrity), το ενδεχόμενο ύπαρξης μιας απάτης σε ότι αφορά την διαδικασία ταυτοποίησης χρήστη (authentication fraud) μπορεί κάλλιστα να επιτρέψει στον επιτιθέμενο να εισάγει ψευδή δεδομένα σε έναν αλγόριθμο μηχανικής μάθησης, κι έτσι να υπάρξει ζημίωση ή και ολοκληρωτική καταστροφή των καλλιεργούμενων βρώσιμων υλών[497].

Ακόμα, σε ότι αφορά στην διαθεσιμότητα των δεδομένων (availability), ενδεικτικά μπορεί να αναφερθεί το ενδεχόμενο διακοπής της παροχής υπηρεσιών λόγω μιας επιτυχούς DoD επιθέσεως, η οποία και θα πλήξει αναπόφευκτα την δυνατότητα παροχής πληροφοριών σε σχεδόν πραγματικό χρόνο (near real-time) που είναι ζωτικής σημασίας για την επιτήρηση και την βελτιστοποίηση των καλλιεργήσιμων εδαφών. Η επιτυχής διενέργεια μιας τέτοιας ενδεχόμενης επίθεσης εύλογα πλήττει όχι μόνο την ομαλή λειτουργία της εφοδιαστικής αλυσίδας (π.χ. αποπροσανατολισμός των δρομολογίων των μη επανδρωμένων πτητικών μέσων που ενδεχομένως να χρησιμοποιούνται σε κάποια αγροτική δραστηριότητα), αλλά παράλληλα (καθώς ο αγροτικό τομέας στις διάφορες εκφάνσεις του είναι μια επιχειρηματική δραστηριότητα) δύναται να πλήξει και την εμπιστοσύνη των εκάστοτε πελατών προς τις αγροτικές επιχειρήσεις, με συνακόλουθη απώλεια εσόδων και αξιοπιστίας[498].

Εν συντομία παρατίθεται εδώ σχηματικά η συνήθης αρχιτεκτονική που απαντάται στην περίπτωση της κρίσιμης υποδομής της καλλιέργειας ακριβείας (PF). Οι Alahmadi et al. περιγράφουν την PF ως έχουσα τέσσερις διαστρωματώσεις (layers), ως ακολούθως:

- Η πρώτη διαστρωμάτωση περιλαμβάνει το σύνολο των αισθητήρων που είναι εγκατεστημένοι και οι οποίοι είναι επιφορτισμένοι με διάφορες λειτουργίες σχετικές με τον περιβάλλοντα χώρο τους κατά ορισμένα χρονικά διαστήματα, όπως η ρύθμιση της παροχής και τα επίπεδα νερού ή το πότισμα των καλλιεργειών. Οι αισθητήρες αυτοί διακρίνονται, όμοια με τις IoT συσκευές και τα εφαρμοσμένα

[497] Ο.π.,σ.5 & 7.

[498] Ο.π.

συστήματα, για το χαμηλό κόστος τους, την συνήθη μονολειτουργικότητα τους και κυρίως για την απουσία επίβλεψης κατά την λειτουργία τους[499].

- Στην δεύτερη διαστρωμάτωση υπάρχουν όλες οι ενδιάμεσες πύλες (gateway layer) που αξιοποιούνται ως σημεία, κυρίως ασύρματης, διεπαφής (interface) ανάμεσα στο διαδίκτυο και στους αισθητήρες καθαυτούς, εδώ δυνητικά περιλαμβάνονται ένα σύνολο πρωτοκόλλων και συσκευών που θα λειτουργούν ως ενδιάμεσοι στην επικοινωνία (συσκευές switch, WiFi, Zigbee, δορυφορικές επικοινωνίες κλπ[500]).
- Στην τρίτη διαστρωμάτωση λαμβάνει χώρα η αποθήκευση και η επεξεργασία των δεδομένων (π.χ. σε περιβάλλον Cloud) που έχουν συλλεχθεί από τους αισθητήρες (storage or processing layer).
- Στην τέταρτη και τελευταία διαστρωμάτωση περιλαμβάνεται το σύνολο των εφαρμογών που χρησιμοποιούν οι εκάστοτε χρήστες (επιστήμονες, αγρότες, επιχειρηματίες, κυβερνητικοί υπάλληλοι κλπ) (application layer) για να ελέγξουν τους αισθητήρες και παράλληλα να αντλήσουν από αυτούς τα διάφορα δεδομένα για τους σκοπούς της αναλύσεως (analytics) και της συνακόλουθης λήψης αποφάσεως[501].

Έχοντας θέσει το γενικότερο πλαίσιο του αγροτικού τομέα ιδωμένου ως κρίσιμης υποδομής (CI), καλούμαστε στην συνέχεια να επικεντρώσουμε στο αντίστοιχο δίπολο SCAs/Αγροτικός τομέας και στις ανάλογες υπό-περιπτώσεις που καταγράφονται σχετικά με αυτό. Ο σύγχρονος αγροτικός/επισιτιστικός τομέας παρουσιάζει, ειδικά εν σχέσει με τις SCAs, μια σειρά από τρωτότητες (τρείς τον αριθμό) που σε μεγάλο βαθμό δικαιολογούν την συνάφεια μεταξύ αυτού και των επιθέσεων που μελετούμε. Οι τρωτότητες (vulnerabilities) αυτές αναφέρονται ακολούθως ως εξής (δεν αναφέρονται εδώ, αλλά παρόλ' αυτά διατηρούν την ισχύ τους, :

- Αρχικά, η ακρίβεια και η βελτιστοποίηση που οι ICT συσκευές δύνανται να προσφέρουν στον αγροτικό/επισιτιστικό τομέα βασίζεται σε μεγάλο βαθμό στην ενσωμάτωση στον τομέα αυτόν αισθητήρων (sensors) ώστε να είναι εφικτή η

[499] Alahmadi, A.N., & Rehman, S.U., & Alhazmi, H.S., & Glynn, D.G., & Shoaib, H., & Sole, P.(2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* 2022, 22, 3520, 1-14, σ.3. DOI: Sensors | Free Full-Text | Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture (mdpi.com) . Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture - PMC (nih.gov) (Τελευταία πρόσβαση 29/9/2022).

[500] Ο.π.

[501] Ο.π.

παρακολούθηση της καλλιέργειας σε πραγματικό χρόνο. Δεδομένης αυτής της παραμέτρου οι SCAs διαφόρων τύπων βρίσκουν πρόσφορο έδαφος για να εκτελεστούν, κι ακόμα αυξάνει, λόγω της ύπαρξης αισθητήρων, δραστικά το εύρος (attack surface[502]) όχι μόνο των πιθανών, μεμονωμένων, επιθέσεων, όσο και εκείνο των δυνατοτήτων συνδυασμού αυτών503.

- Δεύτερον, ο αγροτικός τομέας, σε μεγάλο βαθμό αλλά βεβαίως όχι αποκλειστικά, ευρίσκεται εντός ενός περιβάλλοντος που κατά κύριο λόγο κυριαρχείται από την έντονη παρουσία των φυσικών φαινομένων (π.χ. καιρικές μεταβολές) που εκτός των επιδράσεων που μπορεί να έχουν στις συσκευές ICT & IoT, ταυτόχρονα μπορούν να επιδράσουν πάνω στο πεδίο εμβέλειας και στον σχεδιασμό των SCAs, και ακόμα να δυσχεράνουν την σχεδίαση και εφαρμογή αντιμέτρων όπως έχει ήδη λεχθεί ανωτέρω[504].
- Τρίτον, δεδομένου του μεγέθους και της εκτάσεως του αγροτικού/επισιτιστικού τομέα γίνεται σχεδόν επιβεβλημένη η χρήση διαφόρων εφαρμοσμένων συστημάτων, που εύλογα θα πρέπει (και) να διασυνδέονται (π.χ. networked embedded systems κλπ, ενδεχομένως δε και βαρέα μηχανήματα όχι απλώς ενσωματωμένα κυκλώματα κλπ), δεδομένων των δυσκολιών που αυτά παρουσιάζουν (και που αναφέρθηκαν προηγουμένως), και πάλι η λήψη αντιμέτρων καθίσταται δυσχερείς, αλλά ταυτόχρονα αυξάνει η πιθανότητα ο επιτιθέμενος να μπορεί με μια SCA να διενεργήσει hopping αυξάνοντας την ζημία που θα προκληθεί[505].

Αναφορικά με την αρχιτεκτονική των SCAs που αποτελούν απειλή για την γεωργία στην ψηφιακή εποχή (Digital Agriculture, DigAg.) , οι Alahmadi et al. στο άρθρο τους σημειώνουν πως πρέπει να ληφθούν υπόψη, ευλόγως, όλες εκείνες οι SCAs που απειλούν αισθητήρες και IoT συσκευές για λόγους που έχουν εκτεταμένα αναλυθεί στις δύο προηγούμενες υπό-περιπτώσεις(IoT devices, embedded systems[506]). Κατωτέρω παραθέτουμε ορισμένες ενδεικτικές

---

[502] Για χαρακτηριστικά παραδείγματα με βάσει της λειτουργία IoT συσκευών και αισθητήρων ορά και Alahmadi, A.D., & Rehman, S.U., & Alhazmi, H.S., & Glynn, D.G., & Shoaib, H.,& Sole, P.(2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* 2022, 22, 3520, 1-14,σ.3. DOI:Sensors | Free Full-Text | Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture (mdpi.com) . Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture - PMC (nih.gov) (Τελευταία πρόσβαση 29/9/2022).

[503] Ο.π.,σ.9.

[504] Ενδεικτικά, ο.π.,σ.5.

[505] Ο.π.,σ.4.

[506] Alahmadi, A.D., & Rehman, S.U., & Alhazmi, H.S., & Glynn, D.G., Shoaib, H., & Sole, P.(2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* 2022, 22, 3520, 1-14, σ.6. DOI:

περιπτώσεις επιθέσεων πλευρικού καναλιού που θα μπορούσαν κάλλιστα να στοχεύσουν τον αγροτικό/επισιτιστικό τομέα:

- Microarchitectural SCAs: καθώς η αρχιτεκτονική του PF προϋποθέτει την εγκατάσταση εξοπλισμού σε απομακρυσμένα σημεία και τον εξίσου απομακρυσμένο χειρισμό των συσκευών αυτών, τότε δυνητικά ο επιτιθέμενος (ειδικά αν έβρισκε ,και, φυσική πρόσβαση σε αυτές) θα μπορούσε να προχωρήσει σε μια αντίστροφη μηχανική (reverse engineering) και έχοντας γνώση των μηχανισμών να χρησιμοποιήσει και άλλες τεχνικές για να λάβει τις πληροφορίες που επιθυμεί[507].
- Power Analysis SCAs, Electromagnetic SCAs: όμοια με την προηγούμενη περίπτωση, και με όσα παραδείγματα έχουν αναφερθεί ανωτέρω, ο επιτιθέμενος σε περίπτωση που βρει φυσική πρόσβαση σε κάποια συσκευή εγκατεστημένη στον περιβάλλοντα χώρο θα είναι σε θέση να λάβει μετρήσεις (αλλά και απομακρυσμένα σε άλλες περιπτώσεις) και να εκτελέσει τις εν λόγω επιθέσεις[508].
- Memory Deduplication SCAs: ο επιτιθέμενος , έχοντας και πάλι φυσική πρόσβαση στην εκάστοτε συσκευή, θα μπορούσε να ανακτήσει δείγματα μνήμης (memory traces) και να προχωρήσει σε επίθεση πλευρικού καναλιού αντίστοιχης λογικής[509].

Sensors | Free Full-Text | Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture (mdpi.com) . sensors-22-03520-v4.pdf (Τελευταία πρόσβαση 29/9/2022).

[507] Ο.π.,σ.7.

[508] Ο.π.,σ.7-8.

[509] Ο.π.,σ.8.

- Acoustic SCAs[510]: οι συγγραφείς καταγράφουν εδώ την χρήση hardware bugs ώστε ο επιτιθέμενος να προχωρήσει σε καταγραφή ακουστικών δειγμάτων για παραπέρα ανάλυση αυτών[511].
- Διάφορες περιπτώσεις Cache SCAs (π.χ. page fault exploit, VM duplication κλπ): εδώ η εστίαση αφορά σε περιπτώσεις όπου οι συσκευές που αξιοποιούνται, και που έχουν χαμηλά πρότυπα προστασίας, θα μπορούν να δεχθούν επίθεση είτε εντός του περιβάλλον Cloud (ορά σχετικές περιπτώσεις ανωτέρω) είτε σχετικές με την μνήμη cache και το περιβάλλον εικονικής μηχανής, όπου ενδεχομένως να υπάρχει από πλευράς χρηστών κάποιο multitenancy[512].
- Optical SCAs: εδώ οι συγγραφείς αναφέρουν την πιθανότητα στόχευσης της διεπαφής δικτύου (network interface) μέσω της αξιοποίησης εκροών φωτεινότητας (*LED interface*, *light induction*) για να μπορέσει ο επιτιθέμενος να παρατηρήσει

[510] Επ' αφορμή την ακουστική εκροή (acoustic leakage) δίνεται η ευκαιρία να αναδειχθεί η πολυσχιδής διάσταση του αγροτικού χώρου, σε ότι αφορά το κομμάτι της καλλιέργειας, καθώς επίσης και η δυνατότητα που μια τέτοια ετερογένεια παρέχει σε ότι αφορά στον συνδυασμό ή στην μετεξέλιξη εκροών. Επί παραδείγματι τμήμα του αγροτικού χώρου δεν είναι μόνο το έδαφος, αλλά προφανώς και το υδάτινο στοιχείο σε ότι αφορά φέρ' ειπείν τις ιχθυοκαλλιέργειες. Οι Ahmad et al. αν και δεν κάνουν άμεση αναφορά στις SCAs εντούτοις στο άρθρο τους περιγράφουν το θαλάσσιο περιβάλλον και την δυνάμει αξιοποίηση του ακουστικού στοιχείου για την διενέργεια επιθέσεων έναντι πληθώρας IoT συσκευών που είναι εγκατεστημένες εντός του θαλάσσιου περιβάλλοντος, και που εξαιτίας αυτού υφίστανται δυσχέρειες στην λειτουργία τους, όπως η επιδιόρθωση τους κάτω από το νερό η αλλαγή μπαταρίας κλπ. Περαιτέρω, η ακουστική εκροή θα αλληλοεπιδρούσε με τρόπο διαφορετικό κατά τι σε σχέση για παράδειγμα με τον περιβάλλοντα χώρο των αγροτικών καλλιεργειών, επαναφέροντας το σημείο συζήτησης για την αλληλεπίδραση εκροών και περιβαλλοντικών συνθηκών της προηγούμενης υπό-περίπτωσης (σχετικά με την χρήση παραμετρικών ηχείων κλπ). Σε αυτή την αλληλεπίδραση η ακουστική συγκέντρωση, οι συγγραφείς αναφέρονται γενικά στον ήχο όχι στην εκροή των συσκευών απαραίτητα, σε ένα στρώμα (layer) κάνει ώστε να δημιουργούνται ορισμένες αντανακλάσεις στην επιφάνεια του νερού (ray bending). Η παρατήρηση αυτή αφενός επαναφέρει το ερώτημα αν το πλευρικό κανάλι είναι σχετικό μόνο με ότι σχετίζεται με την εκροή από μια συσκευή ή αν μπορεί να δημιουργηθεί από τον ανθρωπογενή παράγοντα ή το ίδιο το περιβάλλον της συσκευής και αφετέρου αν η εκροή πρέπει να θεωρείται κατά μονάς ή αν αντίθετα μπορεί μέσω hopping, εκμεταλλευόμενη άλλες συσκευές ή την φυσική διαντίδραση του περιβάλλοντος (ray bending), να ενισχυθεί ή να μετατραπεί σε έτερη εκροή που να υποβοηθά ακόμα περισσότερο στην διενέργεια της SCA, έστω δίνοντας πρόσθετες προοπτικές ή διεξόδους στον επιτιθέμενο. Πρβλ. Σχετικά Ahmad, I., & Rahman, T., & Zeb, A., & Khan, I., & Ullah, I., & Hamam, H., & Cheikhrourou, O.(2021). Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks. *Wireless Communications and Mobile Computing,* Vol.2021, Article ID 1444024, 1-15, σ.2 & 4. DOI: https://doi.org/10.1155/2021/1444024 . WCMC_1444024 1..15 (hindawi.com) (Τελευταία πρόσβαση 7/10/2022).

[511] Ο.π.,σ.9.

[512] Ο.π.

ενδεχόμενα μοτίβα λειτουργίας των συσκευών, και άρα να προχωρήσει σε fingerprinting ίσως ενός μέρους ή ολόκληρου του τρόπου λειτουργίας του δικτύου[513].

Εν κατακλείδι, η περίπτωση μελέτης της κρίσιμης υποδομής του αγροτικού χώρου, εκτός του να επιβεβαιώνει τις διαπιστώσεις που έχουν γίνει προηγούμενα (π.χ. ετερογένεια στην αρχιτεκτονική των εκάστοτε χρησιμοποιούμενων συσκευών, απουσία ή μη φιλική προς τον χρήστη διεπαφή, απουσία ή ύπαρξη αστοχιών σε ότι αφορά στην εκπαίδευση του προσωπικού που θα κληθεί να χειριστεί τις εκάστοτε συσκευές), επικεντρώνει την προσοχή των ενδιαφερομένων και σε τρία ακόμα στοιχεία που, αν και έχουν αναφερθεί και αναλυθεί ανωτέρω, μπορούν στην περίπτωση του αγροτικού/επισιτιστικού τομέα να αναδειχθούν σε μεγαλύτερο εύρος, και ίσως υπό έτερη προοπτική.

Πρώτον, εδώ αναδεικνύεται ιδιαίτερα ο ρόλος που διαδραματίζει ο παράγοντας του οικοσυστήματος, δηλαδή του περιβάλλοντος χώρου εντός του οποίου σχεδιάζεται και εφαρμόζεται η αρχιτεκτονική για την ψηφιακή γεωργία. Σχεδόν το σύνολο των συσκευών είναι τοποθετημένο σε απομακρυσμένα σημεία (remoteness, σε ένα αγροτικό περιβάλλον και κυρίως εκτός των ορίων του αστεακού χώρου όπου είναι και το σύνηθες σκηνικό για τα ζητήματα δημιουργίας αντιμέτρων σε ότι αφορά την κυβερνοασφάλεια), και ευρίσκεται σχεδόν καθ' όλη την διάρκεια της ημέρας εκτεθειμένο σε αντίξοες καιρικές συνθήκες ποικίλης εντάσεως[514]. Δεδομένης αυτής της παραμέτρου, δυσχεραίνεται τόσο ο σχεδιασμός αντιμέτρων όσο όμως και η κατανόηση και ορθή μελέτη του ρόλου που διαδραματίζουν τα καιρικά φαινόμενα στην διενέργεια πάσης φύσεως SCAs (π.χ. acoustic, thermal SCAs κλπ), ιδίως αν αναλογιστεί κανείς πως δεν είναι εύκολο στον αγροτικό χώρο να υπάρξει κάποια απομόνωση των φαινομένων αυτών.

Δεύτερον, ένα στοιχείο που διατρέχει οριζοντίως την ετερογενής φύση της αρχιτεκτονικής στην PF είναι αυτό της απομακρυσμένης διαχείρισης (remoteness) των καλλιεργήσιμων εδαφών με την συνεχώς μειούμενη ανθρώπινη παρουσία επί του χώρου. Τέτοιες καταστάσεις μπορούν σε κάποιες περιπτώσεις να συγκλίνουν προς την έλλειψη έγκαιρης παρέμβασης, και από την άλλη να δίνουν στον επιτιθέμενο μια ευκολότερη πρόσβαση (αυτό είναι σημείο προς μελέτη, κι ενδεχομένως δεν ισχύει παντού, αφού είναι πιθανό και τέτοιες περιοχές να φυλάσσονται, ήτοι physical security) που είναι συστατικό στοιχείο για την

[513] Ο.π.

[514] Ο.π.,σ.11.

διενέργεια invasive SCAs, και πάντως εδώ πρόκειται για μια λιγότερο δυσχερή πρόσβαση απ' ότι σε έτερες υποδομές (π.χ. κυβερνητικά γραφεία, εργοστάσια κλπ[515]).

Τρίτον, που σε έναν βαθμό αποτελεί και στόχο (έστω και ακροθιγώς) του επόμενου κεφαλαίου, η ανεπάρκεια και επίσης η δυσχέρεια στην συγκρότηση ενός ολοκληρωμένου πλαισίου για την κυβερνοασφάλεια στην ψηφιακή γεωργία ("*DigAg Cyber-Security Framework*"). Και πάλι εδώ αναφύεται το ζήτημα της ετερογένειας των συσκευών και της εκπαίδευσης του προσωπικού, καθώς επίσης και οι όποιες ειδικές απαιτήσεις που προκύπτουν από τον ιδιάζοντα χώρο στον οποίο θα πρέπει εν μέρει να κινηθεί η κυβερνοασφάλεια, ο οποίος είναι κατά το ήμισυ ίσως αγροτικός και κατά το άλλο μισό αστεακός, διότι μεταβλητές όπως τα καιρικά φαινόμενα δεν έχουν ακόμα μελετηθεί επαρκώς.

Τέλος, εδώ υπεισέρχεται και η μεταβλητή της ετερογένειας των συμβαλλόμενων μερών (stakeholders), καθώς οι εμπλεκόμενοι (π.χ. αγρότες, τεχνικοί, επιχειρηματίες) προέρχονται όχι μόνο από διαφορετικά πεδία, αλλά και από τις πλέον διαφοροποιημένες αγροτικές περιοχές και τομείς. Αυτό σημαίνει πως ο προσπορισμός της γνώσης θα διαφέρει από την μια ομάδα στην άλλη, η προσέγγιση ενδεχομένως στην κυβερνοασφάλεια και τα αντίμετρα το ίδιο, και τέλος το ίδιο θα ισχύσει και σε ότι αφορά την αντίληψη στο εκάστοτε επίπεδο (layer ορθότερα, δηλαδή διαστρωμάτωση) της αρχιτεκτονικής της PF όπως αναπτύχθηκε και ανωτέρω[516].

SCAs & Χρηματοπιστωτικός Τομέας:

Στην προτελευταία αυτή υπό-περίπτωση η εστίαση κινείται γύρω από τα παραδείγματα αφενός των hardware wallets και αφετέρου γύρω από τα κρυπτονομίσματα (cryptocurrencies) όπως το Zcash και το Moreno επί παραδείγματι. Η λογική που διέπει το δίπολο Χρηματοπιστωτικός Τομέας/SCAs διακρίνεται και πάλι από την διαγνωσμένη τάση στην βιβλιογραφία, όπου αφενός οι συγγραφείς επικεντρώνουν γύρω από μια συσκευή ή αλγόριθμο και στο πως η σχέση υλικού-λογισμικού δύναται να υποβοηθήσει στην διενέργεια μιας SCA, και αφετέρου η επιλογή τεχνικών και σχεδιασμού επιθέσεως που θα περιστρέφεται (κυρίως) γύρω από εκροές σχετικές με την κατανάλωση ενέργειας (PA,EM κλπ) και την καταγραφή της χρονικής διάρκειας στην εκτέλεση ενός αλγορίθμου για την επίτευξη της συναλλαγής (π.χ. software based SCAs, time analysis κλπ).

[515] Ο.π.,.σ.9-10.

[516] Ο.π.,σ.10.

Στις ελάχιστες πειραματικές συνθήκες που έγινε κατορθωτό να ανευρεθούν για την υπό-περίπτωση αυτή, οι συγγραφείς εστιάζουν στην διαδικασία της συναλλαγής κρυπτονομισμάτων (cryptocurrency transactions) για να βρουν και να εκμεταλλευτούν καταλλήλως τις διάφορες εκροές (leakages κλπ). Ενδεχομένως, ένα χαρακτηριστικό που μπορεί να προστεθεί στα σχετικά με τις SCAs ερευνώντας τις ηλεκτρονικές συναλλαγές είναι η έννοια του "*cold storage*" , όπου τα μυστικά κλειδιά εντός του hardware wallet βρίσκονται ουσιαστικά σε απομόνωση από τον διαδικτυακό χώρο, είναι δηλαδή μονίμως offline[517].

Αυτή η παρατήρηση προσθέτει μια διαφορετική πτυχή στην ως τώρα ανάλυση, καθώς οι SCAs σε μεγάλο βαθμό μελετιούνται εν σχέση με δικτυωμένες συσκευές (π.χ. IoT) υπό αμελητέα επιτήρηση και σε σχεδόν μόνιμη λειτουργία, αλλά ταυτόχρονα είναι όλο και λιγότερες (στην βιβλιογραφία) οι περιπτώσεις όπου οι SCAs σχεδιάζονται για να επιτεθούν είτε εκτός δικτύου (εδώ με αναφορά κυρίως σε invasive μορφές, αν και όχι κατά τρόπο απόλυτο) είτε σε σε συσκευές που δεν βρίσκονται σε λειτουργία (πρβλ. Την περίπτωση της "*Cold Boot Attack"* που αναφέρεται εν παρόδω στην υποσημείωση 113). Σημειώνεται ακόμα πως εκ νέου , όπως και σε έτερα εφαρμοσμένα συστήματα, ουσιώδη ρόλο στον σχεδιασμό της επιθέσεως αυτής διαδραμάτισε το γεγονός ότι ο κώδικας του Trezor One είναι ανοικτής προέλευσης (open source code), με ότι αυτό συνεπάγεται για τα ζητήματα ασφαλείας που αναφέρθηκαν και ανωτέρω[518].

Κατωτέρω παρατίθενται ορισμένες ενδεικτικές εφαρμογές SCAs έναντι ηλεκτρονικών συναλλαγών:

- Power Analysis/Profile SCAs: στην συγκεκριμένη πειραματική συνθήκη οι San Pedro et al. επιχειρούν να εντοπίσουν το μυστικό PIN ενός hardware wallet στοχεύοντας στο firmware trezor-mcu του πορτοφολιού Trezor One[519]. Η λογική της επιθέσεως τους βασίζεται σε ένα συνδυασμό μια ειδικά τροποποιημένης, για την περίπτωση της πειραματικής συνθήκης, εκδοχής του πορτοφολιού Trezor One (attack vector, εφαρμοσμένο σύστημα επί τις ουσίας) και της συνήθους στρατηγικής που εφαρμόζεται (και την οποία έχουμε ήδη αναλύσει σε έτερες πειραματικές συνθήκες ανωτέρω) στην διενέργεια μιας Power Analysis SCA, ήτοι του διαίρει και βασίλευε

[517]Τονίζεται ότι στις περιπτώσεις που παρουσιάζουν οι συγγραφείς η πτυχή αυτή δεν αναπτύσσεται περαιτέρω αλλά παρόλ' αυτά χρήζει μνείας για την ανάλυση μας. Pedro, M.S., & Servant, V., & Guillement, C.(2019). Side-Channel assessment of Open Source Hardware Wallets. *Cryptology ePrint Archive,* Paper 2019/401, 1-26, σ.2. 401.pdf (iacr.org) (Τελευταία πρόσβαση 2/10/2022).

[518] Ο.π.,σ.24.

[519] Ο.π.,σ.23.

(*divide and conquer*), δηλαδή της ανακάλυψης τμημάτων (bits) του μυστικού κλειδιού ανά ωρολογιακό κύκλο (clock cycle[520]).

Σε αυτή την επίθεση (profiled attack) ο επιτιθέμενος αποστέλλει αιτήματα προς εκτέλεση προς το Trezor One και όσο αυτό τα εκτελεί ο επιτιθέμενος με ένα ψηφιακό παλμογράφο (digital oscilloscope) λαμβάνει δείγματα της κατανάλωσης ισχύος κατά την εκτέλεση των διεργασιών αυτών, χάρις σε ένα resistor που έχει τοποθετηθεί στην συγκεκριμένη συσκευή (harware wallet[521]). Ο αλγόριθμος για τους σκοπούς της επιθέσεως αποτελείται από την βιβλιοθήκη python-trezor από την οποία καλείται στην συνέχεια η εντολή trezorctl για να επικοινωνήσει ο Η/Υ του επιτιθέμενου με το Trezor One[522]. Η λήψη των δειγμάτων ισχύος λαμβάνει χώρα κάθε φορά που στο Trezor One εκτελείται η συνάρτηση storage_containsPin για την επαλήθευση του PIN του χρήστη (και η συνάρτηση storageRom->pin συγκρίνει το PIN με την είσοδο του χρήστη ανά ψηφίο) πριν από την εκτέλεση κάποιας ενέργειας για να δοθεί η έγκριση[523]. Στόχος του επιτιθέμενου είναι μέσα από τις μετρήσεις ισχύος να βρει ένα προς ένα τα ψηφία του PIN καθώς οι εν λόγω συναρτήσεις επιτρέπουν την διάκριση (μέσω της μετρήσεως της ισχύος) ανάμεσα στο κάθε bit του μυστικού κλειδιού (secret) και στην τιμή της εισόδου που έχει δώσει ο χρήστης (differentiability[524]).

Ο εντοπισμός των ψηφίων από τα οποία αποτελείται το PIN γίνεται με τον τρόπο που έχει περιγραφεί ανωτέρω για τις profile/template επιθέσεις, δηλαδή ο επιτιθέμενος συγκροτεί κάποιες κλάσεις δεδομένων (*Discriminant Analysis classifiers*) για να εκπαιδεύσει ένα μοντέλο μηχανικής μάθησης (αλγόριθμο) και κατόπιν εξάγει τον μέσο όρο (mean) του κάθε set , και στην συνέχεια η διακύμανση (variance) του κάθε μέσου όρου συγκρίνεται με την συνολική διακύμανση για όλα τα δείγματα ισχύος από όλα τα sets[525]. Στην συνέχεια το μοντέλο που έχει εκπαιδευθεί από τον επιτιθέμενο χρησιμοποιείται για την εκτέλεση της επίθεσης στην συσκευή στόχο (Trezor One), με νέα δείγματα ισχύος από την συγκεκριμένη να αντλούνται για να συγκριθούν οι είσοδοι προς τον vector με τις τιμές εντός του εκπαιδευμένου classifier, και το τελευταίο να δώσει το ψηφίο με τον υψηλότερο βαθμό συσχέτισης[526].

---

[520] Ο.π.,σ.3.

[521] Ο.π.,σ.4.

[522] Ο.π.,σ.6.

[523] Ο.π.,σ.7.

[524] Ο.π.,σ.8.

[525] Ο.π.,σ.9-10.

[526] Ο.π.,σ.11.

- Timing + Profile SCA: Επιπλέον οι San Pedro et al. Παρουσιάζουν και δεύτερη επίθεση έναντι, αυτή τη φορά, της συνάρτησης scalar multiplication της κρυπτό-βιβλιοθήκης (trezor-crypto) του εν λόγω πορτοφολιού (βιβλιοθήκη ανοικτού κώδικα εν προκειμένω). Η συγκεκριμένη συνάρτηση αξιοποιείται στην κρυπτογραφία ελλειπτικής καμπύλης και περιέχει σημαντικές πληροφορίες, καθώς κατά την δημιουργία του δημόσιου κλειδιού ο scalar multiplication είναι η τιμή του ιδιωτικού κλειδιού (private key), και επίσης στις περιπτώσεις δημιουργίας ψηφιακής υπογραφής (ECDSA signature) ο scalar multiplication λειτουργεί ως το nonce που εσωκλείει την τιμή για το ιδιωτικό κλειδί (private key[527]).

Ο επιτιθέμενος και σε αυτή την παραλλαγή αξιοποιεί την στρατηγική του διαίρει και βασίλευε (*divide and conquer*) επιχειρώντας μέσω λήψης δειγμάτων ισχύος να ανακτήσει ένα προς ένα τα bits του scalar k[528]. Ο επιτιθέμενος για να λάβει της μετρήσεις των δειγμάτων καλεί επανειλημμένα την συνάρτηση point_multiply ενώ η συσκευή στην οποία αυτή εκτελείται παραμένει συνδεδεμένη με ένα resistor κλπ. Αφότου γίνει λήψη των δειγμάτων ακολουθεί ο συγχρονισμός των εκροών (*leakage synchronization,* ενώ διορθώνεται και το jitter για καθένα από αυτά λόγω της ηλεκτρομαγνητικής παρείσφρησης από την λήψη των δειγμάτων), ήτοι η τροποποίηση του κάθε δείγματος προς χάριν ομοιομορφίας[529]. Κατόπιν τούτων, ο επιτιθέμενος συγκροτεί με τα δείγματα τα sets των δεδομένων για την εκπαίδευση του μοντέλου του (profile attack) και την εξαγωγή όπως και πριν των απαραίτητων συσχετίσεων ανάμεσα στις εισόδους και τα secret bits[530].

Στόχος του επιτιθέμενου και κατά την εκπαίδευση και κατά την διενέργεια της επίθεσης του έναντι του vector είναι η ανάκτηση των ενδιάμεσων τιμών (intermediate values) για την αποκάλυψη κάθε bit του scalar k, δηλαδή και πάλι ο εντοπισμός των μέσων όρων και σύγκριση τους. Το νέο στοιχείο εδώ είναι η αξιοποίηση μιας χρονικής εκροής (*timing leakage*) για να υπερκεραστεί το εμπόδιο που θέτει η εκτέλεση της συνάρτησης (point_multiply) σε συνεχή χρόνο (*constant-time execution*) και που σε ορισμένες περιπτώσεις στην βιβλιογραφία προτείνεται ως αντίμετρο (δηλ. Το constant-time execution) έναντι των SCAs[531].

---

[527] Η εν λόγω βιβλιοθήκη αξιοποιείται και από έτερα wallets όπως Keepkey και Archos Safe-T άρα η πειραματική συνθήκη είναι δυνάμει εφαρμόσιμη και σε έτερες περιπτώσεις. Ο.π.,σ.17.

[528] Ο.π.,σ.19.

[529] Ο.π.,σ.19-20.

[530] Ο.π.,σ.20.

[531] Ο.π.,σ.20 & 22.

Η εκροή πληροφοριών σχετικά με τον χρόνο εκτέλεσης (*timing leakage*) εντοπίζεται από τους συγγραφείς σε ένα σημείο ανάμεσα στην λήψη δύο δειγμάτων ισχύος κατά την επανειλημμένη κλήση της συνάρτησης τους (loop[532]), έτσι προκύπτει ότι η κλήση της συνάρτησης conditional_negate που όταν εκτελείται εισάγει ένα XOR (ή αποκλειστικό) και που κάνει ώστε τα δείγματα ισχύος κατά την παραγωγή του XOR να ξεχωρίζουν στο oscilloscope αφού το ένα δείγμα θα πάρει τιμή $f_i(k)=0$ και το επόμενο $f_i(k)=1$, οπότε τα δείγματα θα διακρίνονται ξεκάθαρα διευκολύνοντας τις συσχετίσεις του επιτιθέμενου για την εξαγωγή του ιδιωτικού κλειδιού[533].

- Timing SCAs: Οι Tramer et al. παρουσιάζουν στο άρθρο τους ορισμένες timing SCAs έναντι δύο cryptocurrencies (Zcash & Moreno) για να αποδείξουν ότι είναι εφικτό, μέσα από τέτοιες επιθέσεις, να παραβιαστούν τόσο η μη διασύνδεση των συναλλαγών (transaction unlinkability) όσο και η ανωνυμία των χρηστών (user anonymity), καθόσον όπως οι συγγραφείς παρατηρούν υπάρχει μια έλλειψη συνεχούς χρονικότητας (constant-timeness) στο επίπεδο πρωτοκόλλου (protocol level) την οποία μια SCA δύναται να εκμεταλλευτεί[534], πιο συγκεκριμένα το σημείο εστίασης φαίνεται να είναι το "*το τελευταίο στάδιο του κύκλου ζωής των ανώνυμων συναλλαγών* [...] - *όταν ένα πορτοφόλι διενεργεί νέες συναλλαγές*[535] ".

Το μοντέλο σχεδιασμού της επίθεσης περιλαμβάνει απομακρυσμένες επιθέσεις πλευρικού καναλιού (remote SCAs), χωρίς κάποια κακόβουλη παρέμβαση σε λογισμικό συναλλαγών κρυπτονομισμάτων, καθώς επίσης και τρεις επιτιθέμενους (adversaries), έναν σε επίπεδο δικτύου που παρακολουθεί μη παρεμβατικά το κρυπτογραφημένο traffic ανάμεσα στο πορτοφόλι του χρήστη και μια απομακρυσμένη υπηρεσία, έναν επιτιθέμενο που συμμετέχει στο δίκτυο P2P και έναν τρίτο που ελέγχει απομακρυσμένα ένα P2P node και που παρακολουθεί την επικοινωνία ανάμεσα στο πορτοφόλι του χρήστη και το εν λόγω node[536]. Η γενικότερη στόχευση

[532] Ορά σχήμα 13 , ο.π.,σ.22.

[533] Ο.π.,σ.20-21.

[534] Tramer, F., & Boneh, D., & Paterson, K.G.(2020). *Remote Side-Channel Attacks on Anonymous Transactions.* Paper presented at the proceedings of the 29th USENIX Security Symposium. Virtual Event Venue. August, 12-14, 2739-2756, σ.2741 & 2743.sec20-tramer.pdf (usenix.org) (Τελευταία πρόσβαση 9/2/2022).

