Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Πρόγραμμα Μεταπτυχιακών Σπουδών (ΠΜΣ) Κυβερνοασφάλεια (Cybersecurity)

Ευφυείς Επιθέσεις στο Υλικό με Χρήση Μεθόδων Μηχανικής Μάθησης

Χριστοδούλου Παναγιώτα

AM cscyb19027

Επιβλέπων: Δρ. Εμμανουήλ Θ. Μιχαηλίδης, Διδάσκων ΠΜΣ

Αιγάλεω, Ιούνιος 2021

Πίνακας Περιεχομένων

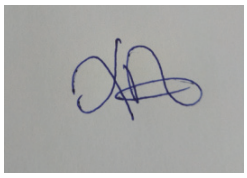
Δήλωση συγγραφέα μεταπτυχιακής εργασίας

Η κάτωθι υπογεγραμμένη Παναγιώτα Χριστοδούλου φοιτήτρια του προγράμματος μεταπτυχιακών σπουδών «Κυβερνοασφάλεια» του Τμήματος μηχανικών πληροφορικής και υπολογιστών της σχολής μηχανικών του πανεπιστημίου Δυτικής Αττικής δηλώνω ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης οι πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών η λέξεων είτε ακριβώς είτε παραφρασμένες αναφέρονται στο σύνολό τους με πλήρη αναφορά στους συγγραφείς, στον εκδοτικό οίκο ή το περιοδικό συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα 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.»

Η δηλούσα



Παναγιώτα Χριστοδούλου

Εξεταστική Επιτροπή

Α/Α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ/ΤΜΗΜΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	Στέφανος Γκρίτζαλης	Καθηγητής Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς	STEFANOS GKRITZALIS 06/08/2023 19:40
2	Παναγιώτης Γιαννακόπουλος	Καθηγητής Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, ΠΑΔΑ	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.08.10 16:43:55 +03'00'
3	Εμμανουήλ Μιχαηλίδης	Ακαδημαϊκός Υπότροφος Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, ΠΑΔΑ	Emmanouil Michailidis Digitally signed by Emmanouil Michailidis Date: 2023.07.28 23:14:27 +03'00'

Περίληψη

Η μηχανική εκμάθηση και οι αλγόριθμοί της χρησιμοποιούνται όλο και περισσότερο στην ανακάλυψη τρωτών σημείων σε λογισμικό και υλικό. Η ευπάθεια υλικού είναι μια εκμεταλλεύσιμη αδυναμία σε ένα σύστημα που επιτρέπει την επίθεση μέσω απομακρυσμένης ή φυσικής πρόσβασης στο υλικό του συστήματος. Ένας άλλος τύπος ευπάθειας υλικού είναι ένα απροσδόκητο ελάττωμα στη λειτουργία που επιτρέπει στους εισβολείς να αποκτήσουν τον έλεγχο ενός συστήματος αποκτώντας προνόμια ή εκτελώντας κώδικα. Η μηχανική μάθηση βοηθά στον εντοπισμό αυτών των σφαλμάτων πιο γρήγορα και εύκολα. Στο παρελθόν, για παράδειγμα, ένα σφάλμα θα μπορούσε να εντοπιστεί εντός εβδομάδων. Σήμερα το ίδιο σφάλμα θα μπορούσε να εντοπιστεί σε λίγα λεπτά, ανάλογα με την περίπτωση. Το πρόβλημα είναι όταν αυτή η δύναμη χρησιμοποιείται για σκοτεινούς σκοπούς.

Λέξεις-κλειδιά: Ασφάλεια υλικού, Μηχανική Μάθηση, αλγόριθμοι, επιθέσεις πλευρικού καναλιού

Abstract

Machine learning and its algorithms have been increasingly employed in the discovery of vulnerabilities in software and systems. A hardware vulnerability is an exploitable weakness in a computer system that enables attack through remote or physical access to system hardware. Another type of hardware vulnerability is an unexpected flaw in operation that allows attackers to gain control of a system by elevating privileges or executing code. Machine learning helps to identify these errors and bugs more quickly and easily. In the past, for example, an error could be identified within weeks. Today the same error could be identified in minutes, depending on the case. The problem is when this power is used for dark purposes.

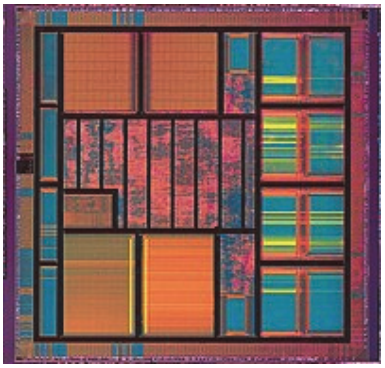
Keywords: Hardware security, Machine Learning, algorithms, side channel attacks

1. Κατηγορίες Υλικού

Η μικρότερη μονάδα στο υλικό είναι το **τρανζίστορ**.

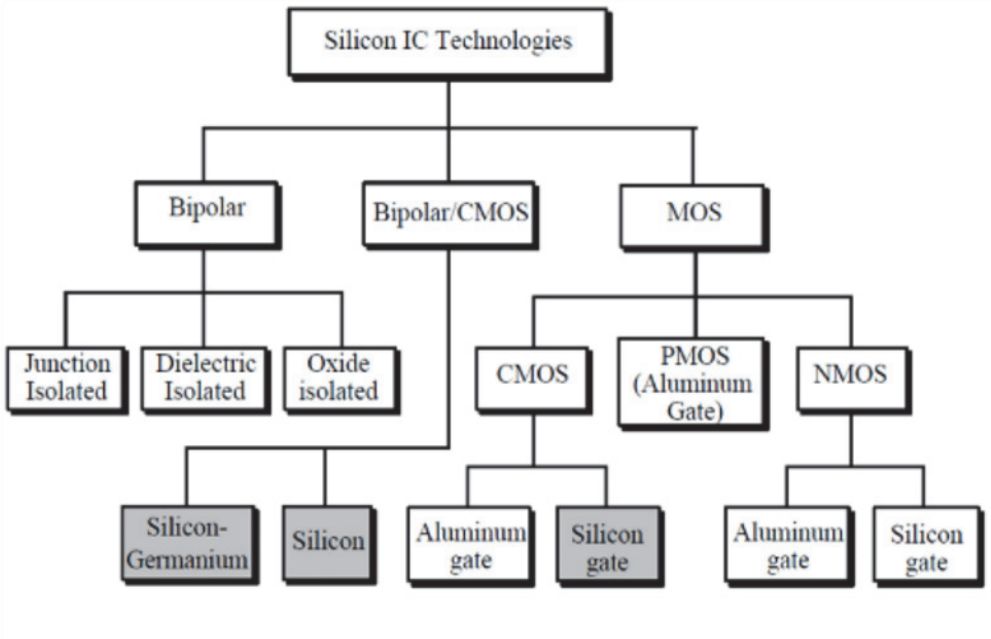
Εικόνα 1: Διάφοροι τύποι τρανζίστορ

Τα τρανζίστορ κατασκευάζονται είτε ως ξεχωριστά ηλεκτρονικά εξαρτήματα είτε ως τμήματα κάποιου **ολοκληρωμένου κυκλώματος**. Ολοκληρωμένο κύκλωμα (γνωστό και ως IC από το αγγλικό integrated circuit) ή απλά ολοκληρωμένο ονομάζεται ένα κύκλωμα συνδεδεμένων λογικών πυλών, δημιουργημένο πάνω σε ένα φύλλο. Η συντριπτική πλειονότητα των ολοκληρωμένων κυκλωμάτων δημιουργούνται πάνω σε φύλλα ημιαγωγών, κατά κύριο λόγο πυριτίου. Το φύλλο (ημιαγωγού) ονομάζεται στα αγγλικά τσιπ (chip), από το οποίο προκύπτει μια εναλλακτική ονομασία του ολοκληρωμένου κυκλώματος.



Εικόνα 2: Ολοκληρωμένο κύκλωμα

Οι κατηγορίες των IC's είναι αρκετές:

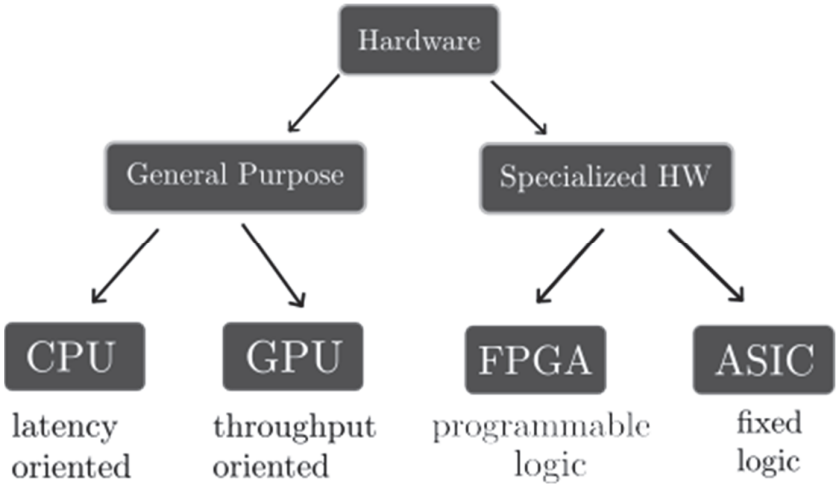


Εικόνα 3: Κατηγορίες Ολοκληρωμένων Κυκλωμάτων

Όταν αυτό το φύλλο είναι της κλίμακας των μικρομέτρων ονομάζεται και μικροτσίπ.

Όταν τα μήκη των πυλών για τα transistor CMOS του πυριτίου είναι κάτω από 100nm (σήμερα είναι στα 7nm) τότε λέγονται νανοτσιπς και οι εφαρμογές που τα χρησιμοποιούν νανοτεχνολογία όπως πχ Silicon-on-insulator (SOI), FinFET transistors, three-dimensional (3D) integrated circuits, Bulk silicon CMOS.

Τα chips συνδυάζονται μεταξύ τους και δημιουργούν **δομές υλικού** οι οποίες χωρίζονται σε γενικού και ειδικού σκοπού. Ακολουθούν οι τέσσερις (κύριες) κατηγορίες:



Εικόνα 4: Κατηγορίες υλικού

Η Κεντρική Μονάδα Επεξεργασίας - ΚΜΕ (αγγλικά: Central Processing Unit - **CPU**), είναι το κεντρικό εξάρτημα που επεξεργάζεται δεδομένα σε έναν ηλεκτρονικό υπολογιστή, ελέγχει τη λειτουργία του και εκτελεί βασικές λειτουργίες διασύνδεσης και μεταβίβασης εντολών. Αν η ΚΜΕ αποτελείται από ένα μόνο ολοκληρωμένο κύκλωμα, τότε ονομάζεται μικροεπεξεργαστής (microprocessor) ή μικροελεγκτής (microcontroller).

Οι επεξεργαστές δεν σχετίζονται αποκλειστικά με τους ηλεκτρονικούς υπολογιστές καθώς πλέον ενσωματώνονται και σε πολλές ηλεκτρονικές συσκευές όπως κινητά τηλέφωνα, ψηφιακές φωτογραφικές μηχανές, βιντεοκάμερες, κονσόλες ηλεκτρονικών παιχνιδιών και άλλα. Για την ακρίβεια, επεξεργαστές ενσωματώνονται σε κάθε είδους συσκευή στην οποία απαιτείται ύπαρξη υπολογιστικής ικανότητας.

Η μονάδα επεξεργασίας γραφικών (graphics processing unit - **GPU**) είναι ένα εξειδικευμένο ηλεκτρονικό κύκλωμα σχεδιασμένο να χειρίζεται και να τροποποιεί γρήγορα τη μνήμη για να επιταχύνει τη δημιουργία εικόνων σε ένα buffer πλαισίων που προορίζεται για έξοδο σε συσκευή απεικόνισης. Οι μονάδες GPU χρησιμοποιούνται σε ενσωματωμένα συστήματα, κινητά τηλέφωνα, προσωπικούς υπολογιστές, σταθμούς εργασίας και κονσόλες παιχνιδιών. Οι σύγχρονες μονάδες GPU είναι πολύ αποδοτικές στο χειρισμό γραφικών υπολογιστών και επεξεργασίας εικόνων. Η ιδιαίτερα παράλληλη δομή τους τους καθιστά πιο αποδοτικούς από τις κεντρικές μονάδες επεξεργασίας γενικής χρήσης (CPU) για αλγόριθμους που επεξεργάζονται παράλληλα μεγάλα μπλοκ δεδομένων. Σε έναν προσωπικό υπολογιστή, μπορεί να υπάρχει GPU σε μια κάρτα βίντεο ή ενσωματωμένη στη μητρική πλακέτα. Σε ορισμένους επεξεργαστές, είναι ενσωματωμένοι στον επεξεργαστή.

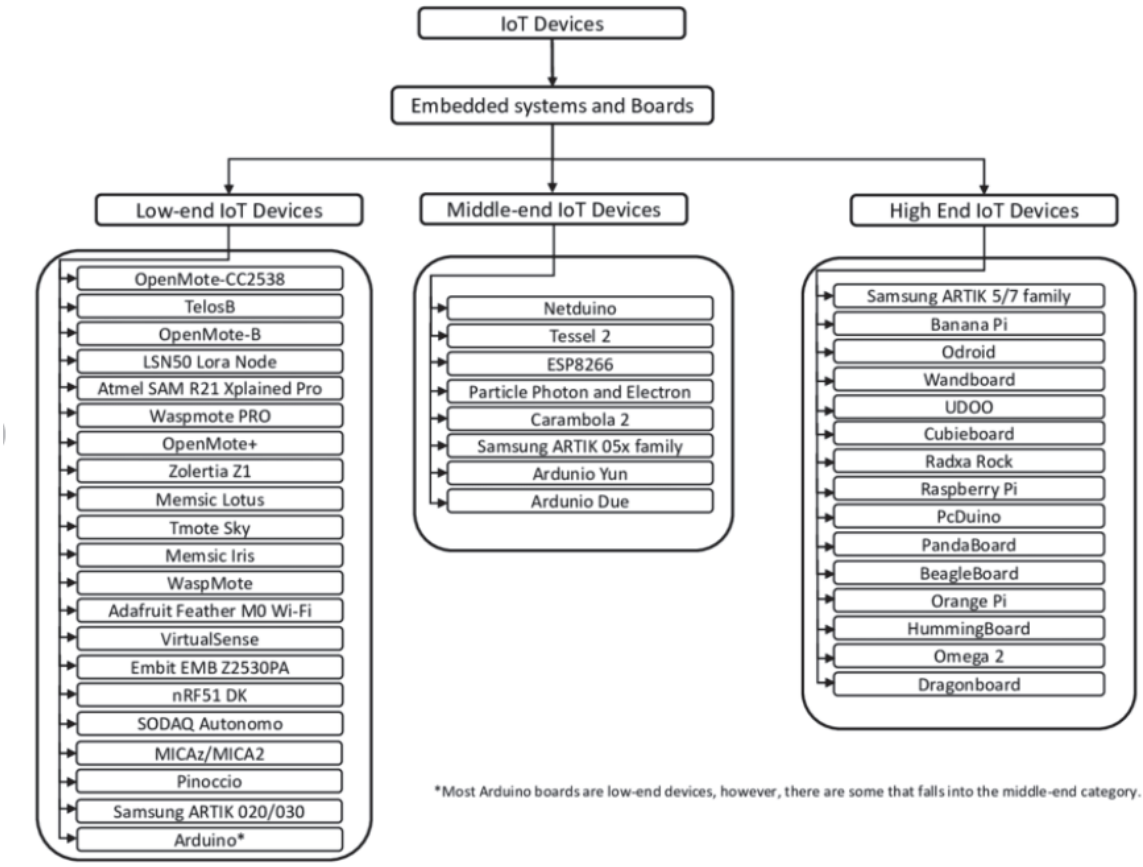
Το (application-specific integrated circuit - **ASIC**) είναι ένα chip ολοκληρωμένου κυκλώματος (IC) προσαρμοσμένο για συγκεκριμένη χρήση, αντί να προορίζεται για γενική χρήση. Για παράδειγμα, ένα τσιπ σχεδιασμένο να λειτουργεί με ψηφιακό καταγραφέα φωνής ή με bitcoin miner υψηλής απόδοσης είναι ένα ASIC. Τα τσιπ ASIC κατασκευάζονται συνήθως με τη χρήση της τεχνολογίας ημιαγωγών (MOS) μεταλλικού οξειδίου, ως ολοκληρωμένα κυκλώματα MOS. Καθώς τα μεγέθη χαρακτηριστικών έχουν συρρικνωθεί και τα εργαλεία σχεδιασμού έχουν βελτιωθεί με την πάροδο των ετών, η μέγιστη πολυπλοκότητα (και επομένως λειτουργικότητα) που είναι δυνατή σε ένα ASIC έχει αυξηθεί από 5.000 λογικές πύλες σε πάνω από 100 εκατομμύρια. Τα σύγχρονα ASIC συχνά περιλαμβάνουν ολόκληρους μικροεπεξεργαστές, μπλοκ μνήμης όπως ROM, RAM, EEPROM, μνήμη flash και άλλα μεγάλα δομικά στοιχεία. Ένα τέτοιο ASIC συχνά ονομάζεται SoC (System-on-chip).

Η συστοιχία επιτόπια προγραμματιζόμενων πυλών (Field-Programmable Gate Array - **FPGA**) είναι τύπος προγραμματιζόμενου ολοκληρωμένου κυκλώματος γενικής χρήσης το οποίο διαθέτει

πολύ μεγάλο αριθμό τυποποιημένων πυλών και άλλων ψηφιακών λειτουργιών όπως απαριθμητές, καταχωρητές μνήμης, γεννήτριες PLL κα. Κατά τον προγραμματισμό του FPGA, ο οποίος γίνεται πάντοτε ενώ αυτό είναι τοποθετημένο στο τυπωμένο κύκλωμα, ενεργοποιούνται οι επιθυμητές λειτουργίες και διασυνδέονται μεταξύ τους έτσι ώστε το FPGA να συμπεριφέρεται ως ολοκληρωμένο κύκλωμα με συγκεκριμένη λειτουργία. Για μικρότερες σχεδιάσεις ή μικρότερους όγκους παραγωγής, οι FPGA είναι πιο οικονομικά αποδοτικές από μια σχεδίαση ASIC, ακόμη και στην παραγωγή. Το μη επαναλαμβανόμενο κόστος μηχανικής (NRE) ενός ASIC μπορεί να ανέλθει σε εκατομμύρια δολάρια. Ως εκ τούτου, οι κατασκευαστές συσκευών συνήθως προτιμούν τις FPGA για την κατασκευή πρωτοτύπων και συσκευών με χαμηλό όγκο παραγωγής και τις ASIC για πολύ μεγάλους όγκους παραγωγής, όπου το κόστος NRE μπορεί να αποσβεσθεί σε πολλές συσκευές.

Οι δομές υλικού με τη σειρά τους συνδυάζονται και χρησιμοποιούνται σχεδόν σε κάθε συσκευή **ηλεκτρονικού εξοπλισμού** που χρησιμοποιείται σήμερα και θεωρούνται επανάσταση στον τομέα της ηλεκτρονικής.

Το δίκτυο επικοινωνίας όλων αυτών των εντελώς διαφορετικών μεταξύ τους συσκευών (οικιακών, αυτοκίνητα με ενσωματωμένους αισθητήρες, κάμερες, κλιματιστικά, φώτα, συστήματα ασφαλείας, smartwatches ακόμα και αυτοκίνητα των οποίων οι περίπλοκοι αισθητήρες εντοπίζουν αντικείμενα στην πορεία τους) ονομάζεται **Διαδίκτυο των πραγμάτων ή Ίντερνετ των πραγμάτων (αγγλικά: Internet of things).** Η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό) και η δυνατότητα του χρήστη να τα ελέγχει από έναν υπολογιστή ή κινητό.



Εικόνα 5: Κατηγορίες υλικού IoT

1.1 Σκοπός αυτής της εργασίας

Η συγκεκριμένη εργασία ασχολείται με μεθόδους Μηχανικής Μάθησης για την επίθεση υλικού.

Το κεφάλαιο 2 περιγράφει τις κατηγορίες των απειλών και τα είδη των επιθέσεων στο υλικό.

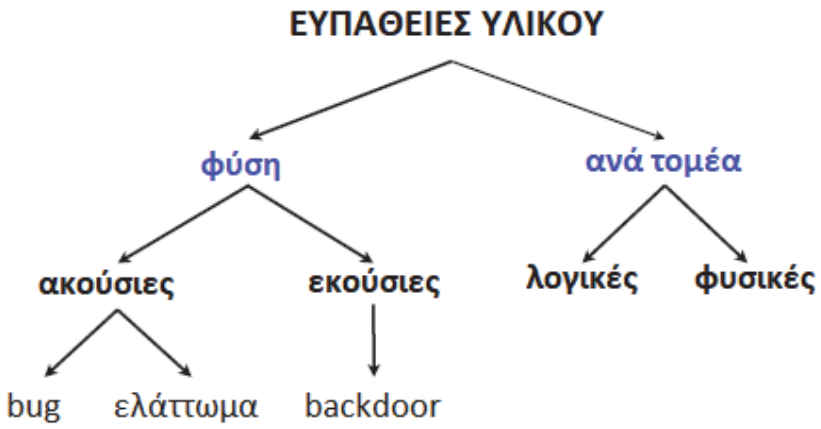
Το κεφάλαιο 3 πραγματεύεται βασικές έννοιες της Μηχανικής Μάθησης και στην συνέχεια αναλύει τις κυριότερες κατηγορίες αλγορίθμων Μηχανικής Μάθησης.

Στο κεφάλαιο 4 αναλύεται η κακόβουλη χρήση της Μηχανικής Μάθησης ήτοι η χρήση της στην πραγματοποίηση επιθέσεων στο υλικό.

2. Ευπάθειες και είδη επιθέσεων στο Υλικό

2.1 Κατηγορίες Ευπάθειας Υλικού

Οι ευπάθειες πρώτα ομαδοποιούνται ανάλογα με τη φύση τους και τον τομέα τους και στη συνέχεια περαιτέρω με διαφορετικά κριτήρια.



Εικόνα 6: Κατηγοριοποίηση ευπαθειών υλικού

Η φύση των ευπαθειών μπορεί να είναι εκούσια ή ακούσια, δηλαδή, η ευπάθεια μπορεί να εισαχθεί στη συσκευή οικειοθελώς ή όχι κατά τη διάρκεια των φάσεων σχεδιασμού και παραγωγής της συσκευής. Οι ακούσιες ευπάθειες διαχωρίζονται περαιτέρω σε σφάλματα (bugs) και ελαττώματα.

Ένα σφάλμα (bug) είναι μια ασυνέπεια μεταξύ μιας προδιαγραφής και της πραγματικής εφαρμογής της, που εισάγεται από λάθος κατά τη διάρκεια μιας συγκεκριμένης φάσης σχεδιασμού που δεν ανιχνεύεται κατά τη διάρκεια της επόμενης φάσης επικύρωσης και επαλήθευσης (Validation & Verification - V&V).

