
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Διπλωματική Εργασία

# Κυβερνο-επιθέσεις σε Έξυπνα Κτήρια και η Αντιμετώπιση τους: Μια συστηματική βιβλιογραφική επισκόπηση

του

ΤΟΤΟΣΗ ΒΑΣΙΛΕΙΟΥ ΠΑΝΑΓΙΩΤΗ – MIS21037

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού

Διπλώματος Ειδίκευσης στα Πληροφοριακά Συστήματα

Σεπτέμβριος 2022

# *Ευχαριστίες*

*Θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Οικονομίδη για την συνεχή βοήθεια του κατά την εκπόνηση της εργασίας*

*Χωρίς την αμέριστη βοήθεια των γονιών μου και της συζύγου μου, η παρούσα διπλωματική εργασία θα ήταν αδύνατη, σας ευχαριστώ για όλα.*

# *Περιεχόμενα*

## *Abstract*

Στην σύγχρονη εποχή η εγκαθίδρυση έξυπνων τεχνολογιών στην οικία μας ή ακόμη και στο κτήριο στο οποίο κατοικούμε είναι δεδομένη. Από τις πιο απλές τεχνολογίες όπως η εγκατάσταση ενός έξυπνου λαμπτήρα μέχρι και ενός ολοκληρωμένου συστήματος αυτοματοποίησης σημαντικών συστημάτων στο κτήριο, όπως RFID αναγνώστες για την είσοδο, αυτοματοποίηση κλιματισμού και ενεργειακής απόδοσης, διαχείριση ανελκυστήρων, και συστήματα κλειστών κυκλωμάτων, όλα τα προαναφερθέντα είναι ευαίσθητα συστήματα τα οποία δύναται να είναι προσπελάσιμα όταν δεν είναι εγκατεστημένα σωστά ή δεν έγινε ορθή διαμόρφωση με σκοπό να είναι ευάλωτα σε κακόβουλους χρήστες. Οι επιθέσεις και οι τρόποι με τους οποίους γίνεται προσπέλαση των συστημάτων είναι αρκετοί και σχετικά απλοί από έναν έμπειρο κακόβουλο χρήστη, κατηγοριοποιούνται σε επίπεδα, σε πρωτόκολλα συνδεσιμότητας (RFID, Near Field Communication, Bluetooth, Zigbee κ.ο.κ) και σε πρωτόκολλα επικοινωνίας (TCP/IP stack κ.ο.κ). Στην παρούσα εργασία πραγματοποιείται συστηματική βιβλιογραφική επισκόπηση και παρουσιάζονται κοινές επιθέσεις, αναλύονται και εμπλουτίζονται από την υπάρχουσα βιβλιογραφία με σκοπό την καλύτερη κατανόηση τους. Επιπλέον παρουσιάζονται frameworks τα οποία χρησιμοποιούν μοντέλα μηχανικής μάθησης για την αναγνώριση μοτίβων και κατηγοριοποίηση των ανωμαλιών που προκύπτουν. Εντοπίζονται κενά στην βιβλιογραφία και παρουσιάζονται συγκεντρωτικοί πίνακες. Κύριος σκοπός της εργασίας είναι η παρουσίαση ενός γενικού οδηγού αντιμετώπισης επιθέσεων αλλά και μίας ολιστικής προστασίας στα συστήματα των έξυπνων κτιρίων.

# *Εισαγωγή*

Η συγκεκριμένη διπλωματική εργασία εμβαθύνει στις επιθέσεις και σε πιθανούς τρόπους αντιμετώπισης κοινών επιθέσεων στα δίκτυα και τις συσκευές των έξυπνων κτηρίων. Σημαντικά συστήματα όπως συστήματα αυτοματισμών και διαχείρισης ενέργειας αλλά και κλιματισμού είναι τα πιο δημοφιλή ανάμεσα στους κακόβουλους χρήστες διότι η πρόσβαση σε αυτά, ουσιαστικά σημαίνει τον πλήρη έλεγχο και παρακολούθηση του κτηρίου. Στην παρούσα ενότητα θα αναπτυχθούν τα επιμέρους στοιχεία των ενοτήτων.

Στο κεφάλαιο της μεθοδολογίας αναπτύσσεται η τεχνική, οι τρόποι και τα βασικά κριτήρια καταλληλόλητας των μελετών οι οποίες εν τέλη επιλέχθηκαν για την συγκεκριμένη μελέτη. Αναπτύσσεται ο τρόπος αναζήτησης, λέξεις κλειδιά καθώς και ένα flowchart το οποίο προτείνεται από την γνωστή μεθοδολογία PRISMA για τις συστηματικές βιβλιογραφικές επισκοπήσεις. Έπειτα παρουσιάζεται το γενικό διάγραμμα εξαγωγής των δεδομένων και οι ερευνητικές ερωτήσεις στις οποίες η εργασία προσπαθεί να απαντήσει.

Έπειτα παρουσιάζεται η «Σύνθεση Α» πρόκειται για την παρουσίαση των δεδομένων και την κατηγοριοποίηση αυτών. Παρουσιάζονται οι επιθέσεις ανά συγκεκριμένες κατηγορίες connectivity και communication protocols, δίνονται βασικοί ορισμοί, συγκρίνονται και εμπλουτίζονται μεταξύ των επιλεγμένων άρθρων. Τέλος παρουσιάζεται συγκεντρωτικός πίνακας των μελετών σε μία top level προσέγγιση.

Στην «Σύνθεση Β» βρίσκονται τα άρθρα και οι μελέτες σχετικά με την αντιμετώπιση και την πρόληψη επιθέσεων στα έξυπνα κτήρια. Πιο συγκεκριμένα παρουσιάζονται συγκεκριμένα frameworks μηχανικής μάθησης αλλά και τα αποτελέσματα αυτών (ποσοστά ακρίβειας, false positives, κτλ.). Επιπλέον πραγματοποιείται σύγκριση μεταξύ των μελετών και αναγνώριση των ελλείψεων

Στο τελευταίο κεφάλαιο παρουσιάζονται τα συμπεράσματα της συγκεκριμένης εργασίας μαζί με έναν οδηγό αντιμετώπισης επιθέσεων στα έξυπνα κτήρια.

# *1.Μεθοδολογία*

## *1.1. Πρωτόκολλο*

Στην παρούσα συστηματική βιβλιογραφική ανασκόπηση και meta-analysis θα χρησιμοποιηθεί το πρωτόκολλο PRISMA 2020 (Page et. al., 2021). Η συγκεκριμένη μεθοδολογία καθοδηγεί την πολιτική αναζήτησης, τα κριτήρια εισαγωγής μίας δημοσίευσης καθώς, και τα κριτήρια απόρριψης της από την παρούσα ανασκόπηση και την εξαγωγή των δεδομένων από τα ερευνητικά άρθρα.

## *1.2. Κριτήρια καταλληλόλητας*

Τα παρακάτω κριτήρια χρησιμοποιήθηκαν με σκοπό την συλλογή σχετικών ερευνητικών εργασιών και άρθρων

Α. Δημοσιεύσεις στην αγγλική γλώσσα σε επιστημονικά περιοδικά (peer-reviewed) ή διπλωματικές διατριβές ή και πρακτικά συνεδριών.

Β. Έρευνες οι οποίες δημοσιεύτηκαν μετά το 2010

## *1.3. Πηγές δεδομένων*

Για την αναζήτηση των άρθρων και ερευνητικών εργασιών χρησιμοποιήθηκαν οι βάσεις δεδομένων Google Scholar, IEEE Xplore και Springer.

## *1.3. Όροι αναζήτησης και διαδικασία*

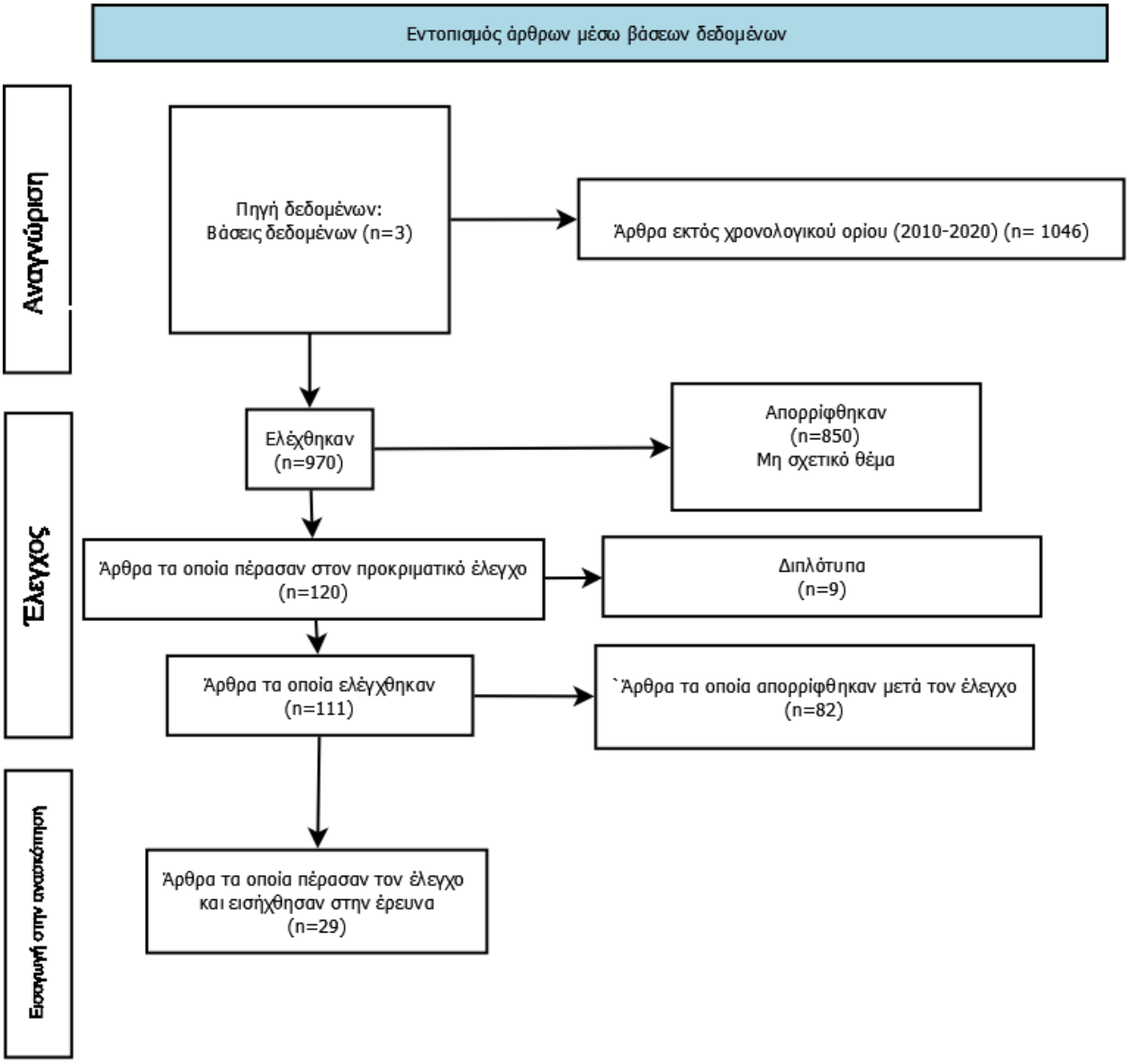
Η διαδικασία αναζήτησης αφορά τις λέξεις κλειδιά οι οποίες χρησιμοποιήθηκαν στις βάσεις δεδομένων με σκοπό την ανάκτηση σχετικών άρθρων. Πιο συγκεκριμένα, η αναζήτηση στη βάση δεδομένων Google Scholar πραγματοποιήθηκε με τις λέξεις κλειδιά “smart buildings” “vulnerabilities”, “attack methods”. Η αναζήτηση πρόσφερε πάνω από 25.000 αποτελέσματα. Στην μηχανή αναζήτησης της IEEE Xplore οι εγγραφές ήταν πιο στοχευμένες και η αναζήτηση

επέστρεψε 100 αποτελέσματα. Τέλος στην μηχανή αναζήτησης της Springer η αναζήτηση επέστρεψε συνολικά 14.206 αποτελέσματα.

Είναι σαφές ότι δεν είναι δυνατό να συμπεριληφθούν όλα τα αποτελέσματα στην παρούσα διπλωματική εργασία. Συνεπώς, ένας προκριματικός έλεγχος συστάθηκε για τον εντοπισμό σχετικών άρθρων. Έπειτα, ελέγχθηκε ο τίτλος του εκάστοτε άρθρου εάν είναι σχετικός με τις φράσεις και τις λέξεις κλειδιά τα οποία αναφέρθηκαν παραπάνω.

Αρχικά από τη μηχανή αναζήτησης Google Scholar έχουν επιλεχθεί συνολικά 75 άρθρα τα οποία έχουν προκριθεί στο στάδιο της προκαταρκτικής εξέτασης. Από την μηχανή αναζήτησης της IEEE επιλέχθηκαν 10 άρθρα. Τέλος, από την μηχανή αναζήτησης της Springer επιλέχθηκαν συνολικά 35 άρθρα. Τα παραπάνω επιλεχθέντα άρθρα έχουν εισέλθει στον προκριματικό έλεγχο όπου θα κριθεί η καταλληλόλητα τους από την αρχική περίληψη.

Σύμφωνα με την μεθοδολογία PRISMA στο συγκεκριμένο στάδιο της παρούσας διπλωματικής εργασίας είναι συνετό να θεσπιστεί το παρακάτω διάγραμμα ροής της έρευνας το οποίο ακολουθεί το πρότυπο του PRISMA (Page et al., 2021)

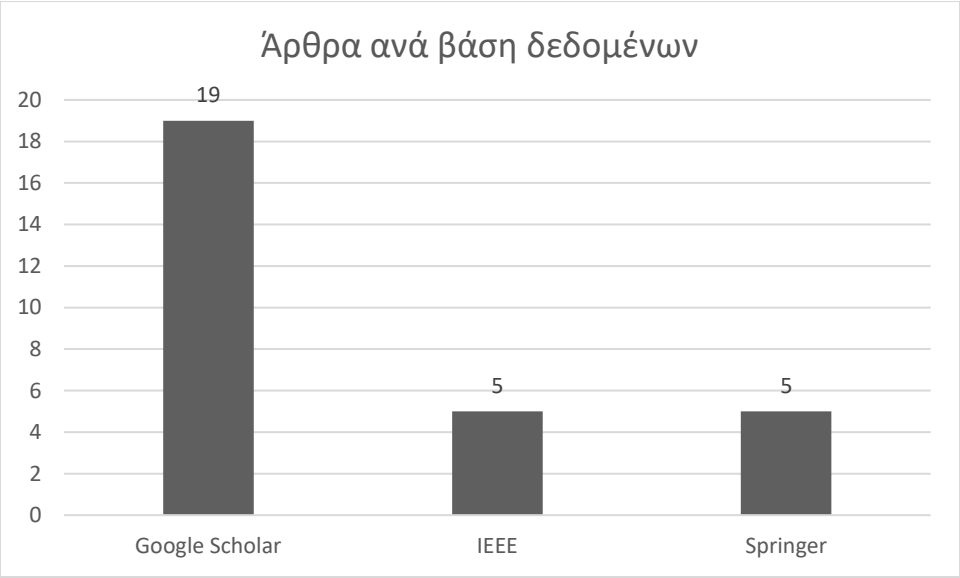



*Διάγραμμα 1- Page, McKenzie, Bossuyt, Boutron, Hoffmann, Mulrow, et al. (2021)*

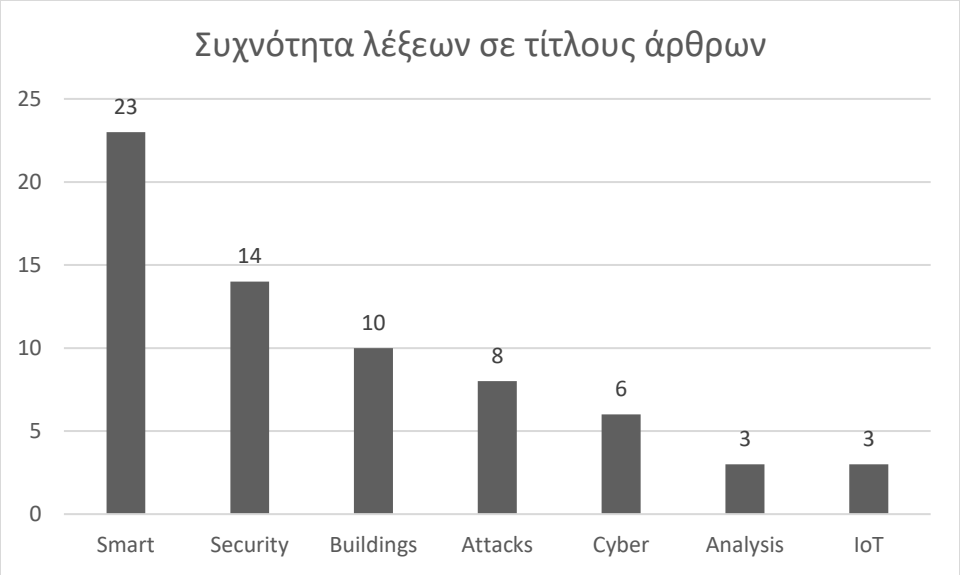
Κατά την διαδικασία εκκαθάρισης των άρθρων και προετοιμάζοντας την ανάγνωση για την καταλληλόλητα των άρθρων προς τους σκοπούς της παρούσας διπλωματικής εργασίας, υπήρξαν συνολικά 9 διπλότυπες εγγραφές οι οποίες απορρίφθηκαν. Παρακάτω βρίσκεται ο πίνακας με τα απορριφθέντα άρθρα.

| Database | Title | Year Published | Type | Link |
|---|---|---|---|---|
| **Google Scholar** | PoisonIvy: (In)secure Practices of Enterprise IoT Systems in Smart Buildings | 2020 | Article | https://dl.acm.org/doi/abs/10.1145/3408308.3427606 |
| **Google Scholar** | Towards 5G-based IoT security analysis against Vo5G eavesdropping | 2021 | Article | https://link.springer.com/article/10.1007/s00607-020-00855-0 |
| **Google Scholar** | On the Automated Management of Security Incidents in Smart Spaces | 2019 | Article | https://ieeexplore.ieee.org/abstract/document/8793072 |
| **Google Scholar** | PoisonIvy: (In)secure Practices of Enterprise IoT Systems in Smart Buildings | 2020 | Article | https://dl.acm.org/doi/abs/10.1145/3408308.3427606 |
| **Google Scholar** | Anomaly Behavior Analysis System for ZigBee in smart buildings | 2022 | Article | https://ieeexplore.ieee.org/abstract/document/7507187?casa_token=u48RnPCOc_EAAAAA:LkfVGS9MyC7nRheuvyK49qmkud7YMdMu7GGBpyVxTo26g3wS7hNYtB4iKUCDX-bXZ2yu-j7Uyw |
| **IEEE Xplore** | On the Automated Management of Security Incidents in Smart Spaces | 2019 | Article | https://ieeexplore.ieee.org/document/8793072 |
| **IEEE Xplore** | Anomaly Behavior Analysis System for ZigBee in smart buildings | 2015 | Article | https://ieeexplore.ieee.org/document/7507187 |
| **Springer** | Towards 5G-based IoT security analysis against Vo5G eavesdropping | 2021 | Article | https://link.springer.com/article/10.1007/s00607-020-00855-0 |

Τα άρθρα τα οποία τελικά εισήχθησαν στην έρευνα και θα πραγματοποιηθεί εξαγωγή δεδομένων από αυτά είναι 29. Οι συγκεκριμένες έρευνες πραγματεύονται ξεκάθαρα τους στόχους της παρούσας διπλωματικής αναφέροντας τρόπους επίθεσης και αντιμετώπισης αυτών σε έξυπνα κτίρια. Παρακάτω παρατίθεται το γράφημα με τον αριθμό των άρθρων ανά βάση δεδομένων. Επιπρόσθετα υπάρχει το γράφημα με τις συχνότερες εμφανίσεις των λέξεων κλειδιών στους τίτλους των άρθρων τα οποία επιλέχθηκαν για περαιτέρω ανάλυση.




*Γράφημα 1 - Αριθμός άρθρων που ανακτήθηκαν ανά βάση δεδομένων*




*Γράφημα 2 - Συχνότητα λέξεων κλειδιών στους τίτλους των άρθρων τα οποία επιλέχθηκαν*

Θεμιτό ως προς την αξιολόγηση των επιλεγμένων άρθρων είναι η παρουσίαση του ερωτηματολογίου το οποίο χρησιμοποιήθηκε. Παρακάτω βρίσκεται ο πίνακας με τις ερωτήσεις που χρησιμοποιήθηκαν.

| **Αρ. Ερ.** | **Ερωτήσεις** |
|---|---|
| **Ερ1** | Προσεγγίζει η θεματική της έρευνας το ερευνητικό ερώτημα; |
| **Ερ2** | Προσφέρει το άρθρο πληροφορίες για τρόπους επιθέσεων και αντιμετώπισης; |
| **Ερ3** | Υπάρχει σαφήνεια στα ευρήματα της έρευνας σε σχέση με τους στόχους; |

Προσεγγίζοντας την αρχή εξαγωγής των δεδομένων είναι θεμιτό να αναφερθούν οι δύο συνθέσεις -ομαδοποιήσεις- που θα χρησιμοποιηθούν για την εξαγωγή των δεδομένων από τα επιλεχθέντα άρθρα. Στην πρώτη σύνθεση βρίσκονται άρθρα τα οποία αναφέρονται σε τρόπους επιθέσεων και ανάλυση αυτών. Στην δεύτερη σύνθεση βρίσκονται άρθρα τα οποία προτείνουν τρόπους αντιμετώπισης κυβερνοεπιθέσεων σε δίκτυα IoT και έξυπνα κτίρια και παρουσιάζουν πρακτικές λύσεις αντιμετώπισης. Στην πλειοψηφία των άρθρων τα δεδομένα δίνονται υπό την μορφή κειμένου, συνεπώς, θα γίνει εξαγωγή δεδομένων με αφηγηματική τεχνική.

