ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΚΑΙ ΕΥΦΥΗ ΠΕΡΙΒΑΛΛΟΝΤΑ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια και Προστασία Ιδιωτικότητας Οικιακών Συσκευών που Λειτουργούν σε Περιβάλλον ΔτΠ

Μεταπτυχιακός Φοιτητής: Σταύρος Μάρας, msciot18003

Επιβλέπων: Χαράλαμπος Ζ. Πατρικάκης Καθηγητής, Πανεπιστήμιο Δυτικής Αττικής, Τμήμα Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών

ΑΙΓΑΛΕΩ, ΙΟΥΛΙΟΣ 2021

UNIVERSITY OF WEST ATTICA

FACULTY OF ENGINEERING

DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Master of Science in

"INTERNET of THINGS AND INTELLIGENT ENVIRONMENTS"

MSc Thesis

Security and Privacy Protection over IoT Enabled Domestic Appliances and Devices

Student: Stavros Maras, msciot18003

MSc Thesis Supervisor: Xaralampos Z. Patrikakis Professor, University of West Attica, Department of Electrical and Electronics Engineering

ATHENS-EGALEO, JULY 2021

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

Χαράλαμπος Ζ. Πατρικάκης Καθηγητής (Επιβλέπων)	Γρηγόριος Καλτσάς Καθηγητής (Μέλος)	Παναγιώτης Παπαγέωργας Καθηγητής (Μέλος)
 Digitally signed by Charalampos Patrikakis Date: 2021.07.27 08:33:18 +03'00'	 Digitally signed by Grigorios Kaltsas Date: 2021.08.03 12:13:23 +03'00'	 Digitally signed by Panagiotis Papageorgas Date: 2021.08.03 10:58:09 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Ο κάτωθι υπογεγραμμένος Μάρας Σταύρος του Γεωργίου, με αριθμό μητρώου msciot18003, φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα 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 όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

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

Ο Δηλών

Μάρας Σταύρος

ΠΕΡΙΛΗΨΗ

Το Διαδίκτυο των Πραγμάτων (ΔτΠ) είναι πλέον μια τεχνολογία που προχωράει σταθερά προς την καθολική της αποδοχή και όροι όπως το έξυπνο σπίτι δεν αποτελούν πλέον σενάριο επιστημονικής φαντασίας, αλλά πραγματικότητα. Οι οικιακές συσκευές και οι εφαρμογές τους, έχουν πλέον εξελιχθεί ώστε να συνδέονται με το οικιακό δίκτυο και να επικοινωνούν με το Διαδίκτυο. Το παραπάνο τις κάνει γνωστές με τον όρο έξυπνες οικιακές συσκευές. Οι έξυπνες οικιακές συσκευές μπορούν να επικοινωνήσουν είτε μεταξύ τους είτε με τον άνθρωπο, αναλύοντας και ανταλλάσσοντας πληροφορίες, χρησιμοποιώντας τα κλασικά πρωτόκολλα επικοινωνίας για την διασύνδεση τους με το οικιακό δίκτυο και το Διαδίκτυο.

Η χρήση της τεχνολογίας ΔτΠ στο πλαίσιο του έξυπνου σπιτιού οδηγεί σε νέες προκλήσεις ασφάλειας και ιδιωτικότητας, καθώς μέσα στο περιβάλλον του ΔτΠ μεταδίδεται τεράστιος όγκος δεδομένων από τις συσκευές. Επομένως, τα έξυπνα σπίτια που βασίζονται στην τεχνολογία του ΔτΠ έχουν απαιτήσεις υψηλού επιπέδου ασφαλείας, καθώς το οικιακό περιβάλλον περιέχει σημαντικές και ιδιωτικές πληροφορίες. Οι σύγχρονες τεχνολογίες μπορεί να προσφέρουν μεγάλες δυνατότητες στους χρήστες, όμως ταυτόχρονα ελλοχεύουν και πολλούς κινδύνους. Ένα έξυπνο σπίτι που βασίζεται στο ΔτΠ είναι πολύ ευάλωτο σε επιθέσεις από το Διαδίκτυο. Στην περίπτωση που το έξυπνο σπίτι ή μια έξυπνη οικιακή συσκευή παραβιαστεί, ο επιτιθέμενος έχει τη δυνατότητα να εισβάλει στο απόρρητο του χρήστη, να υποκλέψει προσωπικά στοιχεία και να παρακολουθεί οτιδήποτε συμβαίνει στο χώρο της οικίας. Για το λόγο αυτό, η λήψη κατάλληλων μέτρων προστασίας είναι κάτι παραπάνω από επιβεβλημένη.

Σε αυτή την εργασίας θα γίνει μελέτη πάνω στη ασφάλειας και την προστασίας της ιδιωτικότητας των οικιακών συσκευών που λειτουργούν σε περιβάλλον ΔτΠ. Για το λόγο αυτό, αρχικά, θα γίνει μια παρουσίαση των έξυπνων οικιακών συσκευών και της δομής επικοινωνίας τους στο έξυπνο σπίτι. Στη συνέχεια, θα γίνει μια ανάλυση των θεμάτων ασφάλειας και ιδιωτικότητας τα οποία μπορεί να υπάρξουν, καθώς και των κυβερνοεπιθέσεων που μπορεί να δεχθούν. Τέλος. θα δοθούν παραδείγματα επιθέσεων σε έξυπνες οικιακές συσκευές σε περιβάλλον ΔτΠ και θα γίνει μια αναφορά στους τρόπους αντιμετώπισης και τις λύσεις των θεμάτων ασφαλείας που έχουν παρουσιαστεί στη βιβλιογραφία.

ΛΕΞΕΙΣ – ΚΛΕΙΔΙΑ: *Ασφάλεια, Διαδίκτυο των Πραγμάτων, έξυπνες οικιακές συσκευές, έξυπνο σπίτι, ιδιωτικότητα, κυβερνοεπίθεση.*

ABSTRACT

Nowadays, Internet of Things (IoT) is a technology that is steadily moving towards universal acceptance. Terms like smart home are no longer a science fiction scenario but a reality. Home appliances and their applications have now evolved to connect to the home network and communicate with the Internet. For this reason, they are known as smart home devices, which can communicate with each other or with humans, analyzing and exchanging information using standard communication protocols to connect to the home network and the Internet.

The use of IoT technology in the context of the smart home leads to new security and privacy challenges, as a huge amount of data is transmitted from the devices within the IoT environment. Therefore, IoT-enabled smart homes have high security requirements, as the home environment contains important and private information. Although, modern technologies can offer great opportunities to users, at the same time they present a serious of risks. An IoT-enabled smart home seems to be very vulnerable to cyber-attacks. In case that a smart home or a smart home devise is compromised, the attacker has the ability to invade the user's privacy, steal personal information and monitor everything that happens in the home. For this reason, taking appropriate protection measures is more than necessary.

The purpose of this paper is to study the security and privacy protection of IoT- enabled smart home devices. For this reason, first, there will be a presentation of smart home devices and their communication architecture in the field of a smart home. Next, an analysis will be made of the security and privacy issues that may arise as well as the cyber-attacks they may undergo. Finally, examples of attacks on IoT-enabled smart home devices will be given and a reference to the security solutions and solutions presented in the literature will be given.

KEYWORDS: *Cyber-attack, Internet of Things, privacy, security, smart home, smart home devices.*

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

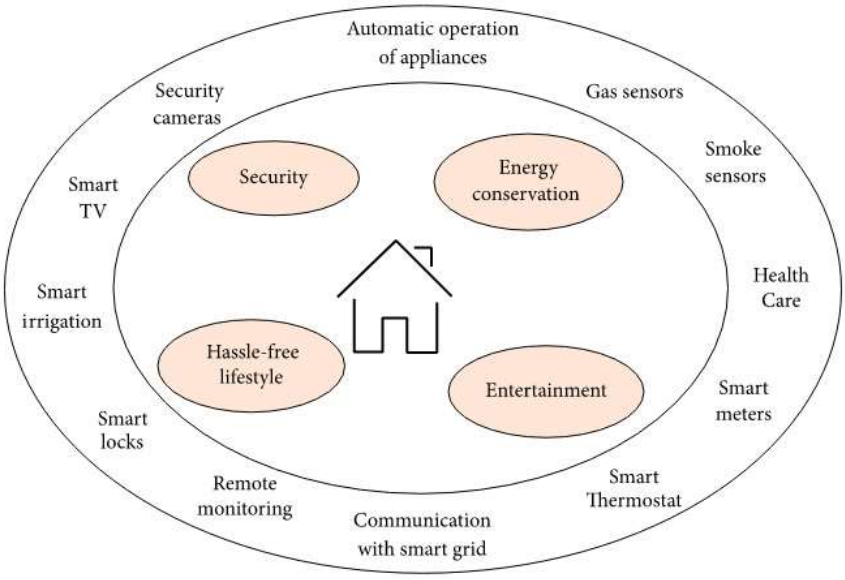
Τα τελευταία χρόνια, το Διαδίκτυο των Πραγμάτων (ΔτΠ) έχει προσελκύσει το έντονο ενδιαφέρον της ακαδημαϊκής και της βιομηχανικής κοινότητας. Θεωρείται ως μέρος του Διαδικτύου του μέλλοντος και θα περιλαμβάνει την ευφυή επικοινωνία μεταξύ δισεκατομμυρίων "πραγμάτων". Αν και μέχρι στιγμής δεν έχει δοθεί ένας ορισμός που να είναι γενικά αποδεκτός, το ΔτΠ μπορεί να θεωρηθεί ως μια παγκόσμια δυναμική δικτυακή υποδομή που έχει τη δυνατότητα να αυτοδιαμορφωνεται, βασίζόμενη σε πρότυπα και διαλειτουργικά πρωτόκολλα επικοινωνίας. Τα φυσικά και τα εικονικά "πράγματα" του ΔτΠ έχουν ταυτότητα και χαρακτηριστικά και μπορούν να χρησιμοποιήσουν έξυπνες διασυνδέσεις για τη δημιουργία ενός δικτύου πληροφοριών [1]. Σκοπός του ΔτΠ είναι η αύξηση των λειτουργιών και της χρησιμότητας του ήδη υφιστάμενου Διαδικτύου. Μέσω του ΔτΠ, οι χρήστες μπορούν να μοιράζονται πληροφορίες που παρέχονται από ανθρώπους, που περιέχονται σε βάσεις δεδομένων αλλά και που παρέχονται από "πράγματα" στον φυσικό κόσμο [2].

Έτσι, το ΔτΠ μπορεί να περιγραφεί ως η σύνδεση των φυσικών "πραγμάτων" με το Διαδίκτυο, αλλά και μεταξύ τους, μέσω διαφορετικών ευφυών τεχνολογιών, δημιουργώντας ένα έξυπνο οικοσύστημα διάχυτου υπολογισμού (pervasive computing) [3]. Βάσει της έννοιας του ΔτΠ, υπολογιστές, αισθητήρες και αντικείμενα αλληλοεπιδρούν μεταξύ τους και επεξεργάζονται δεδομένα, δημιουργώντας ένα νέο τεχνολογικό σύστημα που συνδυάζει έναν αριθμό τεχνολογιών πληροφοριών. Σε ένα δίκτυο ΔτΠ περιλαμβάνονται και συστήματα ελεγκτών (λογισμικό και υπηρεσίες) που έχουν ως σκοπό την επεξεργασία δεδομένων, κάνοντας ανάληση και συλλογή των δεδομένων από τις συσκευές που είναι διασυνδεμένες, για τη λήψη αποφάσεων και την έναρξη ενεργειών από τις ίδιες ή από άλλες συσκευές [4].

Η ακαδημαϊκή και βιομηχανική έρευνα πάνω στον τομέα του ΔτΠ έχει δημιουργήσει μια τεράστια γκάμα εφαρμογών, όπως ο έξυπνος χώρος στάθμευσης, ο έξυπνος φωτισμός, το έξυπνο ηλεκτρικό δίκτυο, οι εφαρμογές M2M και η έξυπνη υγειονομική περίθαλψη [5]. Μια από τι πιο βασικές και σημαντικές εφαρμογές στο ΔτΠ είναι το έξυπνο σπίτι, το οποίο καταφέρνει να συνδιάσει την ενσωμάτωση τεχνολογιών και υπηρεσιών μέσα από το οικιακό δίκτυο, έχοντας την ικανοτητα να αποκρίνονται στις απαιτήσεις των ενοίκων, παρέχοντας τους άνεση, ασφάλεια και ψυχαγωγία. Το έξυπνο σπίτι σαν ιδέα υπάρχει εδώ και πολλά χρόνια, το τελευταίο διάστημα όμως έχει τραβήξει τα βλέμματα της επιστημονικής κοινότητας πάνω του, καθώς αναπτύσσεται και εξελίσσεται μέσα από το περιβάλλον του ΔτΠ. Έχει σαν βάση του τη λογική της αλληλεπίδρασης και επικοινωνίας όλων των έξυπνων οικιακών συσκευών μεταξύ τους, αλλά και με τον άνθρωπο-χρήστη [6].

Ένα έξυπνο σπίτι είναι εξοπλισμένο με προηγμένα αυτόματα συστήματα για διάφορες προγραμματισμένες λειτουργίες και εργασίες, όπως έλεγχο θερμοκρασίας, φωτισμού, λειτουργίας παραθύρων και πορτών κ.λπ. [7]. Το σύνολο των έξυπνων οικιακών συσκευών σε ένα σπίτι αλληλοεπιδρά μέσα στο περιβάλλον του ΔτΠ. Τέτοιες συσκευές μπορεί να είναι ψυχαγωγίας (έξυπνη τηλεόραση, έξυπνο στερεοφωνικό κλπ.), ασφαλείας (έξυπνες κλειδαριές, έξυπνοι συναγερμοί, έξυπνες πόρτες ή παράθυρα, κλπ.) ή άλλες καθημερινές οικιακές συσκευές (έξυπνα πλυντήρια ρούχων, έξυπνα κλιματιστικά, έξυπνες κουζίνες, έξυπνοι θερμοστάτες κλπ.). Χρησιμοποιούν αισθητήρες οι οποίοι συλλέγουν πληροφορίες από την ίδια τη συσκευή ή το περιβάλλον και επικοινωνούν με τις υπόλοιπες συσκευές μέσω

του οικιακού δικτύου ή απομακρυσμένα μέσω του Διαδικτύου, με σκοπό να βελτιώσουν τη εμπειρία του χρήστη, παρέχοντας του άνεση, εργονομία και ασφάλεια. Το έξυπνο οικιακό περιβάλλον είναι σε θέση να παρέχει πολλά οφέλη στους ενοίκους του, όπως αυξημένη άνεση, μεγαλύτερη ασφάλεια και προστασία, καθώς και μια πιο ορθολογική χρήση και κατανάλωση ενέργειας και άλλων πόρων, συμβάλλοντας έτσι σε σημαντική εξοικονόμηση (Εικ.1) [8].

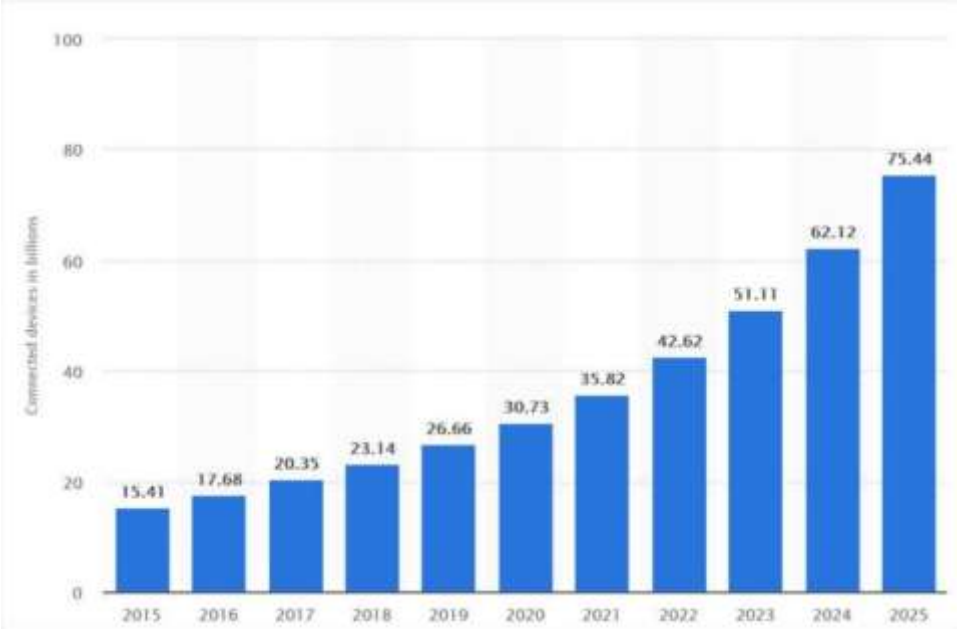


Εικόνα 1: Έξυπνο οικιακό περιβάλλον και σκοποί [8]

Τα περισσότερα από τα διαθέσιμα εμπορικά συστήματα οικιακού αυτοματισμού μπορούν να χωριστούν σε δύο κατηγορίες [9]: τοπικά ελεγχόμενα συστήματα και απομακρυσμένα ελεγχόμενα συστήματα. Τα τοπικά ελεγχόμενα συστήματα χρησιμοποιούν έναν ελεγκτή εντός του σπιτιού, με σκοπό την επίτευξη οικιακού αυτοματισμού, επιτρέποντας στους χρήστες πλήρη χρήση του μέσα από το σπίτι τους, μέσω σταθερής ή ασύρματης διεπαφής. Τα απομακρυσμένα ελεγχόμενα συστήματα χρησιμοποιούν διαδικτυακή σύνδεση ή ενοποίηση με το υπάρχον οικιακό σύστημα ασφαλείας, επιτρέποντας στους χρήστες πλήρη έλεγχο του συστήματος μέσω υπολογιστή ή κινητής συσκευής. Ένα σύστημα έξυπνου οικιακού αυτοματισμού αποτελείται από τρία βασικά μέρη [10]: (α) τον φυσικό εξοπλισμό (ηλεκτρονικός εξοπλισμός - έξυπνοι αισθητήρες και ενεργοποιητές), (β) το σύστημα επικοινωνίας (ενσύρματο / ασύρματο δίκτυο), που συνδέει συνήθως τον φυσικό εξοπλισμό και (γ) το έξυπνο σύστημα επεξεργασίας πληροφοριών (π.χ. μέσω προγραμμάτων τεχνητής νοημοσύνης), για τη διαχείριση και τον έλεγχο του έξυπνου οικιακού συστήματος.

Η χρήση της τεχνολογίας ΔτΠ στο πλαίσιο του έξυπνου σπιτιού οδηγεί σε νέες προκλήσεις ασφάλειας και ιδιωτικότητας, καθώς μέσα στο περιβάλλον του ΔτΠ μεταδίδεται τεράστιος όγκος δεδομένων από τις συσκευές. Πρέπει να αναφέρουμε πως μέχρι το τέλος του 2020, οι έξυπνες συσκευές αναμένεται να έχουν φτάσει τα 31 δισεκατομμύρια περίπου παγκοσμίως, δείχνοντας την ευρεία χρήση πλέον του ΔτΠ (Εικ. 2) [11]. Επομένως, τα έξυπνα σπίτια που βασίζονται στην τεχνολογία του ΔτΠ έχουν απαιτήσεις υψηλού επιπέδου ασφαλείας, καθώς το οικιακό περιβάλλον περιέχει σημαντικές και ιδιωτικές πληροφορίες. Οι σύγχρονες τεχνολογίες μπορεί να προσφέρουν μεγάλες δυνατότητες στους χρήστες, όμως ταυτόχρονα ελλοχεύουν και πολλούς κινδύνους. Ένα έξυπνο σπίτι που βασίζεται στο ΔτΠ είναι πολύ ευάλωτο σε επιθέσεις από το Διαδίκτυο. Στην περίπτωση που το έξυπνο σπίτι ή μια έξυπνη οικιακή συσκευή παραβιαστεί, ο επιτιθέμενος έχει τη δυνατότητα να εισβάλει στο απόρρητο

του χρήστη, να υποκλέψει προσωπικά στοιχεία και να παρακολουθεί οτιδήποτε συμβαίνει στο χώρο της οικίας. Για το λόγο αυτό, η λήψη κατάλληλων μέτρων προστασίας είναι κάτι παραπάνω από επιβεβλημένη [12].



Εικόνα 2: Εξελικτική πορεία των έξυπνων συσκευών στο περιβάλλον ΔτΠ [11]

Όπως αναφέρθηκε, το ΔτΠ συνδυάζει πολλές τεχνολογίες υλοποίησης και επικοινωνίας για την επίτευξη του στόχου, έχοντας ως αποτέλεσμα να αυξάνει η δυσκολία ανάλυσης των θεμάτων ασφαλείας του. Επίσης, τεχνολογίες όπως οι Wi-Fi, 3G, 4G, LTE αλλά και τεχνολογίες ασύρματων δικτύων αισθητήρων-ενεργοποιητών (WSAN) ή ραδιοσυχνότητας πιστοποίησης (RFID) εφαρμόζονται κατά κόρων στο ΔτΠ. Η χρήση όμως όλων αυτών των διαφορετικών τεχνολογιών έχει ως αποτέλεσμα και τη μεταφορά των κενών ασφαλείας και των ευπαθειών τους στην τεχνολογία ΔτΠ. Συνεπώς η μελέτη πάνω στην ασφάλεια, την ιδιωτικότητα και την προστασία των δεδομένων γίνεται σαφώς πιο δύσκολη. Τα κενά που υπάρχουν και οι ευπάθειες των συστημάτων προσελκύουν μεγάλη γκάμα κυβερνοεπιθέσεων από κακόβουλους χρήστες και λογισμικά. Ο βασικός προβληματισμός που υπάρχει σχετίζεται με την ιδιωτικότητα και την προστασία των δεδομένων από επίσημους φορείς και εταιρείες που διαχειρίζονται τα δεδομένα. Οι μελέτες και αναφορές που έχουν γίνει από εταιρείες και ερευνητές έχουν δείξει πως παρά την ευρεία διάδοση του ΔτΠ, τα κενά ασφαλείας που αντιμετωπίζει επηρεάζουν σημαντικά την άποψη των χρηστών, κλονίζοντας την εμπιστοσύνη τους και κάνοντάς τους επιφυλακτικούς απέναντι στην εξέλιξη της τεχνολογίας [13].

Η εργασία θα ασχοληθεί με τη μελέτη της ασφάλειας και της προστασίας της ιδιωτικότητας πάνω σε οικιακές συσκευές που λειτουργούν σε περιβάλλον ΔτΠ. Για το λόγο αυτό, αρχικά γίνεται μια αναφορά στις έξυπνες οικιακές συσκευές που απαρτίζουν ένα έξυπνο σπίτι και λειτουργούν σε περιβάλλον ΔτΠ. Στη συνέχεια, αναλύονται τα θέματα ασφάλειας, ιδιωτικότητας και προστασίας των δεδομένων που μπορούν να παρατηρηθούν κατά την επικοινωνία των συγκεκριμένων συσκευών, αλλά και των χρηστών γενικότερα στο περιβάλλον του ΔτΠ. Έπειτα, γίνεται κατηγοριοποίηση και ανάλυση των κυβερνοεπιθέσεων που μπορούν να δεχτούν αυτές οι συσκευές. Για καλύτερη εικόνα του τρόπου υλοποίησης και πραγματοποίησης τέτοιων κυβερνοεπιθέσεων, παρατίθενται παραδείγματα επιθέσεων εις βάρος έξυπνων οικιακών συσκευών στο περιβάλλον ΔτΠ. Τέλος, αναφέρονται λύσεις και τρόποι αντιμετώπισης των κυβερνοεπιθέσεων ώστε να περιοριστούν τα θέματα που

επηρεάζουν την ασφάλεια και αξιοπιστία του περιβάλλοντος ΔτΠ, κάνοντας τους χρήστες επιφυλακτικούς απέναντι του.

Για την συγγραφή της παρούσας εργασίας θα γίνει ως επί το πλείστο βιβλιογραφική ανασκόπηση. Η αναζήτηση της σχετικής βιβλιογραφίας θα γίνει με τη χρήση γνωστών βάσεων δεδομένων όπως: PubMed, Google Scholar, Google. Επίσης θα γίνει χρήση και αναφορά πληροφοριών από σχετικές μελέτες, πηγές του Διαδικτύου και άρθρα.

Η διάρθωση της μεταπτυχιακής εργασίας, για την μελέτη της ασφάλειας και της προστασίας της ιδιωτικότητας των οικιακών συσκευών που λειτουργούν σε περιβάλλον ΔτΠ είναι η παρακάτω:

Στο κεφάλαιο 1: "Έξυπνες οικιακές συσκευές και πρωτόκολλα επικοινωνίας", γίνεται αναφορά της δομής του περιβάλλοντος μέσα στο οποίο υπάρχουν και λειτουργούν οι έξυπνες οικιακές συσκευές καθώς και των πρωτοκόλλων επικοινωνίας τους στο πλαίσιο του ΔτΠ.

Στο κεφάλαιο 2: "Θέματα ασφαλείας και ιδιωτικότητας των έξυπνων οικιακών συσκευών στο περιβάλλον ΔτΠ", παρουσιάζεται μια ανάλυση της γενικής αρχιτεκτονικής του περιβάλλοντος ΔτΠ, καθώς και των θεμάτων ασφαλείας και ιδιωτικότητας που αντιμετωπίζουν οι έξυπνες συσκευές σε ένα τέτοιο περιβάλλον.

Στο κεφάλαιο 3: "Ανάλυση και κατηγοριοποίηση των κυβερνοεπιθέσεων", γίνεται μια ανάλυση του τύπου των επιθέσεων και παρουσιάζεται μια κατηγοριοποίησή τους με βάση τους τομείς που μπορούν να εξαπολυθούν στο περιβάλλον του ΔτΠ.

Στο κεφάλαιο 4: "Παραδείγματα κυβερνοεπιθέσεων", γίνεται αναφορά σε πραγματικές επιθέσεις που έχουν συμβεί και σε κενά ασφαλείας που έχουν εντοπιστεί. Η αναφορά αυτή περιλαμβάνει επαληθευμένες επιθέσεις, δηλαδή πραγματικά περιστατικά ή επιθέσεις που έχουν εφαρμοστεί και δημοσιευτεί από μελετητές.

Στο κεφάλαιο 5: "Λύσεις και αντιμετώπιση", γίνεται αναφορά στις λύσεις που υπάρχουν και στους τρόπους αντιμετώπισης των κυβερνοεπιθέσεων.

Εν κατακλείδι στο κεφάλαιο 6: "Συμπεράσματα-Προτάσεις", η εργασία θα ολοκληρωθεί βγάζοντας κάποια συμπεράσματα που προκύπτουν από την μελέτη της ασφάλειας και της προστασίας της ιδιωτικότητας των οικιακών συσκευών που λειτουργούν σε περιβάλλον ΔτΠ.

ΚΕΦΑΛΑΙΟ 1

Έξυπνες Οικιακές Συσκευές & Πρωτόκολλα Επικοινωνίας

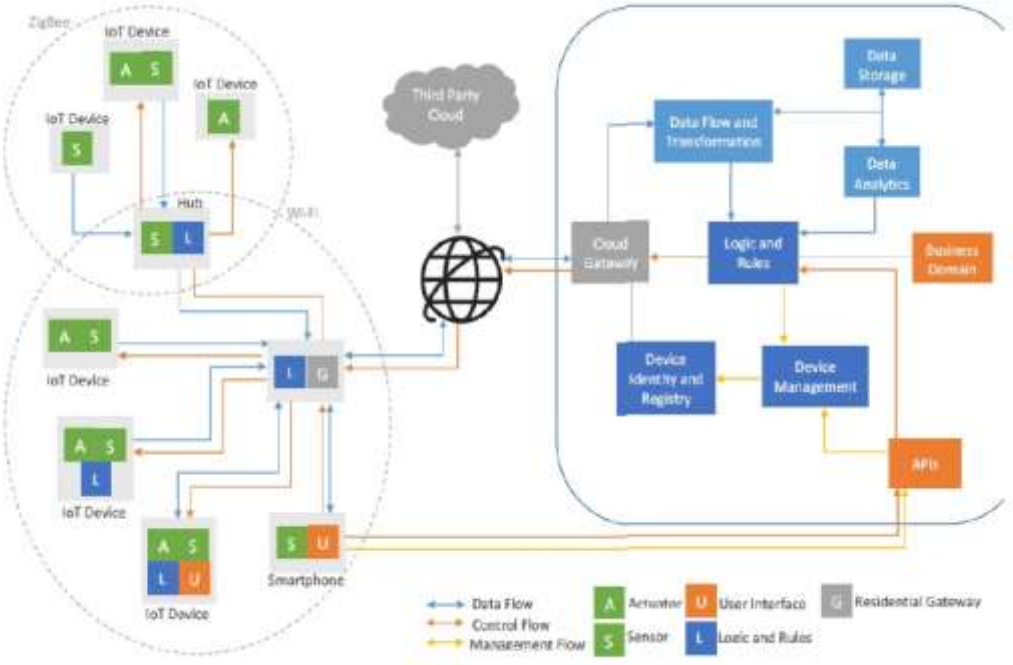
Σε ένα έξυπνο σπίτι, τα στοιχεία τα οποία του προσδίδουν το χαρακτηριστικό της "ευφυΐας", είναι οι έξυπνες οικιακές συσκευές οι οποίες μπορεί να είναι αισθητήρες, ενεργοποιητές, δίαυλοι ή και απλές κοινές συσκευές με ενσωματωμένους αισθητήρες και ενεργοποιητές. Η δομή του δικτύου μέσα από το οποίο γίνεται η επικοινωνία των συσκευών αυτών αποτελεί ένα ακόμη βασικό χαρακτηριστικό του έξυπνου σπιτιού. Επίσης τα πρωτόκολλα επικοινωνίας και οι υπηρεσίες είναι μέρη του δικτύου που παίζουν καθοριστικό ρόλο στη λειτουργία του έξυπνου σπιτιού. Η κατανόηση επομένως των κενών ασφαλείας που υπάρχουν σε ένα έξυπνο σπίτι, προϋποθέτει την παρουσίαση και σχετική ανάλυση της αρχιτεκτονικής δομής του, καθώς και των πρωτοκόλλων επικοινωνίας των έξυπνων συσκευών που το απαρτίζουν.

1.1 Αρχιτεκτονική δομή έξυπνου σπιτιού

Η εφαρμογή των αναδυόμενων τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) στο έξυπνο οικιακό περιβάλλον στοχεύουν στη διευκόλυνση των καθημερινών εργασιών, όπως ο απομακρυσμένος έλεγχος των λειτουργιών του σπιτιού και η διαχείριση της κατανάλωσης ενέργειας. Το έξυπνο σπίτι στο σύνολο του περιλαμβάνει τους αισθητήρες, τις συσκευές και τους ενεργοποιητές, που δεν είναι απαραίτητο να διαθέτουν ευφυΐα. Για να χαρακτηρίσουμε το εν λόγω περιβάλλον ως ευφυές θα πρέπει τα σχετικά δεδομένα να συλλέγονται, να αναλύονται και να αποθηκεύονται μαζικά, έτσι μέσα από αυτή τη διαδικασία να μπορεί να γίνει αντιστοίχιση με συγκεκριμένα μοτίβα ώστε να παίρνονται απόφάσεις, χωρίς να χρειάζεται να επέμβει ο εκάστοτε χρήστης. Το έξυπνο σπίτι έχει μια αρχιτεκτονική η οποία περιλαμβάνει τα παρακάτω: τρόπος επικοινωνίας μεταξύ των συσκευών, το σημείο αποθήκευσης και τον τρόπο με τον οποίο γίνεται η συλλογή των πληροφοριών από τα αισθητήρια όργανα ώστε να αναγνωρίζεται η ρουτίνα χρήσης των συσκευών, την συνολική επεξεργασία αλλά και τον τρόπο που αυτή γίνεται για κάθε πληροφορία που έχει συλλεχθεί ώστε να μπορούν να εξαχθούν μοτίβα και τέλος τον τρόπο που ο ίδιος ο χρήστης μπορεί να έρθει σε επαφή με τις συσκευές κάνοντας μια αμφίδρομη αλληλεπίδραση. [14].

Στην βιβλιογραφία έχουν εμφανιστεί κατά καιρούς διάφορες αρχιτεκτονικές δομές έξυπνων σπιτιών, οι οποίες βασίζονται στην εκάστοτε χρησιμοποιούμενη ΤΠΕ [15]. Αυτή που παρουσιάζει ιδιαίτερο ενδιαφέρον είναι η αρχιτεκτονική δομή των Ghirardello και συν., οι οποίοι χωρίζουν το οικιακό οικοσύστημα που λειτουργεί σε περιβάλλον ΔτΠ, σε τρία βασικά μέρη [13]: τις υπηρεσίες, τις συσκευές και τις συνδέσεις. Με τον τρόπο αυτό η αρχιτεκτονική δομή ενός έξυπνου σπιτιού αποτελείται από: (α) το λειτουργικό τμήμα, (β) το φυσικό τμήμα και (γ) το επικοινωνιακό τμήμα. Το λειτουργικό τμήμα αφορά τις απαραίτητες λειτουργίες και υπηρεσίες που πρέπει να υποστηρίζονται από το έξυπνο σπίτι. Το φυσικό τμήμα περιλαμβάνει όλες τις συσκευές που απαιτούνται για την εκτέλεση των λειτουργιών του έξυπνου σπιτιού. Το επικοινωνιακό τμήμα περιέχει τα πρωτόκολλα που είναι απαραίτητα για τη μετάδοση των ροών ελέγχου και πληροφοριών μεταξύ των συσκευών. Στην εικόνα 3 παρουσιάζεται η συγκεκριμένη αρχιτεκτονική δομή ενός έξυπνου σπιτιού που λειτουργεί σε περιβάλλον ΔτΠ. Η επιλογή της συγκεκριμένης αρχιτεκτονικής δομής έγινε με γνώμονα την ανάλυση των

κινδύνων ασφάλειας και ιδιωτικότητας που μπορούν να απειλήσουν το οικοσύστημα ενός έξυπνου σπιτιού, καθώς μια τέτοια αρχιτεκτονική δομή αναδεικνύει τα τρωτά σημεία ενός έξυπνου σπιτιού πολύ πιο εύκολα. Στις επόμενες ενότητες του κεφαλαίου γίνεται η παρουσίαση αυτών των μερών της αρχιτεκτονικής δομής ενός έξυπνου σπιτιού.



Εικόνα 3: Αρχιτεκτονική δομή έξυπνου σπιτιού που λειτουργεί σε περιβάλλον ΔτΠ [13]

1.2 Λειτουργικό τμήμα

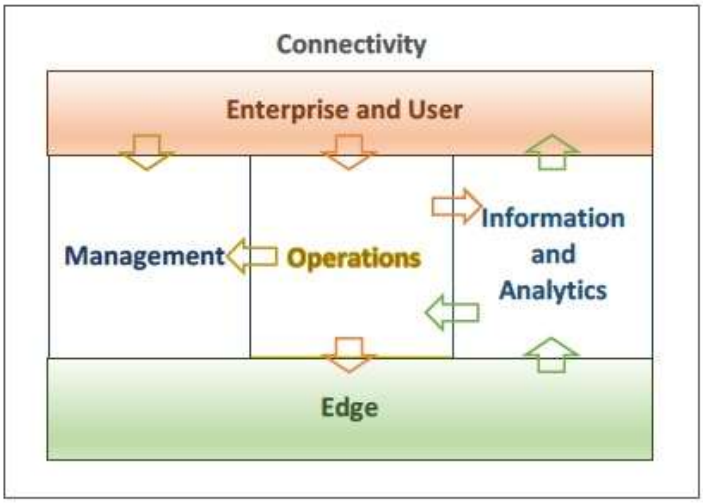
Το λειτουργικό τμήμα ασχολείται με τις λειτουργίες των έξυπνων οικιακών συσκευών στο περιβάλλον ΔτΠ, τη δομή και τις αλληλεπιδράσεις τους. Το δίκτυο ΔτΠ ενός έξυπνου σπιτιού χωρίζεται σε έξι λειτουργικά επίπεδα, καθένα με ένα συγκεκριμένο εύρος δυνατοτήτων, όπως φαίνεται στην εικόνα 4. Στην εικόνα αυτή παρουσιάζονται επίσης οι ροές δεδομένων (πράσινα βέλη), οι ροές ελέγχου (πορτοκαλί βέλη) και οι ροές διαχείρισης (καφέ βέλη) [13]. Κάθε λειτουργικό επίπεδο περιλαμβάνει λειτουργικές μονάδες που εξυπηρετούν πιο συγκεκριμένους σκοπούς, κρίσιμους για το εκάστοτε επίπεδο.

1.2.1 Επίπεδο παρυφών

Το επίπεδο παρυφών (edge layer) παρουσιάζει τις λειτουργίες που επιτρέπουν στις έξυπνες οικιακές συσκευές να αλληλοεπιδρούν με το περιβάλλον τους. Είναι υπεύθυνο για την παρατήρηση του οικιακού περιβάλλοντος, τη δημιουργία δεδομένων και την ανάπτυξη υπηρεσιών σύμφωνα με τις πληροφορίες που εξάγονται από τα δεδομένα. Στο συγκεκριμένο επίπεδο, σημαντικό παράγοντα αποτελεί η λειτουργία των αισθητήρων και των ενεργοποιητών.

Οι αισθητήρες αποτελούν μονάδες hardware υλικού οι οποίες μπορούν να καθορίσουν τις παραμέτρους του γύρω περιβάλλοντός τους και να τις μετατρέψουν σε ψηφιακό σήμα, το οποίο στη συνέχεια υποβάλλεται σε επεξεργασία με σκοπό να γίνει κατανοητή η κατάσταση του εν λόγω περιβάλλοντος. Οι ενεργοποιητές είναι συστατικά του συστήματος ΔτΠ, τα οποία έχουν τη δυνατότητα ελέγχου και διαχείρισης των έξυπνων οικιακών συσκευών με βάση σήματα ελέγχου που λαμβάνουν. Σε ένα έξυπνο δίκτυο, οι αισθητήρες λειτουργούν ως μονάδες εισόδου, συλλέγοντας πληροφορίες για το γύρω περιβάλλον τους, ενώ οι ενεργοποιητές

χρησιμεύουν ως μονάδες εξόδου, εκτελώντας αποφάσεις του συστήματος βάση των πληροφοριών από τους αισθητήρες [16].



Εικόνα 4: Λειτουργικό τμήμα αρχιτεκτονικής δομής έξυπνου σπιτιού [13]

1.2.2 Επίπεδο συνδεσιμότητας

Σκοπός του επιπέδου συνδεσιμότητας (connectivity layer) είναι ο συσχετισμός των έξυπνων οικιακών συσκευών με τις υπηρεσίες νέφους. Από τη στιγμή που οι περισσότερες έξυπνες οικιακές συσκευές στα βασικά τους χαρακτηριστικά περιλαμβάνουν τη μειωμένη ισχύ, την έλλειψη επεξεργαστικής ισχύς και τη μειωμένη μνήμη, όντας δομημένες για την εκτέλεση συγκεκριμένων καθηκόντων, το συγκεκριμένο επίπεδο συνδέει το οικιακό δίκτυο των συσκευών στο Διαδίκτυο, με σκοπό την πρόσβαση στις υπηρεσίες ΔτΠ που βρίσκονται στο νέφος. Οι έξυπνες οικειακές συσκευές που αποτελούν ένα έξυπνο σπίτι σχηματίζουν δίκτυα όπως: PAN (Personal Area Network), BAN (Body Area Network) και LAN (Local Area Network), στα οποία να λειτουργούν ως "περιορισμένοι κόμβοι" [17].

Η σύνδεση αυτή είναι εφικτή μέσω της χρήσης της οικιακής πύλης (Home Gateway - HG), μια έξυπνη οικιακή συσκευή που διαθέτει μεγάλη υπολογιστική δύναμη, αρκετές διεπαφές επικοινωνίας και επαρκή μνήμη ώστε να μπορεί να αναλάβει τα σχετικά καθήκοντα και να εκτελέσει τις απαραίτητες ενέργειες. Η πύλη HG έχει πολλαπλές λειτουργίες οι οποίες περιλαμβάνουν την χρηση της ως δρομολογητής, την παροχή τείχους προστασίας, την παροχή ενός σημείου απομακρυσμένης πρόσβασης Wi-Fi και το βασικό κέντρο εντολών το οποίο είναι υπεύθυνο για τη σωστή και απότελεσματική λειτουργία όλων των συσκευών που απαρτίζουν το έξυπνο σπίτι. Η σημαντικότητα αυτού του ρόλου σχετίζεται με τη παροχή επικοινωνίας του διαδικτύου με το εσωτερικό δίκτυο και το ανάποδο, καλύπτοντας έτσι την επικοινωνία που πρέπει να λάβει χώρα μεταξύ των αισθητήρων, των συσκευών, του νέφους και των συστημάτων [18].

1.2.3 Επίπεδο πληροφοριών και ανάλυσης

Το επίπεδο πληροφοριών και ανάλυσης (Information and Analytics layer) αποτελείται από το σύνολο των απαραίτητων λειτουργιών για τη σωστή και ασφαλή διαχείριση των δεδομένων που συλλέγονται. Το συγκεκριμένο επίπεδο αλληλοεπιδρά με τα επίπεδα λειτουργιών και διαχείρισης, παρέχοντας τις απαραίτητες πληροφορίες για τη λήψη έγκαιρων αποφάσεων από το σύστημα, καθώς και με το επίπεδο χρήστη για την παρουσίαση δεδομένων στους τελικούς χρήστες, που αφορούν τις συνδεδεμένες έξυπνες οικιακές συσκευές. Στο επίπεδο πληροφοριών και ανάλυσης περιλαμβάνονται μονάδες μετάδοσης ροής δεδομένων, ανάλυσης δεδομένων και αποθήκευσης.

Η μονάδα μετάδοσης ροής δεδομένων έχει ως σκοπό την ταχεία και αποτελεσματική μεταφορά των δεδομένων του νέφους προς το οικιακό δίκτυο. Τα δεδομένα αυτά αναγνωρίζονται και επικυρώνονται από την πύλη HG και στη συνέχεια μεταφέρονται για αποθήκευση, ανάλυση ή επεξεργασία πριν ξεκινήσει η αλυσίδα των απαραίτητων ενεργοποιήσεων των έξυπνων οικιακών συσκευών. Καθώς ο όγκος όλων αυτών των δεδομένων είναι μεγάλος, η μονάδα μετάδοσης ροής δεδομένων μπορεί να χρησιμοποιεί εξισορροπητές φορτίου για τη διανομή της πληροφοριακής κίνησης σε πολλούς επεξεργαστές, μονάδες αποθήκευσης κ.λπ. Ο τύπος δεδομένων που μπορεί να χειριστεί συμπεριλάβει δεδομένα τηλεμετρίας, που δημιουργούνται από τους αισθητήρες των συσκευών, μεταδεδομένα συσκευών, που είναι πληροφορίες οι οποίες αφορούν τις συγκεκριμένες ΔτΠ συσκευές, καθώς και ειδοποιήσεις και ενεργοποιήσεις, οι οποίες ενδέχεται να προκύψουν όταν οι έξυπνες οικιακές συσκευές παρουσιάζουν τη δυνατότητα προεπεξεργασίας των δεδομένων στις παρυφές του οικιακού δικτύου [13].

Η μονάδα ανάλυσης χρησιμοποιεί μεθόδους ανάλυσης Big Data και μηχανικής μάθησης για την εξαγωγή ζωτικών πληροφοριών από ακατέργαστα, μη δομημένα δεδομένα. Η επεξεργασία των δεδομένων μπορεί να γίνει μαζικά, όταν δεν απαιτείται ανάλυση σε πραγματικό χρόνο, ή σε πραγματικό χρόνο, όταν απαιτείται η επεξεργασία μεγάλου όγκου δεδομένων που εξαρτώνται από το χρόνο για την άμεση λήψη αποφάσεων. Η μονάδα ανάλυσης λαμβάνει και επεξεργάζεται δεδομένα από τη μονάδα μετάδοσης ροής δεδομένων ή τη μονάδα αποθήκευσης και στη συνέχεια αλληλοεπιδρά με τη μονάδα λογικής και κανόνων, όπου λαμβάνονται επιπλέον ενέργειες ανάλογα με ανάλυση των δεδομένων [19].

Μετά τη λήψη των δεδομένων από την υπηρεσία νέφους, η μονάδα αποθήκευσης είναι επιφορτισμένη με την ασφαλή και μόνιμη αποθήκευσή τους εντός του συστήματος, για τη διευκόλυνση της ανάλυσής τους και τη λήψη αποφάσεων σχετικά με την απαιτούμενη παροχή υπηρεσιών. Τα δεδομένα αυτά μπορούν να προέρχονται από τις έξυπνες οικιακές συσκευές, από υπηρεσίες νέφους ή, στην περίπτωση επεξεργασμένων δεδομένων, από τη μονάδα ανάλυσης. Τα δεδομένα που προέρχονται από τις έξυπνες οικιακές συσκευές και δεν αφορούν τα αναγνωριστικά τους ή μεταδεδομένα, δεν διαχειρίζονται από τη συγκεκριμένη μονάδα, αλλά από τις μονάδες διαχείρισης συσκευών, ταυτότητας και μητρώου συσκευών [20].

1.2.4 Επίπεδο λειτουργιών

Το επίπεδο λειτουργιών (Operations layer) αντιπροσωπεύει το σύνολο των λειτουργιών που αφορούν τη διαχείριση, συνεχή παρακολούθηση και βελτιστοποίηση του οικιακού οικοσυστήματος βάσει λογικής, κανόνων και μοντέλων. Λαμβάνει τα επεξεργασμένα δεδομένα από το επίπεδο πληροφοριών και ανάλυσης και, ανάλογα με την αξία τους, πραγματοποιεί τις απαιτούμενες ενέργειες. Εναλλακτικά, λαμβάνει άμεσες εντολές που πρέπει να εκτελεστούν από το επίπεδο παρυφών ή το επίπεδο χρήστη. Στο επίπεδο λειτουργιών ανήκει η μονάδα λογικής και κανόνων.