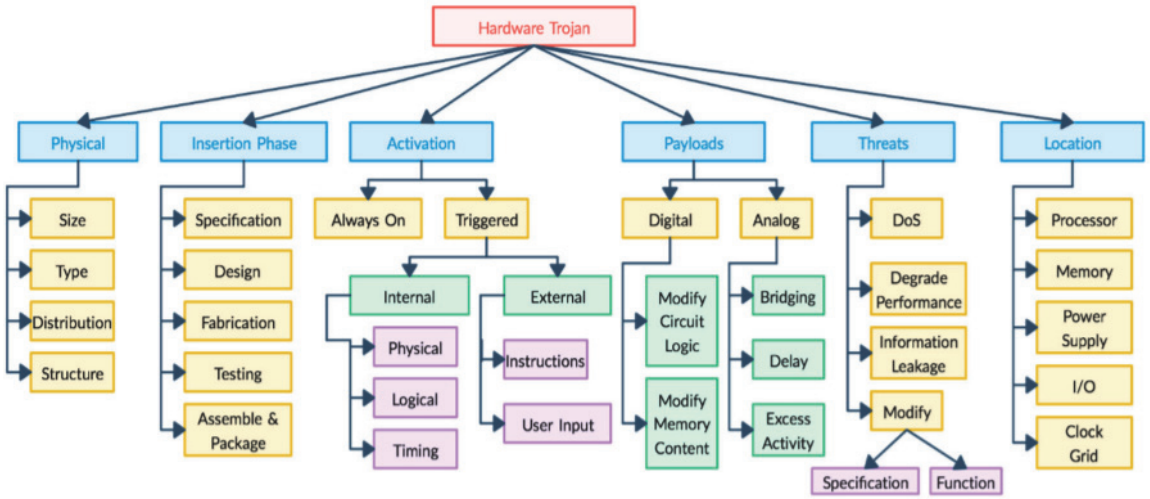
Ένα ελάττωμα είναι, αντίθετα, ένα μη κύριο χαρακτηριστικό που δεν συνιστά ασυνέπεια σε σχέση με τις προδιαγραφές, και αυτό είναι το αποτέλεσμα μιας εσφαλμένης αντίληψης του σχεδιαστή που δεν έλαβε υπόψη την πιθανή επικινδυνότητά του. Ένα ελάττωμα διαφέρει από ένα σφάλμα, επειδή δε συγκρούεται με καμία προδιαγραφή. Για παράδειγμα, στο σχεδιασμό σύγχρονων μικροεπεξεργαστών, η ανάγκη βελτιστοποίησης της απόδοσης μέσω της θεωρητικής (speculative) εκτέλεσης και της επιθετικής χρήσης cache προκάλεσε ελαττώματα όπως τα περίφημα Meltdown και Spectre: τέτοιες ευπάθειες δε δημιουργήθηκαν από λάθος που έκανε ο σχεδιαστής, αλλά εισήχθησαν ακούσια κατά τη φάση βελτιστοποίησης, χωρίς να ληφθούν υπόψη οι κίνδυνοι που θα οδηγούσαν αυτές τις συνθήκες ανταγωνισμού. Το meltdown εκμεταλλεύεται τις συνέπειες της μη σειριακής εκτέλεσης εντολών σε σύγχρονους επεξεργαστές για να διαβάσει αυθαίρετες θέσεις μνήμης πυρήνα, συμπεριλαμβανομένων προσωπικών δεδομένων και κωδικών πρόσβασης. Η μη σειριακή εκτέλεση εντολών είναι απαραίτητο χαρακτηριστικό βελτίωσης της απόδοσης και

υπάρχει σε πολλούς σύγχρονους επεξεργαστές. Η συγκεκριμένη επίθεση είναι ανεξάρτητη από το λειτουργικό σύστημα και δεν βασίζεται σε ευπάθειες λογισμικού. Το meltdown παραβιάζει όλες τις εγγυήσεις ασφάλειας που παρέχονται από την απομόνωση του χώρου διευθύνσεων, καθώς και από τα παρα-εικονικοποιημένα περιβάλλοντα και, επομένως, παραβιάζει κάθε μηχανισμό ασφαλείας που βασίζεται σε αυτό το πλαίσιο. Ως προς τα συστήματα που επηρεάζονται, το meltdown επιτρέπει στον "εχθρό" να διαβάζει τη μνήμη άλλων διεργασιών ή εικονικών μηχανών στο cloud χωρίς να έχει τα αντίστοιχα δικαιώματα ή πρόσβαση, επηρεάζοντας εκατομμύρια πελάτες και σχεδόν κάθε χρήστη κάτοχο ενός προσωπικού υπολογιστή. Το Spectre από την άλλη πλευρά, είναι μια ευπάθεια που επηρεάζει τους σύγχρονους μικροεπεξεργαστές που εκτελούν πρόβλεψη branch. Στους περισσότερους επεξεργαστές, η θεωρητική (speculative) εκτέλεση που προκύπτει από εσφαλμένη πρόβλεψη κλάδου μπορεί να αφήσει παρατηρήσιμες παρενέργειες που μπορεί να αποκαλύψουν ιδιωτικά δεδομένα σε εισβολείς. Για παράδειγμα, εάν το μοτίβο των προσβάσεων στη μνήμη που εκτελείται από θεωρητική (speculative) εκτέλεση εξαρτάται από ιδιωτικά δεδομένα, η προκύπτουσα κατάσταση της προσωρινής μνήμης δεδομένων αποτελεί ένα πλευρικό κανάλι μέσω του οποίου ένας εισβολέας μπορεί να μπορεί να εξαγάγει πληροφορίες σχετικά με τα ιδιωτικά δεδομένα χρησιμοποιώντας μια επίθεση χρονισμού, η οποία θα αναλυθεί παρακάτω εκτενέστερα, [39], [40].

Μια ευπάθεια που εισάγεται σκόπιμα μέσα στο υλικό μιας συσκευής μπορεί να αναφέρεται ως backdoor (κερκόπορτα), καθώς το άτομο που την εισάγει θέλει να εγγυηθεί στον εαυτό του (ή σε κάποιον άλλο) την πιθανότητα μεταγενέστερης πρόσβασης ή κατάχρησης εκτός του συνόλου των προβλεπόμενων περιπτώσεων χρήσης. Αξίζει να σημειωθεί ότι η παρουσία ενός backdoor εκθέτει το υλικό σε απειλές ανεξάρτητα από το γεγονός ότι εισήχθη κακόβουλα ή όχι. Από τη μία πλευρά, ένα παράδειγμα κακόβουλου backdoor είναι ένας trojan υλικού, δηλαδή ένα "κρυφό" κομμάτι κυκλώματος που έχει εισαχθεί σε ένα δεδομένο σημείο των φάσεων σχεδιασμού και παραγωγής, το οποίο μπορεί να εκτελέσει μη εξουσιοδοτημένες ενέργειες όταν οι συνθήκες "ενεργοποίησης" ικανοποιούνται. Είναι γεγονός, ότι με την παγκοσμιοποίηση του σχεδιασμού και της κατασκευής ολοκληρωμένων κυκλωμάτων, η εξωτερική ανάθεση εργασιών παραγωγής έχει γίνει ένας κοινός τρόπος για τη μείωση του κόστους του προϊόντος. Οι συσκευές με ενσωματωμένο υλικό δεν παράγονται πάντα από τις εταιρείες που τις σχεδιάζουν και τις πωλούν, ακόμη και ούτε στην ίδια χώρα όπου θα χρησιμοποιηθούν. Ένας κακόβουλος εισβολέας με πρόσβαση στη διαδικασία κατασκευής μπορεί να εισαγάγει ορισμένες αλλαγές στο τελικό προϊόν.

Οι Δούρειοι Ίπποι υλικού (Hardware Trojans - HTs) μπορούν να τοποθετηθούν σε τμήματα ενός κυκλώματος με αδυναμία ασφάλειας με διάφορα μέσα για να υποκλαπούν τα εσωτερικά ευαίσθητα δεδομένα ή να τροποποιηθεί η αρχική λειτουργικότητα, η οποία μπορεί να οδηγήσει σε τεράστιες οικονομικές απώλειες και μεγάλη ζημιά στην κοινωνία. Επομένως, είναι πολύ σημαντικό να εκτελεστεί ανίχνευση και διάγνωση των HTs, να εντοπιστούν πιθανοί κίνδυνοι

ασφάλειας και να εφαρμοστούν τεχνικές προστασίας σε ολόκληρο τον κύκλο σχεδιασμού του IC, προκειμένου να βελτιωθεί η ασφάλεια των κυκλωμάτων. Το [4], επεξεργάζεται ένα μοντέλο IC που κυκλοφορεί στην αγορά και περιγράφονται οι πιθανές απειλές από HTs που αντιμετωπίζουν τα μέρη που εμπλέκονται στο μοντέλο. Στη συνέχεια, εξετάζονται οι πρόσφατες εξελίξεις της έρευνας στα αντίμετρα κατά των επιθέσεων HTs, οι οποίες κατηγοριοποιούνται σε ανίχνευση, διάγνωση και πρόληψη από HTs. Τέλος, αναδεικνύονται οι προκλήσεις και οι προοπτικές για την άμυνα απέναντι σε HTs, [3].



Εικόνα 7: Κατηγορίες Trojan Horses

Ένας trojan υλικού χαρακτηρίζεται από ένα ωφέλιμο φορτίο, δηλαδή ολόκληρη τη δραστηριότητα που εκτελεί ο trojan όταν είναι ενεργοποιημένος, και από ένα trigger που είναι η συνθήκη που επαληθεύεται στην κατάσταση του κυκλώματος που ενεργοποιεί το ωφέλιμο φορτίο. Σε γενικές γραμμές, οι κακόβουλοι trojan προσπαθούν να παρακάμψουν ή να απενεργοποιήσουν το τείχος προστασίας ενός συστήματος, μπορούν να διαρρεύσουν εμπιστευτικές πληροφορίες μέσω ραδιοεκπομπής ή μέσω άλλου σήματος πλευρικού καναλιού. Ένας trojan μπορεί επίσης να χρησιμοποιηθεί για να απενεργοποιήσει, να αποσυντονίσει ή να καταστρέψει ολόκληρο το κύκλωμα ή τα συστατικά του. Ένας trojan μπορεί να εισαχθεί κατά τη διάρκεια οποιουδήποτε σταδίου παραγωγής (σχεδιασμός, κατασκευή, δοκιμή, συναρμολόγηση) και σε οποιοδήποτε επίπεδο (επίπεδο εγγραφής - μεταφοράς, επίπεδο πύλης, επίπεδο τρανζίστορ και ακόμη και στο φυσικό επίπεδο).

Από την άλλη πλευρά, ένα παράδειγμα μη κακόβουλων backdoors παρέχεται από τις μη καταγεγραμμένες εντολές ορισμένων επεξεργαστών που ανήκουν στην οικογένεια x86, όπως: το μη καταγεγραμμένο opcode ALTINST (0x0F3F), πιθανότατα αρχικά εισήχθη από το σχεδιαστές για σκοπούς εντοπισμού σφαλμάτων, επιτρέπει στο χρήστη να μεταβεί σε μια εναλλακτική αρχιτεκτονική συνόλου εντολών (Instruction Set Architecture - ISA), πιο κοντά στην πραγματική

εσωτερική αρχιτεκτονική RISC και μπορεί να χρησιμοποιηθεί κακόβουλα για να προκαλέσει μια επίθεση επέκτασης προνομίων.

Εκτός από το κριτήριο της φύσης, μια ευπάθεια υλικού ανήκει σε έναν τομέα, είτε λογικό είτε φυσικό. Μια ευπάθεια υλικού είναι λογική όταν έχει εισαχθεί κατά τις πρώτες φάσεις σχεδιασμού της συσκευής, ενώ είναι φυσική όταν σχετίζεται με ευπάθειες που παρουσιάζονται κατά τη διάρκεια των τελευταίων βημάτων της διαδικασίας σχεδιασμού.

Ένα τυπικό παράδειγμα προέρχεται από το γεγονός ότι μια σειρά διαδοχικών εγγραφών σε ένα κελί μνήμης DRAM μπορεί να προκαλέσει γειτονικά κελιά να αναστρέψουν το περιεχόμενό τους, λόγω των επιπτώσεων ηλεκτρικής διαρροής. Μια τέτοια ευπάθεια είναι στην πραγματικότητα άμεσα συσχετιζόμενη με την τεχνολογία που υιοθετήθηκε για την εφαρμογή της μνήμης, ακόμη και αν μια ακριβής ανάλυση των γνωστών αλληλένδετων σφαλμάτων στη DRAM θα μπορούσε να προτείνει την κατάλληλη λύση κατά τη διάρκεια του σχεδιασμού, [38].

2.2 Επιθέσεις στο Generic Υλικό

Επίθεση είναι η εκμετάλλευση μιας ευπάθειας.

Εικόνα 8: Κατηγοριοποίηση επιθέσεων υλικού

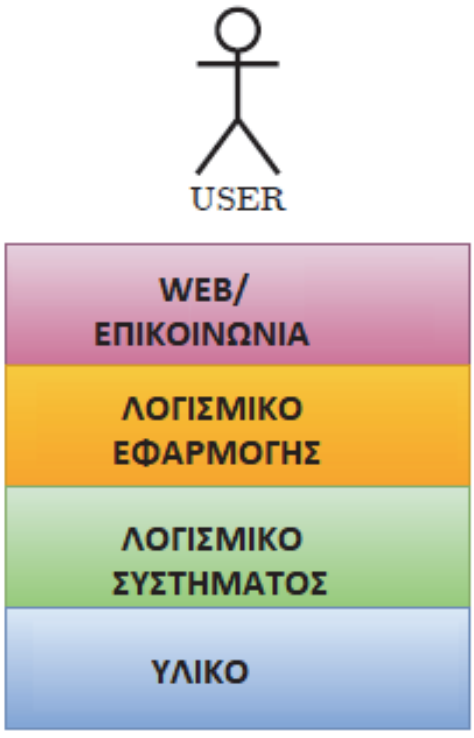
Μια επίθεση υλικού κατηγοριοποιείται αρχικά από το σκοπό για τον οποίο ξεκινά. Ο στόχος είναι η κακόβουλη ενέργεια στην οποία θέλει να προβεί ο εισβολέας εναντίον ενός στοιχείου του επιτιθέμενου υλικού, που ορίζεται ως στόχος. Ο στόχος μπορεί να είναι οι πληροφορίες που χειρίζεται το υλικό, αλλά και μια ιδιότητα του ίδιου του υλικού, είτε λειτουργική είτε μη λειτουργική. Κάποιος μπορεί να ξεκινήσει μια επίθεση για να:

- Κλέψει ένα στόχο (π.χ. ένα κρυπτογραφικό κλειδί, έναν μυστικό κωδικό πρόσβασης, μια πνευματική ιδιοκτησία, έναν πόρο κ.λπ.): Αναφερόμενοι στην τριάδα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας (Confidentiality – Integrity – Availability, CIA), η κλοπή είναι μια ενέργεια που πραγματοποιείται για παραβίαση της εμπιστευτικότητας, καθώς ο εισβολέας αποκτά ένα στοιχείο του οποίου δεν κατέχει τα δικαιώματα πρόσβασης ή χρήσης. Αξίζει να σημειωθεί ότι η λεγόμενη κλοπή πνευματικής ιδιοκτησίας (Intellectual Property -

IP) πρέπει να θεωρηθεί ως περίπτωση επίθεσης IP-πειρατείας και απαιτούνται σχετικές λύσεις για την ασφάλεια υλικού. Η πνευματική ιδιοκτησία είναι στην πραγματικότητα ένας πλήρης στόχος, και ως εκ τούτου θα πρέπει να προστατεύεται ακριβώς όπως κάθε άλλο στοιχείο υλικού.

- Φθείρει έναν στόχο (π.χ. μια λέξη μνήμης, ένα αρχείο άδειας, μια λειτουργικότητα για να την εκμεταλλευτεί κάποιος κ.λπ.): Η φθορά είναι μια ενέργεια που πραγματοποιείται για παραβίαση της ακεραιότητας, καθώς ο εισβολέας τροποποιεί ένα στοιχείο χωρίς να έχει εξουσιοδότηση να το κάνει.
- Αναστείλει ένα στόχο (π.χ. υπηρεσία, σύνολο κρίσιμων δεδομένων, μηχανισμός άμυνας κ.λπ.): Η αναστολή είναι μια ενέργεια που πραγματοποιείται για παραβίαση της διαθεσιμότητας, καθώς ο εισβολέας εμποδίζει την ορθή πρόσβαση ή χρήση ενός στοιχείου από εκείνους που έχουν δικαίωμα να το κάνουν.

Εκτός από τις ευπάθειες, οι επιθέσεις υλικού έχουν πάντα έναν τομέα στον οποίο υλοποιούνται. Μια επίθεση ανήκει στον λογικό τομέα εάν πραγματοποιείται ξεκινώντας από τα ανώτερα επίπεδα σε σχέση με το υλικό π.χ. όταν μια ευπάθεια υλικού, λογική ή φυσική, αξιοποιείται με ενέργειες όχι απευθείας στο ίδιο το υλικό, αλλά σε επίπεδα λογισμικού που τρέχουν πάνω του. Αυτός ο τομέας περιλαμβάνει, για παράδειγμα, επιθέσεις κλιμάκωσης προνομίων που εκμεταλλεύονται την ευπάθεια rowhammer ή εκείνες που εκμεταλλεύονται ευπάθειες στη μικροαρχιτεκτονική του επεξεργαστή όπως η Meltdown, η Spectre ή άλλες, καθώς και επιθέσεις στην κρυφή μνήμη, [38].



Εικόνα 9: Επιπεδοποίηση υπολογιστικού συστήματος

Αντίθετα, μια επίθεση ανήκει στον φυσικό τομέα εάν πραγματοποιείται μέσω ενεργειών που εκτελούνται απευθείας στη συσκευή υλικού που δέχτηκε επίθεση.

Τέλος, μια επίθεση υλικού προσδιορίζεται ανάλογα με τον τρόπο με τον οποίο πραγματοποιείται. Η επίθεση είναι επεμβατική όταν οι ενέργειες που έγιναν εναντίον του επιτιθέμενου υλικού περιλαμβάνουν φυσικές εισβολές, όπως αποκόλληση, αποσυμπίεση, αποσύνδεση των εσωτερικών του στοιχείων. Οι επιθέσεις που έχουν αυτήν τη δυνατότητα είναι, για παράδειγμα, [38]:

- **Επιθέσεις microprobing:** Μια επίθεση microprobing προσπαθεί να εξαγάγει πληροφορίες μετρώντας ηλεκτρικές ποσότητες απευθείας στην πλακέτα πυριτίου της συσκευής στόχου, μόλις αποκτήσει φυσική πρόσβαση σε αυτήν. Η έκθεση της πλακέτας επιτυγχάνεται συνήθως με την αφαίρεση των πλαστικών συσκευασιών μέσω χημικής χάραξης ή/ και με μηχανικές προσεγγίσεις. Όταν είναι δυνατόν, οι επιτιθέμενοι μελετούν τη λίστα δικτύου του στόχου πριν από την επίθεση, έτσι ώστε με αντίστροφη μηχανική να είναι σε θέση να βρουν ταιριάσματα με τη διάταξη αυτή για να εντοπίσουν τη σύνδεση που μεταφέρει ευαίσθητα δεδομένα. Σε αυτό το σημείο, χάρη στον προηγμένο εξοπλισμό ως γεννήτριες Focused Ion Beam (FIB), μπορούν να φράξουν τα καλώδια με νανομετρική ακρίβεια ή να δημιουργήσουν αγώγιμες διαδρομές που χρησιμεύουν ως επαφή ηλεκτρικού δοκιμαστή. Στη συνέχεια χρησιμοποιείται ένας εξοπλισμός ανιχνευτή για την ανάγνωση των σημάτων-στόχων και την εξαγωγή πληροφοριών. Ένας τέτοιος εξελιγμένος εξοπλισμός φαίνεται δύσκολο να διατεθεί, αλλά για παράδειγμα μια γεννήτρια FIB μπορεί να ενοικιαστεί με μόλις μερικές εκατοντάδες δολάρια την ώρα, κάτι που είναι μικρό σαν ποσό σε σχέση με κλοπή πληροφοριών που θα μπορούσε να είναι αποφέρει πολύ μεγαλύτερα ποσά.

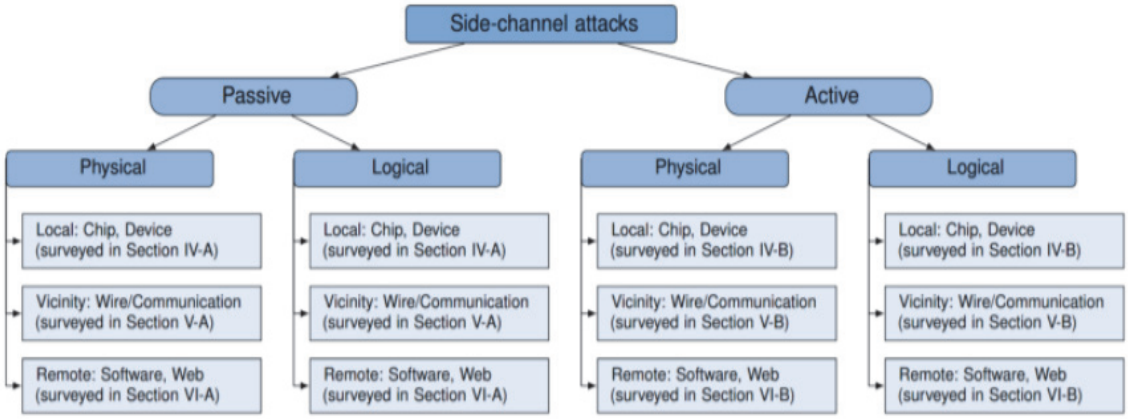
- **Επιθέσεις αντίστροφης μηχανικής:** Μια επίθεση της αντίστροφης μηχανικής είναι παρόμοια με το microprobing σε σχέση με τη φάση συναρμολόγησης (αποσυγκόλληση και αποθυλάκωση), αλλά στην πραγματικότητα έχει διαφορετικό πεδίο εφαρμογής. Στην πραγματικότητα στοχεύει στην κατανόηση της δομής μιας συσκευής ημιαγωγών και των λειτουργιών της, δηλαδή στην κλοπή των πνευματικών ιδιοτήτων του σχεδιαστή. Προφανώς απαιτείται βαθιά γνώση και εξειδίκευση στον προηγμένο σχεδιασμό ολοκληρωμένων κυκλωμάτων. Όλα τα επίπεδα που σχηματίζονται κατά την κατασκευή του κυκλώματος αφαιρούνται ένα προς ένα σε αντίστροφη σειρά και φωτογραφίζονται για να προσδιοριστεί η εσωτερική δομή του κυκλώματος. Στο τέλος, με την επεξεργασία όλων των αποκτηθέντων πληροφοριών, ένα τυπικό αρχείο λίστας δικτύου μπορεί να δημιουργηθεί και να χρησιμοποιηθεί για την προσομοίωση και τελικά τον επανασχεδιασμό της συσκευής προορισμού.

- **Επιθέσεις διατήρησης δεδομένων:** Οι υπολογιστές συνήθως αποθηκεύουν μυστικά δεδομένα στην DRAM, τα οποία δεν προστατεύονται (λόγω της τάσης) όταν παραβιάζεται η

συσκευή. Είναι σύνηθες το σκεπτικό ότι όταν η ισχύς έχει πέσει κάτω από το κανονικό επίπεδο, το περιεχόμενο των πτητικών μνημών διαγράφεται (γι' αυτό ονομάζονται πτητικές). Ωστόσο, έχει αποδειχθεί ότι το φορτίο που είναι αποθηκευμένο σε ένα κελί DRAM έχει δεδομένο ρυθμό αποσύνθεσης που δεν είναι σταθερός και εξαρτάται αυστηρά από τη θερμοκρασία. Σε θερμοκρασίες από −50◦C και κάτω, το περιεχόμενο των RAM μπορεί να "παγώσει" και να διατηρηθεί για μία ή ακόμα και περισσότερες ημέρες. Αυτό συμβαίνει συνήθως σε μια επίθεση ψυχρής εκκίνησης, στην οποία ο χάκερ χρησιμοποιεί δοχεία ψεκασμού ή υγρό άζωτο σε μια πτητική συσκευή που μόλις αποσυνδέθηκε από το αρχικό σύστημα και κερδίζει πολύτιμο χρόνο για να εκτελέσει μια αντιγραφή της μνήμης, δηλαδή, αντίγραφο των περιεχομένων σε μη πτητική συσκευή για μετέπειτα ανάλυση. Η διατήρηση δεδομένων επηρεάζει με διαφορετικό τρόπο μη πτητικούς τύπους μνήμης όπως το EEPROM και το Flash. Ορισμένες λογικές πληροφορίες που πιστεύεται ότι έχουν διαγραφεί μπορούν να εξαχθούν.

Η επίθεση είναι αντίθετα μη επεμβατική όταν μπορεί να πραγματοποιηθεί χωρίς φυσική επαφή με τη συσκευή που δέχεται επίθεση. Οι μη επεμβατικές επιθέσεις χωρίζονται περαιτέρω σε παθητικές και ενεργητικές. Οι παθητικές μη επεμβατικές επιθέσεις πραγματοποιούνται με ανάλυση και μέτρηση μίας (ή περισσότερων) φυσικών δυναμικών οντοτήτων του επιτιθέμενου υλικού. Όλοι οι διαφορετικοί τύποι επιθέσεων πλευρικού καναλιού ανήκουν σε αυτήν την κατηγορία. Οι ενεργητικές μη επεμβατικές επιθέσεις απαιτούν, αντίθετα, συγκεκριμένες ενέργειες στη συσκευή, με σκοπό να αναγκάσουν το σύστημα να μεταβεί σε μη ομαλές καταστάσεις στις οποίες ο στόχος είναι ευκολότερος. Αυτή η κατηγορία περιλαμβάνει όλους τους διαφορετικούς τύπους επιθέσεων σφαλμάτων και επιθέσεις βάσει δοκιμής-υποδομής.

Επιθέσεις πλευρικού καναλιού: Όντας κάτι με φυσική συνοχή, όταν είναι σε δραστηριότητα, το υλικό απελευθερώνει ακούσια στο περιβάλλον έναν ορισμένο αριθμό "ενδείξεων", όπως χρόνος λειτουργίας, καταναλωμένη ενέργεια, απελευθερούμενη ηλεκτρομαγνητική ακτινοβολία, θόρυβος κ.λπ. Αυτά τα στοιχεία, μαζί με τη γνώση ορισμένων λεπτομερειών σχετικά με τη δομή της συσκευής ή για τους αλγόριθμους που εκτελέστηκαν, μπορεί να αποδειχθούν κρίσιμα για την προστασία των πληροφοριών.



