ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Μελέτη ευπαθειών και Κυβερνοφυσικών επιθέσεων σε βιοϊατρικές συσκευές και συσκευές βιομετρικών δεδομένων

Φοιτητής: Ιωάννης Γιαννακόπουλος
ΑΜ: 50346194

Επιβλέπων
Πατρικάκης Χαράλαμπος

Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, Ιούνιος 2021

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

A study of vulnerabilities and Cyberphysical attacks on biometric and biomedical devices

Student: Ioannis Giannakopoulos
Registration Number: 50346194

Supervisor
Patrikakis Charalampos

Professor

ATHENS-EGALEO, June 2021

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

Χαράλαμπος Πατρικάκης, Καθηγητής	Παπαγέωργας Παναγιώτης, Καθηγητής	Φειδάκης Μιχαήλ, Εργαστηριακό Διδακτικό Προσωπικό
Digitally signed by Charalampos Patrikakis Date: 2021.07.22 23:49:01 +03'00'	Digitally signed by Panagiotis Papageorgas Date: 2021.07.25 08:34:58 +03'00'	Michail Feidakis 2021.07.26 08:12:59 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος ΓΙΑΝΝΑΚΟΠΟΥΛΟΣ ΙΩΑΝΝΗΣ του ΗΛΙΑ με αριθμό μητρώου 50346194 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

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

Ο Δηλών
Ιωάννης Γιαννακόπουλος

Περίληψη

Η προόδος των συστημάτων δικτύου που προσφέρουν παντού προσβάσιμες υπηρεσίες , έχει σαν συνέπεια την ανάπτυξη διαφόρων τύπων ασφάλειας. Στην πραγματικότητα, με την εξέλιξη των φυσικών συστημάτων που συνεχίζουν να ενσωματώνονται στα πλαίσια του κυβερνοχώρου, οι κυβερνοαπειλές έχουν πολύ κρίσιμες επιπτώσεις στο φυσικό περιβάλλον. Ως αποτέλεσμα, το ζήτημα της ασφάλειας των φυσικών συστημάτων στον κυβερνοχώρο, απαιτεί ειδική ολιστική μεταχείριση. Σε αυτήν την διπλωματική εργασία, μελετάω την ανταλλαγή μεταξύ ασφάλειας, προστασίας και διαθεσιμότητας σε τέτοια συστήματα , και αναλύω αυτές τις έννοιες για εφαρμογές σε εμφυτεύσιμα ιατροτεχνολογικά προϊόντα . Συζητάω τις προκλήσεις και τους περιορισμούς που σχετίζονται με την ασφάλεια τέτοιων συστημάτων και εστιάζω στον συμβιβασμό μεταξύ των μέτρων ασφαλείας που απαιτούνται για τον αποκλεισμό της μη εξουσιοδοτημένης πρόσβασης στη συσκευή και της προστασίας του ασθενούς σε καταστάσεις έκτακτης ανάγκης όπου τα μέτρα αυτά πρέπει να απορριφθούν για να επιτραπεί η πρόσβαση. Αναλύω τις πιο πρόσφατες προτεινόμενες λύσεις και αντιπαραθέτω τα δυνατά σημεία και τους περιορισμούς τους. Τέλος αναλύεται η επίθεση που πραγματοποίησα σε μια WiFi λάμπα. Το μοντέλο και το όνομα της εταιρείας δεν αναφέρονται για λόγους ασφαλείας.

Λέξεις – κλειδιά

Κυβερνοφυσικά συστημάτα , Ασφάλεια Κυβερνοφυσικών Συστημάτων , Επιθέσεις , Ευπάθειες , Συσκευές ιατρικών δεδομένων , Βιοϊατρικές συσκευές , Ασφάλεια Βιοϊατρικών συσκευών , Εμφυτεύσιμες Ιατρικές συσκευές

Abstract

The progression of networked systems that offer everywhere accessible services has given rise to various types of security tradeoffs. In fact, with the evolution of physical systems that keep getting integrated with cyber frameworks, cyber threats have far more critical effects as they get reflected on the physical environment. As a result, the issue of security of cyber physical systems requires a special holistic treatment. In this diploma thesis, i study the tradeoff between security, safety, and availability in such systems and demonstrate these concepts on implantable medical devices as a case study. I discuss the challenges and constraints associated with securing such systems and focus on the tradeoff between security measures required for blocking unauthorized access to the device and the safety of the patient in emergency situations where such measures must be dropped to allow access. I analyze the up to date proposed solutions and discuss their strengths and limitations.

Keywords

Cyberphysical systems, Security on Cybephysical systems , Attacks , Vulnerabilities , Biometric Devices, Biomedical Devices, Security on Biomedical Devices , Implantable Medical Devices

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Εικόνων

Αλφαβητικό Ευρετήριο

RFID: Radio Frequency Identification

UMTS: Universal Mobile Telecommunications Services

TCP: Transmission Control Protocol

IP: Internet Protocol

CPS : Cyber Physical Systems

ICS : Industrial Control Systems

FCC : Federal Communications Commission

DoS : Denial of Service

DDoS : Distributed Denial of Service

MITM : Man In The Middle

ICDs : Implantable Cardioverter Defibrillator

PKI : Public Key Infrastructure

ACL : Access Control Lists

RD : Resource Depletion

IMDs: Implantable Medical Devices

ΕΙΣΑΓΩΓΗ

Αρχικά παρουσιάζεται ο τρόπος λειτουργίας των Κυβερνοφυσικών Συστημάτων και σε ποιους τομείς της κοινωνίας μπορούν να εφαρμοστούν. Στην συνέχεια γίνεται αναφορά στην αρχιτεκτονική και στους τρόπους ασφάλισης αυτών αλλά και στις μορφές επιθέσεων που μπορούν να δεχθούν. Ακολούθως μελετάται ένας τομέας των Κυβερνοφυσικών Συστημάτων όπως είναι οι βιοϊατρικές συσκευές και συγκεκριμένα οι εμφυτεύσιμες . Σε πρώτη φάση αναλύονται ο τρόπος λειτουργίας , η δομή και οι ευπάθειες αυτών. Στην συνέχεια παρατίθονται εκτενώς τα μέτρα προστασίας και οι τρόποι αντιμετώπισης των εν δυνάμει ευπαθειών αλλά και οι τυχόν αντιπαραθέσεις και οι συμβιβασμοί για την βέλτιστη λειτουργία των συσκευών σε συνάρτηση με την ασφάλεια άλλα και την υγεία των ασθενών.

1. Εισαγωγή στα Κυβερνοφυσικά Συστήματα

1.1 Τα Κυβερνοφυσικά συστήματα

Τα Κυβερνοφυσικά συστήματα (cyber-physical systems- CPS) είναι ένας συνδυασμός στενά ενσωματωμένων φυσικών διαδικασιών, δικτύωσης και υπολογισμού. Η φυσική διαδικασία παρακολουθείται και ελέγχεται από ενσωματωμένα υποσυστήματα μέσω δικτυωμένων συστημάτων με βρόχους ανατροφοδότησης για να αλλάξουν τη συμπεριφορά τους όταν χρειάζεται [1]. Αυτά τα υποσυστήματα λειτουργούν ανεξάρτητα το ένα με το άλλο με την ικανότητα αλληλεπίδρασης με το εξωτερικό περιβάλλον [2] [3] . Οι φυσικές διεργασίες επιτυγχάνονται από πολλές μικροσκοπικές συσκευές με δυνατότητες ανίχνευσης, υπολογισμών και επικοινωνίας (συχνά ασύρματες). Αυτές οι φυσικές συσκευές μπορούν να ταυτοποιηθούν με φυσικά χαρακτηριστικά ή εξοπλισμό ανίχνευσης πληροφοριών, όπως αισθητήρες υπερύθρων ή αναγνώριση ραδιοσυχνοτήτων (RFID), και στη συνέχεια μπορούν να συνδεθούν σε ένα σύστημα δικτύωσης, στις περισσότερες περιπτώσεις στο Διαδίκτυο, για την αποστολή των δεδομένων που συλλαμβάνονται στο υπολογιστικό υποσύστημα. [4]

Με την αυξημένη εστίαση στην ικανότητα χειρισμού δεδομένων, την ικανότητα επικοινωνίας δεδομένων και την ενσωμάτωση συστημάτων πληροφοριών, καθώς και φυσικών συσκευών, αυξάνεται επίσης η ζήτηση για ενσωμάτωση CPS σε διάφορους τομείς, με αποτέλεσμα την ευρεία προσοχή όχι μόνο από τα πανεπιστήμια και τα εργαστήρια έρευνας και ανάπτυξης αλλά και από τη βιομηχανία και τις κυβερνητικές υπηρεσίες [5]. Πριν από την τρέχουσα φόρμα, τα CPS εξελίχθηκαν σε διαφορετικά στάδια: Ενσωματωμένα Συστήματα, Ευφυή Ενσωματωμένα Συστήματα και Συστήματα Συστημάτων [6]. Η τρέχουσα μορφή των CPS χρησιμοποιείται σε πολλούς διαφορετικούς τομείς όπως η ενέργεια, το πετρέλαιο, η βιομηχανία νερού, η χημική μηχανική, η υγειονομική περίθαλψη, η κατασκευή, η μεταφορά, τα συστήματα αυτοκινήτων, η ψυχαγωγία, οι καταναλωτικές συσκευές, καθώς και πολλοί άλλοι τομείς που σχετίζονται άμεσα με τις ανθρώπινες καθημερινές ζωές. Υπολογίστηκε ότι τα φυσικά στοιχεία του κυβερνοχώρου θα αντιστοιχούσαν στο 40% της συνολικής αξίας ενός αυτοκινήτου έως το τέλος του 2015 [7] και ότι το 2020, θα χρησιμοποιηθούν περίπου 25 δισεκατομμύρια αντικείμενα που έχουν προσδιοριστεί με μοναδικό τρόπο. [8]