[535] Η μετάφραση είναι του συγγραφέως, ο.π.,σ.2742.

[536] Ο.π.

είναι ο εντοπισμός του P2P node που ο χρήστης χρησιμοποιεί κατά την διαδικασία διενέργειας μιας πληρωμής[537].

Οι συγγραφείς προτείνουν δύο στρατηγικές για την εκτέλεση της επιθέσεως, πρώτον την ανάλυση της κίνησης των δεδομένων (traffic analysis) κατά την επικοινωνία ανάμεσα στο πορτοφόλι και το node, εδώ ουσιαστικά ο επιτιθέμενος (είτε αυτός που βρίσκεται στο επίπεδο του δικτύου είτε εκείνος που ελέγχει το απομακρυσμένο node) παρακολουθεί μη παρεμβατικά τις αλλαγές που παρατηρούνται στις συναλλαγές ανάμεσα στο δίπολο wallet-node[538].

Η δεύτερη στρατηγική αφορά στην εξαγωγή πληροφοριών για την συμπεριφορά του πορτοφολιού βασιζόμενη στην διαστρωμάτωση του P2P. Έτσι σε περιπτώσεις co-location πορτοφολιού και του node υπάρχει παρατηρήσιμη εκροή όταν ο χρήστης του εν λόγω node διαντιδρά με απομακρυσμένους έτερους χρήστες που δεν βρίσκονται μαζί του σε κατάσταση co-location, έτσι η αλληλεπίδραση P2P node-remote node είναι ικανή να διαρρεύσει στοιχεία για το πορτοφόλι[539]. Η συλλογή των πληροφοριών που αναζητά ο επιτιθέμενος προκύπτει επομένως από τις χρονικές διακυμάνσεις ως προκύπτουσες από την εκτέλεση αριθμητικών πράξεων. Η χρονική διακύμανση στηρίζεται σε μια αλληλουχία συσχετίσεων ανάμεσα στον χρόνο έκδοσης της απόδειξης (proof time) και στο Hamming Weight του συναλλασσόμενου ποσού κρυπτονομισμάτων, και κατόπιν ανάμεσα στο τελευταίο και στην είσοδο (value) που δίνει ο χρήστης[540].

Στην πειραματική συνθήκη έναντι του κρυπτονομίσματος Zcash οι συγγραφείς εκκινούν εκμεταλλευόμενοι την απουσία απομόνωσης (isolation) ανάμεσα στο πορτοφόλι του χρήστη και το P2P node για να επιχειρήσουν διαρροή πληροφοριών σχετικά με το πρώτο προς ένα απομακρυσμένο P2P node που ελέγχει ο επιτιθέμενος δυνητικά (πρόκειται για την δεύτερη από τις δύο ως άνω στρατηγικές[541]). Οι συγγραφείς δοκιμάζουν έναντι του Zcash δύο παραλλαγές (τις ονομάζουν επιθέσεις *PING & REJECT* αντίστοιχα). Στην περίπτωση της *PING* ο επιτιθέμενος εκμεταλλεύεται το γεγονός ότι το Zcash επεξεργάζεται τα μηνύματα από το P2P node κατά τρόπο σειριακό (serially), έτσι οι χρονομετρήσεις δίνουν σε έναν τρίτο στοιχεία για το είδος της δραστηριότητας ενός node (π.χ. αν ένα node διενεργεί συναλλαγή κλπ[542]).

---

[537]. Ο.π.,σ.2743.

[538] Ο.π.

[539] Ο.π.

[540] Ο.π.,σ.2744.

[541] Ο.π.

[542] Ο.π.,σ.2745.

Η λογική της επιθέσεως είναι πως το Zcash ελέγχει πάντα όταν αποκρυπτογραφεί ένα Note ciphertext αν το τελευταίο είναι έγκυρο, ο έλεγχος αυτό γίνεται με μια συνάρτηση κατακερματισμού Pedersen που ελέγχει την εγκυρότητα, αν αυτή υπάρχει τότε εκτελείται η συνάρτηση TrialDecrypt αλλιώς διακόπτεται, εύλογα το χρονικό διάστημα για την αποκρυπτογράφηση μιας έγκυρης συναλλαγής είναι μεγαλύτερο έναντι μιας μη έγκυρης. Η μέτρηση μιας τέτοιας χρονικής διάρκειας λαμβάνει χώρα με τον επιτιθέμενο που ελέγχει ένα απομακρυσμένο P2P να στέλνει ένα μήνυμα ping προς το Zcash αφότου έχει ξεκινήσει ένα νέο αίτημα συναλλαγής προς το τελευταίο. Καθώς το κρυπτονόμισμα όπως ειπώθηκε επεξεργάζεται σειριακά τις συναλλαγές, καθώς η συναλλαγή εστάλη πρώτη θα έχει προτεραιότητα και μετά θα απαντηθεί η κλήση ping, η ταχύτητα ή η βραδύτητα στην απάντηση της τελευταίας φανερώνει αν η προηγηθείσα συναλλαγή ήταν έγκυρη ή μη, και άρα αν το node που την απέστειλε είναι ο payee αυτής ή όχι[543].

Ο επιτιθέμενος ξεκινά με μια κλήση ping που ακολουθεί ένα αίτημα συναλλαγής από τα πριν μη έγκυρο, αυτό του επιτρέπει να δημιουργήσει μια χρονική baseline με βάσει την οποία θα πραγματοποιεί συγκρίσεις μεταξύ αυτής και του χρονικού ορίου επόμενων αιτημάτων συναλλαγής. Παρενθετικά οι συγγραφείς πρότειναν ως σημείο βελτίωσης της επίθεσης ο επιτιθέμενος να λαμβάνει μετρήσεις και όταν αποστέλλεται ένα αίτημα συναλλαγής κατά μονάς και όταν το αίτημα είναι εντός ενός block συναλλαγών, διότι έτσι παρατηρήθηκε πως μειώνεται η διακύμανση εντός του δικτύου και οι μετρήσεις γίνονται πιο έγκυρες[544].

Η επίθεση *REJECT* διέπετε από την λογική της απόρριψης (reject message) ενός μη έγκυρου μηνύματος για εκκίνηση συναλλαγής που στέλνει το P2P node του επιτιθέμενου (malformed transaction). Έτσι όταν ένα τέτοιο αίτημα περιέχει σφάλμα στο version byte η συνάρτηση TrialDecrypt αναλαμβάνει την αντίστοιχη διαχείρισης εξαίρεσης (exception), η τελευταία εμφανίζεται στο νήμα επεξεργασίας των κυρίων μηνυμάτων του πελάτη που έχει στείλει το αίτημα (main message-processing thread), το οποίο με την σειρά του σημαίνει πως όποιος συμμετείχε στην αποστολή του αιτήματος θα λάβει το reject message. Έτσι ο επιτιθέμενος έχει πρόσβαση στο μήνυμα που αφορά την εξαίρεση και μέσω του P2P είναι σαν να αποκτά ένα oracle που θα του επιτρέψει δυνητικά να ελέγχει την αποκρυπτογράφηση του Note έχοντας ξεκινήσει από την αποστολή ενός malformed plaintext[545].

[543] Ο.π.,σ.2745-2746.

[544] Ο.π.,σ.2746.

[545] Ο.π.

Αυτή η επίθεση μπορεί ακόμη να χρησιμέψει για να διαπιστωθεί με ποιο node συνδέεται ένα δημόσιο κλειδί, ο επιτιθέμενος αρκεί να συγκροτήσει ένα plaintext που να περιέχει το λανθασμένο byte και να το κρυπτογραφήσει με το κλειδί του και εν συνεχεία να το εντάξει στην συναλλαγή, κατόπιν αυτή θα αποσταλεί σε όλα τα άλλα P2P nodes και ο επιτιθέμενος θα χρειαστεί μόνο να ελέγξει ποιο από αυτά του επιστρέφει το reject message (ενδεχομένως να απαιτηθούν αρκετές προσπάθειες εδώ, διότι αν ο peer που θα λάβει το malformed ciphertext κάνει relay προς έναν payee, τότε ο τελευταίος θα στείλει μεν ένα reject message πίσω, αλλά όχι στον επιτιθέμενο παρά στον peer που έκανε το relay, κι έτσι ο επιτιθέμενος δεν θα λάβει τίποτα[546]).

Οι συγγραφείς παρουσιάζουν και επιθετικά σχήματα για το Moreno, που είναι μια διαφορετική περίπτωση καθώς οι clients εδώ προχωρούν σε διαχωρισμό ανάμεσα στο πορτοφόλι και τα P2P στοιχεία και τα ενσωματώνουν σε διαφορετικές διαδικασίες[547]. Στην περίπτωση του δίπολου wallet-P2P node του Moreno έχει παρατηρηθεί πως η εκροή συνδέεται με τα συγκεκριμένα διαστήματα κατά τα οποία το πορτοφόλι ανανεώνεται (refresh) στο τέλος μιας συναλλαγής, συγκεκριμένα το πορτοφόλι κάνει sleep στο τέλος κάθε ανανέωσης κι έτσι το πότε αυτό θα στείλει μια νέα συναλλαγή θα εξαρτηθεί από το πόσο χρόνο χρειάστηκε για να ολοκληρώσει μια συναλλαγή κατά το χρονικό διάστημα της προηγούμενης ανανέωσης[548]. Έτσι ένας τρόπος για να λάβει ο επιτιθέμενος πληροφορίες είναι δυνητικά να συγκρίνει τις καθυστερήσεις/χρονικές διαφοροποιήσεις ανάμεσα σε δύο συναλλαγές, όπου στην μια δεν υφίσταται πληρωμή ενώ στην άλλη το πορτοφόλι που εμπλέκεται όντως ολοκληρώνει μια πληρωμή, οι χρόνοι sleep για αυτές τις δύο περιπτώσεις αναμένεται να διαφέρουν σε βαθμό διακριτό[549].

Σε περίπτωση που στο Moreno το πορτοφόλι και το P2P node συνυπάρχουν (co-location) τότε ο επιτιθέμενος (P2P adversary) μπορεί να δοκιμάσει να στείλει ένα get_objects message αφότου το co-located node του χρήστη έχει πράξει το ίδιο. Καθώς ένα τέτοιο μήνυμα έχει ως επακόλουθο το node να λαμβάνει στο mempool του ένα global lock, το ίδιο κι ο επιτιθέμενος επομένως, έτσι υφίσταται η πιθανότητα να υπάρξει ένα lock contention κατά την επεξεργασία του αιτήματος συναλλαγής (για το αν το αίτημα είναι έγκυρο ή μη), διότι μόνο όταν η συναλλαγή έχει πιστοποιηθεί ως έγκυρη το lock αφαιρείται, έτσι προκύπτει μια χρονική καθυστέρηση όταν

[546] Ο.π.,σ.2747.

[547] Ο.π.,σ.2748.

[548] Ο.π.,σ.2750.

[549] Ο.π.

υπάρχουν, για παράδειγμα, δύο lock που έχουν σταλεί. Μέσα από την παρατήρηση του εύρους της καθυστέρησης στην απάντηση του αιτήματος (ο επιτιθέμενος είναι προτιμότερο να στέλνει αιτήματα για μη υπαρκτές συναλλαγές ώστε να αποφύγει τον κίνδυνο κλειδώματος του αιτήματος του πορτοφολιού) μπορεί να γίνει αντιληπτό αν πρόκειται ή όχι για αίτημα πληρωμή προς το πορτοφόλι στόχο[550].

Πέρα από την παρατήρηση χρονοκαθυστερήσεων στην έγκριση αιτημάτων συναλλαγών, ανάλογες συσχετίσεις υφίστανται και σε ότι αφορά το δίπολο του χρηματικού μεγέθους της συναλλαγής (transaction amount) και του χρόνου που χρειάζεται για την δημιουργία της απόδειξης (proof time). Πρόκειται εδώ για στοχοποίηση ενός cryptographic primitive, συγκεκριμένα των ορισμάτων (arguments) succint zero-knowledge (zkSNARKs), και οι συγγραφείς παρατηρούν πως μια timing attack εκμεταλλευόμενη τα ορίσματα αυτά είναι εφικτή μόνο για το Zcash και όχι τόσο αποτελεσματική για το Moreno[551]. Με βάσει τα ορίσματα αυτά οι συγγραφείς παρατηρούν πως ο χρόνο δημιουργίας μιας απόδειξης (proof time) συσχετίζεται με τον αριθμό των στοιχείων πεδίου που είναι μη μηδενικά (non-zero) για τον prover's witness. Καθώς οι συναλλαγές λαμβάνουν χώρα στο δυαδικό σύστημα, το Hamming Weight της συναλλαγής θα επηρεάζει τον χρόνο δημιουργίας της απόδειξης. Αυτή η συσχέτιση HW-δυαδικού συστήματος μπορεί να διαρρεύσει στοιχεία για το μέγεθος της συναλλαγής επομένως, καθώς η δυαδική αναπαράσταση συνδέεται με τις τιμές (values) που περιλαμβάνονται σε κάθε ποσό συναλλαγής[552].

Αν και η παραπάνω περίπτωση δεν είναι εφαρμόσιμη για το Moreno, το τελευταίο έχει μια ακόμα χρονική εκροή που μπορεί να παρατηρηθεί και που αφορά το CLI wallet του. Σε αυτή την περίπτωση όταν ο χρήστης θέλει να πάρει το κλειδί για να εκκινήσει μια συναλλαγή, το CLI wallet του ζητά να εισάγει τον κωδικό χρήστη (user password). Αυτή η ταυτοποίηση χρήστη μέσω κωδικού λαμβάνει χώρα κάθε που ο χρήστης επιχειρεί με το κλειδί του να στείλει αιτήματα για την δημιουργία νέων transaction blocks, το CLI διακόπτει στην περίπτωση αυτή κάθε ανανέωση και ροή νέων αιτημάτων προς το καινούργιο block μέχρι ο χρήστης να ανταποκριθεί βάζοντας τον κωδικό του και μέχρι το CLI να ελέγξει την ορθότητα αυτού. Αυτή η χρονοτριβή σε ότι αφορά την ανανέωση είναι φυσικά παρατηρήσιμη από έναν adversary που βρίσκεται σε

[550] Ο.π.

[551] Ο.π.,σ.2751.

[552] Ο.π.,σ.2752.

κάποιο απομακρυσμένο node και δυνητικά του επιτρέπει να εντοπίσει το node που επιχειρεί να ολοκληρώσει μια συναλλαγή[553].

- Electromagnetic SCAs: Σε αυτό το παράδειγμα εκ νέου υποδεικνύεται το κενό ασφαλείας που προκύπτει από την ετερογένεια των εφαρμοσμένων συστημάτων και την πιθανή ύπαρξη στην αγορά hardware wallets διαφορετικών αρχιτεκτονικών στην κατασκευή hardware (το Trezor One επί παραδείγματι έχει δύο κουμπιά και μια μικρή οθόνη[554], ενώ ο attack vector του συγκεκριμένου παραδείγματος, ο Ledger Blue έχει σχήμα ευφυούς τηλεφώνου και οθόνη αφής[555]) καθώς και ετερογενών καταστάσεων σε ότι αφορά την υποστήριξη που λαμβάνουν από κατασκευαστές[556].

Οι Roth et al. Παρουσίασαν την πειραματική τους συνθήκη όπου η SCA τους στόχευε έναντι ενός hardware wallet τύπου Ledger Blue[557]. Οι συγγραφείς παρατήρησαν ότι το πάτημα πλήκτρων (για τον σχηματισμό του PIN) στην οθόνη αφής του εν λόγω πορτοφολιού προκαλεί κάθε φορά μια ηλεκτρομαγνητική εκροή (RF) της τάξης των 169 MHz η οποία μπορεί να συλλεχθεί με την χρήση ενός πομποδέκτη (receiver) τύπου RTL-SDR για περαιτέρω ανάλυση. Μια κεραία τοποθετημένη περί τα δύο μέτρα μακριά από την συσκευή μπορεί να συλλέξει τα RF δείγματα, ενώ επίσης παρατηρήθηκε πως η σύνδεση του πορτοφολιού με καλώδιο USB αυξάνει το εύρος της εκροής[558]. Κατόπιν οι συγγραφείς χρησιμοποιούν τα συλλεχθέντα δείγματα για να εκπαιδεύσουν ένα νευρωνικό δίκτυο ως template για την μετέπειτα διεξαγωγή της επίθεσης, επίσης χρησιμοποιήθηκε μια συσκευή arduino ως τεχνητός button pusher για να συλλεχθούν περισσότερα δείγματα σε μικρότερο χρόνο[559].

---

[553] Ο.π.,σ.2756.

[554] Ο.π.,σ.3.

[555] Maloney,D.(2019). Side-Channel Attacks shows vulnerabilities of cryptocurrency wallets. *Hackaday*. Side-Channel Attack Shows Vulnerabilities Of Cryptocurrency Wallets | Hackaday (Τελευταία πρόσβαση 3/10/2022).

[556] Ο.π.

[557] Τα αποτελέσματα παρουσιάστηκαν στο συνέδριο 35C3 και υπάρχουν διαθέσιμα στον δικτυακό τόπο Wallet.Fail, ονομαστικά οι συγγραφείς είναι οι ακόλουθοι τρεις, Roth, T., & Datko, J., & Nedospasov,D., για μια αναλυτική παρουσίαση της επιθέσεως τους ορά και Roth, T., & Datko, J., & Nedospasov,D.(2018). Using TensorFlow/ machine learning for automated RF side –channel attack classification. *Leveldown.* Using TensorFlow / machine learning for automated RF side-channel attack classification :: Security for the embedded and connected world (leveldown.de) (Τελευταία πρόσβαση 3/10/2022).

[558] Ο.π.

[559] Ο.π.

Οι συγγραφείς για να προετοιμάσουν και να καθαρίσουν τα δείγματα από τον θόρυβο (noise) χρησιμοποιούν κάποιο φίλτρο bandpass ώστε τα δείγματα του νευρωνικού δικτύου να είναι πιο εύκολα διακρίσιμα και να διευκολύνουν έτσι την εκπαίδευση. Στην συνέχεια με την χρήση της πλατφόρμας Tensorflow οι συγγραφείς χρησιμοποιούν δύο set δεδομένων για την εκπαίδευση του δικτύου τους, ενδεικτικά το πρώτο set (training data) για την εκπαίδευση του δικτύου και το δεύτερο (test data) για δοκιμή μετά την ολοκλήρωση της εκπαίδευσης. Το δίκτυο διαθέτει τρεις διαστρωματώσεις (Flatten layer, Dense Layer με την συνάρτηση ενεργοποίησης Rectified Linear Unit (ReLU), και Dense Layer που περιλαμβάνει την συνάρτηση ενεργοποίησης SoftMax), στην συνέχεια οι συγγραφείς εκπαιδεύουν το δίκτυο τους, ενώ έχουν προηγουμένως χρησιμοποιήσει το AdamOptimizer για να καθορίσουν τα επίπεδα επιδόσεως του δικτύου τους (loss function, metrics κλπ[560]).

Τέλος οι συγγραφείς εισάγουν ένα άλλο set δεδομένων παρμένων από τον attack vector στο νευρωνικό τους δίκτυο και το τελευταίο τους επιστρέφει, με βάσεις τους μέσους όρους όπως διατυπώθηκε και ανωτέρω, το ποσοστό της πιθανότητας αντιστοίχισης ανάμεσα στην ηλεκτρομαγνητική εκροή και το πλήκτρο από το οποίο αυτή απορρέει[561].

Εν κατακλείδι, για την υπό-περίπτωση του χρηματοπιστωτικού τομέας (πιο συγκεκριμένα για τα κρυπτονομίσματα και τα hardware wallets), προκύπτει ότι οι SCAs εδώ (πέρα από τις γνωστές παρατηρήσεις που έχουν αναφερθεί αλλού και που επίσης αφορούν τα εφαρμοσμένα συστήματα) μπορούν να έχουν εφαρμογή επί συσκευών που είναι ακόμα και μονίμως offline (π.χ. TrezorOne, cold boot κλπ), παρά το ότι η σύγχρονη τάση στην βιβλιογραφία είναι οι περισσότερο δικτυοκεντρικές (networked) απομακρυσμένες SCAs (remote, non-invasive κλπ), κάτι που υποδεικνύει ότι οι invasive & semi-invasive τεχνικές δεν πρέπει να αμελούνται σε ότι αφορά την μελέτη και τον σχεδιασμό αντιμέτρων. Και επίσης προκύπτει ακόμα από την εν λόγω υπό-περίπτωση ότι η εκτέλεση των SCAs παραμένει εφικτή και αποτελεσματική ακόμα και σε περιβάλλοντα λειτουργίας που διακρίνονται από constant-timeness (περίπτωση πάλι του TrezorOne).

Καταδεικνύοντας έτσι κενά ασφαλείας (security gaps) ακόμα και όταν η πλατφόρμα των συναλλαγών διακρίνεται από privacy by design (π.χ. Blockchain για τις ανταλλαγές κρυπτονομισμάτων), ενώ το αντίστοιχο hardware που συνδέεται με αυτή χαρακτηρίζεται από ετερογένεια στην αρχιτεκτονική κατασκευής του και επίσης από ανοικτότητα (άρα και προσβασιμότητα) στον κώδικα του (π.χ. TrezorOne κλπ).

[560] Ο.π.

[561] Ο.π.

Ολοκληρώνοντας το παρόν κεφάλαιο, και έχοντας αισίως πραγματευτεί την περιγραφή τόσο του ορισμού της Κρίσιμης Υποδομής (CI) όσο και σε σχέση με μελέτες-περιπτώσεως που αφορούσαν την διενέργεια ποικίλων επιθέσεων πλευρικού καναλιού (SCAs), καλούμαστε να προχωρήσουμε σε μια συνοπτική διατύπωση συμπερασμάτων σχετικών με τα ευρήματα της (βιβλιογραφικής) ερευνητικής μας δραστηριότητος καθώς και με τα όποια κενά (gaps) παρατηρήθηκαν. Τα πορίσματα της βιβλιογραφικής ανασκοπήσεως που διενεργήθηκε μπορούν να αποτυπωθούν ως ακολούθως:

- Εν πρώτοις, οι περιπτώσεις που παρουσιάστηκαν στην βιβλιογραφία σχεδόν εξ΄ ολοκλήρου αντανακλούν ένα επίπεδο ανάλυσης πλησίον αυτού του εκάστοτε attack vector (εδώ όπου εστιάζει σχεδόν εξ' ολοκλήρου η παρούσα διπλωματική εργασία, ήτοι στις IoT συσκευές & στα εφαρμοσμένα συστήματα)[562]. Αυτή η προσέγγιση στις πειραματικές συνθήκες και την βιβλιογραφική ανασκόπηση ανάγει το δίπολο των SCAs και των κρίσιμων υποδομών σε ένα , τρόπον τινά, μικρό-επίπεδο που δεν αναλύει (ίσως και διότι οι κρίσιμες υποδομές συχνά περιλαμβάνουν ευαίσθητες και διαβαθμισμένες πληροφορίες και οι εγκαταστάσεις τους δεν είναι εύκολα προσβάσιμες) και ούτε εύκολα μπορεί να αναχθεί σε ένα ανώτερο επίπεδο αφαίρεσης, για ασφαλέστερη εξαγωγή συμπερασμάτων. Σε αυτή την δυσκολία προστίθεται και το γεγονός ότι ο ορισμός που δίνεται για τις CIs είναι εξίσου γενικώς και συγκεχυμένος με το αντίστοιχο εγχείρημα για τις SCAs, με αποτέλεσμα να μην προσδιορίζονται εύκολα και τα όρια των CI assets που πρέπει να προστατευτούν, αφού δυνάμει σχεδόν τα πιο ετερογενή στοιχεία χαρακτηρίζονται ως κρίσιμη υποδομή (υπηρεσίες, εργοστάσια, γραφεία, γεωργικοί χώροι κλπ).
- Εν δευτέροις, η βιβλιογραφία, όπως παρατηρήθηκε και σε προηγούμενο κεφάλαιο, δεν κατανέμεται ομοιόμορφα ούτε ισόποσα εν σχέση με τις κρίσιμες υποδομές που χρησιμοποιούνται ως παραδείγματα. Έτσι ορισμένες υποδομές όπως ο αγροτικός

[562] Σε αυτό κατατείνουν για παράδειγμα και οι Mao et al. όταν διερευνούν στο άρθρο τους τα αντίμετρα που σχετίζονται με τις Microarchitectural attacks και αποφαίνονται πως η επιφάνεια επιθέσεως ("*attack surface*") για τις εν λόγω SCAs είναι τόσο εκτεταμένη που δεν είναι , προς ώρας, εφικτό να σχεδιαστούν μηχανισμοί πρόληψης ("*prevention mechanisms*") που να καλύπτουν επακριβώς την επιφάνεια αυτή. Ορά σχετικά Mao, Y., & Migliore, V., & Nicomette, V.(2022). MATANA: A Reconfigurable Framework for Runtime Attack Detection Based on the Analysis of Microarchitectural Signals. *Applied Sciences* 2022,12,1452,1-22,σ.2.DOI: https://doi.org/10.3390/app12031452. (PDF) MATANA: A Reconfigurable Framework for Runtime Attack Detection Based on the Analysis of Microarchitectural Signals (researchgate.net) (Τελευταία πρόσβαση 9/10/2022).

τομέας, οι χρηματοπιστωτικές συναλλαγές (σε πρώτη γραμμή τα κρυπτονομίσματα), τα αυτοκινούμενα οχήματα, ο ιατροφαρμακευτικός τομέας, έχουν περισσότερα παραδείγματα που έστω έμμεσα μπορούν να αναχθούν σε μελέτες ευρύτερου περιεχομένου που θα καλύπτουν το φάσμα της υποδομής μέσα στην οποία εντοπίζονται (έστω και αν κάτι τέτοιο μόνο πρωτόλεια και αφαιρετικά εμφανίζεται στην βιβλιογραφία ακόμα). Ενώ έτερες υποδομές , όπως οι υπηρεσίες γραφείου και γενικά οι βιομηχανικοί κλάδοι, δεν έχουν παραδείγματα που να ανάγονται σε ευρύτερα επίπεδα και κυρίως αναφέρονται σε IoT συσκευές και εφαρμοσμένα συστήματα (embedded systems) με κάποια πειραματική συνθήκη ως μελέτη-περίπτωσης κλπ[563].

Αυτή η άνιση κατανομή των βιβλιογραφικών αναφορών, και του ερευνητικού ενδιαφέροντος, κάνει ώστε ορισμένες πτυχές της έρευνας (πέραν της γενικεύσεως που αναφέρθηκε στο πρώτο σημείο) να αναφύονται μόνο ακροθιγώς. Ορισμένα τέτοια σημεία που παρατηρήθηκαν είναι η σπανιότητα περιπτώσεων-μελέτης όπου θα αναζητείται η ύπαρξη και δυνατότητα καταγραφής εκροής ενόσω η συσκευή δεν θα είναι σε λειτουργία (π.χ. cold booted). Οι περιπτώσεις μελέτης που επίσης σπανίζουν αφορούν σε μια ολιστική μελέτη των παραγόντων του περιβάλλοντος χώρου που υποβοηθούν την διενέργεια μιας SCA, και η οποία μελέτη θα μπορεί να επεκταθεί τόσο στην μελέτη του υλικού χώρου όσο και των φυσικών φαινομένων ει δυνατόν (ατμοσφαιρικός αέρας κλπ). Επιπρόσθετα, παρατηρείται κενό σε ότι αφορά στην μελέτη της σύνδεσης ανάμεσα στις SCAs και στα βιομετρικά-συμπεριφοριστικά στοιχεία του ανθρώπινου δυναμικού στις CIs που μόνο εν παρόδω έχουν μελετηθεί στο πλαίσιο της μιας ή της άλλης πειραματικής συνθήκης που περιλαμβάνει έναν ή περισσότερους attack vectors.

- Εν τρίτοις, όταν οι πειραματικές συνθήκες εφαρμογής των SCAs ιδωθούν υπό το πρίσμα των εκάστοτε attack vectors (αυτοκινούμενα οχήματα, IoT συσκευές, εφαρμοσμένα συστήματα, λογισμικό ανοικτού κώδικα) τίθεται εν τέλει το ζήτημα

[563] όπως ορθά παρατηρούν σε άρθρο τους οι Real & Salvador, όταν εξετάζοντας τις SCAs έναντι νευρωνικών δικτύων καταγράφοντας εν τέλει την προβληματική της κλιμάκωσης και της γενίκευσης (scalability, genericity), καθότι πολλά τέτοια παραδείγματα επιθέσεων είναι προσαρμοσμένα στο να λειτουργούν μόνο σε σχέση με συγκεκριμένους στόχους και με ορισμένες σχεδιαστικές επιλογές, δίχως να διερευνώνται πολλές φορές έτερες παραλλαγές. Πρβλ. Real, M.M., & Salvador, R.(2021). Physical Side-Channel Attacks on Embedded Neural Networks:A Survey. *Applied Sciences*, 11, 6790, 1-25, σ.21-22.DOI: Applied Sciences | Free Full-Text | Physical Side-Channel Attacks on Embedded Neural Networks: A Survey (mdpi.com). [2110.11290v1] Physical Side-Channel Attacks on Embedded Neural Networks: A Survey (arxiv.org) (Τελευταία πρόσβαση 16/9/2021).

της γενικεύσεως των αποτελεσμάτων των πειραμάτων αυτών[564][565]. Με τον όρο γενικευσιμότητα στις πραγματικές συνθήκες των CIs εννοούμε κατά βάση δύο σημεία, αφενός την ποικιλία vectors και εργασιακών συνθηκών που πολύ δύσκολα επιτρέπουν την αναπαραγωγή ενός ελεγχόμενου περιβάλλοντος πειραματικής συνθήκης[566].

Αφετέρου, αναφερόμαστε ακόμα στην ετερογένεια όχι μόνο των vectors αλλά και των κατασκευαστών αυτών των τελευταίων, και επομένως των κατασκευαστικών προτύπων (standards) που διέπουν την αρχιτεκτονική λογισμικού και υλικού. Αυτή η κατασκευαστική ετερογένεια, εκτός του να δυσχεραίνει το security by design, κάνει ώστε οι πειραματικές συνθήκες εφαρμογής των εκάστοτε SCAs να μην μπορεί να γενικευτεί αφού οι τελευταίες σε κάποιες περιπτώσεις (π.χ. εκεί που έγινε λόγος για πληκτρολόγια) διαφοροποιούν την δυνατότητα εκμετάλλευσης της εκροής ακόμα και όταν υπάρχουν μικρές αλλαγές, όπως η υφή του υλικού κατασκευής του vector.

Ενώ σε κάποιες άλλες η ετερογένεια που αποτρέπει την γενίκευση των αποτελεσμάτων αφορά στην διασύνδεση συσκευών ή υλικού και λογισμικού με διαφορετικά επίπεδα προστασίας το καθένα (όπως φάνηκε για τα hardware wallets στο τελευταίο

---

[564] Στην ίδια παρατήρηση προχωρούν και οι Delarea & Oren όταν καταδεικνύουν ένα κενό στην βιβλιογραφία που η δική τους έρευνα επί των fault injection attacks επιχειρεί να καλύψει και που σχετίζεται με την εφαρμογή τέτοιων πειραματικών συνθηκών κι εκτός εργαστηρίου. Πρβλ. Delarea, S., & Oren, Y.(2022). Practical, Low-Cost Fault Injection Attacks on Personal Smart Devices. *Applied Sciences* 2022, 12, 417,1-10, σ.2. DOI:https://doi.org/10.3390/app12010417. Applied Sciences | Free Full-Text | Practical, Low-Cost Fault Injection Attacks on Personal Smart Devices (mdpi.com) (Τελευταία πρόσβαση 8/10/2022).

[565] Περιγράφοντας έτερες περιπτώσεις εφαρμογών οι Delarea & Oren οδηγούνται σε παρόμοιο συμπέρασμα, καταλήγοντας ότι ”*Ενώ το να διενεργεί κανείς μια φυσική επίθεση όπως οι FI κατά τρόπο απομακρυσμένο είναι κάτι το ισχυρό, ο επιτιθέμενος θα πρέπει να υπερκεράσει προκλήσεις μηχανολογικής φύσεως, μα και επίσης να είναι σε θέση να προσαρμόσει την κακόβουλη FRU ώστε να ταιριάζει στις συγκεκριμένες ευφυές συσκευές; καθώς η κακόβουλη FRU είναι πανίσχυρη, ο πρώτιστος περιορισμός της είναι πως πρέπει να είναι κομμένη και ραμμένη στα μέτρα της συγκεκριμένης συσκευής στόχου”* (η μετάφραση είναι του συγγραφέως). Ο.π.,σ.9.

[566]Αναφορικά με το σημείο αυτό πρβλ. και σχετική παρατήρηση για τα FRUs(hardware field replaceable units) τα οποία σύμφωνα και με τους Delarea & Oren αποτελούν μια εν πολλοίς διευρυμένη και μη ρυθμισμένη (μέσω κοινών προτύπων) αγορά, και το αποτέλεσμα αυτών των δύο χαρακτηριστικών είναι , σύμφωνα και με τους Shwartz et al., ”[...] *η ηθελημένη ή ακούσια πιθανή ενσωμάτωση κακόβουλων ή παραχαραγμένων εξαρτημάτων μέσα σε , κατ’ τ’ άλλα, ασφαλείς συσκευές*” (η μετάφραση είναι του συγγραφέως, ο οποίος διατυπώνει παρόμοια παρατήρηση μέσω της δικής του βιβλιογραφικής έρευνας αμέσως κατωτέρω στην επόμενη παράγραφο). Ορά σχετικά, ο.π., σ.1-2.

παράδειγμα, ή για τα networked εφαρμοσμένα συστήματα ανωτέρω). Έτσι προκύπτει το ερώτημα, αν η SCA από μόνη της είναι απειλή (risk) ή αν η έλλειψη ομοιογένειας στην αρχιτεκτονική των attack vectors ενδυναμώνει τις SCAs ως στοιχείο απειλής.

Τέλος, δε τέταρτον, κάποιες πειραματικές συνθήκες (όχι όμως όλες) είναι συνδυαστικές (π.χ. μόλυνση κινητής συσκευής με κάποιο malware και κατόπιν εκτέλεση της SCA κλπ), εδώ προκύπτει ένα κενό σχετικά με το αν η αλληλουχία των επιθέσεων είναι που συντελεί στην ισχύ των SCAs ή αν οι SCAs καθαυτές μπορούν κατά μονάς να σταθούν ως απειλές έναντι των CIs. Αν για παράδειγμα το malware εντοπιστεί και αφαιρεθεί από κάποιο πρόγραμμα anti-virus ή αν καταστεί ανέφικτο να τοποθετηθεί μια συσκευή για την λήψη δειγμάτων εκροών από , φέρ' ειπείν, έναν insider (εκ των ένδον απειλή) τότε ίσως η SCA να μην είναι δυνατό να εκτελεστεί, και άρα να μην χρειάζεται τα αντίμετρα να επικεντρωθούν σε αυτή παρά στο προηγούμενο βήμα.

Αλλά και αντιστρόφως, αν εκκινήσουμε από την SCA καθαυτή (αδιάφορο εδώ αν προηγείται άλλη επίθεση ή όχι) τότε πάλι υφίσταται ένα κενό αναφορικά με το αν η απειλή έγκειται κυρίως στην εκτέλεση αυτής της τελευταίας, ή αν η απειλή προκύπτει (ή έστω ενισχύεται ουσιαστικά) από τον συνδυασμό της εκάστοτε SCA με παράγοντες που ενισχύουν την εμβέλεια της, είτε δηλαδή συνδυασμός δύο SCAs ή συνδυασμός SCA και περιβαλλοντικών παραγόντων (π.χ. αντανακλάσεων) που κάνουν ώστε η επίθεση να φτάνει στον στόχο της. Το τέταρτο και τελευταίο κεφάλαιο της ανά χείρας διπλωματικής εργασίας επικεντρώνει αποκλειστικά στην ταξινομητική ανάλυση των αντιμέτρων που υφίστανται έναντι των επιθέσεων πλευρικού καναλιού.

Κεφάλαιο 4ο : Ταξινομητικό εγχείρημα περί αντιμέτρων έναντι των Επιθέσεων Πλευρικού Καναλιού (SCAs)

Στο τέταρτο και τελευταίο κεφάλαιο του ανά χείρας πονήματος καλούμαστε να διερευνήσουμε και να παρουσιάσουμε μια σειρά αντιμέτρων (countermeasures) που διατυπώθηκαν και αναλύθηκαν στο τμήμα της βιβλιογραφίας που μελετήθηκε για τους σκοπούς της παρούσας διπλωματικής εργασίας. Δεδομένης της πληθώρας των αντιμέτρων αυτών αλλά και της δεδομένα μικρής έκτασης του εν λόγω κεφαλαίου, το τελευταίο αυτό θα επιχειρηθεί να οργανωθεί με τέτοιο τρόπο ώστε να επιτευχθούν οι δύο κάτωθι στόχοι :

- Εν πρώτοις, λόγω του πλήθους των αντιμέτρων που έχουν κατά καιρούς προταθεί και αναλυθεί στην σχετική επιστημονική βιβλιογραφία, κρίνεται χρήσιμο να υπάρξει αφενός μια δειγματοληπτική παράθεση αυτών, ώστε να σχηματισθεί μια ως το δυνατόν περισσότερο κατατοπιστική εικόνα αυτών, και αφετέρου η παράθεση τους να γίνει εν είδει ταξινόμησης (ή ταξινομήσεων των αντιμέτρων κατά SCAs, αλλά και των ίδιων των SCAs ως δυνητικών τρόπων άμυνας), ώστε η τελευταία να γίνει περισσότερο εύληπτη όσο και να αναδειχθούν επιμέρους πτυχές κατά την ανάλυση που ακολουθεί σε ότι αφορά το Διαδίκτυο των Πραγμάτων (IoT[567]).