Η μονάδα λογικής και κανόνων περιλαμβάνει τη συλλογή των λειτουργιών λογικής που στοχεύουν στην επιβολή συγκεκριμένων λειτουργιών των υπηρεσιών νέφους του περιβάλλοντος ΔτΠ. Η συγκεκριμένη μονάδα λαμβάνει τα κανονικοποιημένα ή αναλυμένα δεδομένα τηλεμετρίας και δημιουργεί ενέργειες βάσει προκαθορισμένων κανόνων. Επιπλέον, περιλαμβάνει το σύνολο των λειτουργιών που καθορίζουν ποιες εντολές δίνονται στις έξυπνες οικιακές συσκευές, για τη σωστή λειτουργία των ενεργοποιητών τους, καθώς και αυτές που ενεργοποιούν τη χρήση των διεπαφών χρήστη και API [21].

1.2.5 Επίπεδο διαχείρισης

Το επίπεδο διαχείρισης (Management layer) αντιπροσωπεύει το σύνολο των λειτουργιών που αφορούν την παροχή (provisioning), τη συνεχή παρακολούθηση και τον έλεγχο των

έξυπνων οικιακών συσκευών που λειτουργούν στο περιβάλλον ΔτΠ. Βασικές μονάδες του συγκεκριμένου επιπέδου είναι οι μονάδες διαχείρισης συσκευών, ταυτότητας και μητρώου συσκευών.

Η μονάδα διαχείρισης συσκευών περιλαμβάνει το σύνολο των λειτουργιών που διασφαλίζουν ότι οι συσκευές ΔτΠ είναι ασφαλείς και χρησιμοποιούν σωστά τις υπηρεσίες νέφους. Οι λειτουργίες αυτές περιλαμβάνουν την παροχή συσκευών, που αναφέρεται στη διαδικασία εγγραφής νέων συσκευών στο σύστημα ΔτΠ, τη διαμόρφωση συσκευών, η οποία επιτρέπει στους χρήστες να ρυθμίζουν τις συσκευές με συγκεκριμένα χαρακτηριστικά, την παρακολούθηση συσκευών και την ενημέρωσή τους όσον αφορά το λογισμικό/υλικολογισμικό [22].

Οι μονάδες ταυτότητας και μητρώου συσκευών αποθηκεύουν τις πληροφορίες που απαιτούνται για κάθε συνδεδεμένη συσκευή, ώστε να είναι πλήρως λειτουργική και ικανή να χρησιμοποιεί τις υπηρεσίες νέφους. Η μονάδα ταυτότητας περιέχει κρυπτογραφικό υλικό και χαρακτηριστικά που χρησιμοποιούνται από τη μονάδα της πύλης HG για έλεγχο ταυτότητας των εισερχόμενων ροών δεδομένων, ενώ η μονάδα μητρώου αποθηκεύει πληροφορίες, οι οποίες διαφέρουν από τις εγγραφές που περιέχει η μονάδα ταυτότητας συσκευών, και αφορούν τις συσκευές στις οποίες μπορεί να έχει πρόσβαση, έλεγχο και διαχείριση ο εκάστοτε πάροχος νέφους. Συνήθως, οι δύο αυτές μονάδες είναι ξεχωριστές προκειμένου να διασφαλιστεί η μικρή καθυστέρηση της επικοινωνίας μεταξύ των συσκευών και του νέφους, περιορίζοντας την ποσότητα των πληροφοριών που σχετίζονται με την ταυτότητα των συσκευών και για την αποφυγή η μονάδα μητρώου συσκευών να περιέχει κρίσιμο κρυπτογραφικό υλικό [13].

1.2.6 Επίπεδο χρήστη

Το επίπεδο χρήστη (User layer) αντιπροσωπεύει το σύνολο των λειτουργιών που επιτρέπει στους χρήστες των έξυπνων οικιακών και στις παρεχόμενες υπηρεσίες από τρίτα μέρη να έχουν πρόσβαση στις εφαρμογές νέφους, στις λειτουργίες και στα συλλεγόμενα/αναλυόμενα δεδομένα μέσω μιας κοινής διεπαφής. Τέτοιες διεπαφές αφορούν τις Διασυνδέσεις Προγραμματισμού Εφαρμογών (Application Programming Interface –API) και τις διεπαφές χρήστη [23].

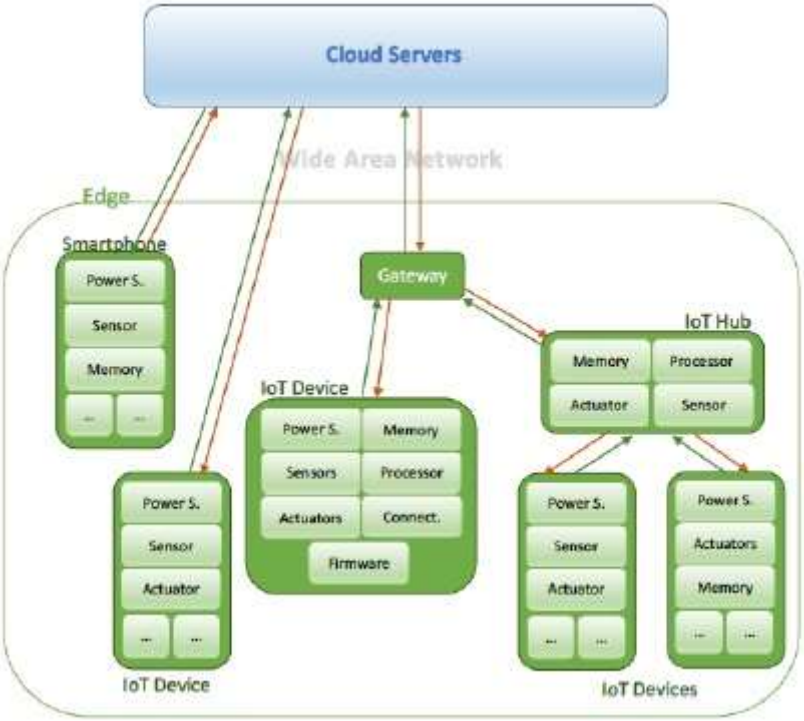
Οι διεπαφές API αποτελούν σύνολα μεθόδων και λειτουργιών που προωθούν την επικοινωνία μεταξύ διαφόρων προγραμμάτων λογισμικού. Στο πλαίσιο ενός έξυπνου οικιακού δικτύου, οι API αντιπροσωπεύουν τον πρωταρχικό τρόπο με τον οποίο οι έξυπνες οικιακές συσκευές επικοινωνούν με διαφορετικές υπηρεσίες ή συσκευές νέφους. Επιπλέον, συνδέονται με τις μονάδες αποθήκευσης ή ανάλυσης δεδομένων μέσω της μονάδας μετάδοσης ροής δεδομένων, καθώς και με τη μονάδα λογικής και κανόνων, όταν λαμβάνονται εντολές προς εκτέλεση [20].

Σε αντίθεση με τις διεπαφές API που γενικά δημιουργούνται για προγραμματιστές εφαρμογών, οι διεπαφές χρήστη αντιπροσωπεύουν τα κύρια σημεία πρόσβασης του τελικού χρήστη σε υπηρεσίες ΔτΠ και πληροφορίες. Βασικό χαρακτηριστικό των διεπαφών χρήστη αποτελεί η ευκολία χρήσης. Μέσω αυτών των διεπαφών, οι τελικοί χρήστες μπορούν να εγγράψουν νέες συσκευές, στέλνοντας τις απαραίτητες πληροφορίες στη μονάδα διαχείρισης συσκευών, να ελέγχουν τις συσκευές τους, στέλνοντας τις κατάλληλες εντολές στη μονάδα λογικής και κανόνων και να παρακολουθούν συνεχώς τις συσκευές τους, λαμβάνοντας δεδομένα σε πραγματικό χρόνο ή επεξεργασμένες και αναλυμένες πληροφορίες. Στο πλείστο των περιπτώσεων η λειτουργία των διεπαφών χρήστη απαιτεί χρήση των διεπαφών API. Παρόλα αυτά, μερικές διεπαφές χρήστη μπορούν να επικοινωνήσουν απευθείας με τις υπηρεσίες νέφους. Η κύρια μέθοδος εφαρμογής των διεπαφών χρήστη είναι μέσω mobile ή web εφαρμογών [24].

1.3 Φυσικό τμήμα

Το φυσικό τμήμα της αρχιτεκτονικής δομής ενός έξυπνου σπιτιού περιλαμβάνει τα στοιχεία λογισμικού και hardware υλικού που απαιτούνται για την υλοποίηση των λειτουργιών που περιγράφονται στο προηγούμενο τμήμα, όπως η συλλογή, μεταφορά και επεξεργασία δεδομένων και η προώθηση των εντολών που δημιουργούνται σε συγκεκριμένα στοιχεία. Εκτός από τις λειτουργίες που ορίζονται στο λειτουργικό τμήμα, το οικιακό οικοσύστημα περιλαμβάνει και πολλές απαιτήσεις που πρέπει να ληφθούν υπόψη από το φυσικό τμήμα, όπως οι υπολογιστικοί περιορισμοί, η μικρή καθυστέρηση μετάδοσης δεδομένων, η μικρή κατανάλωση ενέργειας, η διαλειτουργικότητα ανόμοιων τεχνολογιών, κ.λπ.

Το φυσικό τμήμα της αρχιτεκτονικής δομής ενός έξυπνου σπιτιού αποτελείται ουσιαστικά από τις έξυπνες οικιακές συσκευές και τις μονάδες που περιέχουν (Εικ. 5). Στην περίπτωση που το έξυπνο σπίτι λειτουργεί σε περιβάλλον ΔτΠ, οι συσκευές αυτές αλληλοεπιδρούν με το οικιακό περιβάλλον και μεταδίδουν δεδομένα ή επιτρέπουν σε άλλες συσκευές να αλληλοεπιδρούν και επικοινωνούν με το εν λόγω περιβάλλον [13].



Εικόνα 5: Φυσικό τμήμα ενός έξυπνου σπιτιού [13]

1.3.1 Μονάδες έξυπνων οικιακών συσκευών

Οι έξυπνες οικιακές συσκευές αποτελούνται από μονάδες όπως αισθητήρες, ενεργοποιητές, επεξεργαστές, μνήμη, πηγές ισχύος και υλικολογισμικό [25]. Όπως αναφέρθηκε στην προηγούμενη ενότητα, οι αισθητήρες αποτελούν μέρος και του λειτουργικού τμήματος της αρχιτεκτονικής δομής ενός έξυπνου σπιτιού, καθώς εκτελούν την λειτουργία της ανίχνευσης των αλλαγών του οικιακού περιβάλλοντος. Εκτός αυτού, και όσον αφορά το φυσικό τμήμα της αρχιτεκτονικής δομής του έξυπνου σπιτιού, ένας αισθητήρας είναι υπεύθυνος για τη μετατροπή των αναλογικών σημάτων που δέχεται από το γύρω περιβάλλον σε ψηφιακά και την αποστολή τους σε άλλα ηλεκτρονικές μονάδες. Αξίζει να σημειωθεί ότι οι "αναγνώσεις" των αισθητήρων θα πρέπει να είναι όσο το δυνατόν πιο ακριβείς για την εύρυθμη λειτουργία του οικιακού οικοσυστήματος, καθώς βάσει αυτών λαμβάνονται και οι ανάλογες αποφάσεις απόκρισης του συστήματος στην οποιαδήποτε μεταβολή του οικιακού περιβάλλοντος [26].

Όπως συμβαίνει και με τους αισθητήρες, οι ενεργοποιητές αποτελούν τη φυσική υλοποίηση της λειτουργίας ενεργοποίησης του επιπέδου παρυφών του λειτουργικού τμήματος της αρχιτεκτονικής δομής ενός έξυπνου σπιτιού, ελέγχοντας την ενεργοποίηση ή την απενεργοποίηση μιας συγκεκριμένης οντότητας. Οι ενεργοποιητές λαμβάνουν εντολές απευθείας από τις διεπαφές χρήστη ή έμμεσα μέσω των δεδομένων του αισθητήρα, η επεξεργασία των οποίων γίνεται τοπικά ή, πιο συχνά, μέσω του νέφους. Ένας ενεργοποιητής μπορεί να λειτουργεί ανεξάρτητα είτε σε συνδυασμό με άλλους ενεργοποιητές για την παροχή ενός πιο σύνθετου συνόλου αλλαγών κατάστασης μιας φυσικής οντότητας. Κοινά παραδείγματα ενεργοποιητών αποτελούν τα ηχεία και οι διακόπτες τροφοδοσίας [8].

Οι επεξεργαστές είναι μονάδες υπεύθυνες να ερμηνεύουν τα δεδομένα που παράγονται από τα αισθητήρια όργανα και την επακόλουθη εφαρμογή της λογικής ελέγχου. Η διαδικασία της επεξεργασίας των δεδομένων μπορεί να αφορά πολύ απλές διεργασίες, όπως η μεταβολή της θερμοκρασίας ενός δωματίου, ή εξαιρετικά περίπλοκες, περιπτώσεις στις οποίες μπορεί να χρησιμοποιηθούν τεχνικές μηχανικής εκμάθησης και τεχνητής νοημοσύνης. Παρόλο που ορισμένες τεχνολογίες ΔτΠ, όπως η τεχνολογία του edge computing, χρησιμοποιούν τοπικούς επεξεργαστές για τη μείωση του φόρτου επεξεργασίας των απομακρυσμένων συστημάτων, οι περισσότερες έξυπνες οικιακές συσκευές χρησιμοποιούν ως επί το πλείστο επεξεργασία νέφους, λόγω των περιορισμών ισχύος που διαθέτουν [27].

Οι μνήμες διακρίνονται σε πτητικές και μη πτητικές. Μια πτητική μνήμη (π.χ. RAM) γενικά χρησιμοποιείται για την υποστήριξη της λειτουργίας ενός επεξεργαστή, διατηρώντας δεδομένα και πληροφορίες κατά τη διάρκεια της επεξεργασίας τους. Οι μη πτητικές μνήμες (π.χ. ROM) αποθηκεύουν πληροφορίες σε μόνιμη βάση, ακόμη και μετά την αφαίρεση της πηγής τροφοδοσίας τους. Για το λόγο αυτό αποτελούν ιδανική λύση για τις έξυπνες συσκευές στις οποίες είναι επιθυμητή η τοπική αποθήκευση των δεδομένων των αισθητήρων, για εφεδρική χρήση ή για τη μετέπειτα μαζική μεταφορά τους στο νέφος [28].

Η μονάδα της πηγής ισχύος είναι υπεύθυνη για την παροχή επαρκούς ισχύος στις έξυπνες οικιακές συσκευές, ώστε να διασφαλιστεί η σωστή λειτουργικότητά τους. Η παρεχόμενη ισχύς μπορεί να προέρχεται μέσω άμεσης παροχής από το ηλεκτρικό δίκτυο, μέσω φορητών μπαταριών ή μέσω συλλογής ενέργειας, μια διαδικασία με την οποία η ενέργεια προέρχεται από εξωτερικές πηγές, συλλαμβάνεται και αποθηκεύεται για μικρές, ασύρματες αυτόνομες συσκευές. Η μονάδα της πηγής ισχύος ουσιαστικά καθορίζει τη δυνατότητα φορητότητας των έξυπνων οικιακών συσκευών [29].

Τέλος, η μονάδα του υλικολογισμικού (firmware) περιλαμβάνει την έκδοση του λογισμικού που χρησιμοποιείται για τον έλεγχο και την παρακολούθηση του hardware υλικού μιας έξυπνης οικιακής συσκευής, καθώς και για τη λήψη, την ανάγνωση και το μετασχηματισμό των σημάτων δεδομένων. Η μονάδα αυτή γεφυρώνει τον ψηφιακό με τον φυσικό κόσμο αφαιρώντας τους κοινούς υπολογιστικούς πόρους και επιτρέποντας τη μετατροπή των ψηφιακών σημάτων σε κίνηση. Για οποιαδήποτε συσκευή ΔτΠ που μπορεί να συνδεθεί σε μια πλατφόρμα νέφους, η συχνή ενημέρωση του λογισμικού και του υλικολογισμικού της είναι υψίστης σημασίας, καθώς μόνο με τον τρόπο αυτό δίνεται η δυνατότητα ενημέρωσης του κώδικα σφαλμάτων, επιδιόρθωσης των τρωτών σημείων και προσθήκης νέων λειτουργιών [30].

1.3.2 Έξυπνες οικιακές συσκευές

Στις έξυπνες οικιακές συσκευές περιλαμβάνονται όλες οι οικιακές συσκευές ή τα ηλεκτρονικά είδη ευρείας κατανάλωσης, που συνδέονται και ελέγχονται από το σύστημα οικιακού αυτοματισμού. Όλες οι συσκευές τελευταίας τεχνολογίας οι οποίες είναι μέρος ενός έξυπνου σπιτιού έχουν τη δυνατότητα να παρατηρούν και να ελέγχουν όλες τις ανθρώπινες ενέργειες και συνήθειες μέσα και έξω από το έξυπνο σπίτι, αποτελόντας έτσι μέρος του ΔτΠ. Στις έξυπνες οικιακές συσκευές περιλαμβάνονται οι έξυπνες συσκευές ΔτΠ, τα hub ΔτΠ, η

πύλη HG και διάφορες ηλεκτρονικές συσκευές ευρείας κατανάλωσης, όπως smartphone, tablet, laptop και προσωπικοί Η/Υ [31].

Οι έξυπνες συσκευές ΔτΠ, γνωστές και ως "πράγματα" του Διαδικτύου των Πραγμάτων, είναι φυσικά αντικείμενα με μη υπολογιστική λειτουργία, αλλά με τη δυνατότητα να ανιχνεύουν ή/και να αλληλοεπιδρούν με το γύρω περιβάλλον τους. Οι συγκεκριμένες συσκευές μπορούν επίσης να συνδεθούν σε ένα δίκτυο στο οποίο μεταφέρουν δεδομένα και λαμβάνουν εντολές. Οι έξυπνες οικιακές συσκευές ΔτΠ καλύπτουν μια ευρεία γκάμα συσκευών, από κάμερες ασφαλείας, λαμπτήρες και κλειδαριές μέχρι ψυγεία, πλυντήρια πιάτων και βραστήρες [16].

Τα hub ΔτΠ έχουν σχεδιαστεί ώστε να λειτουργούν ως κεντρικοί ελεγκτές των έξυπνων συσκευών. Διακρίνονται σε ομοιογενή και ετερογενή. Τα ομοιογενή hub κατασκευάζονται από την ίδια εταιρεία που κατασκευάζει τις συσκευές ΔτΠ με τις οποίες μπορεί να συνδεθεί και, ως εκ τούτου, γενικά απαιτούνται για την κανονική λειτουργία των συσκευών αυτών. Χρησιμοποιούνται συχνά στην περίπτωση συσκευών ΔτΠ όπου οι δυνατότητές τους δεν τους επιτρέπουν την αυτόνομη σύνδεση στο δίκτυο WAN ή την επεξεργασία των δεδομένων που παράγουν. Τα ετερογενή hub μπορούν να συνδέουν πολλά διαφορετικά είδη συσκευών επιτρέποντας την μεταξύ τους επικοινωνία. Συνήθως συνοδεύονται από τη δικής του εφαρμογή που επιτρέπει στους χρήστες τον έλεγχο όλων των συνδεόμενων συσκευών μέσω μίας και μόνης πύλης [32].

Η πύλη HG αποτελεί εξοπλισμό του οικιακού δικτύου που συνδέει τις συσκευές ΔτΠ με το Διαδίκτυο. Όντας η φυσική εφαρμογή της πύλης HG του λειτουργικού τμήματος της αρχιτεκτονικής δομής του έξυπνου σπιτιού, λαμβάνει δεδομένα από τις συνδεδεμένες στο οικιακό δίκτυο έξυπνες συσκευές και καθορίζει το κατάλληλο πρωτόκολλο της επικοινωνίας τους. Σε ορισμένες περιπτώσεις, ενδέχεται να ενσωματώνει ορισμένες από τις λειτουργίες των hub ΔτΠ, παρέχοντας τοπική προεπεξεργασία και ανάλυση των δεδομένων ή αμφίδρομη επικοινωνία μεταξύ των συσκευών χωρίς την ανάγκη σύνδεσης με τον διακομιστή νέφους [33].

Οι πρωταρχικές λειτουργίες των ηλεκτρονικών συσκευών ευρείας κατανάλωσης, όπως smartphone, tablet, laptop και προσωπικών Η/Υ αφορούν την υπολογιστική ικανότητα, που στο πλαίσιο του έξυπνου οικοσυστήματος, περιλαμβάνει την παροχή στους τελικούς χρήστες ενός τρόπου με τον οποίο μπορούν να παρακολουθούν και να ελέγχουν τις υπόλοιπες έξυπνες οικιακές συσκευές ΔτΠ. Αν και γενικά δεν θεωρούνται έξυπνες συσκευές ΔτΠ, τα smartphone κατέχουν εξέχουσα θέση στα οικιακά δίκτυα, καθώς περιλαμβάνουν αισθητήρες, όπως μικρόφωνα και επιταχυνσιόμετρα [34].

1.4 Επικοινωνιακό τμήμα

Το επικοινωνιακό τμήμα περιγράφει τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται για τη μεταφορά δεδομένων μεταξύ των έξυπνων οικιακών συσκευών και τη λήψη και μετάδοση πληροφοριών μεταξύ των συσκευών αυτών και των υπηρεσιών νέφους. Με τη χρήση συγκεκριμένων πρωτοκόλλων μπορούμε να προκαθορίσουμε το τρόπο που θα μεταδίδονται οι πληροφορίες, τι υλικό μπορούμε να χρησιμοποιήσουμε, τις πιστοποιήσεις και τις άδειες χρήσης τους.

Όλες οι έξυπνες οικιακές συσκευές διασυνδέονται μεταξύ τους ασύρματα ή καλωδιακά μέσω του εσωτερικού δικτύου του έξυπνου σπιτιού. Κάποια από τα μέσα διάδοσης που χρησιμοποιούνται στο περιβάλλον ΔτΠ για την επικοινωνία των συσκευών αυτών μπορεί να είναι απλές γραμμές τηλεφώνου, ασύρματες ζεύξεις ή ραδιοσυχνότητες και οπτικές ίνες ή κλασικά UTP καλώδια. Οι τρείς μεγάλες κατηγορίες στις οποίες διαχωρίζουμε τα πρωτόκολλα επικοινωνίας βάση τού μέσου που χρησιμοποιούν για να διαδοθούν είναι [18]: (1) ενσύρματα, (2) ασύρματα και (3) υβριδικά. Κάθε φορά για τη σωστή επιλογή πρέπει πρώτα να ξεκαθαρίσουμε τι χρήση θέλουμε να κάνουμε και στη συνέχεια να δούμε το μέγεθος του οικιακού δικτύου στο οποίο θέλουμε να τα εφαρμόσουμε. Τα πρωτόκολλα επικοινωνίας έχουν

ποικίλα χαρακτηριστικά με κάποια από αυτά να προσφέρουν μεγαλύτερη εμβέλεια, άλλα να δίνουν καλύτερη ασφάλεια και κάποια άλλα μειωμένη κατανάλωση ενέργειας.

1.4.1 Πρωτόκολλα ενσύρματης επικοινωνίας

Τα καλώδια απότελούν τη βάση για την επίτευξη της ενσύρματης επικοινωνία. Οι κατηγορίες των καλωδίων που χρησιμοποιούμε περιλαμβάνουν, τις κλασσικές τηλεφωνικές γραμμές, τα ομοαξονικά καλώδια, τις οπτικές ίνες και τα ευρέως πλέον διαδεδομένα συνεστραμμένα ζεύγη με θωράκιση ή χωρίς. [18]. Με τη χρήση των υφιστάμενων καλωδιώσεων παροχής ηλεκτρικής ενέργειας ενός κτηρίου μπορούμε να εφαρμόσουμε τη τεχνολογία του PLC, οι οποία μπορεί να εξυπηρετήσει μεγάλης ταχύτητας ενσύρματες επικοινωνίες καθώς περιλαμβάνει και ένα μεγάλο πλήθος προτύπων. [35].

Παρακάτω θα αναφέρουμε κάποια από τα πλεονεκτήματα που μας δίνει η ενσύρματη επικοινωνία σε σχέση με τους άλλους τύπους [36]:

- *Ασφάλεια και Προστασία*: Η χρηση καλωδιακής υποδομής για τη σύνδεση των έξυπνων οικειακών συσκευών καθιστά σε ένα τεράστιο ποσοστό αδύνατη τη παραβίαση και την υποκλοπή των δεδομένων.
- *Απλή χρήση*: Τα ασύρματα δίκτυα χρειάζονται συνήθως κάποιον κωδικό πρόσβασης καθώς και την επιλογή του σωστού δικτύου σύνδεσης, κάτι το οποίο μπορεί να είναι χρονοβόρο και δύσκολο για τον απλό χρήστη. Με τη χρήση ενσύρματης σύνδεσης αυτές οι πολύπλοκες ενέργειες παύουν να υπάρχουν καθώς η σύνδεση είναι μια απλή σύνδεση καλωδίου.
- *Απόσταση*: Η ασύρματη διασύνδεση με τη χρήση των κλασσικών πρωτοκόλλων (π.χ. Wi-Fi 802.11ac) παρουσιάζει σημαντικό περιορισμό στην εμβέλια μετάδοσης κάτι το οποίο δεν ίσχύει στην ενσύρματη διασύνδεση η οποία μπορεί να καλύψει πολύ μεγάλες αποστάσης.
- *Ρυθμός μετάδοσης δεδομένων*: Συγκρίνοντας τις ταχύτητες μετάδοσης βλέπουμε πως το Wi-Fi 802.11ac έχει ως μέγιστη ταχύτητα το 1,3Gbps σε σχέση με το Ethernet το οποίο μπορεί θεωρητικά να φτάσει μέχρι και τα 100Gbps.
- *Αξιοπιστία*: Δυστυχώς τα ασυρματα δίκτυα είναι αρκετά ευάλωτα σε παρεμβολές από ηλεκτρομαγνητικά πεδία και διάφορα εμπόδια, κάτι το οποίο δεν ισχύει για την ενσύρματη καλωδίωση. Τα δεδομένα που μεταδίδοντα μέσα από ένα καλώδιο μεταφέρονται χωρίς να έχουν καμία παρεμβολή από τις προηγούμενες παρεμβολές, για αυτό και η μετάδοση τους είναι πολύ σταθερή.

Θα αναφέρουμε όμως και κάποια κοινά μειονεκτήματα που έχουν οι ενσύρματες τεχνολογίες επικοινωνίας με τις ασύρματες [36]:

- *Κόστος και πολυπλοκότητα*: Ένα ενσύρματο δίκτυο για να υλοποιηθεί χρειάζεται η εγκατάσταση του να γίνει από εκπαιδευμένο προσωπικό, που πρέπει να δαπανήσει αρκετό χρόνο στη σωστή εγκατάσταση του.
- *Φορητότητα*: Δύσκολη μετακίνηση των συσκευών μετά από την εγκατάσταση των καλωδιώσεων.
- *Ισχύς*: Οι αυξωμειώσεις καθώς και οι διακοπες λειτουργίας της ηλεκτρικής παροχής ενέργειας μπορούν να παίξουν σημαντικό ρόλο στη σωστή και αδιάλειπτη λειτουργία των συσκευων. Αυτό το πρόβλημα σε ένα βαθμό μπορεί να αντιμετωπιστεί με τη χρήση UPS (Uninterruptible Power Supply) το κόστος όμως αγοράς μιας τέτοιας συσκευείες είναι αρκετά δαπανηρό.

- *Επέκταση*: Η επεκτασιμότητα ενός ενσύρματου δικτύου είναι αρκετά δύσκολη και χρονοβόρα σε σχέση με ένα ασύρματο δίκτυο στο οποίο μπορεί να χρειαστεί απλά η προσθήκη ενός δρομολογητή.

Στη συνέχεια παρουσιάζονται μερικά από τα πλέον σύγχρονα συνηθέστερα χρησιμοποιούμενα πρωτόκολλα ενσύρματης επικοινωνίας ενός έξυπνου σπιτιού.

I) Ethernet

Το Ethernet είναι μια δημοφιλής τεχνολογία ενσύρματης επικοινωνίας που αναπτύχθηκε από την εταιρεία Xerox στα μέσα της δεκαετίας του '70 αποκτόντας μεγάλη φήμη όταν το 1980 έγινε η προτυποποίηση του από τη Xerox σε συνεργασία με άλλες δυο μεγάλες εταιρείες τη Digital Equipment Corporation και την Intel. Είναι ένα πρωτόκολλο που υλοποιείται ή υποστηρίζεται από πολλά οικιακά LAN. Χρησιμοποιεί πρακτικά τη μέθοδο μετάδοσης δεδομένων σε μορφή πακέτων (packet switching) μέγιστου μεγέθους (Maximum Transmission Unit - MTU) 1500 bytes και ελάχιστου 46 bytes. Το δίκτυο Ethernet μπορεί και χρησιμοποιεί μια αρκετά μεγάλη γκάμα καλωδιώσεων όπως είναι τα καλώδια συνεστραμένου ζεύγους και οπτικών ινών καιθώς και τα ομοαξονικά καλώδια κάνοντας το ευρέως διαδεδομένο. Στα πιο σύνηθη δίκτυα όπως τα δίκτυα εγκαταστάσεων πελάτη (Customer Premises Networks – CPN) η χρήση καλωδίων χαλκού είναι διαδεδομένη. Το Ethernet είναι ένα από τα πιο αξιόπιστα πρωτόκολλα καθώς έχει το πρόβλημα παρεμβολών εύρου ζώνης. Επίσης ένα δίκτυο Ethernet έχει ως συνήθη ταχύτητα μεταφοράς δεδομένων τα 100Mbps, προσφέροντας παράλληλα και άλλες επιλογές σε ταχύτητες όπως είναι τα 10Mbps, 100Mbps, 1Gbps και 10Gbps [37].

II) IEEE 1394

Το IEEE 1394 είναι πρωτόκολλο για σύνδεση συσκευών σε Η/Υ. Οι πιο γνωστές εφαρμογές που το χρησιμοποιούν είναι το FireWire της Apple και το i.LINK της SONY. Το πρωτόκολλο προσφέρει δύο τρόπους μετάδοσης δεδομένων, την συγχρονισμένη και την ασύγχρονη, σε μια καθορισμένη απόδοση για την πιο αποτελεσματική υποστήριξη ροών πολυμέσων. Η τεχνολογία 1394 Serial Bus αναπτύχθηκε ως ενσύρματη διεπαφή χρησιμοποιώντας ένα ειδικό καλώδιο έξι (6) αγωγών, αλλά μπορεί να προσαρμοστεί και για ασύρματες μεταδόσεις. Το αρχικό πρότυπο ορίζει τρεις ρυθμούς σηματοδότησης των 98,304, 196,608 και 393,216Mbps. Αυτές οι τιμές αναφέρονται στο πρότυπο 1394 ως S100, S200 και S400. Το 1394a υποστηρίζει έως και 400Mbps σε απόσταση 4,5 μέτρων ή 200Mbps για 14 μέτρων καλώδιο 1394. Η προδιαγραφή 1394b, που οριστικοποιήθηκε στις αρχές του 2002, επεκτείνει το πρότυπο ώστε να υποστηρίζει ταχύτητες μεταφοράς δεδομένων της τάξης των 800Mbps και 1,2Gbps, με δυνατότητα επέκτασης έως και τα 3,2Gbps. Το πρωτόκολλο περιλαμβάνει προδιαγραφές για ένα πλήθος μέσων μετάδοσης, συμπεριλαμβανομένων καλωδίων CAT-5 χωρίς θωράκιση, οπτικών ινών και θωρακισμένου συνεστραμμένου ζεύγος, με εύρος κάλυψης που φτάνει έως και τα 100 μέτρα [38].

III) USB

Ο Ενιαίος Σειριακός Δίαυλος, γνωστός και ως Universal Serial Bus (USB), είναι ένα σειριακό πρωτόκολλο και σύνδεσμος φυσικού επιπέδου. Τα δεδομένα μεταδίδονται μέσω ενός ζεύγους συνεστραμμένων καλωδίων με ημιαμφίδρομο διαφορικό τρόπο, παρουσιάζοντας αποτελεσματική καταπολέμηση του ηλεκτρομαγνητικού θορύβου. Ένα άλλο ζεύγος του καλωδίου USB μεταφέρει DC τάση, επιτρέποντας την τροφοδότηση σε πολλές συσκευές χαμηλής ισχύος. Το USB υποστηρίζει υψηλό ρυθμό μεταφοράς δεδομένων και σύνδεση “hot swap” για υπολογιστές, παρέχοντας εύκολη σύνδεση σε μια μεγάλη ποικιλία πολυμέσων και δικτύων USB. Το USB πρωτόκολλο έχει τις παρακάτω ταχύτητες λειτουργίας ανάλογα την έκδοση: 1.5Mbps (χαμηλή ταχύτητα), 12Mbps (πλήρης ταχύτητα, USB 1.1), 480Mbps (υψηλή ταχύτητα, USB 2), 5Gbps (υπερυψηλή ταχύτητα SSUSB/USB 3) και 10Gbps (υπερυψηλή ταχύτητα USB 3.1). Η μέγιστη απόσταση σύνδεσης του πρωτοκόλλου φτάνει τα 5 μέτρα [39].

IV) Homeplug

Η HomePlug Powerline Alliance ανέπτυξε μια οικογένεια κοινά αποδεκτών πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται στο έξυπνο οικοσύστημα, όπως τα HomePlug AV, HomePlug Green PHY και HomePlug Access BPL. Όλα τα πρωτόκολλα της οικογένειας συμμορφώνονται με τα πρότυπα IEEE 1901. Η μέγιστη ταχύτητα μεταφοράς δεδομένων τους μπορεί να φτάσει τα 1200Mbps, ενώ το εύρος κάλυψης τους αγγίζει τα 300m. Για την επίτευξη αξιόπιστης ασφάλειας το HOmePlug κάνει χρήση 128bit κρυπτογράφησης AES. Όλες οι powerline συσκευές περιλαμβάνουν ένα μοναδικό κλειδί ασφαλείας που δεν χρειάζεται αλλαγή και με το πάτημα ενός κουμπιού επιτρέπεται η ταυτοποίηση και εγκατάσταση άλλων παρόμοιων συσκευών. Μια εναλλακτική έκδοση της HomePlug AV είναι HomePlug CC (HomePlug Command Control - HPCC) η οπόια βρίσκει εφαρμογή σε εφαρμογές χαμηλού κόστους και ταχύτητας. [40].

V) X10/UPB

Το X10 αποτελλεί το παλαιότερο πρωτόκολλο που δημιουργήθηκε για έξυπνες οικιακές συσκευές και εξακολουθεί να χρησιμοποιείται. Το πρότυπο μεταδίδει σήματα ψηφιακής πληροφορίας χρησιμοποιώντας την τεχνολογία PLC. Το συγκεκριμένο πρωτόκολλο εξαιτίας της παλαιότητας του (υλοποίηση το 1975) παρουσιάζει κάποια προβλήματα σε σχέση με τη συμβατότητα του με τις συσκευές και τις καλωδιακές εγκαταστάσεις, έχει περιορισμένη λειτουργικότητα, επηρεάζεται από παρεμβολές, έχει αρκετά μεγάλη εξασθένηση στο σήμα μεταξύ δύο αγωγών, καθόλου κρυπτογράφηση, πολύ χαμηλη ταχύτητα μετάδοσης δεδομένων καθώς και απώλεια των εντολών. Στο τομέα της εμβέλιας καλύπτει οριακά μια απόσταση 300m έχοντας ως ταχύτητα μετάδοσης τα 120bps. [41].

Το Universal Powerline Bus (UPB) μπορεί να θεωρηθεί ως τεχνολογία αντικατάστασης του X10. Αποτελεί ένα πρωτόκολλο επικοινωνίας τεχνολογίας PLC με μεγαλύτερη αξιοπιστία και γρηγορότερο ρυθμό μετάδοσης δεδομένων. Το κύριο μειονέκτημά του είναι το γεγονός ότι, ενώ υποστηρίζει έναν πολύ μεγαλύτερο αριθμό συνδεδεμένων συσκευών σε σύγκριση με το X10, η υιοθέτησή του από την αγορά είναι μικρή. Σε σύγκριση με άλλα ενσύρματα πρωτόκολλα επικοινωνίας, τα X10 και UPB παρέχουν σχετικά χαμηλό ρυθμό μεταφοράς δεδομένων, χωρίς δυνατότητες κρυπτογράφησης και η εφαρμογή τους σε ένα έξυπνο σπίτι πρέπει να γίνει από τεχνικό προσωπικό. Επίσης, δεν παρέχουν στις συνδεδεμένες συσκευές πρόσβαση στο Διαδίκτυο [13].

VI) KNX

Το KNX ανήκει ως πρωτόκολλο επικοινωνίας στο μοντέλο του OSI και σχεδιάστηκε για να εξυπηρετεί εφαρμογές σε έξυπνα κτίρια με σκοπό να αντικαταστήσει τρία παλαιότερα πρότυπα το BatiBUS, το EHS και το Instabus. Η ανταλλαγή δεδομένων μεταξύ των συσκευών KNX πραγματοποιείται μέσω ενός διαύλου ζεύγους καλωδίων. Το KNX χρειάζεται δική του αποκλειστική καλωδίωση , για αυτό και είναι αρκετά πολύπλοκο και κοστοβόρο. Καθώς η λειτουργία των μεμονωμένων συσκευών διαύλου εξαρτάται μόνο από τον προγραμματισμό τους, δίνει τη δυνατότητα να μπορούμε να τις τροποποιήσουμε και να τις προσαρμόσουμε όποτε είναι απαραίτητο. Είναι κατάλληλο για χρήση ως πρωτόκολλο σηματοδότησης και εξαιτίας του χαμηλού ρυθμού μετάδοσης δεδομένων. Το πρωτόκολλο δεν μπορεί να υποστηρίξει τοπολογία δικτύου σε δακτύλιο αλλά είναι ικανό να λειτουργήσει σε σε δύκτυα γραμμής, αστέρα και δέντρου. Η έκδοση KNX-PL η οποία αποτελεί μια εκδοχή του KNX χρησιμοποιείται σε δίκτυα ηλεκτρικών γραμμών, επίσης υπάρχει η έκδοση KNX-TP η οποία εφαρμόζεται σε καλωδιώσεις συνεστραμμένου ζεύγους. Για τις RF επικοινωνίες γίνεται χρήση της KNX-RF έκδοσης και για το Ethernet χρησιμοποιούμαι την KNX-IP [42].

1.4.2 Πρωτόκολλα ασύρματης επικοινωνίας

Η ασύρματη επικοινωνία πραγματοποιείται με τη χρήση ηλεκτρομαγνητικών κυμάτων ως μέσο μετάδοσης των πληροφοριών ανάμεσα σε έναν απομακρισμένο πομπό και ένα δέκτη. Στην περίπτωση αυτή, οι πληροφορίες μεταδίδονται μεταξύ συσκευών που μπορεί να έχουν απόσταση από μερικά μέτρα έως εκατοντάδες χιλιόμετρα μέσω καλά καθορισμένων καναλιών επικοινωνίας. Απότελούν το πλέον δημοφιλές πρωτόκολλο επικοινωνίας σε δικτυα έξυπνων σπιτιών καθώς παρουσιάζουν ευκολία στη χρήση και έχουν αρκετά χαμηλό κόστος εγκατάστασης νέων συσκευών. [43].

Τα πλεονεκτήματα της ασύρματης έναντι της ενσύρματης επικοινωνίας είναι πολλά, όπως [44]:

- *Κόστος*: Το κόστος εγκατάστασης της καλωδιακής υποδομής ενός δικτύου εξαλείφεται στην ασύρματη επικοινωνία και συνεπώς μειώνεται το συνολικό κόστος του συστήματος σε σύγκριση με το ενσύρματο σύστημα επικοινωνίας.
- *Φορητότητα*: Η φορητότητα αποτελεί το κύριο πλεονέκτημα του ασύρματο σύστημα επικοινωνίας, καθώς παρέχει ταυτόχρονη ελευθερία κινήσεων και συνδεσιμότητα με το δίκτυο.
- *Ευκολία εγκατάστασης*: Η εγκατάσταση του εξοπλισμού ασύρματης επικοινωνίας είναι πολύ εύκολη, αφού δεν εξαρτάται από την επίπονη εγκατάσταση καλωδιώσεων. Επίσης, ο χρόνος που απαιτείται για τη ρύθμιση ενός ασύρματου συστήματος, όπως για παράδειγμα ένα δίκτυο Wi-Fi, είναι πολύ μικρότερος σε σύγκριση με τη δημιουργία ενός πλήρους καλωδιακού δικτύου.
- *Αξιοπιστία*: Δεδομένου ότι στην ασύρματη επικοινωνία δεν απαιτείται η εγκατάσταση καλωδίων, η πιθανότητα αποτυχίας επικοινωνίας λόγω διάβρωσης των καλωδίων από διάφορες περιβαλλοντικές συνθήκες είναι αδύνατη.
- *Επεκτασιμότητα*: Σε ένα ασύρματο δίκτυο η προσθήκη μιας νέας συσκευής ή συσκευών είναι μια πολύ εύκολη διαδικασία με ελάχιστο κόστος. Βασική προυπόθεση στην εγκατάσταση αποτελεί ο μέγιστος αριθμός που μπορεί να υποστηρίξει το δίκτυο και δεν πρέπει να ξεπεραστεί.

Όπως όλες οι τεχνολογίες, έτσι και οι τεχνολογίες ασύρματης επικοινωνίας έχουν τα δικά τους μειονεκτήματα, τα οποία είναι [44]:

- *Παρεμβολές*: Ένα ασύρματο δίκτυο είναι πολύ εύκολο να επηρεαστεί από εξωτερικές παρεμβολές, οι οποίες μπορούν να διαταράξουν σε μεγάλο βαθμό την ομαλή λειτουργία των εφαρμογών.
- *Ασφάλεια*: Ένα από τα κύρια προβλήματα της ασύρματης επικοινωνίας είναι η ασφάλεια των δεδομένων, με δεδομένο ότι τα σήματα μεταδίδονται μέσω ηλεκτρομαγνητικών κυμάτων και η πιθανότητα υποκλοπής ευαίσθητων πληροφοριών, είναι πολύ μεγάλη.
- *Ρυθμός μετάδοσης δεδομένων*: Είναι προφανές πως στα ασύρματα δίκτυα ο ρυθμός μετάδοσης των δεδομένων είναι μικρότερος από ότι σε ένα ενσύρματο δίκτυο. Αυτό το μειονέκτημα όμως μπορεί να μην είναι τόσο σημαντικό καθώς οι περισσότερες εφαρμογές σε ένα έξυπνο σπίτι δεν απαιτούν μεγάλο ρυθμό μετάδοσης δεδομένων.
- *Κάλυψη*: Το ασύρματο δίκτυο μπορεί να καλύψει ευκολότερα μια μεγάλη περιοχή εν αντιθέση με το ενσύρματο το οποίο περιορίζεται από το μήκος του εκάστοτε καλωδίου. Παρ' όλα αυτά αν οι συσκεύες τοποθετηθούν σε σημείο όπου υπάρχει περιορισμός της κάλυψης από εμπόδια, τότε μπορεί να έχουμε απώλεια πληροφοριών.

- *Προβλήματα υγείας*: Η συνεχής έκθεση σε οποιοδήποτε είδος ακτινοβολίας μπορεί να είναι επικίνδυνη, ακόμα κι αν τα επίπεδα της RF ακτινοβολίας που μπορούν να προκαλέσουν ζημιά στην υγεία των χρηστών δεν έχουν προσδιοριστεί με ακρίβεια.

Στη συνέχεια παρουσιάζονται μερικά από τα πλέον σύγχρονα συνηθέστερα χρησιμοποιούμενα πρωτόκολλα ασύρματης επικοινωνίας ενός έξυπνου σπιτιού.

I) Wi-Fi (IEEE 802.11)

Το Wi-Fi είναι ένα πρωτόκολλο ασύρματης επικοινωνίας που βασίζεται στην οικογένεια προτύπων IEEE 801.11 (IEEE 802.11 a/b/g/n/ah/ax). Από τη στιγμή που το πρωτόκολλο είναι παρόν σε κάθε σπίτι μέσω ενός ασύρματου δρομολογητή (router), επί του παρόντος, ένας τεράστιος αριθμός έξυπνων συσκευών κατασκευάζονται έχοντας το ως βάση για την ασύρματη επικοινωνία τους. Η τεχνολογία παρέχει αξιόπιστη, ασφαλή και υψηλής ταχύτητας επικοινωνία (της τάξης των πολλών εκατοντάδων bit ανά δευτερόλεπτο), υποστηρίζει κρυπτογράφηση WPA2 (μηχανισμός πιστοποίησης κόμβων και κρυπτογράφησης δεδομένων) και λειτουργεί στο φάσμα συχνοτήτων 2,4 - 5,8GHz. Παρά το γεγονός ότι αυτές οι προδιαγραφές είναι βέλτιστες για ροή βίντεο και μεταφορές αρχείων, συνεπάγονται ταυτόχρονα και υψηλότερες καταναλώσεις ισχύος, γεγονός που καθιστούν το πρωτόκολλο "απαγορευτικό" για μικρότερες συσκευές ΔτΠ που λειτουργούν με μπαταρία coin cell. Τα μειονεκτήματα της τεχνολογίας Wi-Fi είναι η σχετικά μικρή εμβέλεια, η ευαισθησία στις παρεμβολές και τα εμπόδια σε εσωτερικούς χώρους που μπορούν να επηρεάσουν σημαντικά τη ταχύτητα και την αξιοπιστία του [37].