Τα CPS έχουν πολλά χαρακτηριστικά, όπως η δυνατότητα σε μεμονωμένα εξαρτήματα να λειτουργούν από κοινού, παράγοντας πολύπλοκα συστήματα [9]. Στα CPS, τα δεδομένα μπορούν να συλληφθούν από φυσικά αντικείμενα ή συσκευές αισθητήρων και να μεταφερθούν

μέσω δικτύων στο σύστημα ελέγχου με την απουσία, σε ορισμένες περιπτώσεις, οποιασδήποτε αλληλεπίδρασης από άνθρωπο σε μηχανή [10] . Τα φυσικά αντικείμενα είναι όλο και περισσότερο εξοπλισμένα με, για παράδειγμα, υπέρυθρους αισθητήρες, barcodes ή ετικέτες RFID που μπορούν να σαρωθούν από έξυπνες συσκευές [11]. Αυτές οι συσκευές μπορούν να συνδεθούν στο Διαδίκτυο για να στείλουν τα προσδιορισμένα δεδομένα και την τοποθέτηση τοποθεσίας που θα χρησιμοποιηθούν για την παρακολούθηση και τη διαχείριση του φυσικού περιβάλλοντος [4]. Οι υπολογιστικές και επεξεργαστικές μονάδες μπορούν επίσης να τοποθετηθούν στο σύννεφο, με τις προκύπτουσες αποφάσεις που εκδίδονται ως ενέργειες στα φυσικά αντικείμενα [11]. Ως παράδειγμα των CPS, τα βιομηχανικά συστήματα ελέγχου (ICS) απομονώνονται από πρωτόκολλα επικοινωνίας και λειτουργικά συστήματα από τα εξωτερικά συστήματα. Προς το παρόν, αυτά τα είδη συστημάτων συνδέονται όλο και περισσότερο μέσω του Διαδικτύου για τη βελτίωση της λειτουργικότητας και της αυτοματοποίησης. Η αυξημένη συνδεσιμότητα του κυβερνοχώρου και του φυσικού κόσμου φέρνει σημαντικές προκλήσεις ασφαλείας των CPS [12] . Δεδομένου ότι η σημασία αυτών των συστημάτων είναι η βελτίωση της λειτουργικότητας, η διασύνδεση μεταξύ των υποσυστημάτων των CPS αυξάνεται. [13]

Τα προβλήματα ασφαλείας που κυμαίνονται από το περιβάλλον των εφαρμογών και την τεχνολογία επικοινωνίας θα πρέπει να αντιμετωπιστούν στα πρώτα στάδια του σχεδιασμού [14]. Επιπλέον, τα εγγενή χαρακτηριστικά και πλεονεκτήματα της χρήσης διαθέσιμων δικτύων, όπως τα Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks), τα δίκτυα επόμενης γενιάς και το Διαδίκτυο, τα CPS αντιμετωπίζουν ολοένα και περισσότερες νέες προκλήσεις ασφαλείας, όπως η διασφάλιση πρωτοκόλλων και η καθιέρωση εμπιστοσύνης μεταξύ των υποσυστημάτων των Κυβερνοφυσικών συστημάτων.[76]

1.2 Αρχιτεκτονική Κυβερνοφυσικών Συστημάτων

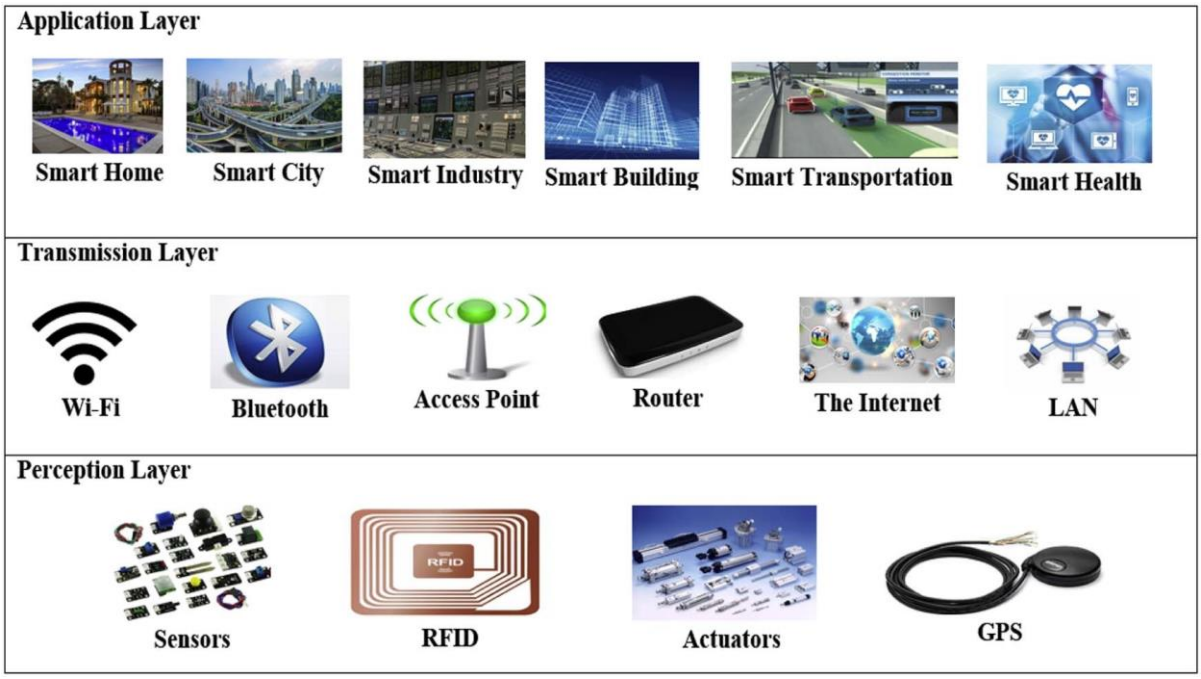

Figure 1 Αρχιτεκτονική Κυβερνοφυσικών Συστημάτων [84]

Ο σύγχρονος ορισμός των CPS είναι η ενσωμάτωση των δυνατοτήτων υπολογισμού, επικοινωνίας και ελέγχου που παρακολουθούν και ελέγχουν τα αντικείμενα στον φυσικό κόσμο. Οι φυσικές διεργασίες ελέγχονται και παρακολουθούνται από συστήματα στον κυβερνοχώρο [12] τα οποία είναι ενσωματωμένοι υπολογιστές και δίκτυα με βρόχους ανάδρασης. Η βασική αρχιτεκτονική των CPS αποτελείται από τρία βασικά επίπεδα : επίπεδο αντίληψης, επίπεδο μετάδοσης , επίπεδο εφαρμογής.

Το πρώτο επίπεδο είναι το Perception Layer . Αυτό το επίπεδο έχει πολλαπλό τερματικό εξοπλισμό, όπως αισθητήρες, ενεργοποιητές, κάμερες, GPS , σαρωτές λέιζερ, έξυπνες συσκευές, ετικέτες RFID με 2-D ετικέτες γραμμικού κώδικα και αναγνώστες [5] [16] [4]. Οι συσκευές σε αυτό το επίπεδο έχουν τη δυνατότητα να συλλέγουν δεδομένα σε πραγματικό χρόνο που απαιτούνται για διαφορετικούς σκοπούς, ερμηνεύουν αυτά που λαμβάνουν από τον φυσικό κόσμο και εκτελούν εντολές από το επίπεδο εφαρμογής. Τα δεδομένα που συλλέγονται μπορεί να περιλαμβάνουν ήχο, φως, μηχανική, χημεία, θερμότητα, ηλεκτρική ενέργεια, βιολογία ή τοποθεσία [13] [17] . Οι αισθητήρες μπορούν να δημιουργήσουν δεδομένα σε πραγματικό χρόνο με τη συνεργασία κόμβων σε μεγάλους και τοπικούς τομείς δικτύου, τα οποία θα συγκεντρωθούν και θα αναλυθούν στο επίπεδο εφαρμογής [18]. Οι αισθητήρες, ανάλογα με τον τύπο τους, μπορούν να συγκεντρώσουν πληροφορίες που σχετίζονται με τη

θερμοκρασία, την επιτάχυνση, την υγρασία, τους κραδασμούς, τη θέση ή τις χημικές αλλαγές του αέρα.[11]

Το δεύτερο επίπεδο είναι το Transmission Layer γνωστό και ως επίπεδο μεταφοράς [5] ή επίπεδο δικτύου [11] , το οποίο είναι υπεύθυνο για την εναλλαγή και την επεξεργασία δεδομένων μεταξύ του επίπεδου αντίληψης και του επίπεδου εφαρμογής. Η αλληλεπίδραση και η μετάδοση δεδομένων σε αυτό το επίπεδο επιτυγχάνεται με τη χρήση τοπικών δικτύων, δικτύων επικοινωνίας, Διαδικτύου ή άλλων υφιστάμενων δικτύων μέσω πολλών τεχνολογιών όπως Bluetooth, 4G και 5G, UMTS, Wi-Fi, Infrared και ZigBee, ανάλογα με τις συσκευές αισθητήρων [11]. Ωστόσο, οι περισσότερες διασυνδέσεις επιτυγχάνονται μέσω του Διαδικτύου για πολλούς λόγους, συμπεριλαμβανομένης της διαθεσιμότητας και της σχέσης κόστους-αποτελεσματικότητας. Αυτό σημαίνει ότι οι λειτουργίες σε πραγματικό χρόνο θα πρέπει να υποστηρίζονται από τα δίκτυα που χρησιμοποιούνται. Δεδομένου ότι είναι σημαντικό να διαχειριστεί και να επεξεργαστεί ογκώδη δεδομένα, το επίπεδο μετάδοσης μπορεί αρχικά να επεξεργαστεί και να διαχειριστεί έναν πολύ μεγάλο όγκο στοιχείων και να πραγματοποιήσει μετάδοση σε πραγματικό χρόνο [5] με ευθύνη για αξιόπιστη υποστήριξη επικοινωνίας [4].