[567] Να σημειωθεί εν παρόδω εδώ πως όταν ο λόγος γίνεται για τα αντίμετρα πρέπει να ληφθεί υπόψη και η διαχωριστική γραμμή ανάμεσα σε τρία στοιχεία που συνήθως θεωρούνται όλα μαζί όταν γίνεται αναφορά στον όρο ”αντίμετρα” (countermeasures), και ίσως εξαιτίας αυτής της διαφαινόμενης τάσης να μπορούν να προκληθούν κάλλιστα και συγχύσεις. Το πρώτο στοιχείο προς διάκριση είναι τα αντίμετρα καθαυτά, ότι δηλαδή αποτελεί στοιχείο σχεδιασμού, το δεύτερο στοιχείο αφορά στην χρήση των SCAs καθαυτών ως δυνητικών αντιμέτρων (forensics), και τέλος το τρίτο στοιχείο συνδέεται με τους περιορισμούς που υφίστανται κατά τον σχεδιασμό και την εκτέλεση των εκάστοτε SCAs. Το τελευταίο αυτό στοιχείο δεν είναι βέβαια αντίμετρο με την παραδοσιακή έννοια του όρου, αλλά καθώς τα αντίμετρα στοιχίζουν σε πόρους και γι’ αυτό πρέπει οι CIs να λάβουν υπόψη τους το μέγεθος της απειλής (risks), κρίνεται σκόπιμο να υπάρχει μια σαφής διάκριση ανάμεσα στην αποτελεσματικότητα των μέτρων και στους περιορισμούς του επιτιθέμενου (ακόμα και σε πειραματικές συνθήκες), καθώς και η σχετική αρθρογραφία κάνει τέτοιες νύξεις περιστασιακά, παρά και τις τεχνολογικές προόδους (π.χ. μηχανική μάθηση, εξοπλισμός) που συν τω χρόνω καθιστούν πιο αποτελεσματικές και προσιτές τις SCAs, χωρίς όμως να άρουν όλους τους δυνάμει περιορισμούς.

- Εν δευτέροις, έχοντας ολοκληρώσει την σταχυολόγηση και ανάλυση των αντιμέτρων για το τμήμα της βιβλιογραφίας που μελετήθηκε, στο παρόν κεφάλαιο θα επιχειρηθεί μια συνοπτική διατύπωση περί της στρατηγικής (εν είδει οδηγού ή κατευθυντήριων γραμμών κλπ) που θα μπορούσε μια κρίσιμη υποδομή να αναπτύξει για το προσωπικό και τις διάφορες IoT συσκευές της, ώστε να τα προστατεύσει και τα δύο κατά τρόπο αποτελεσματικό.

Υπό-ενότητα 4.1: Συνοπτική Παρουσίαση Αντιμέτρων έναντι επιθέσεων πλευρικού καναλιού (SCAs), εγχείρημα περί της ταξινόμησης

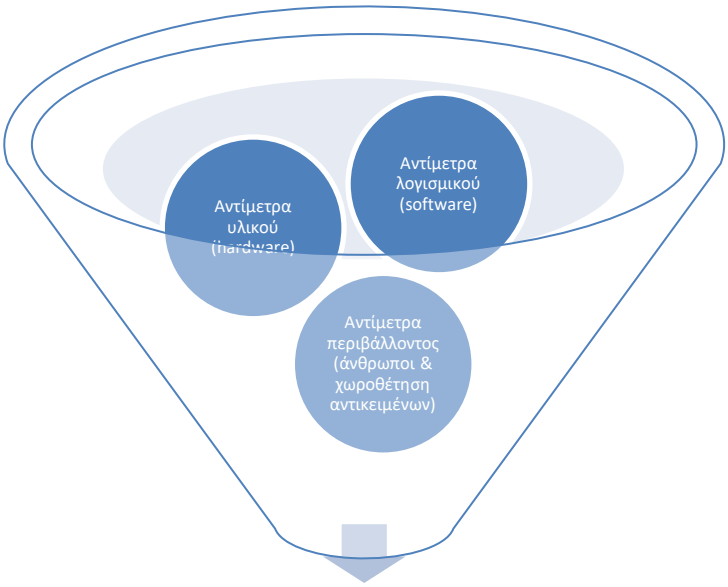
Όπως ήδη έχει αναφερθεί τα αντίμετρα πρέπει να γίνονται αντιληπτά είτε ως η λήψη μέτρων κατά των απειλών των επιθέσεων πλευρικού καναλιού (SCAs) είτε ως η χρήση των αυτών (αρχιτεκτονικών) επιθέσεων για αμυντικούς/προστατευτικούς σκοπούς (π.χ. forensics) που όμως αποτελεί προς ώρας ένα αντικείμενο που έχει μελετηθεί πολύ λιγότερο στην επιστημονική βιβλιογραφία εν σχέσει με την πρώτη περίπτωση. Σε κάθε περίπτωση η έννοια της λήψης των οποιονδήποτε αντιμέτρων αποσκοπεί στην μείωση τόσο της τρωτότητας (vulnerability) όσο και της απειλής (threat) σε ανεκτά, ήτοι διαχειρίσιμα, για την οποιαδήποτε κρίσιμη υποδομή (CIs) επίπεδα. Τούτων δοθέντων, παρακάτω ακολουθεί το εγχείρημα ταξινόμησης των αντιμέτρων για την καλύτερη κατανόηση των πτυχών μιας αμυντικής στρατηγικής έναντι των πάσης φύσεως SCAs.

- Αναφορικά με την μελετηθήσα βιβλιογραφία τα αντίμετρα θα μπορούσε να λεχθεί ότι αναπτύσσονται κατά μήκος τριών αξόνων, ήτοι το υλικό, το λογισμικό, και τέλος ο περιβάλλοντας χώρος(ως στοιχείο του οποίου θα συμπεριληφθεί και ο ανθρώπινος παράγοντας).
- Με βάσει τα όσα μέχρι τώρα έχουν μελετηθεί η παρουσίαση των αντιμέτρων στις ως άνω κατηγορίες θα λάβει χώρα λαμβάνοντας υπόψη το είδος των αντιμέτρων σε καθένα από τους τρεις άξονες, αφενός διότι ο χώρος δεν επαρκεί για να λάβει χώρα η αντίστροφη ανάλυση (ήτοι με βάσει την εκάστοτε επίθεση ή τον εκάστοτε attack vector), και αφετέρου διότι σε αρκετές περιπτώσεις τα αντίμετρα κάθε άξονα μπορεί να συμπίπτουν για περισσότερους του ενός attack vectors ή για περισσότερες της μιας επιθέσεως, και έτσι θα αποφευχθούν αλληλοεπικαλύψεις (overlapping) που θα καθιστούσαν δυσνόητη την ανάγνωση του εν λόγω κεφαλαίου.

- Περαιτέρω, όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, έτσι κι εδώ τα αντίμετρα που θα παρουσιαστούν/αναλυθούν δεν καλύπτουν το σύνολο της μιας ή της άλλης κρίσιμης υποδομής (CI), αλλά αντίθετα κινούνται σε ένα πιο ειδικό επίπεδο ανάλυσης (όπως και πριν, πρόκειται για εκείνο των μεμονωμένων συσκευών IoT κυρίως). Για τον λόγο αυτό δεν φαίνεται να μπορεί να προσφέρει ιδιαίτερη εμβάθυνση η περιγραφή αντιμέτρων ανά vector, καθώς θα είναι εν τέλει αποσπασματική.
- Έχει ιδιαίτερη σημασία να αναφερθεί εδώ πως η καταγραφή των αντιμέτρων, και σε μεγάλο βαθμό αυτό ίσχυσε και στην καταγραφή των επιμέρους επιθέσεων, όποια και όσα από αυτά μπορούν εδώ να συμπεριληφθούν πρέπει να κινείται με γνώμονα αφενός την ταξινόμηση για το τμήμα του υλικού ή του λογισμικού που πρέπει να προστατευτεί, καθώς δεν μπορεί το κάθε αντίμετρο να προστατέψει όλες τις IoT συσκευές μιας υποδομής[568], και αφετέρου τον τρόπο της προσέγγισης του επιτιθέμενου που χρησιμοποιεί μια SCA, καθώς το αντίμετρο θα κληθεί να προσαρμοστεί σε αυτή, ιδίως στις περιπτώσεις που (όπως π.χ. σε ενσωματωμένα συστήματα πολλές φορές) η λογική της ασφάλειας (security) και της ιδιωτικότητας (privacy) δεν γίνεται βάσει αρχικού σχεδιασμού (by design[569]).

[568] "*Επί παραδείγματι, μπορεί να βρεθούμε εις περιβάλλοντα IoT όπου να μην είμαστε εις θέση να υπερβούμε έναν ορισμένο προϋπολογισμό περιοχής ή ισχύος, ή μπορεί απλά να βρεθούμε σε ένα σενάριο όπου τα υψηλότερα επίπεδα ασφαλείας να μπαίνουν στο στόχαστρο, ασχέτως του κόστους του σχετιζόμενου με τα αντίμετρα αυτά"* (η μετάφραση είναι του συγγραφέως). Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28, σ.2. DOI: https://doi.org10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks | HTML (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[569] Ορά χαρακτηριστικά το συμπέρασμα των Ambrose et al. Ambrose, J.A., & Ragel, R.G., & Jayasinghe, D., & Li, T., & Parameswaran, S.(2015). *Side Channel Attacks in Embedded Systems: A Tale of Hostilities and Deterrence*. Paper presented at the 16th Symposium on Quality Electronic Design. Santa Clara, SA, USA. March, 02-04, 1-9, σ.9. DOI: 10.1109/ISQED.2015.7085468. (PDF) Side channel attacks in embedded systems: A tale of hostilities and deterrence (researchgate.net) (Τελευταία πρόσβαση 14/10/2021).



Διάγραμμα 1. *Σχηματική Παρουσίαση Ταξινόμησης Αντιμέτρων έναντι των SCAs*

Σε αρκετές περιπτώσεις όπου παρουσιάζονται αντίμετρα (και για την εναργέστερη κατανόηση μπορούμε να θεωρήσουμε το κάθε αντίμετρο χωριστά από τα άλλα, χωρίς δηλαδή τα αντίμετρα να συνδυάζονται κλπ) η λογική αντιμετώπισης μιας SCA είναι να αποσυνδεθεί η εκροή από την πληροφορία που μπορεί να δώσει στον επιτιθέμενο[570][571], δηλαδή να μην μπορεί

[570] Σε έναν παρόμοιο ορισμό προχωρούν και οι Bache & Guneysu συζητώντας τα αντίμετρα τύπου masking (για τα εν λόγω ορά περισσότερα κατωτέρω), αναφέροντας τα εξής "*εδώ, η σχέση ανάμεσα στα ευαίσθητα δεδομένα και την επίθεση πλευρικού καναλιού επισκιάζεται μέσω της αφαίρεσης των συσχετίσεων* (ενν.dependencies) *ανάμεσα στα δύο ως ένα συγκεκριμένο βαθμό. Σε ένα d-th masking σχήμα, οι ευαίσθητες τιμές διαιρούνται σε πολλαπλά τμήματα (τουλάχιστον d+1) και ένας επιτιθέμενος για να θεωρηθεί πως πέτυχε στην επίθεση του θα πρέπει να συνδυάσει πληροφορίες από τουλάχιστον d+1 τμήματα στα οποία έχουν κατατμηθεί οι τιμές για να μπορέσει να συναγάγει πληροφορίες για μια αρχική τιμή. Καθώς η μέτρηση από μια φυσική επίθεση πλευρικού καναλιού* (ενν.physical side-channel attack) *τείνει να εισάγει κάποιο θόρυβο, η περιπλοκότητα των επιθέσεων έτσι αυξάνεται εκθετικά μέσω της χρήσης του masking υπό τις πλέον πρακτικές συνθήκες"* (η μετάφραση είναι του συγγραφέως). Πρβλ. Bache, F., & Guneysu, T.(2022). Boolean Masking for Arithmetic Additions at Arbitrary Order in Hardware. *Applied Science*s 2022, 12, 2274, 1-14, σ.3. DOI: https://doi.org/10.3390/app12052274. Applied Sciences | Free Full-Text | Boolean Masking for Arithmetic Additions at Arbitrary Order in Hardware (mdpi.com) (Τελευταία πρόσβαση 12/10/2022).

[571] Οι Fadaeinia et al. αναφέρουν χαρακτηριστικά πως "*τα παραδοσιακά αντίμετρα έναντι των επιθέσεων πλευρικού καναλιού, σχεδιάζονταν πρωτίστως για να καταλύσουν την δυναμική συμπεριφορά της διαρροής*". Fadaeinia, B., & Moos,T., & Moradi,A.(2021). Balancing the Leakage Currents in Nanometer CMOS Logic- A

ο τελευταίος να προχωρήσει σε ουσιώδεις συσχετίσεις (correlations) και άρα να διακρίνει με βεβαιότητα (στατιστική τοιαύτη λόγω των μετρήσεων στις οποίες προχωρούν οι αλγόριθμοι μηχανικής μάθησης που εκπαιδεύει ο επιτιθέμενος) ανάμεσα στις διάφορες καταστάσεις λειτουργίας (π.χ. μετρήσεις ισχύος, καταγραφή δονήσεων κατά την πληκτρολόγηση) και εκτέλεσης εργασιών (π.χ. πρόσβαση χρήστη σε μια γραμμή της μνήμης cache[572]).

Υπό μια ταξινομητική προοπτική τα αντίμετρα που οι εκάστοτε συγγραφείς παρουσιάζουν εύλογα ταξινομούνται με διαφορετικούς τρόπους, όμως ενδεχόμενα η πρωταρχική διάκριση μπορεί να γίνει ανάμεσα σε αντίμετρα που ευθύς εξ' αρχής σχεδιάζονται με γνώμονα την ασφάλεια (security by design[573][574]) και σε εκείνα που απλώς έρχονται εκ των υστέρων να διορθώσουν την ευπάθεια (σαν security patches[575]).

Challenge Goal. Applied Sciences 2021, 11 (15), 7143, 1-18,σ.1. doi: https://doi.org/10.3390/app11157143. Applied Sciences | Free Full-Text | Balancing the Leakage Currents in Nanometer CMOS Logic—A Challenging Goal (mdpi.com) (Τελευταία πρόσβαση 1/10/2022).

[572] Πρβλ. Τους Perez et al. όταν αναφέρονται στα S-Boxes και τις κρυπτογραφικές τους ιδιότητες οι οποίες προστατεύουν έναντι επιθέσεων όπως οι Power Analysis SCAs. Τα δύο αυτά στοιχεία είναι η μη γραμμικότητα (nonlinearity) που μοιράζονται ως κοινό στοιχείο τα S-Boxes της ίδιας κλάσης κάθε φορά, και επίσης ο συντελεστής διακύμανσης της συγχύσεως (Confusion Coefficient Variance, CCV), που είναι συνεχείς (constant) πάλι μέσα σε κάθε κλάση. Ορά σχετικά Legon-Perez, C.M., & Sanchez-Muina, R., & Miyares-Moreno, D., & Bardaji-Lopez, Y., Martinez-Diaz, I., Rojas, O., Sosa-Gomez, G.(2021). Search-Space Reduction for S-Boxes Resilient to Power Attacks. *Applied Sciences* 2021, 11, 4815,1-20, σ.9. DOI: https://doi.org/10.3390/app11114815. Applied Sciences | Free Full-Text | Search-Space Reduction for S-Boxes Resilient to Power Attacks (mdpi.com) (Τελευταία πρόσβαση 28/9/2022).

[573] Για τις δυσχέρειες ενός τέτοιου εγχειρήματος, και ειδικά σε σχέση με μια κατηγορία SCAs, ορά σχετικά μεταξύ άλλων και την υποσημείωση 548 που αναφέρεται στο πόνημα των Mao et al. για τον σχεδιασμό αντιμέτρων κατά των Microarchitectural SCAs.

[574] Αυτό τονίζουν ομοίως και οι Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez,C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12, 2390, 1-28, σ.22. DOI:https://doi.org.10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks | HTML (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[575] "*Παρόλο που οι HPCs* (Hardware Event Counters) *δεν έχουν σχεδιαστεί με γνώμονα την ασφάλεια, υφίσταται μια εναργής χρήση των HPCs για εντοπισμό μικροαρχιτεκτονικών επιθέσεων σε διάφορα πονήματα έρευνας από την στιγμή που αυτοί είναι εύκολα προσβάσιμοι από το λογισμικό*". Mao, Y., & Migliore, V., & Nicomette, V.(2022). MATANA: A Reconfigurable Framework for Runtime Attack Detection Based on the Analysis of Microarchitectural Signals. *Applied Sciences* 2022, 12, 1452, 1-22, σ.3. DOI:https://doi.org/10.3390/app12031452. Applied Sciences | Free Full-Text | MATANA: A Reconfigurable Framework for Runtime Attack Detection Based on the Analysis of Microarchitectural Signals (mdpi.com) (Τελευταία πρόσβαση 9/10/2022).

Σε δεύτερο επίπεδο, και ως απόρροια της προηγούμενης διάκρισης, υπάρχει η δυνατότητα να ταξινομηθούν τα μέτρα ως προς την περιπλοκότητα και την διαθεσιμότητα του προϋπολογισμού (budget) που η εκάστοτε κρίσιμη υποδομή μπορεί να αντέξει[576]. Αυτή η διάκριση, σε μεγάλο βαθμό αλλά ίσως όχι ολοκληρωτικά δεδομένης και της τεχνολογικής προόδου, εφάπτεται με την διάκριση ανάμεσα σε αντίμετρα υλικού (hardware) και λογισμικού (software) που είναι και η βασική διάταξη του παρόντος κεφαλαίου[577].

Το κόστος και η περιπλοκότητα, αν και φαντάζουν ως εύλογα στοιχεία, πέρα του να σκιαγραφούν τις δυνατότητες μιας υποδομής στον σχεδιασμό και την εφαρμογή αντιμέτρων, αναδεικνύουν επιπλέον μια , όχι και τόσο, εμφανή διάσταση. Πρόκειται για το σκέλος που αφορά την αθέλητη πρόκληση ή μεγέθυνση μιας εκροής (αυτό που σε προηγούμενο κεφάλαιο αναφέρθηκε και μελετήθηκε ως unintended, και υπενθυμίζετε ότι ο όρος δεν είναι ελεύθερος συγχύσεων) που αυξήθηκε ακριβώς επειδή εφαρμόστηκε κάποιο αντίμετρο, ή επειδή εφαρμόστηκαν γενικά αλλαγές σε κάποιο τεχνολογικό προϊόν. Επί παραδείγματι οι Fadaeinia et al. αναλύοντας έναν μηχανισμό προστασίας(Balanced Static Power Logic, BSPL) των CMOS, παρατηρούν πως η προοδευτική σμίκρυνση των CMOS εφαρμοσμένων συστημάτων (περνώντας στην κλίμακα των νανομέτρων πλέον, nm) αυξάνει την εκροή ειδικά για εκείνες τις εφαρμογές που απαιτούν χαμηλή ισχύ αναμονής (low standby power), καθιστώντας επιτακτική την χρήση αντιμέτρων όπως το BSPL[578].

---

[576] Επί παραδείγματι, η χρήση εργαλείων για την αξιοποίηση των πλευρικών καναλιών (ως αντίμετρα αυτή τη φορά, ορά κατωτέρω για περισσότερες πληροφορίες σχετικά) ενέχει κάποιος σχετικό κόστος. Οι Ibrahim et al. παρουσιάζουν ένα αντίμετρο για τον εντοπισμό ψεύτικων usbs μέσω μετρήσεων των ηλεκτρομαγνητικών τους εκροών (EM emmissions), η λήψη των συγκεκριμένων δεδομένων από τις εκροές γίνεται μέσω μιας κεραίας HackRF one SDR,που είναι σχετικά φθηνότερη λύση, ενώ οι συγγραφείς χρησιμοποιούν επίσης την εναλλακτική της χρήσης ενός αναλυτή σήματος και φάσματος τύπου Rohde & Schwarz, ο οποίος καίτοι αξιόπιστος παραμένει μια πιο ακριβή εναλλακτική εν σχέσει με την κεραία SDR. Πρβλ. Liu, H., & Spolaor, R., & Turrin, F., & Bonafede, R., & Conti, M.(2021). USB powered devices: A survey of side-channel threats and countermeasures. *High-Confidence Computing 1 (2021),* 10007, 1-12, σ.9. DOI: 10.1016/j.hcc.2021.100007. USB powered devices: A survey of side-channel threats and countermeasures - ScienceDirect (Τελευταία πρόσβαση 28/10/2022).

[577] Delarea, S., & Oren, Y.(2022). Practical, Low-Cost Fault Injection Attacks on Personal Smart Devices. *Applied Sciences* 2022, 12, 417,1-10, σ.8. DOI: https://doi.org/10.3390/app12010417. Applied Sciences | Free Full-Text | Practical, Low-Cost Fault Injection Attacks on Personal Smart Devices (mdpi.com) (Τελευταία πρόσβαση 8/10/2022).

[578] Fadaeinia, B., & Moos, T., & Moradi, A.(2021). Balancing the Leakage Currents in Nanometer CMOS Logic-A Challenging Goal. *Applied Sciences* 2021, 11, 7143, 1-18, σ.1. DOI: https://doi.org/10.3390/app1157143. Applied Sciences | Free Full-Text | Balancing the Leakage Currents in Nanometer CMOS Logic—A Challenging Goal | HTML (mdpi.com) (Τελευταία πρόσβαση 1/10/2022).

Από την άλλη, η εφαρμογή του BSPL, στόχος του οποίου είναι να δημιουργήσει κυκλώματα με μια συνεχιζόμενη στατικότητα στις εκροές (static leakages) τους ώστε αυτές να μην αυξομειώνονται ανάλογα με τα δεδομένα που τα κυκλώματα επεξεργάζονται και άρα ο επιτιθέμενος να μην μπορεί να προβεί σε συσχετίσεις επ' αυτών, επί των εν λόγω semi-conductors κάνει ώστε το αντίμετρο αυτό να μην είναι αποτελεσματικό, μεταξύ άλλων, για λόγους ασυμβατότητας μεγεθών στους εκάστοτε semi-conductors αυτούς (ήτοι scalability). Αυτό γίνεται διότι, μεταξύ άλλων, όσο μικραίνει το μέγεθος των CMOS (π.χ. λιγότερο από 100 nm) τόσο αυξάνει η εκροή των πυλών των εν λόγω εφαρμοσμένων συστημάτων (gate leakages), διότι μειώνεται και το πάχος των οξειδίων (oxide thickness) που περιλαμβάνει το περίβλημα (coating). Έτσι προκύπτει μια ασυμβατότητα ανάμεσα στο μέγεθος και την αρχιτεκτονική (π.χ. οι NMOS και PMOS transistors που έχουν διαφορετικά bulk voltages πρέπει να διέρχονται από την ίδια πύλη σε ότι αφορά το BSPL) των CMOS και στην δυνατότητα ακριβούς προσαρμογής του αντίμετρου BSPL στα εκάστοτε μεγέθη αυτά[579].

Αποτέλεσμα αυτών των ασυμφωνιών είναι να προκύπτουν δυσχέρειες στον by design σχεδιασμό του αντίμετρου BSPL, όπως η αύξηση του latency & energy overhead, η ανάγκη για περισσότερο χώρο εντός του transistor ώστε να σχεδιαστεί και εφαρμοστεί το BSPL που ταυτόχρονα αυξάνει τον βαθμό περιπλοκότητας στην κατασκευή και χωροθέτηση του δικτύου (layout), και επίσης η αδυναμία προσαρμογής που προκύπτει από το ότι το BSPL το ίδιο σχεδιάστηκε αρχικά για CMOS μεγαλύτερου μεγέθους (π.χ. 180 nm[580]). Έτσι, εδώ το αντίμετρο αφενός δυσχεραίνει τον σχεδιασμό και το κόστος του συστήματος και αφετέρου μπορεί λόγω ασυμβατότητας να επιτρέψει στον επιτιθέμενο να διενεργήσει μια SCA αξιοποιώντας την αρχιτεκτονική του εκάστοτε αντιμέτρου.

Σε τρίτο επίπεδο, αν και ενδεχομένως μια τέτοια διάκριση δεν παρατηρείται ευρέως στην υπάρχουσα βιβλιογραφία, η ταξινόμηση μπορεί να διακρίνει ανάμεσα στην χρήση παραδεδεγμένων αντιμέτρων κατά των SCAs και επίσης στην χρήση των ίδιων των SCAs ως δυνάμει επιλογών σε ότι αφορά στα forensics. Για την τελευταία πτυχή δεν υπάρχουν, ή η δική μας έρευνα δεν απέφερε, μεγάλο αριθμό ευρημάτων, αλλά μπορεί να παρατεθεί το άρθρο των Sayakkara & et al. όπου επιχειρείτε η ανάδειξη της σημασίας των EM SCAs για την διαδικασία των forensics.

Οι συγγραφείς τονίζουν μια σειρά από τρόπους με τους οποίους θα μπορούσαν να αξιοποιηθούν οι ηλεκτρομαγνητικές επιθέσεις πλευρικού καναλιού, μεταξύ αυτών και η

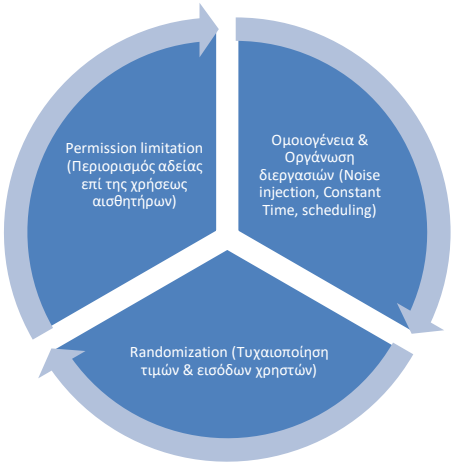
[579] Ο.π.,σ.5.

[580] Ο.π.

αξιοποίηση των ηλεκτρομαγνητικών εκροών στο πεδίο που αφορά το profiling των αρχείων ενός υπολογιστή επί παραδείγματι (file signatures). Έτσι η παρακολούθηση των ηλεκτρομαγνητικών εκροών κατά την επεξεργασία (π.χ. άνοιγμα) ενός φακέλου, και κατόπιν η σύγκριση των με έτερες εκροές που έχουν από τα πριν συλλεχθεί, μπορεί δυνάμει να βοηθήσει τον ειδικό της ψηφιακής εγκληματολογίας να εντοπίσει τυχόν πρόσβαση ή επεξεργασία που έχει λάβει χώρα στον φάκελο αυτό[581].

Στη συνέχεια ακολουθεί η διάκριση των ενδεικτικών αντιμέτρων με βάσει τρεις κατηγοριοποιήσεις (λογισμικό, υλικό, περιβάλλοντας χώρος).

Αντίμετρα Λογισμικού (Software Countermeasures)



Διάγραμμα 2. *Βασικές κατευθυντήριες ως προς την επιλογή αντιμέτρων για την προστασία λογισμικού έναντι των SCAs*[582]

Πρόκειται για την μεγαλύτερη σε μέγεθος ομάδα από τις τρείς που προαναφέρθηκαν σχετικά με τα αντίμετρα. Αυτό είναι ενδεχομένως αναμενόμενο καθώς αν ανατρέξουμε στην πρόσφατη βιβλιογραφία της τελευταίας δεκαετίας αρκετές SCAs εκτελούνται απομακρυσμένα (remote, non-invasive SCAs κλπ), και επομένως στοχεύουν σε μεγάλο βαθμό (βέβαια όχι κατ'

[581] Sayakkara, A., & Le-Khac, N., & Scanlon, M.(2018). Electromagnetic Side-channel Attacks: Potential for Progressing Hindered Digital Forensic Analysis. *Forensic Focus for Digital Forensics & E-Discovery professionals.* Electromagnetic Side-Channel A□ttacks: Potential For Progressing Hindered Digital Forensic Analysis - Forensic Focus (Τελευταία πρόσβαση 13/10/2022).

[582] Το σχήμα είναι του συγγραφέως.

αποκλειστικότητα όπως είδαμε) το λογισμικό ενός attack vector (συσκευές IoT). Τα παραδείγματα που συλλέχθηκαν και που θα παρατεθούν ακολούθως, υπό την οπτική του ταξινομητικού εγχειρήματος, επικεντρώνουν (στον βαθμό που συζητούμε μόνο για το λογισμικό σε αυτό το σημείο) κυρίως στο επίπεδο σχεδιασμού (design level) και πρωτοκόλλου (protocol level[583]).

Κατωτέρω παρατίθενται μια σειρά ενδεικτικών αντιμέτρων ως ακολούθως:

- *App Guardian*: Πρόγραμμα λογισμικού που επιχειρεί να αντιμετωπίσει επιθέσεις τύπου RIG μέσα από την χρήση πληροφοριών πλευρικού καναλιού για διάφορες εφαρμογές λογισμικού. Η λογική του αντίμετρου στο συγκεκριμένο project των Zhang et al. βασίζεται (και) στο γεγονός ότι μια σειρά από SCAs που παρουσιάζονται στην διεθνή βιβλιογραφία αξιοποιούν κάποιο λογισμικό για να προσβάλλουν τον attack vector (π.χ. Android κινητά[584]).
- Τεχνικές συνεχούς χρόνου (*Constant Time Techniques*): Αφορά σε σύνολο τεχνικών για την παρεμπόδιση του επιτιθέμενου στην λήψη ακριβών χρονομετρήσεων (π.χ. σε περιπτώσεις Timing-based SCAs). Ενδεικτική περίπτωση τέτοιων τεχνικών είναι η παρεμβολή λανθάνοντος χρόνου (latent time) κατά την εκτέλεση διεργασιών, όπως στην περίπτωση του υπολογισμού των αριθμών κινητής υποδιαστολής (floating-point) κατά την αποστολή οδηγιών προς επεξεργαστές κλπ. Το αποτέλεσμα είναι ο επιτιθέμενος να δυσχεραίνετε στον ακριβή υπολογισμό του χρόνου που απαιτείται για την ολοκλήρωση μιας τέτοιας διεργασίας, καθώς με την εισδοχή λανθανόντων χρονικών περιόδων οι χρονικές διαφορές συγκαλύπτονται και ο χρόνος εκτέλεσης μιας τέτοιας διεργασίες φαίνεται πάντα ως σταθερός (fixed time[585]).

---

[583] Πρβλ. Levi, I., & Bellizia, D., & Bol, D., & Standaert, F.-X.(2020). Ask Less, Get More: Side-Channel Signal Hiding, Revisited. *IEE Transactions on Circuits and Systems I: Regular Papers,* 67, 12, 4904-4917 (1-14), σ.1. doi:10.1109/TCSI.2020.3005338. 248.pdf (uclouvain.be) (Τελευταία πρόσβαση 2/12/2022).

[584] Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangrad, S.(2017). Systematic Classification on Side-Channel Attacks: A case Study for Mobile Devices. *IEE Communications Surveys & Tutorials*, 20, 1, 465-488(1-24), σ.18. doi:10.1109/COMST.2017.2779824. 1611.03748.pdf (arxiv.org) (Τελευταία πρόσβαση 16/9/2021).

[585] Πρβλ. το έργο, μεταξύ άλλων, των Andrysco et al., Rane et al., Cock et al. και άλλων στο άρθρο των Montasari, R., & Hill, R., & Hosseinian-Far, A., & Montaseri, F.(2019). Countermeasures for Timing-Based Side-Channel Attacks against Shared, Modern Computing Hardware. *International Journal of Electronic Security and Digital Forensics*, 11, 294-320, σ.305-306.doi:10.504/IJESDF.2019.10020551. [PDF] Countermeasures for timing-based side-channel attacks against shared, modern computing hardware | Semantic Scholar (Τελευταία πρόσβαση 10/11/2022).

- Αντίμετρα για την μνήμη cache: Κατά κύριο λόγο τα αντίμετρα έναντι διαφόρων SCAs, όπως cache & Timing-based SCAs, βασίζονται είτε σε τμηματοποίηση της μνήμης cache (ιδιαιτέρως σε περιπτώσεις multitenancy) είτε σε τεχνικές τυχαιοποίησης (*cache randomization*) προς αποφυγή ντετερμινισμού (*non-deterministic behavior*[586]). Στόχος των αντιμέτρων είναι αφενός η αποτροπή της λήψης μετρήσεων ακριβείας και αφετέρου η αποτροπή της κατασπατάλησης πόρων λόγω της επιθέσεως που διενεργείται (επί παραδείγματι όταν ο επιτιθέμενος, στο πλαίσιο μιας cache-based SCA, φορτώνει δικές του memory lines για τους σκοπούς της επιθέσεως του). Τέτοιου είδους αντίμετρα περιλαμβάνουν, μεταξύ άλλων, εφαρμογές διαχείρισης μνήμης που διαχειρίζονται , κατά τρόπο δυναμικό, την αφαίρεση περιεχομένου από την μνήμη cache (π.χ. το λογισμικό «*CacheBar*" των Zhou et al.[587]). Επίσης, μια τεχνική που μπορεί εξίσου να αξιοποιηθεί είναι η δυναμική εποπτεία μοτίβων (patterns) λειτουργίας της διαμοιρασμένης μνήμης επεξεργαστή ώστε να εξαχθούν συμπεράσματα για την ύπαρξη ή μη πλευρικών καναλιών[588].

Βασική προβληματική για την συγκεκριμένη κατηγορία αντιμέτρων, παραμένει η προστασία εξίσου όλων των επιπέδων της μνήμης cache (κάτι που τα περισσότερα αντίμετρα δεν δύνανται να πράξουν). Σε μια προσπάθεια επίλυσης αυτού του προβλήματος οι Jaamoum et al. επιχείρησαν να συνδυάσουν την τεχνική τυχαιοποίησης (*randomization)* σε δύο επίπεδα της μνήμης cache, αφενός στο L1 και αφετέρου στο L3 (πολιτική τυχαίας έξωσης, *lightweight random eviction policy*), για μεγιστοποίηση της ασφάλειας που δύναται να προσφέρει το αντίμετρο[589].

---

[586] Jaamoum, A., & Hiscock, T., & Di Natale, G.(2022). Noise-Free Security Assessment of Eviction Set Construction Algorithms with Randomized Caches.*Applied Sciences* 2022, 12, 2415, 1-22, σ.1.doi:https://doi.org/10.3390/app12052415. Applied Sciences | Free Full-Text | Noise-Free Security Assessment of Eviction Set Construction Algorithms with Randomized Caches (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

[587] Montasari, R., & Hill, R., & Hosseinian-Far, A., & Montaseri, F. (2019). Countermeasures for Timing-Based Side-Channel Attacks against Shared, Modern Computing Hardware. International Journal of Electronic Security and Digital Forensics,11, 294-320, σ.307. doi:10.504/IJESDF.2019.10020551.IJTM/IJCEE PAGE TEMPLATEv2 (hud.ac.uk) (Τελευταία πρόσβαση 10/11/2022).

[588] Τέτοια περίπτωση αποτελεί το «*CC-Hunter*" των Evtyushkin et al. Ο.π.,σ.310.

[589] Πρβλ. Jaamoum, A., & Hiscock, T., & Di Natale, G.(2022),Noise-free Security Assessment of Eviction Set Construction Algorithms with Randomized Caches.*Applied Sciences* 2022, 12, 2415, 1-22, σ.19-20. doi:https://doi.org/10.3390/app12052415. Applied Sciences | Free Full-Text | Noise-Free Security Assessment of Eviction Set Construction Algorithms with Randomized Caches (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

- Τεχνικές διαχείρισης ισχύος (*Power Management Techniques*) : Σκοπός τέτοιου είδους αντιμέτρων είναι να διαρρήξει την συσχέτιση ανάμεσα στην δειγματοληψία ισχύος και στην πληροφορία που μπορεί να αποκαλυφθεί από την μελέτη των πρώτων (π.χ. DPA, EM SCA κλπ). Σε ότι αφορά στο σκέλος της προστασίας λογισμικού (π.χ. αλγόριθμοι κρυπτογράφησης όπως ο AES) έχουν προταθεί διάφορες τεχνικές, και με βάσει την βιβλιογραφία που μελετήθηκε, οι προσεγγίσεις που (κυρίως) αξιοποιούνται είναι εκείνες που είτε επιχειρούν να εισάγουν την τυχαιότητα (randomness) σε ότι αφορά στις εκροές ισχύος (power leakages), είτε εκείνες που επιχειρούν να εισάγουν μια ομοιογένεια με το να καθορίζουν την χωρητικότητα του σήματος (capacitance signal) κατά τρόπο ντετερμινιστικό (deterministic[590][591]).