II) Bluetooth / BLE (IEEE 802.15.1)

Πρόκειται για τυποποιημένο πρωτόκολλο για αποστολή και λήψη δεδομένων μέσω ασύρματης ζεύξης 2,4GHz. Το φάσμα λειτουργίας είναι στα 2402 - 2480MHz, ή 2400 – 3483,5MHz, υποστηρίζοντας 79 κανάλια εύρους 1MHz το καθένα. Η ταχύτητα μεταφοράς δεδομένων φτάνει τα 2Mbps, ενώ η εμβέλεια της τεχνολογίας κυμαίνεται μεταξύ 50 και 150 μέτρων. Χρησιμοποιεί τη τεχνική master/slave για ασύρματη μετάδοση δεδομένων μεταξύ ηλεκτρονικών συσκευών σε μικρή απόσταση, με χαμηλή κατανάλωση ενέργειας. Για την επικοινωνία των συσκευών χρειάζεται να φτιαχτεί ένα "δεσμός" μεταξύ των συσκευών όπου αποθηκεύεται στη μνήμη κάθε συσκευής και τους επιτρέπει να μοιράζονται τις διευθύνσεις τους, το όνομα, το προφίλ και ένα κοινό κλειδί πιστοποίησης. Η τεχνολογία διαθέτει ευφυΐα όσον αφορά την αποφυγή κατειλημμένων καναλιών, χρησιμοποιώντας την τεχνική εναλλαγής συχνότητας (Frequency Hopping Spread Spectrum - FHSS) για να αλλάζει κανάλια. Το Bluetooth βρίσκει εφαρμογή σε πολλές κινητές και wearable συσκευές. Δυστυχώς όμως οι μηχανισμοί ασφαλείας που χρησιμοποιεί δεν είναι ικανοποιητικοί ώστε να μπορούν να εμποδίσουν τις περιπτώσεις υποκλοπών και για το λόγο αυτό δεν μπορεί να ικανοποιήσει τις απαιτήσεις ασφαλείας όπως τα άλλα πρωτόκολλα ασύρματης επικοινωνίας. Η τεχνολογία αν και παρουσιάζει ένα θέμα με τις παρεμβολές από το Wi-Fi, είναι έτσι σχεδιασμένη ώστε να μπορεί να λειτουργεί σωστά σε περιβάλλοντα με θόρυβο [37].

Το BLE (Bluetooth Low Energy) απότελεί παραλλαγή της τεχνολογίας Bluetooth και βρίσκει εφαρμογή σε συσκευές με χαμηλή κατανάλωση ενέργειας, που μπορούν να λειτουργούν με μπαταρία coin cell για μεγάλο χρονικό διάστημα. Μια βελτιωμένη έκδοση του BLE απότελεί το Bluetooth 5 το οποίο έχει καλύτερη εμβέλεια, βελτιωμένη επιλογή καναλιών και αυξημένο ρυθμό μετάδοσης δεδομένων, έχοντας ως σκοπό την υποστήριξη συσκευών ΔτΠ. Το πρωτόκολλο BLE θεωρείται η βέλτιστη επιλογή για συσκευές που δεν απαιτούν συνεχή σύνδεση με back-end διακομιστές, αλλά ταυτόχρονα έχουν τη δυνατότητα να μεταδώσουν τα ελάχιστα απαραίτητα δεδομένα σε πολύς συγκεκιρμένες χρονικές περιόδους. Μετά τη μετάδωση γίνεται άμεση απενεργοποίηση της συσκευής, ώστε να έχουμε τη καλύτερη εξοικονόμηση ενέργειεας για μακροχρόνια χρήση. [18].

III) Zigbee (IEEE 802.15.4)

Βασισμένο στο ασύρματο πρότυπο 802.15.4, το ZigBee είναι ένα πρωτόκολλο επικοινωνίας που λειτουργεί στους 2,4GHz, με εύρος κάλυψης της τάξης των 100 μέτρων και υποστηρίζει ταχύτητα μετάδοσης δεδομένων των 250Kbps. Το πρωτόκολλο χρησιμοποιείται στα δίκτυα αισθητήρων (Wireless Sensor Network - WSN) παρέχοντας υψηλή αξιοπιστία, χαμηλό κόστος, χαμηλή κατανάλωση, δυνατότητες επέκτασης και χαμηλό ρυθμό μετάδοσης δεδομένων. Με σωστή διαμόρφωση, έχει τη δυνατότητα να είναι ένα από τα περισσότερο ασφαλή οικιακά πρωτόκολλα επικοινωνίας, καθώς χρησιμοποιεί την ίδια τεχνολογία κρυπτογράφησης που χρησιμοποιείται από διεθνείς τράπεζες και χρηματοπιστωτικά ιδρύματα. Όντας ένα πρωτόκολλο δικτύου πλέγματος, ένα δίκτυο ZigBee περιλαμβάνει τρεις (3) τύπους συσκευών: έναν ελεγκτή (coordinator) ο οποίος συντονίζει τη σύνθεση του δικτύου, έναν δρομολογητή (router) που επεκτείνει το εύρος και τελικές συσκευές (end device) δικτύου. Καθώς κάθε συσκευή μπορεί να χρησιμοποιηθεί ως δρομολογητής, οι τελικές συσκευές ZigBee δεν χρειάζεται να επικοινωνούν απευθείας με ένα κεντρικό hub [45].

IV) Z-WAVE

Το Z-WAVE αποτελεί εναλλακτική λύση του ZigBee και δημιουργήθηκε ειδικά για οικιακούς αυτοματισμούς. Το Z-WAVE σχηματίzει δίκτυα πλέγματος, δίνοντας τη δυνατότητα στις συσκευύες να επικοινωνούν μεταξύ τους χωρίς να χρειάζεται να υπάρχει κεντρική πύλη ή ελεγκτής. Με μικρό ρυθμό μετάδοσης δεδομένων που φτάνουν το πολύ τα 100Kbps, το Z-Wave προσφέρει επικοινωνία χαμηλής καθυστέρησης σε μια μεγάλη λίστα υποστηριζόμενων συσκευών, οι οποίες μπορούν να επικοινωνούν και να αλληλοεπιδρούν μεταξύ τους. Λειτουργεί στη συχνότητες των 800-900Mhz έχοντας το πλεονέκτημα να αποφεύγει τις παρεμβολές των 2,4GHz που λειτουργούν τα περισσότερα πρωτόκολλα [46].

V) 6LowPAN

Το 6LowPAN είναι μια τεχνολογία δικτύωσης που επιτρέπει την αποτελεσματική μεταφορά πακέτων IPv6 μέσα σε μικρά πλαίσια του στρώματος ζεύξης, όπως αυτά που ορίζονται από το IEEE 802.15.4. Η αρχική σχεδίαση του ήταν για να μπορέσει να υποστηρίξει τα IEEE 802.15.4 ασύρματα δίκτυα χαμηλής ισχύος στη ζώνη των 2,4GHz αλλά κατάφερε να καθιερωθεί στην εξυπηρέτηση πολλών άλλων δικτύων όπως είναι τα ασύρματα δίκτυα χαμηλής ισχύος σε συχνότητες κάτω από το 1GHz. Οι ταχύτητες τις οποίες υποστηρίζει είναι από 20 εως 250Kbps έχοντας εμβέλεια από 10 μέχρι 100 μέτρα. Επειδή βασίζεται στο IPv6, κάθε συσκευή έχει μια μοναδική διεύθυνση IPv6 και είναι προσβάσιμη από το Διαδίκτυο. Το LoWPAN εκμεταλλεύεται στο έπακρο το πλεονέκτημα της ισχυρής ασφάλειας του AES-128 στρώματος ζεύξης που ορίζεται στο IEEE 802.15.4. Συνδιάζει όλα τα εκείνα τα χαρακτηριστικά που χρειάζονται για την ιδανική χρήση σε ένα οικιακό έξυπνο σπίτι, τα οποία είναι: να μπορεί να υποστηρίξει μεγάλα δίκτυα σε τοπολογία πλέγματος, η ισχυρή επικοινωνία και η πολύ μικρή κατανάλωση ισχύος [18].

VI) ECHONET Lite

Το ECHONET Lite είναι ένα ανοικτό δικτυακό πρωτόκολλο που αναπτύχθηκε από την Ιαπωνική εταιρεία ECHONET Consortium (Energy Conservation and Homecare NETwork) το 2011, με σκοπό την επίλυση προβλημάτων, όπως το περιβαλλοντικό ζήτημα και το ζήτημα της ηλικιωμένης κοινωνίας. Το πρωτόκολλο είναι κατάλληλο για το σύγχρονο περιβάλλον και την τελευταία λέξη της τεχνολογίας επικοινωνιών. Ένα από τα χαρακτηριστικά του ECHONET Lite είναι ότι είναι δυνατό να αναπτυχθεί εύκολα σε έξυπνα περιβάλλοντα, όπως το έξυπνο σπίτι, συνδυάζοντας συσκευές και αισθητήρες που διατίθενται στην αγορά. Η χρήση του στοχεύει στην παροχή αξιοπιστίας και χαμηλής κατανάλωσης, χρησιμοποιώντας τις υφιστάμενες υποδομές. Η λειτουργία του βασίζεται στη δημιουργία συστημάτων επικοινωνίας μεταξύ συσκευών όπου στο σύνολο τους θα αποτελούν ένα domain [47].

ΚΕΦΑΛΑΙΟ 2

ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΩΝ ΈΞΥΠΝΩΝ ΟΙΚΙΑΚΩΝ ΣΥΣΚΕΥΩΝ ΣΤΟ ΠΕΡΙΒΑΛΛΟΝ ΔΤΠ

Η εφαρμογή μηχανισμών ασφαλείας σε ένα έξυπνο σπίτι που λειτουργεί σε περιβάλλον ΔτΠ, αποτελεί πραγματική πρόκληση. Εξαιτίας της πολύπλοκης φύσης και των διαφορετικών τεχνολογιών που συνθέτουν ένα τέτοιο περιβάλλον, η εφαρμογή κοινών μηχανισμών σε όλες τις συσκευές, είναι κάτι παραπάνω από δύσκολη διαδικασία. Επίσης δύσκολη είναι και η επεκτασιμότητα, η χρησιμότητα και το επίπεδο προστασίας σε ένα οικιακό δίκτυο, λόγω της διαφορετικής φύσης κάθε συσκευής με τα πρωτόκολλα τα οποία χρησιμοποιεί και τους τρόπους που επικοινωνεί. Λόγω των ευαίσθητων πληροφοριών που μεταδίδονται αλλά και των συσκευών που μπορεί να είναι συνδεδεμένες σε ένα τέτοιο δίκτυο, όπως οι IP κάμερες, οι έξυπνες κλειδαριές ή τα μικρόφωνα που μπορεί να έχουν κάποιες οικιακές συσκευές, η εύρεση τρόπου εφαρμογής των κατάλληλων μηχανισμών ασφαλείας, είναι επιτακτικής ανάγκης. Τα βασικά θέματα ασφαλείας έχουν να κάνουν με τη δομή του οικιακού δικτύου, η οποία σύμφωνα με τα όσα αναφέρθηκαν στο προηγούμενο κεφάλαιο, έχει άμεση σχέση με τις οικιακές συσκευές που είναι συνδεδεμένες στο δίκτυο, τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται και τις υπηρεσίες που χρησιμοποιούνται από τους χρήστες. Με άλλα λόγια, εξαρτώνται ουσιαστικά από τα χαρακτηριστικά του περιβάλλοντος ΔτΠ στο οποίο λειτουργεί το έξυπνο σπίτι. Η κατανόηση αυτών των θεμάτων καθίσταται πιο εύκολη από την ανάλυση της δομής του δικτύου ΔτΠ, μέσα από την οποία είναι εύκολη η εξαγωγή συμπερασμάτων, ως προς την ύπαρξη ζητημάτων ασφάλειας και προστασίας της ιδιωτικότητας σε κάθε ένα από τα επίπεδα από τα οποία αποτελείται.

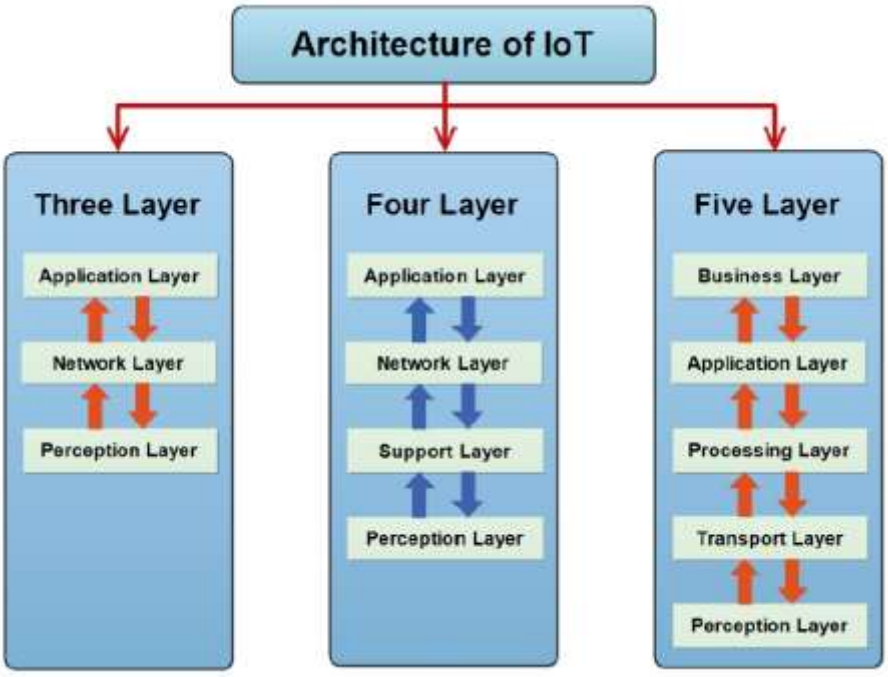
2.1 Αρχιτεκτονικές δομές περιβάλλοντος ΔτΠ

Παρά τα όποια οφέλη δημιουργούνται από τη χρήση του ΔτΠ, οι προκλήσεις που απορρέουν από την εφαρμογή του σε διάφορους τομείς της καθημερινότητας είναι αρκετές, όπως η κακή διαχείριση, η ενεργειακή απόδοση, η διαχείριση ταυτότητας, η ασφάλεια και προστασία της ιδιωτικότητας, με τις δύο τελευταίες να αποτελούν τα πιο κρίσιμα ζητήματα που αντιμετωπίζει η ανάπτυξη του [48]. Η κρισιμότητα αυτών των θεμάτων είναι σαφής από τη στιγμή που στο περιβάλλον ΔτΠ όλες οι συσκευές είναι συνδεδεμένες με το Διαδίκτυο, καθώς χωρίς αυτή τη σύνδεση, δεν μπορούν να λειτουργήσουν σε ένα τέτοιο περιβάλλον. Επομένως, τα θέματα ασφάλειας και ιδιωτικότητας που μπορούν να αντιμετωπίσουν οι έξυπνες οικιακές συσκευές στο περιβάλλον ΔτΠ είναι άρρηκτα συνδεδεμένα με τη χρήση του Διαδικτύου για την ορθή λειτουργικότητά τους [49].

Με την χρήση του Διαδικτύου να αποτελεί αναπόσπαστο κομμάτι του περιβάλλοντος ΔτΠ, τα θέματα της ασφάλειας και της προστασίας της ιδιωτικότητας που αφορούν τον κυβερνοχώρο, αυτόματα μεταφέρονται και στον τομέα εφαρμογής του ΔτΠ, που στην προκειμένη περίπτωση και στα πλαίσια της παρούσας εργασίας, είναι το έξυπνο σπίτι. Επομένως, η ανάλυση της αρχιτεκτονικής δομής του ΔτΠ αποκτά μεγάλη σημασία ως προς την εξέταση των απαιτήσεων που αφορούν τα θέματα αυτά, καθώς με τον τρόπο αυτό δίνεται ευκολότερα η δυνατότητα μελέτης των χαρακτηριστικών του περιβάλλοντος ΔτΠ, ώστε να

γίνει η αναγνώριση και η κατηγοριοποίηση των θεμάτων ασφάλειας και προστασίας της ιδιωτικότητας που προκύπτουν σε κάθε επίπεδο [50].

Στη βιβλιογραφία δεν βρήκαμε να υπάρχει μια κοινά απόδεκτή γενική αρχιτεκτονική δομή του ΔτΠ. Διάφορες αρχιτεκτονικές δομές έχουν κατα καιρούς παρουσιαστεί από την ακαδημαϊκή και ερευνητική κοινότητα. Σύμφωνα με ορισμένους ερευνητές, η αρχιτεκτονική του ΔτΠ έχει τρία επίπεδα, ενώ άλλοι υποστηρίζουν την αρχιτεκτονική των τεσσάρων επιπέδων. Η αρχιτεκτονική των τεσσάρων επιπέδων σε σχέση με αυτή των τριών, πιστεύουν ότι μπορεί να ικανοποιήσει καλύτερα τις απαιτήσεις που υπάρχουν σχετικά με την ασφάλεια. Λόγω των προκλήσεων που αντιμετωπίζει το ΔτΠ σχετικά με την ασφάλεια και την προστασία της ιδιωτικότητας, πολλοί ερευνητές πιστεύουν ότι μόνο η αρχιτεκτονική των πέντε επιπέδων μπορεί να πληροί τις απαιτήσεις αυτές [51].



Εικόνα 6: Αρχιτεκτονικές δομές περιβάλλοντος ΔτΠ (α) τριών, (β) τεσσάρων και (γ) πέντε επιπέδων [49]

Η αρχιτεκτονική τριών επιπέδων είναι η πρωταρχική αρχιτεκτονική δομή που ικανοποιεί την βασική ιδέα του ΔτΠ και προτάθηκε στα πρώτα στάδια ανάπτυξης του. Αποτελείται από τρία επίπεδα: το επίπεδο αντίληψης (perception layer), το επίπεδο δικτύου (network layer) και το επίπεδο εφαρμογών (application layer), όπως φαίνεται στην εικόνα 6(α). Λόγω της συνεχούς ανάπτυξης στο ΔτΠ, η αρχιτεκτονική των τριών επιπέδων δεν μπορούσε να πληροί όλες τις απαιτήσεις του. Ως εκ τούτου, οι ερευνητές πρότειναν μια αρχιτεκτονική με τέσσερα επίπεδα. Στην εν λόγω αρχιτεκτονική δομή, στα τρία προαναφερθέντα επίπεδα προστίθεται και ένα τέταρτο, το επίπεδο υποστήριξης (support layer) (Εικ. 6(β)). Η αρχιτεκτονική των τεσσάρων επιπέδων έπαιξε σημαντικό ρόλο στην ανάπτυξη του ΔτΠ, καθώς πληρούσε πολλές από τις απαιτήσεις ασφάλειας της τεχνολογίας. Όμως δεν μπορούσε να αντιμετωπίσει τα ζήτημα της προστασίας της ιδιωτικότητας. Για το λόγο αυτό, οι ερευνητές πρότειναν μια αρχιτεκτονική δομή των πέντε επιπέδων (Εικ. 6(γ)). Στην αρχιτεκτονική αυτή, τα μόνα κοινά επίπεδα είναι αυτά της αντίληψης και των εφαρμογών. Τα υπόλοιπα τρία αφορούν το επίπεδο μεταφοράς (transport layer), το επεξεργασίας (processing layer) και το επίπεδο επιχειρήσεων (business layer). Η προτεινόμενη αρχιτεκτονική έχει τη δυνατότητα να πληροί όλες τις απαιτήσεις του ΔτΠ που αφορούν την ασφάλεια και την προστασία της ιδιωτικότητας [51].

Στις επόμενες ενότητες θα παρουσιαστεί μια ανάλυση των πέντε επιπέδων της αρχιτεκτονικής δομής του ΔτΠ, καθώς και των θεμάτων ασφάλειας και προστασίας της ιδιωτικότητας που αντιμετωπίζει καθένα από αυτά.

2.2 Θέματα ασφάλειας στο επίπεδο αντίληψης

Το επίπεδο αντίληψης αποτελεί το πρώτο επίπεδο της αρχιτεκτονικής δομής του ΔτΠ. Οι συσκεύες που αποτελούν το επίπεδο αντίληψης έχουν τη δυνατότητα να αντιλαμβάνονται, συλλέγουν, αποθηκεύουν, αναλύουν και μεταδίδουν τις αλλαγές που συμβαίνουν στο φυσικό περιβάλλον, μέσα από τα αισθητήρια όργανα που περιλαμβάνουν. Άλλες ονομασίες που δίνονται στο συγκεκριμένο επίπεδο είναι επίπεδο συσκευών (device layer) ή επίπεδο αισθητήρων (sensor layer) [8].

Στο επίπεδο αντίληψης τα θέματα που υπάρχουν σε ένα οικιακό περιβάλλον ΔτΠ, σχετίζονται κατά κύριο λόγο με την έλλειψη ενός ενιαίου πρότυπου κατασκευής. Στη αγορά υπάρχουν πλέον χιλιάδες συσκευές από διαφορετικούς κατασκευαστές, όπου ο καθένας φτιάχνει τα δικά του χαρακτηριστικά και εφαρμόζει τη δικιά του φιλοσοφία. Δεν υπάρχει λοιπόν ένας κοινός μηχανισμός ασφαλείας που να εφαρμόζεται [52]. Σε πολλές περιπτώσεις οι συσκευές δεν περιλαμβάνουν ενσωματωμένο κάποιο μηχανισμό ασφαλείας, όπως αριθμό PIN ή γνησιότητα χρήστη, και σώζουν τοπικά τα δεδομένα χωρίς καμία κρυπτογράφηση. Η έλλειψη οθόνης αφής ή πληκτρολογίου για την εφαρμογή κάποιου password είναι ένα θέμα που δεν βοηθάει στην εφαρμογή μηχανισμών ασφαλείας που θα προστατεύουν επαρκώς τις συσκευές. Επίσης το μέγεθος τον συσκευών παίζει σημαντικό ρόλο, καθώς αρκετές από τις συσκευές, λόγω του μικρού μεγέθους τους, έχουν απλούς επεξεργαστές με περιορισμένο εύρος λειτουργίας, που καθιστά δύσκολη την εφαρμογή περίπλοκων μηχανισμών ασφάλειας [53]. Η μη εφαρμογή κρυπτογράφησης κάνει τα δεδομένα ευάλωτα σε πιθανές κυβερνοεπιθέσεις. Χωρίς κατάλληλη κρυπτογράφηση τα δεδομένα είναι πλέον εύκολος στόχος για υποκλοπή κατά τη μετάδοση, από κακόβουλους χρήστες [54].

Σημαντικό θέμα στο κομμάτι της ασφάλειας των συσκευών αποτελεί και η σχέση της συλλογής δεδομένων από τις συσκευές με την άγνοια των χρηστών όσον αφορά τη διαχείριση των δεδομένων που τους αφορούν. Καθώς η ευφυΐα γίνεται πλέον το βασικό χαρακτηριστικό των συσκευών, οι χρήστες χάνουν ολοένα και περισσότερο τη δυνατότητα παρακολούθησης και ελέγχου των προσωπικών πληροφοριών που συλλέγονται από αυτές και έχουν πλήρη άγνοια για το τι γίνεται με τα δεδομένα που μεταφέρονται μέσω των συσκευών στο Διαδίκτυο. Οι κίνδυνοι κοινής χρήσης δεδομένων μέσω έξυπνων συσκευών δεν είναι πάντοτε ξεκάθαροι, ιδιαίτερα καθώς ιδιωτικές εταιρείες και κυβερνητικοί οργανισμοί μπορούν να συνδυάσουν δεδομένα και προσωπικές πληροφορίες από διαφορετικές πηγές ώστε να δημιουργήσουν το κατάλληλο μοτίβο που θα αναγνωρίζει τις συνήθειες, τις κινήσεις και ακόμη και τα συναισθήματα των χρηστών [55].

Σε επίπεδο συσκευών τα θέματα που υπάρχουν σε ένα οικιακό περιβάλλον ΔτΠ, σχετίζονται με μη αξιόπιστες παραμετροποιήσεις, έλλειψη ή ελλιπείς μηχανισμούς ταυτοποίησης, εμπιστοσύνη σε εφαρμογές τρίτων, κενά στο υλικολογισμικό της συσκευής και χρήση αδύναμων ή τυποποιημένων κωδικών διαχείρισης. Βάση ερευνών, περίπου το 80% των έξυπνων οικιακών συσκευών που λειτουργούν σε περιβάλλον ΔτΠ είναι ευάλωτες σε κυβερνοεπιθέσεις [56]. Καθώς ένα σύστημα ΔτΠ αποτελείται από τα πέντε επίπεδα που αναφέρθηκαν στην προηγούμενη ενότητα, οι κυβερνοεπιθέσεις και οι κακόβουλες ενέργειες έχουν ως στόχο να χτυπήσουν ένα από αυτά τα επίπεδα ή ακόμα και όλα μαζί.

2.2.1 Ετερογενής αρχιτεκτονική

Όπως έχει ήδη αναφερθεί, ένα έξυπνο σπίτι αποτελείται από μια πληθώρα έξυπνων οικιακών συσκευών που λειτουργούν σε περιβάλλον ΔτΠ, το οποίο διακρίνεται από την ετερογένεια των συστημάτων που περιέχει. Καθώς η ετερογενής φύση του περιβάλλοντος ΔτΠ χτίζεται μέσα

από τη σύνδεση των επιπέδων της αρχιτεκτονικής δομής του, μεγάλη πρόκληση αποτελεί η σωστή και ασφαλής επικοινωνία μεταξύ των συσκευών που απαρτίζουν το δίκτυο, αναγνωρίζοντας η μια την άλλη και ανταλλάσσοντας σημαντικά προσωπικά δεδομένα των χρηστών. Η χρήση διαφορετικών συσκευών που η κάθε μια χρησιμοποιεί διαφορετικά πρωτόκολλα και τεχνολογίες επικοινωνίας αποτελεί σημαντικό θέμα που προβληματίζει όλους τους κατασκευαστές, στο να βρεθεί ένα γενικό κοινά αποδεκτό πρότυπο. Τα κενά ασφαλείας είναι δύσκολο να μελετηθούν λόγω της ετερογενής φύσης των συσκευών, καθώς η κάθε συσκευή μεταφέρει τα τρωτά σημεία της στο σύνολο του περιβάλλοντος ΔτΠ. Επομένως, η ασφάλεια των έξυπνων οικιακών συσκευών εξαρτάται σε μεγάλο βαθμό από τη χρήση και εφαρμογή ενός κοινού προτύπου από όλες τις συσκευές πού θα ελαχιστοποιούσε σημαντικά τα θέματα ασφαλείας και προστασίας της ιδιωτικότητας [5].

2.2.2 Έλλειψη κρυπτογράφησης

Η χρήση κρυπτογράφησης στις πληροφορίες που μεταδίδονται μέσα στο περιβάλλον ΔτΠ πρέπει να γίνεται με τέτοιο τρόπο, ώστε μόνο οι χρήστες που έχουν τις κατάλληλες πιστοποιήσεις να έχουν τη δυνατότητα να διαβάσουν τα δεδομένα. Με τη σωστή κρυπτογράφηση αποφεύγονται φαινόμενα όπως είναι η αλλοίωση των δεδομένων και η υποκλοπή τους κατά τη μετάδοση. Αν κάποια δεδομένα μεταδίδονται χωρίς να έχουν κρυπτογραφηθεί τότε είναι πολύ εύκολο για κάποιο κακόβουλο χρήστη να τα υποκλέψει ή να τα αλλοιώσει και να τα χρησιμοποιήσει για να βλάψει το χρήστη ή το σύστημα [13].

Πολλές συσκευές ΔτΠ χρησιμοποιούν μικρή ή καθόλου κρυπτογράφηση κατά την αποθήκευση και μετάδοση των δεδομένων, καθιστώντας τα εύκολη λεία για κάποιον επίδοξο hacker. Επίσης οι διαφορετικοί τύποι κρυπτογράφησης που χρησιμοποιεί η κάθε συσκευή είναι ένα άλλο πρόβλημα καθώς δεν αναγνωρίζονται από όλες τις συσκευές, με αποτέλεσμα να χάνονται δεδομένα ή να στέλνονται μη κρυπτογραφημένα. Επειδή οι έξυπνες οικιακές συσκευές διαχειρίζονται και επικοινωνούν πολύ ευαίσθητες και σημαντικές πληροφορίες των χρηστών, θα πρέπει η εφαρμογή αξιόπιστης και επαρκής κρυπτογράφησης να είναι προτεραιότητα από τους κατασκευαστές ώστε να εφαρμοστούν οι κατάλληλες κοινές μέθοδοι ασφαλείας [57].

2.2.3 Περιορισμένος αποθηκευτικός χώρος και ισχύ

Οι έξυπνες οικιακές συσκευές καθημερινά συλλέγουν και μεταδίδουν ένα τεράστιο όγκο δεδομένων. Τα δεδομένα που συλλέγονται χρειάζεται να επεξεργαστούν, αναλυθούν και αποθηκευτούν από τη συσκευή που τα συλλέγει ή κάποια άλλη συσκευή επεξεργασίας. Η δυνατότητα επεξεργασίας και αποθήκευσης όμως από τις συσκευές ΔτΠ είναι περιορισμένη. Εξαιτίας του μικρού μεγέθους που έχουν συνήθως οι έξυπνες οικιακές συσκευές είναι πολύ περιορισμένες σε επεξεργαστική ισχύ, ενεργειακή κατανάλωση και αποθηκευτική ικανότητα. Είναι δύσκολο λοιπόν να εφαρμοστούν πολύπλοκοι μηχανισμοί ασφαλείας σε αυτές τις συσκευές [20]. Τα παραπάνω καθιστούν τις έξυπνες οικιακές συσκευές αρκετά ευπαθείς σε επιθέσεις άρνησης υπηρεσίας DoS (Denial of Service) [57].

2.2.4 Ελλιπείς μηχανισμοί ταυτοποίησης

Το μεγαλύτερο πρόβλημα ασφάλειας στις έξυπνες οικιακές συσκευές είναι η ελλιπής χρήση μηχανισμών ταυτοποίησης. Ακόμα και στις περιπτώσεις που τέτοιοι μηχανισμοί υπάρχουν, αυτοί είναι αδύναμοι. Οι μέθοδοι ταυτοποίησης έχουν κάποιους κωδικούς ασφαλείας που σκοπός τους είναι να χρησιμοποιηθούν για τη ταυτοποίηση ενός συστήματος ή μιας συσκευής. Όλες οι έξυπνες συσκευές περιλαμβάνουν ενσωματωμένους βασικούς κωδικούς ταυτοποίησης. Οι βασικοί κωδικοί είναι πολύ εύκολο να σπάσουν από απλά εργαλεία ή προγράμματα που μπορεί να έχει ένας hacker. Η δυσκολία όμως που υπάρχει στην αλλαγή των βασικών κωδικών

από άλλους πιο πολύπλοκους αποτελεί ζήτημα για τις συσκευές, καθώς μένουν απροστάτευτες απέναντι σε επιθέσεις που έχουν σκοπό να χτυπήσουν σε αυτό το τομέα [57].

2.2.5 Προβλήματα στο λογισμικό

Καθώς η πληθώρα των έξυπνων οικιακών συσκευών χαρακτηρίζονται από χαμηλή κατανάλωση ενέργειας, μικρή υπολογιστική ισχύ και ελάχιστη ή μηδαμινή αποθηκευτική ικανότητα, τα χαρακτηριστικά αυτά συνοδεύονται ταυτόχρονα από μειωμένη αξιοπιστία του λογισμικού που ενσωματώνουν. Δεν υπάρχουν επαρκείς έλεγχοι για την αποτελεσματική λειτουργία του λογισμικού κατά την εγκατάσταση του από τον κατασκευαστή. Αυτό μπορεί να δημιουργεί πιθανά κενά ασφαλείας που δεν ανακαλύπτονται άμεσα. Επίσης είναι σχεδόν αδύνατη η αναβάθμιση του λογισμικού ώστε να μπορέσουν να διορθωθούν τυχόν κενά ασφαλείας, με αποτέλεσμα να μένει το λειτουργικό ανυπεράσπιστο απέναντι σε κακόβουλες επιθέσεις. Τέλος η χρήση λογισμικού με παρόμοια βάση υλοποίησης από διαφορετικούς κατασκευαστές κάνει τις συσκευές ευάλωτες. Αν μια κυβερνοεπίθεση χτυπήσει μια συσκευή θα είναι πολύ εύκολο να χτυπήσει μια δεύτερη διαφορετική συσκευή που χρησιμοποιεί το ίδιο λογισμικό με τη πρώτη [57].

2.3 Θέματα ασφάλειας στο επίπεδο μεταφοράς

Το επίπεδο μεταφοράς του ΔτΠ πραγματοποιεί τις ίδιες λειτουργίες με το επίπεδο δικτύου των προηγούμενων αρχιτεκτονικών δομών. Είναι υπεύθυνο για την ασφαλή μετάδοση των δεδομένων που έχουν συλλέξει οι συσκευές του επιπέδου αντίληψης. Για τη μετάδοση των δεδομένων σε αυτό το επίπεδο γίνεται χρήση πληθώρας τεχνολογιών όπως είναι οι ασύρματες επικοινωνίες, τα δορυφορικά δίκτυα και οι ενσύρματες επικοινωνίες χαλκού και οπτικών ινών. Σε αυτό το επίπεδο χρησιμοποιούνται και τα περισσότερα πρωτόκολλα ασφαλείας, καθώς η μετάδοση είναι το πιο ευπαθές κομμάτι για να χτυπηθεί από ενδεχόμενες κακόβουλες ενέργειες [13].

Όπως έχει ήδη αναφερθεί, η πολύπλοκη αρχιτεκτονική ενός περιβάλλοντος ΔτΠ κάνει αναγκαστική τη χρήση και εφαρμογή πολλών διαφορετικών πρωτοκόλλων επικοινωνίας. Ως αποτέλεσμα, τα προβλήματα ασφαλείας που αντιμετωπίζει κάθε πρωτόκολλο επικοινωνίας επηρεάζουν αυτό το επίπεδο της δομής του περιβάλλοντος ΔτΠ. Η σημασία των θεμάτων ασφαλείας σε αυτό το επίπεδο σχετίζεται σημαντικά και με τη σημασία των δεδομένων που μεταδίδονται. Όπως έχει επίσης αναφερθεί, η επικοινωνία μεταξύ των έξυπνων οικιακών συσκευών, των κεντρικών κόμβων του δικτύου και το νέφος μπορεί να περιέχει από πολύ απλά δεδομένα, όπως η ενεργοποίηση ή απενεργοποίηση μιας συσκευής, μέχρι κρίσιμης σημασίας πληροφορίες, όπως προσωπικά στοιχεία των χρηστών ή σημαντικούς κωδικούς ασφαλείας. Σχεδόν όλα τα πρωτοκόλλα που εφαρμόζονται για την επικοινωνία στο περιβάλλον ΔτΠ παρουσιάζουν ζητήματα ασφάλειας, όπως αυτά που θα παρουσιαστούν στις επόμενες υποενότητες. Κάποια μπορεί να είναι αρκετά παλιά με αποτέλεσμα να έχουν βρεθεί τρόποι για να παραβιαστούν και να έχει σταματήσει η υποστήριξη τους. Άλλα είναι πολύ καινούργια με αποτέλεσμα να χρειάζονται συνέχεια βελτιώσεις και να παρουσιάζουν ευπάθειες που θέλουν χρόνο για να διορθωθούν. Τέλος πολλές φορές οι τεχνικές προστασίας που εφαρμόζονται δεν είναι επαρκείς, διότι οι συσκευές που χρησιμοποιούν τα πρωτόκολλα έχουν περιορισμούς ως προς την αξιοπιστία, την επεκτασιμότητα και τη συνδεσιμότητα [58].

2.3.1 Θέματα ασφάλειας στα Bluetooth/BLE

Τα πρωτόκολλα Bluetooth / BLE περιλαμβάνουν διάφορους αλγόριθμους ασφαλείας για την κρυπτογράφηση και αποκρυπτογράφηση των πακέτων δεδομένων και τον καθορισμό διαδικασιών σύζευξης (pairing) και ελέγχου ταυτότητας. Η σύζευξη είναι μια διαδικασία που αφορά την προσπάθεια απόκτησης εμπιστοσύνης μιας συσκευής σε μια άλλη μέσω του ελέγχου ταυτότητάς της [59]. Παρόλα αυτά, η διαδικασία σύζευξης αποτελεί και το πλέον τρωτό σημείο

όσον αφορά την ασφάλεια που παρουσιάζουν τα συγκεκριμένα πρωτόκολλα. Οι επιθέσεις μπορούν να πραγματοποιηθούν τόσο κατά τη διάρκεια όσο και μετά το πέρας της διαδικασίας. Για παράδειγμα, οι επιτιθέμενοι μπορεί να εξαπολύσουν επιθέσεις Man-In-The-Middle, βάσει των πληροφοριών που έχουν συλλέξει μετά τη διαδικασία σύζευξης [60].

Εκτός από τα συνηθισμένα είδη επιθέσεων, όπως οι επιθέσεις συσκότισης, παράνομης παρακολούθησης, επέκτασης περιοχής κάλυψης, sniffing και DoS, τα πρωτόκολλα αντιμετωπίζουν και κάποιες άλλες απειλές που μπορούν να επηρεάσουν την απόδοση τους. Η πιο κοινή απειλή που αντιμετωπίζουν οι συγκεκριμένες τεχνολογίες είναι το bluejacking, μια συνήθως αβλαβή απειλή, καθώς χρησιμοποιείται για απλή αποστολή κειμένου, εικόνων ή ηχητικών μηνυμάτων χωρίς την έγκριση των νόμιμων χρηστών των συσκευών. Η δεύτερη απειλή είναι το bluesnarfing. Πρόκειται για μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες, που επιτρέπει την πρόσβαση σε ημερολόγια, λίστες επαφών, email και μηνύματα κειμένου, καθώς και αντιγραφή εικόνων και βίντεο του νόμιμου χρήστη. Το bluesnarfing αποτελεί επίθεση υποκλοπής των πληροφοριών του νόμιμου χρήστη [13].

Επίσης σημαντικό πρόβλημα είναι ότι σε πολλές συσκευές το Bluetooth είναι ενεργοποιημένο από τις βασικές ρυθμίσεις του κατασκευαστή. Η συνεχής λειτουργία του Bluetooth δίνει σε τη δυνατότητα στους φιλόδοξους επιτιθέμενους που χρησιμοποιούν εργαλεία όπως το RedFang και BlueSniff να εξαπολύσουν επιθέσεις bluebugging. Με αυτά τα εργαλεία ο hacker μπορεί να εντοπίσει τις συσκευές που έχουν ανοιχτό το Bluetooth και να συνδεθεί σε αυτές χωρίς να γίνει αντιληπτός από το χρήστη. Το αποτέλεσμα είναι να αποκτά το πλήρη έλεγχο της συσκευής, ελέγχοντας τα δεδομένα που στέλνονται από τη συσκευή [61].

2.3.2 Θέματα ασφάλειας στο Wi-Fi

Παρά το γεγονός ότι αποτελεί το πρωτόκολλο που εφαρμόζεται περισσότερο από κάθε άλλο στις έξυπνες οικιακές συσκευές που λειτουργούν σε περιβάλλον ΔτΠ και παρά την υψηλή αξιοπιστία που παρουσιάζει στην μετάδοση των δεδομένων, το Wi-Fi παρουσιάζει σημαντικά κενά ασφαλείας. Οι μηχανισμοί ασφαλείας που εφαρμόζει μπορούν πλέον εύκολα μέσα σε λίγα λεπτά να παραβιαστούν. Το WEP (Wired Equivalent Privacy) και το WPA (Wi-Fi Protected Access), που είναι από τους πιο παλιούς μηχανισμούς κρυπτογράφησης του WiFi, μπορούν να σπάσουν σε ελάχιστο χρόνο από hackers που έχουν τα κατάλληλα εργαλεία. Ακόμα και το πιο σύγχρονο WPA2 μπορεί να παραβιαστεί, αλλά στη περίπτωση του, ο κακόβουλος χρήστης που θέλει να κάνει την επίθεση, θα χρειαστεί παραπάνω χρόνο για να τα καταφέρει [62].

Επίσης σημαντικό είναι ότι το πρωτόκολλο δεν παρέχει κανένα μηχανισμό κρυπτογράφησης. Επομένως, η αλλαγή οποιουδήποτε μηνύματος είναι εύκολη από τον οποιοδήποτε εισβολέα. Άλλο μεγάλο ζήτημα που παρουσιάζει το Wi-Fi είναι η ευκολία που μπορεί να δεχθεί επιθέσεις λαθρακρόασης (eavesdropping), που αναφέρονται στη μη εξουσιοδοτημένη παρατήρηση και παρακολούθηση της επικοινωνίας των άλλων. Η συγκεκριμένη επίθεση είναι μια διαδικασία συγκέντρωσης πληροφοριών των χρηστών που μεταδίδονται μέσω ασύρματου δικτύου [63].

2.3.3 Θέματα ασφάλειας στο ZigBee

Το ZigBee, όπως και κάθε άλλη ασύρματη τεχνολογία επικοινωνίας, είναι ευάλωτο σε πολλές επιθέσεις δικτύου λόγω της χαμηλής πολυπλοκότητας στο μέγεθος της μνήμης των συσκευών που το χρησιμοποιούν, σε συνδυασμό με την χαμηλή τους υπολογιστική ισχύ. Επίσης, οι περιορισμένες δυνατότητες των συσκευών δεν μπορούν να χρησιμοποιήσουν τα τυποποιημένα πρωτόκολλα ασφαλείας, όπως στους μηχανισμούς δημόσιου κλειδιού. Παρά τις όποιες προσθήκες έχουν γίνει σταδιακά στο ZigBee, για τη βελτίωση της αποδοτικότητας του και των μηχανισμών ασφαλείας που εφαρμόζει, όπως μηχανισμούς κρυπτογράφησης των δεδομένων, οι περιορισμοί στη μνήμη και την επεξεργαστική ισχύ των συσκευών που το χρησιμοποιούν ως πρωτόκολλο επικοινωνίας, απλοποιούν τη κρυπτογράφηση χρησιμοποιώντας σε κάθε

επίπεδο το ίδιο κλειδί ασφαλείας. Με τον τρόπο αυτό, ένας οποιοσδήποτε εν δυνάμει hacker, με τη χρήση των σωστών εργαλείων, θα μπορούσε να σπάσει το κλειδί σε κάποιο από τα επίπεδα της αρχιτεκτονικής δομής του πρωτοκόλλου και να έχει πρόσβαση στα δεδομένα που μεταφέρονται μεταξύ των συσκευών. Επίσης, το κλειδί ασφαλείας που ανταλλάσσεται μεταξύ των συσκευών, είναι αρκετά εύκολο να δεχθεί επιθέσεις sniffing, καθώς έχει μορφή απλού κειμένου [64].

Το ZigBee λειτουργεί σε μόνο 16 κανάλια ραδιοσυχνοτήτων, γεγονός που καθιστά εύκολη την ανεύρεση του καναλιού που χρησιμοποιείται για επικοινωνία από τους επίδοξους hacker, οι οποίοι μπορούν στη συνέχεια να εξαπολύσουν επιθέσεις eavesdropping για να κρυφακούσουν τις μεταδόσεις, να υποκλέψουν πληροφορίες και να αναμεταδώσουν τα παλιά πακέτα έχοντας προσθέσει κακόβουλο περιεχόμενο. Άλλη μια τακτική που εφαρμόζεται είναι η προσθήκη κακόβουλου κόμβου στην επικοινωνία, με αποτέλεσμα τα δεδομένα που μεταδίδονται, να λαμβάνονται και να αναμεταδίδονται μέσω αυτού του κόμβου [65].

2.3.4 Θέματα ασφάλειας στο Z-Wave

Το Z-Wave χρησιμοποιεί ένα κοινό κλειδί ασφαλείας για την επικοινωνία μεταξύ του ελεγκτή με τους κόμβους. Οι πρώτες εκδόσεις του Z-Wave χρησιμοποιούσαν την S0 διαδικασία κρυπτογράφησης και σύζευξης, η οποία όμως παρουσίαζε ένα σοβαρό θέμα ασφάλειας. Για την κρυπτογράφηση χρησιμοποιούσε ένα κλειδί που αποτελείται μόνο από μηδενικά. Καθώς η μετάδοση γίνεται μέσω ραδιοσυχνοτήτων, ένας επιτιθέμενος βρισκόμενος εντός της εμβέλειας μετάδοσης, θα μπορούσε εύκολα να πραγματοποιήσει επιθέσεις sniffing. Στη συνέχεια, σπάζοντας το κλειδί ασφαλείας, θα μπορούσε να έχει πρόσβαση και έλεγχο όλων των συσκευών Z-Wave του δικτύου. Η προσπάθεια που έγινε με την αλλαγή και βελτίωση της διαδικασίας κρυπτογράφησης σε S2, διόρθωσε τα κενά ασφαλείας που παρουσίαζε το S0. Προέκυψε όμως ένα άλλο κενό. Όταν γίνεται σύζευξη μεταξύ μιας συσκευής που χρησιμοποιεί το S0 και μιας που χρησιμοποιεί το S2, ένας κακόβουλος χρήστης που έχει παρεμβάλει στην επικοινωνία μπορεί να υποβαθμίσει το S2 σε S0. Το αποτέλεσμα είναι το S2 να μετατρέπεται σε S0 έχοντας ξανά τις ευπάθειες του S0 [66].

2.3.5 Θέματα ασφάλειας στο 6LoWPAN

Η ασφάλεια στα δίκτυα 6LoWPAN πρέπει να περιορίζει την πρόσβαση δεδομένων μόνο σε εξουσιοδοτημένους χρήστες, να παρέχει ακεραιότητα δεδομένων και να είναι σε θέση να ανιχνεύει την όποια κακόβουλη εισβολή. Από τη στιγμή που το πρωτόκολλο συνδυάζει το πρότυπο IEEE 802.15.4 και το IPv6, απαιτείται ένα σύστημα ανίχνευσης εισβολής για την παρακολούθηση της κυκλοφορίας που προέρχεται και από τις δύο συσκευές σύζευξης. Η έλλειψη ελέγχου ταυτότητας στο επίπεδο 6LoWPAN και οι περιορισμένοι πόροι μνήμης των συσκευών δικτύου καθιστούν τον μηχανισμό κατακερματισμού των πακέτων του 6LoWPAN ευάλωτο σε επιθέσεις. Για παράδειγμα, ένας εισβολέας μπορεί επιλεκτικά να αποτρέψει τη σωστή επανασυναρμολόγηση των πακέτων στον κόμβο προορισμού, απλά στέλνοντας στον εν λόγω κόμβο κομμάτια πακέτων που να είναι συμβατά με το πρωτόκολλο 6LoWPAN [67].