*1.5. Διαδικασία συγκέντρωσης δεδομένων από τις έρευνες*

Για την εξαγωγή των δεδομένων από τις επιλεχθέν μελέτες συγκροτήθηκε διπλό πέρασμα ως προς την ανάγνωση και κατανόηση αυτών. Πιο συγκεκριμένα, στο πρώτο πέρασμα ανάγνωσης των ερευνών, εντοπίστηκαν κοινά σημεία και τεχνικές κατηγοριοποίησης επιθέσεων και τεχνικών αντιμετώπισης. Ουσιαστικά έγινε χαρτογράφηση των ερευνών και πραγματοποιήθηκε μία αρχική κατηγοριοποίηση. Η πρώτη κατηγορία αναφέρεται στις επιθέσεις και η δεύτερη σε τεχνικές αντιμετώπισης ή και προτεινόμενες δομές, εργαλεία και ανίχνευση των επιθέσεων. Συνεπώς υπήρξε μία top level προσέγγιση με σκοπό την κατανόηση και κατηγοριοποίηση των μελετών.

Στο δεύτερο πέρασμα, συγκροτήθηκε εξαγωγή δεδομένων με βάση κοινά σημεία των ερευνών. Πρακτικά, πραγματοποιήθηκαν αναφορές για το έκαστο άρθρο, σημειώνοντας όλες τις ομοιότητες και διαφορές στις οποίες συγκλίναν οι μελετητές και διαφέραν. Παρακάτω, στην ανάλυση και επεξήγηση των ευρημάτων υπάρχει ξεκάθαρη περιγραφή για την προαναφερθείσα πρόταση.

| **Πεδίο** | **Περιγραφή** |
|---|---|
| Τίτλος | Δίνεται ο τίτλος και οι πληροφορίες αναφοράς |
| Δημοσίευση | Δίνεται το μέσο δημοσίευσης της έρευνας, διαδικτυακή πηγή, περιοδικό κ.ο.κ |
| Έτος | Χρόνος δημοσίευσης |
| Κύρια ιδέα | Δίνεται με περιληπτικό τρόπο η ιδέα που πραγματεύεται η έρευνα |
| Συνεισφορά | Υπάρχουν συνεισφορές του συγγραφέα στο συγκεκριμένο πεδίο |
| Μεθοδολογία | Λίστα με διαφορετικές μεθοδολογίες αλλά και θεωρητικό υπόβαθρο το οποίο χρησιμοποιήθηκε για να τεκμηριώσει τα αποτελέσματα της έρευνας |
| Αποτελέσματα | Τα συμπεράσματα τα οποία προέκυψαν από την μελέτη |
| Κενά τα οποία προέκυψαν | Υπήρχαν ασυνάφειες; Κενά στο θεωρητικό υπόβαθρο; Περιορισμοί που αναφέρθηκαν |

### *1.6.1. Στοιχεία δεδομένων*

Στην παρούσα ενότητα, θα αναλυθούν οι μέθοδοι οι οποίοι χρησιμοποιήθηκαν για να αποφασιστεί με ποιον τρόπο ακριβώς θα συμπεριληφθούν δεδομένα στην παρούσα μελέτη. Στην παρούσα φάση της διπλωματικής συστάθηκαν μέθοδοί για την εισαγωγή ή μη δεδομένων από τις έρευνες οι οποίες εισήχθησαν. Γενικότερα τα δεδομένα τα οποία αφορούσαν στην ξεκάθαρη περιγραφή επιθέσεων σε έξυπνα κτίρια και η περιγραφή αυτών, ανάλυση των τεχνικών και τρόπων εκκίνησης, αλλά και των καταστροφικών αποτελεσμάτων έχουν ανακτηθεί για να παρουσιαστούν στην παρούσα μελέτη. Όσον αφορά τις πρακτικές αντιμετώπισης παρόμοια συλλογιστική ακολουθήθηκε. Πιο συγκεκριμένα, τα επιμέρους μέρη των πρακτικών αντιμετώπισης, τους τρόπους ανίχνευσης από τεχνητή νοημοσύνη ή από συγκεκριμένα μοτίβα, false injection ανίχνευση και ανώμαλη λειτουργία αισθητήρων. Κοινό σημείο στις μελέτες οι οποίες επιλέχθηκαν για την συγκεκριμένη συστηματική βιβλιογραφική ανασκόπηση, είναι η παρουσίαση των δεδομένων σε γραπτή μορφή με κάποιες εξαιρέσεις οι οποίες θα αναλυθούν στη συνέχεια.

### *1.6.2. Ελλείπουσες ή ασαφείς πληροφορίες*

Στα άρθρα των Bondarev & Prokhorov (2017) και Kruthika Rathinavel et al. (2017) εντοπίστηκαν πολύ συγκεκριμένες αναφορές σε επιθέσεις δίχως την ανάπτυξη υπόβαθρου. Αυτό σαφώς δεν σημαίνει ότι δεν είναι έγκυρες ή αναξιόπιστες, απλώς ο τρόπος γραφής των συγγραφέων αλλά και η παρουσίαση των ευρημάτων εκ μέρους τους οδηγούν σε υποθέσεις. Θα αξιολογηθούν και θα αναλυθούν οι παραπάνω έρευνες στα επόμενα κεφάλαια.

## *1.7. Ρίσκο προκατάληψης*

Όπως αναφέρθηκε στην ενότητα 1.6.2, στην μελέτη των Kruthika Rathinavel et al. (2017) προτείνεται ένα σύστημα αντιμετώπισης επιθέσεων το οποίο όπως αναφέρεται και στην μελέτη είναι κατοχυρωμένη πατέντα αλλά κατέχει και εμπορικό σήμα (trademark). Η συγκεκριμένη μελέτη είναι η μόνη στα άρθρα τα οποία εισήχθησαν στην παρούσα διπλωματική. Είναι συνετό να αναφερθεί το παρόν άρθρο και να προστεθεί στα ρίσκα προκατάληψης ως προς

την παρουσίαση των δεδομένων καθώς το συγκεκριμένο σύστημα δύναται να εκμεταλλευτεί οικονομικά και να είναι απαραίτητη η διαφήμιση του. Συνεπώς θα αξιολογηθεί και θα κριθεί αντικειμενικά όπως και οι υπόλοιπες μελέτες.

# *2. Σύνθεση Α*

Όπως αναφέρθηκε παραπάνω στην παρούσα ανασκόπηση θα υπάρξουν δύο συνθέσεις. Η πρώτη αφορά τις επιθέσεις σε δίκτυα IoT και έξυπνα κτίρια. Θα χρησιμοποιηθεί αφηγηματική σύνθεση με την οποία θα παρουσιαστούν τα δεδομένα των ερευνών. Είναι σημαντικό να σημειωθεί ότι πραγματοποιήθηκαν δύο περάσματα για την κάθε σύνθεση γεγονός το οποίο αναφέρθηκε παραπάνω. Αρχικά, έγινε βασική εξαγωγή δεδομένων (πρακτική εξαγωγή) κατά την οποία τίτλοι, έτη δημοσίευσης, βάσεις δεδομένων και ονόματα συγγραφέων συγκεντρώθηκαν. Εν συνεχεία, συντάχθηκαν σύντομες περιλήψεις για το εκάστοτε άρθρο σύμφωνα με το μορφότυπο IMRaD. Το μορφότυπο IMRaD αναφέρεται σε τέσσερις βασικούς πυλώνες introduction (εισαγωγή), methods (μεθοδολογία), results (αποτελέσματα) και discussion (περαιτέρω συζήτηση) (Sollaci & Pereira, 2004). Κύριος σκοπός είναι η άντληση δεδομένων, σχετικών με ερευνητικά ερωτήματα, ορισμούς προβλημάτων και συνεισφορές.

## *2.1. IoT Layers*

Στην μελέτη των Akram Abdul-Ghani et al. (2018) αλλά και στην μελέτη Mosenia & Jha (2017) οι ερευνητές καταφέρνουν να οργανώσουν τις επιθέσεις σε τέσσερις μεγάλες κατηγορίες οι οποίες είναι 1) physical based attacks 2) protocol based attacks 3) data based attacks και 4) software based attacks. Πιο συγκεκριμένα στην πρώτη κατηγορία αναφέρονται σε επιθέσεις οι οποίες δύναται να πραγματοποιηθούν σε αισθητήρες, συσκευές ανάγνωσης RFID, κάρτες και tags. Στην δεύτερη κατηγορία πραγματοποιούνται επιθέσεις στα πρωτόκολλα επικοινωνίας μεταξύ συσκευών IoT. Είναι γνωστό ότι οι IoT συσκευές χρησιμοποιούν δικό τους stack στο οποίο χρησιμοποιούν πρωτόκολλά 6loWPAN και IEEE 802.15.4 διότι θεωρούνται «lightweight». Στην τρίτη κατηγορία κατηγοριοποιούνται επιθέσεις που αφορούν τα δεδομένα είτε αυτά βρίσκονται στις ίδιες IoT συσκευές ή στο cloud. Τέλος στην τέταρτη κατηγορία αφορά

επιθέσεις στο application layer των IoT συσκευών είτε αυτό είναι στο λογισμικό είτε στο υλικολογισμικό (Firmware). Στην συγκεκριμένη μελέτη παρουσιάζονται όλα τα πρωτόκολλα επικοινωνίας καθώς και τα χαρακτηριστικά τους. Οι συγγραφείς προσφέρουν σαφές θεωρητικό υπόβαθρο.

Στην έρευνα των Kumar et al. (2016) αναφέρονται τα layers των IoT δικτύων. Παρουσιάζεται τέσσερα επίπεδα. Το Application layer στο οποίο βρίσκονται οι end users και εκείνοι που ωφελούνται από ένα δίκτυο IoT, το perception layer στο οποίο τοποθετούνται όλες οι υλικές συσκευές (αισθητήρες, RFID readers, κλπ.), το Network layer το οποίο ευθύνεται για την επικοινωνία των συσκευών μεταξύ τους αλλά και με το ευρύ διαδίκτυο και το physical layer το οποίο ουσιαστικά πρόκειται για την «ραχοκοκαλιά» των IoT συσκευών.

Παρόμοιες παρατηρήσεις αναφέρονται και από την έρευνα των Krishnan et al. (2017). Παρότι επικεντρώνονται περισσότερο στις επικοινωνίες. Κατηγοριοποιούν τις επιθέσεις με βάση τις επικοινωνίες όπως near field communication και Wi-Fi Communication.

Στην μελέτη των Sheikh et al. (2019) αναφέρονται ξεκάθαρα για τα επίπεδα τα οποία αναφέρθηκαν παραπάνω και εστιάζουν στα BMS (building management systems). Δεν υπάρχει ταξινόμηση και κατηγοριοποίηση επιθέσεων αλλά παρουσιάζουν άμεσες επιθέσεις πάνω στο BMS.

Η μελέτη των Kruthika Rathinavel et al. (2017) αναφέρει για το δικό τους framework ενός BAS (building automation systems) αναφέρονται στα επίπεδα που αποσκοπούν στην παρουσίαση της αρχιτεκτονικής του δικού τους συστήματος.

Και στην περίπτωση των Sun et al. (2014) αναφέρονται τα επίπεδα και κατηγοριοποιούνται οι επιθέσεις ανάλογα σε ποιο επίπεδο βρίσκονται. Στην συγκεκριμένη έρευνα παρουσιάζεται και μία κατηγορία η οποία αναφέρεται σε πολλαπλά επίπεδα επιθέσεων (multi-layer attacks). Έπειτα από την κατηγοριοποίηση αναφέρονται σε μέτρα τα οποία δύναται να παρθούν με σκοπό την αποφυγή επιθέσεων (θα αναφερθούν παρακάτω στην σύνθεση Β κατά την οποία θα αναπτυχθούν πρακτικές αντιμετώπισης) Τέλος, στην μελέτη των Inayat et al. (2021) αναφέρονται ξανά τα επίπεδα και κατηγοριοποίηση επιθέσεων με βάση τα προαναφερθέντα επίπεδα. Είναι συνετό να αναφερθεί ότι η συγκεκριμένη έρευνα αναφέρεται εκτενώς στην επίθεση ασύρματων δικτύων και όχι απαραίτητα σε συστήματα BEMS.

Καθίσταται σαφές, ότι οι περισσότερες μελέτες έχουν κατηγοριοποιήσει τις επιθέσεις με βάση τα επίπεδα των IoT δικτύων και παρουσιάζουν συγκεκριμένες λύσεις για να αποφευχθούν κακόβουλοι χρήστες από το να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα. Στο επόμενο κεφάλαιο υπάρχει εκτενής πίνακας με όλες τις επιθέσεις ανά κατηγορία και ανά επίπεδο.

### *2.2. Επιθέσεις, τρωτά σημεία και λύσεις*

Στην παρούσα ενότητα θα κατηγοριοποιηθούν οι επιθέσεις και θα αναλυθούν τα επιμέρους στοιχεία τους. Θα πραγματοποιηθεί στοχευμένη ανάλυση των χαρακτηριστικών των επιθέσεων καθώς και σύγκριση αυτών μεταξύ των μελετών.

#### *2.2.1 Physical Based Attacks*

Αρχικά τα Physical Based Attacks στα συστήματα των έξυπνων κτιρίων αφορούν οτιδήποτε αποτελείται σε φυσική, υλική μορφή. RFID readers, αισθητήρες, RFID tags, κάμερες κ.ο.κ. αποτελούν χαρακτηριστικά παραδείγματα συστημάτων IoT τα οποία δύναται να δεχθούν πληθώρα επιθέσεων οι οποίες θα παρουσιαστούν παρακάτω.

##### ***Object replication attacks***

Στις object-replication επιθέσεις ο κακόβουλος χρήστης έχει τη δυνατότητα να προσθέσει ένα καινούργιο φυσικό (physical) αντικείμενο στο δίκτυο (Akram Abdul-Ghani et al., 2018; Mosenia & Jha, 2017). Οι επιθέσεις αυτές προκαλούν δραματική μείωση στην επίδοση του δικτύου (Akram Abdul-Ghani et al., 2018; Mosenia & Jha, 2017). Πρόκειται για ενεργή επίθεση (active attack) (Sun et al., 2014), εσωτερική (internal attack) ή εξωτερική (external attack) καθώς ο κακόβουλος χρήστης προσθέτει αντικείμενα που δεν ανήκουν στο domain του δικτύου ή να υπάρχουν εκτεθειμένοι εσωτερικοί κόμβοι (Sun et al., 2014). Οι εσωτερικές επιθέσεις είναι αρκετά σοβαρές καθώς απειλούν την εμπιστευτικότητα, αυθεντικοποίηση και την ακεραιότητα των δεδομένων (Inayat et al., 2021; Sun et al., 2014). Ο κακόβουλος χρήστης δύναται να καταφέρει να αλλοιώσει ή να παραπλανήσει πακέτα (Mosenia & Jha, 2017), να αποκτήσει

πρόσβαση σε ευαίσθητα δεδομένα (Mosenia & Jha, 2017) και να εξάγει κρυπτογραφικά κοινά κλειδιά (Akram Abdul-Ghani et al., 2018; Mosenia & Jha, 2017).

| **Έρευνα** | **Χαρακτηριστικά / Απόψεις** |
|---|---|
| Akram Abdul-Ghani et al. (2018) | Ο κακόβουλος χρήστης, μπορεί να προσθέσει ένα φυσικό αντικείμενο στο δίκτυο IoT. Πιο συγκεκριμένα είναι δυνατό αυτό το κακόβουλο αντικείμενο να μιμηθεί και να αναπαράγει την ταυτοποίηση των συσκευών. Παράλληλα, μειώνει την αξιοπιστία και την ταχύτητα του δικτύου, ενώ ταυτόχρονα δύναται να διαφθείρει τα εισερχόμενα και εξερχόμενα πακέτα. |
| Mosenia & Jha (2017) | Στην συγκεκριμένη επίθεση αναφέρεται ότι ο κακόβουλος χρήστης, προσθέτει ένα κακόβουλο κόμβο με τον οποίο μπορεί να ελέγξει τα πακέτα, να αλλάξει την πορεία τους. |
| **Σύνοψη** | Σοβαρή επίθεση σε δίκτυα IoT καθώς δύναται να εξάγει τα κρυπτογραφημένα κλειδιά των συσκευών και να αποκτήσει πρόσβαση. Επιπρόσθετα, η απόδοση του δικτύου επηρεάζεται σφοδρά από τέτοιου τύπου επιθέσεις. Τέλος είναι δυνατό να άρουν εξουσιοδοτημένους κόμβους από την κανονική λειτουργία τους. |

### *Hardware Trojan*

Οι Akram Abdul-Ghani et al. (2018) αναφέρουν ότι πολυάριθμες μελέτες έχουν καταδείξει ότι η ευαισθησία ενός ενσωματωμένου κυκλώματος (integrated circuit) σε επίθεση με

Hardware Trojan είναι το κύριο ελάττωμα ασφαλείας του. Στην άποψη αυτή συμφωνούν και οι Mosenia & Jha (2017) καθώς υπογραμμίζουν ότι το Hardware Trojan αποτελεί σοβαρό κίνδυνο ασφαλείας. Και οι δύο (Akram Abdul-Ghani et al., 2018; Mosenia & Jha, 2017) αναφέρουν ότι κύριος στόχος μιας τέτοιας επίθεσης είναι η κακόβουλη τροποποίηση του ενσωματωμένου κυκλώματος προκειμένου να αποκτήσει πρόσβαση στο υλικολογισμικό του και σε ευαίσθητα δεδομένα. Οι Mosenia & Jha (2017) κάνουν μια πιο λεπτομερή ανασκόπηση – συγκριτικά με τους Akram Abdul-Ghani et al. (2018) – στις επιθέσεις Hardware Trojan, διαχωρίζοντας τες σε 2 κατηγορίες και αναφέροντας επίσης τρόπους ανίχνευσης. Οι επιθέσεις Hardware Trojan συμβαίνουν κατά τη φάση της σχεδίασης και είναι αδρανείς έως ότου ενεργοποιηθούν από κάποιο γεγονός ή από τον δημιουργό τους. Ο επιτιθέμενος τροποποιεί σκόπιμα τη σχεδίαση πριν/κατά τη διάρκεια της κατασκευής και καθορίζει έναν μηχανισμό ενεργοποίησης που ενεργοποιεί την κακόβουλη συμπεριφορά του Trojan προκειμένου να ενσωματώσει ένα Hardware Trojan στο αρχικό κύκλωμα. Σύμφωνα με τους μηχανισμούς ενεργοποίησής τους, τα Hardware Trojan χωρίζονται συνήθως σε δύο κατηγορίες: α) εξωτερικά ενεργοποιούμενα Hardware Trojan, οι οποίοι μπορούν να ενεργοποιηθούν από μια κεραία ή έναν αισθητήρα που μπορεί να αλληλοεπιδράσει με τον εξωτερικό κόσμο, και β) εσωτερικά ενεργοποιούμενα Hardware Trojan, οι οποίοι ενεργοποιούνται μετά την εγκατάσταση του δούρειου ίππου. Οι Mosenia & Jha (2017) συνοψίζουν τους τρόπους ανίχνευσης σε τρεις, με τη χρήση side-channel σημάτων όπως ο χρόνος, η ισχύς και η χωρική θερμοκρασία.

| **Έρευνα** | **Χαρακτηριστικά / Απόψεις** |
|---|---|
| Akram Abdul-Ghani et al., (2018) | Σκοπός της επίθεσης είναι η πρόσβαση στο firmware της συσκευής και η εξαγωγή δεδομένων από αυτή. Τέτοιου τύπου malware μπορεί να μείνει κρυμμένο μέχρι ο κακόβουλος χρήστης να το ενεργοποιήσει απομακρυσμένα. |
| Mosenia & Jha, (2017) | Στην παρούσα μελέτη δίνεται διαχωρισμός των trojan malware. Δύναται να γίνει η εκκίνηση του κακόβουλου λογισμικού εξωτερικά, δηλαδή να δοθεί η εντολή απομακρυσμένα μέσω κεραίας ή ενός αισθητήρα ο οποίο είναι συνδεδεμένος στο |

| | |
|---|---|
| | διαδίκτυο ή και εσωτερικά βάση ενός γεγονότος στην συσκευή πχ. Να ενεργοποιηθεί μετά από συγκεκριμένη χρονική στιγμή. |
| **Σύνοψη** | Επιθέσεις με μεγάλο εύρος ζημίας καθώς η εισαγωγή τέτοιου malware γίνεται κατά την διαδικασία της κατασκευής του κυκλώματος |

### *Object Tampering / Side-Channel Attack*

Τα Edge Devices είναι εξαιρετικά ευαίσθητα σε επιθέσεις υλικού/λογισμικού, δεδομένου ότι λειτουργούν σε εχθρικά περιβάλλοντα όπου μπορεί να υπάρξει φυσική πρόσβαση στις συσκευές. Λόγω της πρόσβασης ο επιτιθέμενος μπορεί να τροποποιήσει το λειτουργικό σύστημα, να πειράξει τα κυκλώματα, να ξαναγράψει κώδικα ή να ανακτήσει πολύτιμα κρυπτογραφικά δεδομένα (Mosenia & Jha, 2017). Κίνδυνο πρόσβασης παρά της υπάρχουσας κρυπτογράφησης απειλούν και οι επιθέσεις side-channel (Akram Abdul-Ghani et al., 2018), όπου η επίθεση αποσκοπεί στην παραβίαση αυτών των μηχανισμών με την ανάλυση των πληροφοριών του Side-Channel από τα αντικείμενα IoT. Οι Mosenia & Jha, 2017 αναφέρουν ως τρόπο αντιμετώπισης για τις επιθέσεις Object Tampering και Side-Channel την τροποποίηση κυκλώματος. Στην τροποποίηση κυκλώματος (circulation modification) οι κόμβοι μπορούν να ενσωματωθούν με φυσικό υλικό που ενισχύει την προστασία από φυσικές επιθέσεις (Mosenia & Jha, 2017). Για παράδειγμα, για την προστασία από την αλλοίωση των αισθητήρων, έχουν προταθεί διάφορες μηχανικές/ηλεκτρικές μέθοδοι προστασίας από αλλοίωση για τον σχεδιασμό των φυσικών πακέτων των κόμβων, οι οποίες χρησιμοποιούνται παραδοσιακά σε αισθητήρες οικιακού αυτοματισμού, π.χ. σε ανιχνευτές καπνού. Επιπλέον, η χρήση μηχανισμών αυτοκαταστροφής παρέχει μια εναλλακτική προσέγγιση για την άμυνα έναντι φυσικών επιθέσεων.