Όπως αναφέρθηκε και ανωτέρω ο σχεδιασμός τέτοιων αντιμέτρων, ανάλογα το επίπεδο στο οποίο στοχεύουν, μπορεί να αποβεί είτε χρονοβόρος είτε και κοστοβόρος. Οι Jevtic & Otero τονίζουν το τελευταίο αυτό σημείο στο αντίμετρο το οποίο παρουσιάζουν, και προσπαθούν ταυτόχρονα να το υπερκεράσουν προτείνοντας παρεμβάσεις (από την πλευρά του αντίμετρου) στο επίπεδο της αρχιτεκτονικής του συστήματος (architectural level) έναντι έτερων επιπέδων (π.χ. επίπεδο κυκλώματος κλπ). Στο εν λόγω άρθρο οι συγγραφείς παρουσιάζουν, με την συνδρομή του *θεωρήματος Price* (*Price Theorem*), ένα αντίμετρο που επιχειρεί να διαχωρίσει το μετρήσιμο σήμα

---

[590] Για την πρώτη περίπτωση ορά ενδεικτικά το έργο των Singh et al., ενώ για την δε δεύτερη ορά το έργο των Jevtic et al. Και τα δύο παρατίθενται εν περιγραφική συντομία, στο Jevtic, R., & Otero, M.G.(1011). Methodology for Complete Decorrelation of Power Supply EM Side-Channel Signal and Sensitive Data. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 69, 2256-2260, σ.2257. doi:10.1109/TCSII.2022.3144071. Methodology for Complete Decorrelation of Power Supply EM Side-Channel Signal and Sensitive Data | IEEE Journals & Magazine | IEEE Xplore (Τελευταία πρόσβαση 23/11/2022).

[591] Σε ότι αφορά την συγκεκριμένη υποκατηγορία και την προστασία του λογισμικού υφίστανται εύλογα και έτερες προτάσεις, για λόγους όμως χώρου απλώς αρκούμαστε στο να υπογραμμίσουμε τους βασικούς άξονες πάνω στους οποίους αυτές κινούνται. Έτερα παραδείγματα μπορούν να περιλαμβάνουν μια δυναμικά ρυθμιζόμενη τάση ρεύματος ("*dynamic voltage/frequency scaling*") , εισαγωγή masking απευθείας στον κώδικα ενός αλγόριθμου, σύγκριση των εκροών με κάποιο μοτίβο ή με μια πρόβλεψη για την αναμενόμενη κατανάλωση ισχύος κατά την εκτέλεση, για παράδειγμα, ενός αλγόριθμου κρυπτογράφησης. Για μια σύντομη παράθεση των εν λόγω εναλλακτικών ορά, μεταξύ άλλων και το άρθρο των Agosta, G., & Barenghi, A., & Pelosi, G., & Scandale, M.(2015). The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34, 8, 1320-1333, σ.1332. doi:10.1109/TCAD.2015.2430320. (PDF) The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks (researchgate.net) (Τελευταία πρόσβαση 7/11/2022).

(*measured signal*) από εκείνο της φόρτωσης (*load signal*). Έτσι, στόχος των συγγραφέων είναι, με την χρήση του *Θεωρήματος Price* να φτάσουν σε μια μηδενική συσχέτιση ανάμεσα στα δύο αυτά σήματα, ώστε σ θεωρητικό επίπεδο να μην μπορεί ο επιτιθέμενος να συσχετίσει την ηλεκτρομαγνητική εκροή από μια συσκευή με τα ευαίσθητα δεδομένα που η τελευταία θα επεξεργάζεται εκείνη την στιγμή[592].

- Lattice scheduling: Πρόκειται για σειρά αντιμέτρων που αφορούν στην οργάνωση των διεργασιών ενός υπολογιστικού συστήματος με στόχο την σαφή μείωση των εκροών[593].Επί παραδείγματι, οι Wang et al. χρησιμοποιούν ένα τέτοιο αντίμετρο έναντι Timing SCAs, σε συνθήκες διαμοιρασμού μνήμης μεταξύ μη έμπιστων χρηστών, με το να εισάγουν αφενός μιας δομή queuing και αφετέρου με την εισαγωγή στατικών time-slots, δηλαδή με το να δίνετε μόνο σε ένα τομέα ασφαλείας (*security domain*) η δυνατότητα να χρησιμοποιεί πόρους μνήμης σε κάθε στιγμή, και όχι σε όλους τους τομείς ταυτοχρόνως[594].

- *Leakage Resilience*: Τα αντίμετρα αυτά στοχεύουν στην μείωση της εκροής μέσα από την επιβολή περιορισμού στην επαναλαμβανόμενη χρήση κλειδιών κρυπτογράφησης για κάθε τέτοιον αλγόριθμο. Επί παραδείγματι οι Dziembowski et al. πρότειναν την δημιουργία ενός αλγόριθμου ο οποίος θα αναλάμβανε την διαρκή δημιουργία τέτοιων κλειδιών περιορισμένης επαναλαμβανόμενης χρήσης[595].

- *Noise Addition*: Βασικός στόχος εδώ είναι η αντιστροφή της κατάστασης όσον αφορά το SNR (Signal-to- Noise ratio) σε σχέση με τις αντίστοιχες επιθέσεις στις οποίες το τελευταίο έχει αναφερθεί. Ήτοι το αντίμετρο στοχεύει εδώ στην μείωση της αναλογίας Signal to Noise Ratio, ώστε οι μετρήσεις που θα πραγματοποιήσει ο επιτιθέμενος να μην του αποδώσουν εν τέλει σημαντικό αριθμό πληροφοριών. Αυτή η

---

[592] Ο.π.,σ.2256.

[593]Ο.π.,σ.303.

[594] Wang, Y., & Ferraiuolo, A., & Suh, G.E.(2014). *Timing Channel Protection for a Shared Memory Controller.* Paper presented at the Proceedings of the 20th International Symposium on High Performance Computer Architecture (HPCA). Orlando, FL, USA. February 15-19, 1-12, σ.1 & 5. wang-ferraiuolo-hpca-14.pdf (cornell.edu) (Τελευταία πρόσβαση 28/11/2022).

[595] Πρβλ. την επισήμανση για το έργο των Dziembowski et al. στο ακόλουθο κεφάλαιο, Batina, L., & Djukanovic, M., & Heuser, A., & Picek, S.(2021). It Started with Templates: The Future of Profiling in Side-Channel Attacks. Στο Avoine, G., & Hernandez-Castro, J.(επιμ.), *Security of Ubiquitous Computing Systems* (133-145),σ.145. Springer, Cham. doi: https://doi.org/10.1007/978-3-030-10591-4_8. document (inria.fr) (Τελευταία πρόσβαση 25/11/2022).

έξωθεν παρεμβολή θορύβου εντός ενός πλευρικού καναλιού γίνεται με διάφορους τρόπους όπως επί παραδείγματι με την εφαρμογή ψευδών διαδικασιών ή διαδικασιών που προκαλούν κάποιου είδους shuffling. Σημειώνεται πως όσο περισσότερο διαρκεί μια SCA, τόσο λιγότερο πιθανό είναι ένα τέτοιου είδους αντίμετρο να καταστεί αποτελεσματικό έναντι της τελευταίας[596].

- Signature verification: αφορά σε μια software-based προσέγγιση όπου η υπογραφή RSA-CRT πρέπει να επιβεβαιωθεί πριν την επιστροφή της συναρτήσεως κρυπτογράφησης. Αυτό το αντίμετρο πρότειναν οι Delarea & Oren για την αντιμετώπιση των fault injection attacks στην πειραματική τους συνθήκη, προτείνοντας παράλληλα την ενσωμάτωση του σε βιβλιοθήκες ανοικτού κώδικα, όπως η PyCrypto στην δική τους περίπτωση[597].

- Τυχαιοποίηση διατάξεως πλήκτρων επί του πληκτρολογίου(*Keyboard Layout Randomization*): αντίμετρο που ήδη βρίσκει σχετικά ευρεία εφαρμογή σε περιπτώσεις εισαγωγής pin κλπ (π.χ. ανέπαφες συναλλαγές), η διάταξη των πλήκτρων δεν ακολουθεί την τυπική σειρά κι έτσι ο επιτιθέμενος συναντά δυσχέρειες στην συσχέτιση ανάμεσα στα πλήκτρα που πατήθηκαν και στην κίνηση των δακτύλων (εδώ ο λόγος γίνεται για SCAs που αξιοποιούν δονήσεις για να επιτεθούν σε συσκευή IoT όπως ένα κινητό). Εύλογα η εφαρμογή του μέτρου ενέχει περιορισμούς, καθότι για συνθετότερες λειτουργίες που απαιτούν χρήση πληκτρολογίου το συγκεκριμένο αντίμετρο δεν προσφέρει, μια φιλική προς τον εκάστοτε χρήστη, λύση[598].

- Sensitive data renewal: Οι Al-Shareeda et al. μελετούν την χρησιμότητα του Polynomial-Based Scheme του Chebyshev έναντι επιθέσεων πλευρικού καναλιού που στοχεύουν κατά δικτύων (5G) αυτοκινούμενων οχημάτων. Το αντίμετρο που προτείνουν συνίσταται στην περιοδική ανανέωση (renewal) της ενδιάμεσης ψευδωνυμικής ταυτότητας (inter-pseudonym identity $IPID_V$) που είναι αποθηκευμένη στα δεδομένα πρόβλεψης ταξιδίου (Travel Prediction-Based Data, TPD) εντός της OBU

[596] Durvaux et al. στο ο.π.,σ.144.

[597] Η χρήση του εν λόγω αντίμετρου αποτυπώθηκε και στα αποτελέσματα της πειραματικής τους συνθήκης, ο.π.

[598] Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017).Systematic Classification on Side-Channel Attacks: A case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials*, 20, 1, 465-488 (1-24), σ.17. doi:10.1109/COMST.2017.2779824. 1611.03748.pdf (arxiv.org) (Τελευταία πρόσβαση 16/9/2021).

(On-Board Unit[599]). Η ανανέωση δεδομένων δεν αποκλείει την ύπαρξη πλευρικού καναλιού, αλλά έρχεται ως patch να μετριάσει σημαντικά την χρησιμότητα των όποιων πληροφοριών προκύπτουν από το τελευταίο.

- Άδειες χρήσης (*Permissions*): Η εφαρμογή ενός τέτοιου αντίμετρου είναι ευρύτερη εν σχέσει με τα ανωτέρω, καθώς επιχειρεί να καλύψει το σύνολο του λογισμικού που εγκαθίσταται σε μια συσκευή (π.χ. android phones) και επίσης των αισθητήρων που τυχόν δεν διαθέτουν πρόβλεψη για σχετικές άδειες. Η εφαρμογή ενός τέτοιου αντίμετρου δύσκολα μπορεί να είναι καθολική, μεταξύ άλλων, διότι πολλοί χρήστες (end-users) δεν επιθυμούν σε πολλές περιπτώσεις να προβούν σε τέτοιες ενέργειες[600].

- Περιορισμός πρόσβασης στις συχνότητες των αισθητήρων (*Limiting Access or Sampling Frequency*): Σε συνέχεια του προηγούμενου αντίμετρου, πέραν του περιορισμού στην πρόσβαση ενός αισθητήρα γενικά, μπορεί να υπάρξει μέριμνα και για μείωση του εύρους των συχνοτήτων εντός του οποίου μπορεί να γίνει δειγματοληψία επί της λειτουργίας κάποιου αισθητήρα (sampling frequency). Βασικό πρόβλημα που προκύπτει εδώ, εκ νέου, είναι η λειτουργικότητα του ίδιου του αισθητήρα και κατ' επέκταση της ίδιας της συσκευής IoT[601].

- Προστασία εισόδων από χρήστες (*User Input Protection*):Ευρύ φάσμα αντιμέτρων που στοχεύουν στην προστασία είτε του μέσου με το οποίο γίνεται η είσοδος (π.χ. πληκτρολόγιο οθόνης), είτε στην μείωση των περιβαλλοντικών (κοντινών αντικειμένων) παραγόντων που επιτρέπουν στον επιτιθέμενο να καταγράψει την εκροή. Στην πρώτη περίπτωση εντάσσονται περιπτώσεις τυχαιότητας πλήκτρων (π.χ. τα πλήκτρα σε ένα πληκτρολόγιο αφής να τοποθετούνται εις το μέσον της οθόνης, ώστε να μην ξεχωρίζει τόσο εύκολα το μοτίβο της κίνησης των δακτύλων που πληκτρολογούν),

---

[599] Al-Shareeda, M., & Manickam, S., & Mohammed, B.A., & Al-Mekhlafi, Z.G., & Qtaish, A., & Alzahrani, A.J., & Alshammari, G., & Sallam, A.A., & Almekhlafi, K.(2022).Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks. *Applied Sciences* 2022, 12, 5939, 1-17, σ.11 & 15. doi:https://doi.org/10.3390/app12125939. Applied Sciences | Free Full-Text | Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks (mdpi.com) (Τελευταία πρόσβαση 12/8/2022).

[600] Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangrad, S.(2017). Systematic Classification on Side-Channel Attacks: A case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials*, 20, 1, 465-488 (1-24), σ.17. doi:10.1109/COMST.2017.2779824. 1611.03748.pdf (arxiv.org) (Τελευταία πρόσβαση 16/9/2021).

[601] Ο.π.,σ.18.

τυχαιοποίησης της λειτουργίας δόνησης (vibration) ώστε να μην μπορεί εύκολα να εξάγει μοτίβα ο επιτιθέμενος με βάση τα δείγματα του εν λόγω αισθητήρα, καθώς και περιπτώσεις ανάπτυξης λογισμικού για ταυτοποίηση χρήστη σε συσκευές android που αξιοποιούν οθόνες αφής[602][603]. Στην δεύτερη περίπτωση, που είναι γενικότερη της πρώτης κατά κάποιο τρόπο, στόχος είναι να προστατευτούν αντικείμενα πλησίον μιας συσκευής IoT για να αποτραπεί το hopping από το αντικείμενο προς την συσκευή στόχο. Επί παραδείγματι, οι Raguram et al. προτείνουν την μείωση της φωτεινότητας της οθόνης μετά της χρήσης κάποιας κάλυψης (coating) επί των γυαλιών μυωπίας του χρήστη που χειρίζεται την συσκευή IoT (εδώ το παράδειγμα είναι και συνδυαστικό, καθώς πραγματοποιεί αναφορά και στην υποκατηγορία των αντιμέτρων περιβάλλοντος που θα αναφερθεί εκτενέστερα κατωτέρω[604]).

---

[602] Ο.π.,σ.17.

[603] Ενδεικτικά εδώ αναφέρουμε το παράδειγμα σχεδιασμού αντιμέτρου για εισαγωγή PIN σε κινητή συσκευή που παραθέτουν στο άρθρο τους οι Krombholz et al. Το αντίμετρο που προτείνουν οι συγγραφείς, σε γενικές γραμμές, βασίζεται σε εισαγωγή PIN μέσω, όχι ενός μοτίβου κινήσεως των δακτύλων, αλλά αντίθετα ασκήσεως πίεσης επί των πλήκτρων πάνω σε μια οθόνη αφής (συσκευή Android κλπ), μέθοδος εν γένει γνωστή ως «*Force-PIN Design*". Καθώς οι οθόνες αφής δύνανται να αναγνωρίσουν τον βαθμό σχετικής πίεσης που ασκείται επί αυτών, οι συγγραφείς στο άρθρο τους παρουσίασαν μια εφαρμογή για κινητές συσκευές, όπου οι χρήστες για μεγαλύτερη προστασία θα ασκούν διαβαθμισμένη πίεση επί μιας οθόνης αφής τεσσάρων πλήκτρων (όμοιας με των παραδοσιακών iPhones), και ανάλογα με την πίεση που ασκείται θα εμφανίζεται το αντίστοιχο πλήκτρο (π.χ. αν στο πλήκτρο 3 ασκηθεί μεγαλύτερη πίεση τότε η είσοδος θα είναι το πλήκτρο 6 κοκ). Με τον τρόπο αυτό αφενός θα πιστοποιείτε ο χρήστης και αφετέρου ο επιτιθέμενος δεν θα δύναται να προβεί σε συσχετίσεις με βάσει SCAs που θα στοχεύουν σε συλλογή πληροφοριών από αποτυπώματα επί της οθόνης (smudge attacks) ή μέσω διενέργεια επιθέσεως shoulder surfing για παράδειγμα. Εκ νέου τονίζεται ότι η συνθήκη στο άρθρο ήταν κατά βάση πειραματική, και άρα το νεαρό της ηλικίας των χρηστών τους επέτρεπε να κατανοήσουν πιο εύληπτα την πρακτικότητα της εν λόγω εφαρμογής. Επομένως, εδώ το βασικό μειονέκτημα είναι τα δημογραφικά στοιχεία («*demographics*") των χρηστών, και όπως ισχύει γενικά για τα αντίμετρα που αναμένουν ο χρήστης να πράξει τα δέοντα για την εφαρμογή τους, τα εν λόγω δημογραφικά χαρακτηριστικά (ηλικία, εξοικείωση, μυοσκελετική δομή) καθορίζουν σε αρκετά μεγάλο βαθμό το user-friendliness του όποιου τέτοιου αντίμετρου. Krombholz, K., & Hupperich, T., & Holz, T.(2016). *Use the Force: Evaluating Force- Sensitive Authentication for Mobile Devices*. Paper presented at the 12th Symposium on Usable Privacy and Security (SOUPS 2016). Denver, CO, USA. June 22-24, 207-219, σ. 209 & 216. soups2016-paper-krombholz.pdf (usenix.org) (Τελευταία πρόσβαση 29/11/2022).

[604] Ορά την αναφορά στο έργο των Raguram et al. στο άρθρο των Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S. (2017). Systematic Classification on Side-Channel Attacks: A case Study for Mobile Devices. *IEE Communications Surveys & Tutorials*, 20, 1, 465-488 (1-24), σ.17. doi:10.1109/COMST.2017.2779824. 1611.03748.pdf (arxiv.org) (Τελευταία πρόσβαση 16/9/2021).

- Προστασία της εφαρμογής αλγόριθμων κρυπτογράφησης (*Protection of cryptographic implementations*): Ένα παράδειγμα τέτοιου είδους αντίμετρου αποτελούν οι τεχνικές τυχαιοποίησης (*randomization*) είτε για ότι αφορά στην εκτέλεση του αλγόριθμου (αυτό που στην βιβλιογραφία εμφανίζεται με τον όρο shuffling, ήτοι η αναδιάταξη των διεργασιών εκτέλεσης ενός αλγόριθμου[605]) είτε σε ότι αφορά στις τιμές των κλειδιών («*key-dependent values*[606]"). Επίσης δε, έχουν προταθεί και οι τυχαίες κατανομές στους αλγορίθμους των look-up tables, όπως και η χρήση δεικτών αντί τιμών για την πρόσβαση σε ευαίσθητα δεδομένα[607].
- Επαλήθευση σημείου (*Point Validation*): Οι Zhang et al. παρουσιάζουν μια σειρά από αντίμετρα για αλγορίθμους που χρησιμοποιούν ελλειπτικές καμπύλες (elliptic curve, identity-based algorithms). Η συγκεκριμένη μέθοδος ελέγχει αν ένα σημείο είναι εντός της καμπύλης, σε περίπτωση που κάτι τέτοιο δεν επαληθεύεται τότε δεν θα δίνεται καμία έξοδος (output[608]).
- Έλεγχος ακεραιότητας καμπύλης (*Curve Integrity Check*): εκ νέου στο πλαίσιο συνθήκης που αφορά fault SCAs και identity-based algorithms ως στόχους, οι ερευνητές προτείνουν ένα αντίμετρο που θα ελέγχει για την ύπαρξη σφαλμάτων (faults) στις παραμέτρους της καμπύλης. Η λογική του αντιμέτρου έχει να κάνει με τον έλεγχο των παραμέτρων της καμπύλης που ευρίσκονται στην μνήμη του υπολογιστικού συστήματος, μέσω π.χ. ενός redundancy check, πριν την εκτέλεση του (identity-based) αλγόριθμου ώστε να επιβεβαιωθεί η μη ύπαρξη σφαλμάτων (fault[609]).

---

[605] Σε αυτή την υποκατηγορία εύλογα ο λόγος γίνεται για το σχεδιαστικό επίπεδο (design level).Levi, I., & Bellizia, D., & Bol, D., & Standaert, F.-X. (2020). Ask Less, Get More: Side-Channel Signal Hiding , Revisited. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 67, 12, 4904-4917 (1-14), σ.1. doi:10.1109/TCSI.2020.3005338. 248.pdf (uclouvain.be) (Τελευταία πρόσβαση 2/12/2022).

[606] Ο.π.

[607] Ορά το έργο των συγγραφέων στο ακόλουθο πόνημα, Sayakkara, A., & Le-Khac, N.A., & Scanlon, M.(2019). A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics. *Digital Investigation*, 29, 43-54 (1-14), σ.8. doi: [1903.07703] A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics (arxiv.org). 1903.07703.pdf (arxiv.org) (12/10/2021).

[608] Zhang, Q., & Wang, A., & Niu, Y., & Shang, N., & Xu, R., & Zhang, G., & Zhu, L.(2018). Side-Channel Attacks and Countermeasures for Identity-Based Cryptographic Algorithm SM9. Security and Communication Networks, 2018, 1-15, σ.12. doi:https://doi.org/10.1155/2018/9701756. 9701756.pdf (hindawi.com) (Τελευταία πρόσβαση 30/11/2022).

[609] Ο.π.

- Έλεγχος συνοχής (*Coherence Check*): Όπως και στις δύο προηγούμενες περιπτώσεις πρόκειται πάλι για την περίπτωση των fault SCAs, το αντίμετρο αυτό ελέγχει τα αποτελέσματα που δίνει ο αλγόριθμος (identity-based) κρυπτογράφησης έναντι ενός έγκυρου μοτίβου, ώστε μέσω τη σύγκρισης να εντοπιστούν τυχόν σφάλματα (fault[610]).

- *Rotating Sboxes Masking* (*RSM*): Αντίμετρο των Kuroda et al. για προστασία έναντι SCAs υποστηριζόμενων από μοντέλα μηχανικής μαθήσεως (non-profiled). Το *RSM* περιλαμβάνει 16 τύπους Sboxes που ο καθένας περιέχει μια masked (16-byte) τιμή με στόχο να γίνεται masking των ενδιάμεσων τιμών (intermediate values) πριν και μετά την εκτέλεση του αλγορίθμου Sbox[611].

- *Table re-computing masking*: Επίσης αντίμετρο που πρότειναν οι Kuroda et al. έναντι των SCAs που υποστηρίζονται από μοντέλα μηχανικής μαθήσεως. Σε αυτή την περίπτωση ο πίνακας του Sbox συγκροτείται επί τι βάσει δύο τυχαίων αριθμών(τιμές mask 16-byte), κι έτσι όλα τα σημεία (nodes) θα προστατεύονται από masks τυχαίων αριθμών για αποφυγή ύπαρξης εκροών[612].

- *SoftTempest*: Αντίμετρο που εν γένει στοχεύει στην μείωση των οπτικών εκροών από την οθόνη μιας συσκευής. Στόχος εδώ είναι η αναδιάταξη της αναπαραγωγής των pixels που απαρτίζουν το περιεχόμενο της οθόνης ("*data-stream order*"). Ενδεικτικές τέτοιες λύσεις περιλαμβάνουν την τυχαία δημιουργία pixels είτε (εναλλακτική που είναι φθηνότερη) την επίτευξη μιας σταθερής ενεργειακής ροής μέσα από την προσαρμογή των χρωμάτων των χαρακτήρων και του φόντου, με αποτέλεσμα τα παραγόμενα pixels να μην ξεχωρίζουν τόσο εύκολα όταν ο επιτιθέμενος θα επιχειρήσει να μετρήσει την οπτική εκροή[613].

---

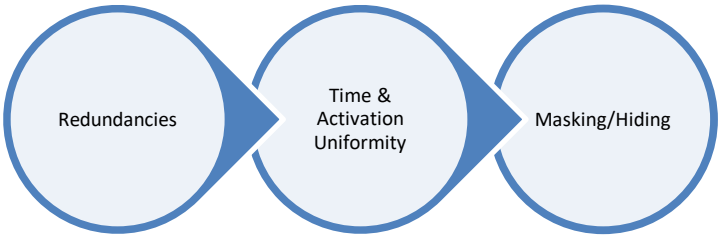
[610] Ο.π.

[611] Kuroda, K., & Fukuda, Y., & Yoshida, K., & Fujino, T.(2021). *Practical Aspects on Non-profiled Deep-learning Side-channel Attacks against AES Software Implementation with Two Types of Masking Countermeasures including RSM.* Paper presented at the Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security (ASHES '21). Virtual Event, Republic of Korea. November 19,29-40, σ.34. doi:10.1145/3474376.3487285. Microsoft Word - ashes24-kurodaSC.docx (acm.org) (Τελευταία πρόσβαση 10/10/2022).

[612] Ο.π.,σ.32.

[613] Πρβλ. το έργο των Kuhn, M.G., & Anderson, A.J., Kuhn, M.G., & Tanaka, H. et al. στο άρθρο των Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., & Molton, St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security,*

Αντίμετρα Υλικού (Hardware Countermeasures)



Διάγραμμα 3. *Ενδεικτικά αντίμετρα υλικού έναντι των SCAs*[614]

Σε ένα τέταρτο επίπεδο, και ενδεχομένως εκεί όπου οδηγούν οι προηγούμενες τρεις ταξινομητικές διακρίσεις/παρατηρήσεις, τα αντίμετρα δύνανται όπως διακριθούν (και) ανάλογα με το επίπεδο στο οποίο καταλήγουν να εφαρμόζονται. Έτσι υφίστανται αντίμετρα διαφορετικών επιπέδων και επομένως σχεδιαστικών αναγκών ανάλογα με το επίπεδο αφαίρεσης (abstraction level). Το οποίο επίπεδο μπορεί να είναι αυτό του δικτύου (circuit level), εκείνο της πύλης (gate level) κοκ. Υπό αυτή την προοπτική, η εστίαση επανέρχεται εκ νέου στην σχεδιαστική λογική (by design) περί του κάθε αντιμέτρου, αλλά επίσης αναδεικνύεται και η θεματική της δυνατότητας συνδυαστικής χρήσης αντιμέτρων, και επομένως και της συμβατότητας των εκάστοτε συνδυασμών, με βάσει τις ανάγκες και τα χαρακτηριστικά των συσκευών IoT μιας οποιασδήποτε κρίσιμης υποδομής[615].

Σε ότι αφορά στην κατηγορία του υλικού οι κύριοι τύποι αντίμετρων που θα παρουσιαστούν σε αυτή την υπό-ενότητα είναι το redundancy, το uniformity (ομοιομορφία), το

Springer, 2021, 10.1007/s41635-021-00112-6. Hal-03176249, 1-24, σ.15. Whispering devices: A survey on how side-channels lead to compromised information (archives-ouvertes.fr) (Τελευταία πρόσβαση 22/11/2022).

[614] Το σχήμα είναι του συγγραφέως.

[615] Ορά την σχετική παράθεση για την ταξινόμηση ανά επίπεδο των Tena-Sanchez et al., αν και ο λόγος γίνεται για αντίμετρα υλικού (και στο εκείθεν άρθρο και στην παρούσα υπό-ενότητα), ωστόσο η ταξινομητική προοπτική μπορεί να έχει εύλογα ευρύτερη εφαρμογή. Πρβλ. Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28, σ.2. doi: https://doi.org/10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

masking και το hiding[616]. Υπογραμμίζεται εκ νέου εδώ, όπως και ανωτέρω, πως η ταξινόμηση λαμβάνει χώρα με βάσει το τρίπτυχο (λογισμικό/υλικό/αντίμετρα περιβάλλοντος, εδώ ο λόγος γίνεται για το υλικό βεβαίως) αφενός και αφετέρου με βάσει το επίπεδο σχεδιασμού και εφαρμογής του εκάστοτε αντίμετρου, που στην παρούσα υπό-ενότητα αφορά κυρίως (αν όχι κατ' αποκλειστικότητα) στο επίπεδο του κυκλώματος (circuit level) και εκείνο της πύλης (gate level).

Υφίστανται εύλογα και ενδιάμεσες περιπτώσεις, που δύνανται όπως συνδυάσουν στο πλαίσιο ενός αντίμετρου τόσο το masking όσο και το hiding. Παράδειγμα ενός τέτοιου συνδυασμού αποτελεί το αντίμετρο που προτείνουν οι Popp & Mangard, με την ονομασία MDPL ("*masked dual-rail precharge logic*"). Αφενός η προφόρτωση (precharge) του dual-rail αποτρέπει την εμφάνιση των glitches και αφετέρου όλα τα μεταδιδόμενα σήματα χρησιμοποιούν την ίδια μάσκα, έτσι ώστε για κάθε ένα σήμα να μεταδίδεται και ένα αντίστοιχο συμπληρωματικό του, για να μην μπορεί ο επιτιθέμενος να ξεχωρίσει τις εκπομπές[617]. Στην συνέχεια παρουσιάζονται συνοπτικά οι τρεις ενδεικτικές περιπτώσεις αντιμέτρων που αναφέρθηκαν ονομαστικά ανωτέρω.

Αναφορικά με την πρώτη κατηγορία αντιμέτρων εδώ παραθέτουμε τρεις ενδεικτικές περιπτώσεις ήτοι το *hardware*, το *temporal*, και επίσης το *information redundancy*. Μια ενδεικτική παράθεση ακολουθεί ευθέως κατωτέρω:

- *Hardware redundancy*: Αντίμετρο που βασίζεται σε αντιγραφή (*duplication*) του κυκλώματος, δηλαδή σε δημιουργία ενός αντιγράφου ούτως ώστε να

[616]Εύλογα η λίστα των σχετικών αντιμέτρων για το υλικό δεν εξαντλείται στις δύο αναγραφόμενες υπό-περιπτώσεις, αλλά ο χώρος είναι περιορισμένος. Στην παραπομπή αυτή αναφέρονται, εν παρόδω, σχετικά αντίμετρα υλικού όπως η χρήση περιβλήματος τύπου Faraday (Faraday Cage) για την μείωση των εκροών (EM), ο σχεδιασμός των chips για να λειτουργούν ασύγχρονα δίχως να βασίζονται στην χρήση του ρολογιού του συστήματος (asynchronism), και επίσης η χρήση *dual line logic* για την αναπαράσταση των bits 0 & 1 όπου θα πρέπει πάντα να συνδυάζονται δύο bits για να αναπαραστήσουν το καθένα από τα δυαδικά ψηφία και άρα θα καθίσταται δυσχερές για τον επιτιθέμενο να μαντέψει ορθά με βάσει τις εκροές που θα έχει συλλέξει. Πρβλ. ενδεικτικά το άρθρο των Sayakkara, A., & Le-Khac, N.A., & Scanlon, M.(2019). A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics. *Digital Investigation*, 29, 43-54(1-14), σ.8. doi: [1903.07703] A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics (arxiv.org). 1903.07703.pdf (arxiv.org) (Τελευταία πρόσβαση 12/10/2021).

[617] Πρβλ. Popp & Mangard στο άρθρο των, Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chave, R.(2022). Gate-level hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12, 2390, 1028, σ.17. doi: https://doi.org.10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks | HTML (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

συγκριθούν κατόπιν τα αποτελέσματα (π.χ. της κρυπτογράφησης) μεταξύ τους και να καταστεί εμφανές αν υπάρχει κάποια παρατηρήσιμη διαφορά (π.χ. fault). Η τεχνική αυτή μπορεί να εκτελεστεί με μια σειρά τρόπους, όπως με την χρήση (κατ' επανάληψη) αντιγράφων Sboxes ή με την ανταλλαγή τιμών ανάμεσα σε μήτρες ("*redundant state matrixes"*). Βασικό μειονέκτημα του εν λόγω αντιμέτρου είναι εύλογα το κόστος σε υπολογιστικούς πόρους που το σύστημα θα κληθεί να επωμιστεί λόγω της χρήσης αντιγράφων, και της κατ' επανάληψη εκτέλεσης των αλγορίθμων για να γίνουν οι συγκρίσεις[618].

- *Temporal redundancy*: Στην περίπτωση του αντιμέτρου αυτού οι διεργασίες του κρυπταλγόριθμου (computations) επαναλαμβάνονται είτε αντιστρόφως σε κάθε γύρο κρυπτογράφησης είτε, πάλι, μέσω αντιγραφής (*duplication*). Κατ' αυτό τον τρόπο το αποτέλεσμα που δίνει η κρυπτογράφηση ελέγχεται είτε με την τιμή από τον προηγούμενο γύρο κρυπτογράφησης είτε με εκείνη από τον επόμενο. Έτσι τα αποτελέσματα από τον κάθε γύρο συγκρίνονται μεταξύ τους, είτε ακόμα και οι τιμές αυτών χρησιμοποιούνται για κάθε επόμενο γύρο, σε μια προσπάθεια μέσω της σύγκρισης να εντοπιστούν τυχόν σφάλματα (faults) που έχει παρεμβάλει ο επιτιθέμενος. Σε αντίθεση με την προηγούμενη περίπτωση, εδώ το αντίμετρο δεν είναι κοστοβόρο αλλά αντίθετα χρονοβόρο, καθώς σε κάθε γύρο απαιτείται ο διπλάσιο χρόνος υπολογισμού των τιμών μιας και πρέπει κάθε φορά να η διεργασία (computation) να επαναλαμβάνεται αντιστρόφως για λόγους σύγκρισης[619].
- *Information redundancy*: Σε αυτή την περίπτωση η λογική του αντίμετρου υπαγορεύει την προσθήκη επιπλέον πληροφοριών πριν την εκτέλεση των ενδιάμεσων διεργασιών ("*intermediate computations*"), ώστε να εντοπιστούν τυχόν παραποιήσεις (ήτοι faults) κατά την εκτέλεση αυτών. Η εφαρμογή μιας τέτοιας τεχνικής περιλαμβάνει μόνο μικρό overhead, αλλά κυρίως έγκειται στο ότι επιτρέπει την μη ντετερμινιστική εκτέλεση του αλγόριθμου εισάγοντας (π.χ. μέσω ενός parity checker/predictor) μια μη γραμμικότητα, η οποία δεν επιτρέπει εύκολα στον επιτιθέμενο να ανεύρει την συσχέτιση ανάμεσα στο parity checker & predictor πριν και μετά την εκτέλεση του αλγορίθμου

[618] Potestad-Ordonez, F.E., & Tena-Sanchez, E., & Acosta-Jimenez, A.J., & Jimenez-Fernandez, C.J., Chaves, R.(2022). Hardware Countermeasures Benchmarking against Fault Attacks. *Applied Sciences* 2022, 12 (5), 2443, 1-20, σ.8. doi:https://doi.org/10.3390/app12052443.Applied Sciences | Free Full-Text | Hardware Countermeasures Benchmarking against Fault Attacks (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

[619] Ο.π.

κρυπτογράφησης. Εντούτοις, η χρήση των parities επιτρέπει εντοπισμό σφαλμάτων ανάλογα με το είδος των τελευταίων αλλά και με το είδος του parity που ενσωματώνεται στα δεδομένα για τον έλεγχο (π.χ. αν το parity bit είναι άρτιο θα εντοπίσει τυχόν περιττά σφάλματα, όχι όμως και σφάλματα που είναι κι αυτά άρτια και αντιστρόφως[620]).

- Συνδυασμός αντιμέτρων: Τέλος υφίσταται ακόμα η δυνατότητα τα ως άνω αντίμετρα να συνδυαστούν για την επίτευξη μεγαλύτερου βαθμού ασφαλείας. Ένα χαρακτηριστικό παράδειγμα που μπορεί εδώ να παρατεθεί είναι ο συνδυασμός του *hardware* & του *temporal redundancy.* Σε αυτό τον συνδυασμό οι διεργασίες της κρυπτογράφησης και αποκρυπτογράφησης λαμβάνουν χώρα διπλό αριθμό φορών (redundancy), και εκτελούνται ακολουθιακά. Ο κάθε γύρος κρυπτογράφησης και αποκρυπτογράφησης διαιρείται εξ' ημισείας, και το καθένα από τα δύο μέρη χρησιμοποιείται αλλεπάλληλα για να ελεγχθούν συγκριτικά τα αποτελέσματα των δύο διεργασιών (ήτοι το ένα διαιρεμένο τμήμα αντιπαραβάλλεται με το αποτέλεσμα της κρυπτογράφησης, και το έτερο με εκείνο της αποκρυπτογράφησης, σε μορφή χιαστί, για κάθε γύρο[621]).