2.4 Θέματα ασφάλειας στο επίπεδο επεξεργασίας

Το επίπεδο επεξεργασίας ή με την εναλλακτική ονομασία επίπεδο μεσαίου λογισμικού (middleware), έχει ως βασικό σκοπό του τη συλλογή των πληροφορίων που αποστέλλονται από το στρώμα μεταφοράς, καθώς και την επεξεργασία τους. Επίσης είναι υπεύθυνο για την εξάλειψη των περιττών πληροφοριών, εξάγοντας μόνο τα δεδομένα που είναι απαραίτητα. Ένα επιπλέον χαρακτηριστικό του επιπέδου είναι πως αφαιρεί μεγάλο μέρος των Big Data του ΔτΠ, κάτι που μπορεί να επηρεάσει την απόδοση της τεχνολογίας. Επιθέσεις με τη χρήση malware και επιθέσεις εξάντλησης πόρων μπορούν να επηρεάσουν το επίπεδο επεξεργασίας και να διαταράξουν την απόδοση του συστήματος [13].

Πέραν από την επεξεργασία των δεδομένων το επίπεδο επεξεργασίας αναλαμβάνει να συνδέσει το σύστημα με το νέφος και την βάση δεδομένων, πραγματοποιώντας παράλληλα και την αποθήκευση των δεδομένων. Καθώς οι τεχνολογίες του νέφους και του ΔτΠ εξελίσονται καθημερινά όλο και περισσότερο, το επίπεδο της επεξεργασίας καταφέρνει να αποκτά πιο ισχυρές δυνατότητες υπολογισμού και αποθήκευσης. Επίσης, αυτό το επίπεδο παρέχει διεπαφές API για κάλυψη των απαιτήσεων του επιπέδου εφαρμογών. Η ασφάλεια της βάσης δεδομένων αλλά και του νέφους αποτελούν επίσης κύρια ζητήματα που πρέπει να αντιμετωπίσει το επίπεδο επεξεργασίας και που επηρεάζουν την ποιότητα των παρεχόμενων υπηρεσιών στο επίπεδο εφαρμογών [68].

2.4.1 Έλεγχος ταυτότητας και εξουσιοδότηση εισόδου

Ο μηχανισμός ελέγχου ταυτότητας παίζει σημαντικό ρόλο στα θέματα ασφάλειας και προστασίας της ιδιωτικότητας του ΔτΠ. Οι υπάρχοντες μηχανισμοί ελέγχου ταυτότητας δεν μπορούν να παρέχουν ακριβείς λεπτομέρειες επαλήθευσης [69]. Για παράδειγμα, κατά την ενημέρωση μιας εφαρμογής μπορεί να ληφθεί και κακόβουλο ωφέλιμο φορτίο, το οποίο οι επίδοξοι εισβολείς μπορούν να χρησιμοποιήσουν για να ελέγξουν τις συσκευές εξ αποστάσεως [70]. Ευπάθειες υπάρχουν και στα μοντέλα εξουσιοδότησης εισόδου στο νέφος. Ένα ψευδώνυμο σε συνδυασμό με ένα κωδικό ασφαλείας είναι τα στοιχεία που χαρακτηρίζουν το χρήστη και ταυτόχρονα κρύβουν τη πραγματική του ταυτότητα. Η συχνή όμως ανανέωση αυτών των στοιχείων για λόγους ασφαλείας κάνει το όλο σύστημα μη αποδοτικό και προκαλεί τεράστιο υπολογιστικό κόστος [68].

2.4.2 Προστασία τοποθεσίας

Η θέση του χρήστη είναι πολύ σημαντική στο περιβάλλον του ΔτΠ. Ανάλογα με τη τοποθεσία στην οποία βρίσκεται, το σύστημα εκπαιδεύεται στο να στέλνει και να εκτελεί συγκεκριμένες ενέργειες αυτόματα. Η θέση του χρήστη δεν προστατεύεται άμεσα αλλά μόνο κάτω από τον περιορισμό που εφαρμόζεται με τη χρήση τους ψευδώνυμου. Σε περίπτωση επίθεσης φυσικής καταγραφής της θέσης, το σύστημα δεν έχει κάποιο περιορισμό για να το αντιμετωπίσει. Ένα σύνολο από hackers θα μπορούσε να στοχεύσει τους κόμβους και τις θέσεις που επισκέπτεται συχνά ο χρήστης. Με αυτό το τρόπο θα έχουν τη δυνατότητα να παρακολουθήσουν και να καταγράψουν τα στοιχεία που αφορούν τη θέση του χρήστη και μεταδίδονται μεταξύ χρήστη και κόμβου, ώστε με τα κατάλληλα εργαλεία να μπορέσουν να υποκλέψουν τα προσωπικά δεδομένα του [71].

2.4.3 Έλλειψη ασφάλειας δεδομένων

Κατά την υλοποίηση του έξυπνου σπιτιού σε περιβάλλον ΔτΠ, το νέφος μπορεί να χρησιμοποιηθεί και ως χώρος αποθήκευσης δεδομένων, καθώς δίνει τη δυνατότητα καλύτερης διαχείρισης των αρχείων και χρήσης τους ανά πάσα στιγμή. Το νέφος σε μια τέτοια περίπτωση αποτελεί αρκετά ευαίσθητη περιοχή, καθώς πολλά αρχεία υψηλής σημασίας, με προσωπικά δεδομένα των χρηστών, αποθηκεύονται εκεί. Για το λόγο αυτό επιθέσεις όπως DDoS, εμφύτευσης SQL και back door, έχουν σαν σκοπό να παραβιάσουν και να αποτρέψουν την ομαλή λειτουργία του [72].

2.4.4 Θέματα ασφάλειας ενοποίησης περιβάλλοντος ΔτΠ και νέφους

Η ενοποίηση του νέφους με το περιβάλλον ΔτΠ έχει παρουσιάσει θέματα στην απόδοση των συστημάτων σχετικά με την επικοινωνία και την αποθήκευση των δεδομένων που μεταδίδονται. Ο τεράστιος όγκος των δεδομένων που πρέπει να επεξεργαστούν, καθώς πλέον οι έξυπνες οικιακές συσκευές είναι εκατομμύρια, αποτελεί ένα ακόμα θέμα που πρέπει να αντιμετωπιστεί άμεσα καθώς τα συστήματα νέφους που υπάρχουν και είναι δύσκολα

επεκτάσιμα. Η φύση του ΔτΠ, με τις χιλιάδες διαφορετικές συσκευές, εφαρμογές και λειτουργικά συστήματα που χρησιμοποιεί, είναι δύσκολο να εναρμονιστεί με το νέφος, αντιμετωπίζοντας πολλούς περιορισμούς [73].

Για την επικοινωνία του νέφους με το περιβάλλον του ΔτΠ, οι περιορισμοί στην ασφάλεια θεωρούνται αναγκαίοι. Το νέφος προσπαθεί να ενταχθεί στα χαρακτηριστικά του πρωτοκόλλου επικοινωνίας που εφαρμόζει το περιβάλλον του ΔτΠ. Ένα κακόβουλο όμως μοντέλο του νέφους έχει σκοπό να καταστρέψει τα πρωτόκολλα επικοινωνίας που εκτελούνται, με σκοπό να παρακάμψει τους μηχανισμούς ασφαλείας. Με αυτή τη μέθοδο έχει τη δυνατότητα να αποσπάσει σημαντικά προσωπικά δεδομένα του χρηστή ή να ελέγξει την επικοινωνία για δικούς του σκοπούς.

Λόγω της δυναμικής λειτουργίας του νέφους στο ΔτΠ, είναι απαραίτητη η ασφαλής αναδρομολόγηση των μηνυμάτων. Κάθε νέος χρήστης που συνδέεται στο περιβάλλον του ΔτΠ και έχει επικοινωνία με το νέφος, θα μπορεί να λαμβάνει κωδικοποιημένα όποια μηνύματα του στέλνονται από τη στιγμή που συνδέθηκε και μετά. Αντίστοιχα ένας χρήστης που αποσυνδέεται δεν θα μπορεί να λαμβάνει πλέον τα μηνύματα που αποστέλλονται, παρά μόνο μέχρι τη στιγμή που ήταν συνδεμένος στο σύστημα.

Τέλος η αξιοπιστία και ο απομακρυσμένος έλεγχος των έξυπνων οικιακών συσκευών μέσα από το νέφος έχει μεγάλη σημασία καθώς επηρεάζεται από όλα τα παραπάνω θέματα, προκαλώντας αμφιβολίες για την σωστά εναρμονισμένη λειτουργία των δύο συστημάτων [74].

2.5 Θέματα ασφάλειας στο επίπεδο εφαρμογών

Το επίπεδο εφαρμογών ορίζει όλες τις εφαρμογές που χρησιμοποιούν την τεχνολογία ΔτΠ, όπως το έξυπνο σπίτι, οι έξυπνες πόλεις, τα έξυπνα οχήματα, κλπ. αναλαμβάνοντας παράλληλα την παροχής αυτών των υπηρεσιών σε αυτές τις εφαρμογές. Ανάλογα με τις πληροφορίες που συλλέγονται από τα αισθητήρια όργανα, ενδέχεται να έχουμε διαφορά των υπηρεσιών σε σχέση με τις εφαρμογές. Η έλλειψη ενός πιστοποιημένου πρότυπου υλοποίησης του επιπέδου εφαρμογών του ΔτΠ, δημιουργεί πολλά διαφορετικά προβλήματα, αυξάνοντας πολύ την πολυπλοκότητα του επιπέδου, καθώς δεν υπάρχει περιορισμός στη χρήση και εφαρμογή διαφορετικών λειτουργικών και τεχνολογιών [75].

Το επίπεδο εφαρμογών παρουσιάζει πολλά ζητήματα βασικό στοιχείο των οποίων είναι η ασφάλεια. Ειδικότερα, όταν το ΔτΠ χρησιμοποιείται για την υλοποίηση ενός έξυπνου σπιτιού, εισάγει πολλά τρωτά σημεία και ευπάθειες του εσωτερικού αλλά και του εξωτερικού δικτύου. Για την εφαρμογή μιας ισχυρής ασφάλειας σε ένα έξυπνο σπίτι που λειτουργεί στο περιβάλλον του ΔτΠ, ένα από τα κύρια ζητήματα είναι ότι οι έξυπνες οικιακές συσκευές παρουσιάζουν περιορισμούς στην υπολογιστική ισχύ και στον χώρο αποθήκευσης [12]. Τα κοινά προβλήματα των εφαρμογών που εμφανίζονται στο επίπεδο αυτό και οι μηχανισμοί ασφαλείας που εφαρμόζονται δεν είναι αποτελεσματικοί σε πολλές περιπτώσεις. Κοινά προβλήματα των εφαρμογών είναι η ταυτοποίηση του χρήστη και η πρόσβαση που αποκτά στα δεδομένα, οι μηχανισμοί που προστατεύουν τα δεδομένα και βοηθούν στην επαναφορά τους, η δυσκολία της διαχείρισης τόσο μεγάλου όγκου δεδομένων και τα κενά ασφαλείας που παρουσιάζουν οι εφαρμογές [75].

2.5.1 Κενά ασφαλείας εφαρμογών

Οι εφαρμογές που σχεδιάζονται και γράφονται για το ΔτΠ δεν είναι ομοιόμορφα δομημένες διότι μπορεί να αποτελούνται από διαφορετικές γλώσσες προγραμματισμού που έχουν γραφτεί από διαφορετικούς προγραμματιστές. Όταν ένας προγραμματιστής γράφει ένα κώδικα από την αρχή για κάποια εφαρμογή μπορεί να παρουσιάσει κενά ασφαλείας στη δομή του. Οι διαφορετικοί εκτελέσιμοι κώδικες είναι αιτίες για buffer overflow. Τα κενά ασφαλείας στη δομή του κώδικά δίνουν τη δυνατότητα στους επίδοξους εισβολείς να πραγματοποιήσουν επιθέσεις έγχυσης κακόβουλου κώδικα, DoS, sniffing και phishing [57].

2.5.2 Μηχανισμοί προστασίας δεδομένων

Οι αλγόριθμοι ασφαλείας και προστασίας που εφαρμόζονται δεν είναι επαρκείς, παρουσιάζοντας αρκετά σφάλματα σε πολλές περιπτώσεις. Στη μετάδοση της επικοινωνίας τα δεδομένα που χρησιμοποιούνται μεταφέρονται μεταξύ των κόμβων και των συσκευών για αποθήκευση και μελλοντική τους επαναφορά από τον χρήστη. Εξαιτίας όμως των θεμάτων ασφαλείας σε αρκετές περιπτώσεις έχουμε απώλειας των δεδομένων, ή ακόμα χειρότερα πλήρη καταστροφή τους, με αποτέλεσμα να χάνονται σημαντικές πληροφορίες. Είναι σημαντικό λοιπόν να υπάρχει επαρκής προστασία των δεδομένων τόσο στη μετάδοση όσο και στην αποθήκευση τους [76].

2.5.3 Διαχείριση των Big Data

Η καθολική χρήση του ΔτΠ και η πληθώρα των συσκευών που χρησιμοποιούνται σε αυτό, σε συνδυασμό με τον αυξανόμενο αριθμό των χρηστών, έχει φέρει ένα τεράστιο όγκο δεδομένων που μεταδίδονται, επεξεργάζονται και διαχειρίζονται από τις εφαρμογές σύμφωνα με τις υπάρχουσες απαιτήσεις. Είναι πολύ εύκολο λοιπόν τα χαθούν δεδομένων κατά τη μετάδοση εξαιτίας παρεμβολών και κακόβουλων παρεμβάσεων. Ο όγκος των δεδομένων είναι σημαντικό να μπορεί να διαχειρίζεται σωστά καθώς μπορεί να προκαλέσει προβλήματα στην απόδοση και χρήση των εφαρμογών αλλά και ολόκληρου του περιβάλλοντος του ΔτΠ [13].

2.5.4 Ταυτοποίηση χρήστη

Η χρήση διαφορετικών εφαρμογών σημαίνει και χρήση τους από πολλούς διαφορετικούς χρήστες. Κάθε εφαρμογή μπορεί να έχει χιλιάδες χρήστες με αποτέλεσμα η προσπάθεια για κακόβουλες προσβάσεις να είναι σαφώς μεγαλύτερη. Η ύπαρξη αδύναμων μηχανισμών ταυτοποίησης, σε συνδυασμό με μη αποτελεσματικά διαπιστευτήρια χρηστών (username και password), δίνει τη δυνατότητα για ευκολότερη κακόβουλη πρόσβαση. Σε αυτή τη περίπτωση μεγάλη σημασία παίζει και η εκάστοτε συσκευή που τρέχει την εφαρμογή και αν έχει επαρκείς πόρους για να τρέξει πολύπλοκους αλγόριθμους ασφαλείας [76].

2.5.5 Θέματα ασφάλειας στο επίπεδο επιχειρήσεων

Το επίπεδο επιχειρήσεων εισήχθη στην αρχιτεκτονική δομή των πέντε επιπέδων, γιατί μας δίνει την δυνατότητα να απεικονίσουμε και να διαχειριστούμε τα δεδομένα του προηγούμενου επιπέδου με τρόπο τέτοιο ώστε να μπορούμε να δημιουργήσουμε αναλυτικά επιχειρηματικά μοντέλα, γραφήματα και διαγράμματα ροής που μας βοηθούν στην αξιολόγηση και υποστήριξη της τεχνολογίας του ΔτΠ [51]. Επιπλέον μα δίνει μια εικόνα για την εκάστοτε λειτουργία και συμπεριφορά των εφαρμογών, ενώ παράλληλα μπορεί και δρα ως διαχειριστής ολόκληρου του συστήματος. Στα υπόλοιπα καθήκοντα του επιπέδου είναι η διαχείριση και ο έλεγχος των εφαρμογών, των επιχειρησιακών μοντέλων και των κερδών του ΔτΠ. Μια επιπλέον λειτουργία που βρίσκουμε σε αυτό το επίπεδο είναι η διαχείριση των απόρρητων δεδομένων του χρήστη, έχοντας ταυτόχρονα τη δυνατότητα να μπορεί να καθορίσει τον τρόπο δημιουργίας, αποθήκευσης και τροποποίησης των πληροφοριών. Θέματα ευπάθειας αυτού του επιπέδου επιτρέπουν στους επίδοξους επιτιθέμενους κακή χρήση των εφαρμογών αποφεύγοντας την επιχειρηματική λογική. Τα περισσότερα προβλήματα σχετικά με την ασφάλεια αφορούν αδυναμίες των εφαρμογών που προκύπτουν από κατεστραμμένο ή απόντα έλεγχο ασφαλείας, οι οποίες αναλύθηκαν σε προηγούμενη ενότητα [13].

ΚΕΦΑΛΑΙΟ 3

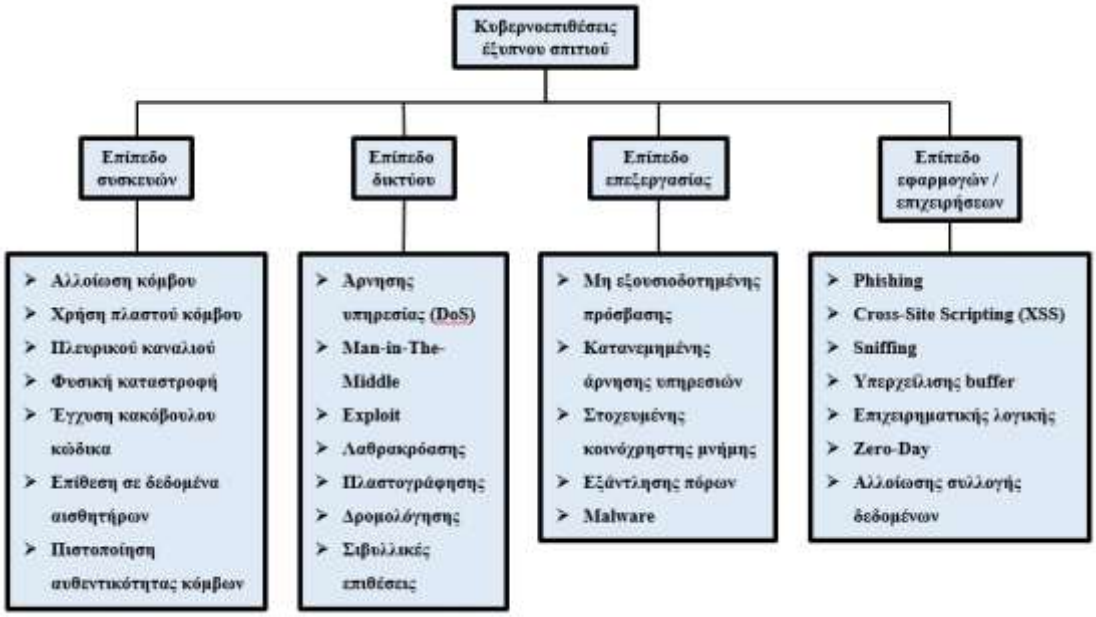
ΑΝΑΛΥΣΗ & ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Η λειτουργία των έξυπνων οικιακών συσκευών σε περιβάλλον ΔτΠ, παρουσιάζει πολλούς κινδύνους. Η σημασία των δεδομένων που μετακινούνται στο οικιακό δίκτυο, η δομή των δικτύων που χρησιμοποιούνται και οι εφαρμογές που βελτιώνουν την καθημερινότητα των ενοίκων του σπιτιού, αποτελεί πρόκληση για τους κακόβουλους χρήστες. Η ασφάλεια και η προστασία όλων των έξυπνων οικιακών συσκευών είναι πολύ σημαντική για τη ζωή των ατόμων που επικοινωνούν και αλληλοεπιδρούν με το περιβάλλον του ΔτΠ. Η πολυπλοκότητα της φύσης του ΔτΠ συνδυάζει πολλές και διαφορετικές προκλήσεις. Οι διαφορετικές έξυπνες οικιακές συσκευές, τα διαφορετικά είδη δικτύων επικοινωνίας, η διαχείριση και αποθήκευση του όγκου των δεδομένων σε συνδυασμό με τη πληθώρα των λογισμικών και εφαρμογών, συνθέτουν ένα δαιδαλώδες περιβάλλον. Η ασφάλεια και η προστασία είναι κύριοι παράγοντες για την ομαλή λειτουργία του συστήματος. Για να μπορεί ένα τέτοιο οικιακό περιβάλλον να είναι αποδοτικό και λειτουργικό θα πρέπει να πληροί τις εξής προϋποθέσεις: εύκολη επεκτασιμότητα, άμεση χρηστικότητα και ικανοποιητική προστασία. Είναι αναγκαίο να ισχύουν όλες οι παραπάνω προϋποθέσεις που αφορούν τα θέματα ασφαλείας, καθώς ενδεχόμενη απώλεια προκαλεί πρόβλημα στο σύνολο της δομής. Πολλές εταιρείες και οργανισμοί προσπαθούν να μελετήσουν και να λάβουν δραστικά μέτρα κατά των επιθέσεων. Σε αυτή την ενότητα θα αναλυθούν μερικές από τις πιο σημαντικές και πιθανές επιθέσεις που μπορεί να δεχθεί το περιβάλλον του ΔτΠ, όσον αφορά τον τρόπο με τον οποίο το επηρεάζουν και θα ταξινομηθούν με βάση το επίπεδο της αρχιτεκτονικής δομής που μπορεί να προσβάλλουν.

3.1 Επιθέσεις κατά της ασφάλειας και ιδιωτικότητας έξυπνου οικιακού περιβάλλοντος ΔτΠ

Η πολυπλοκότητα που παρουσιάζει το περιβάλλον ΔτΠ είναι ο κύριος εχθρός της ασφάλειας ενός έξυπνου σπιτιού. Επίκεντρο των ερευνών όσον αφορά την ασφάλεια ενός έξυπνου σπιτιού είναι τα μεμονωμένα στοιχεία του σύνθετου περιβάλλοντος του ΔτΠ και οι τρόποι επίθεσης εναντίον των έξυπνων οικιακών συσκευών. Η διευκόλυνση και η βελτίωση της ζωής των ενοίκων ενός έξυπνου σπιτιού εξαρτάται από τη σωστή λειτουργία αυτών των συσκευών. Η επίτευξη μιας τέτοιας λειτουργίας καθιστά τους κανόνες του οικιακού αυτοματισμού ακόμα πιο περίπλοκους και ανοίγει ορίζοντες σε πολλές νέες κακόβουλες επιθέσεις, που μέχρι τώρα δεν είχαν διερευνηθεί σε βάθος [77]. Η ασφάλεια και προστασία της ιδιωτικότητας αποτελεί επομένως πραγματική πρόσκληση και απαιτεί περαιτέρω έρευνα για να αντιμετωπιστεί.

Στην εικόνα 7 παρουσιάζονται κάποιες από τις επιθέσεις κατά της ασφάλειας και της ιδιωτικότητας ενός έξυπνου σπιτιού που λειτουργεί σε περιβάλλον ΔτΠ. Η ταξινόμηση των εν λόγω επιθέσεων βασίζεται στην αρχιτεκτονική δομή των πέντε επιπέδων του ΔτΠ που παρουσιάστηκε στο προηγούμενο κεφάλαιο.



Εικόνα 7: Επιθέσεις κατά της ασφάλειας και της ιδιωτικότητας έξυπνου οικιακού περιβάλλοντος ΔτΠ

3.2 Επιθέσεις στο επίπεδο συσκευών

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, το πρώτο επίπεδο της δομής του ΔτΠ, το επίπεδο αντίληψης, αποτελείται από όλες τις έξυπνες συσκευές και τις τεχνολογίες που ενσωματώνουν. Από τη στιγμή που ένα οικιακό δίκτυο που λειτουργεί σε περιβάλλον ΔτΠ μπορεί να περιλαμβάνει μια πληθώρα έξυπνων συσκευών οι οποίες συνδέονται έμμεσα ή άμεσα με το Διαδίκτυο, οι κυβερνοεπιθέσεις εναντίον τους είναι πολλές. Σε αυτό το επίπεδο το μεγαλύτερο ποσοστό των επιθέσεων αφορά την απόκτηση πρόσβασης του επιτιθέμενου στη συσκευή που θέλει να πλήξει. Στην περίπτωση που ο επιτιθέμενος αποκτήσει πρόσβαση στις έξυπνες οικιακές συσκευές, τότε μπορεί να προκαλέσει μεγάλη ζημιά στη λειτουργία του συστήματος [75].

3.2.1 Αλλοίωση κόμβου

Η αλλοίωση κόμβου (node tampering) είναι μια επίθεση που μπορεί να πραγματοποιηθεί πολύ εύκολα αν ο επιτιθέμενος αποκτήσει φυσική πρόσβαση στη συσκευή. Σε αυτή τη περίπτωση θα μπορούσε να την αλλάξει με μια ίδια την οποία έχει προηγουμένως παραμετροποιήσει κατάλληλα. Αλλοίωση θα μπορούσε να γίνει και με την αλλαγή κάποιων εξαρτημάτων της συσκευής. Μια απευθείας σύνδεση με τη συσκευή θα έδινε τη δυνατότητα για πλήρη πρόσβαση σε όλες τις λειτουργίες της συσκευής, καθώς και αλλαγή σημαντικών πληροφοριών. Με τον τρόπο αυτό, ο επιτιθέμενος θα μπορούσε να χρησιμοποιήσει τα ευαίσθητα κλειδιά κρυπτογράφησης της συσκευής, να αλλάξει τον τρόπο επικοινωνίας της μέσα από τους πίνακες δρομολόγησης (routing tables) ή να αχρηστεύσει τελείως την επικοινωνία της με τα ανώτερα επίπεδα της δομής του ΔτΠ [78].

3.2.2 Χρήση πλαστού κόμβου

Η χρήση ενός πλαστού κόμβου (fake node) επικοινωνίας στο πολύπλοκο περιβάλλον του ΔτΠ αποτελεί κλασσική επίθεση στο επίπεδο συσκευών. Ο κακόβουλος χρήστης μπορεί εύκολα να προσθέσει ένα πλαστό κόμβο με σκοπό να στείλει κακόβουλα δεδομένα προς το δίκτυο. Με τον τρόπο αυτό, στο σύστημα αρχίζουν να μεταφέρονται ψεύτικα δεδομένα, χάνοντας έτσι την αξιοπιστία του. Μέσα από αυτή την επίθεση εκτός από ψεύτικα δεδομένα

μπορούν να μεταδοθούν δεδομένα spam. Ο σκοπός της συνεχόμενης αποστολής δεδομένων spam είναι η κατανάλωση της ενέργειας και η μείωση της υπολογιστικής ισχύος των υπόλοιπων έξυπνων συσκευών, ώστε να μην είναι διαθέσιμες για χρήση όταν χρειαστεί. Με αυτό το τρόπο θα μπορούσε να καταρρεύσει η λειτουργία ολόκληρου του συστήματος [75]. Παράδειγμα τέτοιας επίθεσης θα μπορούσε να είναι η ύπαρξη συναγερμού για απόπειρα πυρκαγιάς σε ένα έξυπνο οικιακό περιβάλλον. Εξαιτίας του πλαστού κόμβου, οι έξυπνες οικιακές συσκευές θα έστελναν ψευδή δεδομένα πως όλα λειτουργούν κανονικά ή δεν θα ήταν σε θέση να λειτουργήσουν.

3.2.3 Επιθέσεις πλευρικού καναλιού

Οι επιθέσεις πλευρικού καναλιού (side channel attacks) έχουν ως κύριο στόχο τους να πλήξουν τους μηχανισμούς κρυπτογράφησης των έξυπνων συσκευών. Εν συντομία, μια επίθεση πλευρικού καναλιού στοχεύει την εφαρμογή των μέτρων ασφαλείας και ανακτά μυστικά δεδομένα, αξιοποιώντας πληροφορίες σχετικές με την υλοποίηση των μέτρων αυτών. Για παράδειγμα, τα μυστικά κλειδιά μπορούν να ανακτηθούν με στατιστική ανάλυση του χρόνου απόκρισης ή της κατανάλωσης ισχύος που απαιτούνται κατά την εκτέλεση των αλγορίθμων κρυπτογράφησης. Τα δεδομένα που προστατεύονται σε κρυπτογραφημένα πακέτα μπορούν να αποκαλυφθούν από το μήκος των πακέτων και τον χρόνο απόκρισης [79].

3.2.4 Φυσική καταστροφή

Ως φυσική καταστροφή θεωρείται η άμεση επίθεση στις έξυπνες συσκευές του περιβάλλοντος ΔτΠ, με σκοπό την επίτευξη άρνησης υπηρεσίας (DoS). Το συγκεκριμένο είδος επίθεσης είναι αρκετά δύσκολο να πραγματοποιηθεί καθώς ο κακόβουλος χρήστης θα πρέπει να έχει φυσική πρόσβαση στο χώρο που βρίσκονται οι συσκευές [75]. Αν και η συγκεκριμένη επίθεση μοιάζει αρκετά με την αντίστοιχη της αλλοίωσης κόμβου, διαφέρει σε ένα συγκεκριμένο σημείο. Στην επίθεση της φυσικής καταστροφής, βασικός σκοπός είναι η παύση της λειτουργίας της έξυπνης συσκευής με κάθε τρόπο. Αποτέλεσμα από την επιτυχή κατάληξη μιας τέτοιας επίθεσης είναι η αδυναμία της έξυπνης συσκευής να εξυπηρετήσει τις απαιτήσεις του συστήματος. Ο μόνος τρόπος να αποφευχθεί κάτι τέτοιο είναι η εφαρμογή υψηλών μέτρων ασφαλείας στο χώρο που φιλοξενούνται οι συσκευές. Ειδικά όμως σε έξυπνα οικιακά περιβάλλοντα η εφαρμογή τόσο αυστηρών μέτρων ασφαλείας είναι δύσκολο να υλοποιηθεί [80].

3.2.5 Έγχυση κακόβουλου κώδικα

Στην επίθεση έγχυσης κακόβουλου κώδικα (malicious code injection), όπως και στις περισσότερες που αφορούν το επίπεδο συσκευών, ο επιτιθέμενος πρέπει να έχει άμεση πρόσβαση στη συσκευή για να μπορέσει να την υλοποιήσει. Στην επίθεση αυτή όμως ο σκοπός δεν είναι η φυσική ζημιά της συσκευής αλλά η άμεση πρόσβαση σε αυτή για την εγκατάσταση κακόβουλου κώδικα. Η εγκατάσταση του κακόβουλου κώδικα θα μπορούσε να δώσει πρόσβαση στον επιτιθέμενο σε όλο το περιβάλλον ΔτΠ στο οποίο λειτουργεί η συγκεκριμένη συσκευή. Από τη στιγμή που η επίθεση πραγματοποιείται με επιτυχία, ο κακόβουλος χρήστης αποκτά τον πλήρη έλεγχο της συγκεκριμένης συσκευής, κάτι που του δίνει τη δυνατότητα να καταστρέψει τη συσκευή, να υποκλέψει τα δεδομένα που μεταδίδει ή απλά να παρακολουθήσει τη λειτουργία όλου του συστήματος [81].

3.2.6 Επίθεση σε δεδομένα αισθητήρων

Η επίθεση στα δεδομένα αισθητήρων αποτελεί μια σχετικά απλή εξωσυστημική επίθεση. Στην περίπτωση αυτή, ο επιτιθέμενος χρησιμοποιεί δικά του στοιχεία για να πάρει τις ίδιες μετρήσεις. Αν λοιπόν, για παράδειγμα, ο επιτιθέμενος, χωρίς να γίνει αντιληπτός, τοποθετήσει έναν αισθητήρα θερμοκρασίας κοντά σε έναν αισθητήρα θερμοκρασίας του συστήματος, θα

είναι σε θέση να παίρνει τις ίδιες μετρήσεις με τον αυθεντικό αισθητήρα. Με αυτό το τρόπο θα μπορούσε να μαζεύει κρυφά στοιχεία για τη λειτουργία του συστήματος. Στις επιθέσεις στα δεδομένα αισθητήρων, οι απαιτήσεις εμπιστευτικότητας (confidentiality) των δεδομένων των αισθητήρων μειώνονται, ωστόσο η ακεραιότητα (integrity) και η αυθεντικότητά (authenticity) τους παραμένουν σημαντικά στοιχεία της ασφάλειας του συστήματος και πρέπει να διασφαλιστούν [75].

3.2.7 Πιστοποίηση αυθεντικότητας κόμβων

Η πιστοποίηση της αυθεντικότητας των κόμβων (mass node authentication) δεν αποτελεί επίθεση αλλά μάλλον ένα γενικό πρόβλημα του συστήματος ΔτΠ που μπορεί να χρησιμοποιηθεί για να επηρεάσει την απόδοσή του. Αν ο αριθμός των έξυπνων οικιακών συσκευών είναι μεγάλος, η αξιοπιστία των συσκευών θα πρέπει να πιστοποιείται σε κάθε επικοινωνία τους, ώστε να διατηρείται και η συνολική αξιοπιστία του δικτύου. Με τον τρόπο αυτό όμως προκαλείται ταυτόχρονη μείωση της συνολικής απόδοσης του συστήματος, λόγω του μεγάλου όγκου δεδομένων που μεταφέρεται για την αυθεντικοποίηση των συσκευών [82]. Μια επίθεση που θα χρησιμοποιούσε αυτήν την ευπάθεια του ΔτΠ, θα μπορούσε να είναι ένα μαζικό αίτημα σύνδεσης πολλών νέων συσκευών στο δίκτυο. Η διαδικασία επικοινωνίας και πιστοποίησης τους θα καθυστερούσε ή θα διέκοπτε τελείως την ομαλή λειτουργία του δικτύου.

3.3 Επιθέσεις στο επίπεδο δικτύου

Σύμφωνα με τα όσα αναφέρθηκαν στο προηγούμενο κεφάλαιο, το επίπεδο δικτύων πραγματοποιεί τις ίδιες λειτουργίες με το επίπεδο μεταφοράς της αρχιτεκτονικής δομής του ΔτΠ των πέντε επιπέδων, δηλαδή μεταδίδει με ασφάλεια τις πληροφορίες που συλλέγονται από τις συσκευές αισθητήρων του επιπέδου αντίληψης προς το νέφος ή απευθείας σε άλλους κόμβους του περιβάλλοντος ΔτΠ. Παρά τα όποια μέτρα ασφαλείας για ασφαλή μετάδοση αυτών των πληροφοριών, εξακολουθούν να παρουσιάζονται ζητήματα ασφάλειας, τα οποία μπορεί να επηρεάσουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων [75]. Με βάση το γεγονός ότι το επίπεδο αντίληψης αποτελείται από έναν συνδυασμό πολλών ετερογενών τεχνολογιών, το επίπεδο δικτύου θα πρέπει να είναι σε θέση να υποστηρίξει μια πλειάδα μεθόδων πρόσβασης, στοιχείο που όχι μόνο δυσκολεύει την διαλειτουργικότητα, αλλά δημιουργεί και επιπλέον ζητήματα ασφάλειας. Επίσης, η μεγάλη ποσότητα δεδομένων που συλλέγεται από τους αισθητήρες του επιπέδου αντίληψης, σε συνδυασμό με την επιβάρυνση της επικοινωνίας που προκαλείται από τον μεγάλο αριθμό των ελέγχων ταυτότητας των συσκευών, μπορεί να προκαλέσει συμφόρηση στο οικιακό δίκτυο. Αυτό το πρόβλημα μπορεί να λυθεί με ένα μηχανισμό ελέγχου ταυτότητας των συσκευών που να μην δημιουργεί νέα ζητήματα ασφάλειας [83]. Οι βασικές επιθέσεις σε αυτό το επίπεδο αφορούν την υποκλοπή και την άρνηση υπηρεσίας.

3.3.1 Επιθέσεις άρνησης υπηρεσίας (DoS)

Μια επίθεση DoS εμποδίζει την πρόσβαση των νόμιμων χρηστών σε συσκευές ή άλλους πόρους του δικτύου. Συνήθως επιτυγχάνεται πλημμυρίζοντας τις στοχευμένες συσκευές ή πόρους του δικτύου με περιττές αιτήσεις, προκειμένου να καταστήσει αδύνατο ή δύσκολο στους νόμιμους χρήστες τη χρήση τους. Συχνά, οι επιθέσεις DoS πραγματοποιούνται μέσω κακόβουλων δικτύων (botnet), τα οποία είναι δίκτυα προσβεβλημένων υπολογιστών που έχουν μολυνθεί με κακόβουλο λογισμικό και έχουν τεθεί υπό τον έλεγχο του εισβολέα [84].

3.3.2 Επιθέσεις Man-in-The-Middle

Σε μια επίθεση Man-in-The-Middle, ο εισβολέας παρακολουθεί κρυφά και μεταβάλλει την επικοινωνία μεταξύ των κόμβων αποστολής και λήψης, οι οποίοι πιστεύουν ότι επικοινωνούν

μεταξύ τους απευθείας. Με τον τρόπο αυτό, ο επιτιθέμενος ελέγχει την επικοινωνία των κόμβων και μπορεί να αλλάξει τα μηνύματα που ανταλλάσσονται ανάλογα με τις διαθέσεις του. Οι επιθέσεις αυτού του είδους αποτελούν σοβαρή απειλή για την ασφάλεια πραγματικού χρόνου, επειδή δίνουν στον εισβολέα τη δυνατότητα να συλλάβει και να χειριστεί τις πληροφορίες κατά το δοκούν [85].

3.3.3 Επιθέσεις exploit

Ως επίθεση exploit αναφέρεται οποιαδήποτε παράνομη επίθεση με τη μορφή λογισμικού ή μιας ακολουθίας εντολών, που εκμεταλλεύεται τις ευπάθειες ασφαλείας μιας εφαρμογής, ενός συστήματος ή hardware υλικού. Συνήθης σκοπός τους είναι η απόκτηση ελέγχου του συστήματος και η υποκλοπή πληροφοριών που είναι αποθηκευμένες στο δίκτυο. Οι επιθέσεις exploit συχνά συγχέονται με το κακόβουλο λογισμικό, αλλά ουσιαστικά αποτελούν εισόδους μέσω των οποίων το οποιοδήποτε κακόβουλο λογισμικό μπορεί να εισέλθει σε ένα σύστημα. Οι επιθέσεις exploit μπορεί να πραγματοποιηθούν μέσω της προβολής αναπαραγωγής από ιστότοπους. Με το ξεκίνημα της αναπαραγωγής, ο κρυμμένος κακόβουλος κώδικας μπορεί να αποτυπώσει γρήγορα τον υπολογιστή του χρήστη και να εντοπίσει τον τύπο του λειτουργικού συστήματος που χρησιμοποιεί και τα προγράμματα που εκτελούνται, με σκοπό τον έλεγχο για ελαττώματα και αδυναμίες. Εάν το σύστημα παρουσιάζει κάποια ευπάθεια, μπορεί να την εκμεταλλευτεί και να μολύνει τον υπολογιστή ή το δίκτυο με οποιοδήποτε κακόβουλο λογισμικό, από spyware έως ransomware [86].

3.3.4 Επιθέσεις λαθρακρόασης

Κατά τη μετάδοση των δεδομένων μεταξύ των έξυπνων οικιακών συσκευών ή μεταξύ μιας έξυπνης συσκευής και της πύλης HG, τα δεδομένα είναι πολύ πιθανόν να δεχθούν επίθεση λαθρακρόασης (eavesdropping). Στην περίπτωση αυτή, ο επιτιθέμενος μπορεί να υποκλέψει τα δεδομένα και να τα τροποποιήσει μέσω του καναλιού ασύρματης επικοινωνίας των συσκευών. Οι πληροφορίες που μπορούν να υποκλαπούν με αυτόν τον τρόπο αφορούν το αναγνωριστικό μηνύματος, τις χρονικές σφραγίδες, τις διευθύνσεις των κόμβων πηγής και προορισμού, στοιχεία που μπορεί να οδηγήσουν σε σοβαρή απειλή για την προστασία της ιδιωτικότητας των ενοίκων του σπιτιού [87].

3.3.5 Επιθέσεις πλαστογράφησης

Στις επιθέσεις πλαστογράφησης (spoofing), ο επίδοξος εισβολέας πλαστογραφεί τα σήματα που εκπέμπονται από τις έξυπνες οικιακές συσκευές, με σκοπό την υποκλοπή του αναγνωριστικού των μηνυμάτων. Στη συνέχεια στέλνει δεδομένα που επιθυμεί ο ίδιος πλαστογραφώντας το αναγνωριστικό του εκάστοτε μηνύματος, ξεγελώντας έτσι τη συσκευή στην οποία αποστέλλονται τα μηνύματα ότι προέρχονται από νόμιμη πηγή. Ο τελικός σκοπός της επίθεσης αφορά την απόκτηση πλήρους πρόσβασης του συστήματος από τον επιτιθέμενο [88].

3.3.6 Επιθέσεις δρομολόγησης

Στις επιθέσεις δρομολόγησης, ο επιτιθέμενος προσπαθεί να αλλάξει τις πληροφορίες δρομολόγησης του δικτύου ΔτΠ και να τις διανείμει με σκοπό τη δημιουργία βρόχων δρομολόγησης, τη δημιουργία ψευδών διαφημίσεων διαδρομών, την αποστολή εσφαλμένων μηνυμάτων και γενικότερα οτιδήποτε μπορεί να προκαλέσει κυκλοφοριακή σύγχυση στο δίκτυο ή ακόμα και το μόνιμο μπλοκάρισμα της κυκλοφορίας στο δίκτυο [88].

3.3.7 Σιβυλλικές επιθέσεις

Το περιβάλλον του ΔτΠ είναι ευάλωτο σε Σιβυλλικές επιθέσεις (Sybil attacks), όπου οι εισβολείς μπορούν να διαχειρίζονται ψεύτικες ταυτότητες ή να κάνουν κατάχρηση ψευδο-ταυτότητων, για να θέσουν σε κίνδυνο την αποτελεσματικότητα των συστημάτων. Με τις επιθέσεις αυτές, τα συστήματα ΔτΠ ενδέχεται να δημιουργήσουν λανθασμένες αναφορές και οι χρήστες ενδέχεται να λαμβάνουν ανεπιθύμητο περιεχόμενο ή ακόμα και να χάσουν το απόρρητό τους. Οι Σιβυλλικοί λογαριασμοί που δημιουργούνται από τους εισβολείς διαδίδουν επίσης κακόβουλα προγράμματα και fishing ιστότοπους σε άλλους κακόβουλους χρήστες, με σκοπό την επιπλέον υποκλοπή των προσωπικών στοιχείων των νόμιμων χρηστών. Η ανακάλυψη ενός Σιβυλλικού λογαριασμού είναι ιδιαίτερα δύσκολη υπόθεση, γεγονός που καθιστά την προστασία του περιβάλλοντος ΔτΠ από επιθέσεις τέτοιου είδους, πρωταρχικής σημασίας [89].

3.4 Επιθέσεις στο επίπεδο επεξεργασίας

Σκοπός του επιπέδου επεξεργασίας είναι ο συνδυασμός των δύο προηγούμενων επιπέδων, αντίληψης και μεταφοράς. Λόγω του μεγάλου όγκου δεδομένων που δημιουργούνται σε αυτά τα επίπεδα, η αποθήκευση και η επεξεργασία των πληροφοριών ουσιαστικά συσχετίζονται με τις δυνατότητες αποθήκευσης της βάσης δεδομένων του έξυπνου οικιακού δικτύου, αλλά και τη σύνδεση του συστήματος με το υπολογιστικό νέφος. Στο περιβάλλον του ΔτΠ, το επίπεδο επεξεργασίας μπορεί να αξιολογήσει αυτόματα τις πληροφορίες και να επεξεργαστεί τα δεδομένα βάσει ευφυούς υπολογιστικής διαδικασίας, αποτελώντας το βασικό λόγο για τον οποίο το συγκεκριμένο επίπεδο συνδέεται με το υπολογιστικό νέφος. Οι τεχνολογίες που χρησιμοποιούνται στο επίπεδο επεξεργασίας, υποστηρίζουν τις διαδικασίες αποθήκευσης και επεξεργασίας των δεδομένων. Ταυτόχρονα όμως, όλα τα τρωτά τους σημεία μεταφέρονται σε αυτό. Για το λόγο αυτό, οι απειλές ασφάλειας που κάνουν το έξυπνο οικιακό δίκτυο ευάλωτο και αφορούν αυτό το επίπεδο, έχουν ως αιχμή τις επιθέσεις νέφους [90].

3.4.1 Επιθέσεις μη εξουσιοδοτημένης πρόσβασης

Η μη εξουσιοδοτημένη πρόσβαση αποτελεί ένα από τα μεγαλύτερα θέματα ασφάλειας που αφορούν γενικότερα τα υπολογιστικά συστήματα. Στην περίπτωση των έξυπνων οικιακών δικτύων, με τις επιθέσεις μη εξουσιοδοτημένης πρόσβασης, ο επιτιθέμενος αποκτά εύκολη πρόσβαση στις υπηρεσίες του συστήματος και είναι σε θέση να τροποποιήσει ή ακόμα και να διαγράψει κρίσιμα δεδομένα που μπορούν να προκαλέσουν μεγάλη ζημιά στο δίκτυο ΔτΠ [80].

3.4.2 Επιθέσεις κατανεμημένης άρνησης υπηρεσιών

Μια επίθεση κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service - DDoS) είναι μια προσπάθεια να τερματιστεί εν μέρει ή πλήρως ο στοχευμένος διακομιστής με μια πλημμύρα από κίνηση στο Διαδίκτυο. Ο πρωταρχικός στόχος αυτής της επίθεσης είναι να διαταράξει την τακτική ροή κυκλοφορίας στον διακομιστή ή το δίκτυο του θύματος. Οι επιθέσεις DDoS είναι ογκομετρικές επιθέσεις και συσκευές που λειτουργούν σε περιβάλλον ΔτΠ με χαμηλή ασφάλεια, όπως κάμερες υπολογιστών, συσκευές παρακολούθησης μωρών και εκτυπωτές, διακυβεύονται για να σχηματίσουν ένα botnet. Ως botnet ορίζεται ένα κακόβουλο δίκτυο υπολογιστών, το οποίο ελέγχεται εξ αποστάσεως, από τον λεγόμενο botmaster, χωρίς τη γνώση ή την έγκριση των κατόχων των μεμονωμένων υπολογιστών. Ο botmaster μπορεί να δημιουργήσει στο νέφος διακομιστές εντολών και ελέγχου, με σκοπό την απόκτηση ευαίσθητων πληροφοριών και μη εξουσιοδοτημένης πρόσβασης σε πόρους του νέφους, σε μια προσπάθεια να το οδηγήσουν σε ασυνήθιστη συμπεριφορά, όπως τη διακοπή των παρεχόμενων υπηρεσιών τους [91].