Το τρίτο και πιο διαδραστικό επίπεδο είναι το Application Layer. Η αποστολή του είναι να επεξεργάζεται τις ληφθείσες πληροφορίες από τα επίπεδο μεταφοράς δεδομένων και να εκδίδει τις εντολές που πρέπει να εκτελεστούν από τις φυσικές μονάδες, τους αισθητήρες και ενεργοποιητές [13]. Αυτό το επίπεδο λειτουργεί εφαρμόζοντας σύνθετους αλγόριθμους λήψης αποφάσεων σχετικά με τα συγκεντρωτικά δεδομένα για τη λήψη σωστών αποφάσεων [2] , και ελέγχου εντολών που θα χρησιμοποιηθούν στο διορθωτικές ενέργειες. Επιπλέον, αυτό το επίπεδο λαμβάνει και επεξεργάζεται πληροφορίες από το επίπεδο αντίληψης και στη συνέχεια καθορίζει τις απαιτούμενες αυτοματοποιημένες ενέργειες προς επίλυση [11].

Η παρακολούθηση του συστήματος πραγματοποιείται επίσης σε αυτό το επίπεδο και αποστολή του είναι να παρατηρήσει τη συμπεριφορά των φυσικών διεργασιών, και να εκδώσει εντολές για να αλλάξει τη συμπεριφορά των φυσικών συσκευών για να διασφαλίσει ότι το περιβάλλον εργασίας λειτουργεί στα βέλτιστα. Το επίπεδο εφαρμογής σώζει επίσης προηγούμενες ενέργειες έτσι ώστε να μπορεί να δοθεί η ανατροφοδότηση οποιασδήποτε προηγούμενης δράσης για τη διασφάλιση μελλοντικών επιχειρησιακών βελτιώσεων. Ο σκοπός αυτού του επιπέδου είναι να δημιουργηθεί ένα έξυπνο περιβάλλον [18] και να συνδυαστούν τα Κυβερνοφυσικά συστήματα και οι επαγγελματικές εφαρμογές της βιομηχανίας. Αυτό οδήγησε σε εκτεταμένες και έξυπνες εφαρμογές σε τομείς που μπορεί να περιλαμβάνουν ιδιωτικά και

ασφαλή δεδομένα, όπως: Έξυπνο Δίκτυο ηλεκτρικής ενέργειας, Έξυπνα Σπίτια και Πόλεις, Έξυπνη Μεταφορά [13], Περιβαλλοντική παρακολούθηση, Βιομηχανικός έλεγχος [5], Έξυπνη Υγεία και Έξυπνη Καλλιέργεια. Τέτοιες εφαρμογές ενδέχεται να συλλέγουν τα προσωπικά δεδομένα των χρηστών, όπως πληροφορίες για την υγεία και συνήθειες. Επομένως, είναι σημαντικό να εφαρμοστούν μηχανισμοί για την προστασία των δεδομένων.

1.3 Ασφάλεια Κυβερνοφυσικών Συστημάτων

Σε γενικές γραμμές, η ασφάλεια των CPS ταξινομείται σε δύο τομείς: ασφάλεια πληροφοριών (δεδομένων) και ασφάλεια ελέγχου. Η ασφάλεια των πληροφοριών περιλαμβάνει την ασφάλεια πληροφοριών κατά τη συγκέντρωση δεδομένων, την επεξεργασία και την κοινή χρήση μεγάλης κλίμακας στο περιβάλλον δικτύου, ιδίως στα ανοικτά δίκτυα . Η ασφάλεια ελέγχου περιλαμβάνει την επίλυση τυχόν ζητημάτων ελέγχου στο περιβάλλον του δικτύου και τον περιορισμό του συστήματος ελέγχου από τυχόν επιθέσεις στους αλγόριθμους εκτίμησης και ελέγχου του συστήματος [19] [76]. Η ασφάλεια των πληροφοριών επικεντρώνεται στην προστασία των δεδομένων, για παράδειγμα με τη χρήση κρυπτογράφησης, ενώ η ασφάλεια ελέγχου επικεντρώνεται στην προστασία της δυναμικής των συστημάτων ελέγχου από κυβερνοεπιθέσεις [5]. Επιπρόσθετα στηναναφορα των διακριτικών χαρακτηριστικών μεταξύ των CPS και των παραδοσιακών συστημάτων IT, στην ενότητα αυτή παρουσιάζεται η ανάλυση των σημαντικότερων παραγόντων ασφάλειας, στόχων, επιθέσεων και εκτιμήσεων κινδύνου για τα CPS.

1.3.1 Ασφάλεια στην Πρόσβαση Συσκευών

Η εξασφάλιση πρόσβασης στις συσκευές έχει πρωτεύουσα σημασία . Εάν ο έλεγχος ταυτότητας δεν υποστηρίζεται ή δεν υποστηρίζεται σωστά, μη εξουσιοδοτημένοιχρηστες θα μπορούσαν αποκτήσουν πρόσβαση και να χειριστούν το σύστημα , επομένως, δεν διασφαλίζεται ούτε η αυθεντικότητα των δυαδικών κωδίκων ούτε η εκτέλεση στα Application Layers [20].

1.3.2 Ασφάλεια στην Μετάδοση Δεδομένων

Για τον εντοπισμό κακόβουλων δραστηριοτήτων απαιτείται ασφάλεια μετάδοσης δεδομένων σε δίκτυα επικοινωνίας CPS και ο αποκλεισμός μη εξουσιοδοτημένης πρόσβασης. Για παράδειγμα, αν οι επιτιθέμενοι προσπαθούν να υποκλέψουν τις λειτουργίες κατανάλωσης ενέργειας του συστήματος και συμπεριφορών χρονισμού προκειμένου να αναλύσουν τα

δεδομένα που αποστέλλονται και λαμβάνονται [20]. Ορισμένοι εισβολείς στοχεύουν να διαταράξουν τα δίκτυα, εξαπολύοντας επιθέσεις DoS ή παρεμβαίνοντας στην τοπολογία δρομολόγησης [21] .

1.3.3 Ασφάλεια Εφαρμογών

Το Application Layer συνδυάζει εφαρμογές διαφόρων τύπων με διαφορετικά επίπεδα ασφαλείας. Εδώ, οι ιδιωτικές πληροφορίες των χρηστών μπορούν να αναλυθούν από τους επιτιθέμενους, οδηγώντας σε διαρροή προσωπικών δεδομένων και απώλεια απορρήτου. Λαμβάνοντας υπόψιν ότι τα δεδομένα μπορεί να περιέχουν προηγούμενες και παρούσες τοποθεσίες που επισκέφθηκαν οι χρήστες, ορισμένες τεχνικές προστασίας δεδομένων σε αυτό το επίπεδο περιλαμβάνουν απόκρυψη τοποθεσίας, την ανωνυμία του χώρου ή την κρυπτογράφηση του. Επιπλέον, πολλές εφαρμογές σε αυτό το επίπεδο αναφέρονται στην κοινωνική ζωή των χρηστών, επομένως πρέπει να προστατευθούν [8].

1.3.4 Ασφάλεια στην Αποθήκευση Δεδομένων

Η προστασία αποθηκευμένων μυστικών δεδομένων σε συσκευές CPS είναι σημαντική. Οι περισσότερες συσκευές CPS, όπως οι αισθητήρες, είναι μικροσκοπικοί, ασύρματα συνδεδεμένοι και με περιορισμένους πόρους [21]. Παρόλο που διάφορες λύσεις βασίζονται σε λογισμικό χρησιμοποιούν κρυπτογραφικές τεχνικές για την κρυπτογράφηση δεδομένων σε τέτοιες συσκευές, δεν επαρκούν λόγω των περιορισμών της μνήμης και της αδυναμίας επεξεργασίας αυτών των συσκευών.

1.4 Είδη Επιθέσεων σε Κυβερνοφυσικά Συστήματα

Οι επιθέσεις στα CPS θα μπορούσαν να προκαλέσουν σοβαρές ζημιές στο φυσικό περιβάλλον. Κάθε επίπεδο των CPS είναι επιρρεπές είτε σε παθητικές είτε σε ενεργητικές επιθέσεις. Επιπλέον, τα CPS είναι ευάλωτα σε περισσότερες επιθέσεις από τα παραδοσιακά συστήματα πληροφορικής, όπως σε επιθέσεις από το Διαδίκτυο [13], το οποίο χρησιμοποιείται ήδη ως επίπεδο μετάδοσης. Οι κατηγορίες των επιθέσεων στο Perception Layer, για παράδειγμα, περιλαμβάνουν : επιθέσεις σε κόμβους, όπως αισθητήρες και ενεργοποιητές. Οι κατηγορίες των επιθεσεων στο Transmission Layer περιλαμβάνουν διαρροή δεδομένων ή ζημιές και ζητήματα ασφάλειας κατά τη μετάδοση δεδομένων. Οι κατηγορίες των επιθέσεων στο Application Layer περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση που οδηγεί σε απώλεια του απορρήτου των χρηστών [5]. Έτσι, απαιτείται ανάλυση πιθανών επιθέσεων και οικοδόμηση

μιας ισχυρής αρχιτεκτονικής ασφαλείας. Αν και κάθε επίπεδο είναι επιρρεπές σε διαφορετικές επιθέσεις, ορισμένες εξ αυτών θα μπορούσαν να στοχεύουν σε όλα τα επίπεδα. Παραδείγματα αυτών των επιθέσεων περιλαμβάνουν:

- ***Denial-of-Service (DoS)***: Ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες. [85]

- ***Man-in-the-Middle (MITM)***: Η επίθεση man-in-the-middle είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες. [89]

- ***Eavesdropping*** : Μια επίθεση Eavesdropping, επίσης γνωστή ως επίθεση snifing ή snooping, είναι κλοπή πληροφοριών καθώς μεταδίδονται μέσω δικτύου από υπολογιστή, smartphone ή άλλη συνδεδεμένη συσκευή. Η επίθεση εκμεταλλεύεται τις μη ασφαλείς επικοινωνίες δικτύου για πρόσβαση στα δεδομένα καθώς αποστέλλονται ή λαμβάνονται από τον χρήστη της. [86]