Δεύτερον, υφίστανται και σε ότι αφορά το υλικό αντίμετρα που στοχεύουν στην επίτευξη της ομοιομορφίας (uniformity) κατά την εκτέλεση διεργασιών. Ενδεικτικά παραθέτουμε τις ακόλουθες δύο περιπτώσεις από το άρθρο των Takatoi et al. για τις ηλεκτρομαγνητικές επιθέσεις (*Simple Electromagnetic Attacks, SEMA*) έναντι ενσωματωμένων νευρωνικών δικτύων (*Embedded Neural Networks*):

- ✓ Χρονική Ομοιομορφία (*Uniform Timing*): Οι Takatoi et al. σημειώνουν πως μέσω της εφαρμογής των μαθηματικών σειρών Taylor (*Taylor series*) είναι εφικτή η επίτευξη της χρονικής ομοιομορφίας για ορισμένες συναρτήσεις ενεργοποίησης (*activation functions*, οι συγγραφείς στο σημείο αυτό κάνουν αναφορά σε τέτοιου είδους συναρτήσεις όπως η *Sigmoid*, *ReLU* & *Leaky ReLU*) σε ένα ενσωματωμένο νευρωνικό δίκτυο, ούτως ώστε να καταστεί δυσχερές για τον επιτιθέμενο (π.χ. στην περίπτωση μιας Timing SCA) να πάρει πληροφορίες για τις εν λόγω συναρτήσεις, καθώς οι τελευταίες θα απαιτούν τον ακριβώς ίδιο χρόνο εκτέλεσης για την κάθε μια (*uniform computational time*), και άρα δεν θα επιτρέπουν να γίνονται εύκολα χρονικά προσδιορισμένες

[620] Ο.π.,σ.9.

[621] Ο.π.,σ.11.

συσχετίσεις από την πλευρά του επιτιθέμενου (μειονέκτημα εδώ θα είναι η μεγαλύτερη αναμονή στον χρόνο εκτέλεσης της συνάρτησης για την άλλη πλευρά[622]).

- ✓ Επιταχυντής Νευρωνικού Δικτύου (*Neural Network Accelerator*): οι Maji et al. πρότειναν στο άρθρο τους, ως αντίμετρο έναντι των επιθέσεων πλευρικού καναλιού μέτρησης ισχύος, την εφαρμογή ενός επιταχυντή νευρωνικού δικτύου (*Neural Network Accelerator*) που θα αξιοποιεί ένα κατώφλι (*threshold*) στην εφαρμογή του εν λόγω δικτύου για την προστασία τόσο των παραμέτρων του τελευταίου όσο και των εισόδων από πλευράς χρήστη[623]. Επίσης στο σκέλος που αφορά τις εν λόγω επιθέσεις (*power-based*) οι Takatoi et al. προτείνουν ακόμα την εφαρμογή *look-up tables* για την εφαρμογή των συναρτήσεων ενεργοποίησης, καθότι τα τελευταία επιτρέπουν την εκτέλεση των εν λόγω συναρτήσεων σε συνεχή χρόνο (ήτοι *constant-time*), και άρα αποτρέπουν τον επιτιθέμενο από το να εντοπίζει μοτίβα τυχόν διαφορών ή διακυμάνσεων στην χρονική διάρκεια όταν διενεργεί διαφόρων ειδών SCAs (π.χ. βασισμένες στις χρονομετρήσεις ή στις αντίστοιχες μετρήσεις ισχύος κλπ[624]).

Σε ότι αφορά στην τρίτη τι τάξει κατηγορία αντιμέτρων, στο σημείο αυτό θα παρουσιαστούν εν συντομία τα αντίμετρα που βασίζονται στο masking (και ακολούθως τα αντίστοιχα για το hiding). Με τον όρο masking περιγράφονται εκείνα τα αντίμετρα στόχος των οποίων είναι να ενισχύσουν την ασφάλεια ενός συστήματος διαρρηγνύοντας την σχέση ανάμεσα στην λήψη δειγμάτων ισχύος και στις ενδιάμεσες τιμές (intermediate values). Πρακτικά ο στόχος αυτός επιτυγχάνεται με το να τυχαιοποιούνται (randomization) οι ενδιάμεσες αυτές τιμές, μέσω του διαμοιρασμού τους (sharing[625]). Εμφανίζονται κι εδώ μια σειρά από παραλλαγές, όπως το

---

[622] Πρβλ. Takatoi et al. στο Takatoi, G., & Sugawara, T., & Sakiyama, K., & Hara-Azumi, Y., & Li, Y.(2022). The Limits of SEMA on Distinguishing Similar Activation Functions of Embedded Deep Neural Networks. *Applied Sciences* 2022, 12(9), 4135, 1-20, σ.8. doi: https://doi.org/10.3390/app12094135. Applied Sciences | Free Full-Text | The Limits of SEMA on Distinguishing Similar Activation Functions of Embedded Deep Neural Networks (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

[623] Ο.π.,σ.18.

[624] Ο.π.

[625] Batina, L., & Djukanovic, M., & Heuser, A., & Picek, S.(2021). It Started with Templates: The Future of Profiling in Side-Channel Attacks. Στο Avoine, G., & Hernandez-Castro, J. (επιμ.) *Security of Ubiquitous Computing Systems* (133-145), σ.145. Springer, Cham. doi: It Started with Templates: The Future of Profiling in Side-Channel Analysis | SpringerLink. [PDF] It Started with Templates: The Future of Profiling in Side-Channel Analysis | Semantic Scholar (Τελευταία πρόσβαση 25/11/2022).

Consolidated Masking Scheme, το Domain-Oriented Masking κα[626]. Σε ότι αφορά την εφαρμογή του masking (π.χ. σε επίπεδο πύλης, πρακτικά υπάρχουν τρεις τρόποι για να λάβει χώρα, είτε θα χρησιμοποιείται μια masked τιμή για κάθε σήμα, είτε μια masked τιμή για κάθε ξεχωριστή ομάδα σημάτων, είτε χρήση της ίδιας masked τιμής για το σύνολο των σημάτων της κάθε εφαρμογής[627].

Καθώς όπως έχει ήδη αναφερθεί τα αντίμετρα δεν αναλύονται εν σχέσει με την θεματική των κρίσιμων υποδομών γενικά (αλλά περισσότερο σε ότι αφορά στο IoT γενικότερα), στο σημείο αυτό θα προχωρήσουμε σε μια ενδεικτική μόνο παράθεση ορισμένων εξ' αυτών για λόγους πληρέστερης κατανόησης, ως ακολούθως:

- *iMDPL* (*"improved MDPL"*): οι Popp et al. πρότειναν την βελτίωση του αντίμετρου που αναφέρθηκε στην αρχή της παρούσης υπό-ενότητας (*MDPL,* και το οποίο όπως αναφέρθηκε μπορεί να ταξινομηθεί είτε ως αντίμετρο masking είτε ως hiding, διότι αποτελεί πρόσμειξη και των δύο). Η λογική στην οποία βασίζεται το αντίμετρο είναι αυτή της προσθήκης μιας συσκευής (EPDU, Power Distribution Unit) που θα παράγει ένα bit 0 ως έξοδο σε μια συνθήκη κατά την οποία όλες οι είσοδοι θα είναι διαφορικές (*differential state*), εισάγοντας έτσι μια τυχαιότητα και μειώνοντας την ανάμεσα στις εισόδους και την τροφοδοσία. Η λύση γενικά κρίνεται ως κοστοβόρα διότι πρέπει να δημιουργηθεί μια τυχαία masked τιμή για το σύνολο του σχεδιασμού του κυκλώματος στο οποίο το αντίμετρο πρόκειται να εφαρμοστεί[628].
- *Masked-SABL* ("*Sense Amplifier Based Logic*"): Το εν λόγω αντίμετρο (όμοια με την περίπτωση του MDPL) μπορεί να αξιοποιηθεί και συνδυαστικά, και βασίζεται στην εισαγωγή μιας *masked m* τιμής για να αποτραπεί η εμφάνιση ανισορροπίας σε ένα κύκλωμα λόγω παλαιότητας. Με την χρήση ενός NMOS transistor τοποθετημένου σε κάθε διαφορικό βρόγχο (*differential branches*), όπου η τιμή *masked*

[626] Bache, F., & Guneysu, T.(2022). Boolean Masking for Arithmetic Additions Arbitrary Order in Hardware. *Applied Sciences* 2022, 12, 2274, 1-14, σ.3. doi: https://doi.org/10/3390/app12052274. Applied Sciences | Free Full-Text | Boolean Masking for Arithmetic Additions at Arbitrary Order in Hardware (mdpi.com) (Τελευταία πρόσβαση 12/10/2022).

[627]Προφανώς με ότι αυτό συνεπάγεται για κόστος και την περιπλοκότητα σε επίπεδο σχεδιασμού των εν λόγω αντιμέτρων. Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R. (2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12 (5), 2390, 1-28, σ.15. doi: https://doi.org/10.3390/app12052274. Applied Sciences | Free Full-Text | Boolean Masking for Arithmetic Additions at Arbitrary Order in Hardware (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[628] Ο.π.,σ.17.

m ελέγχει τον ένα και ένα συμπληρωματικό σήμα της τιμής αυτής (*m*) ελέγχει τον έτερο, η λειτουργία της κάθε λογικής πύλης (η έξοδος που παράγει η πύλη επομένως) θα ενσωματώνει και την masked τιμή αναλόγως αν η τελευταία είναι 0 ή 1. Ήτοι, αν η masked τιμή είναι 0 εκτελείται η συνάρτηση *f(f)*, ενώ αν είναι 1 η εν λόγω συνάρτηση αντιστρέφεται, έτσι όσες τιμές μπορεί να χαθούν λόγω παλαιότητας του κυκλώματος (*aging*) θα αναπληρώνονται από την masked τιμή διατηρώντας μια ομοιομορφία στις εξόδους (constantness). Βασικό πρόβλημα στο εν λόγω αντίμετρο είναι εύλογα το overhead που προκαλείται λόγω της συνεπικουρίας του κυκλώματος από την masked τιμή[629].

❖ *Bitslicing & Boolean Masking*: Στοχεύοντας στην μείωση του κόστους και στην αύξηση της ταχύτητας στην εκτέλεση διεργασιών, έχουν ήδη εμφανιστεί στην διεθνή βιβλιογραφία περιπτώσεις άρθρων όπου το αντίμετρο του masking συνδυάζεται με την τεχνική bitslicing. Η συμβατότητα των δύο έγκειται στο ότι το εν λόγω φάσμα αντιμέτρων (masking) αξιοποιεί διεργασίες που βασίζονται στην αξιοποίηση των bits με τον ένα ή τον έτερο τρόπο (π.χ. τμηματοποίηση των μεταβλητών σε shares και μετά χρήση της συνάρτησης xor όπως είδαμε ήδη). Επί παραδείγματι οι Pozzobon et al. στο παράδειγμα τους (*2-shared mask adder*) καταδεικνύουν την δυνατότητα να μειωθεί το κόστος και ο συνολικός αριθμός των ωρολογιακών κύκλων (clock cycles) για την κρυπτογράφηση, με αποτέλεσμα η λύση αυτή να δύναται όπως εξοικονομήσει πόρους για εφαρμοσμένα συστήματα που φείδονται αυτών (*low powered embedded systems*, όπως MCUs, MPUs, FPGAs κλπ). Ωστόσο, οι ίδιοι συγγραφείς τονίζουν, πως στην δική τους συνθήκη, εμφανίζεται το φαινόμενο αφενός σε μικρά πακέτα πληροφοριών (*small payloads*) ο αλγόριθμος να είναι πιο αργός όταν δεν χρησιμοποιείται παραλληλισμός (*parallelism*) από κοινού με την τεχνική bitslicing και αφετέρου ο αλγόριθμος συνολικά να απαιτεί 7 φορές περισσότερη μνήμη εν σχέσει με άλλα παραδείγματα, κάτι που δημιουργεί πρόβλημα σε ότι αφορά στην προστασία ενσωματωμένων συστημάτων που εξαρχής δεν διαθέτουν αφθονία πόρων[630].

---

[629] Fadaeinia et al. στο ο.π.,σ.17-18.

[630] Ο εν λόγω συνδυασμός είναι αρκετά πολύπλοκος για να αναλυθεί εξαντλητικά στο πλαίσιο μιας , εν παρόδω, αναφοράς αντιμέτρων. Για λεπτομερέστερες αναλύσεις επί του σημείου αυτού παραθέτουμε ενδεικτικά τα κάτωθι δύο άρθρα. Αφενός για όσα παρατίθενται στην οικεία παράγραφο ορά Pozzobon, E., & Renner, S., & Mottok, J., & Matousek, V.(2022). *An optimized Bitsliced Masked Adder for ARM Thumb-2 Controllers*. Paper presented at the 2022 International Conference on Applied Elecronics (AE). Pilsen, Czech Republic. 06-07 September, 1-4, σ.1,4. doi:10.1109/AE54730.2022.9919884. An optimized Bitsliced Masked Adder for ARM

❖ *DOM* ("*Domain-Oriented Masking*"): Οι Kiaei & Schaumont προτείνουν το εν λόγω αντίμετρο πρώτης γραμμής (*first-line Masking*), με βάσει το οποίο η κάθε μεταβλητή χωρίζεται σε δύο μέρη (*shares*), και κατόπιν με μια συνάρτηση XOR ανακτάτε η αρχική αυτή μεταβλητή που βρίσκεται στο ένα από τα δύο προαναφερθέντα μέρη. Κάθε φορά που οι μεταβλητές χωρίζονται, τα ξεχωριστά τμήματα τοποθετούνται σε διαφορετικά domains, για να αποφευχθεί η εμφάνιση collision. Επιπλέον, όταν τα μέρη πρέπει να συνδυαστούν για κάποιον λόγο τότε εκ νέου γίνονται *remasked* για μεγαλύτερη ασφάλεια. Το βασικό πρόβλημα που παρουσιάζεται εδώ, και αντανακλά συνολικά σε πολλά αντίμετρα υλικού και μη, είναι ότι το σχήμα των συγγραφέων είναι θεωρητικό και η εφαρμογή του αφήνεται για μελλοντικά πονήματα, άρα και η αξιολόγηση αυτού είναι δυσχερείς (εν γένει αυτό είναι ένα στοιχείο που διακρίνει τα αντίμετρα, σε εφαρμοσμένα ή απλώς θεωρητικά, και που δεν επιτρέπει την ταξινόμηση και ευχερέστερη ενσωμάτωση γνώσης, και επομένως την επαύξηση της ασφάλειας σε συσκευές IoT[631]).

❖ *Masking with Common Shares*: Οι Wang et al. προσπαθούν να μειώσουν σε αυτό το σχήμα το overhead που προκαλείται στους υπολογιστικούς πόρους από την εφαρμογή αντιμέτρων masking, αυτό επιχειρείται με το να επιτρέπεται στις μεταβλητές που διαχωρίζονται σε τμήματα να διαθέτουν κάποια κοινά shares. Αυτό με την σειρά του επιτρέπει την εκ νέου χρήση των τυχαιοποιημένων shares χωρίς κάθε φορά να χρειάζεται η παραγωγή νέων (όπως π.χ. στο προηγούμενο παράδειγμα), κι έτσι είναι εφικτό να μειωθεί το κόστος και τα shares να χρησιμοποιηθούν και σε διάφορα gadgets. Ακόμα οι συγγραφείς προτείνουν την μείωση στην κατανάλωση πόρων μέσα από τον εκ των προτέρων υπολογισμό (precomputation) των ενδιάμεσων μεταβλητών (και την αποθήκευση τους στην μνήμη RAM) πριν την εκτέλεση της συνάρτησης masking. Κατ' αυτό τον τρόπο μειώνεται το κόστος διότι ο υπολογισμός των ενδιάμεσων διαχωρίζεται

Thumb-2 Controllers | IEEE Conference Publication | IEEE Xplore (Τελευταία πρόσβαση 5/12/2022). Αφετέρου, για μια έτερη πειραματική συνθήκη εφαρμογής ορά μεταξύ άλλων και Bronchain, O., & Cassiers, G.(2022). Bitslicing Arithmetic/Boolean Masking Conversions for Fun and Profit: with Application to Lattice-Based KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems,* 2022, 4, 553-588.doi: 10.46586/tches.v2022.i4.553-588. (PDF) Bitslicing Arithmetic/Boolean Masking Conversions for Fun and Profit: with Application to Lattice-Based KEMs (researchgate.net) (Τελευταία πρόσβαση 5/12/2022).

[631] Πρβλ. Kiaei, P., & Schaumont, P.(2020). Domain-Oriented Masked Instruction Set Architecture for RISC-V. *IACR Cryptology ePrint Archive* 2020 (2020), 465-468 (1-4), σ.2. 465.pdf (iacr.org) (Τελευταία πρόσβαση 5/12/2022).

από τις αντίστοιχες διεργασίες για τις εισόδους που δίνουν οι χρήστες (*online computation*), κι έτσι η χρήση αντιμέτρου masking δεν επιβαρύνει (και) χρονικά την εκτέλεση πρωτοκόλλων. Κι εδώ ωστόσο η συνθήκη είναι πειραματική και ισχύει η παρατήρηση της ανωτέρου παραγράφου[632].

Τα αντίμετρα τύπου hiding βασίζονται στην λογική της δημιουργίας μιας συνθήκης συμμετρίας στην κατανάλωση ισχύος (uniformity, symmetry) για όλες τις υπολογιστικές διεργασίες παραγωγής δεδομένων (δηλαδή να φαίνεται σαν να είχαν όλες τους την ίδια ακριβώς κατανάλωση πόρων κατά την εκτέλεση), ώστε ο επιτιθέμενος να μην δύναται να προβεί σε συσχετίσεις από την λήψη δειγμάτων ισχύος[633]. Το hiding διακρίνεται σε δύο κύριες υποομάδες τεχνικών το randomization και το equalization[634]. Ακολουθούν κατωτέρω ορισμένα ενδεικτικά παραδείγματα:

- *iBSPL*(“*improved Balanced Static Power Logic*”): Στο πλαίσιο της τεχνικής hiding οι Fadaeinia et al. παρουσιάζουν μιας παραλλαγή της BSPL (που αναφέρθηκε σε προηγούμενη παράγραφο του αυτού κεφαλαίου), ονόματι iBSPL (”*improved Balanced Static Power Logic*”). Συγκρίνοντας τα δύο αντίμετρα μεταξύ τους και στο πλαίσιο σεναρίου σχετικού με power analysis SCAs (με χρήση του αλγορίθμου Monte Carlo σε πειραματική συνθήκη), οι συγγραφείς καταδεικνύουν την δική τους εκδοχή ως ικανή να προσφέρει μεγαλύτερη προστασία έναντι της παραδοσιακής BSPL. Οι συγγραφείς στην δική τους εφαρμογή προτείνουν την συστηματική χρήση *off-transistors* σε κάθε γραμμή σήματος της κάθε λογικής πύλης του CMOS για να επιτευχθεί μια ομοιόμορφη κατανάλωση ισχύος ανεξαρτήτως του ποιες εισόδους δίνει ο εκάστοτε χρήστης. Οι συγγραφείς επιλέγουν να προσθέσουν *off-transistors* σε

---

[632] Wang, W., & Guo, C., & Yu, Y., & Ji, F., & Su, Y.(2022). Side-Channel Masking with Common Shares. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022 (3), 290-329, σ.290, 324-325. View of Side-Channel Masking with Common Shares (iacr.org) (Τελευταία πρόσβαση 5/12/2022).

[633] Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12 (5), 2390, 1-28, σ.1, 4. doi: https://doi.org/10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[634] Fadaeinia, B., & Moos,T., & Moradi,A.(2021). Balancing the Leakage Currents in Nanometer CMOS Logic- A Challenging Goal. *Applied Sciences* 2021, 11 (15), 7143,1-18, σ.2. doi: https://doi.org/103390/app11157143. Applied Sciences | Free Full-Text | Balancing the Leakage Currents in Nanometer CMOS Logic—A Challenging Goal (mdpi.com) (Τελευταία πρόσβαση 1/10/2022).

συγκεκριμένες εισόδους, εξόδους, και ενδιάμεσα σήματα για να αυξήσουν την στατική εκροή (*static leakage*), έτσι ώστε η τελική κατανάλωση ισχύος για κάθε λογική πύλη να παρουσιάζεται, λιγότερο ή περισσότερο, ως σταθερή (*constant*), με αποτέλεσμα ο επιτιθέμενος να μην μπορεί εύκολα να προβεί σε συσχετίσεις[635].

❖ *Homogenous dual-rail logic* (*HDLR*): Εν γένει ένα μεγάλο τμήμα των αντιμέτρων βασίζεται σχεδιαστικά σε λογικές dual-rail, δηλαδή σε προσπάθειες συμπλήρωσης του εκάστοτε κυκλώματος με συμπληρωματικά στοιχεία (complementary circuitry) ώστε η τάση στην κατανάλωση ισχύος να παρουσιάζεται ως σαν να ήταν συνεχείς και να διασπάτε κατά τον τρόπο αυτό η αιτιακή σχέση ανάμεσα στην εκροή πληροφορίας και στην αυξομείωση της τάσης του ρεύματος κατά την λειτουργία ενός κυκλώματος. Στην περίπτωση του συγκεκριμένου αντιμέτρου των Tanimura & Dutt το κύκλωμα δρομολογείται κανονικά και κατόπιν η διάταξη του εν λόγω κυκλώματος αναπαράγεται (*duplicated*) ώστε να είναι ακριβώς όμοια με το αρχικό κύκλωμα. Στην συνέχεια εφαρμόζεται η λογική dual-rail όπου οι είσοδοι του συμπληρωματικού (*complementary*) κυκλώματος είναι πανομοιότυπες με εκείνες του αρχικού κυκλώματος, κι έτσι λειτουργούν εύλογα με τρόπο συμπληρωματικό ως προς τις δεύτερες. Έτσι δίνεται στον επιτιθέμενο μια εντύπωση περί συνεχούς (constant) τάσης στην κατανάλωση ισχύος για να μην δύναται να καταλάβει ο τελευταίος ποια λειτουργία εκτελείται με βάσει τις μετρήσεις ισχύος. Βασικό πλεονέκτημα του εν λόγω αντίμετρου είναι πως βρίσκεται στον αντίποδα λογικών σχεδιασμού που προϋποθέτουν φάσεις προφόρτωσης (*precharge*) και αξιολόγησης (*evaluation*), που θα παρουσιαστούν κατωτέρω (καθώς κι αυτές απαντώνται συχνά στην βιβλιογραφία) και που κάνουν ώστε να αυξάνει το overhead και να καταναλώνονται αφειδώς οι πόροι. Ωστόσο, πρέπει να αναφερθεί πως και το συγκεκριμένο αντίμετρο παρουσιάζει ορισμένα μειονεκτήματα, που κι αυτά αναφύονται εν σχέσει με τον σχεδιασμό αντιμέτρων hiding γενικά, όπως η προϋπόθεση ύπαρξης αυξημένου χώρου στην πλάκα του κυκλώματος για να εφαρμοστεί το συμπληρωματικό κύκλωμα (το οποίο και αντιβαίνει σαφώς στην τρέχουσα σχεδιαστική λογική, που θέλει τα κυκλώματα να βαίνουν μειούμενα σε μέγεθος σε ότι αφορά τον σχεδιασμό τους), και επίσης το φαινόμενο του *early propagation*[636] (ήτοι της

[635] Ο.π.,σ.7-8, 16.

[636] Πρβλ. Moradi, A., & Immler, V.(2014). *Early Propagation and Imbalanced Routing How to Diminish in FPGAs*. Paper presented at the 16th International Workshop Cryptographic Hardware and Embedded Systems

αξιολόγησης εισόδου σε διαφορετικά χρονικά διαστήματα, η οποία όπως θα φανεί κατωτέρω αντιμετωπίζεται όταν το αντίμετρο εφαρμόζει φάσεις προφόρτωσης και αξιολόγησης) που επιτρέπει στον επιτιθέμενο να αντλήσει πληροφορίες επί τι βάσει χρονικών μετρήσεων (π.χ. timing-based SCA[637]).

❖ *Three-phase dual-rail precharge logic* (*TDPL*): Το αντίμετρο αυτό όπως υπαγορεύει και η ονομασία του λειτουργεί σε τρεις φάσεις. Στην πρώτη, την φάση της προφόρτωσης (precharge phase), οι έξοδοι προφορτίζονται (precharge) μέσω του V_{dd} ενώ στις δύο επόμενες φάσεις (φάση αξιολόγησης, evaluation, και φάση εκκένωσης, discharge phase) οι έξοδοι εκκενώνονται (discharge) μέσω του GND. Με τον τρόπο αυτό η κατανάλωση ισχύος παρουσιάζεται ως σταθερή και δεν δυσχαιρένει τον επιτιθέμενο στην προσπάθεια ανακάλυψης συσχετίσεων ακόμα και υπό την παρουσία αστοχιών χωρητικότητας (capacitance missmatches). Ωστόσο, η συγκεκριμένη μέθοδος οδηγεί αναπότρεπτα σε αυξημένες απαιτήσεις κατανάλωσης ισχύος, μια απαίτηση που τα ενσωματωμένα συστήματα δύσκολα μπορούν φέρ' ειπείν να εκπληρώσουν, αλλά και πιθανή εκροή πληροφοριών χρονομέτρησης (timing leakage) καθώς οι τρείς εν λόγω φάσεις λαμβάνουν χώρα με ορισμένη χρονική ακολουθία (*timing diagram*[638]).

❖ *Randomized multitopology logic* (*RMTL*): Πρόκειται για αντίμετρο τυχαιοποίησης του προφίλ τροφοδοσίας ρεύματος σε επίπεδο πύλης (gate-level). Ουσιαστικά μια γεννήτρια τυχαίων αριθμών (*RNG*) παράγει ένα σήμα ελέγχου (control signal) το οποίο καθορίζει κάθε φορά μια τυχαία τοπολογία (*random topology*) για κάθε μια πύλη, ώστε να φαίνεται σαν έχει αυτή η τελευταία μια διαφορετική κατανάλωση ισχύος από την υπάρχουσα. Αυτή η τεχνητά προκληθείσα αυξομείωση τιμών τάσεως είναι το βασικό πλεονέκτημα της μεθόδου, καθώς η απουσία της ανάγκης για τέλεια συμμετρία, κάνει την εν λόγω παραλλαγή περισσότερο ή λιγότερο απρόσβλητη σε διάφορες διακυμάνσεις (π.χ. λόγω παλαιότητας του κυκλώματος όπως είχε αναφερθεί παραπάνω όταν ο λόγος γινόταν για τα αντίμετρα masking). Από την άλλη η μέθοδος

(CHES 2014). Busan, South Korea. 23-26 September, 1-18, σ.2. doi:10.1007/978-3-662-44709-3_33. 454.pdf (iacr.org) (Τελευταία πρόσβαση 7/12/2022).

[637] Tena-Sanchez,E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28, σ.6. doi:https://doi.org/10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[638] Ο.π.,σ.9.

κρίνεται ως κοστοβόρα αφού απαιτεί την χρήση *RNG,* ενώ ταυτόχρονα πρέπει να συμπληρώνεται και από άλλα αντίμετρα (με το όποιο κόστος) διότι οι τυχαίες διακυμάνσεις ισχύος που αξιοποιεί οδηγούν σε εκροές που μπορούν ενδεχόμενα να εκμεταλλευτούν οι SCAs, όπως οι DPAs για παράδειγμα (Differential Power Analysis[639]).

❖ *Glitch-free duplication* (*GliFreD*): Πρόκειται για αντίμετρο που σχεδιάστηκε αποκλειστικά με γνώμονα τον σχεδιασμό των FPGAs. Η λογική του σχεδιασμού σε αυτό το αντίμετρο αφορά στην συνδυαστική χρήση αφενός των *LUTs* (*Lookup Tables*) και αφετέρου των *Master-Slave-flip-flops* (*FFs*[640]). Το κάθε *LUT* ενεργοποιείται από ένα *global signal* και παράγει κατόπιν ως έξοδο ένα *register* (επίσης *globally-enabled*). Από την άλλη ανάμεσα σε κάθε *LUT* παρεμβάλλεται και από ένα *FF* με στόχο να αποτρέψει την ,κατά άμεσο τρόπο, μετάβαση από το ένα *LUT* στο αμέσως επόμενο. Κάθε LUT είναι συνδεδεμένο με δύο global signals(*active* & *CLK*) ένα για την φάση προφόρτωσης (*precharge phase*) και έτερος για την φάση αξιολόγησης (*evaluation phase*), η σύνδεση των δύο σε δύο διαφορετικά *multiplexer* επίπεδα (0 & 1) πρέπει να λαμβάνει χώρα κάθε φορά, διότι με τον τρόπο αυτό αποφεύγονται τα glitches των δεδομένων του κάθε *LUT*.

Κατόπιν, στο σχεδιαστικό σκέλος, όλο το κύκλωμα πρέπει να αντιγραφεί και να συνεπικουρείται από ένα αντίστοιχο εφεδρικό (*duplication*), καθώς μόνο έτσι θα επιτυγχάνεται ένας σταθερός αριθμός αλλαγής πύλης(*constant number of gate toggling*) για όλη την λειτουργία του κυκλώματος(αυτό συμβαίνει διότι στο συγκεκριμένο σχήμα δεν επαρκεί η χρήση μόνο ενός *FF* μετά από κάθε LUT για να επιτευχθεί η σταθερότητα, και επομένως πρέπει όλα τα στοιχεία του κυκλώματος να εφαρμόζουν την λογική των φάσεων προφόρτωσης & αξιολόγησης που ακολουθούν εδώ τα *FFs*[641]). Το βασικό μειονέκτημα του εν λόγω αντίμετρου έγκειται στην σχεδιαστική του πολυπλοκότητα και επίσης στην ανάγκη ύπαρξης διευρυμένου χώρου στην πλάκα του κυκλώματος, καθώς όλα πρέπει να γίνονται εις διπλούν, ήτοι πρέπει να υφίστανται τόσα *FFs* όσα *LUTs* υπάρχουν, επίσης πρέπει να υφίστανται διπλά σήματα ελέγχου και συμπληρωματικά

[639] Ο.π.,σ.12.

[640] Ο.π.,σ.12.

[641] Πρβλ. Wild, A., & Moradi, A., & Guneysu, T.(2018). GliFreD: Glitch-Free Duplication Towards Power-Equalized Circuits on FPGAs. *IEEE Transactions on Computers*, 67, 3, 375-387 (1-8), σ.2-3. Doi: 10.1109/TV.2017.2651829. *124.pdf (iacr.org) (Τελευταία πρόσβαση 14/10/2022).

κυκλώματα, κάτι που οδηγεί αναπόδραστα σε επιπλέον κόστη (επίσης δε και ανάγκη για αυξημένους πόρους επί εφαρμοσμένων συστημάτων που δεν έχουν αυτή την δυνατότητα) καθώς και σε πιθανή αδυναμία μαζικής κατασκευής τέτοιων κυκλωμάτων από πλευράς των κατασκευαστών[642].

❖ "*Dual-Hiding SCA Resistant FPGA- Based Asyncrhonous-Logic AES*[643]": Οι Chong et al. παρουσιάζουν ένα αντίμετρο που επιχειρεί να αξιοποιήσει το hiding επί τι βάσει δύο αξόνων, ήτοι της διαρρύθμισης του εύρους του κυκλώματος (*amplitude moderation*, κάθετος άξονας) και επίσης της χρονικής διαρρύθμισης (*time moderation*) στον οριζόντιο άξονα αυτή την φορά. Στην πειραματική τους συνθήκη οι ερευνητές πρότειναν, σε πειραματική συνθήκη επί ενός κυκλώματος ασύγχρονης λογικής , *async-logic circuit*, με δοκιμή επί των FPGAs *Sakura-X* & *Arty-7,* την χρήση αφενός της γραμμής ελέγχου τυχαιοποιημένης λογικής (*randomized delay-line control*) και αφετέρου την χρήση του ελέγχου πολλαπλασιασμού δεδομένων ασύγχρονης λογικής (*async-logic data-propagation control*), προς επίτευξη ενός hiding αντίμετρου που θα εδράζεται επί των δύο ως άνω αξόνων[644].

Πρακτικά οι συγγραφείς παρουσιάζουν, μεταξύ άλλων, έναν συνδυασμό παραδεδεγμένων αντιμέτρων, καθώς στον μεν οριζόντιο άξονα του αντίμετρου εισάγουν τυχαίες καθυστερήσεις στην παραγωγή και επεξεργασία των δεδομένων (*randomized data-driven delays*) μέσω της εισαγωγής *delay jitters.* Ενώ στον δε κάθετο άξονα επιχειρούν την εισαγωγή κάποιου θορύβου (*noise injection*) μαζί με τον έλεγχο των δεδομένων που αναφέρθηκε ανωτέρω για να καλυφθούν οι ηλεκτρομαγνητικές αυξομειώσεις στην κατανάλωση ισχύος. Ειδικότερα οι συγγραφείς του εν λόγω πονήματος συνδυάζουν έως και 5 ξεχωριστά αντίμετρα για να επιτύχουν το διπλό hiding

---

[642] Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28, σ.12. doi: https://doi.org/10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[643] Chong, K.-S., & Ng, J.-S., & Chen, J., & Lwin, N.K.Z., & Kyaw, N.A., & Ho, W.-G., & Chang, J., & Gwee, B.-H.(2021). Dual-Hiding Side-Channel-Attack Resistant FPGA-Based Asynchronous-Logic AES: Design, Countermeasures and Evaluation. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 11, 2, 343-356 (1-15), σ.1. doi:10.1109/JETCAS.2021.3077887. Dual-Hiding Side-Channel-Attack Resistant FPGA-Based Asynchronous-Logic AES: Design, Countermeasures and Evaluation | IEEE Journals & Magazine | IEEE Xplore (Τελευταία πρόσβαση 7/12/2022).

[644] Ο.π.,σ.12.

στους δύο άξονες (για έλεγχο της κατανάλωσης ισχύος στον κάθετο άξονα και για αντίστοιχο έλεγχο του χρόνου εκτέλεσης στον οριζόντιο). Εν συντομία τα πέντε αυτά συνδυαστικά αντίμετρα έχουν ως εξής:

I. Χρήση ενός κυκλώματος για δημιουργία και αποστολή σήματος (*32-bit signal circuit,Sel*) με στόχο την εισδοχή τυχαίων καθυστερήσεων (*randomized*) για να λειτουργούν από κοινού με την ασύγχρονη λογική του κυκλώματος. Το εν λόγω κύκλωμα χρησιμοποιεί μια σειρά από συναρτήσεις XOR για να μετατρέψει το μέγεθος των δεδομένων που κρυπτογραφούνται σε ένα αντίστοιχο του κυκλώματος αυτού, αυτό συμβαίνει για τον πρώτο κύκλο κρυπτογράφησης του AES(ως μέτρο προστασίας για την περίπτωση που ο επιτιθέμενος επιχειρήσει να προμηθευθεί κι εκείνος ένα κύκλωμα *Sel* για τους σκοπούς της επιθέσεως του), ενώ για κάθε επόμενο γύρο το *Sel* παράγει το σήμα του με βάσει την ακριβώς προηγούμενη έξοδο κρυπτογράφησης (ήτοι από τα 128-bit στα 32-bit[645]).

II. Τυχαία εφαρμογή του σήματος του 32-bit κυκλώματος *Sel* σε διαφορετικές κάθε φορά γραμμές καθυστέρησης (*delay-lines*), με την κάθε μια γραμμή να παρουσιάζει 32 διαφορετικές καθυστερήσεις με ελέγχους της τάξεως των 5-bit. Όλες αυτές οι καθυστερήσεις εφαρμόζονται επομένως τυχαία κατά τις διεργασίες κρυπτογράφησης δεδομένων, κλειδιού και σημάτων ελέγχου σε κάθε γύρο, με απώτερο σκοπό τον έλεγχο (ορθότερα συγκάλυψη) των εμφανιζόμενων υψηλών τάσεων (peaks) καθ' εκάστη στιγμή (ώστε η κατανάλωση ρεύματος να παρουσιάζεται ως συνεχώς σταθερή[646]).

III. Ενεργοποίηση των λογικών κυκλωμάτων latches με χρήση 4 σημάτων reset (*NRST*). Με τον τρόπο αυτό η εκκίνηση των κυκλωμάτων γίνεται τυχαία κι έτσι μπορεί να ελεγχθούν οι παράμετροι χρόνου και κατανάλωσης ισχύος για τις διεργασίες που αφορούν στα *dual-rail* μακροκελιά (*macrocells*[647]).

IV. Αξιοποίηση *backward delay controls* (για τα στάδια 1 & 2) για καλύτερο έλεγχο στην σταθεροποίηση των χρονικών διακυμάνσεων (timing) σε κάθε γύρο κρυπτογράφησης του AES. Στο πρώτο στάδιο γίνεται η χειραψία για το κλειδί και τα δεδομένα ώστε μέσω της πύλης *CMuller* να συνδυαστούν τα

[645] Ο.π.,σ.7.

[646] Ο.π.

[647] Ο.π.

σήματα ολοκλήρωσης αυτών των δύο. Κατόπιν του συνδυασμού αυτού 4 γραμμές καθυστέρησης (ελεγχόμενες από το *SEL*) αναλαμβάνουν να δημιουργήσουν *delay jitters* για τα 4 SBoxes κατά την λειτουργία του κυκλώματος ασύγχρονης λογικής. Εν συνεχεία, στο δεύτερο στάδιο αυτή την φορά, μια από τις γραμμές καθυστέρησης παράγει ένα σήμα *Cont,* ώστε να μην εξαρτιόνται όλες οι διαφορετικές χρονοκαθυστερήσεις μόνο από το κύκλωμα *SEL* (για τον ίδιο λόγο με πριν, ήτοι για να προβλεφθεί η συνθήκη κατά την οποία ο επιτιθέμενος θα δημιουργήσει κι εκείνος ένα αντίστοιχο κύκλωμα, π.χ. σε περιπτώσεις *template Attacks* κλπ[648]).