3.4.3 Επιθέσεις στοχευμένης κοινόχρηστης μνήμης

Στις επιθέσεις στοχευμένης κοινόχρηστης μνήμης, ο επιτιθέμενος εκμεταλλεύεται την κοινόχρηστη μνήμη (cache ή κύρια μνήμη) των εικονικών μηχανών του νέφους. Πρόκειται για μια επίθεση που μπορεί να οδηγήσει σε διάφορους άλλους τύπους επιθέσεων, όπως οι επιθέσεις πλευρικού καναλιού ή οι επιθέσεις έγχυσης κακόβουλου κώδικα [92].

3.4.4 Επιθέσεις εξάντλησης πόρων

Στις επιθέσεις εξάντλησης πόρων (exhaustion attack), ο επιτιθέμενος προσπαθεί να εξαντλήσει τους πόρους του δικτύου ΔτΠ, με σκοπό τη διατάραξη της διαδικασίας επεξεργασίας των δεδομένων. Οι επιθέσεις αυτές εμφανίζονται ως μεταγενέστερο αποτέλεσμα άλλων επιθέσεων, όπως η επίθεση DoS ή επιθέσεων που αποσκοπούν στην εξάντληση των πόρων του συστήματος, όπως οι πόροι μπαταρίας και μνήμης. Η κατανεμημένη φύση του περιβάλλοντος του ΔτΠ αποτρέπει την μεγάλη απειλή αυτών των επιθέσεων και η εφαρμογή διαδικασιών προστασίας εναντίον τους είναι σχετικά εύκολη [93].

3.4.5 Επιθέσεις malware

Τα malware είναι πολυμορφικά (polymorphic) και μεταμορφικά (metamorphic) κακόβουλα λογισμικά με δυνατότητα να αλλάζουν τον κώδικά τους, καθώς διαδίδονται [94]. Η χρήση τους στις επιθέσεις έχει ως στόχο την εμπιστευτικότητα των πληροφοριών των χρηστών. Μια επίθεση με χρήση malware αφορά την εφαρμογή ιών (virus), spyware, adware, δούρειων ίππων (Trojan) και worms, για αλληλεπίδραση με το σύστημα. Μετά την εφαρμογή τους, τα malware παίρνουν τη μορφή εκτελέσιμων κωδικών, σεναρίων και περιεχομένων, που δρουν εναντίον των απαιτήσεων του συστήματος, για υποκλοπή εμπιστευτικών πληροφοριών και πρόκληση επιθέσεων DoS και DDoS [95].

3.5 Επιθέσεις στο επίπεδο εφαρμογών και επιχειρήσεων

Οι διάφορες εφαρμογές που υλοποιούνται στο επίπεδο εφαρμογών παρουσιάζουν διαφορετικές απαιτήσεις ασφαλείας. Η διαφορετικότητα αυτή των εφαρμογών ενισχύεται και από την απουσία κάποιου προτύπου όσον αφορά το σχεδιασμό τους για το περιβάλλον του ΔτΠ. Ένα από τα χαρακτηριστικά του επιπέδου των εφαρμογών είναι η κοινή χρήση των δεδομένων, η οποία αντιμετωπίζει διάφορα προβλήματα, όπως το θέμα του απορρήτου των δεδομένων και του ελέγχου πρόσβασης σε αυτά. Κάθε εφαρμογή μπορεί να προσπελαύνεται από περισσότερους του ενός χρήστες με διαφορετικά δικαιώματα πρόσβασης. Για το λόγο αυτό, το επίπεδο εφαρμογών απαιτεί κατάλληλη πιστοποίηση αυθεντικότητας χρηστών και τον ανάλογο μηχανισμό ελέγχου πρόσβασης [75]. Οι επιθέσεις στο επίπεδο εφαρμογών αφορούν επιθέσεις στο λογισμικό των εφαρμογών και αποτελούν τη μεγαλύτερη πρόκληση για ένα σύστημα ΔτΠ. Οι επιθέσεις αυτές χρησιμοποιούνται για να καταστρέψουν τους πόρους του συστήματος χρησιμοποιώντας επιβλαβείς ιούς, όπως ο trojan, τα warms, το spyware, κ.λπ., που παραβιάζουν την εμπιστευτικότητα των δεδομένων, τροποποιούν τα δεδομένα, προξενούν δυσλειτουργία των συσκευών ΔτΠ και αποκτούν πρόσβαση σε χρήσιμες πληροφορίες [90]. Μπορούν επίσης να δημιουργήσουν κενά (loophole), με σκοπό την απενεργοποίηση της προσβασιμότητας στους πόρους του δικτύου και τη δημιουργία απεριόριστου χρόνου αναμονής σε απεσταλμένα αιτήματα, αλλά και τη δημιουργία διαδρομών επικοινωνίας που αναπαράγουν πακέτα δεδομένων ή εισάγουν μολυσμένα πακέτα δεδομένων [96].

3.5.1 Επιθέσεις phishing

Στις επιθέσεις phishing, ο επιτιθέμενος μπορεί να υποκλέψει χρήσιμες πληροφορίες και να αποκτήσει πρόσβαση σε προσωπικά δεδομένα, πλαστογραφώντας την εξουσιοδοτημένη ταυτότητα των χρηστών. Η απόκτηση πρόσβασης στα προσωπικά δεδομένα των χρηστών

γίνεται με χρήση μολυσμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή διαδικτυακούς συνδέσμους. Τα προσωπικά δεδομένα των χρηστών που μπορεί να υποκλαπούν αφορούν διαπιστευτήρια σύνδεσης, πληροφορίες πιστωτικών καρτών, κ.λπ. [75], [90]. Στο περιβάλλον του έξυπνου σπιτιού, οι έξυπνες οικιακές συσκευές, μεμονωμένα, δεν μπορούν να προσφέρουν προφανή αξία για τους εγκληματίες στον κυβερνοχώρο, ωστόσο μπορούν να παρέχουν μια διεπαφή χρήστη, την οποία κάθε επίδοξος εισβολέας μπορεί να χρησιμοποιήσει για να πραγματοποιήσει κάποιας μορφής επίθεση κοινωνικής μηχανικής (social engineering attack). Για παράδειγμα, ο επιτιθέμενος μπορεί να αποκτήσει τον έλεγχο μιας πλατφόρμας υπηρεσιών νέφους ενός έξυπνου μετρητή ΔτΠ, η οποία παρέχει ενημερώσεις του λογισμικού του μετρητή. Στην περίπτωση αυτή, η επίθεση αποσκοπεί στο να παρακολουθείται η μη κρυπτογραφημένη επικοινωνία μεταξύ των υπηρεσιών νέφους και του έξυπνου μετρητή και να εισάγονται κακόβουλες πληροφορίες στη ροή των δεδομένων ή να αποστέλλονται άμεσα μηνύματα στο μετρητή, αν έχει αποκτήσει τον πλήρη έλεγχο του νέφους. Και στις δύο περιπτώσεις, η επίθεση μπορεί να ενεργοποιεί μήνυμα στον έξυπνο μετρητή, όταν αισθητήρας κίνησης του σπιτιού υποδείξει ότι οι χρήστες είναι σπίτι, που να ζητά αναβάθμιση του λογισμικού του μετρητή. Εάν οι χρήστες δράσουν ανάλογα, τότε έχουν πέσει θύματα ηλεκτρονικού "ψαρέματος" [97].

3.5.2 Επιθέσεις Cross-Site Scripting (XSS)

Οι επιθέσεις Cross-Site Scripting (XSS) αποτελούν το πιο επικίνδυνο είδος επιθέσεων των web εφαρμογών. Πρόκειται για επιθέσεις έγχυσης, στις οποίες οι επιτιθέμενοι εισάγουν client-side scrip, όπως για παράδειγμα java script, σε αξιόπιστους ιστότοπους χιλιάδων επισκεπτών. Ο κώδικας αυτός θα εκτελεστεί στο πρόγραμμα περιήγησης ιστού του θύματος που θα επιχειρήσει να επισκεφθεί τον συγκεκριμένο ιστότοπο. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν μία cross-site scripting ευπάθεια, προκειμένου να παρακάμψουν ελέγχους πρόσβασης, όπως το Same-Origin Policy. Με αυτόν τον τρόπο, οι εισβολείς μπορεί να τροποποιήσουν το περιεχόμενο της εφαρμογής σύμφωνα με τις ανάγκες τους, δημιουργώντας θέματα ασφάλειας, όπως παραβίαση δεδομένων, υποκλοπή cookies, κωδικών πρόσβασης, στοιχείων πιστωτικών καρτών κ.λπ., και να χρησιμοποιήσουν τις πληροφορίες αυτές για παράνομους λόγους. Συσκευές ΔτΠ, όπως αποθήκευση συνδεδεμένη στο δίκτυο (Network-Attached Storage - NAS), δρομολογητές, συστήματα DVR, κάμερες IP και έξυπνοι οικιακοί κόμβοι, είναι μόνο μερικές από τις συνδεδεμένες συσκευές στις οποίες θα μπορούσαν να κρυφτούν script XSS [98].

3.5.3 Επιθέσεις sniffing

Στις επιθέσεις sniffing, ο εισβολέας εισάγει στο σύστημα εφαρμογές sniffer, με σκοπό την απόκτηση πληροφοριών του δικτύου ΔτΠ, οι οποίες θα μπορούσαν να οδηγήσουν ακόμη και στην ολοκληρωτική καταστροφή του μηχανισμού ασφαλείας του επιπέδου εφαρμογών. Τα κυριότερα κακόβουλα εργαλεία που χρησιμοποιούνται σε αυτές τις επιθέσεις αφορούν τα packet sniffer ή packet analyzer, τα οποία είναι λογισμικά που χρησιμοποιούνται για την υποκλοπή και ανάλυση πληροφοριών από τα πακέτα δεδομένων που εισέρχονται σε ένα δίκτυο και εξέρχονται από αυτό. Τα packet sniffers καταγράφουν την κίνηση των πακέτων, συλλαμβάνουν το καθένα από αυτά και, αν απαιτείται, αποκρυπτογραφούν τα δεδομένα τους, δίνοντας ποικίλες πληροφορίες στους επιτιθέμενους [76].

3.5.4 Επιθέσεις υπερχείλισης buffer

Τα υποσυστήματα εφαρμογών είναι πάντα ευάλωτα στις επιθέσεις υπερχείλισης buffer (buffer overflaw attack). Η υπερχείλιση buffer είναι μια ανωμαλία όπου ένα πρόγραμμα, ενώ γράφει δεδομένα σε ένα buffer, υπερβαίνει το όριο του και αντικαθιστά τις παρακείμενες θέσεις μνήμης. Ένας επιτιθέμενος μπορεί να το χρησιμοποιήσει για να ενεργοποιήσει κακόβουλους

κώδικες οι οποίοι θα προξενήσουν τις εξαπόλυση επιθέσεων άλλων ειδών, με απώτερο σκοπό την έκθεση σε κίνδυνο ολόκληρης της υποδομής του δικτύου. Οι επιθέσεις buffer overflow θεωρούνται ως ένα από τα πιο διαδεδομένα είδη επιθέσεων του δικτύου ΔτΠ. Κυρίως προκύπτουν από την έλλειψη οριακού ελέγχου στις λειτουργίες της γλώσσας C για επεξεργασία των buffer δεδομένων. Η γλώσσα C χρησιμοποιείται κατά κόρο στα δίκτυα ΔτΠ, λόγω των περιορισμένων πόρων των έξυπνων συσκευών. Το γεγονός αυτό σε συνδυασμό με τις μεγάλες απαιτήσεις επεξεργασίας δεδομένων, αφήνει τις συσκευές αυτές "ανοιχτές" στο πρόβλημα των επιθέσεων υπερχείλισης buffer. Οι εν λόγω επιθέσεις αποτέλεσαν τη βάση επιθέσεων που έχουν πραγματοποιηθεί σε ένα ευρύ φάσμα στοχευμένων πλατφορμών, όπως βάσεις δεδομένων, συστήματα χαμηλού επιπέδου και λειτουργικά συστήματα [99].

3.5.5 Επιθέσεις επιχειρηματικής λογικής

Οι επιθέσεις επιχειρηματικής λογικής (business logic attack) εκμεταλλεύονται τα ελαττώματα που τυχόν υπάρχουν στον προγραμματισμό των εφαρμογών. Σε μια τέτοια επίθεση, ο επιτιθέμενος ελέγχει και διαχειρίζεται την ανταλλαγή πληροφοριών μεταξύ του χρήστη και της βάσης δεδομένων της εφαρμογής. Τα ελαττώματα που μπορεί να εκμεταλλευτεί ο επιτιθέμενος αφορούν την ακατάλληλη κωδικοποίηση της εφαρμογής, τους κωδικούς πρόσβασης επικύρωσης ανάκτησης δεδομένων, τις επικυρώσεις εισόδου στην εφαρμογή και τεχνικές κρυπτογράφησης [49].

3.5.6 Επιθέσεις Zero-Day

Οι ευπάθειες Zero-Day που μπορεί να παρουσιάσει μια εφαρμογή μπορούν να αποτελέσουν τρύπα ασφαλείας όχι μόνο της ίδιας της εφαρμογής αλλά και ολόκληρου του συστήματος στο οποίο λειτουργεί. Εάν οι ενημερώσεις ασφάλειας της εφαρμογής εκδοθούν μετά από τον εντοπισμό τέτοιων τρωτών σημείων από επίδοξους επιτιθέμενους, τότε μπορεί να υπάρξουν σοβαρές συνέπειες για το σύστημα. Αντιθέτως, η ταυτοποίηση των τρωτών σημείων της εφαρμογής από τους χρήστες μπορεί να βοηθήσει στον μετριασμό αυτών των απειλών, προτού οι εταιρείες προγραμματισμού των εφαρμογών προβούν στην έκδοση των ενημερώσεων ασφαλείας. Έτσι, ο τρόπος και ο χρόνος αναγνώρισης των τρωτών σημείων μιας εφαρμογής παίζουν καθοριστικό ρόλο για τις επιθέσεις Zero-Day σε δίκτυα ΔτΠ. Ένα σφάλμα λογισμικού μπορεί να εντοπιστεί κατά τη φάση δοκιμής του. Ωστόσο, σε ορισμένες περιπτώσεις, μπορεί να περάσει απαρατήρητο και να γίνει εκμεταλλεύσιμο μετά από μεγάλο χρονικό διάστημα χρήσης. Τέτοια σενάρια είναι επικίνδυνα και μετατρέπουν την ευπάθεια Zero-Day σε πιθανή επίθεση. Το όνομα της επίθεσης επινοήθηκε λαμβάνοντας υπόψη τον αμελητέο χρόνο που προσφέρεται στους προγραμματιστές ή στους παρόχους υπηρεσιών για παραποίηση αυτών των τρωτών σημείων μετά την πρώτη τους αναγνώριση. Με την συγκεκριμένη επίθεση, σκοπός του φιλόδοξου εισβολέα είναι να πάρει τον έλεγχο χωρίς τη συγκατάθεση και φυσικά τη γνώση του χρήστη [100].

3.5.7 Επιθέσεις αλλοίωσης συλλογής δεδομένων

Οι επιθέσεις αλλοίωσης της συλλογής δεδομένων (data aggregation distortion attack) πραγματοποιούνται κατά τη μετάδοση δεδομένων προς τις ασύρματες συσκευές των χρηστών από το επίπεδο επιχειρήσεων. Αυτά τα δεδομένα μπορούν να αλλοιωθούν από κάποιον επιτιθέμενο που πραγματοποιεί επίθεση eavesdropping προτού φτάσουν στον προορισμό τους. Με τον τρόπο αυτό ο επιτιθέμενος είναι σε θέση να δημιουργήσει ουσιαστικά προβλήματα στην τοπική επεξεργασία των δεδομένων που μπορεί να πραγματοποιείται από κάποια έξυπνη συσκευή με την αντίστοιχη υπολογιστική ικανότητα [101].

3.6 Σύνοψη των επιθέσεων

Σε ένα έξυπνο σπίτι που λειτουργεί σε περιβάλλον ΔτΠ, οι συσκευές μεταδίδουν πληροφορίες μέσω μη ασφαλούς μέσου και αν κάποιος εισβολέας αποκτήσει πρόσβαση σε

αυτό, τότε μπορεί να αποκτήσει και να διαχειριστεί προς όφελός του πλήθος εμπιστευτικών πληροφοριών που αφορούν τους ενοίκους του. Τα έξυπνα οικιακά δίκτυα είναι ευάλωτα σε απειλές ασφαλείας και προστασίας της ιδιωτικότητας που προέρχονται κυρίως από εξωτερικούς κακόβουλους κόμβους λόγω της σύνδεσης του έξυπνου σπιτιού με το Διαδίκτυο. Στο παρόν κεφάλαιο παρουσιάστηκαν μερικές από τις σημαντικότερες επιθέσεις που μπορεί να δεχθεί το περιβάλλον του ΔτΠ, όσον αφορά τον τρόπο με τον οποίο το επηρεάζουν και ταξινομήθηκαν με βάσει το επίπεδο της αρχιτεκτονικής δομής που μπορεί να προσβάλλουν. Στον πίνακα 1 παρουσιάζεται μια σύνοψη αυτών των επιθέσεων. Στον πίνακα αυτό, παρουσιάζεται ο τύπος της εκάστοτε επίθεσης, τα επίπεδα στα οποία μπορεί να εξαπολυθεί και ο βαθμός επικινδυνότητας του.

Πίνακας 1: Επιθέσεις ανά επίπεδο έξυπνου οικιακού περιβάλλοντος ΔτΠ

Είδος επίθεσης	Επίπεδο αντίληψης /συσκευών	Επίπεδο μεταφοράς /δικτύου	Επίπεδο επεξεργασίας	Επίπεδο εφαρμογών	Επίπεδο επιχειρήσεων	Βαθμός επικινδυνότητας
Αλλοίωση κόμβου	✓	-	-	-	-	Υψηλός
Χρήση πλαστού κόμβου	✓	-	-	-	-	Υψηλός
Πλευρικού καναλιού	✓	-	-	-	-	Μέτριος
Φυσική καταστροφή	✓	-	-	-	-	Μέτριος
Έγχυση κακόβουλου κώδικα	✓	-	-	✓	✓	Υψηλός
Επίθεση σε δεδομένα αισθητήρων	✓	-	-	-	-	Μέτριος
Πιστοποίηση αυθεντικότητας κόμβων	✓	✓	-	-	-	Υψηλός
Άρνηση υπηρεσίας (DoS)	-	✓	-	-	-	Υψηλός
Man-in-The-Middle	-	✓	-	-	-	Υψηλός
Exploit	-	✓	-	✓	-	Υψηλός
Λαθρακρόαση	-	✓	-	-	-	Χαμηλός
Πλαστογράφηση	-	✓	-	-	-	Υψηλός
Δρομολόγησης	-	✓	-	-	-	Υψηλός
Sybil	-	✓	-	-	-	Υψηλός
Μη εξουσιοδοτημένη πρόσβαση	-	-	✓	✓	✓	Υψηλός
Κατανεμημένη άρνηση υπηρεσιών	-	-	✓	-	-	Υψηλός
Στοχευμένη κοινόχρηστη μνήμη	-	-	✓	-	-	Μέτριος
Εξάντληση πόρων	-	✓	✓	-	-	Μέτριος
Malware	-	-	✓	✓	✓	Υψηλός
Phishing	-	-	-	✓	-	Μέτριος
Cross-Site Scripting (XSS)	-	-	-	✓	-	Υψηλός
Sniffing	-	-	-	✓	-	Υψηλός
Υπερχείλιση buffer	-	-	-	✓	✓	Υψηλός
Business logic	-	-	-	-	✓	Μέτριος
Zero-Day	-	-	-	✓	✓	Υψηλός
Αλλοίωση συλλογής δεδομένων	-	-	-	✓	✓	Υψηλός

ΚΕΦΑΛΑΙΟ 4

ΠΑΡΑΔΕΙΓΜΑΤΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Οι τεχνολογίες του οικιακού αυτοματισμού που λειτουργούν σε περιβάλλον ΔτΠ, επιτρέπουν στους χρήστες να έχουν εξ αποστάσεως διαχείριση, έλεγχο και αλληλεπίδραση με τις έξυπνες οικιακές συσκευές μέσω των κινητών συσκευών τους. Λόγω της προσιτότητας και της άμεσης διαθεσιμότητας στους καταναλωτές, οι έξυπνες οικιακές συσκευές που λειτουργούν σε περιβάλλον ΔτΠ είναι πολύ δημοφιλείς, ξεπερνώντας κατά πολύ όλους τους άλλους τομείς στους οποίους μπορεί να εφαρμοστεί η τεχνολογία του ΔτΠ. Οι περισσότερες από αυτές τις συσκευές δεν χρησιμοποιούνται μόνο στο περιβάλλον του έξυπνου σπιτιού, αλλά μπορούν να εγκατασταθούν και σε κρίσιμες υποδομές, όπως εργοστάσια, νοσοκομεία, στρατιωτικές εγκαταστάσεις, κυβερνητικούς οργανισμούς, κ.α. Σε πολλές περιπτώσεις μάλιστα, πολλές από αυτές τις συσκευές αλληλοεπιδρούν άμεσα ή έμμεσα με εξοπλισμό τέτοιων υποδομών, όπως για παράδειγμα οι έξυπνοι μετρητές που επικοινωνούν με το έξυπνο δίκτυο παροχής ηλεκτρικής ενέργειας (smart grid). Μια τέτοια αλληλοεπίδραση έχει ως αποτέλεσμα, επιθέσεις που στοχεύουν την ασφάλεια των έξυπνων οικιακών δικτύων να μπορούν να επηρεάσουν και την ασφάλεια άλλων κρίσιμων υποδομών. Στο παρόν κεφάλαιο γίνεται μια αναφορά πραγματικών κυβερνοεπιθέσεων που είχαν στόχο την υποδομή έξυπνων σπιτιών και την εκμετάλλευση των κενών ασφαλείας τους. Η αναφορά αυτή θα περιλαμβάνει επαληθευμένες επιθέσεις, δηλαδή πραγματικά περιστατικά ή επιθέσεις που έχουν εφαρμοστεί και δημοσιευτεί από μελετητές. Επειδή οι έξυπνες οικιακές συσκευές χρησιμοποιούνται μόνο για υποστήριξη των λειτουργιών ενός έξυπνου σπιτιού και όχι ως μέρος ενός κρίσιμου συστήματος ελέγχου, η ταξινόμηση των επιθέσεων θα γίνει με βάση τον πραγματικό τους στόχο και όχι με βάση την αρχιτεκτονική του συστήματος όπως στα προηγούμενα κεφάλαια.

4.1 Κυβερνοεπιθέσεις σε έξυπνα οικιακά περιβάλλοντα ΔτΠ

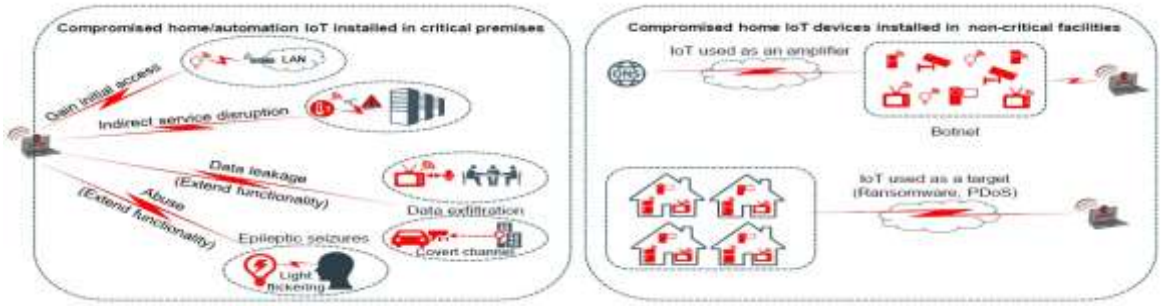
Το 2015, η αμερικανική εταιρεία λογισμικού Symantec παρουσίασε μια έρευνα πάνω στις κοινές ευπάθειες που βρέθηκαν μετά από ανάλυση 50 οικιακών συσκευών που λειτουργούν στο περιβάλλον ΔτΠ. Οι ευπάθειες αφορούσαν αδύναμα σχήματα ελέγχου ταυτότητας (π.χ. χρήση αδύναμων ενσωματωμένων κωδικών πρόσβασης χωρίς καν την εφαρμογή πολιτικών "κλειδώματος"), διαδικασίες ενημέρωσης υλικολογισμικού χωρίς έλεγχο ταυτότητας και χρήση μη κρυπτογραφημένων επικοινωνιών. Επίσης, βρέθηκαν διάφορες ευπάθειες σε πολλές από τις διαδικτυακές εφαρμογές που χρησιμοποιούνται για τον έλεγχο των συσκευών από απόσταση ή στις σχετικές πλατφόρμες νέφους [102].

Πολλοί ερευνητές έχουν ανακαλύψει επίσης, ελαττώματα ασφαλείας σε διάφορα ασύρματα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στις έξυπνες οικιακές συσκευές, όπως τα ZigBee, Z-Wave και Wi-Fi. Η σουηδική εταιρεία παροχής λύσεων κυβερνοασφάλειας Cognosec παρουσίασε μια έρευνα πάνω σε κρίσιμες ευπάθειες που βρέθηκαν σε ZigBee έξυπνες οικιακές συσκευές οι οποίες μπορούν να οδηγήσουν σε ολοκληρωτικό έλεγχο του οικιακού δικτύου από τους επιτιθέμενους. Η πρακτική ανάλυση ασφάλειας κάθε συσκευής που αξιολογήθηκε έδειξε ότι οι εν λόγω συσκευές έχουν σχεδιαστεί για εύκολη εγκατάσταση και χρήση, αλλά δεν διαθέτουν δυνατότητες διαμόρφωσης για την ασφάλεια και εκτελούν μια ευάλωτη διαδικασία σύζευξης που επιτρέπει σε εξωτερικά μέρη να πραγματοποιήσουν με ευκολία επιθέσεις sniffing για την υποκλοπή των κλειδιών κρυπτογράφησης του δικτύου. Αυτό

αποτελεί κρίσιμη ευπάθεια, καθώς η ασφάλεια της κάθε συσκευής εξαρτάται αποκλειστικά από το απόρρητο αυτών των κλειδιών. Δοκιμές με λαμπτήρες, αισθητήρες κίνησης, αισθητήρες θερμοκρασίας και κλειδαριές πόρτας έδειξαν επίσης ότι οι κατασκευαστές των συσκευών εφάρμοσαν τα ελάχιστα χαρακτηριστικά ασφάλειας που απαιτούνται για πιστοποίηση και ότι οι χρήστες δεν διαθέτουν άλλες επιλογές για την αύξηση του επιπέδου ασφάλειας των συσκευών [103].

Οι Badenhop και συν. πραγματοποίησαν ανάλυση ασφάλειας σε δίκτυο έξυπνων οικιακών συσκευών Z-Wave για τον εντοπισμό των τρωτών σημείων που αφορούν την ακεραιότητα του κόμβου πηγής και των δεδομένων του πρωτοκόλλου δρομολόγησης. Οι μελετητές ανακάλυψαν ότι η τοπολογία και οι διαδρομές δρομολόγησης μπορούν να τροποποιηθούν από κάποιον επιτιθέμενο μέσω εκμετάλλευσης του χαρακτηριστικού της τυφλής εμπιστοσύνης που είναι εγγενές στους κόμβους δρομολόγησης του δικτύου. Στην συγκεκριμένη περίπτωση, μια επίθεση Black Hole ήταν αρκετή για να φανερώσει τις ευπάθειες του δικτύου όσον αφορά τη δρομολόγηση [104].

Παρά την ασφάλεια που παρέχουν οι τεχνικές 4-way και group key handshake στις συσκευές Wi-Fi, οι Vanhoef & Piessens, απέδειξαν ότι οι εν λόγω συσκευές είναι ευάλωτες σε επιθέσεις επανεγκατάστασης κλειδιών. Αυτές οι επιθέσεις δεν παραβιάζουν τις ιδιότητες ασφαλείας των συσκευών, αλλά επισημαίνουν τους περιορισμούς των μοντέλων που χρησιμοποιούν, όπως ο μη καθορισμός του χρόνου χρήσης του κλειδιού από το πρωτόκολλο εμπιστευτικότητας δεδομένων. Οι μελετητές απέδειξαν επίσης, ότι και οι τεχνικές PeerKey και fast BSS transition handshake είναι ευάλωτες στις ίδιες επιθέσεις. Αυτές οι ευπάθειες επιτρέπουν στους επιτιθέμενους να χρησιμοποιήσουν την Wi-Fi επικοινωνία των συσκευών για την μετάδοση πλαισίων broadcast και multicast. Τα αποτελέσματα των συγκεκριμένων επιθέσεων εξαρτώνται από τον τρόπο χρήσης του πρωτοκόλλου εμπιστευτικότητας δεδομένων [105].



Εικόνα 8: Παραδείγματα κυβερνοεπιθέσεων εναντίον έξυπνων οικιακών συσκευών [57]

Το 2017, ερευνητές αποκάλυψαν μια λίστα προεπιλεγμένων διαπιστευτηρίων σύνδεσης που αντιστοιχούν σε μεγάλο αριθμό οικιακών δρομολογητών και περισσότερων από 1.700 συσκευών ΔτΠ. Οι ερευνητές ανέφεραν ότι μόνο στις 144 από αυτές τις συσκευές οι χρήστες είχαν αλλάξει το όνομα χρήστη και τον κωδικό πρόσβασης για τον έλεγχο ταυτότητας σε υπηρεσίες telnet [106]. Στην έρευνά της σχετικά με το ζήτημα των botnet, που αποτελούνται κυρίως από έξυπνες οικιακές συσκευές ΔτΠ, βάσει πραγματικών δεδομένων που συλλέχθηκαν μεταξύ Ιανουαρίου και Ιούνιου του 2017, η εταιρία F5 Labs αποκάλυψε μία τεράστια αύξηση των επιθέσεων μέσω των υπηρεσιών telnet εναντίον των συσκευών αυτών [107].

Θεωρητικά, οι κυβερνοεπιθέσεις σε έξυπνες συσκευές ΔτΠ που είναι εγκατεστημένες σε οικιακό περιβάλλον είναι λιγότερο σημαντικές από τις επιθέσεις που εξαπολύονται εναντίον συσκευών που χρησιμοποιούνται σε κρίσιμα δίκτυα, όπως έξυπνα δίκτυα παροχής ηλεκτρικής ενέργειας, μεταφορών ή νοσοκομείων. Ωστόσο, οι έξυπνες οικιακές συσκευές μπορούν επίσης να χρησιμοποιηθούν στις εγκαταστάσεις κρίσιμων υποδομών. Επίσης, αν και σε ένα έξυπνο σπίτι χρησιμοποιούνται μόνο για δευτερεύουσες και υποστηρικτικές λειτουργίες, η φυσική τους εγγύτητα με κρίσιμα συστήματα, μπορεί να προκαλέσει έμμεσες επιθέσεις σε αυτά με

ολέθρια αποτελέσματα. Στην εικόνα 8 παρουσιάζονται τέτοιου είδους επιθέσεις εναντίον έξυπνων οικιακών συσκευών. Οι κυβερνοεπιθέσεις αυτές μπορεί να ενεργοποιηθούν μέσω συσκευών που έχουν σύνδεση με κάποιο κρίσιμο σύστημα. Στην περίπτωση που κάτι τέτοιο δεν ισχύει, οι ευπάθειές τους μπορούν να χρησιμοποιηθούν για την ενίσχυση των επιπτώσεων της εκάστοτε επίθεσης [57].

4.2 Κυβερνοεπιθέσεις σε συσκευές εγκατεστημένες σε κρίσιμα συστήματα

Όπως φαίνεται στην εικόνα 8, οι κυβερνοεπιθέσεις που έχουν ως στόχο έξυπνες οικιακές συσκευές ΔτΠ που είναι εγκατεστημένες σε κρίσιμα συστήματα μπορούν να χωριστούν σε τέσσερεις κατηγορίες [57]: (α) απόκτησης πρόσβασης, (β) έμμεσης διακοπής/άρνησης κρίσιμων υπηρεσιών, (γ) διαρροής δεδομένων και (δ) κακόβουλης χρήσης συστήματος. Αυτές οι επιθέσεις συνήθως επιτυγχάνονται με την επέκταση της λειτουργικότητας των συσκευών με απροσδόκητους τρόπους. Κάποιες από τις κυβερνοεπιθέσεις μπορεί να ανήκουν σε περισσότερες από μία κατηγορίες που παρουσιάζονται στην συγκεκριμένη ταξινόμηση. Για το λόγο αυτό, έγινε προσπάθεια ώστε να τοποθετηθούν στην πιο κατάλληλη. Στον Πίνακα 2 παρουσιάζεται η προτεινόμενη ταξινόμηση των τεσσάρων κατηγοριών κυβερνοεπιθέσεων που έχουν ως στόχο έξυπνες οικιακές συσκευές ΔτΠ που είναι εγκατεστημένες σε κρίσιμα συστήματα, μαζί με την περιγραφή και τον βαθμό επικινδυνότητάς τους.

4.2.1 Κυβερνοεπιθέσεις απόκτησης πρόσβασης

Η εταιρεία Check Point Software Technologies δημοσίευσε τα ευρήματά της όσον αφορά την ευπάθεια που παρουσιάζουν οι έξυπνοι λαμπτήρες Philips Hue στο υλικολογισμικό τους, η οποία επιτρέπει στους εισβολείς να πάρουν τον έλεγχο ενός μεμονωμένου λαμπτήρα, να του περάσουν κακόβουλο υλικολογισμικό και να διαδώσουν κακόβουλο λογισμικό, όπως ransomware ή spyware, σε ολόκληρο το οικιακό δίκτυο. Η πραγματική ευπάθεια προέρχεται από το πρωτόκολλο χαμηλής ισχύος Zigbee που χρησιμοποιούν η Philips και πολλοί άλλοι κατασκευαστές προϊόντων ΔτΠ για επικοινωνία συσκευών. Η συγκεκριμένη ευπάθεια ανακαλύφθηκε για πρώτη φορά το 2017, σε μελέτη των Ronen και συν. Η εταιρεία χρησιμοποίησε στα τέλη του 2019 τις ίδιες ακριβώς μεθόδους για να δοκιμάσει την ασφάλεια των έξυπνων λαμπτήρων με αυτές που είχαν χρησιμοποιήσει οι Ronen και συν. διαπιστώνοντας ότι δύο χρόνια μετά, η ευπάθεια εξακολουθεί να υφίσταται [108].

Πίνακας 2: Ταξινόμηση κυβερνοεπιθέσεων που έχουν ως στόχο έξυπνες οικιακές συσκευές ΔτΠ που είναι εγκατεστημένες σε κρίσιμα συστήματα

Κατηγορία κυβερνοεπίθεσης	Περιγραφή	Βαθμός επικινδυνότητας
Απόκτησης πρόσβασης	Επίθεση σε έξυπνους ηλεκτρικούς λαμπτήρες για την απόκτηση μη εξουσιοδοτημένης πρόσβασης Wi-Fi	Υψηλός
	Επίθεση στην οικιακή πύλη HG για την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο εσωτερικό οικιακό δίκτυο	Υψηλός
Έμμεσης διακοπής / άρνησης κρίσιμων υπηρεσιών	Επίθεση σε έξυπνους θερμοστάτες για την έμμεσο έλεγχο της λειτουργίας συστημάτων IT	Μέτριος
Διαρροής δεδομένων	Χρήση έξυπνων τηλεοράσεων για τη δημιουργία κρυφών καναλιών audio	Υψηλός
	Τροποποίηση της λειτουργικότητας έξυπνων λαμπτήρων για τη δημιουργία flickering και τη δημιουργία κρυφών καναλιών	Υψηλός
	Ανάλυση της κυκλοφορίας δικτύου έξυπνων μετρητών για την παρακολούθηση της παρουσίας ή απουσίας των ενοίκων στο σπίτι	Υψηλός
	Ανάλυση της κυκλοφορίας δικτύου έξυπνων οικιακών συσκευών για την παρακολούθηση των δραστηριοτήτων των ενοίκων στο σπίτι	Υψηλός
Κακόβουλης χρήσης συστήματος	Τροποποίηση της λειτουργικότητας έξυπνων λαμπτήρων για τη δημιουργία flickering και την πρόκληση φωτοεπιληψίας	Υψηλός

Οι Ronen και συν. ήθελαν να μελετήσουν τη δυνατότητα μόλυνσης με worms γειτονικών συσκευών ΔτΠ και την πιθανότητα εξάπλωσης της μόλυνσης σε μεγάλες περιοχές, υπό την προϋπόθεση ότι η πυκνότητα των συσκευών ΔτΠ υπερβαίνει μια συγκεκριμένη κρίσιμη τιμή. Συγκεκριμένα, ανέπτυξαν και επαλήθευσαν μια τέτοια μόλυνση χρησιμοποιώντας τους έξυπνους λαμπτήρες Philips Hue ως πλατφόρμα. Η εξάπλωση του ιού επιτεύχθηκε με μόνη χρήση της ενσωματωμένης ZigBee ασύρματης συνδεσιμότητας και φυσική εγγύτητα των λαμπτήρων. Η επιτυχημένη επίθεση επιτρέπει στον εισβολέα να ενεργοποιήσει ή να απενεργοποιήσει όλα τα φώτα, να τους δημιουργήσει μόνιμη δυσλειτουργία ή να τα εκμεταλλευτεί για την πραγματοποίηση μαζικών επιθέσεων DDOS. Για να καταστεί δυνατή μια τέτοια επίθεση, οι μελετητές έπρεπε να βρουν έναν τρόπο απομακρυσμένης πρόσβασης στους ήδη εγκατεστημένους λαμπτήρες και την πραγματοποίηση ενημερώσεων του υλικολογισμικού τους Over-The-Air (OTA). Η απομακρυσμένη πρόσβαση επετεύχθη ανακαλύπτοντας και αξιοποιώντας ένα σημαντικό σφάλμα στην εφαρμογή του Touchlink που αποτελεί τμήμα του πρωτοκόλλου ZigBee Light Link (ZLL), το οποίο υποτίθεται ότι μπορεί να σταματήσει τέτοιες προσπάθειες με ένα τεστ εγγύτητας. Για να καταφέρουν την πραγματοποίηση ενημερώσεων OTA του υλικολογισμικού τους, οι μελετητές ανέπτυξαν μια νέα έκδοση της επίθεσης πλευρικού καναλιού με σκοπό την εξαγωγή του καθολικού κλειδιού AES-CCM, το οποίο χρησιμοποιεί η Philips για κρυπτογράφηση και έλεγχο ταυτότητας νέου υλικολογισμικού [109].

Όπως φαίνεται στην εικόνα 9, ένα έξυπνο σύστημα εσωτερικού φωτισμού, δίνει στους χρήστες του τη δυνατότητα ασύρματου ελέγχου των λαμπτήρων είτε μέσω τηλεχειρισμού είτε μέσω μιας εφαρμογής smartphone χρησιμοποιώντας την πύλη HG. Στο συγκεκριμένο σύστημα χρησιμοποιείται το βιομηχανικό πρότυπο ZLL, το οποίο προορίζεται για διαλειτουργικά και πολύ εύχρηστα προϊόντα φωτισμού και ελέγχου. Το πρότυπο υποστηρίζεται από τους περισσότερους από τους σημαντικότερους κατασκευαστές οικιακού φωτισμού, όπως η Philips, η GE και η OSRAM [109].

Εικόνα 9: Παράδειγμα έξυπνου συστήματος εσωτερικού φωτισμού [109]

Κατά την επίθεση εναντίων των έξυπνων ηλεκτρικών λαμπτήρων, ο εισβολέας αποκτά τον έλεγχο ενός μεμονωμένου λαμπτήρα χρησιμοποιώντας την ευπάθεια του πρωτοκόλλου Zigbee και εγχέει κακόβουλο λογισμικό σε αυτόν. Έτσι, μπορεί πλέον να αλλάζει το χρώμα ή τη φωτεινότητα των λαμπτήρων για να εξαπατήσει τον ιδιοκτήτη του δικτύου όσον αφορά την ορθή λειτουργία τους. Ο μόνος τρόπος επιδιόρθωσης ενός έξυπνου λαμπτήρα είναι η αφαίρεση του από το έξυπνο σύστημα φωτισμού και, στη συνέχεια, η επαναπροσθήκη του σε αυτό. Η επαναπροσθήκη όμως του λαμπτήρα στο σύστημα, ενεργοποιεί το κακόβουλο υλικολογισμικό του, το οποίο εκκινεί μια διαδικασία πλημμύρας του ΔτΠ hub ελέγχου του οικιακού δικτύου με δεδομένα, στα οποία μπορεί να περιλαμβάνονται άλλο κακόβουλο λογισμικό, λογισμικό εντολών και ελέγχου για μελλοντικές επιθέσεις εναντίον του δικτύου, κ.α. Με τον τρόπο αυτό, ο επιτιθέμενος έχει εξασφαλίσει την μόλυνση του ΔτΠ hub ελέγχου του οικιακού δικτύου και μπορεί πλέον να ελέγχει ολόκληρο το δίκτυο [108].

Πολλές από τις έξυπνες οικιακές πλατφόρμες συνδέονται στο νέφος μέσω της οικιακής διαδικτυακής πύλης HG. Στην περίπτωση που οι επιτιθέμενοι καταφέρουν να προσβάλλουν με επιτυχία την συγκεκριμένη πύλη, μπορεί να αποκτήσουν τον πλήρη έλεγχο όλων των οικιακών συσκευών που συνδέονται στην εκάστοτε πλατφόρμα. Οι Stamm και συν. παρουσίασαν μια επίθεση που μπορεί να ξεκινήσει όταν ο πελάτης (client) επισκεφτεί έναν μολυσμένο ιστότοπο, ο οποίος εκτελεί αυτόματα μια Java applet με σκοπό την ανίχνευση των εσωτερικών IP του οικιακού διαδικτυακού δρομολογητή. Κάτι τέτοιο επιτυγχάνεται από τη στιγμή που το script δημιουργεί μια σύνδεση αντίστροφης υποδοχής (socket) μεταξύ του πελάτη και του εισβολέα στην οποία η IP διεύθυνση του πελάτη παρέχει μια προβολή ολόκληρου του σχήματος διευθυνσιοδότησης του εσωτερικού δικτύου. Έχοντας ολοκληρωμένες τις πληροφορίες που αφορούν το δρομολογητή, ο εισβολέας μπορεί να εκμεταλλευτεί την κατάσταση όπου οι περισσότεροι ιδιοκτήτες σπιτιού δεν αλλάζουν τον προεπιλεγμένο κωδικό πρόσβασης από τον κατασκευαστή και επιχειρούν να συνδεθούν χρησιμοποιώντας τα προεπιλεγμένα διαπιστευτήρια. Μετά την επιτυχή είσοδο, ο εισβολέας θα τροποποιήσει τις απαραίτητες ρυθμίσεις διαμόρφωσης και θα αποκτήσει πλήρη πρόσβαση στην πύλη HG, ελέγχοντας όλες τις εξερχόμενες συνδέσεις και τη διαχείριση του οικιακού δρομολογητή [110].

4.2.2 Κυβερνοεπιθέσεις έμμεσης διακοπής/άρνησης κρίσιμων υπηρεσιών

Οι Fernades και συν. παρουσίασαν ένα σενάριο επίθεσης κατά των θερμοστατών Nest που μπορούν να λειτουργήσουν σε περιβάλλον ΔτΠ και είναι σχεδιασμένοι για τον εξ αποστάσεως έλεγχο κεντρικών μονάδων κλιματισμού μέσω δικτύου Wi-Fi. Ο εν λόγω θερμοστάτης μπορεί επίσης να επικοινωνεί με άλλες συσκευές Nest μέσω του πρωτοκόλλου Zigbee και να συνδεθεί στις υπηρεσίες νέφους της ίδιας εταιρείας για τη μεταφόρτωση στατιστικών στοιχείων χρήσης που μπορεί να χρησιμοποιηθούν από παρόχους ενέργειας για τη βελτίωση της ενεργειακής απόδοσης. Εκμεταλλευόμενοι τις ενσωματωμένες διεπαφές επικοινωνίας και τις ευπάθειες της διαδικασίας εκκίνησης της συσκευής, οι μελετητές κατάφεραν να εγκαταστήσουν το δικό τους προσαρμοσμένο rootkit και πυρήνα Linux, διασφαλίζοντας έτσι τον απομακρυσμένο έλεγχο της συσκευής ακόμα και μετά από ενημέρωση υλικολογισμικού. Με τον τρόπο αυτό απέδειξαν ότι στην περίπτωση που ένας παραβιασμένος έξυπνος θερμοστάτης εγκατασταθεί σε μια κρίσιμη υποδομή, όπως στο δωμάτιο ενός κέντρου δεδομένων, θα μπορούσε να πραγματοποιηθεί επίθεση DoS μόνο με την αλλαγή της θερμοκρασίας δωματίου, η οποία, με τη σειρά της, θα μπορούσε να οδηγήσει σε δυσλειτουργία ή ακόμα και σε τερματισμό λειτουργίας των διακομιστών του δικτύου [111].