Εικόνα 10: Κατηγοριοποίηση επιθέσεων πλευρικού καναλιού

Οι πιο γνωστές κατηγορίες επιθέσεων πλευρικού καναλιού είναι, [38]:

- **Επιθέσεις χρονισμού:** Μια επίθεση χρονισμού πλευρικού καναλιού προσπαθεί να ανακτήσει ευαίσθητα δεδομένα μετρώντας τον χρόνο υπολογισμού τους σε ένα κομμάτι υλικού. Στις περισσότερες περιπτώσεις, η εφαρμογή του αλγορίθμου εξαρτάται σε μεγάλο βαθμό από τις πραγματικές τιμές της εισόδου του. Αν ένας εισβολέας γνωρίζει αυτή τη συσχέτιση, μπορεί να εξαγάγει, για παράδειγμα, το κλειδί κρυπτογράφησης ή τον κωδικό πρόσβασης που υποβάλλεται σε επεξεργασία.

- **Επιθέσεις ισχύος:** Η πραγματική κατανάλωση ενέργειας μιας προγραμματιζόμενης συσκευής εξαρτάται τόσο από τις εκτελεσθείσες εντολές όσο και από τα επεξεργασμένα δεδομένα. Μια επίθεση ισχύος πλευρικού καναλιού προσπαθεί να διαβάσει αντίστροφα αυτήν τη διαδικασία και να ανακτήσει ευαίσθητα δεδομένα που επεξεργάστηκαν, μετρώντας τη διακύμανση της κατανάλωσης ισχύος της συσκευής υλικού.

- **Επιθέσεις ηλεκτρομαγνητικής ακτινοβολίας:** Όποτε διαρρέεται ρεύμα, δημιουργείται ένα ηλεκτρομαγνητικό πεδίο γύρω από αυτό. Αυτή η ακτινοβολία μεταφέρει ακούσια πληροφορίες σχετικά με την πηγή και καταφεύγοντας σε κατάλληλες συσκευές λήψης, όπως ένα επαγωγικό πηνίο, που βρίσκεται κοντά στην συσκευή, μπορεί κανείς να ανακατασκευάσει το ψηφιακό σήμα από το οποίο προήλθε.

- **Ακουστικές επιθέσεις:** Η ακουστική κρυπτοανάλυση εκμεταλλεύεται τους κραδασμούς που παράγονται από στοιχεία υλικού κάθε είδους και σε οποιοδήποτε επίπεδο, από το επίπεδο της συσκευής μέχρι το επίπεδο κυκλώματος. Μπορούν να τοποθετηθούν κρυφές συσκευές ακρόασης από εισβολείς για να καταγράψουν τον ήχο που εκπέμπεται από πληκτρολόγια, και στη συνέχεια, μια σημαντική ποσότητα ανιχνεύσιμων δεδομένων μπορεί να υποβληθεί σε επεξεργασία με ανάλυση σήματος ή / και αλγόριθμους μηχανικής μάθησης για να συσχετίσει

ένα συγκεκριμένο ηχητικό κύμα με το πατημένο πλήκτρο. Οι ακουστικές εκπομπές στην υπερηχητική ζώνη εμφανίζονται σε στοιχεία κυκλώματος π.χ. σε πηνία και πυκνωτές ως συνέπεια του ρεύματος που διέρχεται μέσω αυτών. Τα κυκλώματα ρύθμισης τάσης στις μητρικές πλακέτες του υπολογιστή είναι υπεύθυνα για την ακουστική εκπομπή που σχετίζεται άμεσα με τη δραστηριότητα της CPU.

- **Οπτικές επιθέσεις:** Εκτός από τη διαρροή ρεύματος ή την εκπομπή ακτινοβολίας, ένα τρανζίστορ που επαναλειτουργεί επίσης εκπέμπει λίγο φως με τη μορφή μερικών φωτονίων για πολύ μικρό χρονικό διάστημα. Εάν ένας εισβολέας είναι σε θέση να εντοπίσει μια τέτοια εκπομπή, μπορεί να επεξεργαστεί λογικές πληροφορίες από το κύκλωμα. Εναλλακτικά, οι εκπομπές φωτός που μεταφέρουν πληροφορίες μπορούν επίσης να αξιοποιηθούν όταν τα LED χρησιμοποιούνται ως δείκτες δραστηριότητας συσκευής.

Επιθέσεις σφαλμάτων: Συνίστανται στην έγχυση εσκεμμένων (κακόβουλων) σφαλμάτων στη συσκευή προορισμού, με στόχο να την φέρουν σε ένα σύνολο καταστάσεων από τις οποίες μπορούν να εξαχθούν ψευδώς εσωτερικά στοιχεία πληροφοριών. Οι τύποι επιθέσεων σφαλμάτων ομαδοποιούνται κυρίως σύμφωνα με τις τεχνικές έγχυσης σφαλμάτων. Οι πιο σχετικές είναι, [38]:

- **Επιθέσεις τροφοδοσίας ισχύος:** Εάν ένας εισβολέας είναι σε θέση να εισχωρήσει στη γραμμή τροφοδοσίας ισχύος της συσκευής προορισμού και να συνδέσει τη μονάδα ισχύος του, μπορεί να χαμηλώσει την ισχύ στη συσκευή. Εάν η ισχύς είναι χαμηλότερη, η καθυστέρηση των λογικών πυλών αυξάνεται και στην περίπτωση κρίσιμων διαδρομών μπορεί να συμβεί δειγματοληψία λανθασμένων τιμών. Αυτό σημαίνει πρακτικά ότι ένα, ή περισσότερα, ελαττωματικά bits, εγχέονται στο σύστημα. Από την άλλη πλευρά, εάν ένα κύκλωμα αποκτήσει περισσότερη ισχύ απ' ό,τι χρειάζεται, μπορούν να πραγματοποιηθούν επιβλαβείς ενέργειες.

- **Επιθέσεις ρολογιού:** Η διάρκεια ενός μόνο κύκλου μπορεί να μειωθεί με την επιβολή μιας πρόωρης εναλλαγής του σήματος ρολογιού. Με αυτόν τον τρόπο, τα καταχωρημένα byte μπορούν να καταστραφούν. Για να αλλάξει η διάρκεια του κύκλου ρολογιού, ο εισβολέας πρέπει να πάρει άμεσο έλεγχο της γραμμής ρολογιού, γεγονός που συμβαίνει συνήθως όταν στοχεύονται οι έξυπνες κάρτες. Καθώς μια μη προγραμματισμένη εναλλαγή ρολογιού εισάγει δυσλειτουργία (glitch) στα εσωτερικά σήματα, αυτές οι επιθέσεις είναι επίσης γνωστές ως Glitch Attacks.

- **Επιθέσεις έκθεσης σε αύξηση θερμοκρασίας:** Η αύξηση της θερμοκρασίας στο περιβάλλον στο οποίο λειτουργεί η συσκευή-στόχος μπορεί να αξιοποιηθεί για να χρησιμοποιηθεί σε κάποια επίθεση. Τα ηλεκτρόνια μέσα στα τρανζίστορ διεγείρονται από τη γύρω θερμότητα και παράγονται τυχαία ρεύματα, τα οποία μπορεί να οδηγήσουν σε εναλλαγές bits (τόσο σε κελιά μνήμης SRAM εντός των επεξεργαστών όσο και σε κελιά μνήμης DRAM) ή ακόμη και

στην επιτάχυνση της γήρανσης του κυκλώματος, με την ακραία συνέπεια της καταστροφής του όταν η υπερθέρμανση φτάσει σε ένα δεδομένο κατώφλι.

- **Επιθέσεις έκθεσης σε ακτινοβολία:** Ένας πρακτικός τρόπος για την πρόκληση βλαβών χωρίς να χρειάζεται να εισχωρήσει ο εισβολέας στη συσκευή είναι να προκαλέσει ισχυρές ηλεκτρομαγνητικές διαταραχές κοντά σε αυτήν. Τα κυμαινόμενα ρεύματα που προκαλούνται στο κύκλωμα από ισχυρούς ηλεκτρομαγνητικούς παλμούς προκαλούν προσωρινές μεταβολές του επιπέδου ενός σήματος, οι οποίες μπορεί, για παράδειγμα, να καταγράφονται από ένα κύκλωμα latch ή ένα flip - flop. Όταν η διαταραχή γίνεται όλο και μεγαλύτερη, τα εξαρτήματα της συσκευής ενδέχεται να σταματήσουν να λειτουργούν ή ακόμη και να καταστραφούν.

Επιθέσεις βάσει δοκιμής-υποδομής: Οι σχεδιαστές υλικού βασίζονται συστηματικά στις μεθοδολογίες Σχεδιασμού για Δοκιμές και Χτίσιμο με Ατομικά Τεστ (Design-for-Testability και Built-in Self Test - BIST) για να βελτιώσουν τη δυνατότητα δοκιμής του συστήματος-στόχου τόσο στο τελικό στάδιο της παραγωγής όσο και στο πεδίο λειτουργίας. Ορισμένες από αυτές τις μεθοδολογίες υιοθετούνται ευρέως ώστε να γίνουν πρότυπα, π.χ. το IEEE 1149.1 (γνωστό και ως Boundary Scan) και το IEEE 1500. Δυστυχώς, αυτές οι υποδομές δοκιμών, υποχρεωτικές για την επίτευξη των επιθυμητών επιπέδων δοκιμής από άποψη κόστους, στις περισσότερες περιπτώσεις δημιουργούν σοβαρούς κινδύνους ασφαλείας. Για παράδειγμα, όταν οι καρφίτσες μιας τυπικής διεπαφής 1149.1 αφήνονται προσβάσιμες προς τα έξω, ένας πιθανός εισβολέας μπορεί εύκολα να εκμεταλλευτεί την αλυσίδα σάρωσης για να αποθηκεύσει τα δεδομένα στα συνδεδεμένα αρχεία. Μόλις γίνει γνωστή η θέση των στοιχείων στόχου (π.χ. καταχωρητές που περιέχουν μυστικά κλειδιά) μέσα στην αλυσίδα, η επίθεση επιτυγχάνεται πολύ εύκολα, [38].

2.2.1 Ανάγκη για ασφάλεια στο generic υλικό – προτεινόμενες λύσεις

Τα τελευταία χρόνια, έχουν προταθεί διάφορες τεχνικές για την ασφάλεια του υλικού, όπως οι Φυσικές Μη Κλωνοποιήσιμες Συναρτήσεις (Physically Unclonable Functions - PUFs) και οι Γεννήτριες Πραγματικά Τυχαίων Αριθμών (True Random Number Generators - TRNGs), Ενδεικτικά, έχουν πραγματοποιηθεί οι παρακάτω μελέτες [41]:

- **Κατασκευή PUF και βελτιστοποίηση υλικών:** Έχουν αναπτυχθεί μοντέλα για τη βελτίωση της τυχαίας τάσης κατωφλίου τρανζίστορ και της αποτελεσματικής κινητικότητας σε επίπεδο υλικών συσκευής, χρησιμοποιώντας το poly-Si ως υλικό υποστρώματος. Όλες οι προσεγγίσεις είναι συμβατές με την επεξεργασία CMOS και μπορούν να εκτελεστούν επιλεκτικά σε περιοχές που σχετίζονται με το PUF.

- **Ενσωματωμένη εγγραφή και αξιοπιστία PUF βασισμένη στη μνήμη:** Οι PUF που βασίζονται στην εγγενή μνήμη έχουν το πλεονέκτημα ότι περιέχονται ήδη σε ένα σύστημα ή σε ένα σύστημα-σε-τσιπ (System-On-Chip - SoC). Τα αποτελέσματα δείχνουν σημαντικές

βελτιώσεις στην αξιοπιστία SRAM, Flash και DRAM PUF σε ακραίες διακυμάνσεις τάσης, μεταβολές θερμοκρασίας και τη γήρανση.

- **Εφαρμόσιμο PUF αναλογικού/ μικτού σήματος (Mixed Signal - AMS):** Έχουν σχεδιαστεί αδύναμα PUF που χρησιμοποιούν δυναμικούς latch συγκριτές και τάσεις αντιστάθμισης τυχαίας εισόδου για τη δημιουργία ενός αναγνωριστικού ειδικά για τσιπ. Οι μετρήσεις δείχνουν ότι το PUF επιτυγχάνει καλή μοναδικότητα και αξιοπιστία σε ένα ευρύ φάσμα θερμοκρασιών και τάσεων και με αποτύπωμα χαμηλής περιοχής.
- **Ανθεκτική στη γήρανση RO-PUF:** Η πλειονότητα των υπαρχόντων εργασιών εστιάζει στη βελτίωση της αντοχής PUF έναντι θορύβου και θερμοκρασίας τροφοδοσίας τάσης. Οι αλγόριθμοι επιλογής ζευγών καθορίζουν τις καλύτερες RO για χρήση στο PUF με τη χαμηλότερη ευαισθησία στον θόρυβο και την καλύτερη μακροπρόθεσμη αξιοπιστία.
- **Ανεξάρτητη τεχνολογία TRNG:** Τα TRNG βασίζονται σε μεγάλο βαθμό σε τυχαία φυσικά φαινόμενα όπως θερμικός θόρυβος, θόρυβος λήψης, ρολόι κλπ. για τη δημιουργία τυχαίων αριθμών. Έχουν προταθεί βελτιωμένα σχέδια TRNG που ενισχύουν τον τυχαίο θόρυβο για να επιτύχουν καλύτερη απόδοση TRNG σε παλαιότερες τεχνολογίες.
- **TRNG Attack Detection and Response:** Τα bitstreams που παρέχονται από το TRNG μπορούν να γίνουν λιγότερο τυχαία (πιο προβλέψιμα) σε ορισμένες τάσεις/ θερμοκρασίες και με την πάροδο του χρόνου (λόγω γήρανσης). Έχουν αναπτυχθεί τεχνικές που εντοπίζουν τις προτιμήσεις σε ένα TRNG που θα μπορούσαν να προκληθούν σε επιθέσεις και από γήρανση. Όποτε εντοπίζονται αυτές οι προτιμήσεις, ενεργοποιούνται μηχανισμοί αντιστάθμισης για να κάνουν την έξοδο του TRNG ομοιόμορφη και πάλι τυχαία.

2.3 Επιθέσεις στο Internet of Things

Όπως αναφέρθηκε και πιο πάνω, τα τελευταία χρόνια, η εμφάνιση των επικοινωνιών μηχανή προς μηχανή (Machine to Machine – M2M) οδήγησε σε προβλέψεις που μιλούν για δισεκατομμύρια συσκευές συνδεδεμένες στο Διαδίκτυο των πραγμάτων. Τα κύρια χαρακτηριστικά που λαμβάνονται υπόψη κατά την ανάπτυξη νέων προϊόντων για αυτόν τον τομέα, δηλαδή η λειτουργικότητα, το κόστος και η κατανάλωση ενέργειας, έχουν υποβαθμιστεί από πλευράς σημασίας σε σχέση με τη συνδεσιμότητα και την ασφάλεια: η μελλοντική ανάπτυξη του IoT μπορεί να τεθεί σε κίνδυνο αν οι κίνδυνοι ασφάλειας δεν αντιμετωπιστούν. Στην πραγματικότητα, σε πρόσφατες έρευνες που διεξήχθησαν από την IEEE IoT Initiative, το θέμα της ασφάλειας αναγνωρίστηκε ως η πρώτη ανησυχία μεταξύ των προγραμματιστών για το IoT. Πράγματι, η έλλειψη ασφάλειας μπορεί να επιφέρει κρυφές δαπάνες που πρέπει να αντιμετωπίσουν οι επιχειρήσεις τεχνολογίας και λογισμικού.

Προς το παρόν, καθώς η ποσότητα των συσκευών IoT αυξάνεται εκθετικά με την πάροδο του χρόνου, μπορούν εύκολα να γίνουν ένα χρήσιμο εργαλείο για τους εισβολείς ώστε να εκτελέσουν μαζικές επιθέσεις DDoS σε ευαίσθητες επιχειρηματικές εγκαταστάσεις. Αυτό θα αναγκάσει αυτές τις συσκευές είτε να αναβαθμιστούν, είτε να αποσυνδεθούν από το Διαδίκτυο είτε να αντικατασταθούν από νέες, λόγω της αδυναμίας αναβάθμισής τους. Ωστόσο, αυτό είναι πολύ απίθανο να συμβεί, καθώς οι ιδιοκτήτες των συσκευών ενδέχεται να μην παρατηρήσουν κάποια ασυνήθιστη ενέργεια. Κατά συνέπεια, οι κυβερνήσεις θα αναγκαστούν να οριοθετήσουν κανόνες στο εγγύς μέλλον, καθώς η έλλειψη ασφάλειας στις συσκευές IoT μπορεί να αποτελέσει παγκόσμια απειλή. Η περιοδική αναβάθμιση λογισμικού θα πρέπει να είναι υποχρεωτική, καθώς και η δυνατότητα των συσκευών IoT "να ενημερώνονται σε τακτική βάση, με εύκολο τρόπο, χωρίς τη χρονοβόρα διαδικασία που συνοδεύει τις αναβαθμίσεις λογισμικού σήμερα", [30].

Εμφανίζονται νέες καταστροφικές απειλές, καθώς αυτές που θέτουν σε κίνδυνο την αλυσίδα ασφάλειας εφοδιασμού μπορούν να τροποποιηθούν και να επηρεάσουν ιδίως διακομιστές. Για παράδειγμα, οι υπηρεσίες μέσω Python μπορεί να γίνουν μη ασφαλείς από τη στιγμή που δημιουργούνται, καθώς οι προγραμματιστές ενδέχεται να χρησιμοποιούν κατά λάθος βιβλιοθήκες που έχουν παραβιαστεί ή ακόμα και να συμπεριλάβουν πλαστά πακέτα λογισμικού στα σχέδιά τους μέσω παλιών τεχνικών όπως το typo squatting (ή αλλιώς ψεύτικο URL).

Ως αποτέλεσμα, αναγνωρίζεται ότι μια σημαντική αιτία των πιο συνηθισμένων προβλημάτων ασφαλείας είναι η έλλειψη ευαισθησίας των χρηστών και των προγραμματιστών απέναντι στις βέλτιστες πρακτικές ασφάλειας. Επειδή κάτι τέτοιο δείχνει μελλοντικά δύσκολο και χρονοβόρο, θα ήταν σκόπιμο να ανεξαρτητοποιηθεί το έργο των προγραμματιστών από την ασφάλεια.

Η εφαρμογή προληπτικών μέτρων κατά των παραβιάσεων της ασφάλειας θα πρέπει να αποτελέσει μείζονα ανησυχία, καθώς οι περιορισμοί ασφαλείας στο επίπεδο μεταφοράς (Transport Layer Security – TLS), ή οποιουδήποτε άλλου, δεν μπορούν να εφαρμοστούν εύκολα, ιδίως όταν δίνονται αυξημένα δικαιώματα στους διακομιστές Linux "δεδομένου ότι έχουν το ίδιο επίπεδο δικαιωμάτων με τον πυρήνα, και ως εκ τούτου είναι δύσκολο να αντιμετωπιστούν".

Όσον αφορά την ασφάλεια των συσκευών IoT, είναι σαφές ότι το πολύ περιορισμένο υλικό έχει το πλεονέκτημα της δυσκολίας του να παραβιαστεί, καθώς το βελτιστοποιημένο υλικό δεν μπορεί να είναι στόχος γενικών αυτοματοποιημένων επιθέσεων. Ωστόσο, τα δεδομένα επικοινωνίας ενδέχεται να παραμείνουν σε κίνδυνο: μια πρόσφατη δημοσίευση από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) αναφέρει ότι ένας κύκλος ζωής προϊόντος μπορεί να περιορίζεται από την αδυναμία των πρωτοκόλλων και των αλγορίθμων ασφαλείας του, αναγκάζοντάς το να αναβαθμίσει το υλικό του νωρίτερα ή να εκτελέσει διαδικασίες ενημέρωσης λογισμικού που μπορεί να πολύπλοκες και δαπανηρές. Αυτό συμβαίνει κυρίως επειδή το υλικό είναι κατασκευασμένο για την αρχική του σχεδιασμένη

λειτουργικότητα, προκειμένου να εξοικονομήσει κόστος στη μαζική παραγωγή και να παρατείνει τη διάρκεια ζωής των μπαταριών. Ωστόσο, αυτό το γεγονός περιορίζει τις δυνατότητες ενημέρωσης λογισμικού, αναγκάζοντας τους τελικούς χρήστες να αγοράσουν νέα ενημερωμένα προϊόντα.

Μια συσκευή IoT μπορεί απλώς να είναι μια τυπική συσκευή με ένα μικρό ενσωματωμένο υπολογιστικό στοιχείο. Όταν μια συσκευή IoT αναφέρεται ως συσκευή "χαμηλού κόστους", εννοούμε συχνά το IoT μέρος της (στοιχείο IoT). Οι κατασκευαστές συνήθως ελαχιστοποιούν το κόστος ενός στοιχείου IoT, ευνοώντας την παρουσία του στην αγορά έναντι της ασφάλειάς του.

Οι περιορισμοί των πόρων των συσκευών είναι τυπικές συνέπειες του χαμηλού κόστους. Ορισμένοι περιορισμοί πόρων στο IoT είναι στο κομμάτι της εισόδου / εξόδου (π.χ. οθόνη, πληκτρολόγιο), μεγέθη μνήμης, ταχύτητες επεξεργαστή και μέγεθος μπαταρίας. Το RFC 7228 [34] ορίζει τρεις κατηγορίες συσκευών περιορισμένων πόρων (Πίνακας 5). Οι συσκευές κλάσης 0 είναι γενικά πολύ περιορισμένες για να επικοινωνούν απευθείας με hosts στο διαδίκτυο με ασφάλεια, βασιζόμενοι σε έναν ενδιάμεσο κόμβο για επικοινωνία μέσω πρωτοκόλλου χαμηλής ισχύος, όπως τα Bluetooth Χαμηλής Ενέργειας (Bluetooth Low-Energy - BLE), Zigbee ή 6LoWPAN. Χρησιμοποιούν συνήθως εξειδικευμένους μικροελεγκτές μίας χρήσης. Οι συσκευές της κατηγορίας 1 δυσκολεύονται συνήθως να επικοινωνούν μέσω του διαδικτύου χρησιμοποιώντας πιο τυπικά πρωτόκολλα επικοινωνίας ανώτερων επιπέδων (π.χ. HTTP, TLS), αντί να χρησιμοποιούν ελαφρύτερα πρωτόκολλα μέσω ενδιάμεσων κόμβων. Οι συσκευές της κατηγορίας 2 εξακολουθούν να χρησιμοποιούν πρωτόκολλα και δυνατότητες που έχουν σχεδιαστεί για συσκευές περιορισμένης χρήσης πόρων, αλλά ενδέχεται (ανάλογα με το υλικό και το λογισμικό) να μπορούν να εκτελούν τυπικά πρωτόκολλα για επικοινωνία στο διαδίκτυο. Υπάρχουν συσκευές περιορισμένων και πάνω από την κατηγορία 2 (Κατηγορία "2+") που δεν αναλύονται περαιτέρω.