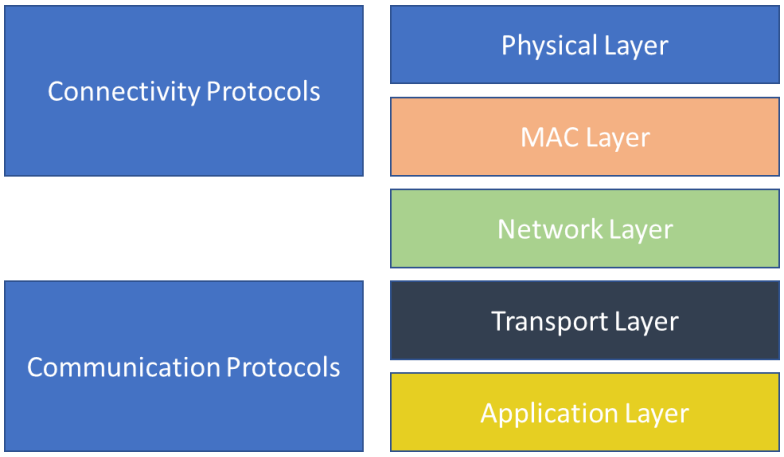
| **Έρευνα** | **Χαρακτηριστικά / Απόψεις** |
|---|---|
| Akram Abdul-Ghani et al., (2018) | Είναι δυνατό κάποιες IoT συσκευές να τοποθετούνται σε περιοχές οι οποίες δεν είναι προστατευμένες, όπως αναφέρθηκε παραπάνω σε |

| | |
|---|---|
| | συνδυασμό επιθέσεων (hardware trojan και replication attack) να αποσπάσουν τα κρυπτογραφημένα κλειδιά ή να αλλάξουν την ομαλή λειτουργία τους. Κατ' επέκταση οι περισσότερες συσκευές διαθέτουν μία στοιχειώδη ασφάλεια για να προστατεύσουν ευαίσθητα δεδομένα. Κακόβουλοι χρήστες μπορούν να αναλύσουν τα δεδομένα τα οποία εξέρχονται κάνοντας χρήση των ίδιων συστημάτων ασφαλείας. |
| Mosenia & Jha, (2017) | Όσον αφορά το Object Tampering στην συγκεκριμένη έρευνα τα χαρακτηριστικά και οι απόψεις είναι σε συμφωνία με την παραπάνω. Στα Side-Channel Attacks χρησιμοποιείται ανεπτυγμένης τεχνολογίας εργαλεία τα οποία έχουν την δυνατότητα να «πιάσουν» τις επικοινωνίες ακόμη και αν αυτές είναι κρυπτογραφημένες. Χαρακτηριστικό παράδειγμα είναι ότι ο κακόβουλος χρήστης μπορεί να γνωρίζει τον αριθμό των ατόμων σε ένα κτήριο, γνωρίζοντας τον αριθμό των συναλλαγών από τον αναγνώστη RFID και το RFID tag |
| **Σύνοψη** | Και σε αυτές τις επιθέσεις καταλήγουμε στην κακή επιλογή τοποθέτησης των IoT συσκευών σε συνθήκες μη ελεγχόμενες και πως οι κακόβουλοι χρήστες μπορούν με ευκολία να καταλάβουν τις συσκευές αυτές |

### *2.2.2 Connectivity - Protocol Based Attacks*

Όπως είναι ήδη γνωστό τα δίκτυα IoT έχουν το δικό τους stack στο οποίο επικοινωνούν μεταξύ τους. Συνήθως το IoT stack αποτελείται από πρωτόκολλα τα οποία δεν καταλαμβάνουν μεγάλη επεξεργαστική ισχύ αλλά παράλληλα είναι οικονομικά στην κατανάλωση ρεύματος

(6loWPAN, IEEE 802.15.4). Όπως αναφέρθηκε σε παραπάνω κεφάλαιο αυτά τα layers είναι τα εξής.




*Διάγραμμα 2 - OSI Layers*[1]

Με βάση το παραπάνω διάγραμμα όλες οι μελέτες έχουν κατηγοριοποιήσει τις επιθέσεις στα δίκτυα IoT και με αυτό το τρόπο θα παρουσιαστούν και στην συγκεκριμένη διπλωματική εργασία. Παρακάτω παρουσιάζεται πίνακας με επιθέσεις στα Connectivity Protocols.

### ***Protocol Based Attacks (Near Field, ZigBee, RFID, Bluetooth, WiFi)***

*Eavesdropping – Υποκλοπή*

Οι Mosenia & Jha (2017) σημειώνουν ότι σε αυτή την επίθεση ο κύριος στόχος του επιτιθέμενου είναι να υποκλέψει, να διαβάσει και να αποθηκεύσει μηνύματα για μελλοντική ανάλυση. Τα υποκλαπέντα δεδομένα μπορούν να χρησιμοποιηθούν ως είσοδος σε άλλες επιθέσεις, όπως η κλωνοποίηση ετικετών (tag cloning). Οι επιθέσεις υποκλοπής μπορούν να συμβούν στα RFID, NFC, Bluetooth, ZigBee (Akram Abdul-Ghani et al., 2018; Krishnan et al., 2017; Seferi Rifat & Giangiacomi Sofia, 2019; Sheikh et al., 2019b)και στο physical layer (Ma, 2021), στο communication layer (Mosenia & Jha, 2017) και στο perception layer (Kumar et al., 2016a).

[1] Το συγκεκριμένο διάγραμμα αντλήθηκε από τις εξής πηγές: (Akram Abdul-Ghani et al., 2018; Brooks et al., 2020b; Kumar et al., 2016a; Sheikh et al., 2019b; Sun et al., 2014)

Η υποκλοπή είναι μια παθητική επίθεση (Lv et al., 2021a; Sun et al., 2014) κατά της εμπιστευτικότητας (Inayat et al., 2021; Nafrees et al., 2021a). Για την αντιμετώπιση τέτοιων επιθέσεων, οι ευαίσθητες ή εμπιστευτικές πληροφορίες που μεταδίδονται πρέπει να υποβάλλονται σε επεξεργασία από τους χρήστες μέσω κρυπτογράφησης για την προστασία της ασφάλειας κατά την μετάδοσης πληροφοριών (Lv et al., 2021a; Mosenia & Jha, 2017; Nafrees et al., 2021a). Μπορούν επίσης να χρησιμοποιηθούν σχήματα ελέγχου ταυτότητας (authentication schemes) και ανάλυση των απαιτήσεων κυβερνοασφάλειας (analysis of the cybersecurity requirements of network layers) των επιπέδων δικτύου (Mosenia & Jha, 2017). Στο φυσικό επίπεδο ένα άλλο αντίμετρο είναι η μέθοδος κλειδώματος (keying method) (Sun et al., 2014). Ο Kumar et al. (2016a) σημειώνει ότι στο perception layer, καθώς ο τρόπος επικοινωνίας είναι ασύρματος και μέσω του διαδικτύου, οι συσκευές IoT είναι πιο ευάλωτες σε επιθέσεις υποκλοπής, επειδή μένουν αφύλακτες. Στο επίπεδο επικοινωνίας, η υποκλοπή (που ονομάζεται επίσης sniffing) αναφέρεται στην εσκεμμένη ακρόαση ιδιωτικών συνομιλιών μέσω των ζεύξεων επικοινωνίας (Mosenia & Jha, 2017).

Η έννοια των επιθέσεων υποκλοπής κατά των RFID δεν είναι καινούργια και αναφέρεται συχνά στη βιβλιογραφία (Mosenia & Jha, 2017). Ο Akram Abdul-Ghani et al. (2018) σημειώνει ότι τα περισσότερα συστήματα RFID δεν διαθέτουν καμία τεχνική κρυπτογράφησης κατά τη διαδικασία μετάδοσης λόγω της χωρητικότητας της μνήμης. Ως αποτέλεσμα, είναι πολύ εύκολο για οποιονδήποτε επιτιθέμενο να αποκτήσει ευαίσθητα δεδομένα από τις ετικέτες RFID. Ο Krishnan et al. (2017) προσθέτει ότι οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν μια εξαιρετικά αποδοτική κεραία για να εξάγουν τα δεδομένα από τα σήματα RF που ανακλώνται από την ετικέτα RFID, ωστόσο πιστεύει ότι εφόσον το RFID λειτουργεί σε παθητική λειτουργία είναι πολύ πιο δύσκολο να υποκλαπεί. Οι Mosenia & Jha (2017) προσθέτουν στη βιβλιογραφία αντίμετρα για τις επιθέσεις υποκλοπής στις ετικέτες RFID. Αυτά είναι η εντολή kill/sleep, η απομόνωση (isolation), ο αποκλεισμός (blocking), το προσωπικό τείχος προστασίας (personal firewall) και τα κρυπτογραφικά συστήματα (cryptographic schemes).

Το NFC είναι επίσης ευάλωτο σε επίθεση υποκλοπής. Το κανάλι επικοινωνίας μεταξύ δύο αντικειμένων IoT που είναι εξοπλισμένα με το πρωτόκολλο NFC είναι ευάλωτο σε μια τέτοια επίθεση, δεδομένου ότι το NFC δεν διαθέτει καμία τεχνική προστασίας (Akram Abdul-Ghani et al., 2018).

Οι Krishnan et al., 2017 πιστεύουν ότι στα δίκτυα Zigbee η χρήση τεχνικών κρυπτογράφησης, όπως τα ψηφιακά πιστοποιητικά (SSL), θα μείωνε τον κίνδυνο επιθέσεων υποκλοπής.

Τέλος, η υποκλοπή μπορεί να γίνει μέσω Bluetooth (Seferi Rifat & Giangiacomi Sofia, 2019). Δεδομένου ότι η επικοινωνία μέσω Bluetooth είναι διαφορετική από την επικοινωνία μέσω άλλων ασύρματων τεχνολογιών, δεν μπορεί εύκολα να υποκλαπεί απευθείας από τον αέρα, αλλά από έναν προσαρμογέα Bluetooth ή την ασύρματη/ Bluetooth NIC στη συσκευή από την οποία έχει ενεργοποιηθεί η σάρωση.

*Replay attack – Επίθεση επανάληψης*

Στην επίθεση επανάληψης, ο επιτιθέμενος υποκλέπτει πρώτα τα μηνύματα που αποστέλλονται από τον χρήστη με ασύρματα ή ενσύρματα μέσα μέσω υποκλοπής (Lv et al., 2021a). Στη συνέχεια, ορισμένα από τα μηνύματα αποστέλλονται επανειλημμένα στα αντικείμενα-στόχους, παραπλανώντας τα ώστε να νομίζουν ότι οι πληροφορίες προέρχονται από τους νόμιμους χρήστες, και στη συνέχεια αποκτούν παράνομα οφέλη (Lv et al., 2021a). Οι επιθέσεις επανάληψης απειλούν την ακεραιότητα (Nafrees et al., 2021b).

Οι επιθέσεις επανάληψης ενεργοποιούν και απενεργοποιούν επανειλημμένα τη συσκευή και παρατηρούν τις αλλαγές των πακέτων (Akram Abdul-Ghani et al., 2018; Krishnan et al., 2017; Lv et al., 2021b; Sheikh et al., 2019b). Εάν τα πακέτα που λαμβάνονται από πολλαπλές ενεργοποιήσεις και απενεργοποιήσεις είναι τα ίδια, τότε οι προϋποθέσεις για τις επιθέσεις επανάληψης πληρούνται πλήρως (Akram Abdul-Ghani et al., 2018; Krishnan et al., 2017; Lv et al., 2021b; Sheikh et al., 2019b). Απλά αντιγράφουν τα περιεχόμενα του πακέτου σύμφωνα με τους δεκαεξαδικούς χαρακτήρες και στη συνέχεια στέλνουν γρήγορα μαζικά αιτήματα στην αντίστοιχη θύρα του διακομιστή με τη βοήθεια εργαλείων. Αυτό το είδος επίθεσης μπορεί να αντιμετωπιστεί με την προσθήκη χρονοσήμανσης ή τυχαίας τιμής (Akram Abdul-Ghani et al., 2018; Krishnan et al., 2017; Lv et al., 2021b; Sheikh et al., 2019b) και μπορεί να συμβεί και στα connectivity protocols RFID, NFC και ZigBee, όπου στο NFC βασίζεται σε μεγάλο βαθμό στην εκτέλεση των εντολών της μονάδας δεδομένων πρωτοκόλλου εφαρμογής (ISO/IEC1443) (Akram Abdul-Ghani et al., 2018).

*Man-in-the-Middle attack*

Η επίθεση Man-in-the-Middle είναι μια επίθεση στον κυβερνοχώρο που απειλεί την εμπιστευτικότητα (confidentiality) (Nafrees et al., 2021b) και την ιδιωτικότητα (privacy) του χρήστη, καθώς απειλεί με αποκάλυψη της ταυτότητάς του (Nafrees et al., 2021b). Οι Lv et al. (2021b) σημειώνουν ότι υπάρχουν δύο τρόποι επίθεσης: παράκαμψη (bypass) και σειριακή σύνδεση (serial connection). Περαιτέρω, εξηγούν Lv et al. (2021b) ότι ο επιτιθέμενος βρίσκεται στη μέση της σύνδεσης και στα δύο άκρα της επικοινωνίας και ενεργεί ως ο ρόλος της ανταλλαγής δεδομένων. Ο επιτιθέμενος μπορεί να αποκτήσει τις πληροφορίες ελέγχου ταυτότητας χρήστη και τις πληροφορίες ελέγχου της συσκευής και στη συνέχεια να αποκτήσει το δικαίωμα ελέγχου της συσκευής μέσω αναπαραγωγής (replay) ή ασύρματης αναμετάδοσης (wireless relay) Lv et al. (2021b).

Αυτή η επίθεση μπορεί να συμβεί στα πρωτόκολλα συνδεσιμότητας RFID, NFC (Akram Abdul-Ghani et al., 2018), Bluetooth (Ma, 2021) και WiFi (Krishnan et al., 2017). Στο RFID μπορεί να συμβεί κατά τη μετάδοση δεδομένων μεταξύ αναγνώστη και ετικετών (Akram Abdul-Ghani et al., 2018). Σε αυτή την περίπτωση, ένας επιτιθέμενος μπορεί να υποκλέψει και να τροποποιήσει το κανάλι επικοινωνίας μεταξύ των στοιχείων του συστήματος RFID (Akram Abdul-Ghani et al., 2018). Οι Krishnan et al., 2017 γράφουν για την επίθεση MITM στο WiFi, ότι ο επιτιθέμενος αναμεταδίδει ή ενδεχομένως τροποποιεί την επικοινωνία μεταξύ δύο μερών. Ο επιτιθέμενος μπορεί να ενεργεί ως ψεύτικη πύλη και να κάνει τον χρήστη να συνδεθεί σε αυτήν, λαμβάνοντας έτσι τα στοιχεία όπως η διεύθυνση MAC του smartphone του χρήστη (Krishnan et al., 2017).

Μονάχα οι Akram Abdul-Ghani et al. (2018) και Sun et al. (2014) απαριθμούν αντίμετρα κατά των επιθέσεων man in the middle. Για να ενισχυθεί η ασφάλεια έναντι του MITM, μπορεί να γίνει ρύθμιση κωδικών πρόσβασης και άλλων μυστικών κλειδιών υψηλού επιπέδου για αμοιβαία πιστοποίηση (Akram Abdul-Ghani et al., 2018). Προκειμένου να ελεγχθεί η παρουσία του επιτιθέμενου MITM, μπορεί να πραγματοποιηθεί η μέθοδος εξέτασης της καθυστέρησης (τεχνική ελέγχου χρόνου). Βοηθά στην ανίχνευση του επιτιθέμενου MITM υπολογίζοντας το χρόνο που απαιτείται για τη λήψη ενός μηνύματος και από τα δύο άκρα. Οι (Sun et al., 2014)

παραθέτουν την αυθεντικοποίηση, την επαλήθευση ταυτότητας και την επαλήθευση αμφίδρομης σύνδεσης (bidirectional link verification) ως αντίμετρα σε αυτόν τον τύπο επίθεσης.

*Bluebugging attack*

Το Bluetooth είναι επιρρεπές σε πολλές επιθέσεις, με την πιο επικίνδυνη από αυτές, το bluebugging, στο οποίο αναφέρονται οι Akram Abdul-Ghani et al. (2018). Σε αυτό τύπο επίθεσης, ένας αντίπαλος θα μπορούσε να βρίσκεται μέσα στη συσκευή του θύματος εκμεταλλευόμενος κάποιες ευπάθειες στο παλιό υλικολογισμικό της συσκευής- ως εκ τούτου, θα μπορούσε να κατασκοπεύει τηλεφωνικές κλήσεις, να στέλνει και να λαμβάνει μηνύματα και να συνδέεται στο διαδίκτυο χωρίς να το γνωρίζουν οι νόμιμοι χρήστες

*DoS – Denial of Service attack*

Οι επιθέσεις άρνησης υπηρεσιών επιχειρούν να μπλοκάρουν τα κανάλια μετάδοσης καταναλώνοντας το περιορισμένο εύρος ζώνης του δικτύου και, ως εκ τούτου, έχουν ως αποτέλεσμα την αποτυχία των νόμιμων αιτημάτων των χρηστών. Ο σκοπός μιας επίθεσης DoS είναι να παρεμβαίνει και να διακόπτει τη ροή πληροφοριών εντός του δικτύου επικοινωνίας και να αρνείται στους χρήστες την πρόσβαση στους πόρους ενός ιστότοπου (Wan et al., 2021). Είναι η πιο συνηθισμένη επίθεση στη Διαθεσιμότητα (Kruthika Rathinavel et al., 2017; Nafrees et al., 2021b).

Η βιβλιογραφία σημειώνει ότι η επίθεση DoS μπορεί να συμβεί στο φυσικό επίπεδο (Llaria et al., 2021), στο επίπεδο MAC (Llaria et al., 2021) και στο επίπεδο δικτύου (Kumar et al., 2016a). Ένας απλός τρόπος για να πραγματοποιηθεί μια DoS στο φυσικό επίπεδο είναι μέσω μιας διαδικασίας παρεμβολής, η οποία μπορεί να πραγματοποιηθεί από το εξωτερικό του δικτύου (Llaria et al., 2021). Προκειμένου να εκτελεστεί μια επίθεση DoS στο επίπεδο MAC, ο επιτιθέμενος (ο οποίος μπορεί να είναι ένας κοινός εξωτερικός χρήστης) προσπαθεί, μέσω ορισμένων τύπων μηνυμάτων, όπως μηνύματα επιβεβαίωσης, να δημιουργήσει συγκρούσεις που παρεμποδίζουν τις νόμιμες επικοινωνίες (Llaria et al., 2021) Στο επίπεδο δικτύου: Οι συσκευές ή ο διακομιστής βομβαρδίζονται με αποτέλεσμα να μην μπορούν να εξυπηρετήσουν τους χρήστες

που χρειάζονται τις υπηρεσίες τους (Kumar et al., 2016a). Επιθέσεις DoS που διακόπτουν τη μεταφορά δεδομένων μεταξύ των συσκευών και της πηγής τους.

Οι αποτελεσματικές λύσεις κατά του DoS, ιδίως στο φυσικό επίπεδο και στο επίπεδο MAC, αποτελούν πρόκληση. Η αλυσίδα μπλοκ, ως λύση για την πρόληψη της παραποίησης δεδομένων, πρέπει να αναπτυχθεί προκειμένου να καταστεί δυνατή η ανάπτυξή της σε περιορισμένες συσκευές (Kumar et al., 2016a). Στο επίπεδο MAC οι Kumar et al. (2016) αναφέρουν ως λύσεις τον κώδικα διόρθωσης σφαλμάτων και την κρυπτογράφηση.

*False Data Injection attack*

Οι Nafrees et al. (2021) κατέταξαν τις επιθέσεις εισβολής δεδομένων στις επιθέσεις sniffing. Οι επιθέσεις FDI συνήθως χειραγωγούν τα δεδομένα μετάδοσης και έτσι υπονομεύουν την ακεραιότητα και την αξιοπιστία των πληροφοριών (Wan et al., 2021). Στο επίπεδο δικτύου οι εξωτερικοί επιτιθέμενοι μπορούν να εισάγουν ψευδή δεδομένα προκαλώντας στο σύστημα ακατάλληλη ή επικίνδυνη αντίδραση (Kumar et al., 2016a). Αυτό μπορεί επίσης να αποτελεί πρόδρομο μιας φυσικής επίθεσης και μπορεί να χρησιμοποιηθεί για τη συγκάλυψη τέτοιων απειλών (Kumar et al., 2016a).

*Spoofing attack*

Οι επιθέσεις spoofing στο πρωτόκολλο συνδεσιμότητας βασίζονται στα RFID και Bluetooth (Akram Abdul-Ghani et al., 2018). Οι Nafrees et al. (2021) σημειώνουν ότι αυτές οι επιθέσεις απειλούν τη διαθεσιμότητα του συστήματος.