- ***Spoofing***: Είναι μια τεχνική για να αποκτήσουμε παράνομη πρόσβαση σε υπολογιστές με την δημιουργία πακέτων TCP/IP, χρησιμοποιώντας τη διεύθυνση και τα στοιχεία κάποιου άλλου αξιόπιστου. Οι δρομολογητές (routers) χρησιμοποιούν την διεύθυνση της IP προορισμού (destination IP) ώστε να διαδώσουν τα πακέτα μέσω διαδικτύου αγνοώντας - αλλάζοντας εικονικά την διεύθυνση της IP πηγής (source IP). Αυτή η διεύθυνση χρησιμοποιείται μόνο από το μηχάνημα προορισμού όταν απαντά πίσω στη πηγή. [87]

- ***Replay (playback)***: Είναι μια μορφή επίθεσης στο δίκτυο στην οποία η έγκυρη μετάδοση δεδομένων επαναλαμβάνεται ή καθυστερεί κακόβουλα ή με δόλιο τρόπο. Αυτό πραγματοποιείται είτε από τον δημιουργό είτε από τον επιτιθέμενο που

παρακολουθεί τα δεδομένα και τα μεταδίδει εκ νέου, πιθανώς ως μέρος μιας επίθεσης πλαστογράφησης από αντικατάσταση πακέτων IP. **[**88]

2 Συσκευές βιομετρικών δεδομένων

2.1 Εμφυτεύσιμες Ιατρικές Συσκευές (IMDs)

Οι εμφυτεύσιμες ιατρικές συσκευές (IMDs) είναι ασύρματα προγραμματισμένες συσκευές για την παρακολούθηση χρόνιων διαταραχών και τη θεραπεία ασθενών με αυτοματοποιημένες θεραπείες, όπως η ρύθμιση του καρδιακού παλμού του ασθενή. Αυτές οι συσκευές ανταλλάσσουν πληροφορίες με συσκευές απομακρυσμένης παρακολούθησης ή προγραμματισμού μέσω του δικτύου, καθιστώντας τις ευάλωτες σε κυβερνοεπιθέσεις. Σε αρκετές περιπτώσεις, η συσκευή δεν ανταποκρίνεται και ο ασθενής πρέπει να υποβληθεί σε χειρουργική επέμβαση για να αντικαταστήσει τη συσκευή. Οποιαδήποτε αλλαγή στις παραμέτρους ή τη ρύθμιση απορρήτου της συσκευής μπορεί να οδηγήσει σε θανάσιμα περιστατικά. Στην εικόνα 2, βλέπουμε μερικά παραδείγματα IMDs και σε ποια σημεία εισάγονται στο σώμα. Μερικά είδη IMDs είναι :

- Εμφυτεύσιμοι καρδιακοί μετατροπείς-απινιδωτές (ICDs): Αυτές είναι οι συσκευές που τροφοδοτούνται με μπαταρία και τοποθετούνται κάτω από το δέρμα για την παρακολούθηση του καρδιακού ρυθμού και τη θεραπεία ακανόνιστου καρδιακού παλμού.

- Εμφυτεύσιμοι διεγέρτες νεύρων: Αυτή η συσκευή είναι ενσωματωμένη στο σώμα και στέλνει ηλεκτρικό ρεύμα για τη θεραπεία του χρόνιου πόνου.

- Διεγέρτες εγκεφάλου: Στέλνουν ηλεκτρικούς παλμούς σε διαφορετικούς στόχους στον εγκέφαλο για τη θεραπεία της κίνησης και των νευροψυχιατρικών διαταραχών.

- Κοχλιακά εμφυτεύματα: Πρόκειται για χειρουργικά εμφυτευμένες ηλεκτρονικές συσκευές για την ενίσχυση της ακοής για άτομα με απώλεια ακοής.

- Αντλίες ινσουλίνης: Εμφυτεύεται στο εσωτερικό του σώματος για την περιοδική χορήγηση ινσουλίνης.

- Γαστρικός διεγέρτης: Τοποθετείται στην κοιλιά για να στείλει ήπιους ηλεκτρικούς παλμούς σε νεύρα του κάτω στομάχου για να μειώσει τη ναυτία και τον εμετό (γαστροπάρεση).

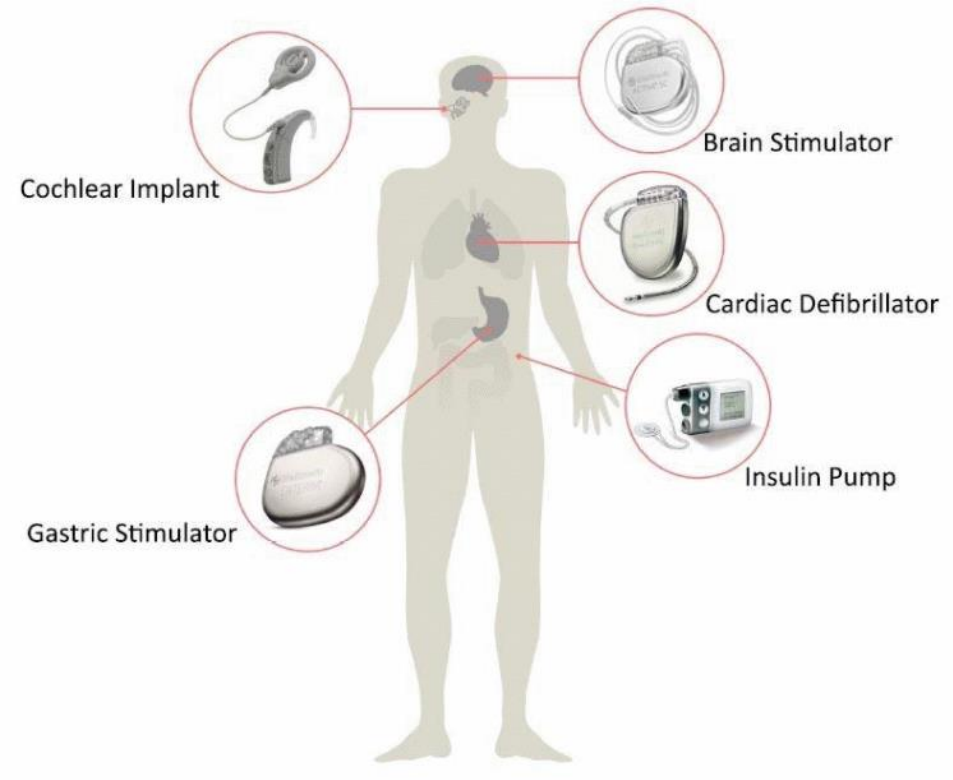

Figure 2 Παραδείγματα IMDs [83]

- **Καρδιακά εμφυτευμένες συσκευές**

Αυτές περιλαμβάνουν συσκευές όπως εμφυτεύσιμους μετατροπείς-απινιδωτές (ICD) και βηματοδότες. Έχουν σχεδιαστεί για τη θεραπεία καρδιακών παθήσεων παρακολουθώντας την ηλεκτρική δραστηριότητα της καρδιάς και εφαρμόζοντας ηλεκτρικά ερεθίσματα κατάλληλης έντασης και θέσης, προκειμένου να κάνουν την καρδιά να χτυπά στην επιθυμητή ταχύτητα [28]. Τα νέα μοντέλα είναι εξοπλισμένα με αισθητήρες πίεσης ικανούς να παρακολουθούν ενεργά τις αλλαγές που θα μπορούσαν να οδηγήσουν σε καρδιακή ανεπάρκεια. Αυτό επιτρέπει την ειδοποίηση του ασθενούς ή του ιατρικού προσωπικού εάν ανιχνευθεί αύξηση της πίεσης στην κόλπο της καρδιάς, καθώς αυτό αποτελεί κατάσταση κινδύνου για τον ασθενή. Τα

καρδιακά εμφυτεύματα μπορούν επίσης να εξοπλιστούν με επιταχυνσιόμετρα για τη μέτρηση του επιπέδου σωματικής δραστηριότητας του ασθενούς. Αυτό μπορεί να οριστεί ως παράμετρος εισόδου στον ελεγκτή IMD, επιτρέποντας τη ρύθμιση της συχνότητας καρδιακής διέγερσης σε αυτή που ταιριάζει καλύτερα κάθε στιγμή [29].

- **Νευροδιεγέρτες**

Αυτές οι συσκευές μεταδίδουν ηλεκτρικά σήματα χαμηλού πλάτους μέσω ενός ή περισσότερων ηλεκτροδίων τοποθετημένων σε διαφορετικές θέσεις του εγκεφάλου. Αυτά τα ηλεκτρόδια εμφυτεύονται σε πολύ συγκεκριμένες περιοχές ανάλογα με την κατάσταση του ασθενούς. Η διαδικασία είναι γνωστή ως Βαθιά Διέγερση του Εγκεφάλου και επιτρέπει τη θεραπεία μιας ποικιλίας παθολογιών όπως Πάρκινσον, δυστονία, επιληψία ή ακόμα και κατάθλιψη που, σε ορισμένες περιπτώσεις, είναι ανθεκτικές στη φαρμακευτική αγωγή μετά από αρκετά χρόνια θεραπείας [30].

- **Σύστημα Παροχής Φαρμάκων**

Ένα Σύστημα Παροχής Φαρμάκων αποτελείται από μια αντλία και έναν καθετήρα που εμφυτεύονται χειρουργικά κάτω από το δέρμα. Η λειτουργία τους είναι να παρέχουν φάρμακα με ελεγχόμενο τρόπο. Δεδομένου ότι το φάρμακο πηγαίνει απευθείας στην στοχευμενη περιοχή, μια αντλία έγχυσης παρέχει σημαντικό βαθμό ελέγχου, ο οποίος επιτρέπει τη χρήση χαμηλότερης δόσης από αυτή που απαιτείται με φάρμακα από το στόμα. Για παράδειγμα, αυτός ο τύπος εμφυτευμάτων έχει χρησιμοποιηθεί με επιτυχία για τον μετριασμό του πόνου σε περιπτώσεις καρκίνου όπου τα παραδοσιακά φάρμακα δεν έχουν καλά αποτελέσματα [31].