Πίνακας 1: Κατηγορίες συσκευών περιορισμένων πόρων: Περιορισμοί μνήμης, λειτουργικά συστήματα (αν υπάρχουν) και μέθοδοι επικοινωνίας

Κατηγορία	Πτητική μνήμη	Μη-πτητική μνήμη	Λειτουργικό Σύστημα και Επικοινωνία
0	$<< 10Kib$	$<< 100Kib$	Υλικό για συγκεκριμένες λειτουργίες, λίγα IoT λειτουργικά συστήματα, βασικά μηνύματα κατάστασης συστήματος και keep-alive μηνύματα, χρειάζεται ενδιάμεσο κόμβο
1	$\sim 10KiB$	$\sim 100KiB$	Λειτουργικά συστήματα για IoT, ελαφριά και ασύρματα (π.χ. BLE)/ ασύρματα πρωτόκολλα βασισμένα στο UDP
2	$\sim 50KiB$	$\sim 250KiB$	Λειτουργικά συστήματα για IoT, ελαφριά και ασύρματα / ασύρματα πρωτόκολλα βασισμένα στο UDP, κοινά πρωτόκολλα υψηλότερων επιπέδων
2+	$> 50KiB$	$> 250KiB$	Λειτουργικά συστήματα για IoT ή ολοκληρωμένα λειτουργικά συστήματα, κοινά πρωτόκολλα υψηλότερων επιπέδων

Επιπτώσεις για την ασφάλεια: Αναζητώντας μειώσεις στα κόστη, οι κατασκευαστές ενδέχεται να χρησιμοποιούν λογισμικό ανοιχτού κώδικα ή γενικό υλικό για την κατασκευή των συσκευών τους, επιλέγοντας λύσεις που παρέχουν την απαιτούμενη λειτουργικότητα για το προϊόν τους. Η χρήση υπερβολικά φορτωμένων από πλευράς εργασιών στοιχείων προσθέτει περιττούς κινδύνους - η πολυπλοκότητα είναι ο εχθρός της ασφάλειας. Για παράδειγμα, οι μη χρησιμοποιούμενες λειτουργικές μονάδες και χαρακτηριστικά τους, συχνά δεν απενεργοποιούνται σωστά, και με αυτόν τον τρόπο παρέχουν επιπλέον έδαφος για επίθεση. Ένα απλό παράδειγμα είναι η χρήση του Linux για το λειτουργικό σύστημα μιας συσκευής (και η μη απενεργοποίηση λειτουργιών ή υπηρεσιών που δεν χρησιμοποιούνται). Αυτό σχετίζεται με την απειρία του κατασκευαστή, καθώς

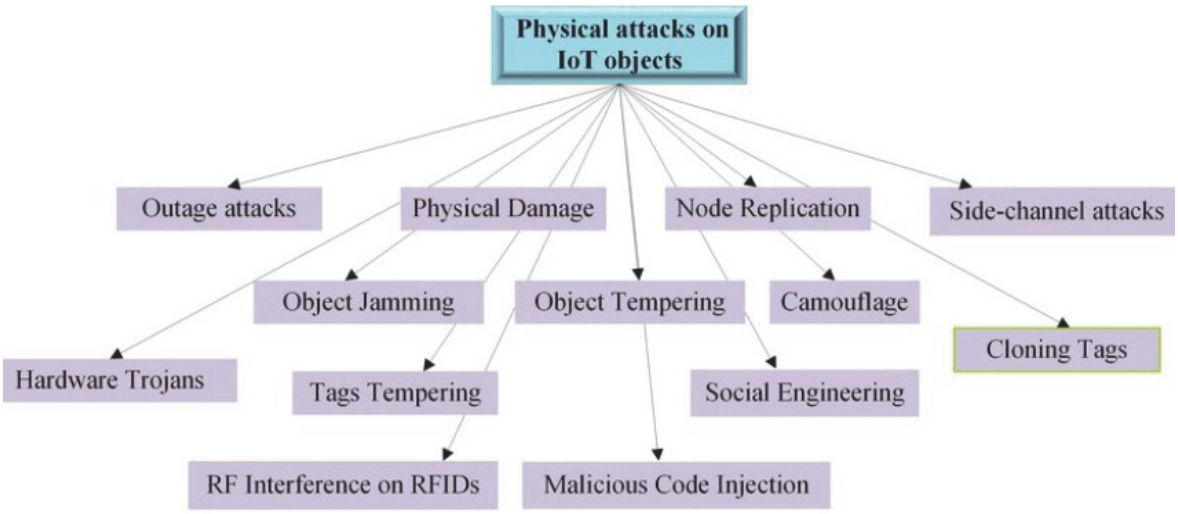
οι νέοι κατασκευαστές που δεν κατανοούν πλήρως τις τεχνικές ή λειτουργικές τους ανάγκες μπορούν να επιλέξουν γενικές, ενδεχομένως υπερβολικά φορτωμένες λύσεις, [34].

Μη τυπικές διεπαφές: Οι διεπαφές συσκευών διαφέρουν αρκετά μεταξύ του Internet of Computers (IoC) και του IoT. Για λόγους ευχρηστίας, η πρόκληση είναι συχνά μεγαλύτερη στην παραμετροποίηση μιας συσκευής παρά στην τυπική λειτουργία της. Ο σχεδιασμός της αλληλεπίδρασης αφορά τους τρόπους με τους οποίους ένας χρήστης αλληλεπιδρά με μια συσκευή. Στο IoC, αυτό γίνεται σχεδόν αποκλειστικά χρησιμοποιώντας πληκτρολόγιο και οθόνη ή συνδυαστικά οθόνη αφής. Οι συσκευές IoT απαιτούν συνήθως κάποια εναλλακτική μέθοδο για τη ρύθμιση ή την παραμετροποίηση της συσκευής (π.χ. εφαρμογή έξυπνου τηλεφώνου, υπηρεσία διαχείρισης cloud). Αυτό οδηγεί σε μια σειρά από προκλήσεις για τους χρήστες για τη διαχείριση ενημερώσεων συσκευών, παραμετροποίησης και αποδέσμευσης.

Το IoT είναι ακόμα αρκετά νέο και η ποικιλομορφία συσκευών είναι υψηλή. Αυτή η ποικιλομορφία ενισχύεται από το ευρύ φάσμα των όσων ορίζουμε ως συσκευή IoT και καθιστά δύσκολη την τυποποίηση του υλικού. Αυτό επιδεινώνει προβλήματα όπως την ασφαλή παραμετροποίηση συσκευής ή ως προς την επικοινωνία μεταξύ συσκευών. Σε συνδυασμό με τις διαφορές στο υλικό, το λογισμικό που εκτελείται στις συσκευές είναι εξειδικευμένο για μια συγκεκριμένη εργασία, γεγονός που καθιστά δύσκολη την παραγωγή λογισμικού, την ενημέρωση και τη διαχείριση μιας μεγάλης ποικιλίας συσκευών. Αυτό βελτιώνεται σε συσκευές με λειτουργικά συστήματα για το IoT όπου μπορούν να χρησιμοποιηθούν κοινός κώδικας υποδομής.

Επιπτώσεις για την ασφάλεια: Τα νέα σχέδια διεπαφών σημαίνουν νέο έδαφος επίθεσης. Οι φωνητικές εντολές έχουν αποδειχθεί καταστροφικές σε έξυπνες οικιακές συσκευές, λαμβάνοντας οποιοδήποτε ήχο στο περιβάλλον ως πιθανή εντολή. Οι είσοδοι του αισθητήρα (θερμοκρασία, θόρυβος) μπορούν να μη χρησιμοποιηθούν σωστά για την παροχή ψεύτικων δεδομένων (π.χ. χειροκίνητη αλλαγή των αναγνώσεων του αισθητήρα). Οι υπηρεσίες cloud παρουσιάζουν μια νέα μορφή επίθεσης, αν και οι βασικές υπηρεσίες cloud αντιμετωπίζουν τις προκλήσεις του IoC. Η κλιμάκωση του IoT παίζει σημαντικό ρόλο. Όσο περισσότερα πράγματα υπάρχουν, τόσο πιθανότερη η επίθεση και να φιλοξενήσει ένα botnet.

Τέλος, η φυσική πρόσβαση σε συσκευές IoT είναι ένας επιπλέον κίνδυνος επίθεσης. Είναι πιο εύκολο για έναν επισκέπτη ή εισβολέα να κλέψει μια μικρή συσκευή IoT από έναν φορητό ή επιτραπέζιο υπολογιστή λόγω της τοποθέτησής του και της παρουσίας του. Μόλις κλαπεί, ο εισβολέας θα μπορούσε να επιτεθεί στο σπίτι χρησιμοποιώντας αυτήν τη συσκευή ή να ανακτήσει ευαίσθητα δεδομένα από τα αποθηκευμένα δεδομένα του, [34].



Εικόνα 11: Κατηγοριοποίηση επιθέσεων στο υλικό σε περιβάλλον IoT

Επιπλέον, ορισμένοι ρυθμιστικοί κανόνες στην Ευρώπη, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation - GDPR), απαιτούν συστήματα που παρέχουν "προστασία της ιδιωτικής ζωής από τη στιγμή του σχεδιασμού", το οποίο απαιτεί την προσέγγιση "ασφάλεια από τη στιγμή του σχεδιασμού" που αναφέρεται στις Συστάσεις ασφαλείας για το IoT από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών. Αυτό θα μπορούσε να καταστήσει ανέφικτη τη χρήση συσκευών με πολλούς περιορισμούς σε ορισμένα σενάρια, καθώς θα ήταν αδύνατο να αναβαθμιστούν με ευελιξία.

Σύμφωνα με διάφορες έρευνες [31], [32], μπορεί να εξαχθεί το συμπέρασμα ότι η μείωση ανάπτυξης του χρόνου των συσκευών IoT αποτελεί επιχειρηματική πολιτική. Τα πιο περιζήτητα πρωτόκολλα εφαρμογών είναι σήμερα τα HTTP (Hypertext Transfer Protocol) και MQTT (Message Queue Telemetry Transport), καθώς είναι μακροπρόθεσμα και εύχρηστα. Το generic υλικό αποτελεί επίσης μια προτιμώμενη εναλλακτική λύση όποτε είναι δυνατόν, καθώς είναι λιγότερο περιορισμένο και επιτρέπει μεγαλύτερη ευελιξία όταν η κατανάλωση ενέργειας δεν είναι το πιο επιθυμητό χαρακτηριστικό. Αυτά τα κομμάτια υλικού επιτρέπουν τη χρήση λύσεων που βασίζονται σε πιο γενικά POSIX (π.χ. λειτουργικά συστήματα που πληρούν συγκεκριμένα πρότυπα συμμόρφωσης για συμβατότητα όπως το Linux), αντί για απλό υλικό (baremetal)· και αυτή η εναλλακτική αποκτά όλο και περισσότερο έδαφος, [30].

Ωστόσο, όλα αυτά τα χαρακτηριστικά διευκολύνουν τους hacker να ελέγχουν τις συσκευές IoT. Αυτό μπορεί να συμβεί αν οι διαδικασίες ασφάλειας και ενημερώσεων δεν αντιμετωπιστούν προσεκτικά, καθώς το generic υλικό και λογισμικό μπορούν να χρησιμοποιηθούν για την εκτέλεση αυθαίρετων εφαρμογών, συμπεριλαμβανομένων και των κακόβουλων. Ως εκ τούτου, οι μη αναγνωρισμένες ευπάθειες επίσης διαδίδονται γρήγορα και γίνεται εφικτή η εισβολή σε αυτά

με αυτοματοποιημένο τρόπο. Παρόλο που ενδέχεται να αποκαλυφθούν γρήγορα τα νέα τρωτά σημεία στα πρωτόκολλα επικοινωνίας και ασφάλειας, οι "επείγουσες" ενημερώσεις είναι δύσκολο να εφαρμοστούν, ακόμη και αν κριθούν υποχρεωτικές. Επιπλέον, πρέπει να αποφεύγονται οι επιλογές αντικατάστασης εξ' ολοκλήρου των συσκευών ανάλογα με τον τελικό χρήστη.

2.3.1 Ανάγκη για ασφάλεια στο IoT – προτεινόμενες λύσεις

Σε αυτό το πλαίσιο, μια προσέγγιση που βασίζεται στην ανεξαρτητοποίηση της ασφάλειας των συσκευών IoT από τις εφαρμογές μπορεί να επιταχύνει την πρόοδο προς την επίτευξη των ακόλουθων στόχων, [30]:

- Μειωμένο κόστος ανάπτυξης και συντήρησης κατά τη διάρκεια του κύκλου ζωής του προϊόντος.
- Ευκολότερες εφαρμογές "ασφαλείας-σχεδιασμού".
- Επεκτασιμότητα και διαλειτουργικότητα σε περιβάλλοντα IoT μεταξύ τομέων.
- Ένας ευκολότερος και φθηνότερος τρόπος πιστοποίησης της συμμόρφωσης της συσκευής με τον κανονισμό ασφαλείας.
- Μια απλούστερη αγορά ασφάλειας: οι hacker "προτιμούν" την πολυπλοκότητα.
- Ένα επαναχρησιμοποιήσιμο πρότυπο ασφάλειας που δε θα περιορίζει τον παραδοσιακό σχεδιασμό κάθετων λύσεων, που θα εφαρμοστεί σε ήδη υλοποιημένα έργα χωρίς αλλαγές στο σχεδιασμό λογισμικού συσκευών IoT.
- Μειωμένη ανθρώπινη αλληλεπίδραση κατά την αναβάθμιση του λογισμικού: Δεν απαιτείται ούτε η αλληλεπίδραση με την αρχική ομάδα ανάπτυξης λογισμικού (που συνήθως δεν είναι διαθέσιμη), ούτε με τον τελικό χρήστη, καθώς οι αναβαθμίσεις μπορούν να πραγματοποιηθούν με αυτοματοποιημένο τρόπο.

Οι τεχνικές ανεξαρτητοποίησης της ασφαλείας συνήθως εφαρμόστηκαν μαζί με συμπληρωματικό ειδικό υλικό. Ένα παράδειγμα της χρήσης ειδικού υλικού για την εξασφάλιση λογικών διαδικασιών είναι η πληρωμή με πιστωτική κάρτα, η οποία μπορεί να εκτελεστεί μέσω εγκεκριμένων συσκευών πληρωμής της βιομηχανίας καρτών πληρωμών (Pin Transaction Security - PCI – PTS). Εκτός αυτού, ένα εγκεκριμένο PTS ενσωματωμένο στα σημεία πώλησης είναι αποδεκτό από τις επιχειρήσεις από τις οποίες απαιτείται συμμόρφωση με τον κανονισμό GDPR.

Η χρήση μιας πιο ολοκληρωμένης λύσης έχει επιτευχθεί επίσης μέσω κρυπτογραφικών PUF που εκμεταλλεύονται στο κάθε κύκλωμα τα μη ανακυκλώσιμα και μοναδικά χαρακτηριστικά του υλικού για απρόβλεπτη (αλλά επαναλαμβανόμενη) απόκριση. Οι κρυπτογραφικές λειτουργίες PUF απαιτούν λιγότερο υλικό και ενέργεια από τους παραδοσιακούς αλγόριθμους και η αξιοπιστία τους βασίζεται στην απρόβλεπτη κατάσταση ορισμένων χαρακτηριστικών που διαθέτει

κάθε κύκλωμα. Η ανεξαρτητοποίηση της ασφάλειας από τις εφαρμογές, χρησιμοποιώντας αυτήν την τεχνολογία που βασίζεται στο υλικό, έχει προταθεί ως λύση για περιβάλλοντα IoT και ιδιαίτερα για διαδικασίες ενημέρωσης firmware.

Ωστόσο, ορισμένες μελέτες έχουν δείξει ότι το κύριο χαρακτηριστικό αυτών των λειτουργιών (η αδυναμία της αντιγραφής) μπορεί να παρακαμφθεί υπό συγκεκριμένες περιστάσεις. Σε πολλές περιπτώσεις, ο εξοπλισμός και τα εργαλεία που απαιτούνται για αυτό, δεν αξίζουν τον κόπο της διαδικασίας της παραβίασης, αλλά αυτό το γεγονός δείχνει ότι ορισμένες εφαρμογές που βασίζονται μόνο σε αυτήν την τεχνολογία ενδέχεται να μην είναι αρκετά ασφαλείς σε όλα τα πιθανά σενάρια. Από αυτήν την άποψη, πρόσφατη έρευνα παρείχε σημαντικά αποτελέσματα στην απλή κλωνοποίηση υλικού όταν οι λειτουργίες XOR PUF χρησιμοποιούνται στην τεχνολογία RFID χρησιμοποιώντας φθηνό generic υλικό και λογισμικό (και μόνο σε χιλιοστά του δευτερολέπτου), [33]. Παρ 'όλα αυτά, το PUF θα πρέπει να θεωρηθεί μια πολλά υποσχόμενη τεχνολογία, η οποία βρίσκεται υπό ανάπτυξη, και θα ξεπεράσει αυτούς τους περιορισμούς, ιδίως σε συνδυασμό με τη νανοτεχνολογία και τη μηχανική μάθηση.

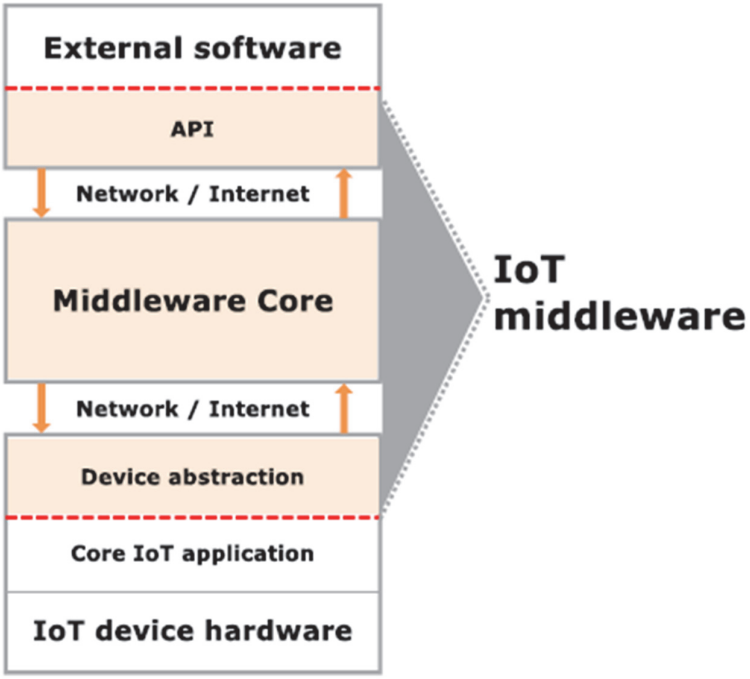
Μια προσέγγιση σε επίπεδο δικτύου που στοχεύει στην ανεξαρτητοποίηση της ασφάλειας για τις εφαρμογές έχει επίσης αντιμετωπιστεί, σε κάποιο βαθμό, μέσω των Software Defined Network - SDN. Μια συντονισμένη απόκριση σε ορισμένες επιθέσεις μπορεί να αυτοματοποιηθεί, παρέχοντας μια επιτυχημένη αντιμετώπιση κατά τον περιορισμό τους σε περιβάλλοντα IoT και προστατεύοντας άλλες συσκευές πριν από την επικείμενη επίθεση.

Είναι επίσης εφικτή η ανεξαρτητοποίηση της ασφάλειας και των εφαρμογών με τη χρήση απλού λογισμικού, αλλά απαιτεί τη χρήση αρκετά ισχυρών συσκευών IoT, ώστε να χειρίζονται μια λύση που δεν πατάνε πάνω απευθείας στο υλικό: σχεδόν οποιαδήποτε συσκευή μπορεί να εκτελεί λειτουργίες λειτουργικού, ακόμη και τις πιο περιορισμένες. Αυτή η λύση πρέπει να είναι σε θέση να εκτελεί αυτόνομα λογισμικό ασφαλείας / firware. Δυστυχώς, αυτό θα απαιτούσε λιγότερο περιορισμένες συσκευές με περισσότερες δυνατότητες υλικού, κυρίως RAM, ROM απαιτώντας περισσότερη ενέργεια.

Οι λύσεις middleware IoT προσφέρουν τη δυνατότητα αφαίρεσης υλικού με σκοπό την αύξηση της διαλειτουργικότητας και τη βελτίωση της ασφάλειας. Αυτές οι προσεγγίσεις βοηθούν στην ανεξαρτητοποίηση της ασφάλειας από το κομμάτι της σχεδίασης λογισμικού. Ωστόσο, καθώς το επίπεδο αφαίρεσης είναι ενσωματωμένο στη συσκευή IoT, έχει τελικά (σε κοινά / σχετικά εκτελέσιμα αρχεία) τις υλοποιήσεις και τις ρυθμίσεις των πρωτοκόλλων ασφαλείας (που βασίζονται γενικά σε TLS / DTLS). Επομένως, μια αναβάθμιση ασφαλείας απαιτεί επίσης ενημέρωση του middleware έτσι ώστε να ενσωματώσει αυτές τις αλλαγές στο επίπεδο συσκευής IoT. Ένα χαρακτηριστικό που θα μπορούσε να είναι επιθυμητό για μια καλύτερη λύση

ανεξαρτητοποίησης της ασφαλείας θα πρέπει να είναι η δυνατότητα αναβάθμισής τους χωρίς να απαιτείται ενημέρωση στο middleware IoT.

Αυτή η προσέγγιση ανεξαρτητοποίησης της ασφαλείας είναι δυνατή σε τέτοιου είδους middleware, αν το λογισμικό αφαίρεσης συσκευών και η εφαρμογή του πυρήνα του IoT είναι ενσωματωμένα σε διαφορετικά εκτελέσιμα αρχεία (Εικόνα 12). Σε αυτήν την περίπτωση, μια επιτυχής ανεξαρτητοποίηση ασφαλείας μπορεί να επιτευχθεί κάθε φορά που εφαρμόζεται μια αναβάθμιση στην πλατφόρμα του middleware που αφορά την ασφάλεια μόνο για τα εκτελέσιμα αρχεία που δεν "κοιτάζουν τι έχουν από κάτω" και δεν αλλάζει το εσωτερικό API που απαιτεί η εφαρμογή του πυρήνα του IoT για την επικοινωνία μέσω του επιπέδου αφαίρεσης της συσκευής. Σε κάθε περίπτωση, μια αποσύνδεση της ασφαλείας για το IoT middleware θα ήταν συνετή προκειμένου να μειωθούν οι χρόνοι επιδιόρθωσης και να απλοποιηθεί η αρχιτεκτονική του μεσαίου λογισμικού. Διαφορετικά, το πρόβλημα αποσύνδεσης ασφαλείας θα είχε μετακινηθεί προς τον τομέα υλοποίησης του λογισμικού middleware.



Εικόνα 12: Δομή IoT middleware

Το υλικό των συσκευών IoT θέτει έναν περιορισμό ως προς το λογισμικό που μπορούν να εκτελέσουν. Σε πολλές περιπτώσεις, οι μικροελεγκτές έχουν χρησιμοποιηθεί ευρέως ως πλατφόρμες υλικού κατά την ανάπτυξη συσκευών IoT, λόγω της χαμηλής κατανάλωσης ενέργειας και του μειωμένου κόστους. Επιπλέον, έχουν αναπτυχθεί νέα πρωτόκολλα ειδικά προσαρμοσμένα για την κίνηση δεδομένων στο IoT, ικανά να εκτελούνται σε περιορισμένους κόμβους και δίκτυα, όπως π.χ. το Πρωτόκολλο Περιορισμένης Εφαρμογής (Constrained Application Protocol - CoAP),

το πρωτόκολλο Αναπαράστασης Κατάστασης Μεταφοράς (REpresentational State Transfer - REST) για χρήση σε περιβάλλοντα χαμηλής ισχύος και επιρρεπή στις απώλειες. Οι περιορισμένες δυνατότητες αυτών των μικροελεγκτών ενδέχεται να οδηγήσουν σε ανασφαλείς εφαρμογές και στην αδυναμία μελλοντικής και απομακρυσμένης ενημέρωσης λογισμικού. Αυτό μπορεί να συμβαίνει όταν οι αλλαγές που απαιτούνται σε βασικές κρυπτογραφικές συναρτήσεις περιλαμβάνουν διαφορετικούς μαθηματικούς τελεστές: για παράδειγμα, οι πρόσφατες ευπάθειες που εντοπίστηκαν στον τυπικό αλγόριθμο ανταλλαγής κλειδιών Diffie-Hellman απαιτούν σημαντικές αλλαγές στη μετάβαση σε ελλειπτικές καμπύλες.

Ωστόσο, δεν είναι όλα τα κομμάτια υλικού IoT τόσο περιορισμένα όσον αφορά την ισχύ επεξεργασίας. Στην πραγματικότητα, πολλά από αυτά έχουν επεξεργαστές ικανούς για προηγμένους υπολογισμούς, όπως π.χ. Συσκευές συστήματος σε ένα κύκλωμα (System on a Chip - SoC). Επομένως, σε πολλές περιπτώσεις, μπορούν να χρησιμοποιηθούν πιο ώριμες λύσεις ασφάλειας όπου είναι εφικτή η ανεξαρτητοποίηση της ασφάλειας, καθώς η χρήση αυτών των αναδυόμενων αρχιτεκτονικών υλικού με υψηλότερες δυνατότητες είναι κατάλληλη, ενώ η κατανάλωση ενέργειας και το κόστος μπορούν να διατηρηθούν σε λογικά επίπεδα.

Από την πηγή [30], προτείνεται μια λύση των προβλημάτων ασφαλείας για τις συσκευές IoT με ένα ορισμένο επίπεδο χωρητικότητας επεξεργασίας (π.χ. συσκευές SoC). Σε αυτές τις περιπτώσεις, αυτές οι πιθανές ευπάθειες θα μπορούσαν να επιλυθούν με την απλή αναβάθμιση αυτού του αρθρωτού λογισμικού ασφαλείας απομακρυσμένα.

Μερικά παραδείγματα εταιρειών που αναπτύσσουν συσκευές SoC / SoM (System on Module – SoM) και όπου αυτή η προσέγγιση είναι εφικτή, είναι οι Emcraft, Pengutronix, Beck-ipc, κ.ά. Μερικά σχετικά τεχνικά παραδείγματα IoT όπου θα μπορούσε να εφαρμοστεί αυτό το σχήμα είναι: α) ενσωματωμένες συσκευές ARM9 βασισμένες σε Linux για βιομηχανικούς σκοπούς, β) FPGAs που φιλοξενούν μικρές πλατφόρμες IoT με βάση το Linux, γ) προσεγγίσεις που βασίζονται σε ενσωματωμένο λειτουργικό Linux σε ασύρματα κυκλώματα μικροελεγκτή.

3. Μηχανική Μάθηση

Ωστόσο υπάρχουν μερικές επιθέσεις στο υλικό οι οποίες δεν μπορούν να αντιμετωπιστούν με τις ως άνω παραδοσιακές μεθόδους. Αυτές είναι οι επιθέσεις με χρήση Αλγορίθμων Μηχανικής Μάθησης οι οποίες είναι πολύ ισχυρές και θεωρούνται “the state of the art” των επιτιθέμενων (attackers).