Στις επιθέσεις που βασίζονται στο RFID, η επίθεση spoofing συμβαίνει όταν μια κακόβουλη ετικέτα προσποιείται ότι είναι έγκυρη ετικέτα και αποκτά μη εξουσιοδοτημένη πρόσβαση (Akram Abdul-Ghani et al., 2018). Μια επίθεση spoofing χρησιμοποιείται για την υποκλοπή των δεδομένων που προέρχονται από την έγκυρη ετικέτα και την αντιγραφή των συλλεχθέντων δεδομένων σε μια άλλη (Akram Abdul-Ghani et al., 2018).

Οι επιθέσεις αυτές αποτελούν τις πιο δημοφιλείς ευπάθειες στο Bluetooth Low Energy, καθώς ο φάρος (beacon) μεταδίδεται δημόσια. Ένα εργαλείο sniffing μπορεί να χρησιμοποιηθεί για τη σύλληψη του UUID του beacon από έναν εισβολέα, να μιμηθεί το beacon και να

παραβιάσει τους κανόνες που έχουν τεθεί από τις εφαρμογές για την επαλήθευση της ταυτότητας, ώστε να μπορεί να έχει πρόσβαση στις υπηρεσίες (Akram Abdul-Ghani et al., 2018). Επίσης οι Akram Abdul-Ghani et al. (2018) σημειώνουν ότι το Bluetooth Spoofing θέτει σε κίνδυνο την ιδιωτικότητα, την ακεραιότητα, την ελεγκσιμότητα, την αξιοπιστία και την μη αποκήρυξη και μερικά από τα αντίμετρα αποτελούν τα «Secure UUID - Rotating UUIDw/ limited token scope, Private Mode with Rotating UUID, Secure Shuffling randomly rotating».

*Fragmentation attack*

Σύμφωνα με τους Akram Abdul-Ghani et al. (2018), η επίθεση κατακερματισμού είναι μια επίθεση που βασίζεται στο WiFi. Για την επιτυχή εκτέλεση αυτής της επίθεσης απαιτείται η υποκλοπή ενός πακέτου. Όλα τα πακέτα που μεταδίδονται μέσω του δικτύου 802.11 έχουν ομοιογενείς επικεφαλίδες γεγονός το οποίο βοηθά τον επιτιθέμενο να μαντέψει τα πρώτα 8 bytes των επικεφαλίδων με XOR αυτών των 8 bytes και 8 bytes κρυπτογραφημένου κειμένου, για να πάρει 8 bytes από το IV.

Οι επιθέσεις κατακερματισμού θέτουν σε κίνδυνο την ιδιωτικότητα, την ακεραιότητα, την αυθεντικότητα, την αξιοπιστία, τη μη αποκήρυξη και την εμπιστευτικότητα. Τα αντίμετρα για τέτοιου είδους επιθέσεις περιλαμβάνουν τη χρήση πολύ μικρού χρόνου επανακλειδώματος, την απενεργοποίηση της αποστολής της αναφοράς αποτυχίας MIC, την απενεργοποίηση του TKIP και τη χρήση δικτύου μόνο με CCMP, τη χρήση μηχανισμών ασφαλείας υψηλότερου επιπέδου, όπως IPsec, DTLS, HTTP/TLS ή CoAP/DTLS, DTLS για CoAp (Akram Abdul-Ghani et al., 2018).

*The Hole196 Vulnerability*

Αυτή η ευπάθεια βασίζεται στο WiFi και ανακαλύφθηκε από τον Sohail Ahmad . Ο Ahmad διαπίστωσε ότι υπάρχει ένα κενό στα τυποποιημένα πρωτόκολλα 802.11 ακριβώς στη σελίδα 196. Ένας εισβολέας, ο οποίος είναι μη εξουσιοδοτημένος χρήστης του δικτύου, θα μπορούσε να στείλει ένα ψεύτικο αίτημα ARP με τη διεύθυνση MAC του σημείου πρόσβασης και οι άλλοι χρήστες θα ενημερώσουν τους πίνακες ARP τους βάσει του αιτήματος. Μετά την

ενημέρωση των πινάκων ARP τους, οι χρήστες θα διαβιβάσουν τα πακέτα τους στη διεύθυνση MAC του επιτιθέμενου αντί για το σημείο πρόσβασης. Ο επιτιθέμενος, σε αυτό το σενάριο, μπορεί να πάρει τα πακέτα που αποκρυπτογραφούνται από το σημείο πρόσβασης, να τα διαβάσει και να ξανα κρυπτογραφήσει αυτά τα πακέτα με το δικό του κλειδί (Akram Abdul-Ghani et al., 2018).

*ZED Sabotage attack*

Αποτελεί επίθεση προς το πρωτόκολλο ZigBee. Ο κύριος στόχος μιας τέτοιας επίθεσης είναι να βανδαλίσει το ZED στέλνοντας περιοδικά ένα συγκεκριμένο σήμα για να ξυπνήσει το αντικείμενο ώστε τελικά να αδειάσει η μπαταρία του (Akram Abdul-Ghani et al., 2018).

*Gateway attack*

Στα gateway attacks κόβεται η σύνδεση μεταξύ των αισθητήρων και των συστημάτων διαχείρισης που συνδέονται στο διαδίκτυο (Akram Abdul-Ghani et al., 2018; Kumar et al., 2016; Sheikh et al., 2019). Οι επιθέσεις αυτές θα μπορούσαν να περιλαμβάνουν επιθέσεις DoS ή επιθέσεις δρομολόγησης που εξαπολύονται στην πύλη και έχουν ως αποτέλεσμα να μην υπάρχει ή να υπάρχει λανθασμένη πληροφορία που μεταδίδεται από το Διαδίκτυο στους αισθητήρες/κόμβους/ενεργοποιητές, θέτοντας έτσι σε κίνδυνο τη λειτουργία των subdomains, όπως τα δίκτυα οχημάτων ή οι έξυπνες πόλεις (Akram Abdul-Ghani et al., 2018; Kumar et al., 2016; Sheikh et al., 2019).

*FalseTiming attack*

Το FalseTiming attack συμβαίνει κατά μία Distributed DoS επίθεση. Κατά την επίθεση στέλνονται πακέτα σε συσκευές οι οποίες βρίσκονται κοντά μεταξύ τους σε απόσταση χωρίς όμως να έχουν συνδεθεί ξανά μεταξύ τους. Συνεπώς στέλνονται πακέτα χωρίς να υπάρχει η αποδοχή από τον χρήστη. Επίσης είναι δυνατό να γίνεται αλλαγή του adaptor σε συγκεκριμένα timeslots με σκοπό να στέλνονται πακέτα με μεγαλύτερη ταχύτητα, με αποτέλεσμα η εξάντληση της μπαταρίας αλλά και καταλαμβάνει την μνήμη της συσκευής μεγαλύτερη ταχύτητα, με

αποτέλεσμα η εξάντληση της μπαταρίας αλλά και καταλαμβάνει την μνήμη της συσκευής (Wan et al., 2021).

*Routing attacks*

Οι επιθέσεις που επηρεάζουν τον τρόπο δρομολόγησης των μηνυμάτων ονομάζονται επιθέσεις δρομολόγησης . Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει τέτοιες επιθέσεις για να πλαστογραφήσει, να ανακατευθύνει, να παραπλανήσει ή να απορρίψει τα πακέτα στην επικοινωνία επίπεδο. Ο απλούστερος τύπος επίθεσης δρομολόγησης είναι η επίθεση αλλοίωσης στην οποία ο επιτιθέμενος αλλάζει τις πληροφορίες δρομολόγησης, π.χ. δημιουργώντας βρόχους δρομολόγησης ή ψευδή μηνύματα σφάλματος.

Οι επιθέσεις δρομολόγησης αποτελούν απειλή κατά της εμπιστευτικότητα, υπευθυνότητας (accountability), μη άρνησης και ιδιωτικότητας (Mosenia & Jha, 2017). Οι Mosenia & Jha (2017) χωρίζουν τις επιθέσεις δρομολόγησης σε 5 κατηγορίες.

1. Black Hole: Η επίθεση ξεκινάει με ένα κακόβουλο κόμβο στον οποίο καταλήγει όλη η κίνηση του δικτύου, ο κακόβουλος κόμβος δείχνει στο δίκτυο ότι αυτός είναι ο συντομότερος κόμβος για την αποστολή πακέτων. Αποτέλεσμα τα πακέτα να ελέγχονται από τον κακόβουλο χρήστη και να τα διαχειρίζεται ή να τα απορρίπτει.
2. Gray Hole: Παρόμοια επίθεση με παραπάνω, η διαφορά είναι ότι κακόβουλοι κόμβοι απορρίπτουν πακέτα.
3. Worm Hole: Κλασσική επίθεση και αρκετά επικίνδυνη καθώς συμβαίνει και στα δίκτυα τα οποία δύναται να εγγυηθούν την αξιοπιστία τους. Ο επιτιθέμενος καταγράφει τα πακέτα που στέλνονται και έπειτα τα καθοδηγεί σε έναν διαφορετικό προορισμό.
4. Hello Flood: Σε μια επίθεση hello flood οι κόμβος μεταδίδει Hello packets για να δηλώσει την παρουσία του στους υπόλοιπους κόμβους του δικτύου. Παράλληλα οι κόμβοι που δέχονται δεδομένα είναι δυνατό να δεχθούν πακέτα τα οποία είναι κοντά μεταξύ τους. Ο επιτιθέμενος χρησιμοποιεί κόμβο με υψηλή ισχύ μετάδοσης για να στείλει Hello Packets σε όλους του υπόλοιπους κόμβους.

5. Sybil: Ο επιτιθέμενος χρησιμοποιεί sybil κόμβους οι οποίοι είναι κόμβοι με ψεύτικες ταυτότητες και έχουν την δυνατότητα να παρακάμψουν τους αξιόπιστους κόμβους σε ένα δίκτυο.Οι (Mosenia & Jha, 2017) προτείνουν αξιόπιστη δρομολόγηση ως αντίμετρο.

| **Έρευνα/ες** | **Επίθεση** | **Χαρακτηριστικά / Απόψεις** |
|---|---|---|
| Krishnan et al., (2017)<br>Akram Abdul-Ghani et al., (2018)<br>Kumar et al., (2016)<br>Nafrees et al., (2021)<br>Mosenia & Jha, (2017) | Eavesdropping (Near Field, RFID, Bluetooth, ZigBee) | Από τις πιο κλασσικές επιθέσεις όπου οι κακόβουλοι χρήστες με την χρήση ειδικού εξοπλισμού (υψηλής ισχύος κεραία ή αρκετά κοντινή απόσταση) ή και λογισμικού μπορούν να υποκλέψουν το σήμα. Πάραυτα είναι δυσκολότερο να υπάρξει υποκλοπή εάν ο RFID reader λειτουργεί σε passive mode και ο εκάστοτε χρήστης δημιουργεί το RF πεδίο σε άλλη συσκευή |
| Akram Abdul-Ghani et al., (2018)<br>Llaria et al., (2021)<br>Sheikh et al., (2019)<br>Nafrees et al., (2021)<br>Sun et al., (2014)<br>Mosenia & Jha, (2017)<br>Lv et al., (2021) | Replay Attack (Near Field, RFID, Bluetooth, ZigBee) | Στην συγκεκριμένη επίθεση ο εισβολέας αναπαράγει το σήμα το οποίο έχει «πιάσει» από μία εξουσιοδοτημένη συσκευή και το αναπαράγει ώστε να αποκτήσει πρόσβαση, με το αναγνωριστικό του αληθινού εξουσιοδοτημένου σήματος. Πιο συγκεκριμένα ο εισβολέας στέλνει, επανειλημμένα κακόβουλα δεδομένα αλλά και δεδομένα με καθυστέρηση. Σε αυτή την επίθεση συνήθως, πρώτα οι εισβολείς χρησιμοποιούν το Eavesdropping attack για να υποκλέψουν το σήμα. |
| Akram Abdul-Ghani et al., (2018) | Man in the middle Attack (MITM) (RFID, Near Field, | Ο κακόβουλος χρήστης έχει την δυνατότητα να υποκλέψει σε |

| | | |
|---|---|---|
| Kumar et al., (2016)<br>Krishnan et al., (2017)<br>Nafrees et al., (2021)<br>Sun et al., (2014)<br>Ma, (2021)<br>Lv et al., (2021) | WiFi) | πραγματικό χρόνο τα δεδομένα και να μπορέσει να τα προβάλει, αλλά και να τα διαχειριστεί, επιπρόσθετα μπορεί να έχει προσβασή στα δεδομένα της εκάστοτε συσκευής στην οποία πραγματοποιείται η επίθεση. Συνήθως υπάρχει ένας μεσάζοντας, δηλαδή μία συσκευή που ο κανονικός χρήστης έχει την εντύπωση ότι είναι αυθεντική και εξουσιοδοτημένη. Η συγκεκριμένη επίθεση δύναται να εκτελεστεί σε διάφορα μέσα WiFi , RFID κ.ο.κ (χαρακτηριστικό παράδειγμα είναι όταν ο εισβολέας μιμείται ένα WiFi access point). Στα έξυπνα κτήρια είναι εφικτό να προβάλει τα δεδομένα ενός αισθητήρα ή ενός μετρητή, συνήθως είναι δύσκολες επιθέσεις για να αναγνωριστούν |
| Akram Abdul-Ghani et al., (2018) | BlueBugging (Bluetooth) | Η επίθεση αυτή πραγματοποιείται μέσω ήδη infected συσκευών που κάνουν χρήση τρωτά σημεία πάνω στο firmware, με αποτέλεσμα να μπορεί ο κακόβουλος χρήστης να κατασκοπεύσει τις την συσκευή του θύματος. |
| Akram Abdul-Ghani et al., (2018)<br>Wan et al., (2021)<br>Llaria et al., (2021)<br>Kumar et al., (2016)<br>Krishnan et al., (2017)<br>Sheikh et al., (2019) | DoS – Denial of Service (Bluetooth, WiFi, RFID, Near Field) | Στην συγκεκριμένη επίθεση στέλνονται πολλά δεδομένα ταυτόχρονα. Σκοπός της επίθεσης να προκαλέσει στις συσκευές μεγάλο φόρτο κατά συνέπεια να τελειώσει η μπαταρία της συσκευής. Επιπρόσθετα τα DoS attacks έχουν |

| | | |
|---|---|---|
| Seferi Rifat & Giangiacomi Sofia, (2019)<br>dos Santos et al., (2021)<br>Nafrees et al., (2021)<br>Sun et al., (2014)<br>Mosenia & Jha, (2017) | | την δυνατότητα να μπλοκάρουν το δίκτυο και ταυτόχρονα να αποτρέπουν εξουσιοδοτημένους χρήστες να χρησιμοποιούν τις συσκευές. Παράδειγμα είναι τα TCLs (Thermostatically Controlled Loads) στα οποία δύναται να επιτευχθεί DoS επίθεση και να εμποδίσει την ομαλή λειτουργία των έξυπνων κτιρίων. Συνεπώς αν αποκτήσει πρόσβαση στην κεντρική μονάδα η οποία είναι υπεύθυνη για το HVAC δύναται να καθυστερούν οι πραγματικές μετρήσεις της θερμοκρασίας στο εκάστοτε κτήριο. |
| Wan et al., (2021)<br>Sun et al., (2014) | False Data Injection | Επίθεση κατά την οποία τα δεδομένα τα οποία στέλνονται είναι αλλαγμένα, με αποτέλεσμα απώλεια ακεραιότητας και αξιοπιστίας στα δεδομένα. |
| Seferi Rifat & Giangiacomi Sofia, (2019)<br>Akram Abdul-Ghani et al., (2018) | Spoofing (Bluetooth, RFID) | Συνήθεις επίθεση σε χαμηλής ενέργειας Bluetooth. Συγκεκριμένα εργαλεία τα οποία μπορούν να διαβάσουν το UUID της συσκευής και να την μιμηθούν με σκοπό να εισβάλουν στις υπηρεσίες που ήδη συνδεδεμένες με την συσκευή |
| Seferi Rifat & Giangiacomi Sofia, (2019)<br>Krishnan et al., (2017)<br>Akram Abdul-Ghani et al., (2018) | Fragmentation Attack (WiFi) | Αρχικά για να επιτύχει η συγκεκριμένη επίθεση πρέπει να έχει γίνει υποκλοπή στα πακέτα που στέλνονται, οπότε ένα μέρος της επίθεσης ξεκινάει με Eavesdropping Attack. Όλα τα πακέτα τα οποία στέλνονται σε δίκτυα 802.11 έχουν |

| | | |
|---|---|---|
| | | τα ίδια headers με αποτέλεσμα να μπορεί ο κακόβουλος χρήστης να προβλέψει τα πρώτα 8 bytes |
| Akram Abdul-Ghani et al., (2018) | The Hole196 Vulnerability (WiFi) | Στέλνοντας ένα ψεύτικο ARP request μαζί με το MAC address του access point στο οποίο θα αναγκάσει τους υπόλοιπους χρήστες να ανανεώσουν τα ARP tables και να συνδεθούν με το κακόβουλο access point, σκοπός είναι να αποκρυπτογραφήσει τα πακέτα που στέλνονται να τα διαβάσει και να κρυπτογραφήσει τα πακέτα με το δικό του κλειδί |
| Akram Abdul-Ghani et al., (2018) | ZED Sabotage Attack (ZigbBee) | Η συγκεκριμένη επίθεση κάνει χρήση του πρωτόκολλου ZigBee End Device κατα την οποία στέλνονται σήματα σε συγκεκριμένες χρονικές στιγμές με σκοπό να εξαντλήσει την μπαταρία της συσκευής |
| Sheikh et al., (2019)<br>Akram Abdul-Ghani et al., (2018)<br>Kumar et al., (2016) | Gateway Attacks | Στα gateway attacks κόβεται η σύνδεση μεταξύ των αισθητήρων και των συστημάτων διαχείρισης που συνδέονται στο διαδίκτυο. Είναι δυνατό αυτές οι επιθέσεις να συνοδεύονται από DoS επιθέσεις αλλά και Routing Attacks (Αναλύονται παρακάτω). Σκοπός της επίθεσης ή λανθασμένες πληροφορίες που λαμβάνονται στους αισθητήρες ή και κόμβους, καταστρέφοντας την αξιοπιστία των μετρήσεων. |

| | | |
|---|---|---|
| Wan et al., (2021) | FalseTiming Attack (Bluetooth) | Το FalseTiming attack χαρίζεται χαρακτηριστικά από το Distributed DoS. Στέλνονται πακέτα σε συσκευές οι οποίες βρίσκονται κοντά μεταξύ τους σε απόσταση χωρίς όμως να έχουν συνδεθεί ξανά μεταξύ τους. Συνεπώς στέλνονται πακέτα χωρίς να υπάρχει η αποδοχή από τον χρήστη. Επίσης είναι δυνατό να γίνεται αλλαγή του adaptor σε συγκεκριμένα timeslots με σκοπό να στέλνονται πακέτα με μεγαλύτερη ταχύτητα, με αποτέλεσμα η εξάντληση της μπαταρίας αλλά και καταλαμβάνει την μνήμη της συσκευής |
| Akram Abdul-Ghani et al., (2018)<br>Mosenia & Jha, (2017) | Routing Attacks | Επιθέσεις σαν τα routing attacks αναφέρονται στο πως επηρεάζονται τα πακέτα τα οποία στέλνονται. Πιο συγκεκριμένα, οι επιθέσεις αυτές χρησιμοποιούνται για να επηρεάσουν πακέτα να αλλάξουν τα περιεχόμενα, να καθυστερήσουν την παράδοση, να αλλάξουν τον τελικό προορισμό ή ακόμη και να μπλοκάρουν τα εξερχόμενα και εισερχόμενα πακέτα. Χαρακτηριστικό παράδειγμα είναι ότι ο κακόβουλος χρήστης αλλάζει τον προορισμό των πακέτων χρησιμοποιώντας επανάληψη δρομολόγησης ή στέλνοντας ψεύτικα μηνύματα λάθους. Οι επιθέσεις δρομολόγησης χωρίζονται |

σε 5 κατηγορίες.

Black Hole: Η επίθεση ξεκινάει με ένα κακόβουλο κόμβο στον οποίο καταλήγει όλη η κίνηση του δικτύου, ο κακόβουλος κόμβος δείχνει στο δίκτυο ότι αυτός είναι ο συντομότερος κόμβος για την αποστολή πακέτων. Αποτέλεσμα τα πακέτα να ελέγχονται από τον κακόβουλο χρήστη και να τα διαχειρίζεται ή να τα απορρίπτει.

Gray Hole: Παρόμοια επίθεση με παραπάνω, η διαφορά είναι ότι κακόβουλοι κόμβοι απορρίπτουν πακέτα.

Worm Hole: Κλασσική επίθεση και αρκετά επικίνδυνη καθώς συμβαίνει και στα δίκτυα τα οποία δύναται να εγγυηθούν την αξιοπιστία τους. Ο επιτιθέμενος καταγράφει τα πακέτα που στέλνονται και έπειτα τα καθοδηγεί σε έναν διαφορετικό προορισμό.