V. Το χρονικό εύρος των τυχαίων καθυστερήσεων έχει ένα ανώτατο και ένα κατώτατο όριο (*min-max*). Η λογική που υπαγορεύει αυτά τα ανώτατα και κατώτατα όρια είναι αφενός η φύση του ίδιου κυκλώματος που παράγει τις καθυστερήσεις, κι έτσι οι καθυστερήσεις που εμφανίζονται και στους δέκα γύρους κρυπτογράφησης του AES είναι περίπου ίδιες σε χρονικό μέγεθος και λειτουργούν αθροιστικά (η καθυστέρηση του ενός γύρου προστίθεται στον επόμενος κοκ) για να δώσουν το τυχαιοποιημένο αποτέλεσμα να διαρραγεί η σχέση εκροής-πληροφοριών. Αφετέρου, τα όρια προσδιορίζονται και από την εξάρτηση των ίδιων των δεδομένων από την ασύγχρονη λογική που διέπει το κύκλωμα. Αυτό συνεπάγεται πως οι καθυστερήσεις θα είναι εν τέλει ομοιογενείς λιγότερο ή περισσότερο, καθώς μια μικρότερη καθυστέρηση στον ένα γύρο θα εξισορροπείται από μια μεγαλύτερη σε έναν άλλο, και στο τέλος όλες θα κινούνται γύρω από έναν μέσο όρο, που θα τις εμφανίζει χωρίς μεγάλες αποκλίσεις κατά την προσπάθεια του επιτιθέμενου να εξετάσει τα δείγματα χρονομέτρησης (άρα ο χρόνος θα παρουσιάζεται, λόγω των μέσων καθυστερήσεων ως συνεχής[649]).

❖ *Cell delay-based dual-rail precharge logic* (*SC-DDPL*): Οι Bellizia et al. ερευνούν στο πόνημα τους την δυνατότητα εφαρμογής μιας μεθόδου dual-rail επί σταθερών πυλών (*standard gates*). Η μέθοδος που προτάθηκε από τους συγγραφείς βασίστηκε επομένως στην λογική των *standard cells* (*DPL logic*) με

[648] Ο.π.

[649] Οι συγγραφείς στο σημείο αυτό τονίζουν ότι η σημασία για τον οριζόντιο άξονα έγκειται περισσότερο στο αθροιστικό στοιχείο (άθροισμα των καθυστερήσεων του κάθε γύρου) και λιγότερο στον μέσο όρο αυτόν. Ο.π.,σ.7-8.

χρήση κωδικοποιήσεως *TEL*(*Time Enclosed Logic*).Η διαφορά σε ότι αφορά στην κωδικοποίηση, στην περίπτωση του *TEL*, είναι ότι οι λογικές τιμές (*logic values*) κωδικοποιούνται όχι επί τι βάσει της κατανάλωσης ισχύος (*voltage domain*) αλλά επί της χρονικής διαφοράς στην κωδικοποίηση των δύο σημάτων που προκύπτουν από την λογική dual-rail[650]. Αυτή η μετατόπιση μπορεί να μειώσει την πιθανότητα ο επιτιθέμενος να εκμεταλλευτεί με επιτυχία τις εκροές, διότι το σκέλος του χρόνου δεν επηρεάζεται άμεσα από τις όποιες ανισορροπίες στην χωρητικότητα του φορτίου που μεταφέρεται εντός του κυκλώματος (*capacitance unbalances*).

Επιπλέον, η χρήση της κωδικοποίησης *TEL* επιτρέπει την αντιμετώπιση ευπαθειών ασφαλείας (π.χ. *capacitance mismatches*) καθώς μέσω αυτής η φάση αξιολόγησης (*evaluation phase*) διαρκεί συγκριτικά λιγότερο εν σχέσει με έτερες περιπτώσεις. Λόγω της μικρής διάρκειας της φάσεως αυτής η δυναμική κατανάλωση ισχύος για την παραγωγή των δεδομένων λαμβάνει χώρα μόνο σε πολύ υψηλές συχνότητες, και οι συγγραφείς , μεταξύ άλλων προτείνουν εδώ την χρήση *on-chip* φιλτραρίσματος για την μείωση της πιθανότητας εμφάνισης εκροών από την επεξεργασία δεδομένων σε υψηλές συχνότητες. Επομένως με τον τρόπο αυτό επιτυγχάνεται και η φαινομενική σταθερότητα (constant) στην κατανάλωση ισχύος[651].

Εν γένει, το παρόν σχήμα διαθέτει το βασικό πλεονέκτημα τόσο της εφαρμογής σε FPGAs ή ASICs ενσωματωμένα συστήματα, όσο και το (από σχεδιαστικής απόψεως) ευεργέτημα να μένει σχετικά ανεπηρέαστο από ευπάθειες σχετικές με την χωρητικότητα (*mismatches*[652]). Ωστόσο, πρόκειται εκ νέου για

---

[650] Πρβλ. το άρθρο των Bellizia et al. στο πόνημα των Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28, σ.13. doi: https://doi.org/10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[651] Πρβλ. Bellizia, D., & Bongiovanni, S., & Olivieri, M., & Scotti, G.(2020). SC-DDPL: A Novel Standard-Cell Based Approach for Counteracting Power Analysis Attacks in the Presence of Unbalanced Routing. *IEEE Transactions on Circuits and Systems I: Regular Papers,* 67, 7, 2317-2330(1-14), σ.1,12. Doi:10.1109/TCSI.2020.2979831. (uniroma1.it) (Τελευταία πρόσβαση 7/12/2022).

[652] Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12 (5), 4135, 1-28, σ.13. doi: https://doi.org/10.3390/app12052390. Applied Sciences | Free Full-Text | Gate-

πειραματική συνθήκη που εμφανίζει και πάλι την έλλειψη scalability καθώς σχεδιάζεται με γνώμονα συγκεκριμένες αρχιτεκτονικές εφαρμοσμένων συστημάτων (περισσότερα για το εν λόγω σημείο αναφέρονται και στα συμπεράσματα του τρέχοντος κεφαλαίου).

Ολοκληρώνοντας την υπό-ενότητα που αφορά στα αντίμετρα υλικού παραθέτουμε την πρωτόλεια παρατήρηση (που θα αναλυθεί κάπως εκτενέστερα κατωτέρω, στα συμπεράσματα του οικείου κεφαλαίου) πως, πέρα από τις όποιες αδυναμίες και τα μειονεκτήματα που εμφανίζουν (π.χ. ευρεία κατανάλωση πόρων, ασυμμετρίες στις πατέντες των κυκλωμάτων κλπ), τα αντίμετρα που μελετήθηκαν και παρουσιάστηκαν ανωτέρω σε ένα αρκετά μεγάλο βαθμό καταργούν τον ίδιο τον σκοπό του σχεδιασμού και της εφαρμογής τους. Αυτό σημαίνει πως παρατηρείται η ενδογενής τάση αρκετά αντίμετρα π.χ. αντίμετρο *RMTL, TDPL* κλπ) να εφαρμόζουν τεχνικές που ενώ μειώνουν την πιθανότητα ο επιτιθέμενος να εκμεταλλευτεί μια συγκεκριμένη εκροή, σχεδόν ταυτόχρονα όμως αφήνουν ανοικτό το ενδεχόμενο να δημιουργηθεί, ή να αυξηθεί, μια άλλη εκροή που θα καταστήσει το αντίμετρο ευπαθές σε μια άλλη παραλλαγή των SCAs. Ήτοι, και τα αντίμετρα σε κάποιο βαθμό εμπίπτουν στην ίδια λογική που καθιστά και τις συσκευές IoT ευάλωτες έναντι των SCAs, δηλαδή ευπάθεια που προκύπτει όχι από μια σχεδιαστική αδυναμία (ή σφάλμα), αλλά σε εκείνη που προκύπτει από την ίδια την λειτουργία αυτών.

Αντίμετρα περιβάλλοντος (Workspace Countermeasures)

Διάγραμμα 4. *Παράμετροι συγκροτήσεως των αντιμέτρων περιβάλλοντος έναντι των SCAs*[653]

Η τρίτη κατηγορία αντίμετρων που θα παρουσιαστεί στο κεφάλαιο αυτό ενέχει έναν πιο γενικό χαρακτήρα εν σχέσει με τις δύο προηγηθείσες. Ο συμπεριφοριστικός χαρακτήρας του

Level Hardware Countermeasure Comparison against Power Analysis Attacks (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[653] Το σχήμα είναι του συγγραφέως.

ανθρώπινου παράγοντα ενυπάρχει και στις δύο προηγούμενες κατηγορίες, αλλά εδώ πρέπει να ληφθεί υπόψη συνδυαστικά με την παράμετρο της χωροθέτησης εντός μιας οποιασδήποτε κρίσιμης υποδομής. Κάποια κοινώς παραδεκτά παραδείγματα παρατίθενται αμέσως κατωτέρω:

- Ζωνοποίηση (*Zoning*): Πρόκειται για αντίμετρο που αρχικά είχε προταθεί από τον NSA στις αρχές της δεκαετίας του '80. Η λογική του εν λόγω αντιμέτρου εδράζεται στο στοιχείο της απόστασης/εγγύτητας που χαρακτηρίζει τις SCAs στις σχέσεις τους με τους attack vectors. Καθώς όπως καταδείχθηκε ανωτέρω πολλές SCAs χρησιμοποιούν hopping για να φτάσουν στην καταγραφή εκροής από την συσκευή στόχο, και επομένως προϋποθέτουν μια σχετική εγγύτητα σε αρκετές περιπτώσεις (φυσικά όχι πάντα), τότε προτείνεται η δημιουργία μια ζώνης γύρω από την εκάστοτε συσκευή στόχο (π.χ. περιμετρικά ενός ενσωματωμένου συστήματος), εντός της οποίας περιμέτρου δεν θα υπάρχει κανενός είδους ηλεκτρονικός εξοπλισμός. Έτσι ούτε ο επιτιθέμενος θα μπορεί να τοποθετήσει πλησίον της συσκευής κάποιο μηχάνημα καταγραφής εκροών, ή να πλησιάσει την συσκευή με αυτό, ούτε και θα υφίστανται έτερες συσκευές που θα ενισχύουν (hopping) την εμβέλεια της όποια SCA. Εύλογα η πρακτικότητα του αντίμετρου αυτού βαίνει μειούμενη, καθώς η ανάπτυξη των κρίσιμων υποδομών αυξάνει αναλογικά και τον αριθμό ηλεκτρονικών συστημάτων εντός αυτής, αλλά ταυτόχρονα και η εξέλιξη των SCAs δύναται όπως αυξήσει την εμβέλεια των τελευταίων[654].
- Τοποθέτηση Περιβλήματος εξοπλισμού (*shielding equipment*): Ενδεχομένως το πλέον διαδεδομένο αντίμετρο σε αυτή την κατηγορία. Η μείωση των εκροών επιτυγχάνεται εδώ με την κάλυψη του attack vector μέσω της χρήσης μαγνητικών ή αγώγιμων υλικών, με αποτέλεσμα να απομονώνεται κατάλληλα η συσκευή από εξωτερικές προσπάθειες λήψης δειγμάτων. Εύλογα, ανάλογα με το asset που γίνεται στόχος πρέπει να υπάρχει και διαφορετικό είδος περιβλήματος προς χρήση, καθώς η χρήση αυτού μπορεί σε κάποιες περιπτώσεις είτε να μην είναι εφικτή (π.χ. android συσκευές) ή να μειώνει την λειτουργικότητα (π.χ. μπορεί να συμβεί με οθόνες

[654] Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O., & Nogues, E., Molton, St. (2021). Whispering Devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer, 2021, 10.007/s41635-021-00112-6. Hal-03176249,* 1-24,σ.14. Whispering devices: A survey on how side-channels lead to compromised information (archives-ouvertes.fr) (Τελευταία πρόσβαση 22/11/2022).

υπολογιστών). Εν γένει για την προστασία οθονών (π.χ. touch screens) έχει προταθεί και η χρήση φίλτρων οθόνης (polarizing filters[655]).

- Τοποθέτηση περιβλήματος υποδομών (*Shielding Structure*): Περίπτωση αντιμέτρου που ομοιάζει με την προηγούμενη παράγραφο, με την βασική διαφοροποίηση την κλίμακα εφαρμογής. Εδώ το αντίμετρο του περιβλήματος καλύπτει το σύνολο ενός κτιρίου, ή πιο ρεαλιστικά, ενός ορισμένου χώρου που υπάγεται στην κατηγορία της κρίσιμης υποδομής ώστε να αποκλειστεί η δυνατότητα του επιτιθέμενου να συλλέξει εκροές από το εσωτερικό του. Πρόκειται για αντίμετρο που είναι περισσότερο δυσχερές σε σχέση με το προηγούμενο ως προς την εφαρμογή του, αφενός για λόγους προϋπολογισμού (budget) και αφετέρου διότι η ορθή εφαρμογή του θα προϋπέθετε την κάλυψη επίσης των μερών της υποδομής που διέρχονται του χώρου αυτού (π.χ. υδραυλικές σωληνώσεις, ηλεκτρικά καλώδια κλπ) και άρα θα έπρεπε να λάβει υπόψη της την αρχιτεκτονική της κατασκευής του χώρου αυτού (κάτι που δεν είναι πάντα εφικτό δεδομένου ότι κάποιες εγκαταστάσεις νοικιάζονται και δεν κατασκευάζονται εξ' αρχής για τις ανάγκες μιας κρίσιμης υποδομής[656]).

Υπό-ενότητα 4.2: Η αξιοποίηση των SCAs ως αντιμέτρων καθαυτών

Σε ορισμένες, σπανίως παρατηρούμενες, περιπτώσεις κατά την βιβλιογραφική ανασκόπηση παρατηρείται το φαινόμενο οι ερευνητές να ακολουθούν την ακριβώς αντίστροφη οδό εν σχέσει με τις παραπάνω κατηγορίες. Έτσι, αντί να μελετήσουν τύπους αντιμέτρων έναντι των SCAs, επιλέγουν να αναδείξουν την μελέτη των εκροών για σκοπούς που θα εξυπηρετούν την ηλεκτρονική εγκληματολογία (ήτοι forensics[657]). Η προοπτική αυτή, αν και δεν έχει

[655] Ο.π.

[656] Ο.π.,σ.14-15.

[657] Σημειώνεται εδώ πως η χρήση τεχνικών που διενεργούνται εν γένει σε επιθέσεις για λόγους προστασίας έναντι των SCAs είναι μια ευρύτερη κατηγορία που σποραδικά μπορεί να εντοπιστεί στην βιβλιογραφία περί των αντιμέτρων κατά των επιθέσεων πλευρικού καναλιού. Επί παραδείγματι, οι Gu et al. στο συγγραφικό τους πόνημα μεταξύ άλλων αναφέρουν στο πλαίσιο αντιμέτρων έναντι επιθέσεων πλευρικού καναλιού που προβαίνουν σε χρήση μηχανικής μάθησης για την δημιουργία μοντέλων επιθέσεως (π.χ. template attacks) την περίπτωση της One-Pixel attack, όπου με την αλλαγή ενός και μόνο pixel δύναται να καταστεί εφικτό να εξαπατηθεί ο classifier ενός μοντέλου που βασίζεται επί της μηχανικής μαθήσεως. Η παρούσα υπό-ενότητα δεν επικεντρώνει σε τέτοιες περιπτώσεις, παρόλ' αυτα ορά ενδεικτικά Gu, R., & Wang, P., & Zheng, M., & Hu, H., & Yu, N.(2020). Adversarial Attack Based Countermeasures against Deep Learning Side-Channel Attacks. Journal of University of Science and

μελετηθεί ιδιαίτερα μέχρι και την στιγμή που ολοκληρώθηκε η ανά χείρας διπλωματική εργασία, εντούτοις μπορεί να αξιοποιηθεί από τους ειδικούς της εκάστοτε κρίσιμης υποδομής τόσο για την καλύτερη κατανόηση των επιθέσεων καθαυτών, όσο και για την συνδρομή που μια τέτοια προοπτική δύναται να προσφέρει στην προσπάθεια σχεδιασμού και τυποποίησης των αντιμέτρων, ώστε τα τελευταία να μπορούν κατά το δυνατόν να προσαρμοστούν στις ανάγκες και τον σχεδιασμό καθεκάστης κρίσιμης υποδομής. Ενδεικτικά παραθέτουμε κατωτέρω ορισμένα παραδείγματα χρήσης των πλευρικών καναλιών στο πλαίσιο της θεματικής των αντιμέτρων:

- Οι Tsalis et al. τονίζουν την ύπαρξη μιας σειράς αναφορών στην διεθνή βιβλιογραφία οι οποίες καταδεικνύουν την χρήση διαφόρων πλευρικών καναλιών (π.χ. ηλεκτρομαγνητικών εκροών, εκροών κατανάλωσης ισχύος κλπ) στο εγχείρημα του εντοπισμού ανωμαλιών (anomaly detection) , επί παραδείγματι, κατά την λειτουργία ενός επεξεργαστή ή ενός κυκλώματος κλπ. Οι προσπάθειες εντοπισμού τυχόν επιθέσεων κατά της εύρυθμης λειτουργίας των συσκευών του διαδικτύου των Πραγμάτων σε μια κρίσιμη υποδομή μέσα από την χρήση πλευρικών καναλιών, βασίζονται (παρά τις διαφορετικές μεθοδολογίες που παρουσιάζονται στην βιβλιογραφία) στην καταγραφή της τυπικής λειτουργίας του εκάστοτε καναλιού (μέσω συλλογής δειγμάτων/δεδομένων), και κατόπιν της σύγκρισης των δειγμάτων αυτών με έτερα δεδομένα από την λειτουργία καθεκάστης συσκευής (embedded system, IoT devices), για τυχόν εντοπισμό διαφόρων ανωμαλιών σε αυτή την τελευταία[658].
- Στο συγγραφικό πόνημα των Sayakarra et al. εξετάζεται επιπλέον η προοπτική της αξιοποίησης των ηλεκτρομαγνητικών εκροών (EM SCAs) στο πλαίσιο της ψηφιακής εγκληματολογίας (digital forensics).Οι συγγραφείς τονίζουν την έλλειψη σχετικών προτύπων σε ότι αφορά στην χρήση των EM SCAs στο πλαίσιο των forensics

Technology of China, 50(10), 1343-1358 (1-22), σ.6. (PDF) Adversarial Attack Based Countermeasures against Deep Learning Side-Channel Attacks (researchgate.net) (Τελευταία πρόσβαση 25/11/2022).

[658] Πρβλ. την αντίστοιχη εργογραφία στο πόνημα των Tsalis, N., & Vasilelis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems, 283-313. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos (Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311). Cham:Springer.https://www.researchgate.net/profile/Luca-Faramondi/publication/330072032_Identification_of_Vulnerabilities_in_Networked_Systems_Theories_Methods_Tools_and_Technologies/links/5c6d7ac192851c1c9df11ca4/Identification-of-Vulnerabilities-in-Networked-Systems-Theories-Methods-Tools-and-Technologies.pdf#page=281 (Τελευταία πρόσβαση 16/9/2021).

(τόσο για εργαλεία όσο και για αντίστοιχα frameworks), αλλά παραθέτουν ενδεικτικά ορισμένα εργαλεία για τους σκοπούς ενός τέτοιου εγχειρήματος. Τέτοια εργαλεία αποτελούν το TempestSDR και το HackRF για την μέτρηση ηλεκτρομαγνητικών εκροών εξ οθόνης, και ακόμα το SCAP framework, αυτό το τελευταίο δύναται όπως παράσχει (μελλοντικά έστω) μια πλατφόρμα για την δημιουργία εργαλείων προς συλλογή και χρήση (και για σκοπούς forensics) εκροών πλευρικού καναλιού. Το ζήτημα της δημιουργίας τέτοιων πλατφορμών για σχεδιασμό και εφαρμογή αντιμέτρων αναδεικνύει, εν τέλει, και την πτυχή της ενσωμάτωσης γνώσεως στο πλαίσιο ενός οργανισμού (κρίσιμη υποδομή) για την προστασία των IoT συσκευών του[659].

Υπό-ενότητα 4.3: Ενδεικτικές κατευθυντήριες (Indicative Guidelines) έναντι των SCAs για την προστασία των συσκευών του Διαδικτύου των Πραγμάτων (IoT) στις Κρίσιμες Υποδομές

Στο σχήμα που ακολουθεί αμέσως κατωτέρω συνοψίζονται οι βασικές δυσχέρειες που αναφύονται κατά την παράθεση και σχετική συζήτηση των αντιμέτρων που προηγήθηκε σε αυτό το κεφάλαιο, ως προς τον σχεδιασμό, την εφαρμογή, και την επιστημονική αξιολόγηση τους, όπως αυτά παρουσιάζονται στο πλαίσιο της διεθνούς βιβλιογραφίας που μελετήθηκε δειγματοληπτικά:

[659] Για το έργο των Blanco et al. (SCAP Framework) πρβλ. ενδεικτικά Sayakkara, A., & Le-Khac, N.A., & Scanlon, M.(2019). A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics. *Digital Investigation*, 29, 43-54(1-14), σ.8-9. doi: [1903.07703] A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics (arxiv.org). 1903.07703.pdf (arxiv.org) (Τελευταία πρόσβαση 12/10/2021).

Διάγραμμα 5. *Συνόψιση παραμέτρων που δυσχεραίνουν τον σχεδιασμό & την εφαρμογή αντιμέτρων εν γένει (software & hardware Countermeasures[660])*

Στο πλαίσιο των γενικότερων συμπερασμάτων που καταλήγει το κεφάλαιο αυτό μετά τις ενδεικτικές παραθέσεις αντιμέτρων και την εξίσου ενδεικτική παράθεση των μεταβλητών των σχετικών με την ταξινόμηση των πρώτων, επιχειρείτε μια σχηματική παράθεση κατευθυντήριων για την προστασία των κρίσιμων υποδομών έναντι των επιθέσεων πλευρικών καναλιών. Η ανάλυση των συμπερασμάτων και κατευθυντήριων που ακολουθεί είναι ενδεικτική, σε καμία περίπτωση εξαντλητική, και προσπαθεί να καλύψει το κενό που υπάρχει στην βιβλιογραφία και που αφορά στην μελέτη των SCAs υπό το πρίσμα της προστασίας των κρίσιμων υποδομών όπως έχει ήδη αναφερθεί ανωτέρω. Οι κατευθυντήριες ενδεικτικά θα μπορούσαν να περιλαμβάνουν τα κατωτέρω σημεία (συμπεράσματα):

- Για την αποτελεσματικότερη εφαρμογή των αντιμέτρων οι ειδικοί που εργάζονται στις εκάστοτε κρίσιμες υποδομές καλούνται να υπερκεράσουν αρχικά την παρατηρούμενη έλλειψη τυποποίησης σε ότι αφορά τα αντίμετρα ασφαλείας που

[660] Το σχήμα είναι του συγγραφέως.

αφορούν είτε σε μια συγκεκριμένη κατηγορία SCA είτε στην προστασία μιας ορισμένης συσκευής που αποτελεί μέρος μιας κρίσιμης υποδομής (π.χ. εξοπλισμός γραφείου, ενσωματωμένο σύστημα κλπ[661]).

- Εν δευτέροις, κατά τον σχεδιασμό αντιμέτρων, είτε αυτός προέρχεται από κάποιο τμήμα της κρίσιμη υποδομής είτε από κάποιον εξωτερικό συνεργάτη (υπερεργολαβία κλπ), πρέπει να δίδεται η δέουσα προσοχή στην σωστή εκτέλεση λειτουργιών, όπως φέρ' ειπείν η σωστή ανάθεση τιμών σε κάποιο register, ώστε δυνητικά να μειωθεί η πιθανότητα ο επιτιθέμενος που διενεργεί μια SCA να εντοπίσει μια ορισμένη τιμή εντός του register κατά την διαδικασία, για παράδειγμα, διασπάθισης της μνήμης (memory spill) σε ένα υπολογιστικό σύστημα.

Αν υπάρξουν σχεδιαστικές αστοχίες σε τέτοιες περιπτώσεις είναι εύλογο πως ο επιτιθέμενος μπορεί να προβεί σε σχετικά ακριβείς μετρήσεις. Σε ότι αφορά στον σχεδιασμό αντιμέτρων για εφαρμογή σε μια κρίσιμη υποδομή, αυτό συνεπάγεται την δυνητική αύξηση του φόρτου εργασίας (workload) και συνακόλουθα την καταβολή μεγαλύτερης προσπάθειας στην εκπαίδευση προσωπικού, διότι θα πρέπει να αποφασιστεί από τους ιθύνοντες μιας υποδομής αν το βάρος θα δοθεί στον σχεδιασμό ή στην εφαρμογή του αλγόριθμου για παράδειγμα[662]. Σε τέτοιες περιπτώσεις μπορεί να δημιουργηθούν δυσχέρειες λόγω έλλειψης πόρων ή λόγω (και πάλι) αδυναμίας να προσαρμοστεί ένα αντίμετρο, που δημιουργήθηκε, από έναν commercial provider ακριβώς στις ανάγκες της υποδομής ή σε εκείνες της αντιμετώπισης της επιθέσεως πλευρικού καναλιού. Ενδεχομένως να πρέπει να γίνει επιλογή στο αν θα αξιοποιηθεί ένας εξωτερικός συνεργάτης ή αν θα εκπαιδευτεί κατάλληλα το αντίστοιχο προσωπικό της υποδομής.

---

[661] Liu, H., & Spolaor, R., & Turrin, F., & Bonafede, R., & Conti, M.(2021). USB powered devices: A survey of side-channel threats and countermeasures. *High-Confidence Computing 1* (2021), 100007, 1-11, σ.4. DOI:10.1016/j.hcc.2. USB powered devices: A survey of side-channel threats and countermeasures | Semantic Scholar (28/10/2022).

[662] Στο συγκεκριμένο παράδειγμα προτείνονται δύο λύσεις, είτε η χειροκίνητη εποπτεία της συναρμολόγησης (assembly) από πλευράς του Developer (Coron), είτε ο προγραμματιστής να επωμιστεί το βάρος του ελέγχου του αλγόριθμου όταν θα τον εφαρμόζει σε μια γλώσσα χαμηλού επιπέδου (Balasch et al.). Ορά σχετικά το άρθρο των Agosta, G., & Barenghi, A., & Pelosi, G., & Scandale, M.(2015). The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 34, 8, 1320-1333, σ.1322. DOI: 10.1109/TCAD.2015.2430320. (PDF) The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks (researchgate.net) (τελευταία πρόσβαση 7/11/2022).

- Εν τρίτοις, ο σχεδιασμός αντιμέτρων πρέπει να λαμβάνει υπόψη του και το στοιχείο της χωροθέτησης σε ότι αφορά τις κρίσιμες υποδομές (τωόντι δυσχερές εγχείρημα αφενός διότι πλέον αυξάνουν οι περιπτώσεις τηλεργασίας και αφετέρου διότι ο σχεδιασμός των κτιριακών υποδομών δεν είναι πάντοτε στην ευχέρεια των ιθυνόντων μιας κρίσιμης υποδομής, όπως για παράδειγμα σε περιπτώσεις ενοικίασης κτιρίων κλπ). Σε κάθε περίπτωση πρέπει να καταβάλλεται προσπάθεια ώστε να χωροθετούνται τα assets μιας οποιασδήποτε υποδομής (προφανώς αναλόγως του για ποια υποδομή πρόκειται θα ισχύουν διαφορετικές παράμετροι κατάτι, αλλά εδώ δεν μπορούμε να προβούμε λόγω χώρου σε μια εξαντλητική παράθεση ούτε κατά διάνοια) εν σχέσει με την απόσταση που πρέπει να υπάρχει ανάμεσα τους και επίσης εν σχέσει με (για όπου μπορεί να ισχύσει κάτι τέτοιο) την ύπαρξη περιβλήματος.

Αν και εδώ μπορούμε μόνο να προβούμε σε πολύ γενικευτικές παρατηρήσεις θα μπορούμε , με βάσει τα όσα έχουν μελετηθεί και διατυπωθεί σε κάποιες περιπτώσεις στο κανονιστικό πλαίσιο μιας οποιασδήποτε υποδομής, να είπουμε ότι αναφορικά με το πρώτο σημείο (χωροθέτηση-απόσταση) ήδη υφίστανται υποδομές (π.χ. εταιρείες, κυβερνητικές υπηρεσίες κλπ) που εφαρμόζουν κανονισμούς, εντός των οποίων διατυπώνεται η κατευθυντήριος γραμμή της μη κατοχής για παράδειγμα κινητής συσκευής. Αυτή η προσέγγιση ενδεχομένως να είναι εφικτή ως προς την εφαρμογή της (έως και επιβεβλημένη) για ορισμένες υποδομές (π.χ. μυστικές υπηρεσίες) ή έστω ορισμένους χώρους κάποιων υποδομών, όμως εύλογα δεν μπορεί να εφαρμοστεί κατά τρόπο καθολικό[663].

Ως εναλλακτική μπορεί να προταθεί το μέτρο της εγκατάστασης, εντός των χώρων της κρίσιμης υποδομής, ειδικών αποθετηρίων ή έστω της εγκαθίδρυσης ορισμένων καλών πρακτικών, που μεταξύ άλλων, θα προτείνουν την τοποθέτηση συσκευών που παράγουν εκροές (π.χ. κινητά, ταμπλέτες κλπ) σε άλλους χώρους ή έστω πιο μακρυά από τους εταιρικούς υπολογιστές, καθώς όπως έχει ήδη παρατηρηθεί η καταγραφή των εκροών και η εκτέλεση της επιθέσεως σε αρκετές περιπτώσεις δεν μπορεί να ευοδωθεί σε μεγάλες αποστάσεις από τις συσκευές στόχους. Για την δεύτερη περίπτωση (ύπαρξη περιβλήματος) ενδεικτικά μπορούμε να αναφέρουμε πως ορισμένα βασικά συστατικά στοιχεία των υποδομών που εύλογα παράγουν

---

[663] Πρβλ. μεταξύ άλλων Marquardt, P., & Verma, A., & Carter, H., & Traynor, P.(2011). *(sp) iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers.*Paper presented at the proceedings of the 18th ACM Conference on Computer and Communications Security, CSS 2011. Chicago, Illinois, USA. October,17-21,2011,1-12,σ.10.spiPhone-Decoding-Vibrations-From-Nearby-Keyboards.pdf (graywolfsurvival.com) (Τελευταία πρόσβαση 05/01/2022).

μεγάλο μέρος των εκροών (λόγω και του μεγέθους της εκάστοτε υποδομής) θα μπορούσαν να καλυφθούν για να μειωθεί η εκπομπή των τελευταίων[664].

- Τέταρτον, οι Montasari et al. παρατηρούν, με αναφορά στις timing SCAs, πως αρκετά αντίμετρα δημιουργούνται, κατόπιν εορτής, ως απάντηση σε τέτοιου είδους επιθέσεις. Για τον λόγο αυτό οι συγγραφείς προτείνουν την κατάρτιση μιας σειράς ποσοτικοποιημένων κριτηρίων για την αξιολόγηση των αντιμέτρων. Αν και η παρατήρηση αυτή είναι αρκούντως γενικευτική, πρέπει να ειπωθεί μια σειρά κριτηρίων που πρέπει εύλογα να υφίστανται ώστε τα μεμονωμένα αντίμετρα που συνήθως παρουσιάζονται αφορμή κάποια μελέτη-περίπτωσης (όχι πάντα βεβαίως) να μπορέσουν στην συνέχεια να ταξινομηθούν και να λειτουργήσουν προδραστικά, με το να γίνουν ίσως εφαρμόσιμα σε ευρύτερες κατηγορίες των SCAs[665].
- Πέμπτον, δεδομένων των βασικών προβλημάτων που προκύπτουν από την προσπάθεια εφαρμογής αντιμέτρων, ήτοι του overhead που προκαλείται και της συνακόλουθης μείωσης στην απόδοση ενός υπολογιστικού συστήματος (και εύλογα και της κρίσιμης υποδομής σε ένα βαθμό, αφού το αντίμετρο θα εφαρμόζεται καθολικά ή σε μεγάλο τμήμα αυτής), από αυτό προκύπτει η ανάγκη για ύπαρξη της κατάλληλης συνέργειας. Όπως επισημαίνουν οι Montasari et al. , και όπως ίσως μπορεί να καταδειχθεί και από μια εκάστη άρθρων στην διεθνή βιβλιογραφία επί της θεματικής των αντιμέτρων, ένας αριθμός προτεινόμενων λύσεων κινείται κυρίως σε ακαδημαϊκό επίπεδο και δεν καταλήγει να έχει κάποια πρακτική εφαρμογή, επομένως έχει είτε μικρή ή και καθόλου αποτελεσματικότητα έναντι διαφόρων SCAs.

Ενδεχομένως, η επαύξηση της αποτελεσματικότητας θα μπορούσε να προκύψει με στενότερη συνεργασία ανάμεσα στους άμεσα εμπλεκομένους, ήτοι ακαδημαϊκή κοινότητα, ιδιωτικές εταιρείες και κρίσιμες υποδομές, ούτως ώστε να καταστεί πιο

---

[664] Παραθέτουμε εκ νέου το παράδειγμα της ζωνοποίησης (*Zoning*), ορά ενδεικτικά το άρθρο των Lavaud, C., & Gerzaguet, R., & Gautier, M., & Berder, O. & Nogues, E., & Molton, St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security, Springer, 2021, 10.1007/s41635-021-00112-6. Hal-03176249,* 1-24, σ.14. Whispering devices: A survey on how side-channels lead to compromised information (archives-ouvertes.fr) (Τελευταία πρόσβαση 15/10/2021).

[665] Πρβλ. Montasari, R., & Hill, R., & Far, A.H., & Montaseri, F.(2019). Countermeasures for Timing-Based Side-Channel Attacks against Shared, Modern Computing Hardware. *International Journal of Electronic Security and Digital Forensics,* 11, 294-320, σ.310-311. doi:10.504/IJESDF.2019.10020551. [PDF] Countermeasures for timing-based side-channel attacks against shared, modern computing hardware | Semantic Scholar (Τελευταία πρόσβαση 10/11/2022).

προσοδοφόρα τόσο η ενσωμάτωση νέας γνώσης όσο και ο σχεδιασμός αντιμέτρων με γνώμονα τις ανάγκες και τους διαθέσιμους πόρους(ιδεατά στο πλαίσιο συγκρότησης ενός τμήματος R&D για τον σκοπό της μελέτης και δημιουργίας αντιμέτρων, εντός του ευρύτερου πλαισίου ενός τμήματος κυβερνοασφάλειας, και με συνακόλουθη συγκρότηση αντίστοιχων τυποποιήσεων, standards, για forensic analysis κλπ[666667668]).

Η ανά χείρας διπλωματική εργασία περατώνεται με την παράθεση των συγκεντρωτικών συμπερασμάτων στο κεφάλαιο που ακολουθεί αμέσως κατωτέρω.

[666] Ο.π.,σ.310.

[667] Ορά σχετική υποσημείωση υπ' αριθμόν 603.