- **Βιο-αισθητήρες**

Το εμφύτευμα αποτελείται από έναν αισθητήρα ή ένα σύνολο αισθητήρων που τοποθετούνται μέσα στο ανθρώπινο σώμα για την παρακολούθηση οποιουδήποτε μέρους του. Είναι σε θέση να μετρήσουν ορισμένες φυσιολογικές παραμέτρους και να χρησιμοποιήσουν τέτοια μέτρα για να λάβουν αποφάσεις. Σε αυτό το είδος των εμφυτευμάτων υπάρχει μια ειδική συσκευή που λειτουργεί ως κόμβος ελέγχου, επικοινωνώντας με τους αισθητήρες και με άλλες εξωτερικές οντότητες (π.χ. Προγραμματιστής) [32] [33] [34] .

2.1.1 Λειτουργία IMDs

Τα συστήματα υγειονομικής περίθαλψης που ενσωματώνουν πολυάριθμες λειτουργίες επικοινωνίας και δικτύωσης έχουν πολλαπλασιαστεί τα τελευταία χρόνια. Αυτό κατέστησε δυνατή ανάπτυξη δίκτυα ιατρικών αισθητήρων τα οποία, για παράδειγμα, μπορούν να παρακολουθούν ασθενείς στα σπίτια τους [35] [36] [37] [38]. Ιατροί, φροντιστές ή ακόμη και ο ίδιος ο ασθενής μπορεί να διεξάγει συνεχή και πιο ευέλικτο έλεγχο για την κατάστασή της υγείας του, καθώς επίσης να έχει εξ αποστάσεως πρόσβαση σε ιατρικά δεδομένα, να επικοινωνεί σε περίπτωση επείγουσας ανάγκης. Και προωθεί την αυτονομία των ασθενών που, σε πολλές περιπτώσεις, είναι ηλικιωμένοι άτομα ή άτομα με μειωμένη κινητικότητα. Παρόμοιες δυνατότητες επικοινωνίας και δικτύωσης ενσωματώνονται όλο και περισσότερο στις IMD. Εξοπλισμένος με ραδιοπομπό, η IMD μπορεί να επικοινωνήσει με μια εξωτερική συσκευή —γνωστή γενικά ως "προγραμματιστής" ή "αναγνώστης"— και να της αποστείλει φυσιολογικά δεδομένα όπως σήματα ηλεκτροκαρδιογραφήματος (ΗΚΓ) στην περίπτωση βηματοδοτών και ICD, τα οποία ο γιατρός μπορεί να χρησιμοποιηθεί για την παρακολούθηση της παθολογίας του ασθενούς. Εκτός από την υποβολή ερωτημάτων για ανιχνευμένα δεδομένα, ο προγραμματιστής μπορεί επίσης να διατάξει την IMD να προσαρμόσει ή να απενεργοποιήσει τις θεραπείες, εκτέλεση ενημερώσεων λογισμικού κ.λπ.

Η αύξηση των IMD με δυνατότητες ασύρματης επικοινωνίας και δικτύωσης έχει σημαντικά πλεονεκτήματα, όπως:

- Επιτρέπει τη συνεχή παρακολούθηση των φυσιολογικών παραμέτρων του ασθενούς και άλλων συμπτωμάτων που καταγράφονται από τη συσκευή, γεγονός που μειώνει το χρόνο που απαιτείται για την τακτική παρακολούθηση των ιατρικών καταστάσεων και επιπλέον, προκαλεί λιγότερες διαταραχές στις καθημερινές δραστηριότητες του ασθενούς.

- Ενίσχυση της εποπτείας και της διαχείρισης της επιχείρησης IMD, η οποία επιτρέπει την αντιμετώπιση κάθε προβλήματος που ενδέχεται να προκύψει και εφαρμόζει κατάλληλα μέτρα διόρθωσης σε μικρότερο χρονικό διάστημα.

- Οι δύο προηγούμενες θέσεις συνεπάγονται επίσης σε μείωση του συνολικού κόστους που εμπλέκεται στον εντοπισμό της κατάστασης του ασθενούς και στη διαχείριση της λειτουργίας της IMD.

2.1.2 Τρόποι Λειτουργίας των IMDs

Μια IMD έχει δυο τρόπους λειτουργίας: κανονική και έκτακτης ανάγκης. Ένας σημαντικός στόχος είναι να εξευρεθεί μια λογική αντιστάθμιση μεταξύ αυτών των δύο πιθανών καταστάσεων:

1. **Ασφάλεια σε κατάσταση κανονικής λειτουργίας.** Ο ασθενής ελέγχει ποιος μπορεί να αλληλεπιδράσει με την IMD του. Στην περίπτωση αυτή, είναι πολύ σημαντικό να εφαρμοστεί ένας πολύ ισχυρός μηχανισμός ελέγχου πρόσβασης όσο και πρωτόκολλα κρυπτογράφησης στη σύνδεση επικοινωνίας για να μην επιτρέπονται κακόβουλες και μη εξουσιοδοτημένες προσβάσεις. Η IMD πρέπει να αγνοεί τις αιτήσεις δεδομένων χωρίς διακρίσεις ή τις εντολές επαναπρογραμματισμού συσκευών. Ιδανικά, το εμφύτευμα θα πρέπει να είναι μη ανιχνεύσιμο σε μη εξουσιοδοτημένες ομάδες.
2. **Ασφάλεια σε κατάσταση έκτακτης ανάγκης.** Εξίσου σημαντική με την προσφορά ισχυρού ελέγχου πρόσβασης, ασφαλών επικοινωνιών, ακόμη και η μη ανιχνευόμασταν, είναι η ικανότητα πρόσβασης σε κατάσταση έκτακτης ανάγκης. Σκεφτείτε έναν ασθενή που εισέρχεται σε ένα δωμάτιο έκτακτης ανάγκης σε ένα νοσοκομείο διαφορετικό από αυτό που επισκέπτεται συχνά. Για να περιπλέξουμε περαιτέρω τα πράγματα, υποθέστε ότι ο ασθενής επισκέπτεται μια ξένη χώρα. Ακόμη και υπό αυτές τις συνθήκες, το προσωπικό υγειονομικής περίθαλψης πρέπει να είναι σε θέση να επικοινωνεί με το εμφύτευμα, να προσδιορίζει τον τύπο του (π.χ. μοντέλο και εμπορικό σήμα), να εξάγει φυσιολογικά δεδομένα ή πληροφορίες σχετικά με τη θεραπεία, ακόμη και να επικαιροποιεί τη διαμόρφωσή του, εάν απαιτείται. Ακόμη και σε ένα ασφαλές σύστημα, σε μια κατάσταση έκτακτης ανάγκης, όπως μια επείγουσα χειρουργική επέμβαση ενός ασθενούς που κατέχει ένα ICD, στο οποίο είναι υποχρεωτικό να απενεργοποιηθεί το εμφύτευμα, το IMD θα πρέπει πάντα να ανταποκρίνεται πριν από την απενεργοποίηση.

2.2 Ευπάθειες των IMDs

Οι ασύρματες IMDs, όπως χρησιμοποιούνται αυτή τη στιγμή στην ιατρική πρακτική, παρουσιάζουν πολλές ευπάθειες. Η επικοινωνία μεταξύ των IMDs και ενός σταθμού βάσης ή συσκευής προγραμματιστή μπορεί να υποκλαπεί και, εάν τα σήματα δεν προστατεύονται από πρωτόκολλα κρυπτογράφησης ή/και ελέγχου ταυτότητας, ένας εισβολέας μπορεί να συλλέξει

ή να τροποποιήσει τις πληροφορίες, ενδεχομένως ενώ βρίσκεται εκατοντάδες μέτρα μακριά. Ακόμη και αν προστατεύονται από κρυπτογράφηση, παρόλο που πολλές υπάρχουσες συσκευές δεν προστατεύονται, η απλή παρουσία και το μοτίβο τέτοιων σημάτων μπορεί να παρέχουν πληροφορίες που θα μπορούσαν να είναι πολύτιμες για έναν εισβολέα.

Ο σταθμός βάσης ή ο προγραμματιστής μπορεί επίσης να είναι ο στόχος παρεμβολών. οι επικοινωνίες του με άλλες συσκευές σε ένα ασύρματο δίκτυο (ή μέσω του διαδικτύου) μπορούν να συλλεχθούν και να τροποποιηθούν και η συσκευή μπορεί να παραβιαστεί μέσω φυσικής ή απομακρυσμένης εισαγωγής κακόβουλου κώδικα. Αυτό το τελευταίο ζήτημα είναι σημαντικό, καθώς οι IMDs σχεδιάζονται όλο και περισσότερο για να διασυνδέονται με ηλεκτρονικές συσκευές ευρείας κατανάλωσης, όπως smartphones και υπολογιστές tablet, ανοίγοντας τη δυνατότητα κακόβουλου λογισμικού να στοχεύει την καταναλωτική συσκευή και, ως εκ τούτου, να αποκτά πρόσβαση σε εφαρμογές προγραμματιστών που ελέγχουν το IMD. Οι πιθανές επιθέσεις δεν περιορίζονται στα ψηφιακά συστήματα, με τον αναλογικό αισθητήρα και τα στοιχεία των IMD να είναι ευάλωτα σε επιθέσεις πλαστογράφησης [77].