3.1 Τι είναι Μηχανική Μάθηση;

Η εκμάθηση μέσω προσωπικής εμπειρίας και γνώσης, η οποία διαδίδεται από γενιά σε γενιά, βρίσκεται στο επίκεντρο της ανθρώπινης νοημοσύνης. Επίσης, στην καρδιά οποιουδήποτε επιστημονικού πεδίου βρίσκεται η ανάπτυξη μοντέλων (συχνά ονομάζονται θεωρίες) προκειμένου να εξηγήσουν τα διαθέσιμα πειραματικά στοιχεία σε κάθε χρονική περίοδο. Με άλλα λόγια, μαθαίνουμε πάντα από τα δεδομένα. Διαφορετικά δεδομένα και διαφορετικές μελέτες στα δεδομένα δημιουργούν διαφορετικούς επιστημονικούς κλάδους.

Ειδικότερα, σκοπός των μοντέλων Μηχανικής Μάθησης είναι να εντοπίσουν και να αποκαλύψουν μια πιθανή κρυφή δομή και μοτίβα κανονικότητας που σχετίζονται με τον μηχανισμό παραγωγής τους. Αυτές οι πληροφορίες με τη σειρά τους βοηθούν την ανάλυσή και την κατανόηση της φύσης των δεδομένων, τα οποία μπορούν να χρησιμοποιηθούν για την πραγματοποίηση προβλέψεων για το μέλλον. Εκτός από τη μοντελοποίηση της υποκείμενης δομής, μια σημαντική κατεύθυνση για τη Μηχανική Μάθηση είναι η ανάπτυξη αποτελεσματικών αλγορίθμων για το σχεδιασμό των μοντέλων και για ανάλυση και για πρόβλεψη. Επίσης σημαντικό είναι να αναφερθεί η περίπτωση των μεγάλων δεδομένων (big data), όταν κάποιος πρέπει να ασχοληθεί με τεράστιες ποσότητες δεδομένων, τα οποία μπορεί να εκπροσωπούνται σε χώρους μεγάλων διαστάσεων. Η ανάλυση δεδομένων για τέτοιες εφαρμογές απαιτεί από τους αλγόριθμους να είναι υπολογιστικά αποτελεσματικοί και ταυτόχρονα ισχυροί στην απόδοσή τους, επειδή ορισμένα από αυτά τα δεδομένα μπορεί να περιέχουν θόρυβο και επίσης, σε ορισμένες περιπτώσεις, τα δεδομένα μπορεί να μην έχουν τιμές.

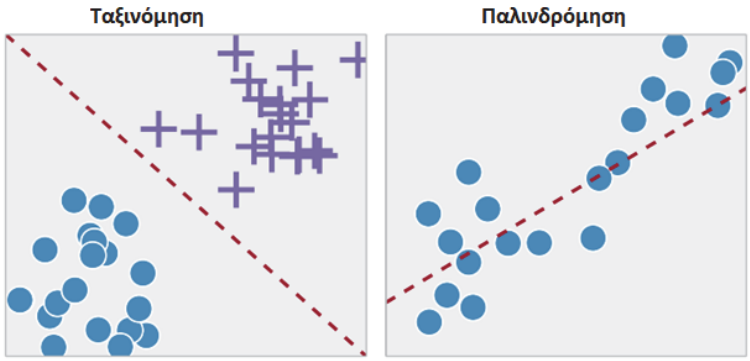
Τέτοιες μέθοδοι και τεχνικές βρίσκονται στο επίκεντρο της επιστημονικής έρευνας για αρκετές δεκαετίες σε διάφορους κλάδους, όπως Στατιστική και Στατιστική Μάθηση, Αναγνώριση προτύπων, Επεξεργασία και Ανάλυση Σημάτων και Εικόνας, Επιστήμη Υπολογιστών, Εξόρυξη Δεδομένων, Μηχανική Όραση, Βιοπληροφορική, Βιομηχανικός Αυτοματισμός και υποστήριξη Ιατρικής Διάγνωσης με υπολογιστή. Το σύνολο αυτών των μεθόδων ονομάζεται Μηχανική Μάθηση και υποδηλώνει τη χρήση μιας μηχανής / υπολογιστή για να μάθει αναλογικά τον τρόπο που ο εγκέφαλος μαθαίνει και προβλέπει. Σε ορισμένες περιπτώσεις, οι μέθοδοι εμπνέονται άμεσα από τον τρόπο με τον οποίο λειτουργεί ο εγκέφαλος, όπως συμβαίνει με τα νευρωνικά δίκτυα, [11].

3.2 Τύποι μηχανικής μάθησης (εποπτευόμενη και μη εποπτευόμενη μάθηση)

3.2.1 Εποπτευόμενη Μάθηση

Στην εποπτευόμενη μάθηση [15], εκπαιδεύεται το μηχάνημα χρησιμοποιώντας δεδομένα που είναι καλά "επισημασμένα". Αυτό σημαίνει ότι ορισμένα δεδομένα έχουν ήδη επισημανθεί με τη σωστή απάντηση. Η εποπτευόμενη μάθηση μπορεί να συγκριθεί με τη μάθηση που λαμβάνει χώρα παρουσία ενός επόπτη ή ενός δασκάλου.

Είδη Τεχνικών Εποπτευόμενης Μηχανικής Μάθησης



Εικόνα 13: Είδη Τεχνικών Εποπτευόμενης Μηχανικής Μάθησης

a. Παλινδρόμηση

Η τεχνική παλινδρόμησης προβλέπει μία τιμή εξόδου χρησιμοποιώντας εκπαιδευτικό σύνολο δεδομένων.

Παράδειγμα: Αν κάποιος επιθυμεί να προβλέψει την κοστολόγηση ενός σπιτιού από ένα εκπαιδευτικό σύνολο δεδομένων, μπορεί να χρησιμοποιήσει τη μέθοδο της παλινδρόμησης. Οι μεταβλητές εισόδου θα είναι η τοποθεσία, το μέγεθος ενός σπιτιού κ.λπ.

b. Ταξινόμηση

Ταξινόμηση σημαίνει ομαδοποίηση της εξόδου σε μια κλάση. Αν ο αλγόριθμος αντιστοιχίζει την είσοδο σε δύο διαφορετικές κατηγορίες, ονομάζεται δυαδική ταξινόμηση. Η επιλογή μεταξύ περισσότερων από δύο κατηγοριών αναφέρεται ως ταξινόμηση πολλαπλών κλάσεων.

Παράδειγμα: Προσδιορισμός του κατά πόσον κάποιος θα παραλείψει να πληρώσει το δάνειό του.

Δυνατά σημεία: Οι έξοδοι έχουν πάντα μια πιθανή ερμηνεία και ο αλγόριθμος μπορεί να κανονικοποιηθεί για να αποφευχθεί το φαινόμενο του overfitting.

Αδυναμίες: Η παλινδρόμηση στην ανάλυση δεδομένων ενδέχεται να έχει χαμηλή απόδοση όταν υπάρχουν πολλαπλά ή μη γραμμικά όρια αποφάσεων. Αυτή η μέθοδος δεν είναι ευέλικτη, συνεπώς δεν μπορεί να αναγνωρίσει πολύπλοκες σχέσεις.

3.2.2 Μη Εποπτευόμενη Μάθηση

Η μη εποπτευόμενη μάθηση είναι μια τεχνική μηχανικής μάθησης, όπου το μοντέλο δε χρειάζεται επίβλεψη. Αντ' αυτού, πρέπει να επιτραπεί στο μοντέλο να λειτουργεί από μόνο του για να ανακαλύψει πληροφορίες. Ασχολείται κυρίως με τα μη επισημασμένα δεδομένα. Οι μη εποπτευόμενοι αλγόριθμοι μάθησης επιτρέπουν την εκτέλεση πιο πολύπλοκων εργασιών επεξεργασίας σε σύγκριση με την εποπτευόμενη μάθηση. Ωστόσο η μη εποπτευόμενη μάθηση μπορεί να είναι πιο απρόβλεπτη σε σύγκριση με άλλες μεθόδους φυσικής μάθησης και ενισχυτικής μάθησης.

Οι βασικοί λόγοι για τη χρήση της μη εποπτευόμενης μάθησης είναι οι εξής:

- Η μη εποπτευόμενη μηχανική μάθηση βρίσκει κάθε είδους άγνωστα μοτίβα στα δεδομένα.
- Οι μη εποπτευόμενες μέθοδοι βοηθούν στην εύρεση δυνατοτήτων που μπορούν να είναι χρήσιμες για την κατηγοριοποίηση.
- Πραγματοποιείται σε πραγματικό χρόνο, έτσι ώστε όλα τα δεδομένα εισόδου να αναλύονται και να επισημαίνονται παρουσία των εκπαιδευομένων.
- Είναι πιο εύκολη η λήψη μη επισημασμένων δεδομένων από έναν υπολογιστή από ό,τι των επισημασμένων δεδομένων, γεγονός που σημαίνει ότι απαιτεί χειροκίνητη παρέμβαση.

Είδη μη εποπτευόμενων τεχνικών μηχανικής εκμάθησης

Τα μη εποπτευόμενα μαθησιακά προβλήματα ομαδοποιήθηκαν περαιτέρω σε προβλήματα συσταδοποίησης και συσχέτισης.

a. Συσταδοποίηση

Εικόνα 14: Είδη μη εποπτευόμενων τεχνικών μηχανικής εκμάθησης

Η συσταδοποίηση είναι μια σημαντική έννοια όταν πρόκειται για την περίπτωση της μη εποπτευόμενης μάθησης. Ασχολείται κυρίως με την εύρεση δομής ή μοτίβου σε μια συλλογή δεδομένων που δεν έχουν κατηγοριοποιηθεί. Οι αλγόριθμοι συσταδοποίησης επεξεργάζονται τα δεδομένα και βρίσκουν φυσικές συστάδες (ομάδες) αν υπάρχουν στα δεδομένα. Υπάρχει επίσης και η δυνατότητα τροποποίησης όσον αφορά το πόσες συστάδες πρέπει να αναγνωρίσουν οι αντίστοιχοι αλγόριθμοι, προσαρμόζοντας το βαθμό λεπτομέρειας αυτών των ομάδων.

b. Συσχέτιση

Οι κανόνες συσχέτισης μας επιτρέπουν να δημιουργήσουμε συσχετίσεις μεταξύ αντικειμένων δεδομένων μέσα σε μεγάλες βάσεις δεδομένων. Αυτή η μη εποπτευόμενη τεχνική αφορά την ανακάλυψη σχέσεων μεταξύ μεταβλητών σε μεγάλες βάσεις δεδομένων. Για παράδειγμα, οι άνθρωποι που αγοράζουν ένα νέο σπίτι πιθανότατα να αγοράσουν νέα έπιπλα.

Σύνοψη για εποπτευόμενη και μη μηχανική μάθηση - σύγκριση

- Στην εποπτευόμενη εκμάθηση, το μηχάνημα εκπαιδεύεται χρησιμοποιώντας δεδομένα που είναι καλά "επισημασμένα".
- Η μη εποπτευόμενη μάθηση είναι μια τεχνική μηχανικής μάθησης, όπου το μοντέλο δε χρειάζεται επίβλεψη.
- Η εποπτευόμενη μάθηση μας επιτρέπει τη συλλογή δεδομένων ή την παραγωγή δεδομένων εξόδου με βάση από προηγούμενη εμπειρία. Για παράδειγμα, μπορεί κάποιος να καθορίσει το χρόνο που απαιτείται για να φτάσει πίσω σπίτι του με βάση τις καιρικές συνθήκες, τις ώρες της ημέρας και τις διακοπές.
- Η μη εποπτευόμενη μηχανική εκμάθηση βοηθά στην εύρεση όλων των ειδών άγνωστων προτύπων στα δεδομένα. Για παράδειγμα, το μωρό μπορεί να αναγνωρίσει άλλα σκυλιά με βάση την προηγούμενη μη εποπτευόμενη μάθηση.
- Η παλινδρόμηση και η ταξινόμηση είναι δύο τύποι εποπτευόμενων τεχνικών μηχανικής μάθησης.
- Η συσταδοποίηση και η συσχέτιση είναι δύο τύποι μη εποπτευόμενης μάθησης.
- Σε ένα μοντέλο εποπτευόμενης μάθησης, οι μεταβλητές εισόδου και εξόδου θα δοθούν ενώ με το μοντέλο μη εποπτευόμενης μάθησης, θα δοθούν μόνο δεδομένα εισόδου

Ο Πίνακας 3 συνοψίζει τις διαφορές εποπτευόμενης και μη μηχανικής μάθησης, [21].

Πίνακας 2: Διαφορές εποπτευόμενης και μη εποπτευόμενης μάθησης

Εποπτευόμενη	Μη εποπτευόμενη
Στους εποπτευόμενους αλγόριθμους μάθησης, η έξοδος για τη δοσμένη είσοδο είναι γνωστή.	Στους εποπτευόμενους αλγόριθμους μάθησης, η έξοδος για τη δοσμένη είσοδο είναι άγνωστη.
Οι αλγόριθμοι μαθαίνουν από τα επισημασμένα δεδομένα. Αυτά τα δεδομένα βοηθούν στην αξιολόγηση της ακρίβειας σε εκπαιδευτικό σύνολο δεδομένων.	Ο αλγόριθμος παρέχεται με μη επισημασμένα δεδομένα, από όπου προσπαθεί να βρει μοτίβα και συσχετίσεις μεταξύ των δεδομένων αντικειμένων.
Πρόκειται για μια τεχνική μοντέλου πρόβλεψης που προβλέπει τα μελλοντικά αποτελέσματα με ακρίβεια.	Πρόκειται για μια τεχνική περιγραφικού μοντέλου που εξηγεί την πραγματική σχέση μεταξύ των στοιχείων και της προϊστορίας τους.
Περιλαμβάνει αλγορίθμους ταξινόμησης και παλινδρόμησης.	Περιλαμβάνει αλγορίθμους εκμάθησης κανόνων συσταδοποίησης και συσχέτισης.
Αυτό το είδος μάθησης είναι σχετικά πολύπλοκο, καθώς απαιτεί επισημασμένα δεδομένα.	Είναι λιγότερο πολύπλοκο, καθώς δεν υπάρχει ανάγκη για κατανόηση και επισήμανση δεδομένων.
Είναι πιο ακριβής από τη μη εποπτευόμενη μάθηση, καθώς τα δεδομένα εισόδου και η αντίστοιχη έξοδος είναι γνωστά, και η μηχανή το μόνο που χρειάζεται να κάνει είναι να αποδώσει προβλέψεις.	Έχει μικρότερη ακρίβεια καθώς τα δεδομένα εισόδου είναι μη επισημασμένα. Γι’ αυτό το λόγο η μηχανή πρέπει πρώτα να καταλάβει και να επισημάνει τα δεδομένα και μετά να αποδώσει προβλέψεις.
Πρόκειται για μια διαδικασία ανάλυσης δεδομένων που γίνεται μέσω διαδικτύου και δεν απαιτεί ανθρώπινη αλληλεπίδραση.	Πρόκειται για διαδικασία ανάλυσης δεδομένων πραγματικού χρόνου.

3.3 Αλγόριθμοι Μηχανικής Μάθησης

Οι αλγόριθμοι, [16], ομαδοποιούνται συχνά με βάση την ομοιότητα ως προς τη λειτουργία τους (πώς λειτουργούν). Για παράδειγμα, μέθοδοι που βασίζονται σε δέντρα και μέθοδοι που βασίζονται στο νευρωνικό δίκτυο. Αυτός είναι ο πιο χρήσιμος τρόπος για την ομαδοποίηση αλγορίθμων.

Αυτή είναι μια χρήσιμη μέθοδος ομαδοποίησης, αλλά δεν είναι τέλεια. Υπάρχουν αλγόριθμοι που θα ταίριαζαν σε πολλές κατηγορίες, όπως το Learning Vector Quantization που είναι και μια μέθοδος βασισμένη στο νευρωνικό δίκτυο και μια μέθοδος που βασίζεται σε στιγμιότυπα. Υπάρχουν επίσης κατηγορίες που έχουν το ίδιο όνομα που περιγράφουν το πρόβλημα και την κατηγορία του αλγορίθμου, όπως Παλινδρόμηση και Συσταδοποίηση. Αυτές τις περιπτώσεις τις χειριζόμαστε επιλέγοντας την ομάδα που υποκειμενικά είναι η "καταλληλότερη".

Σε αυτήν την ενότητα, παραθέτουμε πολλούς από τους δημοφιλείς αλγόριθμους μηχανικής μάθησης που ομαδοποιούνται με όσο πιο καλύτερο διαισθητικό τρόπο. Η λίστα δεν είναι περιλαμβάνει ούτε όλες τις ομάδες ούτε όλους τους αλγορίθμους, ωστόσο περιέχει τα πιο αντιπροσωπευτικά και χρήσιμα στοιχεία.

3.3.1 Αλγόριθμοι παλινδρόμησης

Η παλινδρόμηση ασχολείται με τη μοντελοποίηση της σχέσης μεταξύ των μεταβλητών που βελτιώνεται επαναληπτικά χρησιμοποιώντας ένα μέτρο σφάλματος στις προβλέψεις που έκανε το μοντέλο.

Οι μέθοδοι παλινδρόμησης χρησιμοποιούν τη στατιστική και έχουν επιλεγεί στη στατιστική μηχανική μάθηση. Αυτό μπορεί να προκαλέσει σύγχυση επειδή μπορούμε να χρησιμοποιήσουμε την παλινδρόμηση για να αναφερθούμε στην κατηγορία του προβλήματος και στην κατηγορία του αλγορίθμου. Πραγματικά, η παλινδρόμηση είναι μια διαδικασία. Οι πιο δημοφιλείς αλγόριθμοι παλινδρόμησης είναι:

- Κανονική παλινδρόμηση Ελαχίστων Τετραγώνων (Ordinary Least Squares Regression - OLSR)
- Γραμμική παλινδρόμηση
- Λογιστική παλινδρόμηση
- Σταδιακή παλινδρόμηση
- Πολυπαραλλαγές Splines Προσαρμοστικής Παλινδρόμησης (Multivariate Adaptive Regression Splines - MARS)

- Τοπικά εκτιμώμενο εξομαλυμένο διάγραμμα διασποράς (Locally Estimated Scatterplot Smoothing - LOESS)

3.3.2 Αλγόριθμοι βασισμένοι σε στιγμιότυπα

Το μοντέλο μάθησης που βασίζεται σε στιγμιότυπα είναι ένα πρόβλημα απόφασης με στιγμιότυπα ή παραδείγματα εκπαιδευτικών συνόλων δεδομένων που θεωρούνται σημαντικά ή είναι απαραίτητα για το μοντέλο.

Τέτοιες μέθοδοι συνήθως δημιουργούν μια βάση δεδομένων με παραδείγματα δεδομένων και συγκρίνουν τα νέα δεδομένα με τη βάση δεδομένων χρησιμοποιώντας ένα μέτρο ομοιότητας για να βρουν την καλύτερη αντιστοίχιση και να κάνουν μια πρόβλεψη. Για αυτόν τον λόγο, οι μέθοδοι που βασίζονται σε στιγμιότυπα ονομάζονται επίσης μέθοδοι "ο νικητής τα παίρνει όλα" και μέθοδοι μάθησης με βάση τη μνήμη. Έμφαση δίνεται στην αναπαράσταση των αποθηκευμένων στιγμιότυπων και στα μέτρα ομοιότητας που χρησιμοποιούνται μεταξύ των στιγμιότυπων. Οι πιο δημοφιλείς αλγόριθμοι με βάση τα στιγμιότυπα είναι:

- Κ-Κοντινότερος γείτονας (K-Nearest Neighbor - KNN)
- Μάθηση ποσοτικού διανύσματος (Learning Vector Quantization - LVQ)
- Χάρτης αυτο-οργάνωσης (Self-Organizing Map - SOM)
- Τοπική μάθηση με βαρύτητες (Locally Weighted Learning - LWL)
- Υποστήριξη διανυσματικών μηχανών (Support Vector Machines - SVM)

3.3.3 Αλγόριθμοι Κανονικοποίησης

Μια επέκταση που έγινε σε μια άλλη μέθοδο (τυπικά στις μεθόδους παλινδρόμησης) που αποδίδει πέναλτι στα μοντέλα ανάλογα με την πολυπλοκότητά τους, ευνοώντας τα απλούστερα μοντέλα που είναι επίσης καλύτερα στη γενίκευση.

Οι αλγόριθμοι κανονικοποίησης έχουν απαριθμηθεί χωριστά, επειδή είναι δημοφιλείς, ισχυροί και γενικά με απλές τροποποιήσεις σε σχέση με άλλες μεθόδους. Οι πιο δημοφιλείς αλγόριθμοι κανονικοποίησης είναι:

- Παλινδρόμηση Κορυφής
- Ελάχιστη απόλυτη συρρίκνωσης και Τελεστής Επιλογής (Least Absolute Shrinkage and Selection Operator - LASSO)
- Ελαστικό Δίκτυ
- Παλινδρόμηση Ελάχιστης Γωνίας (Least-Angle Regression - LARS)

3.3.4 Αλγόριθμοι Δέντρων Αποφάσεων

Οι μέθοδοι δένδρων αποφάσεων κατασκευάζουν ένα μοντέλο αποφάσεων που λαμβάνονται με βάση τις πραγματικές τιμές των χαρακτηριστικών στα δεδομένα.

Οι αποφάσεις διακλαδίζονται σε δομές δέντρων έως ότου ληφθεί απόφαση πρόβλεψης για μια δεδομένη εγγραφή. Τα δέντρα αποφάσεων εκπαιδεύονται σε δεδομένα για ταξινόμηση και προβλήματα παλινδρόμησης. Τα δέντρα αποφάσεων είναι τις περισσότερες φορές είναι γρήγορα και ακριβή και γι' αυτό το λόγο και αρκετά χρησιμοποιούμενα στη μηχανική μάθηση. Οι πιο δημοφιλείς αλγόριθμοι δέντρων αποφάσεων είναι:

- Δέντρο ταξινόμησης και παλινδρόμησης (Classification and Regression Tree - CART)
- Επαναληπτικό διχοτομερές 3 (Iterative Dichotomiser 3 - ID3)
- C4.5 και C5.0 (διαφορετικές εκδόσεις μιας ισχυρής προσέγγισης)
- Ανίχνευση αυτόματης αλληλεπίδρασης Chi-squared (Chi-squared Automatic Interaction Detection - CHAID)
- Κορμός απόφασης
- M5
- Δέντρα απόφασης με συνθήκες

3.3.5 Αλγόριθμοι Bayesian

Οι Bayesian μέθοδοι είναι εκείνες που εφαρμόζουν ρητά το Θεώρημα του Bayes για προβλήματα όπως η ταξινόμηση και η παλινδρόμηση. Οι πιο δημοφιλείς Bayesian αλγόριθμοι είναι:

- Naive Bayes (NB)
- Gaussian Naive Bayes
- Multinomial Naive Bayes
- Averaged One-Dependence Estimators (AODE)
- Bayesian Belief Network (BBN)
- Δίκτυο του Bayes (Bayesian Network - BN)

3.3.6 Αλγόριθμοι Συσταδοποίησης

Η συσταδοποίηση, όπως η παλινδρόμηση, περιγράφει την κλάση του προβλήματος και την κλάση των μεθόδων.

Οι μέθοδοι συσταδοποίησης τυπικά οργανώνονται από τις προσεγγίσεις μοντελοποίησης όπως η κεντροειδής και η ιεραρχική. Όλες οι μέθοδοι ασχολούνται με τη χρήση των εγγενών δομών στα δεδομένα για την καλύτερη οργάνωση των δεδομένων σε ομάδες μέγιστης ομοιότητας. Οι πιο δημοφιλείς αλγόριθμοι συσταδοποίησης είναι:

- k-Means
- k-Medians
- Μεγιστοποίηση Προσδοκίας (Expectation Maximisation - EM)
- Ιεραρχική συσταδοποίηση

3.3.7 Αλγόριθμοι Μάθησης με Κανόνες Συσχέτισης

Οι μέθοδοι μάθησης με κανόνες συσχέτισης εξάγουν κανόνες που εξηγούν καλύτερα τις παρατηρούμενες σχέσεις μεταξύ μεταβλητών στα δεδομένα.

Αυτοί οι κανόνες μπορούν να ανακαλύψουν σημαντικούς και εμπορικά χρήσιμους συσχετισμούς σε μεγάλα πολυδιάστατα σύνολα δεδομένων που μπορούν να αξιοποιηθούν από έναν οργανισμό. Οι πιο δημοφιλείς αλγόριθμοι μάθησης με κανόνες συσχέτισης είναι:

- Αλγόριθμος Apriori
- Αλγόριθμος Eclat

3.3.8 Αλγόριθμοι Τεχνητού Νευρωνικού Δικτύου

Τα τεχνητά νευρωνικά δίκτυα είναι μοντέλα που εμπνέονται από τη δομή και / ή τη λειτουργία των βιολογικών νευρωνικών δικτύων.