[668] Η ανάγκη για θεμελίωση και διαρκή ανανέωση τυποποιήσεων και ταξινομήσεων έχει (ή θα έχει) ως άμεση συνέπεια την δυνατότητα για ταχύτερη και πιο εύληπτη ενσωμάτωση της γνώσης. Ένα παράδειγμα ενός τέτοιου εγχειρήματος, ποσοτικής φύσεως κατά βάση, είναι των Potestad-Ordonez et al. Οι οποίοι στο πόνημα τους, που επικεντρώνει στις fault injection SCAs και τα πιθανά αντίμετρα τους, χρησιμοποιούν τον δείκτη *Fault Coverage Corrected* (*PCC*) για να ποσοτικοποιήσουν την εφαρμογή των αντιμέτρων στις διάφορες πτυχές τους, π.χ. πλεονεκτήματα/μειονεκτήματα, παρουσίαση τους σε γράφημα, το επίπεδο ασφάλεια που καταγράφουν στην βιβλιογραφία κλπ. Αυτή η ποσοτικοποίηση εν συνεχεία οδηγεί σε πιθανή ομαδοποίηση αντιμέτρων για να καταστεί ευκολότερη η αξιοποίηση τους με βάσει τις εκάστοτε ανάγκες των συσκευών IoT που ενσωματώνουν οι κρίσιμες υποδομές (πέρα από το μίκρο-επίπεδο), ενώ από την άλλη οι ομαδοποιήσεις αυτές επιτρέπουν την καλύτερη δυνατή κατανόηση σχετικά με το ποιες είναι οι πιθανές εκροές στις οποίες μπορεί να οδηγήσουν οι όποιες εφαρμογές αντιμέτρων (π.χ. στο συγκεκριμένο άρθρο το αντίμετρο *information redundancy,* μπορεί δυνητικά να μειώνει την παρείσφρηση σφαλμάτων, faults, αλλά αυξάνει τον χρόνο εκτέλεση του αλγόριθμου κρυπτογράφησης και άρα τις εκροές τις σχετικές με τις χρονομετρήσεις κλπ). Πρβλ. Potestad-Ordonez, F.E., & Tena-Sanchez, E., & Acusta-Jimenez,A.J., & Jimenez-Fernandez, C.J., & Chaves, R.(2022). Hardware Countermeasures Benchmarking against Fault Attacks. *Applied Sciences* 2022, 12(5), 2443, 1-20, σ.17. doi:https://doi.org/10.3390/app12052443.Applied Sciences | Free Full-Text | Hardware Countermeasures Benchmarking against Fault Attacks (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

Μέρος 3ο
ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπεράσματα

Το κεφάλαιο με το οποίο ολοκληρώνεται το ανά χείρας πόνημα θα διακριθεί σε δύο μέρη για τους σκοπούς της εναργέστερης κατανόησης αυτού, τα δύο αυτά μέρη παρατίθενται όπως κατωτέρω:

- Το πρώτο μέρος του παρόντος κεφαλαίου αφιερώνεται στην παράθεση των συμπερασμάτων στα οποία κατέληξε η βιβλιογραφική αναζήτηση του οικείου θέματος που αναλύθηκε διεξοδικά στα κεφάλαια που προηγήθηκαν. Στόχος εδώ είναι να λάβει χώρα μια κριτική αποτίμηση της υπάρχουσας βιβλιογραφίας που μελετήθηκε και με τον τρόπο αυτό να εξαχθεί η συμβολή του παρόντος πονήματος στην σχέση του με το επιστημονικό θέμα που αναλύθηκε ανωτέρω.
- Το δεύτερο μέρος αποσκοπεί στην εν παρόδω παράθεση ορισμένων κατευθύνσεων προς τις οποίες θα μπορούσε , μελλοντικά, να επεκταθεί η έρευνα περί των επιθέσεων πλευρικού καναλιού στο Διαδίκτυο των πραγμάτων (IoT). Η στόχευση εδώ αφορά σε μελλοντική πραγμάτευση ορισμένων σημείων (ενδεχομένως δε και κενών) που αναφύονται στην διεθνή βιβλιογραφία, και τα οποία δύνανται όπως δώσουν συν τω χρόνω «τροφή» για ενδελεχή ανάλυση και πρακτική εφαρμογή.

Κριτική Αποτίμηση της βιβλιογραφικής Ανασκοπήσεως

Έχοντας πλέον ολοκληρώσει την βιβλιογραφική ανασκόπηση, στο μέτρο του εφικτού σε κάθε περίπτωση, καλούμαστε κατωτέρω να παραθέσουμε ορισμένα σημεία που χρήζουν κριτικής αποτίμησης, αφενός σε σχέση με τα κενά που παρατηρήθηκαν στην βιβλιογραφία που μελετήθηκε, και αφετέρου σε σχέση με τις δυσχέρειες που παρατηρήθηκαν στις πτυχές του δίπολου SCAs-IoT που η διεθνής βιβλιογραφία έχει να επιδείξει (εκ νέου η αναφορά σχετίζεται μόνο με τα ξενόγλωσσα άρθρα που ανευρέθηκαν και μελετήθηκαν επαρκώς). Τα σημεία κριτικής παρατήρησης παρατίθενται ως ακολούθως:

- Το τμήμα της βιβλιογραφίας που μελετήθηκε ανέδειξε μια σημαντική έλλειψη επαγωγής (scalability),καθώς σε σημαντικό βαθμό, αν όχι εξ' ολοκλήρου περιορίστηκε σε απλές παραθέσεις SCAs, είτε συνολικά είτε κάποιων μεμονωμένων κατηγοριών, και επίσης σε μελέτες περιπτώσεως με την ανάλυση να περιορίζεται σε μια πειραματική συνθήκη (σε αναλογία 1:1 συνήθως, όπου ένας τύπος SCA αναλύεται έναντι

ενός ή μερικών attack vectors, όπως κινητών συσκευών, κυκλωμάτων, μνήμης cache κλπ). Αποτέλεσμα αυτής της τάσεως είναι και το ότι η οπτική της κρίσιμης υποδομής που περιλαμβάνει πολλά ενσωματωμένα συστήματα και συσκευές IoT δεν περιέρχεται ποτέ στο επίκεντρο των αναλύσεων των άρθρων που μελετήθηκαν. Άμεση συνέπεια της έλλειψης επαγωγής είναι και η ταυτόχρονη απουσία σύγκρισης (τουλάχιστον κατά τρόπο που θα ήτο εναργής και σχετικά εύχρηστος στο να διενεργηθεί) και ενσωμάτωσης νέας γνώσης σε ταξινομητικά σχήματα, τα οποία δυνητικά θα χρησίμευαν για την καλύτερη κατανόηση των επιθέσεων και επομένως για τον πιο αποτελεσματικό σχεδιασμό αντιμέτρων[669].

- Δεύτερον, στο μεγαλύτερο τμήμα της βιβλιογραφικής ανασκόπησης που διενεργήθηκε για τους σκοπούς του ανά χείρας πονήματος, παρατηρήθηκε ακόμα μια σημαντική έλλειψη δεικτών, ή οποιασδήποτε φόρμουλας (metrics) για την συγκριτική αξιολόγηση, των αποτελεσμάτων από την διενέργεια είτε επιθέσεων πλευρικού καναλιού είτε από το αντίστοιχο εγχείρημα του σχεδιασμού και της εφαρμογής αντιμέτρων. Όσον αφορά τις επιθέσεις και τα αντίμετρα τους το συντριπτικό τμήμα της βιβλιογραφίας εμφάνισε μια διττή, κατά βάση, προσέγγιση όπου είτε τα δύο αυτά μέρη αναλύονταν μόνο κατά τρόπο θεωρητικό είτε η εφαρμογή και των δύο περιοριζόταν κατά βάση σε διενέργεια πειραματικών συνθηκών. Με τον τρόπο αυτό αναφύονταν μια ετερογένεια (methodological heterogeneity) στην βιβλιογραφία που μελετήθηκε, η οποία αν και λειτουργούσε ευεργετικά ενδεχομένως για το σκέλος της ακαδημαϊκής έρευνας, εντούτοις όμως σε ότι αφορά στην προστασία των συσκευών IoT και στην αντίστοιχη των Κρίσιμων Υποδομών προκύπτει σχεδόν αναπόδραστα το ζήτημα της έλλειψης συνοχής και δυνατότητας ενσωμάτωσης νέας γνώσης, καθότι η ετερογένεια αυτή δυσχεραίνει αρκετά τον έγκαιρο εντοπισμό των αναφυόμενων τάσεων όσον αφορά τόσο στις απειλές (π.χ. νέες SCAs ή συνδυασμός των ήδη υπαρχόντων) όσο και στα αντίμετρα[670].

---

[669]Πρβλ. (και) την σχετική παρατήρηση στο Potestad-Ordonez, F.E., & Tena-Sanchez, E., & Acosta-Jimenez, A.J., & Jimenez-Fernandez, C.J, & Chaves, R.(2022). Hardware Countermeasures Benchmarking against Fault Attacks. *Applied Sciences* 2022, 12, 2443, 1-20, σ.17. doi: https://doi.org/10.3390/app12052443. Applied Sciences | Free Full-Text | Hardware Countermeasures Benchmarking against Fault Attacks (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

[670] Για μια αντίστοιχη παρατήρηση ορά επίσης και τα εγχειρήματα συγκριτικής παράθεσης και αξιολόγησης (μέσω ανάλυσης βιβλιογραφίας, δεικτών και γραφημάτων) στα κάτωθι άρθρα, αφενός στο Montasari, R., & Hill, R., & Hosseinian-Far, A., & Montaseri, F.(2019). Countermeasures for Timing Based Side-Channel

- Τρίτον, η ετερογένεια που αναφέρθηκε ανωτέρω είναι επίσης απότοκο (πέραν της διαφορετικής μεθοδολογίας που διαφορετικοί συγγραφείς μπορεί να αξιοποιούν για να δομήσουν τα πονήματα τους) της εννοιολογικής αμφισημίας (ambiguity, double structure) που ανακύπτει κατά τα διάφορα εγχειρήματα ταξινομήσεως (αυτό παρατηρήθηκε κυρίως στις ταξινομήσεις τις σχετικές με τις SCAs, αλλά ευλόγως δεν μπορεί να αποκλειστεί ένα τέτοιο ενδεχόμενο και σε ότι αφορά στα αντίμετρα).

Η αμφισημία αυτή αποτυπώνεται στην σχετική απουσία αποκλειστικότητας των κατηγοριών που εντοπίζονται εντός των ταξινομητικών εγχειρημάτων της διεθνής βιβλιογραφίας. Παρατηρήθηκε επομένως πως όταν, επί παραδείγματι, ένα ταξινομητικό εγχείρημα εκκινεί με βάσει την μια ή την έτερη επίθεση πλευρικού καναλιού (π.χ. optical SCAs, DPAs, acoustic SCAs κλπ), και προσπαθεί κατ' επέκταση να συγκροτήσει αποκλειστικές κατηγορίες επιθέσεων, καταλήγει να εδραιώνει την κατηγορία αλλά παράλληλα να μην μπορεί να περιορίσει σε μια αποκλειστική κατηγοριοποίηση την εκροή της τελευταίας (leakage, emanation κλπ). Καθώς ένας καθολικός ορισμός για το τι συνιστά SCA, όπως καταδείχθηκε, δεν έχει καταστεί προς ώρας εφικτός, δεν είναι επίσης εφικτό να συγκροτηθούν αποκλειστικές κατηγορίες ταξινόμησης, διότι δεν είναι όλες οι πτυχές των SCAs εξίσου εμφανείς και μελετημένες στην βιβλιογραφία.

Αποτέλεσμα όλων αυτών είναι σε αρκετές περιπτώσεις διαφορετικά επιστημονικά πονήματα να επικεντρώνονται σε ίδιες ή παρόμοιες κατηγοριοποιήσεις, αλλά εντούτοις να καταλήγουν σε αποκλίνουσες ταξινομητικές απεικονίσεις. Κι έτσι να μειώνεται η πρακτικότητα τέτοιων εγχειρημάτων, καθώς δεν μπορούν οι ταξινομήσεις να υποβοηθήσουν επαρκώς στον σχεδιασμό καθολικών αντιμέτρων (κι έτσι ενδεχομένως αυξάνεται το κόστος, και η περιπλοκότητα στον σχεδιασμό αφού τα όποια αντίμετρα θα πρέπει να συμπληρώνονται από άλλα ή να επανασχεδιάζονται[671]).

Attacks against Shared, Modern Computing Hardware. International Journal of Electronic Security and Digital Forensics, 11, 294-320 (1-26), σ.16. doi:10.504/IJESDF.2019.10020551. IJTM/IJCEE PAGE TEMPLATEv2 (hud.ac.uk) (Τελευταία πρόσβαση 10/11/2022). Και αφετέρου Potestad-Ordonez, F.E., & Tena-Sanchez, E., & Acosta-Jimenez, A.J., & Jimenez-Fernandez, C.J., & Chaves, R.(2022). Hardware Countermeasures Benchmarking against Fault Attacks. *Applied Sciences* 2022, 12, 2443, 1-20, σ.15 κε. doi: https://doi.org/10.3390/app12052443. Applied Sciences | Free Full-Text | Hardware Countermeasures Benchmarking against Fault Attacks (mdpi.com) (Τελευταία πρόσβαση 14/10/2022).

[671] Δεν μπορεί να γίνει μια εξαντλητική παράθεση εδώ, καθώς και ο χώρος δεν επαρκεί αλλά και ένα τέτοιο εγχείρημα θα ήταν αρκετά περίπλοκο για ένα κεφάλαιο που αφιερώνεται στα συμπεράσματα, θα αρκεστούμε επομένως σε μια παράθεση που αναφέρθηκε (και) ανωτέρω, η οποία αφορά στις οπτικές SCAs όπου ο επιθετικός

- Τέταρτον, από την βιβλιογραφία που μελετήθηκε προκύπτει (και από τα τρία ως άνω σημεία που παρατέθηκαν και που αφορούν στην κριτική αποτίμηση της βιβλιογραφικής ανασκόπησης) ακόμα πως οι επιθέσεις πλευρικού καναλιού αν και έχουν μια συνεχώς αυξανόμενη παρουσία στις επιστημονικές συζητήσεις, παραμένει ωστόσο μη απόλυτα εξακριβωμένος ο ρόλος τους στην αλυσίδα κυβερνοεπιθέσεως (*cyber-attack chain* ή *cyber kill chain*).Πράγματι αν και πολλά άρθρα τονίζουν την συνεχώς αυξανόμενη ένταση της απειλής που αντιπροσωπεύουν οι SCAs, εντούτοις οι τελευταίες πρέπει σε πολλές περιπτώσεις (όχι πάντα βεβαίως) να συνεπικουρούνται από έτερες επιθέσεις που προετοιμάζουν το έδαφος.

Έτσι, δεν είναι ξεκάθαρο αν τα αντίμετρα θα μπορούσαν να αρκεστούν στο να σταματήσουν την μια επίθεση για να αποτρέψουν την εκτέλεση της SCA κατόπιν, και επίσης παραμένει προς διερεύνηση το αν εν γένει οι SCAs μπορούν να θεωρηθούν ως σημαίνουσες απειλές κατά μονάς ή περισσότερο υπό το πρίσμα ενός συνδυασμού επιθέσεων όπου οι SCAs θα έχουν δευτερεύοντα ή πρωτεύοντα ρόλο (ούτε αυτό το τελευταίο σημείο είναι ευδιάκριτο, καθώς και από εδώ θα προκύψει το αν χρήζει ή μη να

προσδιορισμός ”οπτικές” είναι αρκετά ευέλικτος στις μεθοδολογίες επιθέσεως που μελετήθηκαν για τους σκοπούς αυτής της διπλωματικής εργασίας (στο δεύτερο κεφάλαιο του πρώτου μέρους της οποίας αναλύεται εκτενέστερα το εν λόγω σημείο). Επί παραδείγματι, η εκδήλωση οπτικών επιθέσεων περιλαμβάνει ένα ευρύ φάσμα παραλλαγών όπως την συμπερίληψη οθονών, γυαλιών μυωπίας, λαμπτήρων LED στην κατάρτιση της μεθοδολογίας επιθέσεως. Στις τρεις αυτές περιπτώσεις υπάρχει το οπτικό στοιχείο, αλλά απλά και μόνο η παράθεση τους σε μια κατηγορία δεν την καθιστά ούτε αποκλειστική ούτε κατανοητή χωρίς εξειδίκευση στο εν λόγω υποκατηγορία ή και στις υπόλοιπες. Ειδικότερα, οι λαμπτήρες LED τονίζουν την σημασία της παρατήρησης της μετάδοσης της φωτεινότητας και την χρονική σημασία αυτής, τα γυαλιά την δυνατότητα η εκροή να διασπαθίζεται στον χώρο μέσω αντανάκλασης, ενώ η οθόνη πέρα από τις αντανακλάσεις προσφέρεται και για άλλες επιθέσεις πλευρικού καναλιού, π.χ. αν πρόκειται για οθόνης αφής τότε μπορεί να χρησιμοποιηθεί συνδυαστικά το αποτύπωμα και η αντανάκλαση. Αποτέλεσμα όλης αυτή της ποικιλομορφίας είναι οι κατηγορίες ταξινόμησης είτε να πρέπει να εμφανίζουν πολύπλοκες διακλαδώσεις και επομένως να μην είναι εύληπτες, ή να είναι μεμονωμένες αφήνοντας όμως εκτός κάθε φορά κάποιες παραλλαγές που δεν είναι ίσως τόσο διαδεδομένες, και άρα οι κατηγοριοποιήσεις δεν θα είναι έτσι πλήρεις. Πρβλ. Lavaud, C., & Gerzaguet, R., & Gantier, M., & Berder, O., & Nogues, F., & Molton, St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and System Security*, Springer, 2021, 1-24, σ.6-7. doi:10.1007/s41635-021-00112-6.hal-03176249. Whispering devices: A survey on how side-channels lead to compromised information (archives-ouvertes.fr) (Τελευταία πρόσβαση 15/10/2021). Και επίσης, το άρθρο των Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification on Side-Channel Attacks: A case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials*,20,1,465-488(1-24),σ.8-9.doi:10.1109/COMST.2017.2779824. https://arxiv.org/pdf/1611.03748.pdf (Τελευταία πρόσβαση 16/9/2021).

γίνει αντιμετώπιση ρίσκου στην μια ή στην άλλη περίπτωση στο πλαίσιο στρατηγικής κυβερνοασφάλειας της κάθε υποδομής για τις IoT συσκευές της[672]).

- Πέμπτον, και ως απόρροια του προηγούμενου σημείου, εκ της βιβλιογραφικής ανασκοπήσεως προέκυψε ακόμα πως και η εφαρμογή αντιμέτρων δύναται όπως προκαλέσει εκροές. Αν και η συντριπτική πλειοψηφία των άρθρων που μελετήθηκαν παρουσιάζει τις εκροές ως προκύπτουσες από τις συσκευές IoT, εντούτοις υπάρχουν και κάποιες ελάχιστες περιπτώσεις όπου υποστηρίζεται το αντίθετο[673]. Κατά τον τρόπο αυτό προκύπτει ένα ερώτημα που δεν απαντάται στην διεθνή βιβλιογραφία (έστω το τμήμα που μελετήθηκε) και το οποίο αφορά στην ακριβή αιτιακή σχέση ανάμεσα στις SCAs και στις εκροές. Επομένως, πέραν του να εκμεταλλεύονται τις όποιες ήδη υπάρχουσες εκροές δεν έχει ακόμα διευκρινιστεί πλήρως αν οι ίδιες οι SCAs δύνανται να καθιερώσουν οι ίδιες κανάλια μέσω των οποίων θα διέρχονται οι εκροές. Ορθότερα, το ζήτημα που δεν διευκρινίζεται ιδιαίτερα στην βιβλιογραφία είναι το αν η εκροή και το πλευρικό κανάλι μπορούν να μελετιούνται από κοινού ή αν αποτελούν ξεχωριστές οντότητες, κι επομένως αν τα αντίμετρα θα υπήρχε τρόπος να σχεδιαστούν ανάλογα με το αν η καίρια ευπάθεια είναι η εκροή (που πρέπει να εξισορροπηθεί) ή το κανάλι μέσω του οποίου ο επιτιθέμενος συλλέγει δειγματοληπτικά τις μετρήσεις της όποιας εκροής[674].
- Έκτον, ερμηνεύοντας το τμήμα της διεθνούς βιβλιογραφίας που μελετήθηκε υπό το πρίσμα του τριμερούς σχήματος που προτάθηκε αρχικά από τον

[672] Ενδεικτικά παραθέτουμε τα ακόλουθα παραδείγματα άρθρωνc Και επίσης, Maiti, A., & Jadiwala, M., & He, J., & Bilogrevic, I. (2018). Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches. *IEEE Transactions on Mobile Computing* PP (99), 1-16, σ.3. doi:10.1109/TMC.2018.2794984. (PDF) Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches (researchgate.net) (Τελευταία πρόσβαση 23/03/2022).

[673] Επί παραδείγματι, το αντίμετρο *RMTL* (*Randomized Topology logic*). Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022).Gate-level Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28, σ.12. doi:https://doi.org/10.3390/app12052390.Applied Sciences | Free Full-Text | Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks (mdpi.com) (Τελευταία πρόσβαση 10/10/2022).

[674] Πρβλ. επί παραδείγματι την σχετική παραπομπή υπ' αριθμόν 52 (που συμπληρώνει την αντίστοιχη υποσημείωση υπ' αριθμόν 36) όπου γίνεται η παρατήρηση για τα άρθρα που χρησιμοποιούν τον όρο πλευρικό κανάλι (*side-channel*) και εκείνα που κάνουν λόγο για εν κρυπτώ κανάλι (*covert channel*).

Kocher περί τα μέσα της δεκαετίας του ’90 (*invasive*, *semi-invasive*, *non-invasive*[675]), δύναται να διατυπωθεί πως η σύγχρονη τάση της τελευταίας δεκαετίας είναι η μετατόπιση προς τις απομακρυσμένες μη επεμβατικές μεθοδολογίες επιθέσεως. Ένας συγκριτικά υπέρτερος αριθμός άρθρων περιλαμβάνει σχήματα επιθέσεως που βασίζονται στην μηχανική μάθηση (*Machine Learning*) και που επιχειρηματολογούν, έστω και εμμέσως, περί της οικονομίας (affordability) καθώς και ενδεχομένως περί της ευκολίας (feasibility) στην διενέργεια μιας επιθέσεως πλευρικού καναλιού(ειδικά αν συγκριθεί με την εποχή που έλαβε χώρα η επίθεση *Tempest*[676]) . Εντός ενός ιστορικού πλαισίου η παραπάνω παρατήρηση είναι εν μέρει ορθή, αλλά σε συγχρονικό πλαίσιο είναι επίσης αρκούντως γενικόλογη και οδηγεί σε έλλειψη στάθμισης σε ότι αφορά τις προσεγγίσεις του risk treatment (ήτοι αν αυτό είναι σημαντικό και αξίζει να αντιμετωπιστεί ή μη[677]).

Όπως αναφέρθηκε και στο πρώτο σημείο αυτού του κεφαλαίου, αλλά εδώ η παράθεση είναι περισσότερο για την διατύπωση και όχι για την ποσοτική διάσταση, οι SCAs παρουσιάζονται (βάσει επιχειρηματολογίας) ως ιδιαιτέρως ισχυρές, αλλά η γενικολογία και πολλές φορές η έλλειψη κοινής «γλώσσας» (*ontology*) δεν επιτρέπει την ανάπτυξη συνεργειών (*synergies*) που θα ενσωματώνουν κοινές κατευθυντήριες και ούτε επίσης την ακριβόλογη επικοινωνία (*dissemination*) περί απειλών (risks) και αντιμέτρων σε ετερογενείς ομάδες ανθρώπινου δυναμικού που λόγω διαφοροποιημένου υπόβαθρου (και όπως τονίστηκε ανωτέρω αυτό είναι κοινός τόπος για τις κρίσιμες υποδομές) θα

[675] Standaert, F.X.(2010). Introduction to Side-Channel Attacks. Στο I.M.R. Verbauwhede(Επιμ.), *Secure Integrated Circuits and Systems* (σ.27-42), σ.2-3. Leuven: Springer Link. (PDF) Introduction to Side-Channel Attacks (researchgate.net) (Τελευταία πρόσβαση 26/11/2021).

[676] Ορά υποσημείωση υπ’ αριθμόν 82.

[677] Πρβλ. μεταξύ πολλών άλλων περιπτώσεων και την υποσημείωση υπ’ αριθμόν 57, όπου για την συγκεκριμένη μελέτη περίπτωσης (εκτυπωτές για εκτύπωση ιατροφαρμακευτικών συνταγών, εντός νοσοκομειακής μονάδας) αφενός καταδεικνύεται ότι όσο και να αυξηθούν οι δυνατότητες για μια μη επεμβατική SCA, ενδεχομένως και για το αμέσως επόμενο διάστημα θα πρέπει να διατηρηθεί το χαρακτηριστικό της εγγύτητας για την συλλογή δειγμάτων εκροών πριν τα μοντέλα της μηχανικής μάθησης μπορέσουν να εκπαιδευτούν κοκ. Αφετέρου, το παράδειγμα της υποσημείωσης υπ’ αριθμόν 57 δείχνει επίσης ότι ο βαθμός επιτυχίας του αλγόριθμου μπορεί να επηρεαστεί από αντίμετρα εκ διαμέτρου αντίθετα, τόσο πιο εξεζητημένα όσο και απλούστερα σε σύλληψη (όπως οι απομάκρυνση συσκευών πλησίον της συσκευής στόχου, που αναφέρθηκε σαν ιδέα στην υπό-ενότητα των αντιμέτρων περιβάλλοντος στο προηγούμενο κεφάλαιο, και επίσης ενέργειας που υπάγονται στην καθημερινότητα του ανθρώπινου δυναμικού, όπως το κλείσιμο μιας πόρτας ή η χρήση ακουστικού αφρολέξ, *acoustic foam*).

αποθαρρυνθούν περαιτέρω από το να σχηματίσουν μια κοινή γλώσσα αντίληψη περί των επιθέσεων πλευρικών καναλιών και των αντιμέτρων επί των τελευταίων.

Η παράθεση των ανωτέρω σημείων αφορούσε σε ένα γενικότερο επίπεδο αποτίμηση το δίπολο SCAs-διεθνή αρθρογραφία (με ενδεικτική αναφορά σε πτυχές αντιμέτρων και κρίσιμων υποδομών). Κατωτέρω ακολουθούν μια σειρά από σημεία που επικεντρώνουν σε κριτικές παρατηρήσεις επί του ετέρου δίπολου, ήτοι αυτό των επιθέσεων πλευρικού καναλιού και των συσκευών IoT (με ενδεικτική μόνο αναφορά στις κρίσιμες υποδομές λόγω έλλειψης μιας τέτοιας ανάλυσης στο τμήμα της διεθνούς βιβλιογραφίας που μελετήθηκε). Τα εν λόγω σημεία έχουν ως ακολούθως:

- Πέρα από τις δομικές αδυναμίες των IoT συσκευών (που αναφέρθηκαν σε προηγούμενα κεφάλαια και που επομένως δεν θα αναφερθούν εκτενώς στο σημείο αυτό, όπως η απουσία διεπαφής φιλικής προς τον χρήστη, η συνεχής λειτουργία ομού μετά της απουσίας συχνής επίβλεψης από τους αρμόδιους, η κατασκευαστική ετερογένεια σε ότι αφορά στην προέλευση των εν λόγω συσκευών, η χρήση μη πιστοποιημένου λογισμικού κλπ) σε ότι αφορά στις επιθέσεις πλευρικού καναλιού έναντι των πρώτων, πρέπει να αναφερθεί πως η βιβλιογραφία (το τμήμα αυτής που μελετήθηκε) καταδεικνύει ακόμα την εισέτι μεγαλύτερη ευελιξία (versatility) και ποικιλομορφία (variety) που οι επιθέσεις αυτές αποκτούν όταν ο στόχος τους είναι οι IoT συσκευές (π.χ. κινητά android, routers κλπ).

Οι συσκευές IoT παρουσιάζουν επομένως ευρεία ετερογένεια τόσο μεταξύ τους όσο και συγκρινόμενες με το περιβάλλον εντός του οποίου λειτουργούν και το οποίο υποστηρίζουν (π.χ. Η/Υ, Κρίσιμες Υποδομές). Η συγκριτική ετερογένεια τους είναι τριπλή, αφορά στην κατανάλωση ισχύος, στην εφαρμογή αλγόριθμων κρυπτογράφησης και τέλος στην ύπαρξη αισθητήρων, που σε ορισμένες περιπτώσεις δεν απαιτούν άδεια πρόσβασης (*permissions*[678]).

[678] Πρβλ. Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification on Side-Channel Attacks: A case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials*, 20, 1, 465-488 (1-24), σ.3. doi:10.1109/COMST.2017.2779824. 1611.03748.pdf (arxiv.org) (Τελευταία πρόσβαση 16/9/2021). Και επίσης, Shafiq, M., & Gu, Z., & Cheikhrouhou, O., & Alhakami, W., & Hamam, H.(2022). The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT- Based Security Attacks. Wireless Communications and Mobile Computing, 2022, 1-12, σ.10.doi:1611.03748.pdf (arxiv.org). WCMC_8669348 1..12 (hindawi.com) (Τελευταία πρόσβαση 23/11/2022).

Αυτή η ετερογένεια που παρουσιάζουν δημιουργεί και από την πλευρά των IoT συσκευών ζητήματα επαγωγής σε ότι αφορά την επέκταση των περιπτώσεων στις Κρίσιμες Υποδομές. Εν άλλοις λόγοις, οι μελέτες-περιπτώσεως δεν μπορούν να αναχθούν εύκολα σε ανώτερο επίπεδο, διότι οι κανονισμοί λειτουργίας των Υποδομών διαφοροποιούνται ανάλογα την περίπτωση για την οποία γίνεται λόγος (π.χ. κυβερνητικά κτίρια, νοσοκομεία κλπ). Οι πόροι και οι σχεδιαστικές δυνατότητες των αντιμέτρων επίσης είναι ετερογενείς γιατί τα ενσωματωμένα συστήματα και οι συσκευές IoT είτε φείδονται πόρων λόγω της αρχιτεκτονικής τους είτε διότι έχουν μικρότερες επεξεργαστικές δυνατότητες σε σχέση με τα υπόλοιπα συστήματα της Υποδομής (π.χ. αλγόριθμοι σε φορητές συσκευές IoT[679]).

Επίσης δε, η ετερογένεια ανάμεσα σε IoT και Κρίσιμες Υποδομές προκύπτει και από την πολυμέρεια της λειτουργίας των πρώτων λόγω των αισθητήρων που ενσωματώνουν, κι έτσι αυξάνουν την αλληλεπίδραση μεταξύ περιβάλλοντος και χρηστών (end-users) κι επομένως την εξατομίκευση των περιπτώσεων εφαρμογής, διότι οι αισθητήρες μπορούν να είναι ασταθείς και να δυσχεραίνουν τόσο τον επιτιθέμενο όσο και την ενσωμάτωση γνώσης, αφού η διαρρύθμιση των Υποδομών θα είναι παράγοντας που μπορεί να αναδεικνύει διαφορετικές περιπτώσεις κάθε φορά και ανά περίπτωση[680].

- Το δεύτερο σημείο που αφορά στις συσκευές IoT και την σχέση τους με τις SCAs έχει να κάνει με την επέκταση της αλυσίδας επιθέσεως μέσω του hopping. Αντιστρέφοντας την οπτική και όταν οι συσκευές IoT μελετηθούν υπό το πρίσμα των επιθέσεων στην βιβλιογραφία, τότε καταγράφεται μια σχετική διάρρηξη στην σχέση IoT-περιβάλλοντος χώρου (εργασίας). Αυτό σημαίνει πως το τριμερές σχήμα του Kocher μπορεί να μετασχηματιστεί σε κάποιο βαθμό, και τα καινοφανή στοιχεία που θα μπορούσαν να προστεθούν θα αφορούσαν, αφενός στην αυξημένη δυνατότητα για επιθέσεις που θα συνδυάζουν περισσότερους του ενός vectors, και αφετέρου δυνατότητα

[679] Gunathilake, N.A., & Al Dubai, A., & Buchanan, W.J., & Lo, O. (2020). *Electromagnetic Analysis of an Ultra-Lightweight Cipher:PRESENT*. Paper presented at the 10th International Conference on Information Technology Convergence and Services(ITCSE 2021). Sydney, Australia. June, 26-27, 185-205, σ.185-186. Format guide for AIRCC (arxiv.org) (17/5/2022).

[680] Marquardt, P., & Verma, A., & Carter, H., & Traynor, P.(2011). *(sp) iPhone: Decoding vibrations from nearby keyboards using mobile accelerometers*. Paper presented at the proceedings of the 18th ACM Conference on Computer and Communications Security, CSS 2011. Chicago, Illinois, USA. October 17-21, 10-12, σ.10. doi: 10.1145/2046707.2046771. spiPhone-Decoding-Vibrations-From-Nearby-Keyboards.pdf (graywolfsurvival.com) (Τελευταία πρόσβαση 05/1/2022).

να πληγεί μια Κρίσιμη Υποδομή και κατά τρόπο απομακρυσμένο (π.χ. όταν οι συσκευές IoT αφορούν στην τηλεργασία, τα Smart Homes κλπ[681]).

Εδώ η εγγύτητα και η απομακρυσμένη προσέγγιση είναι πιο ευέλικτες και μπορούν σε ένα βαθμό να συνδυαστούν καθώς ο επιτιθέμενος θα μπορούσε πιο εύκολα να προσεγγίσει τον τηλεργαζόμενο (π.χ. αν βρίσκεται σε μια καφετέρια και εργάζεται εκεί ως τηλενομάς) για να συλλέξει δείγματα εκροής, παρά να εισχωρήσει σε μια Υποδομή που θα φρουρείται. Παράλληλα, εδώ αυξάνει η δυσχέρεια στην κατανόηση του δίπολου IoT-CI (Critical Infrastructure), αυτή την φορά γιατί η έννοια της Υποδομής επεκτείνεται και σε άλλους χώρους, κι έτσι δεν είναι εύκολο να δημιουργηθούν εύχρηστες κατηγοριοποιήσεις.

- Το τρίτο σημείο που μπορεί να παρατηρηθεί εδώ είναι πως οι SCAs μπορούν να είναι πιο επιτυχημένες, όχι αποκλειστικά με βάσει τα αποτελέσματα των μοντέλων μηχανικής μαθήσεως, αλλά και ιδιαίτερα αν συνδυαστούν με το λεγόμενο social engineering. Μπορεί να συναχθεί πως για τις επιθέσεις κατά συσκευών IoT σε Κρίσιμες Υποδομές, και ειδικότερα για το στάδιο επεξεργασίας των εκροών (π.χ. ανάκτηση περιεχομένου ενός κειμένου κλπ), είναι ίσως ευκολότερο για την διεξαγωγή και την συνακόλουθη επιτυχία τους ο επιτιθέμενος να έχει μια πρότερη γνώση της Υποδομής και άρα αυτό θα μπορούσε να ευσταθεί για τις περιπτώσεις που ο τελευταίος είναι μια εκ των ένδον απειλή (insider threat[682]).

Κι εδώ αναφύεται ένα κενό συχνά στην βιβλιογραφία, αφού με βάσει τα όσα άρθρα μελετήθηκαν δεν εντοπίστηκε μια σαφής συγκριτική ένδειξη για το αν οι SCAs συγκεντρώνουν περισσότερες πιθανότητες επιτυχίας όταν ο επιτιθέμενος έχει πρότερη γνώση της συνθήκης (όπως στις Template Attacks) ή αν αυτές οι πιθανότητες θα παρέμεναν σταθερές και για τις SCAs που διενεργούνται χωρίς αυτή την πρότερη γνώση του template.

---

[681] Abrishamchi, M.A.N., & Abdullah, A.H., & Cheok, A.D., Bielawski, K.S.(2017). *Side Channel Attacks on Smart Home Systems: A short Overview*. Paper presented at the IECON 2017-43RD Annual Conference of the IEEE Industrial Electronics Society. Beijing, China. October 29- November 1, 4926-4932,σ.4926-4927. [PDF] Side channel attacks on smart home systems: A short overview | Semantic Scholar (Τελευταία πρόσβαση 12/12/2021).

[682] Για παράδειγμα, Bakes, M., & Durmuth, M., & Gerling, S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers*. Paper presented at the 19th USENIX Security Symposium. DC, USA. August 11-13, 1-16, σ.9-10. Acoustic Side-Channel Attacks on Printers | Request PDF (researchgate.net) (Τελευταία πρόσβαση 10/10/2021).

- Τέταρτον, αναφορικά με τα ενσωματωμένα συστήματα (που βεβαίως αποτελούν τμήμα κι αυτά του IoT), παρατηρήθηκε πως οι ευπάθειες τους που τα καθιστούν προσοδοφόρους στόχους των εκάστοτε SCAs είναι αφενός η μονολειτουργικότητα τους και αφετέρου η περιορισμένη ύπαρξη πόρων που μεταξύ άλλων επηρεάζει και τον σχεδιασμό αντιμέτρων όπως καταδείχθηκε ανωτέρω (εν παρόδω σημειώνεται πως οι ευπάθειες στο μεγαλύτερο τμήμα τους είναι κοινές και για τις ευφυείς συσκευές και για τα ενσωματωμένα συστήματα, π.χ. δυσχέρεια στην παραμετροποίηση της ασφάλειας σε ότι αφορά τους τελικούς χρήστες που τα χειρίζονται κλπ). Ειδικότερα, σημειώνεται πως ένα από τα λίγα σημεία της βιβλιογραφίας (αν όχι το μοναδικό που εντοπίστηκε) που στάθηκε, αν και χωρίς ιδιαίτερη εμβάθυνση, στα ενσωματωμένα συστήματα(αλλά και στις ευφυείς συσκευές) υπό την προοπτική των SCAs στις Κρίσιμες Υποδομές είναι εκείνο της απομακρυσμένης τους λειτουργίας (remoteness) σε χώρους που η εποπτεία είναι ελλιπής αλλά και δυσχερείς[683].

Τέτοια, ενδεικτικά, ήταν η περίπτωση της ψηφιακής γεωργίας (πρβλ. *Precision Farming* κλπ) όπου εκτός των ευπαθειών που είναι γενικά παραδεκτές για τα εν λόγω συστήματα και που αναφέρθηκαν σε διάφορα άρθρα, στην εν λόγω περίπτωση ήρθαν να προστεθούν δύο ακόμα ενδιαφέροντα στοιχεία που δυνητικά υποβοηθούν την διενέργεια SCAs. Αρχικά, μια σχετικά παραμελημένη παράμετρος είναι εκείνη των καιρικών φαινομένων στα οποία είναι εκτεθειμένες οι συγκεκριμένες συσκευές (π.χ. αγροτικές καλλιέργειες, υποθαλάσσιες υποδομές κλπ), και στο πως θα μπορούσαν δυνητικά τα καιρικά φαινόμενα να συνδράμουν έναν επιτιθέμενο στην διενέργεια μιας επιθέσεως πλευρικού καναλιού (π.χ. το στοιχείο του αέρα[684]).