4.2.3 Κυβερνοεπιθέσεις διαρροής δεδομένων

Τον Μάρτιο του 2017, ο διεθνής μη κερδοσκοπικός οργανισμός μέσων μαζικής ενημέρωσης WikiLeaks δημοσίευσε έγγραφα που αποκάλυψαν ένα project της CIA, με την κωδική ονομασία Weeping Angel. Η δημοσίευση περιλάμβανε και διάφορες δυνατότητες που επιτρέπουν την εισβολή σε συσκευές που μπορούν να συνδεθούν στο Διαδίκτυο, όπως έξυπνες τηλεοράσεις και smartphone. Ιδιαίτερο ενδιαφέρον παρουσιάζει η δυνατότητα χρήσης του μικροφώνου ορισμένων μοντέλων έξυπνης τηλεόρασης για τη δημιουργία κρυφών καναλιών (covert channel). Ένα κρυφό κανάλι αποτελεί τύπο επίθεσης που δημιουργεί τη δυνατότητα μεταφοράς αντικειμένων πληροφοριών μεταξύ διαδικασιών που υποτίθεται ότι δεν επιτρέπεται να επικοινωνούν σύμφωνα με την πολιτική ασφάλειας ενός υπολογιστή ή ενός δικτύου. Η δημοσίευση περιγράφει τον τρόπο με τον οποίο μια στοχευμένη τηλεόραση είναι δυνατόν να τεθεί σε κατάσταση ψευδούς απενεργοποίησης. Στη συνέχεια, με τον ιδιοκτήτη του σπιτιού να πιστεύει εσφαλμένα ότι η έξυπνη τηλεόραση είναι απενεργοποιημένη, το μικρόφωνό της μπορεί να χρησιμοποιηθεί για την καταγραφή συνομιλιών εντός του χώρου και την μετέπειτα διαδικτυακή αποστολή τους σε έναν κρυφό διακομιστή. Μια τέτοια επίθεση εκμεταλλεύεται πολλά από τα γνωστά και άγνωστα τρωτά σημεία του λογισμικού και του δικτύου. Προφανώς,

τέτοιες επιθέσεις θα μπορούσαν να χρησιμοποιηθούν από υπηρεσίες για διαρροή δεδομένων από πολύ ευαίσθητα περιβάλλοντα στα οποία βρίσκονται οι ευάλωτες έξυπνες τηλεοράσεις [112].

Οι Ronen και Shamir μελέτησαν τη δυνατότητα διάφορων επιθέσεων εναντίων έξυπνων λαμπτήρων LED. Μία από τις επιθέσεις εκμεταλλεύεται την έλλειψη κρυπτογράφησης και προστασίας της ακεραιότητας των δεδομένων στην επικοινωνία μεταξύ του ελεγκτή και των έξυπνων LED για τη δημιουργία ενός κρυφού καναλιού. Από τη στιγμή που η διεπαφή API του ελεγκτή δεν εφαρμόζει επικύρωση εισόδου των εντολών, οι μελετητές ήταν σε θέση να εγχύσουν δεδομένα με προσαρμοσμένο ωφέλιμο φορτίο για την τροποποίηση των σημάτων της διαμόρφωσης PWM (Pulse Width Modulation), μια λειτουργία που ρυθμίζει την μεταβολή της φωτεινότητας των LED. Με τον έλεγχο των σημάτων PWM, οι μελετητές μπορούσαν να δημιουργήσουν το φαινόμενο του flickering στους λαμπτήρες, με τέτοια συχνότητα που δεν ήταν ορατό στο ανθρώπινο μάτι. Στη συνέχεια, χρησιμοποιώντας ένα φορητό υπολογιστή, έναν αισθητήρα φωτός, ένα Arduino και ένα τηλεσκόπιο, κατάφεραν να μετατρέψουν το φαινόμενο αυτό σε χρησιμοποιήσιμα δεδομένα από απόσταση έως και 100 μέτρα. Μια τέτοια επίθεση θα μπορούσε να χρησιμοποιηθεί από έναν επιτιθέμενο, ο οποίος θα μπορεί να ελέγχει εξ αποστάσεως ένα παρόμοιο ευάλωτο σύστημα έξυπνου φωτισμού, έμμεσα συνδεδεμένο (π.χ. μέσω του ελεγκτή Wi-Fi) με ένα κρίσιμο σύστημα που έχει ήδη παραβιάσει. Μέσω του φαινομένου του flickering, ο επιτιθέμενος θα μπορούσε να δημιουργήσει ένα κρυφό κανάλι και να υποκλέψει ευαίσθητα δεδομένα, χωρίς να ανιχνεύεται από κανένα δικτυακό σύστημα ασφαλείας [113].

Εναλλακτικά, ευαίσθητα δεδομένα μπορούν επίσης να διαρρεύσουν μέσω επιθέσεων ανάλυσης κυκλοφορίας. Οι Copos και συν. παρουσίασαν μια επίθεση ανάλυσης κυκλοφορίας σε κρυπτογραφημένη κίνηση οικιακού δικτύου. Οι μελετητές ανέλυσαν την κυκλοφορία δικτύου ενός θερμοστάτη και ενός ανιχνευτή καπνού και διοξειδίου του άνθρακα της εταιρείας Nest και έδειξαν ότι ευαίσθητες πληροφορίες σχετικά με την κατάσταση του έξυπνου σπιτιού θα μπορούσαν να αντληθούν από την κρυπτογραφημένη κίνηση του δικτύου. Οι ερευνητές αποκρυπτογράφησαν την κρυπτογραφημένη κίνηση WPA με σκοπό τον προσδιορισμό των host με τους οποίους επικοινωνούν συχνά οι συσκευές. Παρά το γεγονός ότι τα πακέτα δεδομένων είναι κρυπτογραφημένα με SSL/TLS, αναλύοντας τους τύπους αιτημάτων (π.χ. HTTPS, NTP, DNS κ.λπ.) και τη συχνότητα αποστολής τους, οι μελετητές μπόρεσαν να ανακαλύψουν πότε οι συσκευές άλλαζαν τη λειτουργία τους από "Home" (οι ένοικοι είναι σπίτι) σε "Away" (οι ένοικοι λείπουν). Με τον τρόπο αυτό ο εν δυνάμει επιτιθέμενος είναι σε θέση να γνωρίζει την παρουσία ή απουσία των ενοίκων του έξυπνου σπιτιού [114].

Οι Apthorpe και συν. επέκτειναν την προηγούμενη μελέτη, αποδεικνύοντας ότι οι πάροχοι ISP θα μπορούσαν να συμπεράνουν ευαίσθητες δραστηριότητες ενός ενοίκου του σπιτιού, αναλύοντας απλώς τους ρυθμούς μεταβολής της κυκλοφοριακής ροής που δημιουργείται από έξυπνα σπίτια που περιέχουν εμπορικές συσκευές ΔτΠ, ακόμα και όταν αυτές χρησιμοποιούν κρυπτογράφηση. Όπως απέδειξαν οι μελετητές, η μεταβολή της κυκλοφοριακής ροής του δικτύου (αποστολή/λήψη δεδομένων) αντιστοιχεί στις καταστάσεις των συσκευών. Είναι σαφές ότι αν ένας εισβολέας γνωρίζει αυτή την συσχέτιση θα μπορούσε εύκολα να διακρίνει τις δραστηριότητες των ενοίκων εντός του έξυπνου σπιτιού [115].

4.2.4 Κυβερνοεπιθέσεις κακόβουλης χρήσης συστήματος

Οι Ronen και Shamir περιέγραψαν ότι η επίθεση που αναφέρθηκε στην προηγούμενη υποενότητα θα μπορούσε να χρησιμοποιηθεί από έναν επιτιθέμενο για να προκαλέσει επιληπτικές κρίσεις. Είναι γνωστό ότι τα στροβοσκόπια σε συγκεκριμένες περιοχές συχνοτήτων επηρεάζουν άτομα που πάσχουν από φωτοεπιληψία. Μια παρόμοια επίθεση εναντίον πολυάριθμων έξυπνων συστημάτων φωτισμού, εγκατεστημένα σε νοσοκομεία ή

δημόσιους χώρους, θα μπορούσαν να προξενήσουν σοβαρές επιπτώσεις στην ασφάλεια και την υγεία του κοινού [113].

4.3 Κυβερνοεπιθέσεις σε συσκευές εγκατεστημένες σε μη κρίσιμα συστήματα

Ακόμα και στην περίπτωση που οι έξυπνες οικιακές συσκευές είναι εγκατεστημένες σε μη κρίσιμα συστήματα, ενδέχεται να εξακολουθούν να χρησιμοποιούνται ως ενεργοποιητές επιθέσεων. Όπως φαίνεται στην εικόνα 8, οι κυβερνοεπιθέσεις στην περίπτωση αυτή μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες [57]: (α) κυβερνοεπιθέσεις με χρήση των συσκευών ως ενισχυτή επιθέσεων και (β) κυβερνοεπιθέσεις με στόχο τις ίδιες τις συσκευές. Η πρώτη κατηγορία περιλαμβάνει επιθέσεις DDoS που εκμεταλλεύονται ευπάθειες στην ασφάλεια των έξυπνων οικιακών συσκευών ΔτΠ για τη δημιουργία botnet και την ενίσχυση της επίθεσης εναντίον του πραγματικού στόχου. Πραγματικό στόχο της δεύτερης κατηγορίας επιθέσεων είναι οι ίδιες οι έξυπνες οικιακές συσκευές ΔτΠ. Η σημασία των επιθέσεων της δεύτερης κατηγορίας προέρχεται από τη μαζικότητα που τους χαρακτηρίζει, δηλαδή την ταυτόχρονη απειλή εναντίον ενός τεράστιου αριθμού έξυπνων οικιακών συσκευών με μόνιμο DoS (PDoS) ή ransomware. Στον Πίνακα 3 παρουσιάζεται η προτεινόμενη ταξινόμηση των κυβερνοεπιθέσεων που έχουν ως στόχο έξυπνες οικιακές συσκευές ΔτΠ που είναι εγκατεστημένες σε μη κρίσιμα συστήματα, μαζί με την περιγραφή και τον βαθμό επικινδυνότητάς τους.

Πίνακας 3: Ταξινόμηση κυβερνοεπιθέσεων που έχουν ως στόχο έξυπνες οικιακές συσκευές ΔτΠ που είναι εγκατεστημένες σε μη κρίσιμα συστήματα

Κατηγορία κυβερνοεπίθεσης	Περιγραφή	Βαθμός επικινδυνότητας
Χρήση των συσκευών ως ενισχυτή επιθέσεων	Μαζική αποστολή κακόβουλων email σε έξυπνες οικιακές συσκευές	Μέτριος
	Επιθέσεις σε έξυπνες οικιακές συσκευές, εφαρμογές και πλατφόρμες WeMo	Μέτριος
	Επίθεση DDoS σε έξυπνες οικιακές συσκευές για την προσβολή διακομιστών DNS	Μέτριος
	Επίθεση PRNFilter σε διαδικτυακές πύλες SOHO	Υψηλός
Με στόχο τις ίδιες τις συσκευές	Εξ αποστάσεως έλεγχος έξυπνων λαμπτήρων μέσω τροποποιημένου αυτό-διαδιδόμενου firmware	Μέτριος
	Επιθέσεις σε έξυπνες οικιακές συσκευές ΔτΠ μέσω ελέγχου των ευπαθειών εφαρμογών app	Μέτριος
	Επιθέσεις σε έξυπνες τηλεοράσεις μέσω Man-In-The-Middle και ransomeware	Μέτριος
	Εκμετάλλευση του πρωτοκόλλου Zig-Bee για την ενεργοποίηση επιθέσεων DoS, υποκλοπών και έγχυσης εντολών	Χαμηλός
	Επιθέσεις εξάντλησης μπαταριών κινητών συσκευών	Υψηλός

4.3.1 Κυβερνοεπιθέσεις με χρήση των συσκευών ως ενισχυτή επιθέσεων

Το 2014, η εταιρεία παροχής υπηρεσιών ασφαλείας Proofpoint, ανέφερε ένα περιστατικό κυβερνοεπίθεσης που περιλάμβανε χιλιάδες έξυπνες οικιακές συσκευές. Η επίθεση παγκόσμιας εμβέλειας περιλάμβανε την αποστολή περισσότερων από 750.000 κακόβουλων email, που αποστέλλονταν σε burst των 100.000 email τρεις φορές την ημέρα, στοχεύοντας έξυπνες συσκευές επιχειρήσεων και οικιών. Ανάμεσα στις συσκευές που δέχθηκαν επίθεση περιλαμβάνονται είδη όπως δρομολογητές οικιακής δικτύωσης, συνδεδεμένα κέντρα πολυμέσων, τηλεοράσεις και ψυγεία [116].

Το 2015, πραγματοποιήθηκε μελέτη όσον αφορά την ασφάλεια της πλατφόρμας νέφους των έξυπνων σπιτιών WeMo, τα δίκτυα των οποίων αποτελούνται από Wi-Fi συσκευές της εταιρείας Belkin. Σε αυτές τις επιθέσεις, οι ερευνητές κατάφεραν να πραγματοποιήσουν αυθαίρετη εκτέλεση κώδικα (arbitrary code execution) μέσω επιθέσεων SQL injection και να πάρουν τον απομακρυσμένο έλεγχο των συσκευών, παρακάμπτοντας τοπικούς μηχανισμούς

ελέγχου ταυτότητας μέσω σύνδεσης της διεπαφής UART των συσκευών και εκμετάλλευσης των ευπαθειών που βρέθηκαν στην εφαρμογή WeMo [117].

Τον Οκτώβριο του 2016 πραγματοποιήθηκε ένα ακόμα περιστατικό κυβερνοεπίθεσης. Μια συντονισμένη επίθεση DDoS εναντίον της υπηρεσίας DYN DNS, με ρυθμό που ξεπέρασε τα 600Gbps, παράλυσε το Διαδίκτυο. Η επίθεση εμπόδισε τους πελάτες να προσπελάσουν περισσότερα από 1.200 domain, κάποια από τα οποία αφορούσαν γνωστές επιχειρήσεις όπως οι Amazon, Twitter, Spotify, PayPal και Comcast. Η επίθεση προήλθε από το botnet Mirai που περιλάμβανε περίπου 100.000 μολυσμένες έξυπνες οικιακές συσκευές ΔτΠ, όπως οικιακούς δρομολογητές, κάμερες παρακολούθησης και DVR. Η επίθεση πραγματοποιήθηκε κυρίως μέσω αιτημάτων πλημμύρας TCP SYN και επιθέσεων subdomain με άμεσο στόχο το port 53 των διακομιστών DYN DNS. Οι περισσότερες από τις παραβιασμένες έξυπνες οικιακές συσκευές ΔτΠ παρουσίαζαν ευπάθειες κωδικού πρόσβασης (χρήση του προεπιλεγμένου ή αδύναμου κωδικού πρόσβασης) ή/και τρωτά σημεία του λειτουργικού συστήματος [118].

Το 2018, ερευνητές της Cisco Talos ανακοίνωσαν την ανακάλυψη ενός εξελιγμένου κακόβουλου λογισμικού με την ονομασία VPNFilter, ο οποίος αποτελεί σοβαρή απειλή για την ασφάλεια των οικιακών διαδικτυακών πυλών HG. Το ίδιο το κακόβουλο λογισμικό είχε ήδη μολύνει τουλάχιστον 500.000 δρομολογητές SOHO (Small Office Home Office) εταιρειών, όπως οι Linksys, MikroTik, NETGEAR και TP-Link, σε 54 χώρες, καθώς και ορισμένες συσκευές αποθήκευσης QNAP NAS. Ειδικά σχεδιασμένο για να επιτίθεται σε δρομολογητές, το VPNFilter μπορεί να παρεμβληθεί στην διαδικτυακή κίνηση του χρήστη και να χειριστεί τις ιστοσελίδες που επισκέπτεται. Μπορεί να υποκλέψει κωδικοποιημένους κωδικούς πρόσβασης ή να δημιουργήσει ψεύτικα αντίγραφα της ιστοσελίδας, έτσι ώστε ο χρήστης να μην γνωρίζει ότι έχει πέσει θύμα επίθεσης. Το συγκεκριμένο κακόβουλο λογισμικό έχει ισχυρή καταστροφική ικανότητα που μπορεί να καταστήσει τη μολυσμένη συσκευή μη λειτουργική και μπορεί να ενεργοποιηθεί σε μεμονωμένες έξυπνες συσκευές. Μόλις εγκατασταθεί στο δρομολογητή, μπορεί να εμποδίσει τη λειτουργία του, να συλλέξει πληροφορίες από το σύστημα που τρέχει μέσω του δικτύου και να αποκλείσει το δίκτυο [119].

4.3.2 Κυβερνοεπιθέσεις με στόχο τις ίδιες τις συσκευές

Οι Ronen και συν. απέδειξαν τον τρόπο με τον οποίο ένας εισβολέας μπορεί να πάρει τον έλεγχο ενός έξυπνου λαμπτήρα και να εξαπολύσει επιθέσεις με χρήση warms. Βασική ιδέα αποτελεί η παράκαμψη του μηχανισμού ελέγχου εγγύτητας που χρησιμοποιούν τα έξυπνα φώτα κατά τη σύνδεση σε ένα δίκτυο, ώστε να ξεγελαστούν και να συνδεθούν σε κακόβουλο δίκτυο. Στη συνέχεια μέσω της διαδικασίας ενημέρωσης OTA, στα φώτα γίνεται εγκατάσταση ενός τροποποιημένου υλικολογισμικού που επιτρέπει τον έλεγχο της συσκευής από τον εν δυνάμει επιτιθέμενο. Η παράκαμψη του μηχανισμού ελέγχου εγγύτητας πραγματοποιήθηκε μέσω εκμετάλλευσης ενός ελαττώματος της εφαρμογής BitCloud Touchlink της Atmel. Για την ανάκτηση του ενσωματωμένου κλειδιού του hardware υλικού, χρησιμοποιήθηκαν οι τεχνικές DPA (Differential Power Analysis) και CPA (Correlation Power Analysis). Στη συνέχεια, οι μελετητές χρησιμοποίησαν το ανακτημένο κλειδί για να "μονιμοποιήσουν" ένα αρχείο υλικολογισμικού που είχαν προηγουμένως μολύνει με κακόβουλο κώδικα. Αυτό τους επέτρεψε να εκτελέσουν διάφορες επιθέσεις, όπως μόνιμη δυσλειτουργία των συσκευών με επιθέσεις μόνιμης άρνησης υπηρεσιών (Permanent Denial of Service – PDoS) ή χρήση των παραβιασμένων συσκευών για το jamming γειτονικών ασύρματων δικτύων που λειτουργούν στην ίδια μπάντα συχνοτήτων [120].

Οι Fernades και συν. παρουσίασαν μια διεξοδική ανάλυση των ευπαθειών αλλά και των επιθέσεων εναντίον 499 εφαρμογών ελέγχου έξυπνου σπιτιού και 132 device handler. Χρησιμοποιώντας τεχνικές ανάλυσης στατικού κώδικα, οι ερευνητές ανακάλυψαν ότι περισσότερο από το 55% των εφαρμογών που εξέτασαν στερούνταν βασικών μηχανισμών

προστασίας για ευαίσθητα δεδομένα, όπως για παράδειγμα κωδικούς κλειδώματος πόρτας. Στη συνέχεια, έδειξαν πιθανά σενάρια επίθεσης σε ένα σύστημα παρακολούθησης σπιτιού που λειτουργεί σε περιβάλλον ΔτΠ, όπως υποκλοπή ή παραποίηση των κωδικών κλειδώματος πόρτας, απενεργοποίηση των λειτουργιών "Vacation mode" καθώς και ενεργοποίηση ψευδών συναγερμών πυρκαγιάς [121].

Αρκετοί ερευνητές έχουν πραγματοποιήσει δοκιμές ασφαλείας σε έξυπνες τηλεοράσεις. Ανακάλυψαν ότι μέσω επιθέσεων Man-In-The-Middle, ένας εισβολέας θα μπορούσε να ανακατευθύνει μη εξουσιοδοτημένα και μη κρυπτογραφημένα αιτήματα HTTP, σε περιπτώσεις λήψης υλικολογισμικού ή εφαρμογών, σε κακόβουλους ιστότοπους και να αποκτήσει έλεγχο των συσκευών [122]. Παράδειγμα τέτοιων επιθέσεων αποτελεί το FLocker (Frantic Locker), ένα ransomware για Android, που όμως είναι σε θέση να μολύνει και να κλειδώσει έξυπνες τηλεοράσεις που λειτουργούν με το λειτουργικό σύστημα Android. Το συγκεκριμένο ransomware εμφανίστηκε το Μάιο του 2015, και η Trend Micro αναφέρει ότι εντοπίστηκαν πάνω από 7.000 διαφορετικές εκδόσεις του, καθώς ο κώδικας του συνεχίζει να εξελίσσεται. Μόνο τον Απρίλιο του 2016 η Trend Micro αναφέρει ότι εντόπισε πάνω από 1.200 παραλλαγές του FLocker και γενικότερα παρατήρησε μια ανάπτυξη στην ώθηση του κακόβουλου λογισμικού. Η οθόνη που ζητάει τα λύτρα φαίνεται να είναι παρόμοια με αυτή που χρησιμοποιείται από το Cyber.Police (Dogspectus) ransomware, το οποίο έχει αποκτήσει την ικανότητα να μολύνει συσκευές Android χωρίς να χρειάζεται κάποια αλληλεπίδραση από τον χρήστη. Η πιο πρόσφατη εξέλιξη στις δυνατότητες του FLocker είναι ότι μπορεί να εξαπλωθεί μέσω ανεπιθύμητων μηνυμάτων SMS που περιέχουν κακόβουλους συνδέσμους. Μόλις λοιπόν ο χρήστης κατεβάσει το ransomware μέσω αυτών των συνδέσμων, το κακόβουλο λογισμικό κρύβεται για 30 λεπτά, για την αποφυγή των εργαλείων ανάλυσης ιών. Ο κακόβουλος κώδικας είναι κρυμμένος σε ένα αρχείο HTML στο εσωτερικό του φακέλου "Assets." Αυτό το αρχείο κρύβει ένα αρχείο DEX με τις κακόβουλες ρουτίνες. Μετά τα 30 λεπτά, το Flocker ξεκινά την εχθρική του συμπεριφορά απέναντι στον χρήστη ζητώντας να του δώσει δικαιώματα διαχειριστή. Εάν ο χρήστης αρνηθεί, το FLocker παγώνει την οθόνη με ένα ψεύτικο μήνυμα για ενημέρωση του συστήματος για να τρομάξει τον χρήστη και να του δώσει την απαιτούμενη πρόσβαση. Όταν αποκτήσει το FLocker προνόμια διαχειριστή, θα αρχίσει να επικοινωνεί με τον διακομιστή C&C (διοίκησης και ελέγχου), από όπου κατεβάζει και άλλο APK μαζί με το σημείωμα για τα λύτρα, σε μορφή HTML & JS. Το FLocker εμφανίζει το σημείωμα για τα λύτρα σε ολόκληρη την οθόνη και ξεκινά την λειτουργία του δεύτερου APK, το οποίο κρυπτογραφεί τα αρχεία της συσκευής με ένα κλειδί κρυπτογράφησης AES. Το FLocker ζητά από τους χρήστες 200 δολάρια σε κάρτες δώρων μέσω του iTunes [123].

Ο Scheel παρουσίασε μια επίθεση στην οποία, ένας επιτιθέμενος είναι σε θέση να αποκτήσει απομακρυσμένο έλεγχο ενός μεγάλου αριθμού έξυπνων τηλεοράσεων, μέσω αποστολής ειδικά κατασκευασμένων τηλεοπτικών σημάτων DVB-T (εντολές HbbTV) για να αποκτήσει πρόσβαση root. Η συγκεκριμένη επίθεση χρησιμοποιεί δύο γνωστά ελαττώματα ασφαλείας των ενσωματωμένων προγραμμάτων περιήγησης ιστού και ισχύει για το 90% των έξυπνων τηλεοράσεων, που πουλήθηκαν τα τελευταία χρόνια [124].

Οι Morgner και συν. παρουσίασαν μια σειρά επιθέσεων που βασίζονται σε γνωστές ευπάθειες του πρωτοκόλλου ZLL. Οι επιθέσεις χωρίστηκαν σε δύο κύριες κατηγορίες: αυτές που δεν απαιτούν οποιαδήποτε χρήση κρυπτογραφικών πρωτοκόλλων (blink, reset, DoS) και αυτές που απαιτούν πρόσβαση στο κύριο κλειδί ZLL (πειρατεία, εξαγωγή κλειδιού δικτύου και έγχυση εντολών). Τα στοχευμένα συστήματα περιλάμβαναν δημοφιλή μοντέλα φωτισμού, όπως τα Philips Hue, Osram Lightify και GE Link. Στόχος των μελετητών ήταν να δείξουν μια σειρά επιθέσεων κατά του πρωτοκόλλου ZLL, χρησιμοποιώντας την ευπάθεια κύριου κλειδιού και τα μη ασφαλή πλαίσια Inter-PAN, που χρησιμοποιούνται για την επικοινωνία μεταξύ των δικτύων PAN ενός έξυπνου σπιτιού [125].

Οι επιθέσεις εξάντλησης μπαταρίας ή εξάντλησης ενέργειας είναι ένας ακόμη τρόπος με τον οποίο οι εισβολείς μπορούν να στοχεύσουν τις έξυπνες οικιακές συσκευές ΔτΠ όσον αφορά τη διαθεσιμότητα τους. Οι Vasserman και συν. παρουσίασαν διάφορες επιθέσεις εξάντλησης μπαταριών, τις γνωστές επιθέσεις βαμπίρ, που στοχεύουν ad hoc ασύρματα δίκτυα αισθητήρων. Οι επιθέσεις βαμπίρ χρησιμοποιούν πρωτόκολλα δρομολόγησης με στόχο την μόνιμη απενεργοποίηση των δικτύων μειώνοντας την ισχύ της μπαταρίας των συσκευών. Αυτές οι επιθέσεις δεν εξαρτώνται από συγκεκριμένα πρωτόκολλα ή υλοποιήσεις, αλλά βασίζονται στις ιδιότητες πολλών δημοφιλών χαρακτηριστικών πρωτοκόλλων δρομολόγησης, όπως κατάσταση σύνδεσης, διανύσματος απόστασης, δρομολόγηση πηγής, κ.α. Οι μελετητές απέδειξαν μέσω προσομοίωσης ότι ανάλογα με τη θέση του επιτιθέμενου στο δίκτυο, η ενεργειακή κατανάλωση του δικτύου αυξάνεται από το 50 στο 100%. Παρόλο που η μελέτη αφορά επιθέσεις βαμπίρ σε ad hoc δίκτυα αισθητήρων, τα έξυπνα οικιακά δίκτυα θα μπορούσαν εξίσου εύκολα να πέσουν θύματα τέτοιων επιθέσεων, καθώς πολλές έξυπνες οικιακές συσκευές είναι κινητές, λειτουργούν με μπαταρία και χρησιμοποιούν πρωτόκολλα δρομολόγησης παρόμοια με αυτά που χρησιμοποιούνται στα ad hoc δίκτυα αισθητήρων, όπως το AODV που χρησιμοποιείται από συσκευές ZigBee [126].

ΚΕΦΑΛΑΙΟ 5

ΛΥΣΕΙΣ & ΑΝΤΙΜΕΤΩΠΙΣΗ

Τα τελευταία χρόνια, παρατηρείται μια συνεχόμενη αύξηση των μελετών που εμφανίζονται στη βιβλιογραφία όσον αφορά την αντιμετώπιση των θεμάτων ασφάλειας και ιδιωτικότητας σε όλα τα επίπεδα της αρχιτεκτονικής του ΔτΠ., αλλά και σε όλους τους τομείς εφαρμογής του, ανάμεσα στον οποίους συγκαταλέγεται και το έξυπνο σπίτι. Ιδιαίτερα στο πλαίσιο του έξυπνου σπιτιού, έχουν προταθεί πολλές διαφορετικές τεχνικές και λύσεις, με μεγαλύτερη έμφαση την ασφάλεια και την προστασία της ιδιωτικότητας των έξυπνων οικιακών συσκευών με περιορισμένους πόρους. Όπως έχει αναφερθεί σε προηγούμενα κεφάλαια, ένα από τα ζητήματα που κάνουν το ΔτΠ περίπλοκο είναι το γεγονός ότι πολλές συσκευές που λειτουργούν στο περιβάλλον του χρησιμοποιούν πολύ απλά λειτουργικά συστήματα σε επεξεργαστές που έχουν ελάχιστη υπολογιστική χωρητικότητα και μικρή μνήμη, καθιστώντας πιο δύσκολη την εκπλήρωση βασικών απαιτήσεων ασφάλειας και προστασίας της ιδιωτικότητας. Στο παρόν κεφάλαιο, εξετάζονται διάφορες προτάσεις και λύσεις για την αντιμετώπιση αυτών των θεμάτων. Η ανάλυση των προτεινόμενων λύσεων εστιάζεται σε τέσσερεις διαφορετικές πτυχές, όπως είναι τα κρυπτογραφικά πρωτόγονα, τα πρωτόκολλα ελέγχου ταυτότητας, το hardware υλικό και οι σύγχρονοι μηχανισμοί ασφαλείας. Στην συγκεκριμένη ανάλυση θα παρουσιαστούν σχετικές εργασίες που παρουσιάστηκαν στην βιβλιογραφία την τελευταία πενταετία με θέμα την ασφάλεια και την προστασία της ιδιωτικότητας στα έξυπνα σπίτια που λειτουργούν σε περιβάλλον ΔτΠ.

5.1 Λύσεις κρυπτογραφικών πρωτογόνων

Βασικός σκοπός αυτών των λύσεων είναι η αντιμετώπιση των ζητημάτων ασφαλείας και προστασίας της ιδιωτικότητας των ΔτΠ έξυπνων οικιακών δικτύων μέσω κρυπτογραφικών πρωτογόνων (cryptographic primitives) χωρίς να διαταράσσεται η χρηστικότητα των εφαρμογών του έξυπνου οικοσυστήματος. Τα κρυπτογραφικά πρωτόγονα είναι καλά εδραιωμένοι, κρυπτογραφικοί αλγόριθμοι χαμηλού επιπέδου που χρησιμοποιούνται συχνά για τη δημιουργία κρυπτογραφικών πρωτοκόλλων [127].

Για την αντιμετώπιση των ζητημάτων της ασφάλειας και της προστασίας της ιδιωτικότητας στα έξυπνα σπίτια που λειτουργούν σε περιβάλλον ΔτΠ, απαιτείται η χρήση κατάλληλων κρυπτογραφικών λύσεων στις ενσωματωμένες εφαρμογές. Ωστόσο, λόγω των περιορισμών στους πόρους που παρουσιάζουν οι περισσότερες από τις έξυπνες οικιακές συσκευές, τα συμβατικά κρυπτογραφικά πρωτόγονα μπορεί να αποδειχθούν ακατάλληλα. Για το λόγο αυτό, η ακαδημαϊκή κοινότητα έχει στραφεί τα τελευταία χρόνια προς την μελέτη ενός καινούργιου τομέα που αναφέρεται ως ελαφριά κρυπτογραφία (lightweight cryptography), ο οποίος ασχολείται με την ανάπτυξη νέων κρυπτογραφικών αλγορίθμων που να παρέχουν ισχυρούς μηχανισμούς ασφαλείας και κρυπτογράφηση / αποκρυπτογράφηση σε εφαρμογές χαμηλής ισχύος και άλλες λειτουργίες της πανταχού παρούσας υπολογιστικής (ubiquitous computing). Οι Singh και συν. παρουσίασαν μια σύνοψη των ελαφρών κρυπτογραφικών πρωτογόνων που έχουν προταθεί στη βιβλιογραφία [128].

Τα πρωτόκολλα διαχείρισης κλειδιών κρυπτογράφησης αποτελούν τη βάση της ασφαλούς επικοινωνίας μεταξύ των έξυπνων συσκευών και οι μελετητές ασχολούνται εντατικά σε αυτόν τον τομέα. Οι Komninos και συν. μελέτησαν τα ζητήματα ασφάλειας και προστασίας της

ιδιωτικότητας του έξυπνου οικιακού περιβάλλοντος, εστιάζοντας περισσότερο στην σύνδεσή του με το έξυπνο δίκτυο παροχής ηλεκτρικής ενέργειας. Ωστόσο, ορισμένα από τα ζητήματα ασφαλείας και τους τρόπους αντιμετώπισής τους που παρουσιάστηκαν μπορούν να εφαρμοστούν σε ένα γενικότερο πλαίσιο του έξυπνου οικιακού περιβάλλοντος. Οι μελετητές κατηγοριοποίησαν τα θέματα ασφάλειας με βάση την εμπιστευτικότητα, την αυθεντικότητα, τη διαθεσιμότητα και τη μη απόρριψη και παρουσίασαν ως πιθανούς τρόπους αντιμετώπισής τους τη χρήση τεχνικών κρυπτογράφησης (όσον αφορά την εμπιστευτικότητα) τεχνικές ανωνυμοποίησης (όσον αφορά το απόρρητο των δεδομένων) [129].

Ένα σχήμα διαχείρισης κλειδιών κρυπτογράφησης που βασίζεται στον έλεγχο ταυτότητας (Identity-Based Encryption - IBE) και επιτρέπει στους κόμβους με μη περιορισμένους πόρους να μεταβιβάζουν ακριβείς υπολογισμούς σε κόμβους με περιορισμένους πόρους, προτάθηκε από τους Papanikolaou και συν. Σε αντίθεση με σχήματα κρυπτογράφησης δημόσιου κλειδιών που χρειάζονται υποδομή δημόσιου κλειδιού (Public Key Infrastructure - PKI) για την αντιστοίχιση κλειδιών σε ταυτότητες μέσω ψηφιακών υπογεγραμμένων πιστοποιητικών, κάτι που επιβαρύνει το συνολικό overhead κατά τη διαχείριση των πιστοποιητικών, στην κρυπτογράφηση IBE, το δημόσιο κλειδί είναι μια αυθαίρετη σειρά πληροφοριών που σχετίζονται αποκλειστικά με τον χρήστη, όπως διεύθυνση e-mail, ημερομηνία γέννησης κ.α. Παρόλα αυτά, το υψηλό υπολογιστικό κόστος της κρυπτογράφησης αυτής δεν μπορεί να υποστηριχθεί από τις περισσότερες έξυπνες οικιακές συσκευές. Για να ξεπεραστεί αυτό το πρόβλημα, οι μελετητές χρησιμοποίησαν τον έλεγχο IBE σε κρυπτογράφηση ελλειπτικής καμπύλης (Elliptic Curve Cryptography - ECC), που υποστηρίζεται από ενσωματωμένα συστήματα με περιορισμένους πόρους. Το προτεινόμενο σχήμα επιτρέπει σε έναν κόμβο με περιορισμό πόρων να μοιραστεί με ασφάλεια κρυπτογραφημένες πληροφορίες με απομακρυσμένους κόμβους εκτός δικτύου, οι οποίοι συνήθως δεν είναι περιορισμένων πόρων, και ως εκ τούτου μπορεί να πραγματοποιήσει εκτεταμένους υπολογισμούς [130].

Οι Saied και συν. πρότειναν μια ελαφριά συνεργατική προσέγγιση σχήματος εγκαθίδρυσης κλειδιού (key establishment) για τη μετατροπή υφιστάμενων πρωτοκόλλων ασφαλείας ώστε να είναι κατάλληλα για συσκευές με περιορισμένους πόρους. Αντί να μειώσει το κόστος των κρυπτογραφικών αλγορίθμων, το προτεινόμενο συνεργατικό σχήμα απαλλάσσει τις συσκευές με περιορισμένους πόρους από το υπολογιστικό και επικοινωνιακό overhead που δημιουργείται κατά την ανταλλαγή κλειδιών, μεταφέροντας αυτήν την επιβάρυνση σε γειτονικούς κόμβους με την κατάλληλη ισχύ, οι οποίοι βοηθούν στην εκτέλεση των εργασιών. Οι μελετητές υποστήριξαν ότι χρησιμοποιώντας αυτό το σχήμα, οι κόμβοι περιορισμένων πόρων μπορούν να εξοικονομήσουν έως και 35% της ενέργειάς τους κατά τη μεταφορά κλειδιών που απαιτούνται στην χειραψία του πρωτοκόλλου TLS (Transport Layer Security), σε σύγκριση με άλλα σχήματα [131].

Οι Kumar και συν. πρότειναν ένα ελαφρύ σχήμα εγκαθίδρυσης κλειδιού συνεδρίας (session key-establishment) και ελέγχου ταυτότητας (IBE) για έξυπνα οικιακά περιβάλλοντα. Με την εγκαθίδρυση του κλειδιού ασφαλείας, το σχήμα παρέχει εμπιστευτικότητα δεδομένων κατά τη μετάδοση μηνυμάτων, αμοιβαίο έλεγχο ταυτότητας οντοτήτων και προστασία της ακεραιότητας δεδομένων. Το σχήμα είναι ελαφρύ, δεδομένου ότι έχει σχεδιαστεί χρησιμοποιώντας μόνο συμμετρικά κρυπτογραφικά πρωτόγονα [132]. Σε άλλη τους μελέτη, οι Kumar και συν. πρότειναν ένα σχήμα εγκαθίδρυσης κλειδιών και ελέγχου ταυτότητας που υποστηρίζει επίσης την ανωνυμία των έξυπνων συσκευών, προκειμένου ο τύπος τους να μην μπορεί να βρεθεί από κάποιον επίδοξο επιτιθέμενο [133].

Οι Song και συν. πρότειναν ένα πρωτόκολλο ασφαλείας που επιτυγχάνει παρόμοιους στόχους. Η κύρια ιδέα των μελετητών αφορά τη δημιουργία ενός ενεργειακά αποδοτικού, ασφαλούς και διατήρησης του απορρήτου πρωτοκόλλου επικοινωνίας για έξυπνα οικιακά συστήματα. Στο προτεινόμενο πρωτόκολλο, οι μεταδόσεις των δεδομένων στο έξυπνο οικιακό

σύστημα ασφαλίζονται από ένα συμμετρικό σχήμα κρυπτογράφησης με μυστικά κλειδιά που δημιουργούνται από χαοτικά συστήματα. Η ενσωμάτωση ενός κώδικα IBE των μηνυμάτων που ανταλλάσσονται μεταξύ των συσκευών εγγυάται την ακεραιότητα και την αυθεντικότητα δεδομένων [134].

Οι Wazid και συν. πρότειναν ένα αποτελεσματικά ασφαλή σχήμα ελέγχου ταυτότητας (IBE) που προορίζεται συγκεκριμένα για συσκευές με περιορισμένους πόρους. Βασική ιδέα του σχήματος αποτελεί η εγγραφή του χρήστη και των έξυπνων συσκευών μέσω κάποιας αρχής εγγραφής (Registration Authority). Στη συνέχεια, ο έλεγχος ταυτότητας πραγματοποιείται με βάση τα μυστικά κλειδιά που δημιουργήθηκαν κατά τη φάση εγγραφής. Η αποτελεσματικότητα του σχήματος επιτυγχάνεται με τη χρήση μόνο πρωτογενών συμμετρικών κλειδιών (symmetric key primitives) [135].

Σε όλα τα παραπάνω σχήματα, θεωρείται ως δεδομένο ότι ο πάροχος υπηρεσιών είναι απόλυτα αξιόπιστος και ότι η πύλη HG δεν έχει παραβιαστεί.

Οι Choi και συν. ανέλυσαν τις επιθέσεις στο υλικολογισμικό των έξυπνων συσκευών με στόχο την επίτευξη δυσλειτουργιών τους. Οι μελετητές πρότειναν ένα σχήμα επαληθεύσιμης και επικυρωμένης ενημέρωσης του υλικολογισμικού ως τρόπο αντιμετώπισης αυτού του είδους των επιθέσεων, σύμφωνα με το οποίο η ενημέρωση μπορεί να γίνει ταχύτατα, μειώνοντας έτσι το παράθυρο της επίθεσης. Βασικό στοιχείου του συγκεκριμένου σχήματος αποτελεί ο συνδυασμός υπολογισμού βάσει σύζευξης των συσκευών, ψηφιακής υπογραφής Schnorr Signature Scheme και συμμετρικής αλυσίδας κατακερματισμού (symmetric-based hash chain) [136].

Οι Apthorpe και συν. απέδειξαν ότι οι πληροφορίες που συλλέγονται και μεταδίδονται μέσω του Διαδικτύου από τις έξυπνες συσκευές μπορούν να εξαχθούν από τους παρόχους ISP αλλά και από επίδοξους εισβολείς. Οι επιθέσεις που μπορούν να πραγματοποιηθούν κάνουν χρήση των μεταδεδομένων της δικτυακής κίνησης των δεδομένων. Περιλαμβάνουν, σε πρώτο στάδιο, την ανεύρεση του τύπου της συσκευής μέσω του αποτυπώματός της και, σε δεύτερο στάδιο, την εξαγωγή πληροφοριών που αφορούν τους χρήστες του σπιτιού μέσω των ρυθμών μεταβολής της κίνησης. Φυσικά, η γνώση του τύπου της έξυπνης οικιακής συσκευής, από μόνη της αποτελεί διαρροή απορρήτου. Για την αντιμετώπιση μιας τέτοιας επίθεσης, οι μελετητές πρότειναν τη χρήση συνδυασμού σήραγγας VPN (tunneling) και διαμόρφωση της δικτυακής κίνησης των δεδομένων [137].

Σε μια άλλη μελέτη που εξετάζει το ίδιο ζήτημα ασφάλειας, δηλαδή επιθέσεις με βάση την κυκλοφορία του δικτύου ακόμη και όταν οι πληροφορίες είναι κρυπτογραφημένες, οι Liu και συν. πρότειναν ένα πλαίσιο διαφύλαξης της ιδιωτικότητας με τεχνική αποφυγής της ανίχνευσης με σύγχυση (obfuscation) της κίνησης των δεδομένων για την αντιμετώπιση των επιθέσεων ανάλυσης κυκλοφορίας. Οι μελετητές δημιούργησαν ένα σχήμα δρομολόγησης πολλαπλών αλμάτων που εγγυάται τη σύζευξη μεταξύ των κόμβων πηγής και προορισμού, διατηρώντας παράλληλα την ασφάλεια και την προστασία της ιδιωτικότητας των πληροφοριών που αποστέλλονται και λαμβάνονται μεταξύ των πυλών HG των σπιτιών σε ένα έξυπνο κοινοτικό περιβάλλον [138].

Πολλές από τις μελέτες που έχουν παρουσιαστεί στη βιβλιογραφία ασχολούνται αποκλειστικά με την απόδοση των αλγορίθμων ασφαλείας για συσκευές ΔτΠ.

Οι Buchanan και συν. δημοσίευσαν ένα έγγραφο σχετικά με τις ελαφριές μεθόδους κρυπτογραφίας και πραγματοποίησαν εις βάθος ανάλυση ορισμένων από αυτές. Πιο συγκεκριμένα, χρησιμοποίησαν συγκριτική προτυποποίηση (benchmarking) FELICS (Fair Evaluation of Lightweight Cryptographic Systems) για να ελέγξουν την αποτελεσματικότητα των αλγορίθμων για εφαρμογές λογισμικού σε μικροελεγκτές των 8-bit, 16-bit και 32-bit. Από την σύγκριση που πραγματοποίησαν έβγαλαν ενδιαφέροντα συμπεράσματα, αλλά τα

πειράματά τους διεξήχθησαν για σταθερά μεγέθη μπλοκ και όχι σε περιπτώσεις πραγματικής χρήσης εφαρμογών hardware υλικού ή αισθητήρων ΔτΠ [139].

Οι Peireira και συν. παρουσίασαν μια λεπτομερή αξιολόγηση συμμετρικών κρυπτογραφικών πρωτογόνων που παρέχουν διαφορετικές υπηρεσίες ασφαλείας σε πραγματικές πλατφόρμες και λειτουργικά συστήματα δικτύων ΔτΠ και ασύρματων αισθητήρων (WSN). Οι μελετητές χρησιμοποίησαν ένα μικρό σύνολο τυχαία επιλεγμένων κρυπτογραφικών αλγορίθμων, όπως AES, Curupira και Trivium, και μερικών μη τυποποιημένων αλγορίθμων, όπως ο Marvin [140].

5.2 Λύσεις πρωτοκόλλων ελέγχου ταυτότητας και ελέγχου πρόσβασης

Οι διαδικασίες ελέγχου ταυτότητας και ελέγχου πρόσβασης διαδραματίζουν βασικούς ρόλους όσον αφορά την ασφάλεια και την προστασία της ιδιωτικότητας των συσκευών ΔτΠ. Ο έλεγχος ταυτότητας αποτρέπει μη εξουσιοδοτημένες οντότητες από το να αποκτήσουν πρόσβαση σε συσκευές, δεδομένα και πληροφορίες διασφαλίζοντας ότι οι επικοινωνιακές οντότητες είναι αυτές που ισχυρίζονται ότι είναι, ενώ ο έλεγχος πρόσβασης αποτρέπει τη μη εξουσιοδοτημένη χρήση ενός πόρου. Ο σχεδιασμός και η εφαρμογή τέτοιων διαδικασιών σε συσκευές με περιορισμένους πόρους αποτελεί μια πραγματική πρόκληση που αντιμετωπίζει η ερευνητική κοινότητα, με πλήθος μελετών να ασχολούνται με το συγκεκριμένο θέμα.

Οι Pereira και συν. παρουσίασαν ένα σχήμα ελέγχου ταυτότητας και ελέγχου πρόσβασης που βασίζεται στο πρωτόκολλο CoAP (Constrained Application Protocol). Το προτεινόμενο πλαίσιο αξιοποιεί τα πλεονεκτήματα των σχημάτων Kerberos και RADIUS (Remote Authentication Dial In User Service) ώστε να αποτελέσει μια ενεργειακά αποδοτική λύση ελέγχου AAA (Authentication, Access and Accounting) για συσκευές ΔτΠ που δεν διαθέτουν πόρους. Οι διαδικασίες ελέγχου ταυτότητας και πρόσβασης περιλαμβάνει 2 βήματα. Το πρώτο βήμα αποτελεί τον έλεγχο ταυτότητας, το οποίο περιλαμβάνει τον προσδιορισμό της νομιμότητας του χρήστη με χρήση του αποθηκευτικού χώρου NAS (Network Attached Storage) του CoAP. Ο NAS ελέγχεται διεξοδικά για την ανεύρεση πληροφοριών που αφορούν δικαιώματα του χρήστη και στην περίπτωση νομιμότητάς του στέλνεται μήνυμα έγκρισής του. Το δεύτερο βήμα αποτελεί τον έλεγχο πρόσβασης, στο οποίο το μήνυμα έγκρισης συνοδεύει κάθε αίτημα πελάτη καθορίζοντας τα δικαιώματα πρόσβασης του χρήστη, ενώ παράλληλα ο διακομιστής αποκρίνεται με μήνυμα σφάλματος σε οποιοδήποτε αίτημα πελάτη χωρίς έγκυρο μήνυμα έγκρισης. Ο προτεινόμενος μηχανισμός ελέγχου πρόσβασης δοκιμάστηκε σε πολλές υπηρεσίες με διαφορετικούς τύπους δικαιωμάτων και τα αποτελέσματα έδειξαν ότι το σχήμα ανταποκρίνεται σε αιτήματα σύμφωνα με τα δικαιώματα των πελατών [141].