Hello Flood: Σε μια επίθεση hello flood οι κόμβος μεταδίδει Hello packets για να δηλώσει την παρουσία του στους υπόλοιπους κόμβους του δικτύου. Παράλληλα οι κόμβοι που δέχονται δεδομένα είναι δυνατό να δεχθούν πακέτα τα οποία είναι κοντά μεταξύ τους. Ο επιτιθέμενος χρησιμοποιεί κόμβο με υψηλή ισχύ μετάδοσης για να στείλει Hello Packets σε όλους του

| | |
|---|---|
| | υπόλοιπους κόμβους.<br>Sybil: Ο επιτιθέμενος χρησιμοποιεί sybil κόμβους οι οποίοι είναι κόμβοι με ψεύτικες ταυτότητες και έχουν την δυνατότητα να παρακάμψουν τους αξιόπιστους κόμβους σε ένα δίκτυο. |

*2.2.3 Communication - Protocol Based Attacks*

Τα communication based attacks όπως αναφέρονται και στα επιλεγμένα άρθρα αφορούν κυρίως τις επικοινωνίες μεταξύ IoT συσκευών. Πιο συγκεκριμένα τα μηνύματα τα οποία ανταλλάσσουν μεταξύ τους αλλά και ο έλεγχος των συσκευών. Σε αυτή την ενότητα θα αναπτυχθούν επιθέσεις στο transport layer το οποίο έχει τα πρωτόκολλα TCP και UDP. Έπειτα θα παρουσιαστούν επιθέσεις στο application layer στο οποίο κατηγοριοποιούνται τα πρωτόκολλα HTTP, MQTT και CoAP

*UDP Flood*

Σύμφωνα με τους Akram Abdul-Ghani et al. (2018), η επίθεση UDP flood είναι μία επίθεση DoS όπου ο επιτιθέμενος αποστέλλει έναν μεγάλο αριθμό UDP τυχαίων πακέτων σε διάφορες θύρες με σκοπό να τις αναγκάσει να στείλουν πίσω ICMP πακέτα και τελικά να καταστήσουν το αντικείμενο μη προσβάσιμο.

*TCP High jacking*

Σύμφωνα με τους Akram Abdul-Ghani et al. (2018), το πρώτο βήμα για την επίτευξη μιας επίθεσης TCP high jacking είναι η παρακολούθηση μιας συνεδρίας TCP. Σε αυτή την περίπτωση, ένας επιτιθέμενος μπορεί να ανιχνεύσει και να μαντέψει τους αριθμούς ακολουθίας και τα αθροίσματα ελέγχου των επικοινωνούντων οντοτήτων. Στη συνέχεια, ο επιτιθέμενος

μπορεί να εισάγει ένα κακόβουλο πακέτο TCP που περιέχει το άθροισμα ελέγχου και την ακολουθία που αναμένει ο παραλήπτης, ο οποίος δεν διαθέτει μηχανισμό για να επικυρώσει την πηγή του πακέτου θεωρώντας το ως νόμιμο.

*TCP SYN Flooding*

Σύμφωνα με τους Akram Abdul-Ghani et al. (2018), η επίθεση TCP SYN Flooding είναι η πιο δημοφιλής DoS επίθεση του πρωτοκόλλου TCP. Η επίθεση αυτή αποτελείται από ένα σύνολο υποκλαπέντων πακέτων TCP SYN που κατευθύνονται στην θύρα του θύματος. Οι διακομιστές Web, όπως οι διακομιστές ηλεκτρονικού ταχυδρομείου και οι διακομιστές FTP, και τα συνδεδεμένα αντικείμενα, είναι ευάλωτα σε τέτοιες επιθέσεις.

*Injecting Fraudulent packets*

Ένας εισβολέας μπορεί να εισάγει απατηλά πακέτα σε συνδέσεις επικοινωνίας χρησιμοποιώντας τρεις διαφορετικές μεθόδους επίθεσης: (i) insertion, (ii) manipulation και (iii) replication (ή replay). Στα σενάρια insertion, ο επιτιθέμενος εισάγει νέα πακέτα στην επικοινωνία του δικτύου. Με άλλα λόγια, μια επίθεση εισαγωγής έχει τη δυνατότητα να παράγει και να στέλνει κακόβουλα πακέτα που φαίνονται νόμιμα. Οι επιθέσεις χειραγώγησης περιλαμβάνουν τη σύλληψη του πακέτου και στη συνέχεια την τροποποίηση, π.χ, ενημέρωση των πληροφοριών επικεφαλίδας, του checksum και των δεδομένων, και αποστολή του παραποιημένου πακέτου. Στις επιθέσεις replication, ο επιτιθέμενος συλλαμβάνει τα πακέτα που έχουν ήδη ανταλλαγεί στο παρελθόν μεταξύ δύο «things» με σκοπό την αναπαραγωγή των ίδιων πακέτων. Γενικά, ένα stateless σύστημα, το οποίο δεν παρακολουθεί τα προηγούμενα πακέτα ή την προηγούμενη κατάσταση του συστήματος, είναι αρκετά ευάλωτο σε επιθέσεις replication. (Mosenia & Jha, 2017)

*SSL Stripping*

Το Secure Socket Layer (SSL) stripping αναπτύχθηκε για πρώτη φορά από τον Moxie Marlinspike (Akram Abdul-Ghani et al., 2018). Ο κύριος στόχος της τέτοιας επίθεσης είναι να

προσπαθήσει να αφαιρέσει τη χρήση του SSL/Transport Layer SSL/TLS (SSL/TLS), χειραγωγώντας μη κρυπτογραφημένα πρωτόκολλα για να απαιτούν τη χρήση του TLS. Πιο συγκεκριμένα, χειραγωγεί τόσο τα την κυκλοφορία HTTP όσο και τις σελίδες HTML κατά τη μετάδοσή τους. (Akram Abdul-Ghani et al., 2018)

*Beast*

Η επίθεση beast εξαρτάται σε μεγάλο βαθμό από την εκμετάλλευση των τρωτών σημείων του TLS 1.0, καθώς υλοποιεί Cipher Block Chaining (CBC). Έχοντας χρησιμοποιήσει το HTTP για την εκτέλεση μέσω TLS, ο επιτιθέμενος μπορεί να χρησιμοποιήσει το CBC για την αποκρυπτογράφηση είτε τμημάτων του μηνύματος είτε των cookies HTTP. (Akram Abdul-Ghani et al., 2018)

*Sniffing*

Η χρήση εφαρμογών sniffer μπορεί να βοηθήσει στην υποκλοπή ή παρακολούθηση της δικτυακής κίνησης για την απόκτηση πρόσβασης σε ευαίσθητα δεδομένα, ιδίως εάν τα πρωτόκολλα εφαρμογών έχουν υλοποιηθεί χωρίς μηχανισμό ασφαλείας, όπως το CoAP με no-security mode. (Akram Abdul-Ghani et al., 2018)

| **Έρευνα/ες** | **Επίθεση** | **Χαρακτηριστικά / Απόψεις** |
|---|---|---|
| Akram Abdul-Ghani et al., (2018) | UDP Flood | Το UDP flood δανείζεται χαρακτηριστικά από ένα κλασικό DoS attack ό επιτιθέμενος αποστέλλει πολλά UDP πακέτα σε διαφορετικές θύρες με σκοπό να τις αναγκάσει να στείλουν πίσω ICMP πακέτα και τελικά κάποιες να μην είναι προσβάσιμες. |
| Akram Abdul-Ghani et al., (2018) | TCP High jacking | Ο κακόβουλος χρήστης πρέπει να υποκλέψει μία συνεδρία TCP ώστε |

| | | |
|---|---|---|
| Llaria et al., (2021)<br>Lv et al., (2021) | | να μπορέσει να προβάλει και να μαντέψει την ακολουθία των check-sums. Έπειτα μπορεί να εισάγει το κακόβουλο πακέτο με το check sum χωρίς να υπάρχει στον προορισμό του τρόπος να ελεγχθεί εάν το πακέτο είναι αξιόπιστο. |
| Akram Abdul-Ghani et al., (2018) | TCP SYN Flooding | Η συγκεκριμένη επίθεση ξεκινάει με την υποκλοπή TCP SYN πακέτων τα οποία προορίζονται για τη συσκευή του θύματος της επίθεσης. Η συγκεκριμένη επίθεση είναι αρκετά επικίνδυνη Mail Servers και FTP servers |
| **Mosenia & Jha, (2017)** | Injecting Fraudulent packets | Ο εισβολέας είναι δυνατό να εισάγει αναξιόπιστα πακέτα στις επικοινωνίες μεταξύ IoT συσκευών όπως αναφέρθηκαν και παραπάνω. |
| Akram Abdul-Ghani et al., (2018) | SSL stripping | Σκοπός της επίθεσης είναι να βγάλει εκτός λειτουργίας το SSL/TLS ζητώντας από μη κρυπτογραφημένα πρωτόκολλα την χρήση TLS, για να επιτευχθεί αυτό ο κακόβουλος χρήστης την ώρα όπου μεταδίδονται τα HTTP requests και οι HTML σελίδες τα χειραγωγεί με στόχο να βγάλει εκτός λειτουργίας το SSL/TLS |
| Akram Abdul-Ghani et al., (2018) | Beast | Κάνοντάς χρήση των τρωτών σημείων του TLS 1.0. Ο επιτιθέμενος έχει την δυνατότητα αφού έχει προσπελάσει το TLS με HTTP requests όπως αναφέρθηκε παραπάνω, χρησιμοποιεί CBC |

| | | |
|---|---|---|
| | | (Cipher block chaining) για να αποκρυπτογραφήσει τα μηνύματα ή και HTTP cookies |
| Akram Abdul-Ghani et al., (2018) | Sniffing Attack | Κλασσική επίθεση υποκλοπής και παρακολούθησης της κίνησης του δικτύου χρησιμοποιώντας ειδικό λογισμικό για να αποκτήσει πρόσβαση ο κακόβουλος χρήστης σε ευαίσθητα δεδομένα. Σύμφωνα με την μελέτη εάν δεν έχει εγκατασταθεί σωστά το CoAP πρωτόκολλο και χωρίς να έχει ρυθμιστεί στην λειτουργία ασφάλειας, πρόκειται για μία εύκολη επίθεση παρακολούθησης του θύματος |

Σε αυτό το κομμάτι της ενότητας έχει γίνει μία βασική περιγραφή επιθέσεων σε IoT δίκτυα και συσκευές ενώ παράλληλα καθίσταται σαφές ότι η έρευνα των Akram Abdul-Ghani et al. (2018) είναι από τις μόνες η οποία περιγράφει τις επιθέσεις και τις ταξινομεί. Πιο συγκεκριμένα γίνεται ταξινόμηση σε επίπεδα όπως αναφέρθηκε παραπάνω, η έρευνα παρουσιάζει διεξοδικά επιθέσεις που είναι συνήθεις όχι μόνο σε IoT συσκευές και IoT δίκτυα αλλά και σε επίπεδο λογισμικού και λειτουργικού συστήματος όπως phising attacks, malware κ.ο.κ. Επιπρόσθετα παρουσιάζουν επιθέσεις σε Rest APIs (application programming interface) που πολλές εφαρμογές χρησιμοποιούν στη σύγχρονη εποχή για να αντλήσουν δεδομένα από τον backend server. Φυσικά αναφέρονται οι επιθέσεις στα δεδομένα όπως Data scavenging, Data manipulation, Data exposure και τρόποι που καταφέρνουν οι κακόβουλοι χρήστες να επιτυγχάνουν τέτοιου τύπο επιθέσεις όπως SQL injection, cross site scripting. Άξιο αναφοράς είναι το account hijacking attack όπου οι κακόβουλοι χρήστες χρησιμοποιούν τεχνάσματα κοινωνικής μηχανικής (social engineering) με σκοπό να αποσπάσουν πληροφορίες από τους χρήστες με τεχνικές που αναφέρθηκαν παραπάνω (phising). Συνεπώς, η μελέτη αναφέρει για την συγκεκριμένη επίθεση ότι η υπολογιστική νέφους (cloud computing) και APIs όπως SoAP,

REST και HTTP χρήζουν άμεσης βελτίωσης στους τρόπους με τους οποίους διαχειρίζονται τους αδύναμους κωδικούς πρόσβασης, την μη ορθή αυθεντικοποίηση του εκάστοτε χρήστη και τον έλεγχο των δεδομένων που εισάγονται (input data validation). Συμπερασματικά, η παρούσα έρευνα ταξινομεί τις επιθέσεις, προτείνει βασικούς τρόπους αντιμετώπισης, κατηγοριοποιεί όλες τις επιθέσεις και τις χαρακτηρίζει ανάλογα με την ζημία που προκαλεί (confidentiality, integrity, trustworthiness κτλ.).

Στην μελέτη των Bondarev & Prokhorov (2017) δεν αναλύονται επιθέσεις η οποίες δύναται να συμβούν σε ένα δίκτυο έξυπνου κτιρίου. Παρότι κατηγοριοποιούν τους τρόπους με τους οποίους μία έξυπνη οικία δύναται να διαχειριστεί, δεν υπάρχουν παραδείγματα επιθέσεων. Αναφέρονται κατηγοριοποιημένα σε τέσσερις κατηγορίες Equipment Failures, Software failures, network failures και ο ανθρώπινος παράγοντας. Τα συμπεράσματα της έρευνας είναι προβληματικά και δεν ανταποκρίνονται στον σκοπό των ερευνητικών ερωτημάτων που προκύπτουν. Προτείνεται η εγκατάσταση ενός φίλτρου το οποίο θα βρίσκεται πίσω από την τελική επικοινωνία με τον server χωρίς να δίνεται η δυνατότητα ξεχωριστών φίλτρων ανά αισθητήρα (όπου αναγράφεται φίλτρο, κάνοντας μία εκτίμηση αναφέρονται λογικά στο firewall). Συνεπώς οι συγγραφείς προτείνουν ότι το συγκεκριμένο concept είναι εύκολο στην εγκατάσταση, το κόστος είναι χαμηλό, ελέγχει λανθασμένα δεδομένα τα οποία παραλαμβάνει από τους αισθητήρες. Τέλος στα μειονεκτήματα αναφέρεται το γεγονός ότι υπάρχει ένα μόνο σημείο αποτυχίας (single point of failure) στην περίπτωση κυβερνοεπίθεσης ή και φυσικής φθοράς, εν αντιθέσει με τα firewalls που υπήρχαν στον εκάστοτε αισθητήρα ξεχωριστά. Συμπερασματικά, η έρευνα δεν είναι ολιστική και δημιουργεί περισσότερα ερωτήματα, άξιο αναφοράς είναι ότι δεν υπάρχουν πολλές πηγές για να υποστηρίξουν οι συγγραφείς τα λεγόμενα τους.

Οι ερευνητές στην μελέτη Brooks et al. (2020) προτείνουν μια σειρά από 23 πιθανές επιθέσεις στα συστήματα αυτοματισμού των έξυπνων κτιρίων. Πιο συγκεκριμένα η παρούσα έρευνα βασίζει τα ευρήματα της σε ένα ερωτηματολόγιο στο οποίο έλαβαν μέρος επαγγελματίες του χώρου από 38 χώρες και κατέταξαν με βαθμό επικινδυνότητας τις πιο σοβαρές επιθέσεις. Επισημαίνουν ότι στα συστήματα αυτοματισμού έξυπνων κτιρίων οι επιθέσεις

κατηγοριοποιούνται σε 3 κατηγορίες. Άρνηση (denial), Απώλεια (loss), Χειραγώγηση (Manipulation) στον έλεγχο και την ομαλή παρακολούθηση των συστημάτων. Καθίσταται σαφές, από την έρευνα ότι η συνδεσιμότητα των έξυπνων συσκευών στα έξυπνα κτίρια και η δυνατότητα αυτών σε επικοινωνία με το ευρύ διαδίκτυο δύναται να οδηγήσει σε απομακρυσμένες επιθέσεις αλλά και σε φυσικές επιθέσεις (field cyber attacks). Στην παρούσα μελέτη η παραπάνω κατηγοριοποίηση αναλύεται εκτενέστερα σε Αυτοματοποίηση (Automation), Πεδίο (Field) και Διαχείριση (Management). Οι 23 επιθέσεις είναι οι εξής ταξινομημένες με τον βαθμό επικινδυνότητας: χειροκίνητη παράκαμψη των ελεγκτών διακοπτών εξόδου, έλεγχος κίνησης δικτύου, κακόβουλη εισαγωγή δεδομένων στην κίνηση δικτύου, προγράμματα δικτύου ανοιχτού κώδικα, φυσική πρόσβαση σε ελεγκτή, εισαγωγή μη εξουσιοδοτημένης διαχειριστικής συσκευής, φυσική απενεργοποίηση ενός αισθητήρα ή ενεργοποιητή, παραβίαση του δικτύου αυτοματισμών, παρακολούθηση του δικτύου ΤΠΕ, μη ανιχνεύσιμη παραβίαση σε ελεγκτές, τοποθέτηση μη εξουσιοδοτημένου ελεγκτή, μη εξουσιοδοτημένη πρόσβαση στον κύριο υπολογιστή, εξαγωγή λανθάνουσας μνήμης ενός ελεγκτή, καταστροφή αισθητήρα ή ενεργοποιητή, μη εξουσιοδοτημένος επαναπρογραμματισμός ενός ελεγκτή, παράκαμψη εισόδων και εξόδων ενός ελεγκτή, παραβίαση δικτύου ΤΠΕ, απώλεια ρεύματος, καταστροφή ενός ελεγκτή, κυβερνοεπίθεση σε συσκευές επιπέδου διαχείρισης, με εξουσιοδοτημένος χειρισμός αισθητήρα ή ενεργοποιητή και αισθητήρα ασφαλείας.

Το άρθρο αναφέρεται σε πρακτικές αντιμετώπισης κρίσεων κυβερνοασφάλειας, μεταξύ άλλων αναφέρονται, η άμεση δράση, εκτίμηση των απειλών, σωματική ασφάλεια για πιθανούς εισβολείς, σχεδιασμός ανάκαμψης κρίσεων, συχνή συντήρηση συστημάτων καθώς και να ακολουθούνται τα τελευταία πρότυπα και οδηγίες.

Οι συγγραφείς της έρευνας αναφέρονται σε περιορισμούς όπου συνάντησαν, πρώτος περιορισμός είναι η έλλειψη σημασιολογίας και ορολογίας. Επιπρόσθετα, δεν υπάρχουν ξεκάθαρες πρακτικές αντιμετώπισης οι οποίες μπορούν να αξιοποιηθούν από τα δεδομένα της έρευνας, απόρροια της έλλειψης δεδομένων είναι η μη ορθή διατύπωση του ερωτήματος της έρευνας.

Στην μελέτη Wan et al. (2021) αναφέρονται σε δύο κύριες επιθέσεις σε VFAC (variable frequency air conditioner) και κυρίως σε TCLs (Thermostatically Controlled Loads)

αναφέρονται σε DoS και False Data Injection attacks. Οι ερευνητές αναπτύσσουν μοντέλο το οποίο περιγράφει μαθηματικά την τα TCLs στα έξυπνα κτήρια.

Οι ερευνητές στην μελέτη Llaria et al. (2021) αναφέρονται πλήρως σε όλο το θεωρητικό επίπεδο για την λειτουργία των BEMS (Building energy management systems) και κατ' επέκταση για την σύνδεση των έξυπνων κτιρίων στο έξυπνο δίκτυο ηλεκτροδότησης. Αφού έχουν παραθέσει όλο το θεωρητικό υπόβαθρο, αναφέρονται στις επικοινωνίες μεταξύ των έξυπνων συσκευών. Επιπρόσθετα αναλύουν τα ζητήματα ασφάλειας τα οποία προκύπτουν στα συγκεκριμένα συστήματα και παρουσιάζουν επιθέσεις με βάση το OSI μοντέλο. Παράλληλα, ταξινομούν τις επιθέσεις ανάλογα με τον βαθμό επικινδυνότητας (Confidentiality, Integrity, Availability). Τέλος παραθέτουν τρόπους κατά τους οποίους δύναται να αντιμετωπιστούν οι επιθέσεις οι οποίες αναφέρονται, προτείνουν ειδικές λύσεις και συστήματα ανίχνευσης. Πρόκειται για μία ολοκληρωμένη μελέτη η οποία παρουσιάζει προβλήματα και λύσεις.

Η μελέτη των Kumar et al. (2016) αναφέρονται σε επιθέσεις στα διαδίκτυα των πραγμάτων. Παραθέτουν θεωρητικό υπόβαθρο και αναπτύσσουν τα επίπεδα των IoT δικτύων (Application Layer, Perception Layer, Network Layer, Physical Layer). Έπειτα ταξινομούν τις επιθέσεις ανάλογα με το επίπεδο στο οποίο βρίσκονται και δίνουν βασικούς ορισμούς των επιθέσεων. Επιπρόσθετα παραθέτουν πίνακα ο οποίος αναφέρεται σε ήδη υπάρχουσες μεθόδους για να αποτρέπουν τις επιθέσεις που παρουσιάζουν, αναφέρονται λύσεις αλλά και περιορισμοί που προκύπτουν.

Οι συγγραφείς στην μελέτη Krishnan et al. (2017) αρχικά αναφέρονται στην αρχιτεκτονική του συστήματος και επικεντρώνονται περισσότερα στους τρόπους επικοινωνίας (RFID, NFC, Bluetooth, WiFi, Zigbee). Πιο συγκεκριμένα ταξινομούν επιθέσεις με βάση τα πρωτόκολλα επικοινωνίας δίνοντας βασικά χαρακτηριστικά της εκάστοτε επίθεσης. Τέλος παραθέτουν βασικές λύσεις για τις επιθέσεις που αναφέρονται.

Η έρευνα των Sheikh et al. (2019) πραγματεύεται ένα μοντέλο για την αναγνώριση λαθών σε συστήματα HVAC των έξυπνων κτηρίων. Παραθέτουν θεωρητικό υπόβαθρο και αναλύουν τα επίπεδα των BMS (building management systems). Επιπρόσθετα παρουσιάζουν δύο επιθέσεις στα BMS, την επίθεση DoS και Replay attack. Οι συγγραφείς ανέπτυξαν μοντέλα μηχανικής μάθησης για να κατηγοριοποιήσουν και να ανιχνεύσουν τις επιθέσεις.