Και επίσης, μια ακόμα παράμετρος είναι εκείνη της δυσκολίας επιτήρησης, λόγω της απομακρυσμένης τοποθεσίας, η οποία λειτουργεί εδώ και σε συνδυασμό με τις σταδιακές επιπτώσεις που φέρει η έκθεση των συσκευών σε εξωτερικά φαινόμενα επί την λειτουργία αυτών των τελευταίων (π.χ. αυξημένα ποσοστά υγρασίας). Αυτό το δεύτερο σημείο δεν έχει επαρκώς μελετηθεί, καθώς σε όσες περιπτώσεις σχεδιάστηκαν πειραματικές συνθήκες οι συσκευές είχαν εξ' αρχής εύρυθμη λειτουργία και δεν είναι ιδιαίτερα εφικτό ίσως να υπάρξει μια συγκριτική μελέτη ανάμεσα σε συσκευές λιγότερο ή περισσότερο εκτεθειμένες σε εξωτερικά φαινόμενα ή περισσότερο ή λιγότερο πολυκαιρισμένες αναφορικά με το χρονικό διάστημα στο οποίο

[683] Demestichas, K., & Peppes, N., & Alexakis, T.(2020). Survey on Security Threats in Agricultural IoT and Smart Farming. Sensors, 20(22), 6458, 1-17, σ.8.doi:10.3390/s20226458.(PDF) Survey on Security Threats in Agricultural IoT and Smart Farming (researchgate.net) (Τελευταία πρόσβαση 8/2/2022).

[684] Ο.π.,σ.1.

λειτουργούν. Αυτή είναι μια σημαντική πτυχή καθώς πολλές IoT συσκευές λειτουργούν υπό το πρίσμα της συνεχούς δραστηριότητας (για να διατηρηθεί η διασύνδεση και η πολυλειτουργικότητα των Κρίσιμων Υποδομών, που πολλές εξ' αυτών λειτουργούν 24/7), και προς ώρας δεν είναι κατανοητό πως αυτό το στοιχείο επηρεάζει τις εκροές τους[685].

- Μια ακόμα τάση που παρατηρήθηκε σε σχέση με τα ενσωματωμένα συστήματα στην βιβλιογραφία που μελετήθηκε είναι εκείνη της όλο και εναργέστερης προσέγγισης ανάμεσα στο υλικό και το λογισμικό (π.χ. embedded software). Στο πλαίσιο (και) της διαλειτουργικότητας (*interoperability*) μια τέτοια σύγκλιση ανέδειξε δύο ειδών μεταβλητές που παρουσιάζουν ενδιαφέρον στο πλαίσιο της μελέτης των SCAs έναντι του IoT (και των Κρίσιμων Υποδομών). Αφενός, η αυξανόμενη δυνατότητα των ενσωματωμένων συστημάτων να λειτουργούν υπό όρους δικτύωσης (*networked*) οδηγεί σε σύγκλιση της ύπαρξης και από κοινού λειτουργίας των αναλογικών με τα ψηφιακά τμήματα που ενυπάρχουν σε πολλά ενσωματωμένα συστήματα (π.χ. σε κυκλώματα κλπ[686]).

Μια τέτοια ετερογενείς συνέργεια στοιχείων (components), πέραν του να αναδεικνύει τον ρόλο των κατασκευαστών υλικού στην στρατηγική για την αντιμετώπιση των SCAs, ταυτόχρονα μπορεί να υποδείξει τρόπους συνδυασμού και επαύξησης των εκροών που ένας επιτιθέμενος θα μπορούσε δυνάμει να εκμεταλλευθεί. Αφετέρου, κι αυτό δεν έχει προς ώρας μελετηθεί από την βιβλιογραφία (τουλάχιστον όχι εκείνη που μελετήθηκε για τους σκοπούς της διπλωματικής εργασίας), πρέπει να εξεταστεί αν η συνύπαρξη τέτοιων ετερογενών στοιχείων στα ενσωματωμένα συστήματα μπορεί δυνάμει να οδηγήσει σε συνδυασμούς επιθέσεων πλευρικού καναλιού, ή ακόμα περισσότερο σε ακολουθιακή εναλλαγή SCAs, όπου η μια εκροή

---

[685]Ενδεχομένως στην περίπτωση των υποβρύχιων IoT συσκευών (*Internet of Underwater Things*, *IoUT*) όπου η διαχείριση πόρων και η συντήρηση συσκευών είναι ανοικτά ζητήματα κυρίως λόγω του περιβάλλοντος εντός του οποίου βρίσκονται αυτές οι συσκευές στο πλαίσιο μιας ανάλογης Κρίσιμης Υποδομής (CI). Πρβλ. Yisa, A.G., & Dargahi, T., & Belguith, S., & Hammoudeh, M.(2020). Security challenges of Internet of Underwater Things: A systematic literature review. *Transactions of Telecommunications Technologies*, 32(3), 1-16, σ.1. doi:10.1002/ett.4203. (PDF) Security challenges of Internet of Underwater Things: A systematic literature review (researchgate.net) (Τελευταία πρόσβαση 10/10/2022).

[686] Camurati, G., & Poeplau, S., & Muench, M., & Hayes, T., & Francillon, A. (2018). *Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers*. Paper presented at the 25th ACM Conference on Computer and Communcations Security. Toronto, Canada. October, 15-19, 1-14, σ.2.doi:http://dx.doi.org/10.1145/3243734.3243802. Screaming Channels | Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (Τελευταία πρόσβαση 8/2/2022).

θα μπορεί να μετατραπεί (με την συνδρομή μιας SCAs) σε έτερη εκροή και επομένως να δώσει στον επιτιθέμενο διαφορετικού είδους πληροφορίες (π.χ. επί της ισχύος, της χρονικής διάστασης κλπ).

Ολοκληρώνοντας το κεφάλαιο των συμπερασμάτων καλούμαστε επίσης να παραθέσουμε ορισμένα σημεία προς μελλοντική μελέτη και ερευνητική ανάδειξη δυνάμει. Τα σημεία που παρατίθενται, με βάσει τα όσα μελετήθηκαν και αναλύθηκαν, και που δεν έχουν ακόμα προς ώρας αναδειχθεί επαρκώς στην διεθνή βιβλιογραφία, είναι (ενδεικτικά) τα κάτωθι δύο:

- Εν πρώτοις, η κατεύθυνση της μελλοντικής έρευνας σχετικά με τις SCAs θα μπορούσε μελλοντικά να κινηθεί στην κατεύθυνση της διερεύνησης περισσότερο επιθετικών εφαρμογών των εν λόγω επιθέσεων. Μέχρι τώρα οι SCAs έχουν μελετηθεί μόνο ως παθητικά σχήματα επιθέσεως (passive), ενώ δεν έχει διερευνηθεί το αν θα μπορούσαν να χρησιμοποιηθούν πιο επιθετικά (offensive), ώστε όχι απλά να ανακτήσουν πληροφορίες από έναν στόχο αλλά να είναι σε θέση να πλήξουν (μόνες τους χωρίς την συνδρομή έτερων επιθέσεων) την λειτουργικότητα ενός συστήματος (π.χ. IoT συσκευές), και κατ' επέκταση την συνολική λειτουργία μιας Κρίσιμης Υποδομής (CI).
- Εν δευτέροις, θα μπορούσε μελλοντικά να διερευνηθεί η δυνατότητα διενέργειας συνδυαστικών επιθέσεων πλευρικών καναλιών (*combined Side-Channel Attacks*) για μεγιστοποίηση του οφέλους και για καλύτερο και πιο ανθεκτικό σχεδιασμό αντιμέτρων έναντι αυτών. Μια τέτοια μελέτη θα αποτελούσε ένα ενδιαφέρον εγχείρημα δεδομένης (και) της ευελιξίας που δεδομένα παρουσιάζουν και αξιοποιούν κατά τον σχεδιασμό και την εκτέλεση τους οι εν λόγω επιθέσεις.

Βιβλιογραφία

Ιστοσελίδες

Cybersecurity Glossary Explore Terms: A Glossary of Common Cybersecurity Terminology. *NICCS National Initiative For Cybersecurity Careers and Studies.*

Siemens (χ.χ.). Side-channel attacks. *Tech Design Forum*.

Ξενόγλωσση

χ.σ.(2020). The DIB as critical infrastructure during COVID-19. *NDIA.*

x.σ.(2019-2020). *From January 2019 to April 2020 Information leakage ENISA Threat Landscape*. Athens: ENISA European Union Agency for Cybersecurity,1-20.

χ.σ.(2016). *Healthcare and Public Health Sector-Specific Plan.* Washington: Homeland Security.

χ.σ.(2015). *Financial Services Sector-Specific Plan 2015.* Washington: The Department of Treasury, US Department of Homeland Security.

χ.σ.(2015). *Communications Sector-Specific Plan An Annex to the NIPP 2013.* Washington: Homeland Security.

χ.σ.(2015). *Energy Sector-Specific Plan.* Washington: Homeland Security.

χ.σ.(2015). *Water and Wastewater Systems Sector-Specific Plan.* Washington: Homeland Security, United States Environmental Protection Agency.

χ.σ.(2015). *Government Facilities Sector-Specific Plan an annex to the NIPP 2013.* Washington: Homeland Security GSA.

χ.σ.(2015). *Critical Manufacturing Sector-Specific Plan An Annex to the NIPP 2013.* Washington: Homeland Security.

χ.σ.(2015). *Transportation Systems Sector-Specific Plan.* Washington: Homeland Security United States Department of Transportation.

χ.σ.(χ.χ.). Lehrstuhl fur Eingegettete Sicherheit. *Ruhr-Universitat Bochum*.

χ.σ.(χ.χ.). Changes to better protect critical infrastructure. *Australian Government Department of Home Affairs, Cyber and Infrastructure Security Centre.*

χ.σ.(χ.χ.). The 16 Sectors of Critical Infrastructure Cybersecurity. *Cipher insights Blog.*

χ.σ.(2015). *Food and Agriculture Sector-Specific Plan.* Washington: Food and Drug Administration, USDA, Homeland Security.

χ.σ.(χ.χ.). Side-Channel Attack. *Glossary, Information Technology Laboratory Computer Security Center(CSRC),NIST*.

χ.σ.(χ.χ.). Embedded System Definition. *HEAVY.AI*.

Abrishamchi, M.A.N., & Abdullah, A.H., & Cheok, A.D., Bielawski, K.S.(2017). *Side Channel Attacks on Smart Home Systems: A short Overview*. Paper presented at the IECON 2017-43RD Annual Conference of the IEEE Industrial Electronics Society. Beijing, China. October 29- November 1, 4926-4932.

Agosta, G., & Barenghi, A., & Pelosi, G., & Scandale, M.(2015). The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34, 8, 1320-1333.

Ahmad, I., & Rahman, T., & Zeb, A., & Khan, I., & Ullah, I., & Hamam, H., & Cheikhrourou, O.(2021). Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks. *Wireless Communications and Mobile Computing,* Vol.2021, Article ID 1444024, 1-15.

Alahmadi, A.D., & Rehman, S.U., & Alhazmi, H.S., & Glynn, D.G., & Shoaib, H., & Sole, P.(2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* 2022, 22, 3520, 1-14.

Aldaya, A.C., & Brumley, B.B.(2021). Online Template Attacks:Revisited. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(3),*28-59(1-32).

AlDosari, F.(2017). Security and Privacy Challenges in Cyber-Physical Systems. *Journal of Information Security,8,*285-295.

Alqazzaz, A., & Alrashdi, I., & Alharthi, R., & Aloufi, E., & Zohdy, M.A.(2018).*An Insight into Android Sid-Channel Attacks*. Paper presented at the 2018 International Confrerence on Computational Science and Computational Intelligence (CSCI). Tangerang, Indonesia. September 07-08, 2018, 776-780.

Al-Shareeda, M., & Manickam, S., & Mohammed, B.A., & Al-Mekhlafi, Z.G., & Qtaish, A., & Alzahrani, A.J., & Alshammari, G., & Sallam, A.A., & Almekhlafi, K.(2022).Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks. *Applied Sciences* 2022, 12, 5939, 1-17

Ambrose, J.A., & Ragel, R.G., & Jayasinghe, D., & Li, T., & Parameswaran, S.(2015). *Side Channel Attacks in Embedded Systems: A Tale of Hostilities and Deterrence*. Paper presented at the 16th Symposium on Quality Electronic Design. Santa Clara, SA, USA. March, 02-04, 1-9.

Anglmayer, I.(2021). *European critical infrastructure Revision of Directive 2008/114/EC* (PE 662.604). Brussels: European Parliamentary Research Service.

Azriel, L., & Ginosar, R., & Gueron, S., & Mendelson, A.(2017). Using Scan Side Channel to Detect IP Theft. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25, 12,*3268-3280 (1-13).

Bache, F., & Guneysu, T.(2022). Boolean Masking for Arithmetic Additions Arbitrary Order in Hardware. *Applied Sciences* 2022, 12, 2274, 1-14.

Bakes, M., & Gerling,S., & Pinkal, M., & Sporleder, C.(2010). *Acoustic Side-Channel Attacks on Printers.* Paper presented at the 19th USENIX Security Symposium,DC,USA,August,11-13,1-16.

Batina, L., & Djukanovic, M., & Heuser, A., & Picek, S.(2021). It Started with Templates: The Future of Profiling in Side-Channel Attacks. Στο Avoine, G., & Hernandez-Castro, J. (επιμ.) *Security of Ubiquitous Computing Systems* (133-145). Springer, Cham.

Bellizia, D., & Bongiovanni, S., & Olivieri, M., & Scotti, G.(2020). SC-DDPL: A Novel Standard-Cell Based Approach for Counteracting Power Analysis Attacks in the Presence of Unbalanced Routing. *IEEE Transactions on Circuits and Systems I: Regular Papers,* 67, 7, 2317-2330(1-14).

Biedermann, S., & Katzenbeisser, S., & Szefer, J.(2015). *Hard Drive Side-Channel Attacks using Smartphone Magnetic Field Sensors.* Paper presented at FC 2015: Financial Cryptography and Data Security, Lecture Notes in Computer Science(), vol.8975.San Juan, Puerto Rico, January 30, 2015.

Biswas, A.K., & Ghosal, D., & Nagaraja, Sh.(2016). A Survey of Timing Channels and Countermeasures. *ACM Computing Surveys (CSUR),0,0,*1-39.

Bossuet, L., & Benhani, E.M.(2021). Performing Cache Timing Attacks from the Reconfigurable Part of a Heterogeneous SoC- An Experimental Study. *Applied Sciences*, 11, n.14:6662,1-14.

Brinkmann, R.(2019). Side-Channel Attacks on Embedded Processors. *EE|Times 50*, *Designlines.*

Bronchain, O., & Cassiers, G.(2022). Bitslicing Arithmetic/Boolean Masking Conversions for Fun and Profit: with Application to Lattice-Based KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems,* 2022, 4, 553-588.

Bursztein, E., & Picod, J-M.(2020). *A Hacker's Guide to reducing side-channel attack surfaces using deep learning.* Paper presented at the Defcon 28 & Black Hat. USA, Virtual Event (originally intended to take place in Las Vegas),August,1-9, 1-68.

Camurati, G., & Poeplau, S., & Muench, M., & Hayes, T., & Francillon, A.(2018). *Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers*. Paper presented at the 25th ACM Conference on Computer and Communications Security. Toronto, Canada. October, 15-19, 1-14.

Cheng, P., & Bagci, I.E., & Roedig, U., & Yan, J.(2018). SonarSnoop: Active Acoustic Side-Channel Attacks. *International Journal of Information Security ,* 19, 213-228 (1-13) (2020).

Clark, S.S., & Ransford, B., & Rahmati, A., & Guineau, S., & Sorber, J., & Fu, K., & Xu, W.(2013). *WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices.* Paper presented at the 2013 USENIX Workshop on Health Information Technologies (HealthTech '13), Washington DC, USA, August 12, 1-11.

Chen, P., & Li, L., & Yang, Zh.(2021). *Cross-VM and Cross-Processor Covert Channels Exploiting Processor Idle Power Management.* Paper presented at the USENIX Security '21 30th USENIX Security Symposium. Vancouver, BC, Canada, August, 11-13, 733-750(1-19).

Chong, K.-S., & Ng, J.-S., & Chen, J., & Lwin, N.K.Z., & Kyaw, N.A., & Ho, W.-G., & Chang, J., & Gwee, B.-H.(2021). Dual-Hiding Side-Channel-Attack Resistant FPGA-Based Asynchronous-Logic AES: Design, Countermeasures and Evaluation. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 11, 2, 343-356 (1-15).

Compagno, A., & Conti, M., & Lain, D., & Tsudik, G.(2017). *Don't Skype & Type ! Acoustic Eavesdropping in Voice-Over-I*P. Paper presented at the Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. Abu Dhabi, UAE. April 2-6, 1-13.

Cour, A.S.L., & Afridi, K.K., & Suh, G.E.(2021). Wireless Charging Power Side-Channel Attacks. *A arXiv:2105.12266v2 [cs.CR]*,1-13.

Courousse, D., & Barry, Th., & Robisson, B., & Jaillon, P., & Potin, O., & Lanet, J.-J.(2016). *Runtime Code Polymorphism as a Protection Against Side Channel Attacks.* Paper presented at the 10th IFIP WG 11.2 International Conference on Information Security Theory and Practice (WISTP 2016). Greece, Heraklion. September, 26-27, 1-16.

Davis, A., & Rubinstein, M., & Wadhwa, N., & Mysore, G.J., & Durand, F., & Freeman, W.T. (2014). The Visual Microphone: Passive Recovery of Sound from Video. *ACM Transactions on Graphics, 33, 4, 79,*1-10.

Delarea, S., & Oren, Y.(2022). Practical, Low-Cost Fault Injection Attacks on Personal Smart Devices. *Applied Sciences* 2022, 12, 417,1-10.

Demestichas, K., & Peppes, N., & Alexakis, T.(2020). Survey on Security Threats in Agricultural IoT and Smart Farming. Sensors, 20(22), 6458, 1-17.

Fjader & Riedman στο Heino, O., & Takala, A., & Jukarainen, P., & Kalalahti, J., & Kekki, T., & Verho,P.(2018). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability 2019, 11(3), 838,*1-18.

Fadaeinia, B., & Moos,T., & Moradi,A.(2021). Balancing the Leakage Currents in Nanometer CMOS Logic- A Challenging Goal. *Applied Sciences* 2021, 11 (15), 7143,1-18.

Faruque, M.A., & Chhetri, S.R., & Faezi,S., & Canedo,A.(2016). *Forensics of Thermal Side-Channel in Additive Manufacturing Systems*.Paper presented at the ICCPS '16: Proceedings of the 7th International Conference on Cyber-Physical Systems. Vienna, Austria. April 11-14, 1-15.

Fow, E-G.(2019). A Brief Peek Into the Fascinating World of Side Channel Attacks. *Start it up.*

Giechaskiel, I., & Tian, S., & Szefer, J.(2022). Cross-VM Covert- and Side-Channel Attacks in Cloud FPGAs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS),* 32*,* 1-29.

Goller, G., & Sigl, G.(2015). *Side Channel Attacks on Smartphones and Embedded Devices Using Standard Radio Equipment*. Paper presented at the 6th International Workshop, COSADE 2015. Berlin, Gemrany.April,13-15, 1-16(255-270).

Goodin, D.(2019). Researchers use Rowhammer bit flips to steal 2048-bit crypto key. *Arstechnica*.

Gu, R., & Wang, P., & Zheng, M., & Hu, H., & Yu, N.(2020). Adversarial Attack Based Countermeasures against Deep Learning Side-Channel Attacks. Journal of University of Science and Technology of China, 50(10), 1343-1358 (1-22).

Gunathilake, N.A., & Al Dubai, A., & Buchanan, W.J., & Lo, O. (2020). *Electromagnetic Analysis of an Ultra-Lightweight Cipher:PRESENT*. Paper presented at the 10th International Conference on Information Technology Convergence and Services (ITCSE 2021). Sydney, Australia. June, 26-27, 185-205.

Gupta, M.S.(χ.χ.). Need for SCADA Migration Plan Increases with New Functionality. *ARC Advisory Group.*

Jaamoum, A., & Hiscock, T., & Di Natale, G.(2022). Noise-Free Security Assessment of Eviction Set Construction Algorithms with Randomized Caches. *Applied Sciences* 2022, 12, 2415, 1-22.

Jain, S., & Wang, Q., & Arafin, M.T., & Guajardo, J.(2018). *Probing Attacks on Physical Layer Key Agreement for Automotive Controller Area Networks.* Paper presented at the ESCAR Europe 2017. Aachen, Deutschland. November,7-8,1-12.

Jha, A.(2020). IoT Security-Part 19 (101-Introduction to Side Channel Attacks(SCA)). *Payatu.* IoT Security - Part 19 (101 - Introduction to Side Channel Attacks (SCA)).

Jevtic, R., & Otero, M.G. (1011). Methodology for Complete Decorrelation of Power Supply EM Side-Channel Signal and Sensitive Data. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 69, 2256-2260.

Hasnain, A., & Asfia, Y., & Khawaja, S.G.(2022). *Power profiling-based side-channel attacks on FPGA and Countermeasures: A survey*. Paper presented at the 2022 2nd International Conference on Digital Futures and Transformative Technologies (ICoDT2). Rawalpindi, Pakistan. May 24-26, 1-8.

Heinly, J., & White, A.M., & Frahm, J.-M.(2013).*Seeing double: Reconstructing obscured typed input from repeated compromising reflections*. Paper presented at the CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. Berlin, Germany. November 4-8, 2013,1063-1074.

Heino, O., & Takala, A., & Jukarainen, P., & Kalalahti, J., & Kekki, T., & Verho,P.(2018). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability 2019, 11(3), 838,*1-18.

Heuser, A., & Picek, S., & Guilley, S., & Mentens, N.(2017). Side-Channel Analysis of Lightweight Chipers: Does Lightweight Equal Easy ? *Lecture Notes in Computer Science, 10155:*91-104.

Iijima, R., & Minami, S., & Zhou, Y., & Takehisa, T., & Takahashi, T., & Oikawa, Y., & Mori, T.(2021). Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams and its Feasibility. *IEEE Transactions on Emerging Topics in Computing ,*vol.9, n.4*,*2004-2018.

Izuakor,C. & White, R.(2017). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Paper presented at the 10th Conference on Critical Infrastructure Protection (ICCIP). Arlington, VA, USA. March,10-13, 27-41.

Kiaei, P., & Schaumont, P.(2020). Domain-Oriented Masked Instruction Set Architecture for RISC-V. *IACR Cryptology ePrint Archive* 2020 (2020), 465-468 (1-4).

Khan, H.A., & Alam, M., & Zajic, A., & Prvulovic, M.(2018). *Detailed Tracking of Program Control Flow Using Analog Side-Channel Signals: A Promise for IoT Malware Detection and a Threat for Many Cryptographic Implementations.* Paper presented at the Cyber Sensing 2018, SPIE Defense + Security (SPIE). Orlando, Florida, USA, April 15-19, 1-14.

Khan, M.N.I., & Bashin, Sh., & Liu, B., & Yuan, A., & Chattopadhyay, A., & Ghosh, S.(2021). Comprehensive Study of Side-Channel Attack on Emerging Non-Volatile Memories. *Journal of Low Power Electronics and Applications, 2021, 11(4),38*,1-18.

Kleinman, L.(2020). Organizations Must Develop Zero Trust to Defend Against DDoS Attacks. Here's Why. *Securing the Digital World.*

Knechtel, J., & Sinanoglu, O.(2017). *On mitigation of side-channel attacks in 3D ICs: Decorrelating thermal patterns from power and activity.* Paper presented at the 2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC), 2017. Austin, TX, USA, June, 18-22, 1-6.

Kocher, P., & Jaffe, J., & Jun, B.(1999). *Differential Power Analysis*. Paper presented at the 19th Annual International Cryptology Conference (Advances in Cryptology-CRYPTO'99). Santa Barbara, California, USA, August 15-19, 1-10.

Krombholz, K., & Hupperich, T., & Holz, T.(2016). *Use the Force: Evaluating Force-Sensitive Authentication for Mobile Devices*. Paper presented at the 12th Symposium on Usable Privacy and Security (SOUPS 2016). Denver, CO, USA. June 22-24, 207-219.

Kuroda, K., & Fukuda, Y., & Yoshida, K., & Fujino, T.(2021). *Practical Aspects on Non-profiled Deep-learning Side-channel Attacks against AES Software Implementation with Two Types of Masking Countermeasures including RSM*. Paper presented at the Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security (ASHES '21). Virtual Event, Republic of Korea. November 19,29-40.

Kurtz, A., & Gascon, H., & Becker, T., & Rieck, K., & Freiling, F.(2016). *Fingerprinting Mobile Devices Using Personalized Configurations.* Paper presented at the 2016 Proceedings on Privacy Enhancing Technologies. Darmstadt, Germany. July, 19-22, 1-17.

Lake, J.(2021). What is a side-channel attack and how do they work ? *comparitech*.

Lavaud, C., & Gerzaguet, R., & Gantier, M., & Berder, O., & Nogues, F., & Molton, St.(2021). Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and System Security*, Springer, 2021, 1-24.

Legon-Perez, C.M., & Sanchez-Muina, R., & Miyares-Moreno, D., & Bardaji-Lopez, Y., Martinez-Diaz, I., Rojas, O., Sosa-Gomez, G.(2021). Search-Space Reduction for S-Boxes Resilient to Power Attacks. *Applied Sciences* 2021, 11, 4815,1-20.

Levi, I., & Bellizia, D., & Bol, D., & Standaert, F.-X. (2020). Ask Less, Get More: Side-Channel Signal Hiding , Revisited. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 67, 12*,* 4904-4917 (1-14).

Liu, H., & Spolaor, R., & Turrin, F., & Bonafede, R., & Conti, M.(2021). USB powered devices: A survey of side-channel threats and countermeasures. *High-Confidence Computing 1* (2021), 10007, 1-12.

Liu, Z., & Samwel, N., & Weissbart, L., & Zhao, Z. & Lauret, D., & Batina, L., & Larson, M.(2020). *Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel*. A paper presented at The Network and Distributed System Security Symposium 2021. Virtual venue. 21-25 February,1-15.

Lou, X., & Zhang, T., & Jiang, J., Zhang, Y.(2021). A Survey of Microarchitectural Side-channel Vulnerabilities, Attacks, and Defenses in Cryptography. *ACM Computing Surveys, 54(6),* 1-37.

Lulka, J.(2022). 5 embedded systems terms IoT Admins must know. *TechTarget, IoTAgenda.*

Luo, M., & Myers, A.C., & Suh, G.E.(2020). *Stealthy Tracking of Autonomous Vehicles with Cache Side Channels.* Paper presented at the 29th USENIX Security Symposium. Virtual Event, August, 12-14,1-18(859-876).

Lyu, Y., & Mishra, P..(2017). A Survey of Side-Channel Attacks on Caches and Countermeasures. *Journal of Hardware and Systems Security,*2,33-50(2018).

Maiti, A., & Jadiwala, M., & He, J., & Bilogrevic, I.(2018). Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches. *IEEE Transcactions on Mobile Computing* PP (99),1-16.

Maloney,D.(2019). Side-Channel Attacks shows vulnerabilities of cryptocurrency wallets. *Hackaday*.

Mao, Y., & Migliore, V., & Nicomette, V.(2022). MATANA: A Reconfigurable Framework for Runtime Attack Detection Based on the Analysis of Microarchitectural Signals. *Applied Sciences* 2022, 12, 1452, 1-22.

Marquardt, P., & Verma, A., & Carter, H., & Traynor, P.(2011). *(sp) iPhone: Decoding vibrations from nearby keyboards using mobile accelerometers*. Paper presented at the proceedings of the 18th ACM Conference on Computer and Communications Security, CSS 2011. Chicago, Illinois, USA. October 17-21, 10-12.

Montasari, R., & Hill, R., & Hosseinian-Far, A., & Montaseri, F.(2019). Countermeasures for Timing-Based Side-Channel Attacks against Shared, Modern Computing Hardware. *International Journal of Electronic Security and Digital Forensics*, 11, 294-320.

Montasari, R., & Hosseinian-Far, A., & Hill, R., & Montaseri, F., & Sharma, M., & Shabbir, Sh.(2018). Are Timing-Based Side-Channel Attacks Feasible in Shared, Modern Computing Hardware ?. *International Journal of Organizational and Collective Intelligence,8,2,*32-59.

Moradi, A., & Immler, V.(2014). *Early Propagation and Imbalanced Routing How to Diminish in FPGAs*. Paper presented at the 16th International Workshop Cryptographic Hardware and Embedded Systems (CHES 2014). Busan, South Korea. 23-26 September, 1-18.

Pedro, M.S., & Servant, V., & Guillement, C.(2019). Side-Channel assessment of Open Source Hardware Wallets. *Cryptology ePrint Archive,* Paper 2019/401, 1-26.

Phan, Q-S., & Bang, L., & Pasareanu, C.S., & Malacaria, P., & Bultan, T.(2017). *Synthesis of Adaptive Side-Channel Attacks.* Paper presented at the 2017 IEEE 30th Computer Security Foundations Symposium (CSF). Santa Barbara,CA,USA, August,21-25, 1-15.

Picek, S., & Perin, G., & Mariot, L., & Wu, L., & Batina, L.(2021). SoK: Deep Learning-based Physical Side-channel Attacks. *ACM Computing Surveys,* 1-33.

Pozzobon, E., & Renner, S., & Mottok, J., & Matousek, V.(2022). *An optimized Bitsliced Masked Adder for ARM Thumb-2 Controllers*. Paper presented at the 2022 International Conference on Applied Elecronics (AE). Pilsen, Czech Republic. 06-07 September, 1-4, σ.1-4.

Potestad-Ordonez, F.E., & Tena-Sanchez, E., & Acosta-Jimenez, A.J., & Jimenez-Fernandez, C.J., & Chaves, R.(2022). Hardware Countermeasures Benchmarking against Fault Attacks. *Applied Sciences*, 2022, 12(5), 2443, 1-20.

Pycroft, L., & Aziz, T.Z.(2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices,*15:6*,* 403-406.

Real, M.M., & Salvador,R.(2021). Physical Side-Channel Attacks on Embedded Networks: A Survey. *Applied Science, 11, 6790*, 1-25.

Roth, T., & Datko, J., & Nedospasov,D.(2018). Using TensorFlow/ machine learning for automated RF side –channel attack classification. *Leveldown.*

Saeedi, E., & Kong, Y.(2014). Side-channel Vulnerabilities of Automobiles. *Transaction on IoT and Cloud Computing ,2(2),* 1-8.

Sayakkara, A, & Le-Khac, N.A., & Scanlon, M.(2019). A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics. *Elsevier Digital Investigations,arXiv:1903.07703v1[cs.CR]*,1-13.

Sayakkara, A., & Le-Khac, N., & Scanlon, M.(2018). Electromagnetic Side-channel Attacks: Potential for Progressing Hindered Digital Forensic Analysis. *Forensic Focus for Digital Forensics & E-Discovery professionals.*

Selvam, R., & Shanmugam, D., & Annadurai, S.(2015). *Side Channel Attacks: Vulnerability Analysis of PRINCE and RECTANGLE using DPA.* Paper presented at the Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. Singapore, Republic of Singapore. 14 March- 14 April, 2015, 1-15.

Shafiq, M., & Gu, Z., & Cheikhrouhou, O., & Alhakami, W., & Hamam, H.(2022). The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. *Wireless Communications and Mobile Computing,* 2022, 1-12.

Machine Learning Methods to Detect Voltage Glitch Attacks on IoT/IIoT Infrastructures. *Computational Intelligence and Neuroscience*, 22, 1-7.

Simmon, T.(2017). Critical Infrastructure and the Internet of Things. *Global Commission on Internet Governance Paper Series GCIG,46,*1-11.

Spreitzer, R., & Moonsamy, V., & Korak, T., & Mangard, S.(2017). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys & Tutorials,*20, 1,465-488 (1-24).

Socha, P., & Novotny, M.(2020). *Towards High-Level Synthesis of Polymorphic Side-Channel Countermeasures.* Paper presented at the 2020 23rd Euromicro Conference on Digital System Design(DSD). Slovenia, Kranj. August,26-28, 1-7.

Staddon, E., & Loscri, V., & Mitton, N.(2021). Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Applied Sciences,2021,11,7228,* 1-39.

Standaert, F-X. (2010). Introduction to Side-Channel Attacks.Στο I.M.R. Verbauwhede (Επιμ.), *Secure Integrated Circuits and Systems* (σ.27-42),σ.27. Leuven: Springer Link.

Steiner, I.G., & LeFevre, Z., & Serwadda,A.(2020). Smartphone Speech Privacy Concerns from Side-Channel Attacks on Facial Biomechanics. *Computers & Security*, vol.100,1-16.

Takatoi, G., & Sugawara, T., & Sakiyama, K., & Hara-Azumi, Y., & Li, Y.(2022). The Limits of SEMA on Distinguishing Similar Activation Functions of Embedded Deep Neural Networks. *Applied Sciences* 2022, 12(9), 4135, 1-20.

Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28.

Tessari, P. & Muti, K.(2021). *Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations* (PE 653.637).Brussels: Requested by the INGE committee European Parliament.

Townley, D., & Ponomarev, D.(2019). *SMT-COP: Defeating Side-Channel Attacks on Execution Units in SMT Processors.* Paper presented at the 2019 28th International Conference on Parallel Architectures and Compilation Techniques (PACT). Seattle, WA, USA. September, 23-26, 43-54(1-12).

Tramer, F., & Boneh, D., & Paterson, K.G.(2020). *Remote Side-Channel Attacks on Anonymous Transactions.* Paper presented at the proceedings of the 29th USENIX Security Symposium. Virtual Event Venue. August, 12-14, 2739-2756.

Tsalis, N., & Vasilellis, E., & Mentzelioti, D., & Apostolopoulos, T.(2019). A Taxonomy of Side-Channel Attacks on Critical Infrastructures and Relevant Systems,283-313,σ.298-301. Στο D. Gritzalis & M. Theocharidou & G. Stergiopoulos(Επιμ.), *Advanced Sciences and Technologies for Security Applications Infrastructure Security and Resilience Theories, Methods, Tools and Technologies* (σ.1-311).Cham:Springer.

Udeanu, G.(2015). *A New Approach To The European Programme For Critical Infrastructure Protection.*Paper presented at the 21st International Conference The Knowledge-

Based Organization, Conference Proceedings 1 Management and Military Sciences, 21, 1, 2015, 135-142.

Weinberg, A.(2021). Analysis of top 11 cyber attacks on critical infrastructure. *FirstPoint*.

Yisa, A.G., & Dargahi, T., & Belguith, S., & Hammoudeh, M.(2020). Security challenges of Internet of Underwater Things: A systematic literature review. *Transactions of Telecommunications Technologies*, 32(3), 1-16.

Younis, Y.A., & Kilayat, K., & Merabti, M.(2014). *Cache-Side Channel Attacks in Cloud Computing*. Paper presented at the 2nd International Conference on Cloud Security Management (ICCSM 2014). Cranfield , United Kingdom. October 23-24, 1-11.

Wang, W., & Guo, C., & Yu, Y., & Ji, F., & Su, Y.(2022). Side-Channel Masking with Common Shares. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022 (3), 290-329.

Wang, Y., & Ferraiuolo, A., & Suh, G.E.(2014). *Timing Channel Protection for a Shared Memory Controller*. Paper presented at the Proceedings of the 20th International Symposium on High Performance Computer Architecture (HPCA). Orlando, FL, USA. February 15-19, 1-12.

Weinberg, A.(2021). Analysis of top 11 cyber attacks on critical infrastructure. *FirstPoint*.

Wild, A., & Moradi, A., & Guneysu, T.(2018). GliFreD: Glitch-Free Duplication Towards Power-Equalized Circuits on FPGAs. *IEEE Transactions on Computers*, 67, 3, 375-387 (1-8).

Tena-Sanchez, E., & Potestad-Ordonez, F.E., & Jimenez-Fernandez, C.J., & Acosta, A.J., & Chaves, R.(2022). Gate-level Hardware Countermeasure Comparison against Power Analysis Attacks. *Applied Sciences* 2022, 12(5), 2390, 1-28.

Wright, G., & Gillis, A.S.(χ.χ.). Side-channel attack. *Techtarget.*

Zhang, L., & Hu, W., & Ardeshiricham, A., & Tai, Y., & Blackstone, J., & Mu, D., & Kastner, R.(2018). *Examining the Consequences of High-Level Synthesis Optimizations on*

Power Side-Channel. Paper presented at the 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE). Dresden, Germany. March, 19-23,1-4.

Zhang, Q., & Wang, A., & Niu, Y., & Shang, N., & Xu, R., & Zhang, G., & Zhu, L.(2018). Side-Channel Attacks and Countermeasures for Identity-Based Cryptographic Algorithm SM9. Security and Communication Networks, 2018, 1-15.