Πρόκειται για μια κατηγορία αντιστοίχισης μοτίβων που χρησιμοποιούνται συνήθως για προβλήματα παλινδρόμησης και ταξινόμησης, αλλά είναι πραγματικά ένα μεγάλο υποπεδίο που αποτελείται από εκατοντάδες αλγόριθμους και παραλλαγές για κάθε τύπο προβλήματος. Οι πιο δημοφιλείς αλγόριθμοι τεχνητού νευρωνικού δικτύου είναι:

- Perceptron
- Πολυεπίπεδα Perceptrons (Multilayer Perceptrons - MLP)
- Διάδοση Προς τα Πίσω
- Στοχαστική Μείωση Βαθμίδας
- Δίκτυο Hopfield
- Δίκτυο Λειτουργίας Ακτινικής Βάσης (Radial Basis Function Network - RBFN)

3.3.9 Αλγόριθμοι βαθιάς μάθησης

Οι μέθοδοι βαθιάς μάθησης (Deep Learning – DL) είναι μια σύγχρονη αναβάθμιση για τα τεχνητά νευρωνικά δίκτυα που εκμεταλλεύονται πλήρως την χαμηλή υπολογιστικότητα.

Αφορούν την κατασκευή πολύ μεγαλύτερων και πιο περίπλοκων νευρωνικών δικτύων και, όπως σχολιάστηκε παραπάνω, πολλές μέθοδοι αφορούν πολύ μεγάλα σύνολα δεδομένων με επισημασμένα αναλογικά δεδομένα, όπως εικόνα, κείμενο, ήχος και βίντεο. Οι πιο δημοφιλείς αλγόριθμοι βαθιάς μάθησης είναι:

- Συνελικτικά Νευρωνικά Δίκτυα (Convolutional Neural Networks - CNNs)
- Επαναλαμβανόμενα Νευρωνικά Δίκτυα (Recurrent Neural Networks - RNNs)
- Μακροπρόθεσμα Δίκτυα Μνήμης (Long Short-Term Memory Networks - LSTMs)
- Συσσωρευμένοι αυτόματοι κωδικοποιητές
- Μηχανή Deep Boltzmann (Deep Boltzmann Machine - DBM)
- Δίκτυα Deep Belief (Deep Belief Networks - DBN)

3.3.10 Αλγόριθμοι μείωσης διαστάσεων

Όπως οι μέθοδοι συσταδοποίησης, η μείωση διαστάσεων αναζητά και εκμεταλλεύεται την εγγενή δομή των δεδομένων, αλλά σε αυτήν την περίπτωση με έναν μη εποπτευόμενο τρόπο είτε έχει σκοπό να συνοψίσει ή να περιγράψει δεδομένα χρησιμοποιώντας λιγότερες πληροφορίες.

Αυτό μπορεί να είναι χρήσιμο για την οπτικοποίηση διαστάσεων δεδομένων ή για την απλοποίηση δεδομένων που μπορούν στη συνέχεια να χρησιμοποιηθούν σε μια εποπτευόμενη μέθοδο μάθησης. Πολλές από αυτές τις μεθόδους μπορούν να προσαρμοστούν για χρήση στην ταξινόμηση και παλινδρόμηση:

- Ανάλυση Βασικών Στοιχείων (Principal Component Analysis - PCA)
- Παλινδρόμηση Κύριων Συστατικών (Principal Component Regression - PCR)
- Μερική Ελάχιστη παλινδρόμηση (Partial Least Squares Regression - PLSR)
- Χαρτογράφηση Sammon
- Πολυδιάστατη κλιμάκωση (Multidimensional Scaling - MDS)
- Αναζήτηση προβολής
- Γραμμική Ανάλυση Διακρίσεων (Linear Discriminant Analysis - LDA)
- Ανάλυση Διακριτών Μίξεων (Mixture Discriminant Analysis - MDA)
- Τετραγωνική Ανάλυση Διακρίσεων (Quadratic Discriminant Analysis - QDA)

- Ευέλικτη Ανάλυση Διακρίσεων (Flexible Discriminant Analysis - FDA)

3.3.11 Αλγόριθμοι Συνόλων

Οι μέθοδοι συνόλων είναι μοντέλα που αποτελούνται από πολλαπλά ασθενέστερα μοντέλα που εκπαιδεύονται ανεξάρτητα και των οποίων οι προβλέψεις συνδυάζονται με κάποιο τρόπο για να κάνουν τη συνολική πρόβλεψη.

Καταβάλλεται μεγάλη προσπάθεια για την εύρεση των αδύναμων μοντέλων για να συνδυαστούν και των τρόπων με τους οποίους να συνδυαστούν. Αυτή είναι μια πολύ ισχυρή κατηγορία τεχνικών και ως εκ τούτου είναι πολύ δημοφιλής:

- Boosting
- Bootstrapped Aggregation (Bagging)
- AdaBoost
- Σταθμισμένος Μέσος Όρος (Ανάμειξη)
- Συσσωρευμένη γενίκευση (Συσσώρευση)
- Gradient Boosting Machines (GBM)
- Gradient Boosted Regression Trees (GBRT)
- Random Forest

3.3.12 Άλλοι Αλγόριθμοι Μηχανικής Μάθησης

Ωστόσο, πολλοί αλγόριθμοι δεν καλύφθηκαν. Ορισμένοι αλγόριθμοι αναφέρονται από εξειδικευμένες εργασίες στη διαδικασία της μηχανικής μάθησης, όπως:

- Αλγόριθμοι επιλογής χαρακτηριστικών
- Αξιολόγηση ακρίβειας αλγορίθμου
- Μέτρα απόδοσης
- Αλγόριθμοι βελτιστοποίησης

Επίσης, από ειδικά πεδία της μηχανικής μάθησης, ορισμένοι αλγόριθμοι δεν αναφέρονται, όπως:

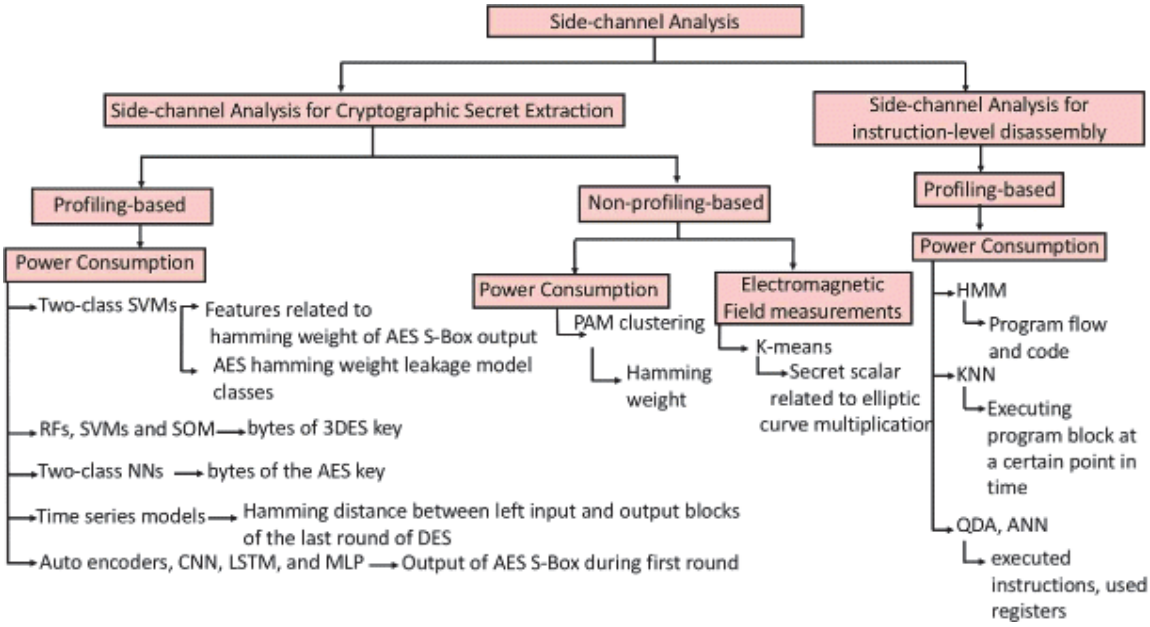
- Υπολογιστική νοημοσύνη (εξελικτικοί αλγόριθμοι, κ.λπ.)
- Υπολογιστική Όραση (Computer Vision - CV)
- Επεξεργασία φυσικής γλώσσας (Natural Language Processing - NLP)
- Συστήματα Συστάσεων

- Μάθηση Ενίσχυσης
- Γραφικά μοντέλα

4. Επιθέσεις υλικού βασισμένες σε μεθόδους Μηχανικής Μάθησης

4.1 Side Channel Analysis – SCA

Οι έξυπνες συσκευές όπως οι έξυπνες κάρτες, τα κινητά τηλέφωνα και οι συσκευές ATM έχουν διαδραματίσει σημαντικό ρόλο στη σύγχρονη κοινωνία σήμερα. Αν και τα κλειδιά που χρησιμοποιούνται στους κρυπτογραφικούς αλγόριθμους είναι συνήθως ασφαλή, με την ανάπτυξη της τεχνολογίας των υπολογιστών, η ευπάθεια της παραδοσιακής λειτουργίας κρυπτογράφησης εκτίθεται σταδιακά. Ένας εισβολέας μπορεί να χρησιμοποιήσει τις πληροφορίες διαρροής που δημιουργούνται από τη φυσική εφαρμογή. Ονομάζεται ως ανάλυση / επίθεση πλευρικού καναλιού (SCA) και μπορεί να θέσει σοβαρά σε κίνδυνο τη συνολική ασφάλεια του συστήματος. Η ζήτηση για ασφάλεια σε πολλές ενσωματωμένες εφαρμογές συσκευών, συμπεριλαμβανομένου του Internet of Things, των χρηματοοικονομικών συναλλαγών, των ηλεκτρονικών επικοινωνιών και της αποθήκευσης δεδομένων, οδήγησε στην ανάπτυξη επιθέσεων πλευρικών καναλιών.



Εικόνα 15: Κατηγορίες επιθέσεων πλευρικών καναλιών που πραγματοποιούνται μέσω Μηχανικής Μάθησης

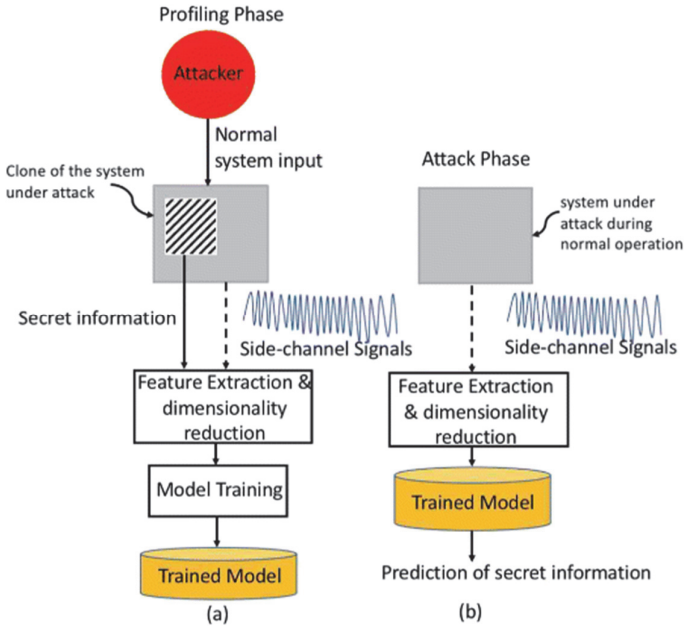
4.1.1 Ανάλυση Πλευρικού Καναλιού για Κρυπτογραφική Εξαγωγή Μυστικών Πληροφοριών

Η ανάλυση πλευρικού καναλιού αποτελεί μείζονα κίνδυνο για την κρυπτογραφία και τις εφαρμογές της, [1]. Οι επιτιθέμενοι αναλύουν σήματα πλευρικού καναλιού, για παράδειγμα, την ηλεκτρομαγνητική ακτινοβολία και την κατανάλωση ενέργειας για την εξαγωγή μυστικών κλειδιών που χρησιμοποιούνται από τους τρέχοντες κρυπτογραφικούς αλγόριθμους. Η μηχανική μάθηση έχει εφαρμοστεί σε επιθέσεις ανάλυσης πλευρικού καναλιού που βασίζονται σε προφίλ και όχι. Σε προσεγγίσεις με βάση το προφίλ, οι εισβολείς έχουν πρόσβαση σε ένα ακριβές

αντίγραφο του υλικού που δέχεται επίθεση, επομένως, μπορούν να λάβουν πληροφορίες πλευρικού καναλιού που αντιστοιχούν σε κάθε συνδυασμό πλήκτρων. Αντίθετα, σε προσεγγίσεις που δε βασίζονται σε προφίλ, οι εισβολείς δεν έχουν πρόσβαση σε ένα αντίγραφο του συστήματος που δέχεται επίθεση.

4.1.1.1 Ανάλυση Επιθέσεων Πλευρικού Καναλιού Βάσει Προφίλ

Στις επιθέσεις βάσει προφίλ, οι εισβολείς δημιουργούν μοντέλα που αντιπροσωπεύουν τη σχέση μεταξύ των συλλεχθέντων σημάτων πλευρικού καναλιού και των αντίστοιχων μυστικών πληροφοριών. Οι επιθέσεις προτύπων δημιουργούν ένα μοντέλο για κάθε μυστικό κλειδί με την υπόθεση ότι τα συλλεγόμενα σήματα πλευρικού καναλιού ακολουθούν μια κανονική κατανομή με πολλαπλές παραλλαγές. Για αποσαφήνιση σχετικά με τη διανομή δεδομένων, εισάγονται εποπτευόμενες τεχνικές μηχανικής μάθησης για τη δημιουργία μοντέλων βάσει δεδομένων. Επιπλέον, τα μοντέλα που βασίζονται στη μηχανική μάθηση είναι αποτελεσματικότερα από τις επιθέσεις προτύπων όταν οι επιτιθέμενοι έχουν πρόσβαση μόνο σε λίγα ίχνη το καθένα με μεγάλο αριθμό σημείων δεδομένων. Υπάρχουν δύο σημαντικές φάσεις στις επιθέσεις προφίλ με βάση τη μηχανική μάθηση: τη φάση της κατασκευής προφίλ και τη φάση της επίθεσης. Κατά τη διάρκεια της φάσης κατασκευής του προφίλ, ο εισβολέας καθορίζει τις μυστικές πληροφορίες που σχετίζονται με ένα συγκεκριμένο στάδιο της κρυπτογραφικής μονάδας για συσχέτιση με τα συλλεγόμενα σήματα πλευρικού καναλιού. Στη συνέχεια, ο εισβολέας συλλέγει σήματα πλευρικού καναλιού για διαφορετικές πιθανές τιμές των στοχευμένων μυστικών πληροφοριών. Επιλέγονται σημεία δεδομένων στα ίχνη πλευρικού καναλιού με το υψηλότερο περιεχόμενο πληροφοριών. Τέλος, ένα εποπτευόμενο μοντέλο μηχανικής μάθησης εκπαιδεύεται για να προβλέψει την αξία των μυστικών πληροφοριών από παρόμοιες συσκευές.



Εικόνα 16: Ανάλυση Επιθέσεων Πλευρικού Καναλιού Βάσει Προφίλ· a φάση κατασκευής προφίλ· b φάση επίθεσης

Το Πρότυπο Αναβαθμισμένης Κρυπτογράφησης (Advanced Encryption Standard - AES) και το Πρότυπο Τριπλής Κρυπτογράφησης Δεδομένων (Triple Data Encryption - 3DES) έχουν γίνει επιθέσεις με την τελευταία λέξη της τεχνολογίας για να αποδειχθεί η αποτελεσματικότητα των επιθέσεων που βασίζονται στη μηχανική μάθηση. Το AES και το 3DES είναι παραδείγματα αλγορίθμων κρυπτογράφησης συμμετρικού κλειδιού, οι οποίοι χρησιμοποιούν το ίδιο κλειδί κατά την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.

Τα ίχνη ισχύος δειγματοληπτούνται από ένα κύκλωμα που εφαρμόζει το πρότυπο AES S-box. Οι ακραίες τιμές αφαιρούνται από τα ίχνη ισχύος και ο συντελεστής συσχέτισης του Pearson, το άθροισμα της τετραγωνικής διαφοράς t και το βασικό στοιχείο ανάλυσης (Principal Component Analysis - PCA) εφαρμόζονται ανεξάρτητα για την επιλογή των πιο αντιπροσωπευτικών σημείων δεδομένων δειγματοληψίας και τη μείωση των διαστάσεων των ιχνών κατανάλωσης ισχύος του δείγματος. Στη συνέχεια, SVM δύο κατηγοριών προβλέπουν τα ακόλουθα από τα συλλεγόμενα ίχνη ισχύος: (1) αν το βάρος Hamming της εξόδου του S-Box είναι ζυγός ή μονός αριθμός, (2) αν το βάρος Hamming της εξόδου του S-Box είναι μεγαλύτερο ή μικρότερο από το προκαθορισμένο όριο του 4 και (3) αν το τέταρτο λιγότερο σημαντικό bit της εξόδου του S-Box έχει τιμή 0 ή 1 (bit (4)).

Τα ίχνη ισχύος μπορούν επίσης να χρησιμοποιηθούν για την πρόβλεψη της τιμής του κλειδιού αλγορίθμου 3DES - ένα byte τη φορά - και για τη διευκόλυνση της επίθεσης brute force όταν προβλέπονται λανθασμένα πλήκτρα. Τα πεδία αποδοχής (Receptive Fields – RF), SVM και οι χάρτες με αυτόματη οργάνωση (Self-Organizing Maps – SOM) εκπαιδεύονται να προβλέπουν

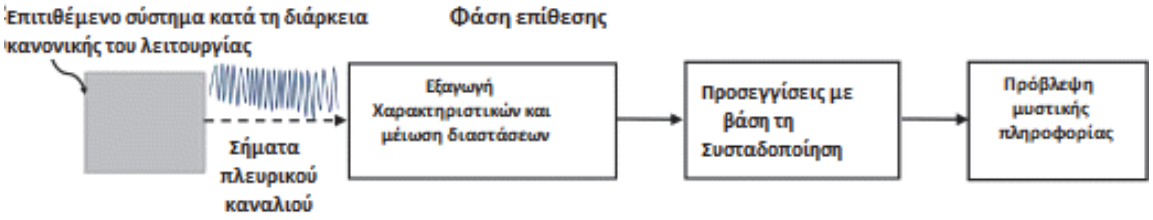
ανεξάρτητα κάθε bit του κλειδιού. Οι μεταβλητές PCA, ελάχιστης διακύμανσης και μέγιστης συσχέτισης (Minimum Redundancy Maximum Relevance – mRMR) και SOM εφαρμόζονται ανεξάρτητα για την επιλογή χαρακτηριστικών. Η κλάση του βάρους Hamming της εξόδου του AES S-Box προβλέπεται από τα ίχνη κατανάλωσης ισχύος χρησιμοποιώντας SVM δύο κατηγοριών με διαφορετικούς τύπους πυρήνα· παραδείγματα περιλαμβάνουν το γραμμικό πυρήνα, τον πυρήνα RBF, τον πολυωνυμικό πυρήνα, τον πυρήνα ισχύος, τον υβριδικό πυρήνα και τον πυρήνα καταγραφής. Ένα SVM δύο κατηγοριών με τον πυρήνα wavelet προβλέπει τα ακόλουθα χρησιμοποιώντας ίχνη ισχύος: (1) το 16ο byte του κλειδιού του πρώτου γύρου στον AES χωρίς μάσκα (Βήμα Αποκρυπτογράφησης 1). (2) η τιμή μετατόπισης που χρησιμοποιείται όταν οι τιμές της μάσκας περιστρέφονται σε μάσκα AES (Βήμα Αποκρυπτογράφησης 2). και (3) το δεύτερο byte του πρώτου γύρου στον AES με μάσκα (Βήμα Αποκρυπτογράφησης 3). Η συσχέτιση του Pearson χρησιμοποιείται για την επιλογή 32 σημείων με την υψηλότερη συσχέτιση με το ίχνος ισχύος.

Σε ορισμένες περιπτώσεις, τα νευρωνικά δίκτυα χρησιμοποιούνται για την πρόβλεψη του κλειδιού AES από ίχνη κατανάλωσης ισχύος που συλλέγονται από τα στάδια AddRoundKey και SubBytes του αλγορίθμου AES. Η ακρίβεια του προβλεπόμενου κλειδιού AES βελτιώνεται αφαιρώντας τα ίχνη κατανάλωσης ισχύος από το μέσο ίχνος ισχύος και χρησιμοποιώντας τα προκύπτοντα ίχνη ισχύος για πρόβλεψη. Η χρονική εξάρτηση μεταξύ των διαφορετικών τιμών κατανάλωσης ισχύος του δείγματος σε διαφορετικές χρονικές στιγμές λαμβάνεται υπόψη κατά την πρόβλεψη της απόστασης Hamming μεταξύ του αριστερού μπλοκ εισόδου και του αριστερού μπλοκ εξόδου του τελευταίου γύρου στον αλγόριθμο DES. Ένα μη γραμμικό μοντέλο χρονοσειρών εκπαιδεύεται για κάθε κλειδί από τα ίχνη κατανάλωσης που συλλέγονται. Τα νευρωνικά δίκτυα αυτόματων κωδικοποιητών, CNN, LSTM και πολλαπλών επιπέδων perceptron (MLP) μπορούν να προβλέψουν την έξοδο του AES S-Box κατά τον πρώτο γύρο από ίχνη κατανάλωσης ισχύος.

4.1.1.2 Ανάλυση Επιθέσεων Πλευρικού Καναλιού Χωρίς Προφίλ

Στην ανάλυση πλευρικού καναλιού που δεν βασίζεται στη δημιουργία προφίλ, εφαρμόζονται μη εποπτευόμενοι αλγόριθμοι μηχανικής μάθησης για να αποκαλύψουν τις μυστικές πληροφορίες χωρίς να έχουν πρόσβαση στο αντίγραφο του συστήματος που δέχεται επίθεση. Για παράδειγμα, όταν κάθε χρήστης έχει ένα μοναδικό κλειδί, ο εισβολέας μπορεί να παρατηρήσει μόνο τα ίχνη που σχετίζονται με διαφορετικούς χρήστες. Υποτίθεται ότι τα ίχνη που ανήκουν σε κλειδιά με παρόμοια βάρη Hamming είναι πιο κοντά το ένα στο άλλο. Επομένως, τα συλλεγόμενα ίχνη ισχύος ομαδοποιούνται σε συστάδες χρησιμοποιώντας τον αλγόριθμο ομαδοποίησης PAM (Partitioning around Medoids - PAM), παρόμοιο με τον K-means. Στη συνέχεια, ο εισβολέας

προβλέπει το βάρος Hamming κάθε συστάδας. Τέλος, το μυστικό κλειδί αποκαλύπτεται από το προβλεπόμενο βάρος Hamming μέσω μιας επίθεσης brute-force.



Εικόνα 17: Ανάλυση Επιθέσεων Πλευρικού Καναλιού Χωρίς Προφίλ

Επιπλέον, ο πολλαπλασιασμός της ελλειπτικής καμπύλης σε κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού μπορεί να δεχτεί επίθεση με ανάλυση της διαρροής από μία σειριακή εκτέλεση χρησιμοποιώντας τον αλγόριθμο συσταδοποίησης K-means. Διαρροή μίας σειριακής εκτέλεσης είναι το σήμα που διαρρέει όταν επεξεργάζονται σειριακά bits ένα προς ένα. Δεδομένου ότι οι εκθέτες εφαρμόζονται με τη μορφή επαναλαμβανόμενων λειτουργιών, παρόμοια bits σε όλες τις λειτουργίες έχουν παρόμοια μοντέλα διαρροής σειριακής εκτέλεσης. Αυτό έχει ως αποτέλεσμα, τα ηλεκτρομαγνητικά ίχνη να συλλέγονται και να χωρίζονται σε διαφορετικά δείγματα. Κάθε δείγμα αντιστοιχεί σε ένα bit στη μυστική βαθμίδα. Παρόμοια δείγματα ομαδοποιούνται μαζί χρησιμοποιώντας συσταδοποίηση K-means και κάθε bit ταξινομείται και καθορίζεται η a posteriori πιθανότητα. Επομένως, δείγματα με χαμηλή posteriori πιθανότητα μπορούν να εκτιμηθούν με μια επίθεση brute force.

Ανάλυση πλευρικού καναλιού βήμα προς βήμα

4.1.2 Ανάλυση πλευρικού καναλιού για αποσύνθεση/αποκάλυψη εντολών

Τα σήματα πλευρικού καναλιού μπορούν να αναλυθούν από εισβολείς όχι μόνο για διαρροή μυστικών κρυπτογραφικών πληροφοριών, αλλά και για να αποκαλυφθούν οι εκτελεσθείσες εντολές όταν εκτελούνται τα προγράμματα. Έχουν προταθεί αρκετές τεχνικές ανάλυσης πλευρικού καναλιού βάσει προφίλ για να αποκαλυφθούν πληροφορίες σχετικά με τα προγράμματα εκτέλεσης. Για παράδειγμα, η ανάλυση πλευρικού καναλιού μπορεί να χρησιμοποιηθεί για να προσδιορίσει ποιο μπλοκ προγράμματος εκτελείται σε κάθε χρονική στιγμή καθώς και τις εκτελεσθείσες εντολές του. Αυτές οι τεχνικές μπορούν να αξιοποιηθούν από τους αντιπάλους με αντίστροφη μηχανική των εκτελούμενων προγραμμάτων.