Το άρθρο των Seferi Rifat & Giangiacomi Sofia (2019) παραθέτει τρωτά σημεία και επιθέσεις. Πιο συγκεκριμένα αναφέρονται σε τρία τρωτά σημεία τα οποία βρίσκονται στα έξυπνα κτήρια. Αυτά είναι το Bluetooth 5.0, Proprietary solutions με τις οποίες αναφέρονται σε λύσεις που δεν συμμορφώνονται με τα διεθνή πρωτόκολλα επικοινωνίας. Έπειτα παρουσιάζουν τέσσερις επιθέσεις με βάση τα τρωτά σημεία τα οποία αναφέρουν στην μελέτη τους. Ειδικότερα αναφέρουν το Reverse Engineering, Social Engineering, Eavesdropping, και Falsetiming attack. Δεν παρουσιάζονται διεξοδικές λύσεις για τις επιθέσεις και τα τρωτά σημεία τα οποία αναφέρονται. Στα συμπεράσματα οι συγγραφείς το αναφέρουν ξεκάθαρα ότι η μελέτη τους δύναται να οδηγήσει σε μία ευρύτερη έρευνα με ανάπτυξη λύσεων.

Στην συγκεκριμένη μελέτη των Kruthika Rathinavel et al. (2017) όπως αναφέρθηκε και στο κεφάλαιο 1.7 ρίσκο προκατάληψης, παρουσιάζεται ένα σύστημα BAS (building automation system) το οποίο είναι εφικτό να παρακολουθεί και να αποτρέπει κοινές επιθέσεις στα έξυπνα κτήρια. Η συγκεκριμένη μελέτη όπως και αναφέρθηκε κρίθηκε ως μελέτη η οποία δύναται να εκμεταλλεύεται οικονομικά, συνεπώς τα αποτελέσματα και οι λύσεις που προκύπτουν πρέπει να λαμβάνονται με προσοχή.

Στη μελέτη των dos Santos et al. (2021) αναφέρονται στις εφικτές επιθέσεις ανά συγκεκριμένες κατηγορίες. Ειδικότερα αναφέρονται σε τρωτά σημεία και εκμετάλλευση αυτών στον έξυπνο φωτισμό, στα κλειστά συστήματα παρακολούθησης. Επιπλέον αναπτύσσουν πείραμα σε εργαστήριο για να εξετάσουν τα τρωτά σημεία και να εκμεταλλευτούν τις ατέλειες των συστημάτων. Συμπερασματικά δόθηκε θεωρητικό υπόβαθρο για την αρχιτεκτονική των συστημάτων, με σκοπό να δοκιμαστεί σε συνθήκες εργαστηρίου η θεωρητική γνώση. Οι συγγραφείς καταλήγουν στο γεγονός ότι τα BAS (building automation systems) είναι εξίσου σημαντικά ως προς την ασφάλεια και την αξιοπιστία όπως και τα βιομηχανικά συστήματα διαχείρισης.

Στην μελέτη των Nafrees et al. (2021) οι συγγραφείς αναφέρονται ολιστικά σε όλους τους τομείς των έξυπνων πόλεων. Όσον αφορά τα έξυπνα κτήρια υπάρχει πίνακας στον οποίο αναφέρονται οι απειλές και προτεινόμενες λύσεις. Οι επιθέσεις που αναφέρονται δεν καλύπτουν όλες τις συσκευές ενός έξυπνου κτηρίου (Fuzzing attack, HVAC Attack, Cascading Attack, Man in the middle).

Η συγκεκριμένη μελέτη των Sun et al. (2014) παρουσιάζονται διεξοδικά όλες οι επιθέσεις που αφορούν τα ασύρματα δίκτυα. Η μελέτη κατηγοριοποιεί τις επιθέσεις με βάση τα OSI layers. Αναλύουν διεξοδικά τις επιθέσεις, και παρουσιάζουν τα χαρακτηριστικά της εκάστοτε επιθέσεις. Άξιο αναφοράς είναι ότι παρουσιάζουν και μέτρα προστασίας αλλά και καλές πρακτικές για την αποφυγή επικίνδυνων επιθέσεων.

Όπως αναφέρθηκε και στην μελέτη των Akram Abdul-Ghani et al. (2018) η παρούσα μελέτη των Mosenia & Jha (2017) παρουσιάζει όλων των τύπων επιθέσεων στα δίκτυα IoT και τα κατηγοριοποιεί με βάση το μοντέλο της Cisco το οποίο αποτελείται από 7 επίπεδα τα οποία περιγράφουν τα IoT δίκτυα. Επιπρόσθετα, κατηγοριοποιούν τις επιθέσεις με βάση το που ακριβώς αποσκοπούν (confidentiality, integrity, trustworthiness κτλ.). Έπειτα αναλύουν τρόπους αντιμετώπισης συγκεντρωτικά για κάθε επίπεδο του μοντέλου Cisco.

Οι συγγραφείς στην μελέτη Lv et al. (2021) πραγματεύονται λύσεις για την αντιμετώπιση των επιθέσεων με την χρήση τεχνητής νοημοσύνης. Η έρευνα τους προτείνει αυθεντικοποίηση των χρηστών μέσω ενός αλγορίθμου τεχνητής νοημοσύνης (χρησιμοποιούν ελλειπτικό μοντέλο κρυπτογράφησης). Παραθέτουν θεωρητικό υπόβαθρο για επιθέσεις στις επικοινωνίες μεταξύ συσκευών IoT. Έπειτα παρουσιάζουν το δικό τους μοντέλο αξιοποιώντας τεχνολογία τεχνητής νοημοσύνης.

Η μελέτη των Wei et al. (2021) παρουσιάζει ένα αναλυτικό μοντέλο για επιθέσεις τύπου jamming attacks πάνω στο πρότυπο IEEE 802.11.

Παρακάτω ακολουθεί συγκεντρωτικός πίνακας με όλες τις πληροφορίες ανά μελέτη. Παρουσιάζονται οι επιθέσεις, οι τρόποι αντιμετώπισης και τυχόν περιορισμοί που δηλώθηκαν στις έρευνες. Σκοπός του πίνακα είναι μια top level προσέγγιση με στόχο τον γρήγορο εντοπισμό πληροφοριών ανά μελέτη αλλά φυσικά και τις διαφορές που προκύπτουν.

*Συγκεντρωτικός πίνακας επιθέσεων ανά μελέτη*

| **Έτος Δημοσίευσης** | **Τίτλος μελέτης** | **Τρόποι επιθέσεων και τρωτά σημεία** | **Τρόποι αντιμετώπισης** | **Επιθέσεις που αναφέρονται** | **Περιορισμοί** |
|---|---|---|---|---|---|
| 2020 | Intelligent building systems: security and facility professionals' understanding of system threats, vulnerabilities and mitigation practice | Στην μελέτη παρουσιάζονται 23 τρωτά σημεία και βαθμολογούνται από ειδικούς για τον βαθμό επικινδυνότητας | Δίνονται γενικοί τρόποι αντιμετώπισης κρίσεων σε γενικά πλαίσια χωρίς να υπάρχει συγκεκριμένη πρακτική | Manual override of controllers output switches, Automation network traffic monitoring, Automation network traffic data injection, Automation level open source network programs, Physical access to a controller, Insertion of an unauthorised management level device, Physical disconnection of a sensor or actuator, Tampering with the automation network, Monitoring the ICT network, No tamper detection on controllers, Insertion of an unauthorised controller ,Unauthorised access to workstation, Extraction of a controller's latent memory, Damaging a sensor or actuator, Unauthorised programming of a controller, Overriding a controller outputs or inputs, Tampering with the ICT network, Loss of mains power, Damaging a controller, Cyberattack on the management level device, | Έλλειψη σημασιολογίας και ορολογία, μη ξεκάθαρες πρακτικές αντιμετώπισης λόγω μη σωστής διατυπωμένης ερώτησης στην έρευνα |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Damage a management level device, Manipulation of a sensor or actuator, Manipulation of security sensor (detector) | |
| 2018 | A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model | Γίνεται ταξινόμηση των επιθέσεων ανά κατηγορία και εξετάζονται όλες οι πιθανές επιθέσεις | Προσφέρουν για κάθε επίθεση τρόπους αντιμετώπισης | Physical-based Attacks: Object Replication Attack, RF interference, Hardware Trojan, Object Jamming, Physical Damage, Camouflage, Malicious Node Injection, Object tampering, Social engineering, side-channel attack, malicious code injection, tag cloning. Protocol-based Attacks: Replay, Spoofing, Tracking, Unauthorized access, Virus, Man in the middle, Killing Tag, Relay attack, data corruption, data modification, data insertion, Bluesnarfing, BlueBugging, BlueJacking, DoS & DDoS, Interception, Hijacking, FMS attack, Korek attack, Chopchop attack, Fragmentation attack, PTW attack, Google Replay attack, Michael Attacks, Ohigashi- | Παρότι υπάρχουν αρκετές επιθέσεις οι οποίες χρήζουν εξειδικευμένη εξήγηση στην συγκεκριμένη μελέτη οι συγγραφείς είχαν στόχο την ταξινόμηση, κατηγοριοποίηση και την παρουσίαση εκτεταμένων λύσεων |

| | |
|---|---|
| | Morii Attack, Hole196 Vulnerability, Dictionary attack, Obtaining the key, ZED sabotage attack. Network Protocol Based attacks: Selective forward attack, sinkhole attack, sybil, wormhole, blackhole, identity, hello flooding, Authentication attack, confidentiality attack. Communication protocol-based attacks: TCP-UDP port scan, UDP Flood, TCP Highjacking, TCP SYN flooding, TCP-UDP fragmentation, Pre shared key attack, Sniffing attack, SSL stripping, beast, Diffie-Hellman Parameters, Klima03, Time, Padding Oracle, Xmpp bomb, XMPPloit, Buffer overflow. Data-at REST Based: Data exposure, data loss, account highjacking, Data scavenging, Data leakage, Data manipulation, Virtual Machine Escape, VM Hopping, Malicious VM, Insecure VM migration, Brute-force attack, Hash collision. IoT Software-based attacks: Malicious code |

| | | | | | |
|---|---|---|---|---|---|
| | | | | injection, Path based DoS, Reprogram attack, Malwares. OS – based attacks: Phising, backdoors, Virus worm attacks, Brute force search attack. Firmware based attacks: Control Highjacking, Reverse Engineering. | |
| 2021 | Throughput Analysis of Smart Buildings-oriented Wireless Networks under Jamming Attacks | Παρουσιάζεται μόνο το Jamming attack στο πρότυπο 802.11 | Αναπτύσσεται αναλυτικό μοντέλο για την αναγνώριση επιθέσεων | Jamming Attack | - |
| 2021 | AI-empowered IoT Security for Smart Cities | Δίνονται πληροφορίες για χρήση ενός μοντέλου τεχνητής νοημοσύνης με σκοπό την αναγνώριση επιθέσεων | Προστασία προκύπτει από το μοντέλο το οποίο αναπτύσσεται | Eavesdropping, Replay Attack, DoS, Man in the middle | - |
| 2021 | Distributed Event-Based Control for Thermostatically Controlled Loads Under Hybrid Cyber Attacks | Στο παρόν άρθρο αναπτύσσεται μοντέλο για Thermostatically Controlled Loads, υποστηρίζουν δύο κύριες επιθέσεις | Το μοντέλο που αναπτύσσεται μπορεί να προβλέψει αλλά και να ανιχνεύσει τυχόν ανωμαλίες κατά την λειτουργία του | DoS, False Data Injection | Μελλοντικά έργα δύναται να ερευνήσουν τον ομαλό διαμοιρασμό ενέργειας σε TCLs στα οποία μπορούν να χρησιμοποιούν πιο εξελιγμένους τρόπους επικοινωνίας και σχεδιασμού |
| 2017 | Analysis of Internal Threats of the System "Smart Home" and Assessment of Ways to Prevent Them | Προτείνεται ένας διαφορετικός τρόπος εγκατάστασης για firewalls σε αισθητήρες | Αναφέρονται τα πλεονεκτήματα και οι τρόποι με τους οποίους μπορεί να βοηθήσει η προτεινόμενη εγκατάσταση | Packet loss, data corruption, Collision | Single point of failure όπως και η ακαταλληλότητα σε ένα decentralized σύστημα |

| | | | | | |
|---|---|---|---|---|---|
| 2021 | Intelligent Buildings in Smart Grids: A Survey on Security and Privacy Issues Related to Energy Management | Αναφορά επιθέσεων στα BEMS συστήματα των έξυπνων κτηρίων ταξινομημένα στο OSI | Αναφέρουν τον τομέα στον οποίο η κάθε επίθεση στοχεύει, παράλληλα προτείνεται υπό την μορφή βιβλιογραφίας μέτρα αντιμετώπισης | Physical: Jamming, TSA, MAC: Collision, Exhaustion, Denial of sleep, Masquerading, Network: Selective forwarding/blackhole/Sinkhole/ Hello flood/ Sybil/ Router advertisement flooding, wormhole, puppet, Application: Desynchronization, flooding, stack smashing, control command, alert message, injection, Data tampering | - |
| 2016 | Security in Internet of Things: Challenges, Solutions and Future Directions | Ταξινόμηση επιθέσεων στο κατά το μοντέλο OSI | Δίνονται στοχευμένες λύσεις σε μορφή πινάκων | Application layer attacks: Malicious Code Attacks, Tampering with node-based apps, Inability to receive security patches, hacking into the smart meter or grid, Perception layer attacks: Eavesdropping, Sniffing attacks, noise in data, Network layer attacks: Gateway attacks, Storage attacks, Injecting fake information, DoS, Physical layer attacks: Physical damage, environmental attacks, loss of power, hardware failure, physical tampering, | - |

| | | | | | |
|---|---|---|---|---|---|
| 2017 | Security Considerations for IoT in Smart Buildings | Έχουν χωρίσει τις επιθέσεις ανάλογα με το πρωτόκολλο επικοινωνίας RFID, WiFi, Zigbee κτλ. | Γενικές προτάσεις ασφάλειας χωρίς εξειδικευμένη αιτιολόγηση | RFID: Eavesdropping, Physical attacks, DoS, Spoofing, Zigbee: Replay attack, Eavesdropping, Data manipulation or injection, WiFi: Man in the Middle, Eavesdropping, DoS, Packet Re-routing. | - |
| 2019 | Cyber Attack and Fault Identification of HVAC System in Building Management Systems | Μοντέλο αναγνώρισης επιθέσεων σε HVAC συστήματα | Ανάπτυξη και πρόταση μοντέλου για την έγκαιρη αναγνώριση επιθέσεων | DoS attack, Replay Attack | - |
| 2019 | Vulnerabilities and Attacks in a Smart Buildings Scenario | Αναφέρονται σε επιθέσεις που πραγματοποιούνται μέσω Bluetooth, Επαναχρησιμοποίηση έτοιμου κώδικα, αλλά και λύσεις οι οποίες δεν συμμορφώνονται με τα διεθνή μέσα | Δεν παρουσιάζονται | Reverse engineering, Social engineering, Eavesdropping, FalseTiming | - |
| 2017 | Security Concerns and Countermeasures in IoT-Integrated Smart Buildings | Παρουσιάζεται σύστημα το οποίο διαχειρίζεται όλο το έξυπνο κτήριο, και προσφέρει ασφάλεια σε κοινές επιθέσεις | Αναφέρονται στους τρόπους με τους οποίους το σύστημα προστατεύει το έξυπνο κ | - | - |
| 2020 | Leveraging operational technology and the Internet of things to attack smart buildings | Αναπτύσσονται σενάρια στα οποία εξετάζονται γνωστά τρωτά σημεία, όπως συστήματα έξυπνου φωτισμού, κλειστών | - | Malware, DoS, Tampering | - |

| | | | | | |
|---|---|---|---|---|---|
| | | κυκλωμάτων κτλ. | | | |
| 2021 | Smart Cities: Emerging technologies and Potential solutions to the Cyber security threads | Αναφέρονται επιθέσεις στα έξυπνα κτήρια αλλά παραθέτουν οι συγγραφείς και επιθέσεις σε έξυπνες πόλεις, έξυπνες δομές υγείας κτλ. | Παρουσιάζονται σε μορφή πίνακα προτεινόμενες λύσεις και μέτρα προστασίας | Fuzzing Attack, HVAC Attack, Cascading Attack, Man in the middle. | Προτείνουν λύσεις εγκαθίδρυσης blockchain τεχνολογιών διότι τα malware και DoS attacks γίνονται ολοένα και πιο συχνά σε έξυπνες δομές και IoT δίκτα |
| 2014 | A Review of Attacks and Security Protocols for Wireless Sensor Networks | Στην συγκεκριμένη μελέτη οι συγγραφείς κατηγοριοποιούν τις επιθέσεις στα ασύρματα δίκτυα αισθητήρων στο OSI μοντέλο | Παρουσιάζονται εκτενής λύσεις ανά επίπεδο OSI | Physical layer: Jamming, Eavesdropping, Tampering. MAC: Collision, Exhaustion, Unfairness. Network layer: Neglect, Homing, Misdirection, Blackholes. Transport layer: Flooding, Desynchronization. Application layer: Repudiation, Data corruption. Multi-layer attacks: DoS, Impersonation Delay, Man in the middle. | Μελέτη στην οποία οι συγγραφείς στοχεύουν στο ευρύ κοινό και όχι σε εξειδικευμένους επαγγελματίες |
| 2017 | A Comprehensive Study of Security of Internet-of-Things | Εκτενής μελέτη στις επιθέσεις σε δίκτυα IoT. Χρησιμοποιούν το μοντέλο με τα 7 επίπεδα της Cisco για κατηγοριοποίηση των επιθέσεων | Λύσεις και πρακτικές για κάθε επίπεδο | Edge node: Hardware trojan, side-channel attacks, DoS, Outage attacks, Tampering, Node replication, Camouflage, Malicious nodes, Tracking, Tag cloning, Counterfeiting, Eavesdropping. Communication: Injection | - |

| | | |
|---|---|---|
| | | Fraudulent packets, DoS, Eavesdropping, Routing Attacks: Black hole, Gray hole, worm hole, Hello Flood, Sybil. Edge computing level: Malicious injection, Integrity attacks against machine learning, |

## *3. Σύνθεση Β*

Στη παρούσα ενότητα θα αναπτυχθούν τρόποι αντιμετώπισης και θα αναλυθούν κυρίως οι έρευνες που στοχεύουν σε λύσεις. Πρακτικά σημαίνει ότι οι έρευνες που επιλέχθηκαν για αυτή την ενότητα παρουσιάζουν μοντέλα, λύσεις, frameworks με σκοπό την αναγνώριση, την πρόβλεψη και την αντιμετώπιση σοβαρών επιθέσεων σε δίκτυα IoT και κατ' επέκταση σε έξυπνα κτίρια. Παρόμοια, με την σύνθεση Α θα αναπτυχθούν τα βασικά σημεία της εκάστοτε μελέτης και θα παρουσιαστεί σχετικός συγκεντρωτικός πίνακας.

Τέσσερις έρευνες (Pan et al., 2016; Patil et al., 2019; Al-Sudani, Zhou, Liu, et al., 2018; Elnour et al., 2021) αναπτύσσουν, αναφέρονται ή παρουσιάζουν μοντέλα επιθέσεων ή προσομοιώσεων επιθέσεων σε συστήματα αυτοματισμού έξυπνων κτηρίων. Οι Patil et al. (2019) μάλιστα χρησιμοποιούν μοντέλο μηχανικής μάθησης για να πετύχουν τον σκοπό τους, την αναγνώριση λαθών σε building management systems αλλά και κυβερνοεπιθέσεων σε έξυπνα κτήρια. Οι Al-Sudani, Zhou, Wen, et al. (2018) είναι οι μόνοι που προτείνουν ένα framework, το SCARA, για την αυθεντικοποίηση των χρηστών που χρησιμοποιούν RFID tags μέσω cloud. Αναγνωρίζουν τρεις βασικούς ρόλους και δεν χρησιμοποιούν την αυθεντικοποίηση μέσω φωτογραφιών όπως οι Al-Sudani, Zhou, Liu, et al. (2018). Οι υπόλοιπες έρευνες (Krundyshev Vasiliy & Kalinin Maxim, 2019; Osisiogu Ukachi, 2019)(Mikhaylov et al., 2013; Hyman et al., 2019; Wall et al., 2019) αναφέρονται κατά κόρον σε τρόπους αντιμετώπισης και μέτρα έναντι των επιθέσεων. Παρακάτω, αναλύεται η κάθε έρευνα και αναφέρονται με μεγαλύτερη λεπτομέρεια τα σημαντικά σημεία της.