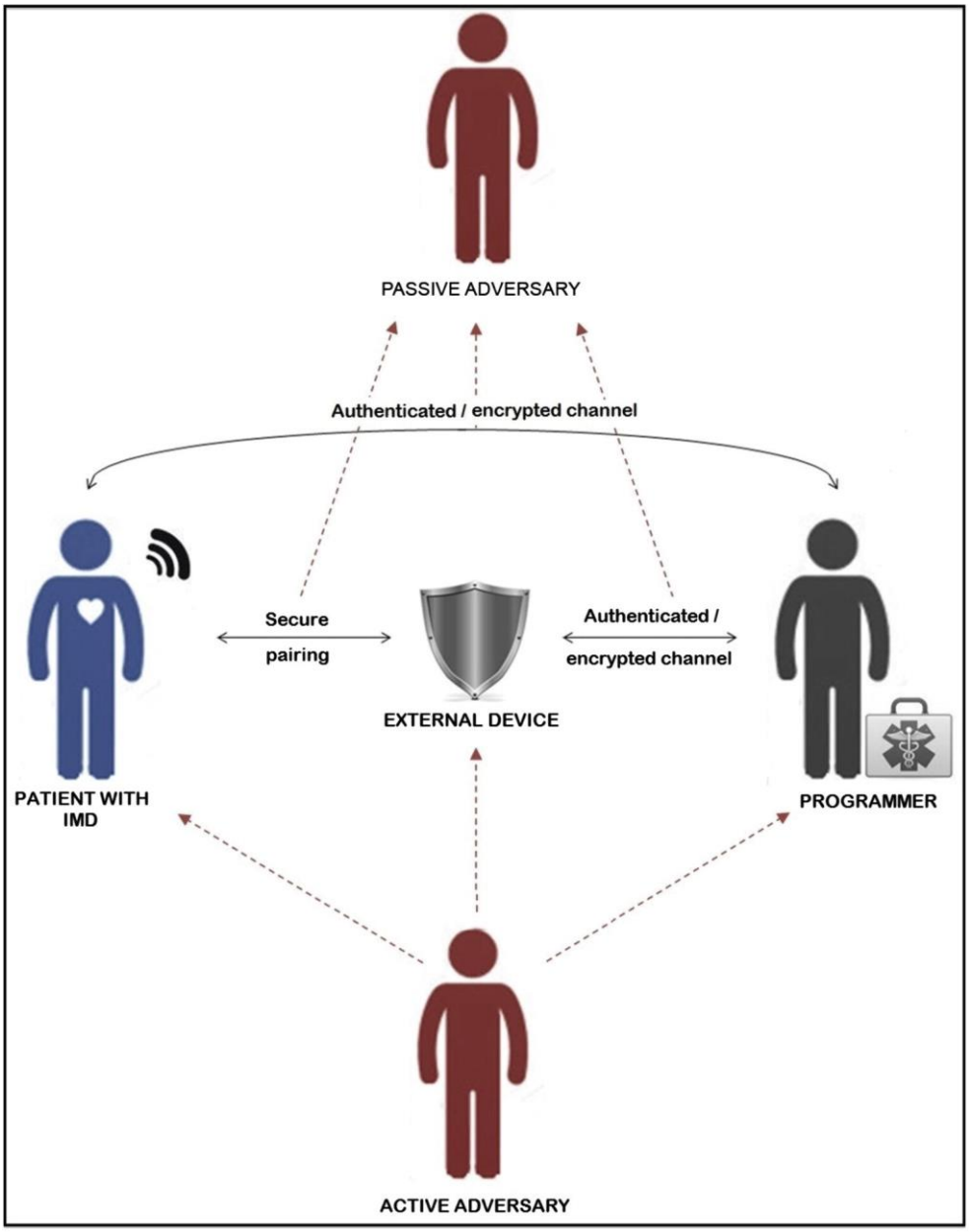

Figure 3 Σενάριο χρήσης IMD [79]

Στην παραπάνω εικόνα παρουσιάζεται η διαδικασία επικοινωνίας μεταξύ ενός ασθενή με IMD και του Προγραμματιστή. Η IMD επικοινωνεί με τον Προγραμματιστή, ο οποίος μπορεί να είναι ένα πρόσωπο ή μια συσκευή εξουσιοδοτημένη να αλληλεπιδρά με το εμφύτευμα (π.χ ιατρικό προσωπικό). Σε κανονική λειτουργία (δηλαδή, αν το εμφύτευμα δεν έχει εντοπίσει κατάσταση έκτακτης ανάγκης), ο Προγραμματιστής πρέπει να ξεκινήσει την επικοινωνία με την IMD, όπως αναφέρεται από τους κανονισμούς της FCC (Federal Communications Commission). Δεδομένου ότι το κανάλι επικοινωνίας είναι ένα κοινό μέσο επικοινωνίας, ο προγραμματιστής θα ελέγξει το κανάλι μέχρι να επιβεβαιωθεί ότι δεν είναι απασχολημένο για να εκκινήσει την επικοινωνία. Στόχος αυτής της επικοινωνίας είναι είτε η αίτηση δεδομένων

(π.χ. σήματα ΗΚΓ ή επίπεδα ινσουλίνης) είτε η αποστολή εντολών (π.χ. τροποποιήσεις της θεραπείας).

Οι απειλές ασφαλείας κατά των IMDs μπορούν να κατηγοριοποιηθούν χρησιμοποιώντας την μεθοδολογία STRIDE. Το ακρωνύμιο προκύπτει από έξι γενικές κατηγορίες επιθέσεων: Εξαπάτηση (Spoofing), Παραβίαση (Tampering), Απόρριψη (Repudiation), Αποκάλυψη πληροφοριών (Information Disclosure), Άρνηση παροχής υπηρεσιών (Denial of Service) και Κλιμάκωση Προνομίων (Escalation of Privilege) . Ο Πίνακας 1.1 συσχετίζει κάθε κατηγορία με την υπηρεσία ασφαλείας που μπορεί να δεχτεί επίθεση σε κάθε περίπτωση και παρέχει μερικά παραδείγματα. Γενικά θεωρείται ότι ακολουθεί το ακόλουθο σύνολο σχέσεων (απαρίθμηση της «υπηρεσίας ασφαλείας» έναντι της συνδεδεμένης απειλής): έλεγχος ταυτότητας - εξαπάτηση, ακεραιότητα - παραβίαση, μη απόρριψη - απόρριψη, εμπιστευτικότητα - αποκάλυψη πληροφοριών, διαθεσιμότητα - άρνηση υπηρεσίας, εξουσιοδότηση - κλιμάκωση προνομίων. Εκτός από αυτές τις συνδέσεις one-to-one, πρέπει να σημειωθεί ότι ορισμένες απειλές ενδέχεται να αντιμετωπίζουν διάφορες υπηρεσίες ταυτόχρονα, ή ότι μία η επίθεση μπορεί να αποσυντεθεί σε ατομικές απειλές. Οι έξι υπηρεσίες ασφαλείας που αναφέρονται παραπάνω έχουν τις συνήθεις σημασίες τους, αν και επικεντρώθηκε στον τομέα IMD:

Security Service	Threats	
Authentication	Impersonate the Programmer Impersonate the IMD Impersonate the external device	Spoofing
Integrity	Patient data tampering Malicious inputs Modify communications	Tampering
Non-repudiation	Delete access logs Repeated access attempts	Repudiation
Confidentiality	Disclose medical information Determine the type of IMD Disclose the existence of the IMD Track the IMD	Information Disclosure
Availability	Drain the battery of the IMD Interfere with the IMD communica-tion capabilities Flood the IMD with data	Denial of Service
Authorization	Reprogram the IMD Update the therapy of the patient Switch-off the IMD	Elevation of privileges

Table 1 Μεθοδολογία STRIDE [82]

Εξακρίβωση της γνησιότητας (Authentication) Η ταυτότητα των μελών πρέπει να διαπιστωθεί σωστά πριν την εκτέλεση οποιασδήποτε άλλης ενέργειας. Στον τομέα των εμφυτεύσιμων ιατρικών συσκευών, κάθε συσκευή του συστήματος (IMDs, προγραμματιστής ή εξωτερική συσκευή) μπορεί να υποδυθεί τον εαυτό της. Για παράδειγμα, εάν η ταυτότητα του προγραμματιστή υποκατασταθεί, μπορεί να είναι η αφετηρία για μια επίθεση κλιμάκωσης προνομίων (Privilege Escalation Attack).

Ακεραιότητα (Integrity) Δεδομένα, είτε αποθηκευμένα στη συσκευή είτε μεταδιδόμενα μέσω ασύρματης σύνδεσης, μπορούν να τροποποιηθούν μόνο από εξουσιοδοτημένα μέλη. Εάν δεν υπάρχει μηχανισμός ελέγχου ακεραιότητας στις IMDs, τα δεδομένα θα μπορούσαν να τροποποιηθούν κατά τη διάρκεια της μετάδοσης μέσω του μη ασφαλούς ασύρματου καναλιού. Επιπλέον, οι IMDs θα μπορούσαν να δεχτούν κακόβουλες εισόδους εντολών, οι οποίες θα μπορούσαν να χρησιμοποιηθούν για την εκτέλεση επίθεσης έγχυσης κώδικα (Code injection Attack) [39] . Από την άλλη πλευρά η έλλειψη ελέγχου ακεραιότητας θα διευκόλυνε τη χειραγώγηση των δεδομένων που είναι αποθηκευμένα στη μνήμη των IMDs να μην μπορούν να ανιχνευθούν -ή να ανιχνευθούν στο απώτερο μέλλον.

Μη-Αμφισβήτηση (Non-Repudiation) Οι εργασίες που εκτελούνται από/πάνω στις IMDs φυλάσσονται με ασφάλεια σε αρχείο καταγραφής . Ο επιτιθέμενος θα μπορούσε να επικεντρωθεί στη διαγραφή αυτών των εισόδων προκειμένου να καλύψει τα ίχνη του. Από την άλλη πλευρά, δεν διαθέτουν όλες οι IMDs σύστημα καταγραφής. Αν αυτό συνέβαινε, ο επιτιθέμενος θα μπορούσε να ξαναπροσπαθήσει να αποκτήσει πρόσβαση στις IMD χωρίς να αφήσει ίχνη. Ακόμη και αν υπάρχει σύστημα καταγραφής, τα συμβάντα θα καταγράφονταν αλλά δεν θα υπήρχε συναγερμός για να ειδοποιήσει τον κάτοχο των IMDs σε περίπτωση κακόβουλου συμβάντος.

Εμπιστευτικότητα (Confidentiality) Τα δεδομένα,που είτε αποθηκεύονται στη συσκευή είτε κοινοποιούνται μέσω του ασύρματου συνδέσμου, μπορούν να διαβαστούν μόνο από εξουσιοδοτημένα μέλη. Ειδικότερα, τα IMDs και ο Προγραμματιστής επικοινωνούν μέσω του καναλιού (401-406 MHz) και οι επικοινωνίες αυτές εκτίθενται σε Eavesdroppers. Εάν οι επικοινωνίες δεν είναι κρυπτογραφημένες, ο επιτιθέμενος θα μπορούσε να αποκαλύψει ιδιωτικές πληροφορίες όπως το μοντέλο IMD ή ακόμη και ιατρικές πληροφορίες του ασθενούς.