Οι Jan και συν. πρότειναν ένα ελαφρύ σχήμα αμοιβαίου ελέγχου ταυτότητας το οποίο επαληθεύει τις ταυτότητες των συσκευών (πελάτες και διακομιστές) που πρόκειται να λάβουν μέρος στην επικοινωνία για παρατήρηση των πόρων σε περιβάλλον ΔτΠ που χρησιμοποιεί πρωτόκολλο CoAP. Το πρόγραμμα επιτρέπει επίσης στους επαληθευμένους πελάτες να έχουν πρόσβαση σε διάφορους πόρους βάσει των αντίστοιχων αιτημάτων τους. Οι μελετητές επεσήμαναν ξεκάθαρα ότι το προτεινόμενο σχήμα αποτελεί μια επέκταση των χαρακτηριστικών ασφαλείας του πρωτοκόλλου CoAP με σκοπό να καταστεί πιο ισχυρό, αποτελεσματικό και ικανό να αντιμετωπίσει μια σειρά από απειλές. Ως εκ τούτου πρότειναν έναν στιβαρό, εύκολο στην εφαρμογή και με μικρότερη υπολογιστική επιβάρυνση αλγόριθμο ελέγχου ταυτότητας ως εναλλακτική λύση για το πρωτόκολλο DTLS (Datagram Transport Layer Security). Η προτεινόμενη διαδικασία ελέγχου ταυτότητας χρησιμοποιεί 4 μηνύματα χειραψίας, δαπανά λιγότερα από 1024 bit ως κόστος σύνδεσης και χρησιμοποιεί το πρότυπο κρυπτογράφησης AES 128-bit. Αν και το προτεινόμενο σχήμα είναι σε θέση να αντιμετωπίσει επιθέσεις όπως υποκλοπές, κατασκευές κακόβουλων κλειδιών, εξάντληση πόρων και DoS, οι μελετητές παρατήρησαν ότι δεν αποτελεί αποτελεσματική λύση για την αντιμετώπιση άλλων επιθέσεων, όπως Sybil, wormhole, sinkhole και επιλεκτικής προώθησης [142].

Οι Turkanovic και συν. πρότειναν ένα σχήμα ελέγχου ταυτότητας χρήστη και συμφωνίας κλειδιού (key agreement) για ετερογενή ad hoc δίκτυα WSN για εφαρμογές ΔτΠ. Το προτεινόμενο σχήμα επιτρέπει στον χρήστη την ασφαλή πρόσβαση σε έναν συγκεκριμένο κόμβο WSN χωρίς τη μεσολάβηση του κόμβου πύλης χρησιμοποιώντας ένα σπάνιο μοντέλο ελέγχου ταυτότητας 4 βημάτων. Το σχήμα υποστηρίζει και τη δυναμική αύξηση του αριθμού των κόμβων αισθητήρων στους οποίους μπορεί να έχει πρόσβαση ο χρήστης. Οι μελετητές χρησιμοποίησαν ένα ελαφρύ πρωτόκολλο συμφωνίας κλειδιού για να διασφαλίσουν τον αμοιβαίο έλεγχο ταυτότητας μεταξύ των συμμετεχόντων οντοτήτων (χρήστης, κόμβος αισθητήρα και κόμβος πύλης). Προκειμένου να διασφαλιστεί ότι το προτεινόμενο σχήμα είναι κατάλληλο για συσκευές περιορισμένων πόρων στο πλαίσιο του ΔτΠ, οι μελετητές απέφυγαν τη χρήση υπολογισμών με μεγάλη επιβάρυνση πόρων, χρησιμοποιώντας απλούς υπολογισμούς κατακερματισμού και Exclusive OR (XOR). Μετά από 2 φάσεις εγγραφής, ο χρήστης κάνει log in χρησιμοποιώντας μια έξυπνη κάρτα και για τον έλεγχο ταυτότητας στέλνει ένα μήνυμα ελέγχου ταυτότητας απευθείας στον κόμβο αισθητήρα που θέλει να συνδεθεί. Η ασφαλής επικοινωνία μπορεί να ξεκινήσει μετά από μια επιτυχημένη συνεδρία διαπραγμάτευσης κλειδιού. Τα αποτελέσματα της αξιολόγησης ασφάλειας έδειξαν ότι το προτεινόμενο σχήμα μπορεί να αντιμετωπίσει επιθέσεις επανάληψης (replay attack), stolen verifier, κλοπής και παραβίασης έξυπνων καρτών, πλαστοπροσωπίας και πολλών συνδεδεμένων χρηστών με την ίδια ταυτότητα σύνδεσης [143].

Οι Shivraj και συν. πρότειναν μια τεχνική One Time Password (OTP) δύο παραγόντων που βασίζεται σε ένα ελαφρύ σχήμα ελέγχου ταυτότητας ECC. Αυτή η τεχνική ήταν καλύτερη από άποψη αποτελεσματικότητας και ασφάλειας σε σύγκριση με τις υπάρχουσες μεθόδους για δύο λόγους. Πρώτον, το κέντρο διανομής κλειδιών (Key Distribution Center - KDC) δεν απαιτεί αποθήκευση κλειδιών. Δεύτερον, δεν αποθηκεύει τα ιδιωτικά και δημόσια κλειδιά των άλλων συσκευών. Αυτό το πρωτόκολλο καταναλώνει ένα μικρό ποσό πόρων χωρίς να επηρεάζει αρνητικά την ασφάλεια. Παρόλα αυτά, παρουσιάζει ένα μειονέκτημα: την έλλειψη υποστήριξης της περίπτωσης κατά την οποία μια συσκευή θέλει να κάνει χρήση διαφορετικού συστήματος ασφαλείας [144].

Οι Hernandez και συν. παρουσίασαν έναν αριθμό ελαφρών μηχανισμών ελέγχου ταυτότητας και εξουσιοδότησης που βασίζονται στο πρωτόκολλο SEAPOL (Slim Extensible Authentication Protocol Over LAN), το οποίο αποτελεί βελτιωμένη έκδοση του EAPOL (Extensible Authentication Protocol Over LAN). Οι προτεινόμενοι μηχανισμοί βοήθησαν στην ενσωμάτωση λειτουργιών ελέγχου ταυτότητας και εξουσιοδότησης σε συσκευές με περιορισμένους πόρους. Το EAPOL σταθμίζει τις συσκευές υποχρεώνοντάς τις να εφαρμόσουν και να εκτελέσουν το EAPOL σε συνδυασμό με το DTLS. Οι προτεινόμενοι μηχανισμοί είναι σε θέση να βελτιστοποιήσουν τη διαλειτουργικότητα των συσκευών που λειτουργούν σε περιβάλλον ΔτΠ, αλλά και να αντιμετωπίσουν τα ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας στην εφαρμογή του στα έξυπνα σπίτια [145].

Λαμβάνοντας υπόψη τη σημαντική αύξηση των φορητών συσκευών ΔτΠ και τις νέες τάσεις στις ηλεκτρονικές πληρωμές, οι Yohan και συν πρότειναν ένα ασφαλές πρωτόκολλο ελέγχου ταυτότητας που βασίζεται στο πρωτόκολλο BLE για μικροπληρωμές με wearable συσκευές ΔτΠ. Το προτεινόμενο σχήμα βασίζεται στον αμοιβαίο έλεγχο ταυτότητας μεταξύ της wearable συσκευής και ενός μετρητή wearable payment counter. Με τον τρόπο αυτό, η επικοινωνία πραγματοποιείται μεταξύ μόνο αυτών των δύο οντοτήτων χωρίς τη βοήθεια οποιασδήποτε ενδιάμεσης συσκευής, όπως ένα smartphone. Το σχήμα δημιουργεί μοναδικό κλειδί συνεδρίας που χρησιμοποιείται για κάθε διαδικασία επικοινωνίας μαζί με μια μυστική συμβολοσειρά (string) που είναι αποθηκευμένη στην wearable συσκευή και τον μετρητή. Το προτεινόμενο πρωτόκολλο αποτελείται από 3 στάδια: το στάδιο αρχικοποίησης, το στάδιο ελέγχου ταυτότητας και το στάδιο πληρωμής. Οι μελετητές ισχυρίστηκαν ότι το προτεινόμενο

πρωτόκολλο μπορεί να αντιμετωπίσει σημαντικές επιθέσεις, όπως πειρατείας συνεδρίας, παθητικής υποκλοπής, επανάληψης και Man-In-The-Middle [146].

Οι Park και συν. παρουσίασαν μια ασφαλή μέθοδο ελέγχου ταυτότητας χρησιμοποιώντας πρωτόκολλο μηδενικής γνώσης (Zero Knowledge Proof – ZKP) σε ένα έξυπνο οικιακό περιβάλλον. Σε αυτήν την προσέγγιση, κατά τη διαδικασία ελέγχου ταυτότητας, δεν ανταλλάσσεται κανένα μυστικό κλειδί μεταξύ του κόμβου και της πύλης HG, αλλά, η πύλη παρέχει στον κόμβο έναν αριθμό, ο οποίος μπορεί να χρησιμοποιηθεί αργότερα από τον κόμβο για να αποδείξει την αυθεντικότητά του [147].

Οι Risalat και συν. παρουσίασαν ένα ασφαλές πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας που βασίζεται στη λειτουργία κατακερματισμού μονής κατεύθυνσης. Αυτό το πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας επιτρέπει δυναμικές ενημερώσεις της τιμής του μυστικού κλειδιού που χρησιμοποιείται. Τα αποτελέσματα της αξιολόγησής του έδειξαν ότι το προτεινόμενο πρωτόκολλο μπορεί να αντιμετωπίσει διάφορες επιθέσεις, όπως επιθέσεις Man-In-The-Middle, επανάληψης, υποκλοπής, ανίχνευσης και αποσυγχρονισμού. Παρά την επιτυχημένη της αξιολόγηση, η μέθοδος παρουσιάζει ένα μειονέκτημα, που αφορά τον τρόπο της δυναμικής ενημέρωσης του μυστικού κλειδιού, καθώς καθιστά εύκολη την εικασία αύξησης του αριθμού σειράς του [148].

Ο Wilson εισήγαγε ένα πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας κατά την επικοινωνία μεταξύ συσκευών σε ένα έξυπνο οικιακό περιβάλλον ΔτΠ, που βασίζεται σε ασύμμετρη κρυπτογραφία. Το προτεινόμενο πρωτόκολλο επιτρέπει στους έξυπνους οικιακούς κόμβους να επικυρώνουν μεταξύ τους και να συμφωνούν σε ένα δυναμικό κοινό μυστικό κλειδί σε κάθε συνεδρία επικοινωνίας χωρίς ανθρώπινη συμμετοχή. Η παραγωγή των μυστικών κλειδιών βασίζεται σε μεθόδους δημιουργίας ψευδο τυχαίων αριθμών. Το αποτέλεσμα της αξιολόγησης του πρωτοκόλλου με τη χρήση των εργαλείων SPAN / AVISPA έδειξε ότι είναι ασφαλές απέναντι σε γνωστές επιθέσεις, όπως Man-In-The-Middle, επανάληψης και υποκλοπής. Ωστόσο, παρόλη την αποτελεσματικότητά του, οι σύγχρονες συσκευές περιορισμένων πόρων δεν είναι ικανές να χειρίζονται ασύμμετρη κρυπτογραφία. Η ασφάλεια της μεθόδου μπορεί να τεθεί σε κίνδυνο λόγω των μειονεκτημάτων που παρουσιάζει στην περίπτωση δημιουργίας και ανταλλαγής μυστικών κλειδιών μεταξύ των συσκευών του έξυπνου σπιτιού κατά τη φάση διαμόρφωσης του, αν αυτή έχει μεγάλη διάρκεια [149].

Οι Dorri και συν. παρουσίασαν μια προσέγγιση που βασίζεται στην τεχνολογία του blockchain, ως μια αποκεντρωμένη μέθοδος ασφάλειας και προστασίας του απορρήτου που σχετίζεται με τον κατανεμημένο χαρακτήρα του ΔτΠ. Στο προτεινόμενο σχήμα, κάθε έξυπνη οικιακή συσκευή αποθηκεύει και διατηρεί το δικό της blockchain που θα διαχειρίζεται και θα ελέγχει την ασφαλή διαδρομή επικοινωνίας. Η ανάλυση της ασφάλειας και της διατήρησης του απορρήτου της συγκεκριμένης μεθόδου, έδειξε ότι η επιβάρυνση στο overhead είναι διαχειρίσιμη και ελάχιστη για τις συσκευές με περιορισμένους πόρους [150].

5.3 Λύσεις hardware υλικού

Τα συστήματα ασφαλείας που βασίζονται σε λύσεις λογισμικού εξακολουθούν να παραμένουν ευάλωτα σε συγκεκριμένους τύπους επιθέσεων. Οι μηχανισμοί ασφαλείας που εφαρμόζονται σε αυτές τις περιπτώσεις αποσκοπούν αποκλειστικά στην προστασία των μηνυμάτων που μεταφέρονται κατά την επικοινωνία. Βασίζονται σε μαθηματικές προσεγγίσεις που μπορεί να μην είναι εύκολα επιλύσιμες από τους επιτιθέμενους χρησιμοποιώντας τους σύγχρονους υπολογιστές, αλλά όταν η ύπαρξη κβαντικών υπολογιστών γίνει πραγματικότητα, μπορούν να επιλυθούν σε μικρότερο χρονικό διάστημα σε σύγκριση με παραδοσιακές μεθόδους εξαγωγής των κλειδιών [152]. Επιπλέον, στους μηχανισμούς ασφαλείας που βασίζονται σε λύσεις λογισμικού, τα κλειδιά αποθηκεύονται στις μη πτητικές μνήμες των συσκευών που είναι επιρρεπείς σε επιθέσεις. Αν και τα συστήματα ασφαλείας που βασίζονται σε λογισμικό ήταν αποτελεσματικά όλα αυτά τα χρόνια, η εξέλιξη του hardware υλικού και

των υπολογιστών μπορεί να επιτρέψει στους επιτιθέμενους να τα παρακάμψουν χρησιμοποιώντας κβαντικούς υπολογιστές [153]. Επομένως, όλοι οι υπάρχοντες μηχανισμοί ασφάλειας λογισμικού διατρέχουν υψηλό κίνδυνο και η αποτροπή επιθέσεων είναι πολύ δύσκολη αν ένα σύστημα χρησιμοποιεί λύσεις ασφαλείας που βασίζονται μόνο στο λογισμικό. Ως εκ τούτου, πολλοί ερευνητές υποστηρίζουν ότι οι προσεγγίσεις ασφαλείας που βασίζονται στο hardware υλικό μπορούν να παρέχουν την υποκείμενη υποστήριξη για την αντιμετώπιση των ζητημάτων ασφάλειας και προστασίας της ιδιωτικότητας που σχετίζονται με τις συσκευές ΔτΠ [154].

Οι λύσεις ασφάλειας που βασίζονται στο hardware υλικό χρησιμοποιούν ένα αποκλειστικό κύκλωμα ολοκληρωμένων ή επεξεργαστή για την εκτέλεση κρυπτογραφικών λειτουργιών και την αποθήκευση των κλειδιών. Οι συγκεκριμένες μονάδες, που είναι γνωστές ως hardware μονάδες ασφάλειας (Hardware Security Modules HSM), μπορούν να αποτρέψουν την πρόσβαση ανάγνωσης και εγγραφής σε δεδομένα και προσφέρουν ισχυρότερη προστασία απέναντι σε διάφορες επιθέσεις. Οι μηχανισμοί που βασίζονται στις μονάδες HSM έχουν χρησιμοποιηθεί για επεξεργασία κρυπτογράφησης και ισχυρό έλεγχο ταυτότητας, διαδικασίες στις οποίες τα ψηφιακά κλειδιά μπορούν να κρυπτογραφηθούν, να αποκρυπτογραφηθούν, να αποθηκευτούν και να διαχειριστούν. Οι μονάδες HSM έχουν χρησιμοποιηθεί παράλληλα με μηχανισμούς λογισμικού, όπως οι PKI και AES, για την κρυπτογράφηση των μηνυμάτων τους [155].

Ένα από τα κύρια προβλήματα με τις λύσεις ασφαλείας που βασίζονται στο hardware υλικό είναι ότι είναι επιρρεπείς στις επιθέσεις Man-In-The-Middle. Σε αυτές τις επιθέσεις, όταν οι επιτιθέμενοι αποκτήσουν πρόσβαση στη μονάδα HSM, μπορούν να κλωνοποιήσουν τη συσκευή. Η χρήση των φυσικών μη κλωνοποιήσιμων συναρτήσεων (Physical Unclonable Functions - PUFs) αποτελεί μια ακαδημαϊκά αποδεκτή λύση σε αυτό το πρόβλημα. Οι συναρτήσεις αυτές εισήχθησαν ως πρωτόγονο ασφαλείας που βασίζεται στο hardware υλικό. Χρησιμοποιούν τις εγγενείς παραλλαγές κατασκευής μιας συσκευής για να δημιουργήσουν ένα αποτύπωμα του hardware υλικού της, κάτι που προσφέρει το πολύτιμο πλεονέκτημα της αδυναμίας κλωνοποίησης της. Αυτή η ιδιότητα δίνει στις συναρτήσεις PUF πλεονέκτημα έναντι άλλων τεχνικών ασφαλείας που βασίζονται στο hardware υλικό, καθώς ο εισβολέας δεν μπορεί να κλωνοποιήσει τις εγγενείς ιδιότητες της συσκευής ακόμη και αν αποκτήσει φυσική πρόσβαση σε αυτή. Επομένως, οι συναρτήσεις PUF είναι μοναδικές για κάθε συσκευή και μπορεί να χρησιμοποιηθούν ως πρωτόγονο ασφαλείας που επιτρέπει τον έλεγχο ταυτότητας και αυθεντικοποίησης της συσκευής. Επιπλέον, οι συναρτήσεις PUF μπορούν να προσφέρουν μια εναλλακτική λύση χαμηλού κόστους κατ' απαίτηση δημιουργίας κρυπτογραφικών κλειδιών από τη συσκευή [156].

Στη βιβλιογραφία, οι συναρτήσεις PUF έχουν χρησιμοποιηθεί κατά κόρον ως hardware αντιμετώπιση των επιθέσεων κατά των έξυπνων σπιτιών ΔτΠ. Οι Xu και συν. μελέτησαν τη χρήση ψηφιακών PUF ως ασφάλεια hardware υλικού με σκοπό τη βελτιστοποίηση της σχεδίασης CAD πιο ασφαλών συσκευών ΔτΠ. Οι μελετητές παρατήρησαν ότι οι αναλογικές συναρτήσεις PUF είναι δύσκολο να ενσωματωθούν σε ψηφιακές λύσεις hardware ασφάλειας και ως εκ τούτου υποστήριξαν τη χρήση ψηφιακών PUF, γνωστών και ως Public Physical Unclonable Functions (PPUFs), που επιτρέπουν τη δημιουργία πρωτοκόλλων δημόσιου κλειδιού. Οι συγγραφείς πιστεύουν ότι οι λύσεις ασφαλείας που βασίζονται στο hardware υλικό θα ενισχύσουν τη βελτιστοποίηση της σχεδίασης CAD, ώστε να δείξει μεγαλύτερη ανθεκτικότητα έναντι των επιθέσεων πλευρικού καναλιού αλλά και φυσικών επιθέσεων και θα χρησιμεύσει ως καλή πλατφόρμα εφαρμογής πρωτοκόλλων ΔτΠ, λόγω της ενεργειακής τους απόδοσης [157].

Διατηρώντας το ίδιο πνεύμα, οι Aman και συν. παρουσίασαν ένα πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας συστημάτων ΔτΠ που βασίζεται σε συναρτήσεις PUF. Οι μελετητές

υποστήριξαν ότι τα μοναδικά χαρακτηριστικά των PUF μπορούν να αξιοποιηθούν για να παρέχουν ασφάλεια σε συσκευές ΔτΠ χωρίς την ανάγκη αποθήκευσης μυστικών κλειδιών στις συσκευές. Η διαδικασία ελέγχου ταυτότητας που παρουσίασαν αποτελείται από 4 βήματα, καθένα από τα οποία περιλαμβάνει 3 μηνύματα. Στο βήμα 1, μια συσκευή ΔτΠ ξεκινά τη διαδικασία ελέγχου ταυτότητας στέλνοντας το αναγνωριστικό της σε έναν διακομιστή και μετά από μερικούς υπολογισμούς, ο διακομιστής επαληθεύει το μήνυμα χρησιμοποιώντας ένα MAC (Message Authentication Code) στο βήμα 4. Εάν ο διακομιστής επαληθεύσει το MAC του μηνύματος 3, αυτό σημαίνει ότι ο έλεγχος ταυτότητας είναι επιτυχής. Ωστόσο, εάν η επαλήθευση MAC αποτύχει σε οποιοδήποτε βήμα, ο έλεγχος ταυτότητας αποτυγχάνει ολοκληρωτικά. Αξιολόγηση του πρωτοκόλλου απέδειξε ότι παρέχει ασφάλεια έναντι πολλών επιθέσεων, όπως κλωνοποίησης ή πλαστοπροσωπίας, επανάληψης, υποκλοπής, Man-In-The-Middle, spoofing, παρέμβασης (interleaving attack) και φυσικές επιθέσεις [158].

Πλησιάζοντας το θέμα από μια διαφορετική οπτική γωνία, ο Rose πρότεινε τη χρήση τεχνολογιών νανοηλεκτρονικού hardware υλικού, όπως μνημαντιστάσεων οξειδίων των μετάλλων (metal oxide memristors), για την εφαρμογή πρωτογόνων και πρωτοκόλλων ασφαλείας σε αναδυόμενες συσκευές ΔτΠ. Η λογική της μελέτης είναι ότι τα πρωτόγονα ασφάλειας νανοκλίμακας μπορούν να παρέχουν τα απαιτούμενα επίπεδα ασφάλειας, ενώ καταναλώνουν αμελητέα ποσότητα ενέργειας. Ο συγγραφέας χρησιμοποίησε memristive Crossbar PUF (XbarPUF) που βασίζεται στο Write-Time Memristive PUF (WTMPUF). Αν και το XbarPUF δεν εξαρτάται από τον ακριβή χρόνο εγγραφής, ο συγγραφέας ανακάλυψε ότι αποδίδει με τον ίδιο τρόπο όπως το WTMPUF. Επιπλέον, η απόδοση του XbarPUF είναι παρόμοια με τα κυκλώματα που κατασκευάζονται με τεχνολογία CMOS, όπως το Arbiter PUF (APUF), με το πλεονέκτημα της μείωσης του αριθμού των τρανζίστορ. Επίσης, η ποσότητα ισχύος που καταναλώθηκε από το XbarPUF κατά τη διάρκεια της μελέτης ήταν σημαντικά μικρότερη σε σύγκριση με την αντίστοιχη ισχύ που καταναλώνονται από τα WTMPUF και APUF [159].

Οι Yang και συν. παρουσίασαν μια έρευνα σχετικά με τις συσκευές ΔτΠ εξαιρετικά χαμηλής ισχύος (Ultra-Low-Power - ULP). Η εργασία τους επικεντρώθηκε στη βελτιστοποίηση των αντισταθμίσεων μεταξύ ισχύος, κόστους και ασφάλειας των συσκευών. Οι συγγραφείς μελέτησαν την εφαρμογή τεχνικών ελέγχου ταυτότητας των συσκευών που βασίζονται στην κρυπτογραφία και εκείνων που βασίζονται στις συναρτήσεις PUF και υπογράμμισαν την ανάγκη για καλύτερα μπλοκ hardware υλικού προκειμένου να υποστηριχθεί ο έλεγχος ταυτότητας των συσκευών και η ασφάλεια των δεδομένων. Η εργασία τους εντόπισε ανοιχτά ζητήματα και μελλοντικές κατευθύνσεις έρευνας όσον αφορά τη ασφάλεια των συσκευών ULP. Οι συγγραφείς απέδειξαν επίσης ότι ο καθορισμός του πρωτοκόλλου που πρέπει να χρησιμοποιηθεί σε κάθε περίπτωση εξαρτάται αποκλειστικά από τον τύπο της εφαρμογής που υλοποιείται. Για παράδειγμα, τα πρωτόκολλα ελέγχου ταυτότητας που βασίζονται στις συναρτήσεις PUF είναι τα καλύτερα στις περιπτώσεις συστημάτων που απαιτούν μηχανές κρυπτογράφησης [160].

5.4 Σύγχρονοι μηχανισμοί ασφαλείας

Παρόλο που η αντιμετώπιση των θεμάτων ασφάλειας και προστασίας ιδιωτικότητας των έξυπνων οικιακών συσκευών ΔτΠ από ολιστική άποψη παραμένει ως πρόβλημα, υπάρχουν αρκετοί σύγχρονοι μηχανισμοί οι οποίοι βασίζονται σε μια σειρά τεχνικών ασφαλείας και κρυπτογραφικών αλγορίθμων, όπως συναρτήσεις κατακερματισμού, κρυπτογράφηση XOR, έλεγχος πρόσβασης και ελαφριά κρυπτογραφικά σχήματα δημόσιου κλειδιού που βασίζονται στην μέθοδο ECC και που μπορούν να δώσουν λύσεις στο συγκεκριμένο πρόβλημα.

5.4.1 Συναρτήσεις κατακερματισμού και γεννήτριες CSPRNG

Στο περιβάλλον του ΔτΠ, μπορούν να χρησιμοποιηθούν συναρτήσεις κατακερματισμού και γεννήτριες CSPRNG (Cryptographically Secure Pseudo Random Number Generators) ως λύσεις ασφαλείας των έξυπνων οικιακών συσκευών. Η χρήση των αλγορίθμων κατακερματισμού γίνεται κυρίως για τη διασφάλιση της ακεραιότητας των έξυπνων οικιακών συστημάτων, ενώ οι γεννήτριες ψευδοτυχαίων αριθμών PRNG μπορούν να χρησιμοποιηθούν σε κρυπτογραφικές εφαρμογές όπου η ασφάλεια αποτελεί κρίσιμο στοιχείο [161].

Οι Sundaram και συν. πρότειναν αλγόριθμους κρυπτογράφησης και κατακερματισμού μέσω των οποίων οι έξυπνες οικιακές συσκευές ΔτΠ μπορούν να στέλνουν μηνύματα μεταξύ τους με ασφάλεια. Ο αλγόριθμος κρυπτογράφησης χρησιμοποιείται για τη διασφάλιση της εμπιστευτικότητας καθώς οι εισβολείς δεν μπορούν να ερμηνεύσουν το κρυπτογραφημένο κείμενο που αποστέλλεται. Για να διασφαλιστεί η ακεραιότητα, χρησιμοποιείται αλγόριθμος κατακερματισμού [162].

Οι Prudanov και συν. πρότειναν ένα ελαφρύ πρωτόκολλο ελέγχου ταυτότητας που επιτρέπει την ταυτόχρονη αναγνώριση νέων συσκευών ΔτΠ (π.χ. αισθητήρες, ενεργοποιητές, μετρητές, κ.λπ.) που συνδέονται με την κεντρική μονάδα επικοινωνίας ενός έξυπνου οικιακού δικτύου. Σύμφωνα με τους μελετητές, οι απαιτήσεις ασφαλείας στο πλαίσιο των έξυπνων οικιακών δικτύων, όσον αφορά τους μηχανισμούς ελέγχου ταυτότητας, περιλαμβάνουν την εμπιστευτικότητα των, τον αμοιβαίο έλεγχο ταυτότητας και την συνολική ασφάλεια του δικτύου. Για το λόγο αυτό, ανέλυσαν την απόδοση του πρωτοκόλλου Yoking-proof, ένα ελαφρύ εργαλείο ελέγχου ταυτότητας διαφόρων συσκευών ΔτΠ και απέδειξαν ότι το συγκεκριμένο πρωτόκολλο μπορεί να εφαρμοστεί και να χρησιμοποιηθεί εύκολα σε ένα περιβάλλον έξυπνου σπιτιού παρέχοντας ασφαλή έλεγχο ταυτότητας των νέων συσκευών που εντάσσονται στο οικιακό δίκτυο, γεγονός που αυξάνει την αντίληψη του χρήστη ως προς την εμπιστοσύνη των διαφορετικών έξυπνων οικιακών λύσεων. Βασικά στοιχεία του πρωτοκόλλου Yoking-proof αποτελούν οι χρήσεις αλγορίθμων κατακερματισμού και γεννητριών PRNG [163].

Οι Oluwade και συν. παρουσίασαν μια τεχνική διαχείρισης της εντροπίας ενός ελαφρού πρωτοκόλλου κρυπτογραφίας με σκοπό την ασφάλεια των έξυπνων οικιακών συσκευών. Σκοπός των μελετητών ήταν η βελτίωση του παραδοσιακού αλγόριθμου κρυπτογράφησης TEA (Tiny Encryption Algorithm). Η εντροπία αποτελεί σημαντικό παράγοντα στις τεχνικές κρυπτογραφίας και αφορά την ασφαλή επικοινωνία μεταξύ δύο κόμβων. Στην συγκεκριμένη μελέτη οι αλγόριθμοι κατακερματισμού και οι γεννήτριες PRNG χρησιμοποιήθηκαν για την ενίσχυση της εντροπίας στη διαχείριση των κλειδιών που τη δημιουργούνται για την επίτευξη ασφαλούς επικοινωνίας μεταξύ των συσκευών ενός έξυπνου σπιτιού που λειτουργεί σε περιβάλλον ΔτΠ. Η αξιολόγηση της τεχνικής απέδειξε ότι μπορεί να αντιμετωπίσει σημαντικές επιθέσεις κατά της ασφάλειας ενός έξυπνου σπιτιού, όπως Man-In-The-Middle, λαθρακρόασης, πλαστοπροσωπίας και επιθέσεις DoS [164].

5.4.2 Κρυπτογράφηση XOR

Η κρυπτογράφηση XOR (eXclusive OR) αποτελεί ελαφριά τεχνική κρυπτογράφησης και ως εκ τούτου χρησιμοποιείται σε πολλούς μηχανισμούς ασφαλείας του περιβάλλοντος ΔτΠ. Είναι μια μέθοδος κρυπτογράφησης που είναι δύσκολο να "σπάσει" με τις λεγόμενες μεθόδους "brute force", δηλαδή τη χρήση τυχαίων κλειδιών κρυπτογράφησης με την ελπίδα να βρεθεί το σωστό, αλλά είναι ευαίσθητη στην αναγνώριση μοτίβων. Το συγκεκριμένο μειονέκτημα μπορεί εύκολα να αντιμετωπιστεί, αν πριν της κρυπτογράφησης προηγηθεί διαδικασία συμπίεσης, κατά την οποία τα μοτίβα αφαιρούνται. Η μέθοδος κρυπτογράφησης XOR δεν χρησιμοποιεί δημόσια κλειδιά, όπως το RSA, αλλά τυχαία. Εάν το κλειδί είναι τυχαίο και το μήκος του τουλάχιστον όσο του μηνύματος που μεταδίδεται κατά την επικοινωνία, η κρυπτογράφηση

XOR είναι πολύ πιο ασφαλής από ότι όταν υπάρχει επανάληψη χρήσης του ίδιου κλειδιού. Όταν το κλειδί δημιουργείται από μια γεννήτρια PRNG, το αποτέλεσμα είναι μια κρυπτογράφηση, η οποία είναι άθραυστη θεωρητικά. Χρησιμοποιεί τη συνάρτηση XOR της άλγεβρας Boolean, έναν δυαδικό τελεστή, που σημαίνει ότι χρειάζεται δύο ορίσματα όταν χρησιμοποιείται. Εάν ένα από τα δύο ορίσματα είναι αληθές και το άλλο όρισμα είναι ψευδές, τότε η έξοδος της συνάρτηση XOR θα είναι ένα όρισμα αληθές [165].

Οι Zhou και συν. παρουσίασαν ένα ελαφρύ σχήμα ελέγχου ταυτότητας δύο παραγόντων που βασίζεται στη χρήση κατακερματισμού απλής κατεύθυνσης και κρυπτογράφησης XOR Η διαδικασία ελέγχου ταυτότητας αποτελείται από τρία βήματα: εγγραφής, επαλήθευσης και ανανέωσης του κωδικού πρόσβασης. Λαμβάνοντας υπόψη το κόστος υπολογισμού ενός τέτοιου σχήματος, η αποδοτικότητά του αποδείχθηκε ικανοποιητική σε περιβάλλοντα περιορισμένων πόρων, όπως είναι τα έξυπνα οικιακά δίκτυα [166].

Οι Lyu και συν. πρότειναν ένα μοντέλο έξυπνου οικιακού συστήματος που βασίζεται σε υπηρεσίες Διαδικτύου και σχεδίασαν ένα σχήμα αμοιβαίου ελέγχου ταυτότητας στο οποίο επιτυγχάνεται συμφωνία ανταλλαγής κλειδιού με σκοπό την αντιμετώπιση της δυνατότητας παρακολούθησης των έξυπνων οικιακών συσκευών από επίδοξους επιτιθέμενους. Συγκεκριμένα, το εν λόγω σύστημα περιλαμβάνει μια πύλη HG IFTTT (IF This Then That), ως εκτελεστή των εντολών ελέγχου και ασφαλείας, ώστε να δίνεται η δυνατότητα στους νόμιμους χρήστες να έχουν πρόσβαση εξ αποστάσεως στις έξυπνες οικιακές συσκευές διατηρώντας την ιδιωτικότητά τους. Το προτεινόμενο σχήμα χρησιμοποιεί αλγόριθμους κρυπτογράφησης ECC, XOR και κατακερματισμού για την επίτευξη αμοιβαίου ασφαλούς ελέγχου ταυτότητας διατηρώντας τα χαρακτηριστικά ασφαλείας και διατήρησης της ανωνυμίας. Τα αποτελέσματα της ανάλυσης ασφάλειας και απόδοσης του προτεινόμενου σχήματος απέδειξαν την επίτευξη ασφαλούς ελέγχου ταυτότητας κατά την επικοινωνία των χρηστών με τις έξυπνες οικιακές συσκευές με παράλληλη προστασία της ιδιωτικότητάς τους [167].

Οι Hussain & Jain πρότειναν έναν μηχανισμό που επιτρέπει τον αμοιβαίο έλεγχο ταυτότητας μεταξύ έξυπνων συσκευών. Ο προτεινόμενος μηχανισμός επιτρέπει στις έξυπνες συσκευές να αποκτούν διαπιστευτήρια ασφαλείας από το διακομιστή και να τα χρησιμοποιούν για τον μεταξύ τους έλεγχο ταυτότητας. Οι μελετητές χρησιμοποίησαν τεχνικές κρυπτογράφησης XOR, κατακερματισμού απλής κατεύθυνσης και συμμετρικών κλειδιών. Η ανάλυση ασφάλειας του μηχανισμού έδειξε ότι είναι ασφαλής, ενώ η ανάλυση απόδοσής του απέδειξε ότι το υπολογιστικό, επικοινωνιακό και αποθηκευτικό overhead είναι μικρότερο (της τάξης του 8%) σε σύγκριση με υπάρχοντες μηχανισμούς ασφαλείας [168].

5.4.3 Έλεγχος πρόσβασης

Μια ισχυρή πολιτική ασφάλειας του περιβάλλοντος του ΔτΠ θα πρέπει να καθορίζει ποιος ή τι έχει πρόσβαση σε τι και σε ποιο βαθμό. Αυτό είναι ιδιαίτερα σημαντικό για την πρόσβαση σε πληροφορίες που περιέχονται ή δημιουργούνται από συσκευές παρυφών στο επίπεδο αντίληψης του ΔτΠ. Η επίτευξη αυτού του στόχου πραγματοποιείται μέσω τεχνικών ελέγχου πρόσβασης. Τα τελευταία χρόνια, στη βιβλιογραφία έχει παρουσιαστεί ένας μεγάλος αριθμός ελαφρών μηχανισμών ασφαλείας πάνω στην αποτελεσματική προστασία απέναντι στην μη νόμιμη πρόσβαση σε πληροφορίες του ΔτΠ, λαμβάνοντας υπόψη τους εγγενείς περιορισμούς που επιβάλλονται από τις συσκευές παρυφών [169].

Μερικές λύσεις ασφαλείας που βασίζονται στον έλεγχο ταυτότητας και στον έλεγχο πρόσβασης παρουσιάστηκαν σε προηγούμενη ενότητα του κεφαλαίου. Στην παρούσα υποενότητα παρουσιάζονται μερικές ακόμα λύσεις που βασίζονται κυρίως στον έλεγχο πρόσβασης. Οι Fotiou και συν. πρότειναν μια ελαφριά λύση με στόχο την αντιμετώπιση του προβλήματος ελέγχου πρόσβασης στο περιβάλλον ΔτΠ. Σε αυτό το σχήμα, οι σύνθετες

αποφάσεις ελέγχου πρόσβασης ανατίθενται σε αξιόπιστα τρίτα μέρη, τα οποία επιβάλλουν ελάχιστο overhead στις συσκευές με περιορισμένους πόρους. Τα αποτελέσματα ανάλυσης του σχήματος απέδειξαν ότι η λύση παρέχει ασφάλεια και ενισχύει την προστασία της ιδιωτικότητας των τελικών χρηστών [170].

Οι Taylor και συν. πρότειναν μια πολυεπίπεδη μέθοδο ελέγχου πρόσβασης των χρηστών σε συσκευές που χαρακτηρίζονται από περιορισμό πόρων και λειτουργούν σε δίκτυο ΔτΠ. Η προτεινόμενη προσέγγιση ενσωματώνει κοινώς διαθέσιμες τεχνολογίες και τεχνικές όπως φυσική εγγύτητα συσκευών, γεωγραφική θέση και κρυπτογράφηση, κάτι που την κάνει εξαιρετικά ανέξοδη ως προς την υλοποίηση και εφαρμογή. Αποτελείται από πέντε ξεχωριστά επίπεδα: αναγνώρισης, μετάδοσης, επαλήθευσης, επικύρωσης και αναφοράς. Η συγκεκριμένη μελέτη δεν ασχολείται καθόλου με τον έλεγχο πρόσβασης μεταξύ συσκευών [171].

Οι Beltran και συν. παρουσίασαν το SMARTIE, μια χρηστο-κεντρική πλατφόρμα με ενσωματωμένο έλεγχο πρόσβασης για αποτελεσματική ασφάλεια σε έξυπνες πόλεις. Οι συγγραφείς ισχυρίστηκαν ότι η πλατφόρμα τους μπορεί να διασφαλίσει την ασφάλεια, τον έλεγχο πρόσβασης και το απόρρητο των χρηστών όσον αφορά την πρόσβαση σε ευαίσθητες πληροφορίες [172].

5.4.4 Μέθοδος κρυπτογράφησης ECC

Η ελαφριά φύση των συσκευών ΔτΠ απαιτεί συχνά διαφορετικές προσεγγίσεις ασφάλειας από τις υπάρχουσες παραδοσιακές τεχνικές, κάτι που παρακινεί τους ερευνητές να ενισχύσουν την ασφάλεια του περιβάλλοντος του ΔτΠ με διαφορετικά πρωτόγονα όπως η μέθοδος ECC. Η μέθοδος ECC είναι ένας τύπος κρυπτογράφησης δημόσιου κλειδιού που βασίζεται στο χειρισμό σημείων σε ελλειπτικές καμπύλες καθώς και στη θεωρία αριθμών. Σήμερα, η μέθοδος ECC χρησιμοποιείται σταθερά ως τεχνική κρυπτογράφησης δημόσιου κλειδιού για την επίτευξη στόχων ασφαλείας, όπως η εμπιστευτικότητα, η ακεραιότητα, η μη απόρριψη και η διαθεσιμότητα. Τα κύρια πλεονεκτήματα της μεθόδου ECC έναντι παλαιότερων τεχνικών κρυπτογράφησης, όπως το RSA, αφορούν το μικρότερο μέγεθος κλειδιού και την ταχύτητα. Με το μειωμένο μέγεθος κλειδιού, οι αλγόριθμοι που βασίζονται στην ECC μπορούν να παρέχουν την ίδια κρυπτογραφική ισχύ με τους ομολόγους τους που βασίζονται στο RSA. Για παράδειγμα, ένα κλειδί ECC 384 bit ισοδυναμεί με ένα κλειδί RSA 7680 bit. Κατά συνέπεια, η ECC αναδύεται ως μία ελκυστική τεχνική κρυπτογράφησης για περιβάλλοντα με περιορισμένους πόρους όπως το έξυπνο σπίτι [173].

Οι Nimmy και συν. πρότειναν ένα πρωτόκολλο ελέγχου ταυτότητας χρηστών πολλαπλών παραγόντων που βασίζεται στην κρυπτογραφία ECC και την κοινή χρήση κλειδιού για έξυπνα οικιακά περιβάλλοντα. Οι μελετητές αξιοποίησαν μεθόδους αναγνώρισης προσώπων για να τα κάνουν ανθεκτικά σε κοινές επιθέσεις. Το προτεινόμενο πρωτόκολλο επιτυγχάνει αμοιβαίο έλεγχο ταυτότητας μεταξύ όλων των συμμετεχόντων οντοτήτων και έτσι διασφαλίζει τη νομιμότητά τους. Επίσης, δημιουργείται ένα κλειδί συνεδρίας για ασφαλή επικοινωνία μεταξύ των χρηστών και των συσκευών. Η ανάλυση στο προτεινόμενο πρωτόκολλο απέδειξε ότι παρέχει σημαντικά καλύτερη ασφάλεια από τα υπάρχοντα σχήματα με λογικό γενικό overhead. Επιπλέον, παρέχει καλύτερη χρηστικότητα μειώνοντας το βάρος απομνημόνευσης κωδικών πρόσβασης από τους χρήστες, επιτρέποντας ακόμα και τη χρήση έξυπνων καρτών [174].

Οι Zahan και συν. πρότειναν τη χρήση της μεθόδου ECC αντί παραδοσιακών τεχνικών κρυπτογράφησης. Η αξιολόγηση του προτεινόμενου συστήματος έγινε μέσω της εφαρμογής του σε μια έξυπνης πόρτας χρησιμοποιώντας το εργαλείο προσομοίωσης Cryptool 2. Οι μελετητές απέδειξαν ότι η μέθοδος ECC αποδίδει καλύτερα από την προσέγγιση που βασίζεται στην τεχνική RSA, παρουσιάζοντας παράλληλα μεγαλύτερη ανθεκτικότητα σε επιθέσεις [175].

Ενσωματώνοντας το θεώρημα CRT (Chinese Remainder Theorem) στην μέθοδο ECC, οι Jiang και συν. δημιούργησαν ένα ελαφρύ πρωτόκολλο συμφωνίας κλειδιού για έξυπνα οικιακά

συστήματα. Αρχικά, χρησιμοποιήθηκε έλεγχος ταυτότητας κατακερματισμού απλής κατεύθυνσης για τον εντοπισμό των κόμβων αισθητήρα αντί για αμοιβαίο έλεγχο ταυτότητας με σκοπό της μείωσης του overhead ελέγχου ταυτότητας. Στη συνέχεια, το θεώρημα CRT εισήχθη για να ενισχύσει την ασφάλεια της μεθόδου ECC. Η ανάλυση ασφάλειας έδειξε ότι το προτεινόμενο πρωτόκολλο μπορεί να επικυρώσει την ακεραιότητα των δεδομένων και να αντιμετωπίσει επιθέσεις, όπως επανάληψης, Man-In-The-Middle, κ.α. Η ανάλυση απόδοσης και τα πειράματα έδειξαν ότι το πρωτόκολλο επιτυγχάνει υψηλή ασφάλεια με χαμηλό overhead επικοινωνίας και υπολογισμού και μπορεί να εφαρμοστεί σε έξυπνα οικιακά συστήματα [176].

5.4.5 Άλλοι προτεινόμενοι μηχανισμοί

Οι ερευνητές εξακολουθούν να μελετούν τις διάφορες πτυχές των ζητημάτων ασφαλείας και προστασίας της ιδιωτικότητας των έξυπνων σπιτιών που λειτουργούν σε περιβάλλον ΔτΠ.

Οι Zhu και συν. πρότειναν ένα αυτόματο πλαίσιο ελέγχου ταυτότητας που βασίζεται στην τεχνολογία του Blockchain για την επίτευξη αυτοδιαχείρισης ταυτότητας από τους ενοίκους ενός έξυπνου σπιτιού. Το προτεινόμενο πλαίσιο μπορεί να εξαγάγει αυτόνομα τις υπογραφές των έξυπνων οικιακών συσκευών και, στη συνέχεια, να δημιουργήσει ταυτότητες με βάση την τεχνολογία του Blockchain για τους ιδιοκτήτες τους. Συσχετίζει επίσης τις υπογραφές των συσκευών με τις ταυτότητες των ενοίκων του σπιτιού ώστε να τις χρησιμοποιήσει ως διαπιστευτήρια ελέγχου ταυτότητας των χρηστών και ως παράμετρο κανονικής συμπεριφοράς των έξυπνων οικιακών συσκευών [177].

Ένα άλλο πλαίσιο που επιτρέπει τη διαχείριση κινδύνου για έξυπνες υποδομές με ανάλυση της συμπεριφοράς ενός συστήματος ανίχνευσης εισβολών παρουσιάστηκε από τους Pacheco και συν. Το έργο τους βασίζεται σε μια μέθοδο ανάλυσης συμπεριφοράς ανωμαλιών που επιτρέπει σε ένα σύστημα ανίχνευσης εισβολών να ανιχνεύει οποιαδήποτε απειλή που μπορεί να θέσει σε κίνδυνο υποδομές που λειτουργούν σε περιβάλλον ΔτΠ. Τα αποτελέσματα της πειραματικής εφαρμογής του πλαισίου έδειξαν ότι μπορεί να χρησιμοποιηθεί για την προστασία έξυπνων υποδομών και των εφαρμογών τους που λειτουργούν σε περιβάλλον ΔτΠ [178].