Η μελέτη των Pan et al. (2016) αρχικά αναφέρεται σε ένα μοντέλο επιθέσεων για τα συστήματα αυτοματισμού έξυπνων κτηρίων. Πιο συγκεκριμένα, στην παρούσα μελέτη ερευνούν την αναγνώριση ανωμαλιών στα συστήματα αυτοματισμού. Για αυτό το λόγο χρησιμοποιούν δεδομένα που έχουν αντλήσει από τα προαναφερθέντα συστήματα. Έπειτα, αναφέρουν τις πηγές των δεδομένων οι οποίες είναι: η χειροκίνητη επιλογή δεδομένων, η συλλογή δεδομένων για την εκάστοτε συσκευή (όπως ώρα, ημερομηνία), το σήμα GPS για την φυσική τοποθεσία της συσκευής και η εξαγωγή δεδομένων από την ροή των πακέτων (χρησιμοποιήσαν τα Headers και το payload των πακέτων). Τέλος, έχουν αντλήσει περιγραφικά δεδομένα τα οποία

δημιουργήθηκαν υπολογιστικά. Αυτό σημαίνει ότι συγκέντρωσαν το συνολικό αριθμό κίνησης πακέτων σε συγκεκριμένη χρονική στιγμή, τυχόν καθυστερήσεις ανάμεσα σε λειτουργίες, τα logs από συσκευές αισθητήρων, actuators και controllers και τα logs για να παρατηρήσουν την δραστηριότητα του δικτύου. Χρησιμοποιήσαν τον αλγόριθμο Decision tables για την κατηγοριοποίηση των επιθέσεων αλλά και των επιτιθέμενων συσκευών. Όλα τα δεδομένα έχουν αντληθεί από fog assets χρησιμοποιώντας δύο μορφές δεδομένων PCADS και S-DNA. Παρακάτω ακολουθεί πίνακας με τα αποτελέσματα της έρευνας. Σκοπός της έρευνας είναι να χρησιμοποιηθεί το μοντέλο για την έγκαιρη αναγνώριση επιθέσεων στα BACS συστήματα.

| Κατηγορία επίθεσης | Ποσοστό αναγνώρισης | Ποσοστό False Positive | Ακρίβεια ταξινόμησης επίθεσης | Προτεινόμενες δράσεις |
|---|---|---|---|---|
| Who-is / Who – has Attack | 98.59% | 0% | 100% | Απόρριψη ανώμαλων πακέτων |
| Write property attack | 99.43% | 0.41% | 100% | Απόρριψη ανώμαλων πακέτων |
| Write property Multiple attack to fire controller | 100% | 0% | 100% | Απόρριψη ανώμαλων πακέτων |
| Write property Multiple attack to gate controller | 99.41% | 3.32% | 100% | Απόρριψη ανώμαλων πακέτων |
| Flooding Conformed Attack | 99.81 | 0% | 100% | Διακοπή σύνδεσης |
| I-Am attack for protocol | 92.23% | 0% | 100% | Απόρριψη κίνησης |
| I am attack for sensors | 93.00% | 0% | 100% | Απόρριψη δεδομένων |

Στη μελέτη τους οι Al-Sudani, Zhou, Wen, et al. (2018) προτείνουν ένα framework το οποίο ονομάζεται SCARA. Σκοπός είναι η αυθεντικοποίηση των χρηστών που χρησιμοποιούν RFID tags μέσω cloud. Στο προτεινόμενο framework τρεις είναι οι βασικοί ρόλοι που περιγράφονται: ο Issuer, ο server και η συσκευή ανάγνωσης RFID. Ο Issuer ουσιαστικά εκδίδει μοναδικά κλειδιά χρησιμοποιώντας κρυπτογραφημένο κανάλι επικοινωνίας. Έπειτα γίνεται η αυθεντικοποίηση. Άξιο αναφοράς αποτελεί το γεγονός ότι μόνο ο αναγνώστης RFID βρίσκεται σε τοπικό υπολογιστή ενώ τα υπόλοιπα μέρη λειτουργούν στο cloud. Παρότι το framework που αναπτύχθηκε από τους συγγραφείς χαρακτηρίζεται ως ασφαλές, δεν έχει ερευνηθεί αν η επίθεση tag tampering μπορεί να περάσει τον έλεγχο ασφαλείας. Επιπρόσθετα, αναφέρεται ότι αν κάποια από τα κλειδιά διαρρεύσει υπάρχει η δυνατότητα να αποκρυπτογραφηθούν τα κλειδιά αλλά και πάλι το σύστημα δεν θα μπορέσει να διαχειριστεί την αυθεντικοποίηση.

Οι ερευνητές Krundyshev Vasiliy & Kalinin Maxim (2019) αναλύουν και προτείνουν μεθόδους για να αναγνωριστούν false data injection επιθέσεις σε έξυπνες δομές και κατ' επέκταση στα έξυπνα κτήρια. Αρχικά θεσπίζουν το θεωρητικό υπόβαθρο για τις false data injection επιθέσεις. Δίνουν τέσσερις βασικές μεθοδολογίες για την αναγνώριση τέτοιου τύπου επιθέσεων. Η πρώτη μέθοδος αναφέρεται στο Correlation approach η οποία είναι η σχέση των αρχικών δεδομένων του αισθητήρα αλλά και της κατάστασης του συστήματος που βρίσκεται. Η μεθοδολογία αυτή θέτει ένα όριο αν ξεπεραστεί τότε η λειτουργία του συστήματος χαρακτηρίζεται μη φυσιολογική, οι ανωμαλίες στις μετρήσεις ελέγχονται όλες μαζί και όχι σε μεμονωμένα συστήματα. Η δεύτερη μέθοδος αφορά στο Behavioral analysis approach, ουσιαστικά πρόκειται για IDS (Intrusion Detection Systems) τα οποία είναι πολύπλοκα και σχετικά δύσκολα στο να αναπτυχθούν, όσο για την ανάλυση χρειάζονται δεδομένα για την εκάστοτε συσκευή. Η τρίτη μέθοδος αναφέρεται στο Classification δηλαδή στην μέθοδο της κατηγοριοποίησης. Σε αυτή την μέθοδο υπάρχει έτοιμη μία βάση δεδομένων με patterns τα οποία προσπαθεί ο αλγόριθμός να ταιριάξει ώστε να κατηγοριοποιηθεί η επίθεση, σαφώς σε μεγάλη κλίμακα υπάρχουν αποκλίσεις και πολλές φορές χάνονται μοτίβα. Τέλος η τέταρτη μέθοδος αναφέρεται στην αναγνώριση ανωμαλιών με τεχνητή νοημοσύνη. Αρχικά το σύστημα εκπαιδεύεται στο να μπορεί να εντοπίζει επιθέσεις, αρκετά πολύπλοκη μέθοδος η οποία είναι προβληματική για μεγάλης κλίμακας εγκαταστάσεις.

Επιστρέφοντας στην μελέτη η μέθοδος η οποία προτείνουν βασίζεται στην συσχέτιση χωρικών και χρονικών δεδομένων ως βάση. Γενικότερα η μέθοδος τους βασίζεται σε συσχετίσεις και αναφέρονται 2 από αυτές. Η πρώτη είναι ότι υπάρχει συσχέτιση δεδομένων σε κοντινούς αισθητήρες, και η δεύτερη υποστηρίζει ότι τα δεδομένα τα οποία παράγουν αισθητήρες που είναι κοντά μεταξύ τους μπορούν να εντοπίσουν την ίδια ανωμαλία στο σύστημα. Για αυτούς τους λόγους χρησιμοποιήθηκε παραλλαγή της μεθοδολογίας k-NN, η μέθοδος χωρίστηκε σε δύο φάσεις, η πρώτη είναι η αναγνώριση spatial μοτίβων και failure detection. Τα δεδομένα τα οποία χρησιμοποίησαν προήλθαν από το UMass Trace Repository με 97% ακρίβεια 1.9% false negatives και 1.1% false positives.

Η μελέτη του Osisiogu Ukachi (2019) πρόκειται για μία ανασκόπηση στην οποία αναφέρονται τρόποι αντιμετώπισης σε φυσικές εγκαταστάσεις και έξυπνα κτήρια. Δίνονται έξι λύσεις και καλές πρακτικές για την αντιμετώπιση cyber-physical επιθέσεων.

Η έρευνα των Patil et al. (2019) πραγματεύεται τη χρήση μοντέλου μηχανικής μάθησης με σκοπό την αναγνώριση λαθών σε BMS (Building management systems) αλλά και κυβερνοεπιθέσεων σε έξυπνα κτήρια. Συνολικά αναγνωρίζονται τρεις καταστάσεις η πρώτη αφορά την ομαλή λειτουργία, η δεύτερη λάθη που συνέβησαν κατά την λειτουργία και η τρίτη αναφέρεται στην επίθεση του συστήματος. Στο data set που χρησιμοποιούν υπάρχουν τρία σενάρια με τις παραπάνω λειτουργίες, ενώ στο τέταρτο υπάρχει συνδυασμός λαθών, επίθεσης και κανονικής λειτουργίας. Χρησιμοποιήθηκαν τέσσερις μέθοδοι εκμάθησης, Random Forest, Support Vector Machine (SVM) K-nearest neighbor και bagging tree. Παρακάτω υπάρχει ο πίνακας με τα αποτελέσματα.

| Σενάριο | Random Forest | SVM | k-NN | Bagging Tree |
|---|---|---|---|---|
| Case1 | 100% | 100% | 65.6% | 99.5% |
| Case 2 | 100% | 100% | 68% | 100% |
| Case 3 | 100% | 100% | 65.6% | 99.5% |
| Case 4 | 98.6% | 98.6% | 45.8% | 97.2% |

Η συγγραφείς αναφέρουν ότι η k-NN μέθοδος έχει το μεγαλύτερο ποσοστό false-positive ενώ η SVM αποδεικνύεται πιο αξιόπιστη μέθοδος.

Συνεχίζοντας, οι Al-Sudani, Zhou, Liu, et al. (2018) αναπτύσσουν μοντέλο για αυθεντικοποίηση των χρηστών πριν εισέλθουν σε ένα κτήριο. Πιο συγκεκριμένα εκτός από την κλασική αναγνώριση με RFID tags χρησιμοποιούν και κάμερα με την οποία φωτογραφίζουν τον χρήστη που θέλει να εισέλθει και αποστέλλουν την φωτογραφία για αυθεντικοποίηση στον server. Στην ίδια λογική λειτουργεί και η αυθεντικοποίηση του RFID tag, και τα δύο (φωτογραφία και αναγνωριστικό του RFID tag) αποθηκεύονται στην βάση δεδομένων. Έπειτα παρουσιάζουν δύο αλγόριθμους που χρησιμοποίησαν κατά την έρευνα. Ο πρώτος αφορά το RFID collision το οποίο δύναται να συμβεί όταν υπάρχουν σε κοντινή απόσταση RFID readers και scanners, ο αλγόριθμος ονομάζεται Adaptive collision free tag identification algorithm (ACTIA), εφόσον περάσουν οι έλεγχοι ο δεύτερος αλγόριθμος ξεκινάει να τρέχει και αφορά την κάμερα, ονομάζεται Image Matching Algorithm (IMA), στέλνεται στον server η φωτογραφία και αναλύει τα χαρακτηριστικά του. Για να δοκιμάσουν τον αλγόριθμο και την αξιοπιστία του χρησιμοποίησαν Data set από την AT&T, με accuracy 71,94%. Τέλος οι περιορισμοί οι οποίοι δηλώνουν οι συγγραφείς αφορούν το πείραμα το οποίο πραγματοποιήθηκε σε συνθήκες εργαστηρίου και δεν υπάρχουν δεδομένα για χρήση στον πραγματικό κόσμο, επιπρόσθετα αναφέρουν ότι το dataset το οποίο χρησιμοποίησαν για την αναγνώριση προσώπου είναι γενικό και δεν γνωρίζουν εάν θα υπάρχει η ίδια ακρίβεια σε διαφορετικά χαρακτηριστικά προσώπου.

Στη μελέτη των Mikhaylov et al. (2013) αρχικά αναφέρονται δύο ιοί που πλήττουν τα συστήματα αυτοματισμού των έξυπνων κτιρίων. Πιο συγκεκριμένα, αναφέρουν για ιούς που επιτίθονται με σκοπό να αποσπάσουν πληροφορίες, όπως να κατασκοπεύσουν τους ενοίκους μίας έξυπνης οικίας, ή και την δραστηριότητα τους στο διαδίκτυο ή και αρχεία τα οποία στέλνουν στους εκτυπωτές. Επιπλέον αναφέρουν ιούς που στοχεύουν στην διαχείριση του έξυπνου κτηρίου, για παράδειγμα οι επιτιθέμενοι να έχουν την δυνατότητα να απενεργοποιούν συναγερμούς ή και να ξεκλειδώνουν πόρτες κ.ο.κ. Έπειτα προτείνουν ένα σύστημα προστασίας για τα συστήματα αυτοματισμών των έξυπνων κτηρίων το οποίο αναφέρει τα εξής: ανάλυση του συστήματος για την παρουσία μη αυθεντικοποιημένων συσκευών αλλά και συνδέσεων, ανίχνευση μη αυθεντικοποιημένων συσκευών και ύποπτες τερματικές εντολές από συνδεδεμένες συσκευές, ανίχνευση διάφορων δραστηριοτήτων όπως κακόβουλα πακέτα ύποπτες δραστηριότητες κτλ., ανάλυση διαφορετικών συχνοτήτων δικτύου για ανίχνευση μετάδοσης δεδομένων, αρχειοθέτηση από τα logs συσκευών, εκτέλεση αυτοματοποιημένων ελέγχων σε βάσεις δεδομένων για ύποπτες παραμέτρους ή και σετ παραμέτρων, εφαρμογή γραφικής

απεικόνισης του συστήματος αυτοματισμού παρουσιάζοντας την δραστηριότητα των συσκευών. Τέλος, τα προβλήματα τα οποία λύνει το προτεινόμενο σύστημα είναι τα εξής: προστασία του συστήματος αυτοματισμού το οποίο έχει εγκατασταθεί σε μετάδοση δεδομένων σε γραμμές ρεύματος (X10), σε συνεστραμμένο ζεύγος (KNX, C-Bus, Ethernet), σε μετάδοση μέσω αέρα (WiFI, Bluetooth).

Η μελέτη των Hyman et al. (2019) αναφέρεται στα SCADA δίκτυα, επιπρόσθετα αναφέρουν την σημαντικότητα του ανθρώπινου παράγοντα και πως η τεχνητή νοημοσύνη μπορεί να βοηθήσει στην ανίχνευση λαθών και αναξιοπιστίας στα SCADA. Εν συνεχεία, προτείνουν 21 μέτρα ασφαλείας τα οποία είναι τα εξής: συχνοί τεχνικοί έλεγχοι σε συσκευές στα δίκτυα SCADA για τον εντοπισμό προβλημάτων ασφαλείας, αξιολόγηση επιπέδου ασφαλείας απομακρυσμένων τοποθεσιών που συνδέονται σε SCADA δίκτυα, δημιουργία κόκκινων και μπλε ομάδων για την δοκιμή επιθέσεων σε SCADA, καθορισμός ευθυνών από τους χρήστες, αυστηρή και συνεχής διαδικασία διαχείρισης κινδύνων, συστηματική εγγραφή backups και διαχείριση ανάκαμψης από καταστροφές, κατασκευή ειδικών πολιτικών και πραγματοποίηση κύκλων εκπαιδεύσεων για την ελαχιστοποίηση κίνδυνου από προσωπικό του οργανισμού να διαρρεύσει από λάθος ευαίσθητες πληροφορίες, λειτουργίες και ελέγχους ασφαλείας.

Στην μελέτη των Elnour et al. (2021) παρουσιάζεται HVAC μοντέλο προσομοίωσης, με το οποίο οι ερευνητές προσομοιάζουν ένα 3-όροφο κτήριο με 12 ζώνες. Τα δεδομένα τα οποία χρησιμοποίησαν εκτείνονται σε χρονική περίοδο 4 μηνών ενώ το δεύτερο data set σε διάστημα 20 ημερών. Στο συγκεκριμένο μοντέλο προσπάθησαν να προσομοιώσουν 4 επιθέσεις. Η πρώτη αφορά την αλλαγή των προκαθορισμένων setpoints του συστήματος το οποίο μπορεί να αλλαχθεί μόνο από διαχειριστές ή μηχανικούς. Η δεύτερη επίθεση αναφέρεται στις μετρήσεις των αισθητήρων, χρησιμοποίησαν man in the middle επίθεση κατά την οποία οι αισθητήρες δεν είχαν την δυνατότητα να παραδώσουν σε πραγματικό χρόνο μετρήσεις. Η τρίτη επίθεση αναφέρεται στην μετάδοση λανθασμένων σημάτων διαχείρισης με σκοπό οι επιτιθέμενοι να καταστρέψουν αντλίες ή ανεμιστήρες ή και θερμοκρασίες όπως και στην δεύτερη επίθεση. Τέλος, στην τέταρτη επίθεση ήταν η τροποποίηση των εντολών προς τις συσκευές, αυτό σημαίνει ότι είχαν τη δυνατότητα να αλλάξουν την λειτουργία συγκεκριμένων συσκευών και να προκαλέσουν ζημιά σε άλλα εξαρτήματα. Χρησιμοποιήθηκαν επτά αλγόριθμοι για να

δοκιμαστεί αν το μοντέλο τους δύναται να αναγνωρίσει επιθέσεις. Παρακάτω υπάρχει πίνακας με τα αποτελέσματα για τον εκάστοτε αλγόριθμο

| Μέθοδος | kNN | LOF(Local outlier factor) | PCA | OCSVM(One class support vector machine) | IF-based model | PCA-IF | 1D CNN-IF |
|---|---|---|---|---|---|---|---|
| Ακρίβεια | 37.33% | 38.07% | 47.40% | 97.78% | 80.93% | 90.01% | 68.85% |
| Recall | 100% | 100% | 93.85% | 17.10% | 50.40% | 60.49% | 74.28% |

Το μοντέλο τους οι συγγραφείς το αποκαλούν semi-supervised, 4 από τις παραπάνω μεθόδους έδωσαν θετικά αποτελέσματα και με σχετικά χαμηλό false alarm. Επίσης το μοντέλο κατάφερε να εντοπίσει σοβαρές επιθέσεις κατά του HVAC συστήματος. Τέλος αναφέρεται ότι στο μοντέλο δεν συμπεριλήφθηκαν επιθέσεις τύπου DoS.

Η έρευνα των Wall et al. (2019) προτείνει μία software defined λύση για την αναγνώριση επιθέσεων στα συστήματα αυτοματισμού των έξυπνων κτηρίων. Πιο συγκεκριμένα, η αρχιτεκτονική του συστήματος που προτείνεται είναι τα εξής: SC (security controller) as Proxy για την ασφαλή αναβάθμιση των συσκευών, εγκατάσταση ειδικών ασφαλών ρυθμίσεων, προσεκτική επιλογή μηχανισμών αυθεντικοποίησης, ανίχνευση εισβολών βασισμένη στην παρακολούθηση των συσκευών, δοκιμή διάφορων τρωτών σημείων σε εφαρμογές. Εμβαθύνοντας στην έρευνα, το μοντέλο το οποίο προτείνεται χρησιμοποιεί έναν κεντρικό controller ο οποίος είναι υπεύθυνος για όλες τις συσκευές του κτηρίου. Αρχικά ο μηχανισμός αναβάθμισης δρα σαν ένας θάλαμος ασφαλείας προτού οι κατασκευαστές στείλουν για παράδειγμα ένα firmware update καταφέρνοντας να το διασταυρώσει και να μην επιτρέπει αποστολές αρχείων από μη αυθεντικοποιημένες πηγές. Η διαχείριση αυθεντικοποίησης προτείνεται να αποτελείται από το πρωτόκολλο oAuth. Επιπρόσθετα, οι συγγραφείς προτείνουν την κρυπτογράφηση της κίνησης, καθώς και την διαφοροποίηση των συσκευών σε ένα ξεχωριστό MAC-layer το οποίο θα λαμβάνει όλα τα requests από αξιόπιστους και μόνο χρήστες. Η ανίχνευση εισβολών εγγράφει δεδομένα τα οποία θα τα διαχειρίζεται το σύστημα. Τέλος αναφέρεται το Configuration Check, και τα Security policies.