Οι τεχνικές βάσει προτύπων μπορούν να χρησιμοποιηθούν για να αποκαλύψουν εντολές όσον αφορά την εκτέλεση προγραμμάτων από την ανάλυση των σημάτων πλευρικού καναλιού. Ωστόσο, η ακρίβεια ανίχνευσης εντολών μειώνεται όταν αλλάζει η κατανομή δεδομένων. Τα κρυφά μοντέλα Markove (Hidden Markove Models - HMMs) χρησιμοποιούνται για την εξαγωγή αποσυντεθημένων εντολών από ίχνη κατανάλωσης ισχύος. Η πιθανότητα των εκτελούμενων εντολών και των επακόλουθων εντολών τους που υπολογίζονται από προγράμματα που είχαν εκτελεστεί στο παρελθόν, χρησιμοποιούνται για τη δημιουργία των HMMs. Ωστόσο, οι εντολές μπορούν να αναγνωριστούν με μέγιστη ακρίβεια 58%. Γι' αυτό το λόγο, έχουν προταθεί πρόσφατα άλλοι αλγόριθμοι βασισμένοι στη μηχανική μάθηση για τη βελτίωση της ακρίβειας της πρόβλεψης σε επίπεδο εντολών χρησιμοποιώντας ίχνη πλευρικού καναλιού. Το μπλοκ ενός κώδικα προγράμματος που εκτελείται σε μια συγκεκριμένη χρονική στιγμή προβλέπεται με τη χρήση του ταξινομητή Κ-πλησιέστερων γειτόνων (KNN) με βάση τη μέτρηση απόστασης δυναμικής παραμόρφωσης χρόνου (Dynamic Time Warping - DTW) από ίχνη κατανάλωσης ισχύος. Το λειτουργικό σύστημα λειτουργεί σε έναν μονοπύρηνο μικροεπεξεργαστή που δεν υποστηρίζει προηγμένα μικρο-αρχιτεκτονικά χαρακτηριστικά, για παράδειγμα, μνήμες cache και διοχέτευση. Ο KNN ταξινομητής εκπαιδεύεται χρησιμοποιώντας ζεύγη ιχνών ισχύος και το αντίστοιχο μπλοκ προγράμματος που εκτελείται. Η τετραγωνική διακριτική ανάλυση (Quadratic Discriminant Analysis - QDA) και οι ταξινομητές νευρωνικών δικτύων χρησιμοποιούνται για την πρόβλεψη των εκτελεσμένων εντολών, την αναγνώριση των χρησιμοποιημένων καταχωρητών και την εκτίμηση των τιμών τους από ίχνη κατανάλωσης ισχύος.

4.2 Επίθεση με βαθιά μάθηση (Deep Learning)

4.2.1 Ιστορική εξέλιξη

Η βαθιά μάθηση είναι ένας κλάδος της μηχανικής μάθησης και είναι πολύ δημοφιλής στο κύμα της μεγάλης ανάπτυξης δεδομένων τα τελευταία χρόνια. Χρησιμοποιεί «βαθιά» νευρωνικά δίκτυα για να μάθει τα χαρακτηριστικά από πολύπλοκα δεδομένα και λαμβάνει αποφάσεις για ένα άλλο σύνολο ανάλυσης δεδομένων. Έχει εξαιρετικές λειτουργίες εξαγωγής και ταξινόμησης χαρακτηριστικών. Είναι επίσης ένα όπλο της νέας εποχής που μπορεί να συνδυαστεί με το SCA. Η βαθιά μάθηση χρησιμοποιεί ένα μοντέλο βαθύ νευρωνικού δικτύου που έχει καλή επίδραση στην επεξεργασία τεχνητής νοημοσύνης, όπως φωνή, εικόνα και κείμενο με ιεραρχική δομή. Η ιστορία της βαθιάς μάθησης είναι στην πραγματικότητα η ιστορία των τεχνητών νευρικών δικτύων. Το 1957, ο Rosenblatt πρότεινε για πρώτη φορά την έννοια του **perceptron**[1] ως

[1] Ο νευρώνας Perceptron ή Αντίληπτρο είναι ένα είδος τεχνητού νευρωνικού δικτύου που εφευρέθηκε το 1957 στο Αεροναυτικό Εργαστήριο του Κορνέλλ (Cornell Aeronautical Laboratory) από τον Φρανκ Ρόζενμπλατ (Frank

ανεξάρτητη μονάδα νευρωνικού δικτύου. Στη συνέχεια, οι Widrow και Hoff όχι μόνο πέτυχαν τεχνητά νευρικά δίκτυα σε υπολογιστές, αλλά πρότειναν επίσης τον περίφημο **gradient descent algorithm**[2], ο οποίος έθεσε τα θεμέλια για το νευρικό δίκτυο **BP**[3] που πρότειναν οι Rumelhart και McCelland. Το **MLP** (=multilayer perceptron) προτάθηκε για πρώτη φορά από τον Werbos το 1981. Είναι επίσης ένας back propagation αλγόριθμος που βασίζεται σε διάφορα συγκεκριμένα νευρικά δίκτυα. Το 1982, το Hopfield πρότεινε το νευρωνικό δίκτυο **Hopfield** για να προσομοιώσει τη μνήμη του εγκεφάλου. Προκειμένου να βελτιστοποιηθεί το νευρωνικό δίκτυο Hopfield, το 1985, οι Hinton και Sejnowski μελετήθηκαν με τον **annealing** αλγόριθμο της μηχανής Boltzmann και της μηχανής περιορισμένης πρόσβασης Boltzmann (RBM) χρησιμοποιώντας δειγματοληψία Gibbs, η οποία έκανε το νευρωνικό δίκτυο σημαντικό. Ως εκ τούτου, από τα τέλη της δεκαετίας του 1980 έως τις αρχές του 21ου αιώνα, άλλες μηχανικές εκμάθηση όπως οι αλγόριθμοι **RF** και **SVM** άνθισαν μέχρι το **DBN** περιορισμένο νευρικό δίκτυο Boltzmann που προτάθηκε το 2005 να είναι πολύ ανώτερο από άλλους αλγόριθμους μηχανικής μάθησης. Για άλλη μια φορά, η έρευνα για τα νευρικά δίκτυα έχει κυριαρχήσει στην κατεύθυνση της AI, και διάφορα βαθιά δίκτυα όπως το **CNN** και το **RNN** έχουν εμφανιστεί το ένα μετά το άλλο. [42]

Rosenblatt). Ο Perceptron είναι ένας δυαδικός ταξινομητής, δηλαδή μία συνάρτηση η οποία απεικονίζει την είσοδο x (ένα διάνυσμα με πραγματικές τιμές) σε μία τιμή εξόδου f(x) (μία και μοναδική δυαδική τιμή).

$$f(x) = \begin{cases} 1 & \text{if } w \cdot x + b > 0 \\ 0 & \text{else} \end{cases}$$

όπου w είναι ένα διάνυσμα από βάρη με πραγματικές τιμές και w . x είναι το εσωτερικό γινόμενο μεταξύ των διανυσμάτων w και x (Υπολογίζεται δηλαδή ένα βεβαρημένο άθροισμα). Το b είναι το 'bias', ένας σταθερός όρος ο οποίος δεν εξαρτάται από καμία τιμή εισόδου.

[2] Το Gradient descent είναι ένας αλγόριθμος επαναληπτικής βελτιστοποίησης πρώτης τάξης για την εύρεση ενός τοπικού ελάχιστου μιας διαφοροποιήσιμης συνάρτησης . Είναι ένας αλγόριθμος βελτιστοποίησης που χρησιμοποιείται για την ελαχιστοποίηση κάποιας λειτουργίας μετακινώντας επαναληπτικά προς την κατεύθυνση της απότομης καθόδου όπως ορίζεται από το αρνητικό της κλίσης. Στη μηχανική εκμάθηση, χρησιμοποιούμε τον Gradient descent για να ενημερώσουμε τις παραμέτρους του μοντέλου μας.

[3] Στην μηχανική εκμάθηση , το backpropagation (backprop , BP) είναι ένας ευρέως χρησιμοποιούμενος αλγόριθμος για την εκπαίδευση νευρικών δικτύων feedforward . Υπάρχουν γενικεύσεις του backpropagation για άλλα τεχνητά νευρικά δίκτυα (ANNs) και για λειτουργίες γενικά. Αυτές οι κατηγορίες αλγορίθμων αναφέρονται γενικά ως "backpropagation". Κατά την τοποθέτηση ενός νευρικού δικτύου , το backpropagation υπολογίζει την κλίση της λειτουργίας απώλειας σε σχέση με τα βάρη του δικτύου για ένα μόνο παράδειγμα εισόδου-εξόδου και το κάνει αποτελεσματικά , σε αντίθεση με έναν απλό άμεσο υπολογισμό της κλίσης σε σχέση με κάθε βάρος ξεχωριστά. Αυτή η αποτελεσματικότητα καθιστά εφικτή τη χρήση gradient μεθόδων για την εκπαίδευση δικτύων πολλαπλών επιπέδων, την ενημέρωση βαρών για την ελαχιστοποίηση της απώλειας. Χρησιμοποιούνται συνήθως gradient descent ή stochastic gradient descent. Είναι ένα παράδειγμα δυναμικού προγραμματισμού.

4.2.2 Βήματα

① Προεπεξεργασία του συνόλου δεδομένων: Στο παραδοσιακό προφίλ SCA, το βήμα προεπεξεργασίας δεδομένων είναι στην πραγματικότητα μια μείωση των διαστάσεων με τη στενή έννοια, συμπεριλαμβανομένων των μοντέλων μηχανικής εκμάθησης. Ακριβώς επειδή το χαρακτηριστικό των δεδομένων είναι τόσο περίπλοκο που δεν μπορεί να παραλειφθεί η προεπεξεργασία. Για το προφίλ SCA που βασίζεται στη βαθιά μάθηση, μπορεί να παραλειφθεί το στάδιο προεπεξεργασίας της μείωσης των διαστάσεων (εκτός αν η διάσταση είναι πολύ υψηλή) και να προεπεξεργαστεί άμεσα το σύνολο δεδομένων. Χωρίζεται σε δύο μέρη: το σύνολο δεδομένων εκπαίδευσης και τα δεδομένα επαλήθευσης. Το σύνολο δεδομένων εκπαίδευσης χρησιμοποιείται για την εκπαίδευση του μοντέλου και το σύνολο δεδομένων επαλήθευσης χρησιμοποιείται για τη μέτρηση του δείκτη.

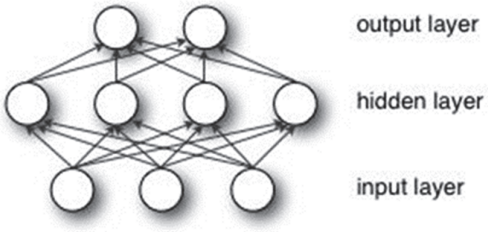
② Επιλέγοντας Μοντέλα και Εκπαίδευση: Η εκπαίδευση του μοντέλου πραγματοποιείται χρησιμοποιώντας διαφορετικά βαθιά νευρωνικά δίκτυα. Υπάρχουν συνήθως ορισμένα μοντέλα: MLP, CNN και RNN.

③ Επαλήθευση και αξιολόγηση: Αρκετά πλαίσια αξιολόγησης χρησιμοποιούνται συχνά για την αξιολόγηση της απόδοσης της λειτουργίας ή για την επιλογή των βέλτιστων παραμέτρων για την οικογένεια παραμετρικών μοντέλων. Ο σκοπός αυτών των μεθόδων είναι να παρέχει μία εκτίμηση της απόδοσης μιας μέτρησης (ακρίβειας) που είναι ανεξάρτητη από την επιλογή μεταξύ του σετ κατάρτισης Dtrain και του σετ δοκιμής Dtest, αλλά εξαρτημένη από την κλίμακα.

④ Αντιστοίχιση και ανάκτηση (Matching and Recovering)

4.2.3 Μοντέλα που χρησιμοποιούνται

① MLP (=Multilayer Perceptron): Το perceptron πολλαπλών επιπέδων ονομάζεται επίσης τεχνητό νευρικό δίκτυο. Εκτός από τα επίπεδα εισόδου και εξόδου, μπορεί να υπάρχουν πολλά κρυφά στρώματα στο μεταξύ. Το απλούστερο MLP περιέχει μόνο ένα κρυφό επίπεδο, δηλαδή τη δομή τριών επιπέδων, όπως φαίνεται στο σχήμα παρακάτω:

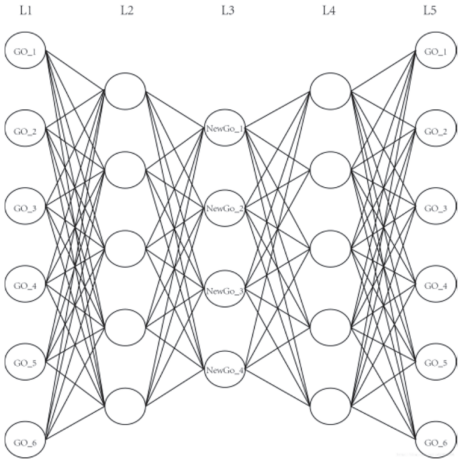


Όπως φαίνεται από το παραπάνω σχήμα, το στρώμα του MLP είναι πλήρως συνδεδεμένο με το στρώμα (η πλήρης σύνδεση σημαίνει ότι κάθε νευρώνας στο άνω στρώμα συνδέεται με όλους τους νευρώνες στο επόμενο στρώμα). Το κάτω στρώμα των πολλαπλών επιπέδων perceptron είναι το επίπεδο εισόδου, το μεσαίο είναι το κρυφό στρώμα και τέλος το επίπεδο εξόδου.

Σχετικά με το επίπεδο εισόδου, για παράδειγμα, εάν η είσοδος είναι ένα διάνυσμα n-διαστάσεων, υπάρχουν n νευρώνες. Αλλά πώς προέρχονται οι νευρώνες στο κρυφό στρώμα; Πρώτον, είναι πλήρως συνδεδεμένο με το επίπεδο εισόδου. Εάν το στρώμα εισόδου αντιπροσωπεύεται από το διάνυσμα X, η έξοδος του κρυφού στρώματος είναι f (w1x + b1), όπου w1 είναι το βάρος, b1 είναι το bias (προτίμηση). Η συνάρτηση f εμφανίζεται συνήθως ως σιγμοειδής ή ως υπερβολή (συνάρτηση υπερβολής). Τέλος, το επίπεδο εξόδου, στην πραγματικότητα, το κρυφό επίπεδο στο επίπεδο εξόδου μπορεί να θεωρηθεί ως λογιστική παλινδρόμηση πολλαπλών κατηγοριών, δηλαδή η παλινδρόμηση softmax. Έτσι, η έξοδος του επιπέδου εξόδου είναι softmax (w1x + b1), το x1 αντιπροσωπεύει την έξοδο του κρυφού στρώματος f (w1x + b1).

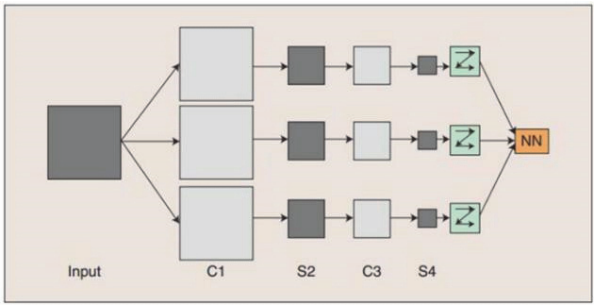
Επομένως, όλες οι παράμετροι του MLP είναι τα βάρη σύνδεσης και αντισταθμίσεις μεταξύ των επιπέδων. Ο ορισμός των καλύτερων παραμέτρων είναι ένα πρόβλημα βελτιστοποίησης. Για την επίλυση του προβλήματος βελτιστοποίησης, το πιο απλό είναι η gradient descent μέθοδος: πρώτα αρχικοποιούμε τυχαία όλες τις παραμέτρους, στη συνέχεια επαναλαμβάνουμε την εκπαίδευση του μοντέλου, υπολογίζοντας συνεχώς τη διαβάθμιση και ενημερώνουμε τις παραμέτρους μέχρι να ικανοποιηθεί μια συγκεκριμένη συνθήκη. (Για παράδειγμα, όταν το σφάλμα είναι αρκετά μικρό και ο αριθμός επαναλήψεων είναι αρκετός). Αυτή η διαδικασία περιλαμβάνει συναρτήσεις κόστους, κανονικοποίηση, ρυθμό μάθησης, υπολογισμούς διαβάθμισης κ.λπ.

② DAE = Differential-algebraic system of equations: Είναι ένας τύπος νευρωνικού δικτύου που μπορεί να θεωρηθεί ότι αποτελείται από δύο μέρη: μια συνάρτηση κωδικοποιητή h = f (x) και έναν ανακατασκευασμένο αποκωδικοποιητή r = g (h). Παραδοσιακά, οι αυτόματοι κωδικοποιητές έχουν χρησιμοποιηθεί για μείωση διαστάσεων ή την εκμάθηση χαρακτηριστικών. Τα νευρωνικά δίκτυα αυτόματης κωδικοποίησης προσπαθούν να μάθουν μια συνάρτηση $hW,b(x)\approx x$. Με άλλα λόγια, προσπαθεί να προσεγγίσει μια συνάρτηση ταυτότητας έτσι ώστε η έξοδος χ' να πλησιάσει την είσοδο x. Με απλά λόγια, το DAE έχει αυξημένο βάθος σε σύγκριση με τον αρχικό αυτόματο κωδικοποιητή, βελτιώνοντας τη μαθησιακή ικανότητα και διευκολύνοντας την προ-εκπαίδευση.

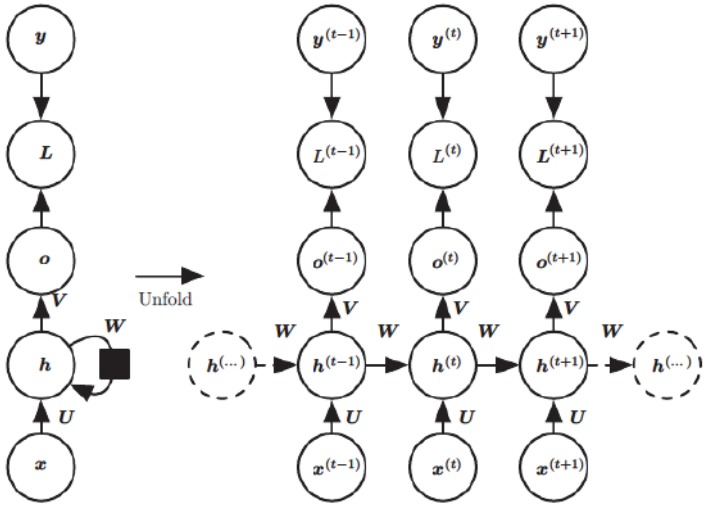


③ CNN =Convolutional Neural Network (ConvNet/CNN): Είναι ένα συνελικτικό νευρωνικό δίκτυο πολλαπλών στρωμάτων όπου κάθε στρώμα αποτελείται από πολλαπλά δισδιάστατα

επίπεδα και κάθε ένα από αυτά τα επίπεδα αποτελείται από πολλαπλούς ανεξάρτητους νευρώνες. Η εικόνα εισόδου περιβάλλεται από τρία εκπαιδεύσιμα φίλτρα (trainable filters) και μια πρόσθετη προτίμηση (addable bias). Μετά από συνέλιξη δημιουργούνται τρεις χάρτες χαρακτηριστικών στο στρώμα C1 και έπειτα τέσσερα pixel σε κάθε ομάδα στο χάρτη χαρακτηριστικών. Στη συνέχεια τα μεγέθη summary, βάρος (weight) και offset δημιουργούν έναν χάρτη χαρακτηριστικών τριών επιπέδων S2 μέσω μιας σιγμοειδούς συνάρτησης. Αυτοί οι χάρτες στη συνέχεια φιλτράρονται για να ληφθεί το επίπεδο C3. Αυτή η ιεραρχική δομή παράγει ξανά το S4 όπως το S2. Τέλος, αυτές οι τιμές pixel ψηφιδοπλέκονται και συνενώνονται σε μια είσοδο φορέα σε ένα παραδοσιακό νευρωνικό δίκτυο για να πάρουν την έξοδο. Γενικά το στρώμα C είναι ένα στρώμα εξαγωγής χαρακτηριστικών. Η είσοδος κάθε νευρώνα συνδέεται με το τοπικό πεδίο υποδοχής του προηγούμενου στρώματος και το τοπικό χαρακτηριστικό εξάγεται. Μόλις εξαχθεί το τοπικό χαρακτηριστικό καθορίζεται η σχέση μεταξύ αυτού και των υπολοίπων χαρακτηριστικών. Το στρώμα S είναι το επίπεδο χαρτογράφησης χαρακτηριστικών και κάθε στρώμα υπολογισμού του δικτύου αποτελείται από πολλούς χάρτες χαρακτηριστικών και κάθε χαρακτηριστικό χαρτογραφείται σε ένα επίπεδο με τα βάρη όλων των νευρώνων στο επίπεδο να είναι ίδια.



④ <u>RNN = Recurrent neural network</u>: Είναι ένας τύπος νευρωνικού δικτύου που χρησιμοποιείται για την επεξεργασία δεδομένων ακολουθίας. Είδαμε ότι το νευρωνικό δίκτυο αποτελείται από ένα επίπεδο εισόδου, ένα κρυφό επίπεδο και ένα επίπεδο εξόδου. Η έξοδος ελέγχεται από μια λειτουργία ενεργοποίησης και τα στρώματα συνδέονται με βάρη. Η λειτουργία ενεργοποίησης καθορίζεται εκ των προτέρων και το μοντέλο του νευρικού δικτύου περιλαμβάνεται στο βάρος με την εκπαίδευση.



Αυτό είναι ένα τυπικό διάγραμμα δομής RNN όπου κάθε βέλος αντιπροσωπεύει έναν μετασχηματισμό, δηλαδή, η σύνδεση βέλους έχει τα βάρη. Η αριστερή πλευρά είναι διπλωμένη προς τα πάνω, η δεξιά πλευρά είναι η ξεδιπλωμένη εμφάνιση και το βέλος δίπλα στο h στην αριστερή πλευρά αντιπροσωπεύει τον "βρόχο" σε αυτή τη δομή που αντανακλάται στο κρυφό στρώμα. Στην ξεδιπλωμένη δομή σταθμίζονται οι νευρώνες του κρυμμένου στρώματος. Δηλαδή, καθώς η ακολουθία εξελίσσεται, το προηγούμενο κρυφό επίπεδο θα επηρεάσει το προηγούμενο κρυφό επίπεδο. Στο σχήμα, το ο αντιπροσωπεύει την έξοδο, το y αντιπροσωπεύει την καθορισμένη τιμή που δίνεται από το δείγμα και το L αντιπροσωπεύει τη συνάρτηση απώλειας.

Εκτός από τα παραπάνω χαρακτηριστικά, το τυπικό RNN έχει τις ακόλουθες δυνατότητες:
1. Τα βάρη μοιράζονται. Τα βάρη w στο σχήμα είναι όλα τα ίδια και τα U και V είναι τα ίδια.
2. Κάθε τιμή εισόδου συνδέεται μόνο με τη δική της διαδρομή και δεν θα συνδεθεί με άλλους νευρώνες.

4.2.4 Σύγχρονη μέθοδος με εξαιρετικά αποτελέσματα

Σύμφωνα με έγγραφα που μπορούν να συλλεχθούν πρόσφατα, η μέθοδος δημιουργίας προφίλ SCA με βάση το βαθύ νευρωνικό δίκτυο έχει μελετηθεί σε λίγα άρθρα τα τελευταία χρόνια. Το 2013, ο πρώτος που χρησιμοποίησε το νευρωνικό δίκτυο σε συνδυασμό με την ανάλυση ισχύος στο SCA ήταν τα απλά δίκτυα τριών επιπέδων που χρησιμοποιούσε ο Martinasek και πέτυχε ακρίβεια ταξινόμησης έως και 90%. Ο Gilmore και ο Hanley πρότειναν μια επίθεση πλευρικού

καναλιού που βασίζεται σε νευρωνικά δίκτυα προσπαθώντας να σπάσει την band-masked[4] υλοποίηση του AES του DPA[5] διαγωνισμού version4.