Αυτό θα έθετε σε κίνδυνο την διστακτικότητα των δεδομένων του κατόχου του εμφυτεύματος. Ακόμα και αν οι επικοινωνίες κρυπτογραφούνται, ένας εισβολέας θα μπορούσε να ανιχνεύσει την παρουσία του εμφυτεύματος ή, ακόμα χειρότερα, να παρακολουθεί τις κινήσεις του κατόχου. Σε αυτή περίπτωση θα ετίθετο σε κίνδυνο η ιδιωτικοτητα της τοποθεσίας.

Διαθεσιμότητα (Availability) Οι υπηρεσίες που προσφέρονται από τις IMD θα πρέπει να είναι διαθέσιμες σε εξουσιοδοτημένα μέλη ανά πάσα στιγμή. Η διαθεσιμότητα είναι ζωτικής σημασίας για τις IMDs, καθώς αυτές οι συσκευές προορίζονται για την θεραπεία ιατρικών παθήσεων των κατόχων τους. Δυστυχώς, μια IMD θα μπορούσε να καταστεί μη προσβάσιμη μέσω του αποκλεισμού του καναλιού (active jamming). Εναλλακτικά, η συσκευή μπορεί να υπερφορτωθεί κατακλύζοντας την IMD με υπερφόρτωση πακέτων. Αυτό θα μπορούσε να χρησιμοποιηθεί για να μπλοκάρει την πρόσβαση στη συσκευή ή για να αδειάσει την μπαταρία της. Εάν η μπαταρία εξαντληθεί, η συσκευή θα καταστεί μόνιμα μη προσβάσιμη και η υγεία του ασθενούς θα μπορούσε να τεθεί σε κίνδυνο.

Εξουσιοδότηση (Authorization) Μια λειτουργία πρέπει να εκτελεστεί μόνο εάν ο αιτούμενος έχει την απαραίτητη εξουσιοδότηση. Για παράδειγμα, οι παράμετροι θεραπείας (πχ. τάση, ρεύμα, όρια, λειτουργία κλπ.), δεν μπορούν να επικαιροποιηθούν από τον ασθενή και μόνο οι γιατροί θα πρέπει να είναι σε θέση να τις τροποποιήσουν. Από την άποψη αυτή, ο επαναπρογραμματιτισμός της IMD πρέπει να γίνεται υπό την κοινή επίβλεψη του γιατρού και ενός τεχνικού (συνήθως από την κατασκευαστική εταιρεία της IMD). Από την άλλη, η IMD πρέπει να λειτουργεί συνεχώς και να απενεργοποιείται μόνο υπό ειδικές συνθήκες που μπορούν να απειλήσουν τη ζωή του ασθενούς (π.χ. καρδιακή χειρουργική επέμβαση με συσκευές ηλεκτροκαυτηριασμου). Στην περίπτωση βηματοδότη, πρέπει να εφαρμόζεται μαγνητικό πεδίο κοντά στη συσκευή (πάνω από το στήθος του ασθενούς) και η διαδικασία αυτή πρέπει να είναι εξουσιοδοτημένη από καρδιολόγο.

ΕΙΔΗ ΕΠΙΤΙΘΕΜΕΝΩΝ

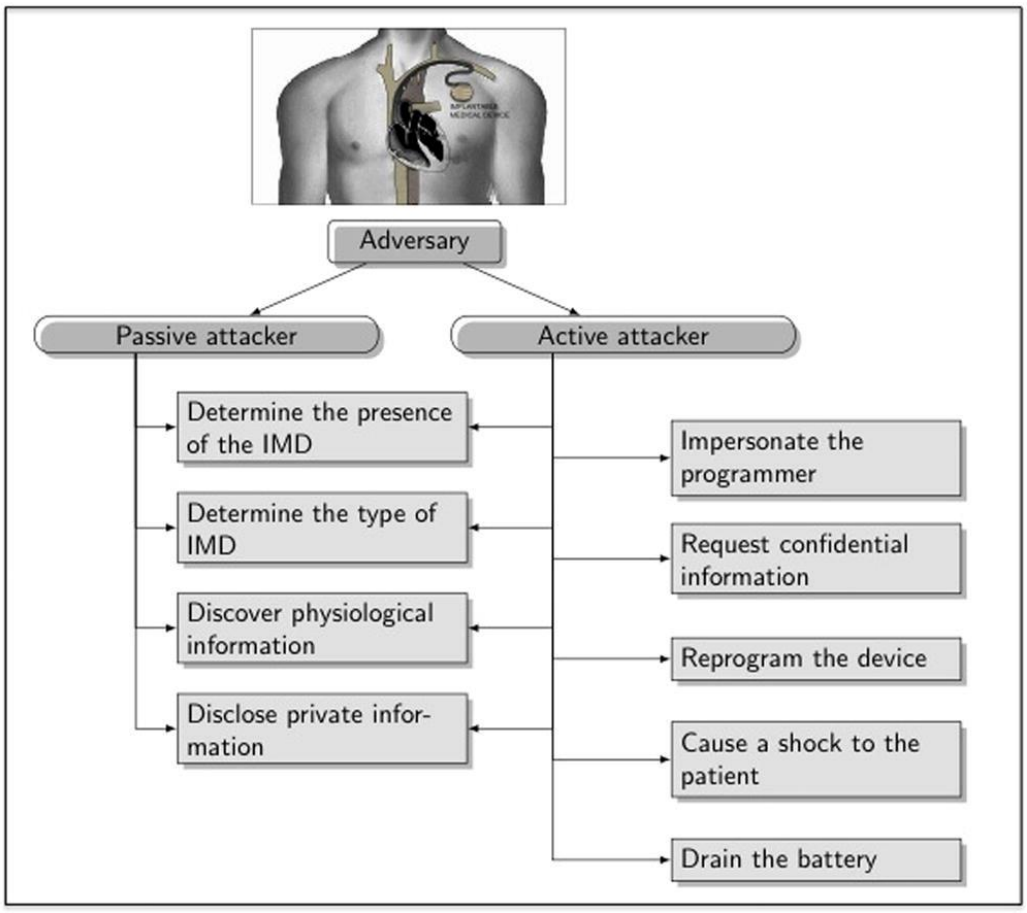

Figure 4 Είδη Επιτιθέμενων [80]

Παθητικός Εισβολέας (Passive Eavesdropper) Ένας παθητικώς εισβολέας μπορεί να ακούσει μόνο το κανάλι και, ως εκ τούτου, να αποκτήσει πρόσβαση στα μηνύματα που ανταλλάσσονται μεταξύ της IMD και του Προγραμματιστή. Υποθέτοντας ότι σε ένα μη ασφαλές κανάλι επικοινωνίας, ένας παθητικός εισβολέας αποτελεί άμεση απειλή για την εμπιστευτικότητα και μπορεί να απειλήσει τον έλεγχο ταυτότητας. Απλά διαβάζοντας μηνύματα ένας παθητικός εισβολέας μπορεί να καθορίσει αν ένα άτομο φέρει ένα εμφύτευμα ή όχι, βρίσκοντας τι είδους εμφύτευμα και άλλα δεδομένα, όπως το μοντέλο, ο σειριακός αριθμός κ.λπ.· καταγράφει δεδομένα τηλεμετρίας και αποκαλύπτει ιδιωτικές πληροφορίες σχετικά με τον ασθενή, όπως την ταυτότητα των αρχείων υγείας του, το όνομα, την ηλικία, τις συνθήκες κ.λπ. Σε όλες τις περιπτώσεις, το συνολικό αποτέλεσμα είναι μια παραβίαση της ιδιωτικής ζωής του ασθενούς.

Ενεργός Επιτιθέμενος (Active Adversary) Σε αυτή την περίπτωση, ο επιτιθέμενος δεν είναι μόνο ικανός να καταγράφει μηνύματα που ανταλλάσσονται μέσω του καναλιού επικοινωνίας, αλλά και να στέλνει εντολές στην IMD, να τροποποιεί μηνύματα κατά τη μεταφορά πριν

φτάσουν στην IMD ή στον Προγραμματιστή ή απλά να τα μπλοκάρει έτσι ώστε να μην φτάσουν ποτέ. Οι επιθέσεις μπορεί να περιλαμβάνουν μια σειρά υποκλοπών, διακοπών, τροποποιήσεων και δημιουργίας μηνυμάτων. Οι στόχοι που επιδιώκει ένας ενεργός εισβολέας είναι διαφορετικοί. Για παράδειγμα, θα μπορούσε να ζητήσει αδιακρίτως πληροφορίες από την IMD με σκοπό την αντηληση της ενέργειας της μπαταρίας του. Θα μπορούσε επίσης να προσπαθήσει να τροποποιήσει τη λειτουργία της συσκευής, να διακόψει την θεραπεία ή να προκαλέσει κάποιου είδους σοκ στον ασθενή [40].

Πρέπει να σημειωθεί ότι δεν είναι απαραίτητο ο επιτιθέμενος (ενεργός ή παθητικός) να βρίσκεται σωματικά κοντά στον ασθενή για να πραγματοποιήσει την επίθεση [41]. Ανάλογα με τη συγκεκριμένη τεχνολογία επικοινωνίας που χρησιμοποιείται για τη σύνδεση του καναλιού, η IMD θα μπορούσε να είναι προσβάσιμη από λίγα μέτρα ή ακόμη και μέχρι 10 μέτρα σε περίπτωση χρήσης προηγμένων τηλεπικοινωνιακών τεχνικών. Επιπλέον, οι συσκευές επικοινωνίας μπορούν να αποκτηθούν πολύ εύκολα στις μέρες μας. π.χ. ορισμένα smartphones μπορούν να εκτελέσουν αυτήν την εργασία.