Με σκοπό την φυσική προστασία των έξυπνων συσκευών ΔτΠ από εισβολείς, οι Nakagawa & Shimojo πρότειναν επίσης έναν μηχανισμό πλατφόρμας πρακτόρων ΔτΠ με διαφανές πλαίσιο υπολογιστικού νέφους για βελτίωση της ασφάλειας του περιβάλλοντος ΔτΠ. Ο μηχανισμός τους βασίζεται σε ένα διαφανές πλαίσιο προγραμματισμού των συσκευών ΔτΠ, το Dripcast, το οποίο διαχωρίζει τις λειτουργίες ΔτΠ από τις συσκευές και τις τρέχει μεμονωμένα σε περιβάλλον νέφους, χωρίς την εξάρτηση από το είδος της επικοινωνίας, τον προγραμματισμό του διακομιστή ή τη θέση της βάσης δεδομένων [179].

Η διαδικασία ελέγχου ταυτότητας των δικτύων Wi-Fi στα σύγχρονα έξυπνα οικιακά περιβάλλοντα περιλαμβάνει κυρίως έλεγχο ταυτότητας κωδικού πρόσβασης ή μέθοδο ελέγχου ταυτότητας ψηφιακού πιστοποιητικού, διαδικασίες που δεν επιτυγχάνουν υψηλό επίπεδο ασφάλειας. Για να βελτιώσουν το επίπεδο αυτό, οι Chen και συν. πρότειναν ένα σύστημα ελέγχου ταυτότητας με γνώση της τοποθεσίας χρησιμοποιώντας έξυπνη σύμβαση. Η μέθοδος υιοθετεί την ιδέα του δευτερεύοντος ελέγχου ταυτότητας και χωρίζεται σε δύο φάσεις: η πρώτη φάση είναι η φάση εγγραφής, η οποία αφορά κυρίως τη συμπλήρωση της διαδικασίας δημιουργίας του δημόσιου και του ιδιωτικού κλειδιού και τη σύνδεση των πληροφοριών της συσκευής με τις πληροφορίες που έχουν κάποια σχέση με αυτή. Η δεύτερη φάση είναι η φάση ελέγχου ταυτότητας, που αφορά την επιβεβαίωση της νομιμότητας των πληροφοριών που αποστέλλονται από τις συσκευές ελέγχοντας αν οι συσκευές αυτές βρίσκονται σε θέση εντός της νόμιμης περιοχής. Η ασφάλεια αυτού του σχήματος ελέγχου ταυτότητας αναλύθηκε όσον αφορά την αντιμετώπιση επιθέσεων στα διαφορετικά στάδια υλοποίησής του. Τα αποτελέσματα της προσομοίωσης έδειξαν ότι το γενικό overhead που εισήγαγε το προτεινόμενο σχήμα ελέγχου ταυτότητας είναι αποδεκτό σε σχέση με την ασφάλεια που παρέχεται από αυτό [180].

ΚΕΦΑΛΑΙΟ 6

Συμπεράσματα – Προτάσεις

Η παρούσας εργασίας μελέτησε την ασφάλεια και τη προστασία της ιδιωτικότητας των οικιακών συσκευών που λειτουργούν σε περιβάλλον ΔτΠ. Η εφαρμογή της τεχνολογίας του ΔτΠ στα σύγχρονα σπίτια και η δημιουργία ενός καινούργιου τομέα, όπως το έξυπνο σπίτι, οδήγησε σε νέες προκλήσεις ασφάλειας. Παρά τα όποια οφέλη που μπορεί να προσφέρει ένα σπίτι που λειτουργεί σε περιβάλλον ΔτΠ στους ενοίκους του, είναι πολύ ευάλωτο σε διαφορετικά είδη απειλών κατά της ασφάλειας και της προστασίας της ιδιωτικότητας. Στην περίπτωση που μια έξυπνη οικιακή συσκευή παραβιαστεί ή ακόμα χειρότερα ολόκληρο το έξυπνο οικιακό δίκτυο προσβληθεί από κακόβουλη επίθεση, τα προσωπικά στοιχεία των ενοίκων αλλά και η ίδια του η ασφάλεια διατρέχουν κίνδυνο. Η ασφάλεια του έξυπνου σπιτιού και των προσωπικών στοιχείων που περιέχει είναι ζωτικής σημασίας για την ασφάλεια και την προστασία των ενοίκων του. Αυτό σημαίνει ότι τα έξυπνα σπίτια που λειτουργούν σε περιβάλλον ΔτΠ θα πρέπει να έχουν πολύ αυστηρές απαιτήσεις ασφάλειας. Επομένως, πρέπει να ληφθούν τα κατάλληλα μέτρα ώστε το έξυπνο σπίτι να καταστεί πιο ασφαλές και κατάλληλο για διαμονή. Αλλά, πριν την επιλογή των κατάλληλων λύσεων, θα πρέπει να είναι γνωστό τι αντιμετωπίζει ένα έξυπνο σπίτι και ποια ακριβώς ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας παρουσιάζει.

Με βάση αυτά τα δεδομένα και ζητούμενα της εργασίας, αρχικά, έγινε μια παρουσίαση των έξυπνων οικιακών συσκευών και της δομής επικοινωνίας τους στο έξυπνο σπίτι. Στη συνέχεια, παρουσιάστηκε μια ανάλυση των θεμάτων ασφάλειας και ιδιωτικότητας τα οποία μπορεί να υπάρξουν καθώς και των κυβερνοεπιθέσεων που μπορεί να δεχθούν. Τέλος, δόθηκαν παραδείγματα επιθέσεων σε έξυπνες οικιακές συσκευές σε περιβάλλον ΔτΠ και έγινε μια αναφορά στους τρόπους αντιμετώπισης και τις λύσεις των θεμάτων ασφαλείας που έχουν παρουσιαστεί στη βιβλιογραφία την τελευταία πενταετία.

Σε ένα έξυπνο σπίτι, τα στοιχεία τα οποία του προσδίδουν το χαρακτηριστικό της "ευφυΐας", είναι οι έξυπνες οικιακές συσκευές. Η δομή του δικτύου μέσα από το οποίο γίνεται η επικοινωνία των συσκευών αυτών αποτελεί ένα ακόμη βασικό χαρακτηριστικό του έξυπνου σπιτιού. Επίσης τα πρωτόκολλα επικοινωνίας και οι υπηρεσίες είναι μέρη του δικτύου που παίζουν καθοριστικό ρόλο στη λειτουργία του έξυπνου σπιτιού. Η κατανόηση επομένως των κενών ασφαλείας που υπάρχουν σε ένα έξυπνο σπίτι, προϋποθέτει την παρουσίαση και σχετική ανάλυση της αρχιτεκτονικής δομής του καθώς και των πρωτοκόλλων επικοινωνίας των έξυπνων συσκευών που το απαρτίζουν. Στην βιβλιογραφία έχουν εμφανιστεί κατά καιρούς διάφορες αρχιτεκτονικές δομές έξυπνων σπιτιών. Για τις ανάγκες της παρούσας εργασίας επιλέχθηκε η αρχιτεκτονική δομή των Ghirardello και συν., οι οποίοι χωρίζουν το οικιακό οικοσύστημα που λειτουργεί σε περιβάλλον ΔτΠ, σε τρία βασικά μέρη: (α) το λειτουργικό τμήμα, (β) το φυσικό τμήμα και (γ) το επικοινωνιακό τμήμα.

Η εφαρμογή μηχανισμών ασφαλείας σε ένα έξυπνο σπίτι που λειτουργεί σε περιβάλλον ΔτΠ, αποτελεί πραγματική πρόκληση. Εξαιτίας της πολύπλοκης φύσης και των διαφορετικών τεχνολογιών που συνθέτουν ένα τέτοιο περιβάλλον, η εφαρμογή κοινών μηχανισμών σε όλες τις συσκευές, είναι κάτι παραπάνω από δύσκολη διαδικασία. Επίσης δύσκολη είναι και η

επεκτασιμότητα, η χρησιμότητα και το επίπεδο προστασίας σε ένα οικιακό δίκτυο, λόγω της διαφορετικής φύσης κάθε συσκευής με τα πρωτόκολλα τα οποία χρησιμοποιεί και τους τρόπους που επικοινωνεί. Λόγω των ευαίσθητων πληροφοριών που μεταδίδονται αλλά και των συσκευών που μπορεί να είναι συνδεδεμένες σε ένα τέτοιο δίκτυο, η εύρεση τρόπου εφαρμογής των κατάλληλων μηχανισμών ασφαλείας, είναι επιτακτικής ανάγκης. Τα βασικά θέματα ασφαλείας έχουν να κάνουν με τη δομή του οικιακού δικτύου, η οποία έχει άμεση σχέση με τις οικιακές συσκευές που είναι συνδεδεμένες στο δίκτυο, τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται και τις υπηρεσίες που χρησιμοποιούνται από τους χρήστες. Με άλλα λόγια, εξαρτώνται ουσιαστικά από τα χαρακτηριστικά του περιβάλλοντος ΔτΠ στο οποίο λειτουργεί το έξυπνο σπίτι. Η κατανόηση αυτών των θεμάτων καθίσταται πιο εύκολη από την ανάλυση της δομής του δικτύου ΔτΠ, μέσα από την οποία είναι εύκολη η εξαγωγή συμπερασμάτων ως προς την ύπαρξη ζητημάτων ασφάλειας και προστασίας της ιδιωτικότητας σε κάθε ένα από τα επίπεδα από τα οποία αποτελείται. Η ακαδημαϊκή και ερευνητική κοινότητα δεν έχει καταφέρει ως τώρα να δώσει μέσα από τη βιβλιογραφία μια κοινά αποδεκτή αρχιτεκτονική δομή για το ΔτΠ. Κατά καιρούς έχουν προταθεί και παρουσιαστεί πολλές και διαφορετικές αρχιτεκτονικές δομές, τριών, τεσσάρων και πέντε επιπέδων. Λόγω των προκλήσεων που αντιμετωπίζει το ΔτΠ σχετικά με την ασφάλεια και την προστασία της ιδιωτικότητας, στο πλαίσιο της παρούσας εργασίας επιλέχθηκε η αρχιτεκτονική των πέντε επιπέδων, συμβαδίζοντας με την άποψη πολλών ερευνητών ότι μόνο αυτή η αρχιτεκτονική δομή μπορεί να πληροί τις απαιτήσεις αυτές.

Η λειτουργία των έξυπνων οικιακών συσκευών σε περιβάλλον ΔτΠ, έχει να παρουσιάσει πολλούς κινδύνους. Η σημασία των δεδομένων που μετακινούνται στο οικιακό δίκτυο, η δομή των δικτύων που χρησιμοποιούνται και οι εφαρμογές που βελτιώνουν την καθημερινότητα των ενοίκων του σπιτιού, αποτελεί πρόκληση για τους κακόβουλους χρήστες. Η ασφάλεια και η προστασία όλων των έξυπνων οικιακών συσκευών είναι πολύ σημαντική για τη ζωή των ατόμων που επικοινωνούν και αλληλεπιδρούν με το περιβάλλον του ΔτΠ. Η πολυπλοκότητα της φύσης του ΔτΠ συνδυάζει πολλές και διαφορετικές προκλήσεις. Οι διαφορετικές έξυπνες οικιακές συσκευές, τα διαφορετικά είδη δικτύων επικοινωνίας, η διαχείριση και αποθήκευση του όγκου των δεδομένων σε συνδυασμό με τη πληθώρα των λογισμικών και εφαρμογών, συνθέτουν ένα δαιδαλώδες περιβάλλον. Η ασφάλεια και η προστασία είναι κύριοι παράγοντες για την ομαλή λειτουργία του συστήματος. Για να μπορεί ένα τέτοιο οικιακό περιβάλλον να είναι αποδοτικό και λειτουργικό θα πρέπει να πληροί τις εξής προϋποθέσεις: εύκολη επεκτασιμότητα, άμεση χρηστικότητα και ικανοποιητική προστασία. Όταν μια από τις παραπάνω απαιτήσεις πάψει να ισχύει, όλη η υποδομή θα παρουσιάσει σοβαρό πρόβλημα. Στο πλαίσιο της παρούσας εργασίας, οι επιθέσεις που έχει να αντιμετωπίσει ένα έξυπνο οικιακό περιβάλλον χωρίστηκαν σε πέντε κατηγορίες, με βάση την αρχιτεκτονική δομή των πέντε επιπέδων του ΔτΠ.

Οι τεχνολογίες του οικιακού αυτοματισμού που λειτουργούν σε περιβάλλον ΔτΠ, επιτρέπουν στους χρήστες να έχουν εξ αποστάσεως διαχείριση, έλεγχο και αλληλεπίδραση με τις έξυπνες οικιακές συσκευές μέσω των κινητών συσκευών τους. Λόγω της προσιτότητας και της άμεσης διαθεσιμότητας στους καταναλωτές, οι έξυπνες οικιακές συσκευές που λειτουργούν σε περιβάλλον ΔτΠ είναι πολύ δημοφιλείς, ξεπερνώντας κατά πολύ όλους τους άλλους τομείς στους οποίους μπορεί να εφαρμοστεί η τεχνολογία του ΔτΠ. Οι περισσότερες από αυτές τις συσκευές δεν χρησιμοποιούνται μόνο στο περιβάλλον του έξυπνου σπιτιού, αλλά μπορούν να εγκατασταθούν και σε κρίσιμες υποδομές, όπως εργοστάσια, νοσοκομεία, στρατιωτικές εγκαταστάσεις, κυβερνητικούς οργανισμούς, κ.α. Σε πολλές περιπτώσεις μάλιστα, πολλές από αυτές τις συσκευές αλληλοεπιδρούν άμεσα ή έμμεσα με εξοπλισμό τέτοιων υποδομών, όπως για παράδειγμα οι έξυπνοι μετρητές που επικοινωνούν με το έξυπνο δίκτυο παροχής ηλεκτρικής ενέργειας (smart grid). Μια τέτοια αλληλοεπίδραση έχει ως αποτέλεσμα, επιθέσεις που στοχεύουν την ασφάλεια των έξυπνων οικιακών δικτύων να μπορούν να επηρεάσουν και την ασφάλεια άλλων κρίσιμων υποδομών. Στην παρούσα εργασία

έγινε μια αναφορά πραγματικών κυβερνοεπιθέσεων που είχαν στόχο την υποδομή έξυπνων σπιτιών και την εκμετάλλευση των κενών ασφαλείας τους. Η αναφορά αυτή περιέλαβε επαληθευμένες επιθέσεις, δηλαδή πραγματικά περιστατικά ή επιθέσεις που έχουν εφαρμοστεί και δημοσιευτεί από μελετητές. Επειδή οι έξυπνες οικιακές συσκευές χρησιμοποιούνται μόνο για υποστήριξη των λειτουργιών ενός έξυπνου σπιτιού και όχι ως μέρος ενός κρίσιμου συστήματος ελέγχου, η ταξινόμηση των επιθέσεων έγινε με βάση τον πραγματικό τους στόχο και όχι με βάση την αρχιτεκτονική του συστήματος.

Τα τελευταία χρόνια, παρατηρείται μια συνεχόμενη αύξηση των μελετών που εμφανίζονται στη βιβλιογραφία όσον αφορά την αντιμετώπιση των θεμάτων ασφάλειας και ιδιωτικότητας σε όλα τα επίπεδα της αρχιτεκτονικής του ΔτΠ., αλλά και σε όλους τους τομείς εφαρμογής του, ανάμεσα στον οποίους συγκαταλέγεται και το έξυπνο σπίτι. Ιδιαίτερα στο πλαίσιο του έξυπνου σπιτιού, έχουν προταθεί πολλές διαφορετικές τεχνικές και λύσεις, με μεγαλύτερη έμφαση την ασφάλεια και την προστασία της ιδιωτικότητας των έξυπνων οικιακών συσκευών με περιορισμένους πόρους. Όπως έχει αναφερθεί σε προηγούμενα κεφάλαια, ένα από τα ζητήματα που κάνουν το ΔτΠ περίπλοκο είναι το γεγονός ότι πολλές συσκευές που λειτουργούν στο περιβάλλον του χρησιμοποιούν πολύ απλά λειτουργικά συστήματα σε επεξεργαστές που έχουν ελάχιστη υπολογιστική χωρητικότητα και μικρή μνήμη, καθιστώντας πιο δύσκολη την εκπλήρωση βασικών απαιτήσεων ασφάλειας και προστασίας της ιδιωτικότητας. Στην παρούσα εργασία, εξετάστηκαν διάφορες προτάσεις και λύσεις για την αντιμετώπιση αυτών των θεμάτων. Η ανάλυση των προτεινόμενων λύσεων εστιάστηκε σε τέσσερεις διαφορετικές πτυχές, όπως είναι τα κρυπτογραφικά πρωτόγονα, τα πρωτόκολλα ελέγχου ταυτότητας, το hardware υλικό και οι σύγχρονοι μηχανισμοί ασφαλείας. Στην συγκεκριμένη ανάλυση παρουσιάστηκαν σχετικές εργασίες της βιβλιογραφίας της τελευταίας πενταετίας με θέμα την ασφάλεια και την προστασία της ιδιωτικότητας στα έξυπνα σπίτια που λειτουργούν σε περιβάλλον ΔτΠ.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΠΗΓΕΣ

[1] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

[2] Zhong, Y. (2015). I2oT: Advanced Direction of the Internet of Things. ZTE Communications, 13(2), 3-6.

[3] Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017, May). Security and privacy issues for an IoT based smart home. In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1292-1297). IEEE.

[4] Miller, M. (2015). The internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world. Pearson Education.

[5] Iqbal, M. A., Olaleye, O. G., & Bayoumi, M. A. (2017). A review on internet of things (IoT): security and privacy requirements and the solution approaches. Global Journal of Computer Science and Technology.

[6] Ul Rehman, S., & Manickam, S. (2016). A study of smart home environment and its security threats. International Journal of Reliability, Quality and Safety Engineering, 23(03), 1640005.

[7] Saad al-sumaiti, A., Ahmed, M. H., & Salama, M. M. (2014). Smart home activities: A literature review. Electric Power Components and Systems, 42(3-4), 294-305.

[8] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.

[9] Pratiksha, D. N., Jayashree, G. G., Pornima, U. K., & Amol, G. B. (2014). Design and Implementation of Cloud based Home Automation. International Journal of Engineering Research & Technology (IJERT), 3(2), 2059-2062.

[10] Suryadevara, N. K., & Mukhopadhyay, S. C. (2015). Smart Homes. Berlin, Germany :: Springer.

[11] IoTech (2020, May). Internet of Things Statistics. https://www.the-iot.co.uk/news/internet-of-things-statistics/ (Προσπελάστηκε στις 12 ΟΚΤ 2020).

[12] Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. sensors, 18(3), 817.

[13] Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). Cyber security of smart homes: Development of a reference architecture for attack surface analysis.

[14] Batalla, J. M., Vasilakos, A., & Gajewski, M. (2017). Secure smart homes: Opportunities and challenges. ACM Computing Surveys (CSUR), 50(5), 1-32.

[15] Kavallieratos, G., Chowdhury, N., Katsikas, S., Gkioulos, V., & Wolthusen, S. (2019). Threat Analysis for Smart Homes. Future Internet, 11(10), 207.

[16] Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative, 1(1), 1-86.

[17] Hassan, Q. F., & Madani, S. A. (2017). Internet of things: Challenges, advances, and applications. Chapman and Hall/CRC.

[18] Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1, 81-98.

[19] Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. Future Generation Computer Systems, 91, 563-573.

[20] Domb, M. (2019). Smart home systems based on internet of things. In Internet of Things (IoT) for Automated and Smart Applications. IntechOpen.

[21] Lin, S. W., Miller, B., Durand, J., Bleakley, G., Chigani, A., Martin, R., ... & Crawford, M. (2017). The industrial internet of things volume G1: reference architecture. Industrial Internet Consortium, 10-46.

[22] Perumal, T., Datta, S. K., & Bonnet, C. (2015, October). IoT device management framework for smart home scenarios. In 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE) (pp. 54-55). IEEE.

[23] Brambilla, M., Umuhoza, E., & Acerbis, R. (2017). Model-driven development of user interfaces for IoT systems via domain-specific components and patterns. Journal of Internet Services and Applications, 8(1), 14.

[24] Kim, M. J., Cho, M. E., & Jun, H. J. (2020). Developing Design Solutions for Smart Homes Through User-Centered Scenarios. Frontiers in Psychology, 11, 335.

[25] Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., & Baccelli, E. (2019). Secure firmware updates for constrained IoT devices using open standards: A reality check. IEEE Access, 7, 71907-71920.

[26] McGrath, M. J., & Scanaill, C. N. (2013). Key sensor technology components: hardware and software overview. In Sensor Technologies (pp. 51-77). Apress, Berkeley, CA.

[27] Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2017). A survey on the edge computing for the Internet of Things. IEEE access, 6, 6900-6919.

[28] Ali, N. (2019). Memory Options for the IoT. Synopsys, Inc. https://www.synopsys.com/designware-ip/technical-bulletin/memory-options.html (Προσπελάστηκε στις 22 ΟΚΤ 2020).

[29] Ünlü, F., Wawrla, L., & Dìaz, A. (2018). Energy harvesting technologies for IoT edge devices. 4E, Int. Energy Agency, Paris, France.

[30] Weber, J. (2017). Fundamentals of IoT device management. Avnet. http://iotdesign.embedded-computing.com/articles/fundamentals-of-iot-device-management (Προσπελάστηκε στις 22 ΟΚΤ 2020).

[31] Ali, B. (2016). Internet of Things Based Smart Homes: Security Risk Assessment and Recommendations. Master of Science in Information Security. Luleå University of Technology. Department of Computer Science, Electrical and Space Engineering.

[32] Samuel, S. S. I. (2016, March). A review of connectivity challenges in IoT-smart home. In 2016 3rd MEC International conference on big data and smart city (ICBDSC) (pp. 1-4). IEEE.

[33] Tsiatsis, V., Karnouskos, S., Holler, J., Boyle, D., & Mulligan, C. (2018). Internet of Things: technologies and applications for a new age of intelligence. Academic Press.

[34] El Khaddar, M. A., & Boulmalf, M. (2017). Smartphone: the ultimate IoT and IoE device. Smartphones from an applied research perspective, 137.

[35] Huo, Y. (2017). Efficient access control for power line communication networks (Doctoral dissertation, University of British Columbia).

[36] Essays, UK. (November 2018). Wireless Network Advantages and Disadvantages. https://www.ukessays.com/essays/information-technology/wireless-network.php?vref=1 (Προσπελάστηκε στις 23 ΟΚΤ 2020).

[37] Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2015, November). Review of communication technologies for smart homes/building applications. In 2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA) (pp. 1-6). IEEE.

[38] Saito, N., & Menga, D. (Eds.). (2015). Ecological Design of Smart Home Networks: Technologies, Social Impact and Sustainability. Elsevier.

[39] Hackman, M. (2019, March). The new USB4 spec promises a lot: Thunderbolt 3 support, 40Gbps bandwidth, and less confusion. PCWorld. https://www.pcworld.com/article/3347403/the-new-usb4-spec-promises-a-lot-thunderbolt-3-support-40gbps-bandwidth-and-less-confusion.html (Προσπελάστηκε στις 23 ΟΚΤ 2020).

[40] Sato, T., Kammen, D. M., Duan, B., Macuha, M., Zhou, Z., Wu, J., ... & Asfaw, S. A. (2015). Smart grid standards: specifications, requirements, and technologies. John Wiley & Sons.

[41] Gunawan, T. S., Yaldi, I. R. H., Kartiwi, M., Ismail, N., Za'bah, N. F., Mansor, H., & Nordin, A. N. (2017). Prototype design of smart home system using internet of things. Indonesian Journal of Electrical Engineering and Computer Science, 7(1), 107-115.

[42] Bekauri, S. (2016). Energy Management in Smart Home. Thesis. VŠB - Technical University of Ostrava, Faculty of Electrical Engineering and Computer Science Department of Cybernetics and Biomedical Engineering.

[43] Pahlavan, K., & Krishnamurthy, P. (2009). Networking fundamentals: Wide, local and personal area communications. John Wiley & Sons.

[44] Islam, M., & Jin, S. (2019). An Overview Research on Wireless Communication Network. Networks, 5(1), 19-28.

[45] Buthelezi, B. E., Mathonsi, T. E., Maswikaneng, S., & Mphahlele, M. (2017). Routing Schemes for ZigBee Low-Rate Power Personal Area Network: A Survey. In 11th International Conference on Data Mining, Computers, Communication and Industrial Applications (DMCCIA-2017).

[46] Yassein, M. B., Mardini, W., & Khalil, A. (2016, September). Smart homes automation using Z-wave protocol. In 2016 International Conference on Engineering & MIS (ICEMIS) (pp. 1-6). IEEE.

[47] Pham, V. C., Lim, Y., Sgorbissa, A., & Tan, Y. (2019). An ontology-driven echonet lite adaptation layer for smart homes. Journal of Information Processing, 27, 360-368.

[48] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 24(3), 10-16.

[49] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. Sensors, 18(9), 2796.

[50] Yarali, A., Srinath, M., & Joyce, R. G. (2018). A Study of Various Network Security Challenges in the Internet of Things (IoT).

[51] Alshohoumi, F., Sarrab, M., AlHamadani, A., & Al-Abri, D. (2019). Systematic review of existing iot architectures security and privacy issues and concerns. Int. J. Adv. Comput. Sci. Appl, 10(7), 232-251.

[52] Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018, June). IoT standardisation: Challenges, perspectives and solution. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (pp. 1-9).

[53] Mohammed, A. F., & Qyser, A. A. M. (2020, February). A Survey on Security Mechanisms in IoT. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-11). IEEE.

[54] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

[55] Rosner, G., & Kenneally, E. (2018, June). Privacy and the Internet of Things: Emerging frameworks for policy and design. UC Berkeley Center for Long-Term Cybersecurity/Internet of Things Privacy Forum.

[56] Rambus.com. Smart Home: Threats and Countermeasures. https://www.rambus.com/iot/smart-home/ (Προσπελάστηκε στις 26 ΟΚΤ 2020).

[57] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20(4), 3453-3495.

[58] Srinidhi, N. N., Kumar, S. D., & Venugopal, K. R. (2019). Network optimizations in the Internet of Things: A review. Engineering Science and Technology, an International Journal, 22(1), 1-21.

[59] Teschler, L. (2020, April). Breaking BLE — Vulnerabilities in pairing protocols leave Bluetooth devices open for attack. Microcontroller Tips. https://www.microcontrollertips.com/breaking-ble-vulnerabilities-in-bluetooth-pairing-provide-openings-for-attack-faq/ (Προσπελάστηκε στις 27 ΟΚΤ 2020).

[60] Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 7(3), 28.

[61] Cyware Social. (2019, October). Different Bluetooth Hacking Techniques That You Should Know To Prevent Loss Of Data. https://cyware.com/news/different-bluetooth-hacking-techniques-that-you-should-know-to-prevent-loss-of-data-56212c8a (Προσπελάστηκε στις 27 ΟΚΤ 2020).

[62] Vanhoef, M., & Piessens, F. (2017, October). Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1313-1328).

[63] Grabovica, M., Popić, S., Pezer, D., & Knežević, V. (2016, June). Provided security measures of enabling technologies in Internet of Things (IoT): A survey. In 2016 Zooming Innovation in Consumer Electronics International Conference (ZINC) (pp. 28-31). IEEE.

[64] Khanji, S., Iqbal, F., & Hung, P. (2019, June). ZigBee Security Vulnerabilities: Exploration and Evaluating. In 2019 10th International Conference on Information and Communication Systems (ICICS) (pp. 52-57). IEEE.

[65] Kudelski Security Research. (2017, November). ZIGBEE SECURITY: BASICS (PART 3). https://research.kudelskisecurity.com/2017/11/21/zigbee-security-basics-part-3/ (Προσπελάστηκε στις 28 ΟΚΤ 2020).

[66] Tierney, A. (2018, May). Z-Shave. Exploiting Z-Wave downgrade attacks. Pen Test Partners LLP. https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/ (Προσπελάστηκε στις 28 ΟΚΤ 2020).

[67] Gloukhovtsev, M. (2018). Iot Security: Challenges, Solutions & Future Prospects. Dell Inc.

[68] Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. Journal of Hardware and Systems Security, 2(2), 97-110.

[69] Alqassem, I., & Svetinovic, D. (2014, December). A taxonomy of security and privacy requirements for the Internet of Things (IoT). In 2014 IEEE International Conference on Industrial Engineering and Engineering Management (pp. 1244-1248). IEEE.

[70] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.

[71] Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-20.

[72] Wu, T. Y., Chen, C. M., Sun, X., Liu, S., & Lin, J. C. W. (2017). A countermeasure to SQL injection attack for cloud environment. Wireless Personal Communications, 96(4), 5279-5293.

[73] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.

[74] Saha, S., & Soumitra, S. (2019). Secured Integration of IoT and Cloud Computing (Doctoral dissertation). Department of Computer Science and Engineering presented in partial fulfillment of the requirements for the Degree of Bachelor of Science in Computer Science and Engineering. United International University, Dhaka, Bangladesh.

[75] Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309.

[76] Swamy, S. N., Jadhav, D., & Kulkarni, N. (2017, February). Security threats in the application layer in IOT applications. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 477-480). IEEE.

[77] Hilt, S., Huq, N, Rösler, M. and Urano, A. (2017). Cybersecurity Risks in Complex IoT Environments: Threats to Smart Homes, Buildings and Other Structures. Trend Micro Research.

[78] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[79] Yan, Y. (2019). Side channel attacks on IoT applications (Doctoral dissertation, University of Bristol).

[80] Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

[81] Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE Symposium on Computers and Communication (ISCC) (pp. 180-187). IEEE.

[82] El-hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) Authentication schemes. Sensors, 19(5), 1141.

[83] Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2018). How can heterogeneous Internet of Things build our future: A survey. IEEE Communications Surveys & Tutorials, 20(3), 2011-2027.

[84] Prabhakar, S. (2017). Network security in digitalization: Attacks and defence. Int. J. Res. Comput. Appl. Robot, 5(5), 46-52.

[85] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

[86] Varadharajan, V., Tupakula, U., & Karmakar, K. (2018). Study of Security Attacks against IoT Infrastructures. Technical Report TR1: ISIF ASIA Funded Project. Advanced Cyber Security Engineering Research Centre (ACSRC). Faculty of Engineering and Built Environment, The University of Newcastle.

[87] Tabassum, A., & Lebda, W. (2019). Security Framework for IoT Devices against Cyber-attacks. arXiv preprint arXiv:1912.01712.

[88] Chinanu, U. E., Oche, O. E., & Okah-Edemoh, J. O. (2018). Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures. Scientific Review, 4(10), 80-89.

[89] Mishra, A. K., Tripathy, A. K., Puthal, D., & Yang, L. T. (2018). Analytical model for sybil attack phases in internet of things. IEEE Internet of Things Journal, 6(1), 379-387.

[90] Ahmed, A. W., Ahmed, M. M., Khan, O. A., & Shah, M. A. (2017). A comprehensive analysis on the security threats and their countermeasures of IoT. International Journal of Advanced Computer Science and Applications, 8(7), 489-501.

[91] Salim, M. M., Rathore, S., & Park, J. H. (2019). Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing, 1-44.

[92] Bhardwaj, M. (2017, September). IoT device security: A comprehensive look, from edge to cloud. IoT World Today. https://www.iotworldtoday.com/2017/09/23/iot-device-security-comprehensive-look-edge-cloud/ (Προσπελάστηκε στις 01 ΝΟΕ 2020).

[93] Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. Journal of Network and Computer Applications, 49, 112-127.

[94] Gandotra, E., Bansal, D., & Sofat, S. (2014). Malware analysis and classification: A survey. Journal of Information Security, 2014.

[95] Canzanese, R., Kam, M., & Mancoridis, S. (2013, September). Toward an automatic, online behavioral malware classification system. In 2013 IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems (pp. 111-120). IEEE.

[96] D'Mello, O., Gelin, M., Khelil, F. B., Surek, R. E., & Chi, H. (2018, July). Wearable IoT Security and Privacy: A Review from Technology and Policy Perspective. In International Conference on Future Network Systems and Security (pp. 162-177). Springer, Cham.

[97] Gan, D., & Heartfield, R. (2016). Social engineering in the internet of everything. Cutter IT Journal, 29(7), 20-29.

[98] Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of System Assurance Engineering and Management, 8(1), 512-530.

[99] Mullen, G., & Meany, L. (2019, June). Assessment of Buffer Overflow Based Attacks On an IoT Operating System. In 2019 Global IoT Summit (GIoTS) (pp. 1-6). IEEE.

[100] Sharma, V., Lee, K., Kwon, S., Kim, J., Park, H., Yim, K., & Lee, S. Y. (2017). A consensus framework for reliability and mitigation of zero-day attacks in IoT. Security and Communication Networks, 2017.

[101] Jha, R. K., Kour, R. S. H., & Kumar, M. (2020). Layer Based Security in Narrow Band Internet of Things (NB-IoT). Computer Networks, 107592.

[102] Barcena, M. B., & Wueest, C. (2015). Insecurity in the Internet of Things. Security response, symantec, 20.

[103] Lomas, N. (2015, August). Critical flaw identified in zigbee smart home devices. TechCrunch. https://techcrunch.com/2015/08/07/critical-flaw-ided-in-zigbee-smart-home-devices/ (Προσπελάστηκε στις 04 ΝΟΕ 2020).

[104] Badenhop, C. W., Graham, S. R., Ramsey, B. W., Mullins, B. E., & Mailloux, L. O. (2017). The Z-Wave routing protocol and its security implications. Computers & Security, 68, 112-129.

[105] Vanhoef, M., & Piessens, F. (2017, October). Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1313-1328).

[106] Goodin, D. (2017, August). Leak of >1,700 valid passwords could make the IoT mess much worse. Ars Technica. https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/ (Προσπελάστηκε στις 04 NOE 2020).

[107] Boddy, S., & Shattuck, J. (2017, December). The hunt for IoT: The rise of thinkbots. F5 Labs Technical Report. https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot-the-rise-of-thingbots (Προσπελάστηκε στις 04 NOE 2020).

[108] Vigliarolo, B. (2020, February). Report: Smart bulbs have a major security problem. Check Point Software Technologies LTD. https://www.techrepublic.com/article/report-smart-bulbs-have-a-major-security-problem/ (Προσπελάστηκε στις 04 NOE 2020).

[109] Ronen, E., Shamir, A., Weingarten, A. O., & O'Flynn, C. (2017, May). IoT goes nuclear: Creating a ZigBee chain reaction. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 195-212). IEEE.

[110] Somé, D. F. (2018). Web applications security and privacy. Doctoral dissertation. Université Côte d'Azur. Inria.

[111] Hernandez, G., Arias, O., Buentello, D., & Jin, Y. (2014). Smart nest thermostat: A smart spy in your home. Black Hat USA, (2015).

[112] Assange, J. (2017). Vault 7: CIA hacking tools revealed. WikiLeaks.(Mar. 2017). Retrieved Mar, 7, 2017.

[113] Ronen, E., & Shamir, A. (2016, March). Extended functionality attacks on IoT devices: The case of smart lights. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 3-12). IEEE.

[114] Copos, B., Levitt, K., Bishop, M., & Rowe, J. (2016, May). Is anybody home? Inferring activity from smart home network traffic. In 2016 IEEE Security and Privacy Workshops (SPW) (pp. 245-251). IEEE.

[115] Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. arXiv preprint arXiv:1708.05044.

[116] Paganini, P. (2014). Proofpoint Discovered More Than 750,000 Phishing and SPAM Emails Launched from 'Thingbots' Including Televisions, Fridge. Security Affairs. January, 19.

[117] Tenaglia, S., & Tanen, J. (2016, November). Breaking BHAD: Abusing Belkin home automation devices. In Proc. Black Hat Europe (pp. 1-46).

[118] Nixon, A., Costello, J., & Wilkholm, Z. (2016). An after-action analysis of the mirai botnet attacks on dyn.

[119] Sapalo Sicato, J. C., Sharma, P. K., Loia, V., & Park, J. H. (2019). VPNFilter malware analysis on cyber threat in smart home Network. Applied Sciences, 9(13), 2763.

[120] Ronen, E., Shamir, A., Weingarten, A. O., & O'Flynn, C. (2017, May). IoT goes nuclear: Creating a ZigBee chain reaction. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 195-212). IEEE.

[121] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.

[122] Candid, W. (2015). How my TV got infected with ransomware and what you can learn from it. Broadcom. https://www.symantec.com/connect/blogs/how-my-tv-gotinfected-ransomware-and-what-you-can-learn-it (Προσπελάστηκε στις 08 NOE 2020).

[123] Duan, E., Zhang, V., & Ye, K. (2016, June). FLocker Mobile Ransomware Crosses to Smart TV. Trend Micro. https://www.trendmicro.com/en_us/research/16/f/flocker-ransomware-crosses-smart-tv.html (Προσπελάστηκε στις 08 NOE 2020).

[124] Claverie, T., Esteves, J. L., & Kasmi, C. (2018). Smart TVs: Security of DVB-T.

[125] Morgner, P., Mattejat, S., & Benenson, Z. (2016). All your bulbs are belong to us: Investigating the current state of security in connected lighting systems. arXiv preprint arXiv:1608.03732.

[126] SISODIA, D. (2020). On the State of Internet of Things Security: Vulnerabilities, Attacks, and Recent Countermeasures. University of Oregon, Tech. Rep.

[127] Vrooman, R. (2017). Enhancing Privacy in Smart Home Ecosystems Using Cryptographic Primitives and a Decentralized Cloud Entity. Master of Science. Delft University of Technology.

[128] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 1-18.

[129] Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16(4), 1933-1954.

[130] Papanikolaou, A., Rantos, K., & Androulidakis, I. (2014, July). Proxied ibe-based key establishment for llns. In The 10th International Conference on Digital Technologies 2014 (pp. 275-280). IEEE.

[131] Saied, Y. B., Olivereau, A., Zeghlache, D., & Laurent, M. (2014). Lightweight collaborative key establishment scheme for the Internet of Things. Computer Networks, 64, 273-295.

[132] Kumar, P., Gurtov, A., Iinatti, J., Ylianttila, M., & Sain, M. (2015). Lightweight and secure session-key establishment scheme in smart home environments. IEEE Sensors Journal, 16(1), 254-264.

[133] Kumar, P., Braeken, A., Gurtov, A., Iinatti, J., & Ha, P. H. (2017). Anonymous secure framework in connected smart home environments. IEEE Transactions on Information Forensics and Security, 12(4), 968-979.

[134] Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy preserving communication protocol for IoT applications in smart homes. IEEE Internet of Things Journal, 4(6), 1844-1852.

[135] Wazid, M., Das, A. K., Odelu, V., Kumar, N., & Susilo, W. (2017). Secure remote user authenticated key establishment protocol for smart home environment. IEEE Transactions on Dependable and Secure Computing.

[136] Choi, B. C., Lee, S. H., Na, J. C., & Lee, J. H. (2016). Secure firmware validation and update for consumer devices in home networking. IEEE Transactions on Consumer Electronics, 62(1), 39-44.

[137] Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. arXiv preprint arXiv:1705.06805.

[138] Liu, J., Zhang, C., & Fang, Y. (2018). Epic: A differential privacy framework to defend smart homes against internet traffic analysis. IEEE Internet of Things Journal, 5(2), 1206-1217.

[139] Buchanan, W. J., Li, S., & Asif, R. (2017). Lightweight cryptography methods. Journal of Cyber Security Technology, 1(3-4), 187-201.

[140] Pereira, G. C., Alves, R. C., Silva, F. L. D., Azevedo, R. M., Albertini, B. C., & Margi, C. B. (2017). Performance evaluation of cryptographic algorithms over IoT platforms and operating systems. Security and Communication Networks, 2017.

[141] Pereira, P. P., Eliasson, J., & Delsing, J. (2014, October). An authentication and access control framework for CoAP-based Internet of Things. In IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society (pp. 5293-5299). IEEE.

[142] Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014, September). A robust authentication scheme for observing resources in the internet of things environment. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 205-211). IEEE.

[143] Turkanović, M., Brumen, B., & Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks, 20, 96-112.

[144] Shivraj, V. L., Rajan, M. A., Singh, M., & Balamuralidhar, P. (2015, February). One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW) (pp. 1-6). IEEE.

[145] Hernandez-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F., & Ladid, L. (2015). Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications, 33(4), 690-702.

[146] Yohan, A., Lo, N. W., Randy, V., Chen, S. J., & Hsu, M. Y. (2016, January). A novel authentication protocol for micropayment with wearable devices. In Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication (pp. 1-7).

[147] Park, G., Kim, B., & Jun, M. S. (2016). A design of secure authentication method using zero knowledge proof in smart-home environment. In Advances in Computer Science and Ubiquitous Computing (pp. 215-220). Springer, Singapore.

[148] Risalat, N. A. M., Hasan, M. T., Hossain, M. S., & Rahman, M. M. (2017, February). Advanced real time RFID mutual authentication protocol using dynamically updated secret value through encryption and decryption process. In 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 788-793). IEEE.

[149] Wilson, P. (2017). Inter-device authentication protocol for the internet of things (Doctoral dissertation).

[150] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.

[151] Alshahrani, M., & Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain. Journal of information security and applications, 45, 156-175.

[152] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.

[153] McGrath, T., Bagci, I. E., Wang, Z. M., Roedig, U., & Young, R. J. (2019). A puf taxonomy. Applied Physics Reviews, 6(1), 011303.

[154] Guez, G. (2017). Why Hardware-Based Design Security is Essential for Every Application. White Paper.

[155] Ehret, A., Gettings, K., Jordan, B. R., & Kinsy, M. A. (2019, September). A Survey on Hardware Security Techniques Targeting Low-Power SoC Designs. In 2019 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1-8). IEEE.

[156] Babaei, A., & Schiele, G. (2019). Physical unclonable functions in the Internet of Things: state of the art and open challenges. Sensors, 19(14), 3208.

[157] Xu, T., Wendt, J. B., & Potkonjak, M. (2014, November). Security of IoT systems: Design challenges and opportunities. In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 417-423). IEEE.

[158] Aman, M. N., Chua, K. C., & Sikdar, B. (2016, May). Position paper: Physical unclonable functions for iot security. In Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security (pp. 10-13).

[159] Rose, G. S. (2016, May). Security meets nanoelectronics for Internet of things applications. In 2016 International Great Lakes Symposium on VLSI (GLSVLSI) (pp. 181-183). IEEE.

[160] Yang, K., Blaauw, D., & Sylvester, D. (2017). Hardware designs for security in ultra-low-power IoT systems: An overview and survey. IEEE Micro, 37(6), 72-89.

[161] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.

[162] Sundaram, B. V., Ramnath, M., Prasanth, M., & Sundaram, V. (2015, March). Encryption and hash based security in Internet of Things. In 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) (pp. 1-6). IEEE.

[163] Prudanov, A., Tkachev, S., Golos, N., Masek, P., Hosek, J., Fujdiak, R., ... & Andreev, S. (2016, November). A trial of yoking-proof protocol in RFID-based smart-home environment. In International Conference on Distributed Computer and Communication Networks (pp. 25-34). Springer, Cham.

[164] Oluwade, O.R.; Olaniyi, O.M.; Abdulsalam, Y.S.; Ajao, L.A. (2018). Entropy management technique in lightweight cryptographically secured smart home. In Proceedings of the 12th International Multi-Conference on ICT Applications (AICTTRA, 2018), Ile-Ife, Nigeria, pp. 258–265.

[165] Wagner, L. (2020, January). Why is Exclusive Or (XOR) Important in Cryptography? Qvault.io. https://qvault.io/2020/01/18/why-is-exclusive-or-xor-important-in-cryptography/ (Προσπελάστηκε στις 14 NOE 2020).

[166] Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Generation Computer Systems, 91, 244-251.

[167] Lyu, Q., Zheng, N., Liu, H., Gao, C., Chen, S., & Liu, J. (2019). Remotely access "my" smart home in private: An anti-tracking authentication and key agreement scheme. IEEE Access, 7, 41835-41851.

[168] Hussain, M., & Jain, U. (2020). Simple and secure device authentication mechanism for smart environments using Internet of things devices. International Journal of Communication Systems, 33(16), e4570.

[169] Ravidas, S., Lekidis, A., Paci, F., & Zannone, N. (2019). Access control in Internet-of-Things: A survey. Journal of Network and Computer Applications, 144, 79-101.

[170] Fotiou, N., Kotsonis, T., Marias, G. F., & Polyzos, G. C. (2016, September). Access control for the Internet of Things. In 2016 International Workshop on Secure Internet of Things (SIoT) (pp. 29-38). IEEE.

[171] Taylor, M., Reilly, D., & Lempereur, B. (2017). An access control management protocol for Internet of Things devices. Network Security, 2017(7), 11-17.

[172] Beltran, V., Martinez, J. A., & Skarmeta, A. F. (2017, June). User-centric access control for efficient security in smart cities. In 2017 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.

[173] Shruti, P., & Chandraleka, R. (2017). Elliptic curve cryptography security in the context of internet of things. vol, 8, 90-93.

[174] Nimmy, K., Sankaran, S., & Achuthan, K. (2018, December). A novel multi-factor authentication protocol for smart home environments. In International Conference on Information Systems Security (pp. 44-63). Springer, Cham.

[175] Zahan, A., Hossain, M. S., Rahman, Z., & Shezan, S. K. A. (2020). Smart home IoT use case with elliptic curve based digital signature: an evaluation on security and performance analysis. International Journal of Advanced Technology and Engineering Exploration, 7(62), 11-19.

[176] Jiang, Y., Shen, Y., & Zhu, Q. (2020). A Lightweight Key Agreement Protocol Based on Chinese Remainder Theorem and ECDH for Smart Homes. Sensors, 20(5), 1357.

[177] Zhu, X., Badr, Y., Pacheco, J., & Hariri, S. (2017, September). Autonomic identity framework for the internet of things. In 2017 International Conference on Cloud and Autonomic Computing (ICCAC) (pp. 69-79). IEEE.

[178] Pacheco, J., Zhu, X., Badr, Y., & Hariri, S. (2017, September). Enabling risk management for smart infrastructures with an anomaly behavior analysis intrusion detection system. In 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W) (pp. 324-328). IEEE.

[179] Nakagawa, I., & Shimojo, S. (2017, July). IoT agent platform mechanism with transparent cloud computing framework for improving IoT security. In 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 684-689). IEEE.

[180] Chen, Y., Wang, X., Yang, Y., & Li, H. (2020). Location-Aware Wi-Fi Authentication Scheme Using Smart Contract. Sensors, 20(4), 1062.