Το 2016, ο Maghrebi και άλλοι του Safran Group χρησιμοποίησαν την κλασική template μέθοδο επίθεσης, τη μέθοδο μηχανικής μάθησης και τη μέθοδο τεχνολογίας βαθιάς μάθησης για να εκτελέσουν ένα βασικό σπάσιμο στα δεδομένα του διαγωνισμού του DPA αντίστοιχα. Τα πειραματικά αποτελέσματα δείχνουν ότι το αποτέλεσμα επίθεσης προτύπου που βασίζεται σε βαθύ νευρωνικό δίκτυο είναι καλύτερο από άλλα και έχει υψηλότερο ποσοστό επιτυχίας. Στην βαθιάς μάθησης template[6] επίθεση, η μέθοδος εξαγωγής χαρακτηριστικών που υιοθετήθηκε από τον Maghrebi είναι πιο αποτελεσματική από την AE(=Acoustic emission) learning classification.

Ο Martinasek και οι συνάδελφοί του συνέκριναν τις μεθόδους που βασίζονται στο MLP(=Multilayer perceptron) με άλλες κλασσικές μεθόδους, όπως template επιθέσεις ή τυχαίες επιθέσεις. Πραγματοποίησαν πειράματα με βάση τον αλγόριθμο κρυπτογράφησης AES-128 και έδωσαν τις υπερπαραμέτρους[7] MLP και μερικές πληροφορίες σχετικά με την εκπαίδευση. Η έρευνα δείχνει ότι η τεχνολογία MLP από τη θεωρία της βαθιάς μάθησης είναι μια αποτελεσματική εναλλακτική λύση στην παραδοσιακή ανάλυση προτύπων και είναι καλύτερη από τις προηγούμενες τεχνολογίες SVM και τυχαίων δασών. Ωστόσο, αυτές οι επιθέσεις είναι πιο παραμετροποιημένες και δεν παρέχουν τις ακριβείς πληροφορίες σχετικά με την

---

[4] Σε υλοποιήσεις masked AES, τυχαία ενδιάμεσα δεδομένα προστίθενται συνεχώς στα plaintexts κατά τη διάρκεια της διαδικασίας κρυπτογράφησης για να καλύψουν τη διαρροή πλευρικού καναλιού από (S-boxes) που επεξεργάζονται τα μυστικά δεδομένα. Στο τέλος της κρυπτογράφησης, τα τυχαία ενδιάμεσα δεδομένα που παράγονται ως αποτέλεσμα της λειτουργίας masking αφαιρούνται από τα σωστά δεδομένα κρυπτογράφησης. Ένας συμβατικός αλγόριθμος που χρησιμοποιεί masked AES, ωστόσο, απαιτεί μεγάλους πίνακες αναζήτησης (LUTs= look-up tables) και η απόδοση μειώνεται σημαντικά λόγω του μεγάλου όγκου των τιμών του masking.

[5] Differential power analysis (DPA) είναι μια επίθεση πλευρικού καναλιού που περιλαμβάνει στατιστική ανάλυση μετρήσεων κατανάλωσης ισχύος από ένα κρυπτοσύστημα . Η επίθεση εκμεταλλεύεται μεροληψίες ποικίλης κατανάλωσης ισχύος μικροεπεξεργαστών ή άλλου υλικού κατά την εκτέλεση λειτουργιών χρησιμοποιώντας μυστικά κλειδιά. Οι επιθέσεις DPA έχουν ιδιότητες επεξεργασίας σήματος και διόρθωσης σφαλμάτων που μπορούν να εξαγάγουν μυστικά από μετρήσεις που περιέχουν πολύ θόρυβο για να αναλυθούν χρησιμοποιώντας απλή ανάλυση ισχύος. Χρησιμοποιώντας το DPA, ένας αντίπαλος μπορεί να αποκτήσει μυστικά κλειδιά αναλύοντας μετρήσεις κατανάλωσης ενέργειας από πολλαπλές κρυπτογραφικές λειτουργίες που εκτελούνται από μια ευάλωτη έξυπνη κάρτα ή άλλη συσκευή.

[6] Οι template επιθέσεις είναι ένας ισχυρός τύπος επίθεσης πλευρικού καναλιού. Αυτές οι επιθέσεις είναι ένα υποσύνολο επιθέσεων προφίλ, όπου ένας εισβολέας δημιουργεί ένα "προφίλ" μιας ευαίσθητης συσκευής και εφαρμόζει αυτό το προφίλ για να βρει γρήγορα το μυστικό κλειδί του θύματος. Οι template επιθέσεις απαιτούν περισσότερες ρυθμίσεις από τις επιθέσεις CPA(=Chosen-plaintext attack).

[7] Στη μηχανική εκμάθηση, μία υπερπαραμέτρος είναι μια παράμετρος της οποίας η τιμή χρησιμοποιείται για τον έλεγχο της μαθησιακής διαδικασίας. Αντίθετα, οι τιμές άλλων παραμέτρων (τυπικά βάρη κόμβου) προέρχονται μέσω προπόνησης. Οι υπερ-παράμετροι μπορούν να ταξινομηθούν ως μοντέλα υπερπαραμέτρων, τα οποία δεν μπορούν να συναχθούν κατά την προσαρμογή του μηχανήματος στο σετ προπόνησης, επειδή αναφέρονται στην εργασία επιλογής μοντέλου που κατ 'αρχήν δεν επηρεάζουν την απόδοση του μοντέλου αλλά επηρεάζουν την ταχύτητα και ποιότητα της μαθησιακής διαδικασίας. Ένα παράδειγμα υπερπαραμέτρου μοντέλου είναι η τοπολογία και το μέγεθος ενός νευρικού δικτύου.

παραμετροποίηση και την κατάρτιση του αλγορίθμου. Αυτός ο περιορισμός περιορίζει τον συνδυασμό μεθόδων βαθιάς μάθησης στο πλευρικό κανάλι.

Η Eleonora Cagli κατάφερε να προτείνει μια μέθοδο επίθεσης από άκρο σε άκρο που βασίζεται στο CNN(=Convolutional Neural Network (ConvNet/CNN)), η οποία είναι πολύ αποτελεσματική για μη ευθυγραμμισμένες επιθέσεις τροχιάς, και χρησιμοποιεί δύο αλγόριθμους για τεχνικές βελτίωσης δεδομένων για την αποφυγή ελλειμμάτων μάθησης και υπερβολικής προσαρμογής στη μαθησιακή διαδικασία.

Ο Houssem Maghrebi συνέκρινε τις δομές δικτύου σε MLP, RF, CNN και RNN με το παραδοσιακό TA(=Threshold Algorithm) και τις ταξινόμησε σε προστατευμένες και μη προστατευμένες επιθέσεις AES. Διαπίστωσαν ότι το LSTM(=Long short-term memory) είχε καλή απόδοση στο να σπάσει τον αλγόριθμο κρυπτογράφησης AES με βάση το Chipwhisper και ότι το αποτέλεσμα του unprotected AES που επιτεύχθηκε από το FPGA ήταν χειρότερο από το CNN και το MLP. Όταν σπάει ο with protection AES, η DL(=Deep Leraning) είναι γενικά καλύτερη από τον RF(=Random forest) και το MLP. Αποδεικνύει ότι όταν οι διαρροές λογισμικού σχετίζονται στενά με το χρόνο και οι οποίες μπορούν να επιτύχουν υψηλότερες αναλογίες σήματος προς θόρυβο, ο αντίπαλος μπορεί να δώσει προτεραιότητα στη χρήση του RNN(=Recurrent neural network). Αυτό παρέχει επίσης ένα μοντέλο για την έρευνά μας από CNN έως RNN.

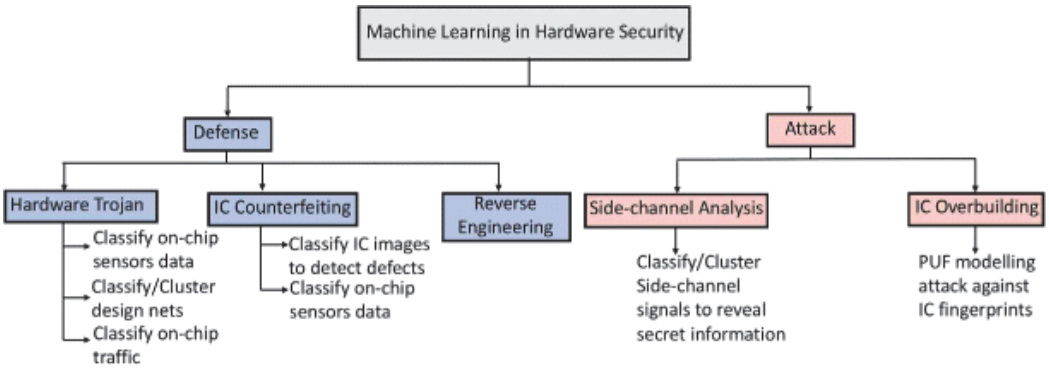
Ο Ιωάννης Πέτρος Σαμιώτης βελτιστοποίησε το ονομαζόμενο SCA-net για τη δομή CNN που χρησιμοποιήθηκε στο διαγωνισμό DPA v2 και v4 αναλύοντας τις αδυναμίες των εφημερίδων Cagli και Maghrebi. Το SCA-Net που αναφέρεται αποτελείται από 4 συνελικτικά στρώματα και 4 ενδιάμεσα στρώματα συγκέντρωσης, ακολουθούμενο από ένα στρώμα ταξινόμησης. Όλοι οι συνελικτικοί πυρήνες έχουν έναν πυρήνα μεγέθους 6 και κάθε επίπεδο περιέχει πολλαπλές λειτουργίες ενεργοποίησης. Στο πείραμα, συγκρίθηκαν οι αρχιτεκτονικές SCA -net και Maghrabi et al CNN για να αποδειχθεί ότι το βελτιστοποιημένο αποτέλεσμα SCA-net είναι καλύτερο.

Προκειμένου να κατασκευαστεί ένα γενικό πλαίσιο για τη μελέτη και τη σύγκριση της αποτελεσματικότητας των μεθόδων μηχανικής μάθησης και των ενσωματωμένων κρυπτογραφικών αλγορίθμων, οι Ryad Benadjila και Emmanuel Prouff συνέκριναν τα μαθησιακά αποτελέσματα των VGG-16(=Visual Geometry Group) και MLP στη μοντελοποίηση και διαπίστωσαν ότι το VGG-16 είχε καλύτερη απόδοση, ειδικά για συσκευές κρυπτογράφησης με πρόσθετη κάλυψη (additional cover). Και παρείχαν ένα ορόσημο για τις υπερπαραμέτρους και δημιούργησαν μια νευρωνική network-based side channel attack ASCAD(=Advanced Security Consulting Alarm Division) βάση δεδομένων στην οποία καθιερώθηκε μια νέα μεθοδολογική βάση για μηχανική μάθηση στον τομέα των επιθέσεων πλευρικών καναλιών.

Ο Benjamin Timon πρότεινε επίσης βελτιώσεις στις παραδοσιακές επιθέσεις πλαϊνού καναλιού χωρίς μοντελοποίηση με βάση τις παραπάνω τρεις εφαρμογές της μοντελοποίησης DL στο SCA

Χρησιμοποιεί τις μεθόδους MLP και CNN για να συγκρίνει το CPA και το CPA υψηλής τάξης σε περίπτωση προστατευτικής επίθεσης. Η DL πέτυχε ένα καλό αποτέλεσμα.

4.3 Overbuilding Ολοκληρωμένων Κυκλωμάτων



Εικόνα 18: Οι επιθέσεις υλικού βασισμένες σε μεθόδους Μηχανικής Μάθησης διακρίνονται σε πλευρικού καναλιού και IC overbuilding

Οι πειρατείες IP και οι επιθέσεις overbuilding αναφέρονται σε περιπτώσεις, όπου ένας χρήστης ή / και μία foundry, στους οποίους παρέχεται πρόσβαση στην IP, κάνουν καταχρηστική χρήση και πειρατεία της IP για να κατασκευάσουν περισσότερα ICs περισσότερα από αυτά που εντάλθηκε ο κατόχος IP (κάτοχος δικαιωμάτων). Οι στόχοι αυτής της επίθεσης μπορεί να είναι η κλοπή του IP σχεδιασμού και η ανίχνευση του εμπορικού μυστικού (trade secret). Σε μια άλλη περίπτωση, ο αρχικός σχεδιασμός ή / και το στοιχείο, π.χ. το IC, μπορεί να πλαστογραφηθεί ή να αναπαραχθεί από έναν αντίπαλο, με σκοπό να υποκλέψει τις ευαίσθητες πληροφορίες, να τροποποιήσει τη λειτουργικότητα του IC, να προσαρμόσει τις επιθέσεις άρνησης υπηρεσίας και να μειώσει την αξιοπιστία του IC. Αυτές οι επιθέσεις μπορούν να ξεκινήσουν σε όλες σχεδόν τις φάσεις της αλυσίδας εφοδιασμού IC.

Εκτός από το τεράστιο κόστος και τις απώλειες (π.χ. απώλεια φήμης) για τον κατασκευαστή IC, τέτοιες επιθέσεις μπορούν να επηρεάσουν τον τελικό χρήστη είτε αυτός είναι η κυβέρνηση, μια βιομηχανία, επιχειρήσεις ή απλοί καταναλωτές. Για την μείωση ή την πρόληψη αυτών των ανεπιθύμητων ενεργειών, πρέπει να χρησιμοποιούνται μηχανισμοί για τη διάκριση μεταξύ ενός overbuilt IC (=παραχθέν πάνω από τον επιθυμητό αριθμό) και ενός πραγματικού (= κατασκευασμένο μέσα στα όρια που έχει θέσει ο IP owner).

Τα PUFs (Physical Unclonable Function) - υλικό για την παραγωγή κλειδιών- χρησιμοποιούνται συνήθως για τοποθέτηση δακτυλικών αποτυπωμάτων στα IC τα οποία βασίζονται σε φυσικά χαρακτηριστικά που είναι μοναδικά για το κάθε IC και επομένως είναι δύσκολο να αναπαραχθούν. Ωστόσο, τα μοντέλα μηχανικής μάθησης τελευταία έχουν εκπαιδευτεί για να μάθουν τη

συμπεριφορά των PUF. Χρησιμοποιούνται διάφορα ζεύγη πρόκλησης-απόκρισης (Challenge-Response Pairs - CRPs) για την εκπαίδευση αυτών των μοντέλων. Τα μοντέλα μηχανικής μάθησης έχουν αποδειχθεί αποτελεσματικά στη μοντελοποίηση των ταλαντωτών δακτυλίου και των κριτών PUF. Οι εξελικτικές στρατηγικές, οι στρατηγικές ανάλυσης παλινδρόμησης και των SVM χρησιμοποιούνται για την κλωνοποίηση του κριτή, του ταλαντωτή δακτυλίου, του διαχωριστή XOR, και για την ασφάλεια σε χαμηλό επίπεδο του PUF, αλλά και την ανατροφοδότησή του. Τα ζεύγη πρόκλησης - απόκρισης με βάση την καθυστέρηση χρησιμοποιούνται για την εκπαίδευση των μοντέλων. Οι προκλήσεις λειτουργούν ως χαρακτηριστικά εισόδου και η αντίστοιχη απόκριση λειτουργεί ως τελική έξοδος του μοντέλου. Ο αλγόριθμος AdaBoost χρησιμοποιείται για την πρόβλεψη της απόκρισης των Bistable Ring PUFs (BR-PUFs) και του Twisted Bistable Ring PUFs (TBR-PUFs). Στην συνέχεια το νευρικό δίκτυο στο οποίο διοχετεύονται τους επιτρέπει να δημιουργήσουν πολλές εικόνες «ψεύτικων» αποτυπωμάτων που μοιάζουν πειστικά με τα πραγματικά ξεγελώντας έναν σαρωτή ή μια οπτική επιθεώρηση.

5. Συμπεράσματα

Όπως αναφέρθηκε παραπάνω, θεωρούμε την κακόβουλη χρήση της μηχανικής μάθησης ως εφαρμογή μοντέλων μηχανικής μάθησης στην επίθεση κάποιου στόχου. Κατανοώντας ότι η μηχανική μάθηση παρέχει άνευ προηγουμένου αναλυτική δύναμη, μπορεί να χρησιμοποιηθεί από έναν αντίπαλο τόσο εύκολα όσο ένας καλός ηθοποιός. Ωστόσο, παρατηρούμε επίσης ότι αυτή η συγκεκριμένη στρατηγική είναι εντελώς νέα, και ναι μεν υπάρχουν λίγα παραδείγματα αυτού του μηχανισμού στην έρευνα αλλά πολλά στην πράξη. Από τα αποτελέσματα της επίθεσης στο υλικό, η μηχανική μάθηση μπορεί να αποκτήσει τα καλύτερα μέσα επίθεσης για ένα συγκεκριμένο σύστημα. Επίσης στο στάδιο της αποφυγής, ο κακόβουλος μπορεί να αποκρύψει τις ενέργειες επίθεσης χρησιμοποιώντας προγράμματα μηχανικής μάθησης, όπως χειρισμό της στρατηγικής άμυνας του συστήματος ή αναπαραγωγή νόμιμων δραστηριοτήτων.

6. Αναφορές

[1] Elnaggar, R., Chakrabarty, K., "Machine Learning for Hardware Security: Opportunities and Risks". J Electron Test 34, 183–201 (2018): https://link.springer.com/article/10.1007/s10836-018-5726-9

[2] Sperling E., "Security Holes In Machine Learning And AI", Semiconductor Engineering:https://semiengineering.com/security-holes-in-machine-learning-and-ai/

[3] Z. Huang, Q. Wang, Y. Chen and X. Jiang, "A Survey on Machine Learning Against Hardware Trojan Attacks: Recent Advances and Challenges," in IEEE Access, vol. 8, pp. 10796-10826, 2020.

[4] Huang, Zhao & Wang, Quan & Chen, Yin & Jiang, Xiaohong. (2020). "A Survey on Machine Learning against Hardware Trojan Attacks: Recent Advances and Challenges." IEEE Access. PP. 1-1: https://www.researchgate.net/publication/338467645_A_Survey_on_Machine_Learning_against_Hardware_Trojan_Attacks_Recent_Advances_and_Challenges

[5] Li, H., Q. Liu, Jiliang Zhang and Y. Lyu. "A Survey of Hardware Trojan Detection, Diagnosis and Prevention.", 2015 14th International Conference on Computer-Aided Design and Computer Graphics (CAD/Graphics) (2015): 173-180: https://www.semanticscholar.org/paper/A-Survey-of-Hardware-Trojan-Detection%2C-Diagnosis-Li-Liu/1755770e538b3dcc60bd0fd1697a768a380d9804

[6] Bizarro P., "Machine learning innovations for fighting financial crime in an Open Banking era", IT Magazine: https://itmagazineme.com/index.php/2019/09/21/machine-learning-innovations-for-fighting-financial-crime-in-an-open-banking-era/

[7] Dong, Chen, J. Chen, Wenzhong Guo and J. Zou. "A machine-learning-based hardware-Trojan detection approach for chips in the Internet of Things.", International Journal of Distributed Sensor Networks 15 (2019): https://www.semanticscholar.org/paper/A-machine-learning-based-hardware-Trojan-detection-Dong-Chen/67114eee5f3b1ae858e60c948819f60abee783c4

[8] Williams M., "Engineers develop methods for AI bottlenecks with machine-learning algorithms", Control Engineering, June 2020: https://www.controleng.com/articles/engineers-develop-methods-for-ai-bottlenecks-with-machine-learning-algorithms/

[9] Harris B., "Factorization Machines: A New Way of Looking at Machine Learning", Security Intelligence, November 2015: https://securityintelligence.com/factorization-machines-a-new-way-of-looking-at-machine-learning/

[10] Walsh S., "Exabeam to Use Machine Learning to Tackle IoT Device Security", RT Insights, March 2018: https://www.rtinsights.com/exabeam-to-use-machine-learning-to-tackle-iot-device-security/

[11] Theodoridis S., "Machine Learning: A Bayesian and Optimization Perspective" (1st. ed.). Academic Press, Inc., USA, 2015.

[12] Wikipedia, "Data mining": https://en.wikipedia.org/wiki/Data_mining

[13] "Knowledge Discovery in Databases", August 2017: https://www.techopedia.com/definition/25827/knowledge-discovery-in-databases-kdd

[14] Wikipedia, "Artificial Intelligence": https://en.wikipedia.org/wiki/Artificial_intelligence

[15] Guru 99, "Supervised vs Unsupervised Learning: Key Differences": https://www.guru99.com/supervised-vs-unsupervised-learning.html

[16] Brownlee J., "A Tour of Machine Learning Algorithms", Machine Learning Mastery, August 2019: https://machinelearningmastery.com/a-tour-of-machine-learning-algorithms/

[17] Zamani, M. "Machine Learning Techniques for Intrusion Detection", 2013.

[18] Bettaieb, Seifeddine, Seung Yeob Shin, M. Sabetzadeh, L. Briand, Grégory Nou and Michael Garceau, 2019: "Decision Support for Security-Control Identification Using Machine Learning".

[19] Dickson B., "How IoT security can benefit from machine learning", Techrunch, April 2016: https://techcrunch.com/2016/04/22/how-iot-security-can-benefit-from-machine-learning/

[20] Akinsola J. E. T., "Supervised Machine Learning Algorithms: Classification and Comparison". International Journal of Computer Trends and Technology (2017). 48. 128 - 138.

[21] Software Testing Help, "Types Of Machine Learning: Supervised Vs Unsupervised Learning", September 2020: https://www.softwaretestinghelp.com/types-of-machine-learning-supervised-unsupervised/

[22] Taranenko L., "Unsupervised Machine Learning to improve data quality": https://mobidev.biz/blog/unsupervised-machine-learning-improve-data-quality

[23] Wikipedia, "Dimensionality reduction": https://en.wikipedia.org/wiki/Dimensionality_reduction#Dimension_reduction

[24] Readthedocs.io, "Benchmarking Performance and Scaling of Python Clustering Algorithms":

https://hdbscan.readthedocs.io/en/latest/performance_and_scalability.html#comparison-of-fast-implementations

[25] Wikipedia, "Anomaly detection": https://en.wikipedia.org/wiki/Anomaly_detection

[26] Wikipedia, "Association rule learning": https://en.wikipedia.org/wiki/Association_rule_learning

[27] Fu, C., Wang, X., Zhang, L., and Qiao, L., “Mining algorithm for association rules in big data based on Hadoop”, in "Advances in Materials, Machinery, Electronics II", 2018, vol. 1955, no. 1.

[28] Khadse V., Mahalle P. N., Biraris, S. V. "An Empirical Comparison of Supervised Machine Learning Algorithms for Internet of Things Data", 2018 Fourth International Conference on Computing Communication Control and Automation, Pune, India, 2018, pp. 1-6.

[29] Hassan C. A. Ul, Khan M. S., Shah M. A., "Comparison of Machine Learning Algorithms in Data classification", 2018 24th International Conference on Automation and Computing, Newcastle upon Tyne, United Kingdom, 2018, pp. 1-6.

[30] De Hoz Diego J. D., Saldana J., Fernández-Navajas J., Ruiz-Mas J., "IoTsafe, Decoupling Security From Applications for a Safer IoT," IEEE, vol. 7, pp. 29942-29962, 2019.

[31] "IoT Developer Survey", Eclipse IoT Working Group, IEEE IoT, AGILE IoT. (2017): https://ianskerrett.wordpress.com/2017/04/19/iot-developer-trends-2017-edition/

[32] "IoT Developer Survey", Eclipse IoT Working Group, IEEE IoT, AGILE IoT. (2016): https://iot.ieee.org/images/files/pdf/iot-developer-survey-2016-report-final.pdf

[33] Becker G. T., "The gap between promise and reality: On the insecurity of XOR arbiter PUFs," in Proc. Conf. Cryptograph. Hardw. Embedded Syst. (CHES). Saint Malo, France, Sep. 2015, pp. 535–555.

[34] Bellman C., Oorschot P., "Analysis, Implications, and Challenges of an Evolving Consumer IoT Security Landscape", School of Computer Science, Carleton University, Ottawa, Canada, 2019, pp.1-7.

[35] R. Sandip, B. Abhishek, B. Swarup, "To Secure the Internet of Things, We Must Build It Out of “Patchable” Hardware", IEEE Sptectrum, October 2017: https://spectrum.ieee.org/telecom/security/to-secure-the-internet-of-things-we-must-build-it-out-of-patchable-hardware

[36] R. Sagar, R. Jhaveri, C. Borrego, "Applications in Security and Evasions in Machine Learning: A Survey", 2020. Electronics. 9. 97.

[37] Huang Z., Wang Q., Chen Y., Jiang X., Xiaohong, "A Survey on Machine Learning Against Hardware Trojan Attacks: Recent Advances and Challenges". IEEE Access, 2020, PP. 1-31.

[38] P. Prinetto, and G. Roascio, "Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy." ITASEC (2020).

[39] Wikipedia, Spectre: https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)

[40] Wikipedia, Meltdown: https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)

[41] D. Forte, "Design and Fabrication of Physically Unclonable Functions (PUFs), True Random Number Generators (TRNGS), and Other Hardware Security Primitives", Florida & FICS Research: https://dforte.ece.ufl.edu/research/hardware-security-primitives/

[42] Shijie Song et al “Overview of Side Channel Cipher Analysis Based on Deep Learning” Research: https://iopscience.iop.org/article/10.1088/1742-6596/1213/2/022013/pdf