## 3.1 Συγκεντρωτικός πίνακας

| **Έτος δημοσίευσης** | **Τίτλος Μελέτης** | **Κύρια Ιδέα** | **Μοντέλα Μηχανικής Μάθησης /Frameworks** | **Συνολικό Ποσοστό Ακρίβειας** | **Περιορισμοί** |
|---|---|---|---|---|---|
| 2016 | Anomaly Behavior Analysis for Building Automation Systems | Αναγνώριση μοτίβων επιθέσεων σε συστήματα αυτοματισμού έξυπνων κτιρίων | Decision Tables | 95% | - |
| 2018 | SCARA: A Framework for Secure Cloud-Assisted RFID Authentication for Smart Building Access Control | Προτείνεται framework για την διαχείριση RFID tags και την αυθεντικοποίηση αυτών | SCARA | - | Δεν έχει ερευνηθεί το tag tampering |
| 2019 | Prevention of false data injections in smart infrastructures | Αναγνώριση false data injection επιθέσεις σε συστήματα αυτοματισμού έξυπνων κτηρίων | k-NN, SVM, Fuzzy neural network | 86% | - |
| 2019 | A Machine Learning Approach to Distinguish Faults and Cyberattacks in Smart Buildings | Πρόταση μοντέλου μηχανικής μάθησης για την αναγνώριση επιθέσεων σε BMS | Random Forest, k-NN, SVM, Bagging Tree | 90% (k-NN είχε αρκετά χαμηλή ακρίβεια) | k-NN μικρή ακρίβεια σε σχέση με τους υπόλοιπους αλγόριθμους |
| 2018 | Detecting Unauthorized RFID | Ανάπτυξη μοντέλου | Προτείνονται αλγόριθμοι κατασκευής των συγγραφέων όπως (IMA) Image Machine | 70% | Το πείραμα πραγματοποιήθηκε σε |

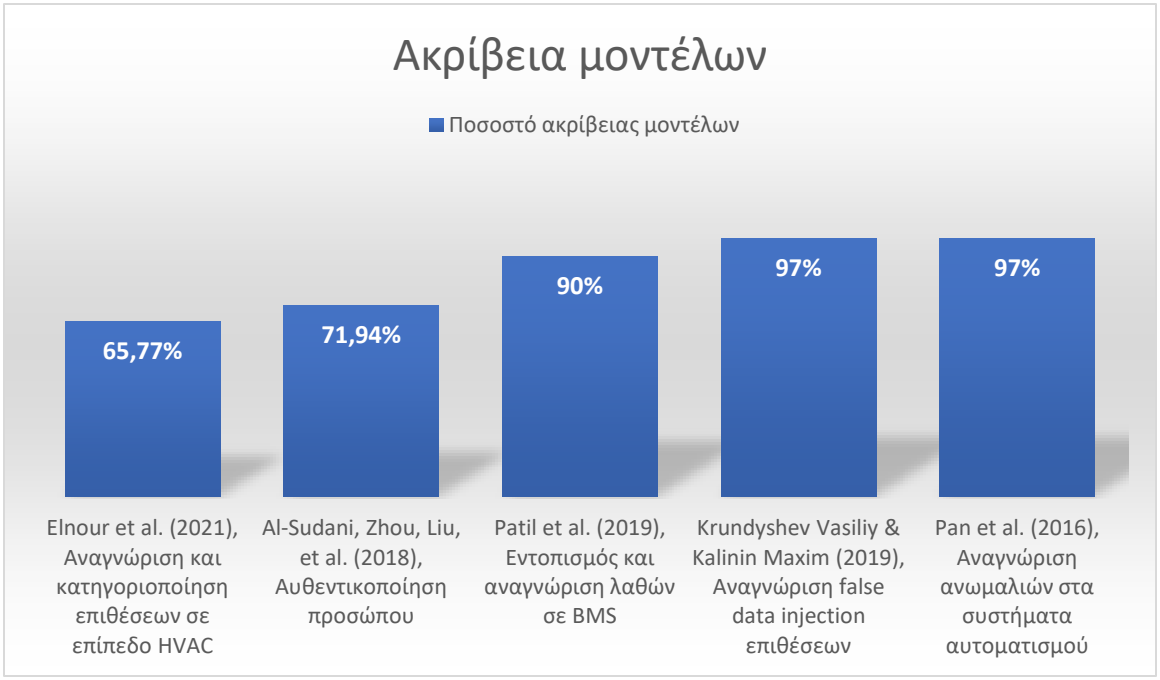
| | | | | | |
|---|---|---|---|---|---|
| | Tag Carrier for Secure Access Control to a Smart Building | αυθεντικοποίησης χρηστών σε RFID εγκαταστάσεις με προσθήκη αναγνώρισης προσώπου | Algorithm | | συνθήκες εργαστηρίου και δεν υπάρχουν δεδομένα για χρήση στον πραγματικό κόσμο, επιπρόσθετα αναφέρουν ότι το dataset το οποίο χρησιμοποίησαν για την αναγνώριση προσώπου είναι γενικό και δεν γνωρίζουν εάν θα υπάρχει η ίδια ακρίβεια σε διαφορετικά χαρακτηριστικά προσώπου |
| 2013 | Method and System for Protection of Automated Control Systems for “Smart Buildings” | Αναφορά μεθοδολογίας με σκοπό την ασφάλεια των έξυπνων κτιρίων | - | - | - |
| 2019 | Secure Controls for Smart Cities; Applications in Intelligent Transportation Systems and Smart Buildings | Προτείνουν 21 τρόπους για να επιτευχθεί ασφάλεια στα δίκτυα SCADA | - | - | - |
| 2021 | Application of data-driven attack detection framework for secure operation in smart buildings | Παρουσιάζεται μοντέλο προσομοίωσης το οποίο αναφέρεται σε HVAC, προσομοιάζονται 4 | kNN, LOF(Local outlier factor), PCA, OCSVM(One class support vector machine), IF-based model, PCA-IF, 1D CNN-IF | 65% | Αναφέρεται ότι στο μοντέλο δεν συμπεριλήφθηκαν επιθέσεις τύπου DoS |

| | | | | | |
|---|---|---|---|---|---|
| | | επιθέσεις | | | |
| 2019 | Software-Defined Security Architecture for Smart Buildings using the Building Information Model | Προτείνεται μία software defined λύση για την αναγνώριση επιθέσεων στα συστήματα αυτοματισμού των έξυπνων κτηρίων | - | - | - |

## *3.2 Συγκεντρωτικός πίνακας απόδοσης αλγορίθμων μηχανικής μάθησης*

| ***Επιθέσεις/Αλγόριθμοι*** | **k-NN** | **Decision Tables** | **Random Forest** | **Bagging Tree** | **Support Vector Machine** | **LOF (Local Outlier Factor)** | **PCA** | **OCSVM (One class support vector machine)** | **IF-based model** | **PCA-IF** | **1D CNN-IF** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Who-is / Who – has Attack* | | 98.59% | | | | | | | | | |
| *Write property attack* | | 99.43% | | | | | | | | | |
| *Αναγνώριση και κατηγοριοποίηση επιθέσεων σε επίπεδο HVAC* | 37.33% | | | | | 38.07% | 47.40% | 97.78% | 80.93% | 90.01% | 68.85 % |
| *Write property Multiple attack to fire controller* | | 100% | | | | | | | | | |
| *Συνδυασμός λαθών, επίθεσης και κανονικής λειτουργίας BMS* | 45.8% | 98.6% | | 97.2% | 98.6% | | | | | | |
| *Write property Multiple attack to gate controller* | | 99.41% | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Flooding Conformed Attack* | | 99.81% | | | | | | | | | |
| *I-Am attack for protocol* | | 92.23% | | | | | | | | | |
| *I am attack for sensors* | | 93.00% | | | | | | | | | |
| *False – data Injection* | 97% | | | | | | | | | | |
| *Λάθη που συνέβησαν κατά την λειτουργία BMS* | 65.6% | 100% | | 99.5% | 100% | | | | | | |



# *4. Οδηγός αντιμετώπισης*

Όπως διαπιστώθηκε από την παρούσα μελέτη, υπάρχουν πολλοί τρόποι ένας κακόβουλος χρήστης να αποκτήσει πρόσβαση στις λειτουργίες της οικίας ή και ολόκληρου του κτηρίου. Η κρίσιμη ερώτηση είναι πως δύναται να προστατευτούμε από τέτοιες επιθέσεις. Η απάντηση δυστυχώς δεν είναι ολοκληρωμένη, πάντοτε θα υπάρχει τρόπος και zero-day vulnerabilities τα οποία θα γίνονται exploit από έμπειρους κακόβουλους χρήστες. Πάραυτα υπάρχει τρόπος να καθυστερήσουμε την διείσδυση και να δυσκολέψουμε πιθανούς εισβολείς. Συνεπώς, στη συγκεκριμένη ενότητα, προτείνονται διάφοροι τρόποι που προκύπτουν από την παραπάνω μελέτη με σκοπό την προστασία ενός έξυπνου κτηρίου.

Αρχικά είναι σημαντικό τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται σε συσκευές και συστήματα διαχείρισης να αποτελούνται και να συμμορφώνονται με τα διεθνή πρότυπα επικοινωνίας της IEEE. Είναι σημαντικό να μην υπάρχουν proprietary πρωτόκολλα τα οποία δεν είναι ελεγμένα από διεθνής φορείς. Κατ’ επέκταση και από την πλευρά των κατασκευαστών η επαναχρησιμοποίηση έτοιμου κώδικα και βιβλιοθήκες η οποίες είναι ξεπερασμένες συμβάλουν στη μείωση της ασφάλειας.

Συνεχίζοντας, προτείνεται η συναλλαγή πληροφοριών σε απομακρυσμένους servers ή στο cloud μέσω κρυπτογραφημένων επικοινωνιών και συνεχείς αυθεντικοποίηση των πακέτων, φυσικά πρόσβαση σε αυτές τις λειτουργίες δύναται να έχουν δύο άτομα, καθώς μεγαλύτερος αριθμός σημαίνει μεγαλύτερο ρίσκο. Πιο συγκεκριμένα, είναι γνωστό ότι ένα RFID tag είναι τόσο εύκολο να αντιγραφεί από φορητές συσκευές οι οποίες λαμβάνουν και αντιγράφουν την ταυτότητα και παριστάνουν το αυθεντικό tag (βλ. Εικόνα 1). Η παρακάτω συσκευή είναι διαθέσιμη για όλους και έχει την δυνατότητα να γράφει RFID tags και να εκτελεί replay attacks- φυσικά πρόκειται για  μία από τις πολλές λειτουργίες που προσφέρει. Συνεπώς, είναι σημαντικό πάντα να υπάρχει ένα token και ένα challenge κατά την ανάγνωση ενός RFID tag το οποίο να γίνεται αυθεντικοποίηση στο cloud.

Όσον αφορά τα συστήματα διαχείρισης των έξυπνων κτηρίων, είναι υψίστης σημασίας να διαθέτουν, επεξεργασία δεδομένων σε πραγματικό χρόνο. Πρέπει να υπάρχουν προ-εγκατεστημένοι αλγόριθμοί ή αλλιώς Intrusion Detection Algorithms με τους οποίους

ανιχνεύονται έγκαιρα ανωμαλίες στις λειτουργίες των αισθητήρων, ειδοποιούν εγκαίρως τους διαχειριστές, με σκοπό την εκκίνηση διαδικασιών, για την αναγνώριση της ζημίας κ.ο.κ. Όπως αναφέρθηκε παραπάνω είναι σημαντικό και σε αυτή την κατηγορία η επεξεργασία να γίνεται off-site σε cloud servers.


*Εικόνα 1- https://www.minimachines.net/actu/flipper-zero-91486 (2022)*

Στην εποχή μας η αναγνώριση και η κατηγοριοποίηση επιθέσεων με μοντέλα μηχανικής μάθησης βρίσκεται στην άνθηση της, και πρέπει να το εκμεταλλευτούν οι κατασκευαστές και οι διαχειριστές έξυπνων κτηρίων.

Όπως αναφέρουν και οι παραπάνω μελέτες, δεν πρέπει συσκευές οι οποίες είναι υψίστης σημασίας για την αυθεντικοποίηση χρηστών να βρίσκονται σε περιοχές στις οποίες δεν υπάρχει παρακολούθηση, διότι ο κακόβουλος χρήστης έχει την ευκαιρία να πραγματοποιήσει ένα object tampering attack. Να αλλάξει δηλαδή τη συσκευή, αισθητήρα με μία ακριβώς ίδια αλλά με σκοπό να τρέχει κακόβουλο λογισμικό και να αποτελεί τον δούρειο ίππο του δικτύου. Συνεπώς, προτείνεται η συνεχής αυθεντικοποίηση των συσκευών (αυτοματοποιημένη καθημερινή διαδικασία) και η εγγραφή όταν μία συσκευή, χωρίς υπαρκτό λόγο απενεργοποιείται ή αποσυνδέεται από το δίκτυο, ενημερώνοντας τους εκάστοτε φορείς.

Συμπερασματικά, όλα τα δίκτυα και τα συστήματα όπως αναφέρθηκε είναι προσπελάσιμα, αλλά περισσότερο και άλλα λιγότερο. Καθίσταται σαφές ότι η επεξεργασία

εγγραφή και οι κρυπτογραφημένες διαδικασίες δεν πρέπει να τρέχουν σε local επίπεδο, πρέπει να υπάρχει πλήρης εμπιστοσύνη στους cloud providers. Είναι σημαντικό να υπάρχει συνεχής αυθεντικοποίηση και με οποιαδήποτε αλλαγή να ειδοποιούνται οι διαχειριστές. Εάν συμβεί προσπέλαση του συστήματος θα πρέπει η ζημία να είναι όσο δυνατόν μικρότερη, για αυτό το λόγο είναι σημαντικοί οι off-site servers και οι μέθοδοι αυθεντικοποίησης που χρησιμοποιούν οι providers. Έπειτα οι διαχειριστές πρέπει να είναι όσο το δυνατόν μικρότεροι στον αριθμό και συνήθως να μην έρχονται σε επαφή με το ευρύ κοινό που εισέρχεται ή εξέρχεται από το κτήριο, διαφορετικά δημιουργείται σοβαρός κίνδυνος για τεχνικές social engineering οι οποίες φυσικά είναι εκτός του εύρους της συγκεκριμένης διπλωματικής.

# *5. Συμπεράσματα*

Στην παρούσα διπλωματική εργασία σκοπός ήταν να συγκεντρωθεί όσο περισσότερη πληροφορία είναι εφικτή για τις επιθέσεις σε έξυπνα κτήρια, τα οποία ολοένα και περισσότερο βρίσκονται στην καθημερινή ζωή μας είτε υπό την μορφή ενός gadget είτε ενός ολοκληρωμένου συστήματος για την οικεία μας. Παρουσιάστηκαν επιθέσεις σε όλα τα επίπεδα και μοντέλα αναχαίτησης επιθέσεων από κακόβουλους χρήστες. Παρά τις προσπάθειες όλων αυτών των ερευνών ένα σημαντικό σημείο ήταν ξεκάθαρο καθ’ όλη την διάρκεια της έρευνας. Το σημείο/πρόταση αν θέλετε είναι ότι πάντα θα βρεθεί τρόπος για να παραβιαστούν τα συστήματα αυτοματοποίησης και πάντα οι κακόβουλοι χρήστες θα είναι ένα βήμα μπροστά. Για αυτό τον λόγο σε αυτή την εργασία παρουσιάστηκαν μοντέλα μηχανικής μάθησης τα οποία δύναται να αναγνωρίζουν μοτίβα και να προλαμβάνουν επιθέσεις σε πρώιμα στάδια. Πιο συγκεκριμένα, είναι σχεδόν απαραίτητο στη σύγχρονη εποχή να στηριζόμαστε σε συστήματα τεχνητής νοημοσύνης και μηχανικής μάθησης ώστε να υποδεικνύουν στον ανθρώπινο παράγοντα τις μαινόμενες επιθέσεις.

Εν συνεχεία, στο κομμάτι των επιθέσεων παρότι υπάρχουν σημαντικές έρευνες οι οποίες συμβάλουν στην ταξινόμηση τους και κατηγοριοποίηση, πολλές από αυτές είναι ήδη ξεπερασμένες και η σκήνη της κυβερνοασφάλειας έχει ήδη προχωρήσει. Σχεδόν καθημερινά τρωτά σημεία ανακαλύπτονται οπότε είναι οριακά ανέφικτο τα επιστημονικά άρθρα να έχουν τα

κατάλληλα άμεσα αντανακλαστικά για άμεση δημοσίευση. Συνεπώς, ιστορικά μιλώντας οι έρευνες που επικεντρώνονται σε επιθέσεις έχουν αρκετά στοιχεία και καλύπτουν το βασικό θεωρητικό υπόβαθρο.

Αναφέροντας τα παραπάνω λοιπόν, είναι σημαντικό οι έρευνες να στραφούνε περισσότερο στην αντιμετώπιση με μεθόδους μηχανικής μάθησης (όπως και έχει γίνει), αλλά και σε έρευνες οι οποίες αναφέρονται σε προτάσεις για την ασφάλεια συγκεκριμένων συσκευών. Για την προαναφερθείσα πρόταση, στην παρούσα διπλωματική υπήρχαν τέτοιου τύπου μελέτες οι οποίες προτείναν αλλαγές για την καλύτερη ασφάλεια των συστημάτων, χωρίς όμως να υπάρχει έρευνα σε εργαστηριακές συνθήκες για να τεκμηριώσει τα λεγόμενα των συγγραφέων. Οι προτάσεις είναι ευπρόσδεκτές αρκεί να τεκμηριώνονται με έρευνα και δεδομένα.

Τέλος, η βιβλιογραφία καλύπτει ιστορικά ένα μεγάλο κομμάτι επιθέσεων αλλά όπως αναφέρθηκε χρειάζονται περισσότερες έρευνες και μελέτες για την αντιμετώπιση κρίσιμων επιθέσεων στις έξυπνες οικίες.

# *Βιβλιογραφία*


Akram Abdul-Ghani, H., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 9, Issue 3). www.ijacsa.thesai.org

Al-Sudani, A. R., Zhou, W., Liu, B., Almansoori, A., & Yang, M. (2018). Detecting Unauthorized RFID Tag Carrier for Secure Access Control to a Smart Building. In *International Journal of Applied Engineering Research* (Vol. 13, Issue 1). http://www.ripublication.com

Al-Sudani, A. R., Zhou, W., Wen, S., & Al-Mansoori, A. (2018). SCARA: A framework for secure cloud-assisted RFID authentication for smart building access control. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11058 LNCS*, 202–211. https://doi.org/10.1007/978-3-030-02744-5_15

Brooks, D. J., Coole, M., & Haskell-Dowland, P. (2020a). Intelligent building systems: security and facility professionals' understanding of system threats, vulnerabilities and mitigation practice. *Security Journal*, *33*(2), 244–265. https://doi.org/10.1057/s41284-019-00183-9

dos Santos, D. R., Dagrada, M., & Costante, E. (2021). Leveraging operational technology and the Internet of things to attack smart buildings. *Journal of Computer Virology and Hacking Techniques*, *17*(1). https://doi.org/10.1007/s11416-020-00358-8

Elnour, M., Meskin, N., Khan, K., & Jain, R. (2021). Application of data-driven attack detection framework for secure operation in smart buildings. *Sustainable Cities and Society*, *69*. https://doi.org/10.1016/j.scs.2021.102816

Hyman, B. T., Alisha, Z., & Gordon, S. (2019). Secure Controls for Smart Cities; Applications in Intelligent Transportation Systems and Smart Buildings. *International Journal of Science and Engineering Applications*, *8*(6), 167–171. https://doi.org/10.7753/IJSEA0806.1004ï

Inayat, U., Ali, F., Khan, H. M. A., Ali, S. M., Ilyas, K., & Habib, H. (2021). Wireless Sensor Networks: Security, Threats, and Solutions. *4th International Conference on Innovative Computing, ICIC 2021*. https://doi.org/10.1109/ICIC53490.2021.9693021

Krishnan, N., Karthikeyan, M., Tamilnadu College of Engineering, Institute of Electrical and Electronics Engineers. Madras Section. Podhigai Subsection, Institute of Electrical and Electronics Engineers. Madras Section. Signal Processing/Computational Intelligence/Computer Joint Societies Chapter, & Institute of Electrical and Electronics Engineers. (2017). *Security Considerations for IoT in Smart Buildings*.

Krundyshev Vasiliy, & Kalinin Maxim. (2019). Prevention of false data injections in smart infrastructures. *IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*.

Kruthika Rathinavel, Manisa Pipattanasomporn, Murat Kuzlu, & Saifur Rahman. (2017). *Security concerns and countermeasures in IoT-integrated smart buildings*.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016a). Security in internet of things: Challenges, solutions and future directions. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2016-March*, 5772–5781. https://doi.org/10.1109/HICSS.2016.714

Llaria, A., Santos, J. dos, Terrasson, G., Boussaada, Z., Merlo, C., & Curea, O. (2021). Intelligent buildings in smart grids: A survey on security and privacy issues related to energy management. In *Energies* (Vol. 14, Issue 9). MDPI AG. https://doi.org/10.3390/en14092733

Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021a). AI-empowered IoT Security for Smart Cities. *ACM Transactions on Internet Technology*, *21*(4). https://doi.org/10.1145/3406115

Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, *7*, 7999–8012. https://doi.org/10.1016/j.egyr.2021.08.124

Mikhaylov, D., Zhukov, I., Starikovskiy, A., Zuykov, A. L., Tolstaya, A., & Xim Fo, M. (2013). Method and System for Protection of Automated Control Systems for "Smart Buildings." *I.J. Computer Network and Information Security*, *9*, 1–8. https://doi.org/10.5815/ijcn

Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, *5*(4), 586–602. https://doi.org/10.1109/TETC.2016.2606384

Nafrees, A. C. M., Sujah, A. M. A., & Mansoor, C. (2021a). Smart Cities: Emerging technologies and Potential solutions to the Cyber security threads. *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques, ICEECCOT 2021 - Proceedings*, 220–228. https://doi.org/10.1109/ICEECCOT52851.2021.9707994

Osisiogu Ukachi. (2019). A Review on Cyber -Physical Security of Smart Buildings and Infrastructure. *Institute of Electrical and Electronics Engineers Nile University*.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The Prisma 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*. https://doi.org/10.1136/bmj.n71

Pan, Z., Pacheco, J., & Hariri, S. (2016). Anomaly behavior analysis for building automation systems. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, *0*. https://doi.org/10.1109/AICCSA.2016.7945692

Patil, A., Kamuni, V., Sheikh, A., Wagh, S., & Singh, N. (2019, December 1). A Machine Learning Approach to Distinguish Faults and Cyberattacks in Smart Buildings. *2019 9th*

*International Conference on Power and Energy Systems, ICPES 2019*. https://doi.org/10.1109/ICPES47639.2019.9105507

Seferi Rifat, & Giangiacomi Sofia. (2019). Vulnerabilities and Attacks in a Smart Buildings Scenario. *2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT)*, 296–298.

Sergey E. Bondarev, & Andrey S. Prokhorov. (2017). *Analysis of Internal Threats of the System "Smart Home" and Assessment of Ways to Prevent Them*.

Sheikh, A., Kamuni, V., Patil, A., Wagh, S., & Singh, N. (2019a, December 1). Cyber Attack and Fault Identification of HVAC System in Building Management Systems. *2019 9th International Conference on Power and Energy Systems, ICPES 2019*. https://doi.org/10.1109/ICPES47639.2019.9105438

Sollaci, L. B., & Pereira, M. G. (2004). The introduction, methods, results, and discussion (IMRAD) structure: a fifty-year survey. *Journal of the Medical Library Association*, *92*(3), 364. /pmc/articles/PMC442179/

Sun, F., Zhao, Z., Fang, Z., Du, L., Xu, Z., & Chen, D. (2014). A review of attacks and security protocols for wireless sensor networks. *Journal of Networks*, *9*(5), 1103–1113. https://doi.org/10.4304/jnw.9.5.1103-1113

Wall, A., Butzin, B., Golatowski, F., Rethfeldt, M., & Timmermann, D. (2019). *Software-Defined Security Architecture for Smart Buildings using the Building Information Model; Software-Defined Security Architecture for Smart Buildings using the Building Information Model*. https://technical.buildingsmart.org/standards/ifc/ifc-schema-specifications/

Wan, Y., Long, C., Deng, R., Wen, G., Yu, X., & Huang, T. (2021). Distributed event-based control for thermostatically controlled loads under hybrid cyber attacks. *IEEE Transactions on Cybernetics*, *51*(11), 5314–5327. https://doi.org/10.1109/TCYB.2020.2978274

Wei, X., Wang, T., & Tang, C. (2021). Throughput Analysis of Smart Buildings-oriented Wireless Networks under Jamming Attacks. *Mobile Networks and Applications*, *26*(4), 1440–1448. https://doi.org/10.1007/s11036-019-01481-7