Συνοπτικά, τα τεχνικά μέσα που απαιτούνται για την πραγματοποίηση των περισσότερων επιθέσεων κατά των IMDs είναι φθηνά και εύκολα στην απόκτηση και χρήση τους. Κατά συνέπεια, οι παθητικοί επιτιθέμενοι μπορούν εύκολα να κρυφακούσουν ευαίσθητες πληροφορίες σχετικά με έναν κάτοχο εμφυτεύματος χωρίς μεγάλη δυσκολία. Ακόμα και αν ο επιτιθέμενος δεν είναι κάποιος που προσπαθεί να απειλήσει την ασφάλεια του ασθενούς, τα δεδομένα που είναι αποθηκευμένα σε αυτό μπορεί να είναι πολύ πολύτιμα για πολλά άτομα και οργανισμούς.

Τέλος, εκτός από τα γενικά τρωτά σημεία του συστήματος και των καναλιών, οι επιτιθέμενοι μπορούν να χειριστούν μια σειρά από λειτουργίες που αφορούν τις IMD για την επίτευξη των στόχων τους [42] [43]:

- *Χειρισμός της απόστασης*. Η εγγύτητα αναφέρεται στην απόσταση μεταξύ του εισβολέα και της IMD. Πολλές τρέχουσες προτάσεις έχουν κάποια μορφή ελέγχου πρόσβασης βάσει αποστάσεων, επιτρέποντας την πρόσβαση στην IMD μόνο εάν ο προγραμματιστής βρίσκεται σε μικρή απόσταση. Το σκεπτικό εδώ είναι να αναγκάσουμε τον επιτιθέμενο να είναι σωματικά πολύ κοντά στον ασθενή για να πραγματοποιήσει την επίθεση. Στην πράξη, ωστόσο, ο επιτιθέμενος μπορεί να χρησιμοποιήσει μια παραβιασμένη συσκευή κοντά στον ασθενή για να ξεκινήσει την

επίθεση, συμπεριλαμβανομένων εκείνων που χρησιμοποιούνται σε ιατρικές εγκαταστάσεις.

- *Χειρισμός των λειτουργιών των IMD.* Οι IMD είναι προγραμματισμένες να εκτελούν διάφορες δραστηριότητες, όπως η ανίχνευση βιοϊατρικών παραμέτρων στην περιοχή του σώματος όπου εμφυτεύονται, η θεραπεία μιας ιατρικής κατάστασης (ενεργοποίηση), η επεξεργασία δεδομένων που συλλέγονται και η επικοινωνία με άλλες συσκευές [44]. Αυτές οι λειτουργίες μπορούν να χρησιμοποιηθούν καταχρηστικά από έναν εισβολέα, για παράδειγμα με την πρόκληση εσφαλμένης ανίχνευσης για την ενεργοποίηση μιας συγκεκριμένης απόκρισης στο εμφύτευμα.
- *Χειρισμός της κατάστασης του ασθενούς* Η κατάσταση του ασθενούς παίζει βασικό ρόλο στο σχεδιασμό πολλών αντιμέτρων. Για παράδειγμα, ένας εμφυτευμένος βιοαισθητήρας μπορεί να ενεργοποιήσει έναν συναγερμό εάν ορισμένες παράμετροι τεθούν εκτός του εύρους ασφαλείας. Σε ορισμένες περιπτώσεις, ένας τέτοιος συναγερμός θέτει την IMD σε κατάσταση έκτακτης ανάγκης και απενεργοποιεί αυτόματα τους μηχανισμούς ελέγχου πρόσβασης.

2.3 Περιορισμοί

Οι IMD έχουν περιορισμένες δυνατότητες σε τρεις ξεχωριστές διαστάσεις: ενέργεια, αποθήκευση και υπολογιστική ισχύ. Και οι τρεις έχουν επιπτώσεις στην ασφάλεια, είτε επειδή μπορούν να χρησιμοποιηθούν καταχρηστικά είτε επειδή περιορίζουν τους μηχανισμούς ασφαλείας που μπορούν να αποκτηθούν.

Ενέργεια (Energy) Οι IMDs τροφοδοτούνται από μια ενσωματωμένη μπαταρία που παρέχει ενέργεια σε όλες τις λειτουργίες που ενσωματώνονται στη συσκευή (π.χ. παρακολούθηση, επεξεργασία, επικοινωνία κ.λπ.). Μόλις εμφυτευτεί η IMD, η μπαταρία μπορεί να διαρκέσει από 8 χρόνια στην περίπτωση νευροδιεγερτών [45] έως 10 έτη στην περίπτωση βηματοδότη [46]. Η χρήση της μπαταρίας έχει άμεσο αντίκτυπο κατά τη διάρκεια ζωής του εμφυτεύματος. Μόλις εξαντληθεί, πρέπει να αντικατασταθεί, η οποία απαιτεί χειρουργική διαδικασία με τους σχετικούς κινδύνους. Ορισμένα μοντέλα υποστηρίζουν μπαταρίες που μπορούν να φορτιστούν ασύρματα χρησιμοποιώντας μαγνητικά πεδία, αλλά τα όργανα κοντά στο εμφύτευμα θα μπορούσαν να καταστραφούν.

Αποθήκευση (Storage) Η αποθήκευση είναι αρκετά περιορισμένη στις τρέχουσες IMDs. Η μνήμη που είναι διαθέσιμη στη συσκευή χρησιμοποιείται για την αποθήκευση ιστορικών

δεδομένων από διαφορετικά συμβάντα και επεισόδια που προκύπτουν σχετικά με την παθολογία του ασθενούς. Για παράδειγμα, οι βηματοδότες και τα ICD αποθηκεύουν σήματα ΗΚΓ που συνέβησαν όταν η συσκευή αποφάσισε να εφαρμόσει διέγερση. Η μνήμη RAM αυτής της συσκευής κυμαίνεται από 2 KB έως 36 KB για την πρώτη και από 128 KB έως 1024 KB για την τελευταία. Στην περίπτωση των ICD, περίπου το 75% αυτής της μνήμης αφιερώνεται στην αποθήκευση σημάτων ΗΚΓ [47] .Οι συσκευές με χαμηλό ρυθμό ανίχνευσης όπως ένας Βιοστατικος Ελεγκτής Γλυκόζης απαιτούν 8 KB για αποθήκευση δεδομένων [48] . Μια συνέπεια της ενσωμάτωσης μιας μειωμένης μνήμης on-chip είναι ότι οι μηχανισμοί ασφαλείας πρέπει να καταναλώνουν όσο το δυνατόν λιγότερη μνήμη για να την αποθηκεύσουν για τις πιθανές απαιτήσεις αποθήκευσης που απαιτούνται από τις ιατρικές λειτουργίες της συσκευής. Μπορεί κανείς να αναρωτηθεί για την πιθανότητα αύξησης της ποσότητας μνήμης RAM στις IMDs, δεδομένου ότι αυτό το είδος μνήμης δεν είναι ακριβό στις μέρες μας. Φαίνεται να υπάρχουν δύο κύριοι λόγοι για τη διατήρηση των περιορισμών στο μέγεθος της μνήμης. Από τη μία πλευρά, η αύξηση της ποσότητας μνήμης συνιστά αύξηση του μεγέθους του εμφυτεύματος. Αυτό είναι ένα κρίσιμο χαρακτηριστικό, δεδομένου ότι οι IMDs βρίσκονται συχνά μέσα ή πάνω στο σώμα του ασθενούς και αυτή η παράμετρος (περιοχή συσκευής) θα πρέπει να διατηρείται στο ελάχιστο. Από την άλλη, ακόμα και αν το μέγεθος της συσκευής δεν αποτελεί πρόβλημα, η αύξηση της ποσότητας μνήμης θα μπορούσε να επηρεάσει τη διάρκεια ζωής της μπαταρίας. Οι λειτουργίες πρόσβασης (π.χ. ανάγνωση, γραφή και διαγραφή) απαιτούν κατανάλωση ενέργειας [49] , οπότε η εκτέλεσή τους σε μεγάλο όγκο δεδομένων θα μείωνε τη διάρκεια ζωής της μπαταρίας και ακόμη και θα την εξαντλούσε σε σύντομο χρονικό διάστημα.

Υπολογιστική Δύναμη και Επικοινωνία (Computing and Communication) Τόσο οι δυνατότητες υπολογιστικής δύναμης όσο και επικοινωνίας είναι εξαιρετικά περιορισμένες στις IMD λόγω περιορισμών ισχύος. Η επικοινωνία είναι το πιο ενεργοβορο τμήμα για τις IMD. Ως εκ τούτου, εάν ελαχιστοποιηθούν οι επικοινωνίες, η διάρκεια ζωής της μπαταρίας μπορεί να παραταθεί [50] [51]. Όσον αφορά την υπολογιστική δύναμη, αυτή υποστηρίζεται γενικά από έναν μικροσκοπικό μικροελεγκτή. Για παράδειγμα, ένας μικρο-νευροδιεγερτης καταναλώνει μια περιοχή περίπου 5mm2, η οποία είναι περίπου σαράντα φορές μικρότερη από την περιοχή που χρησιμοποιείται για έναν μικροελεγκτή γενικής χρήσης [52] . Σε γενικές γραμμές, ολόκληρο το τσιπ του εμφυτεύματος καταλαμβάνει μια έκταση περίπου αρκετών εκατοντάδων τετραγωνικών χιλιοστών.

2.4 Σημεία Τριβής και Αντιπαραθέσεων

Όπως περιγράφεται στο τμήμα 2.1.2 ,η IMD μπορεί να λειτουργήσει με δύο τρόπους λειτουργίας: *κανονική και εκτάκτου ανάγκης*. Οι μηχανισμοί που έχουν σχεδιαστεί για τη διατήρηση των ιδιοτήτων ασφάλειας και προστασίας της ιδιωτικής ζωής και στους δύο τρόπους πρέπει να εξετάζουν διάφορες εντάσεις:

Security vs Safety Σήμερα σε ένα πραγματικό σενάριο είναι κοινότοπο να υποθέσουμε ότι όλα τα μέσα, τόσο τα θεμιτά (νέα γενιά IMDs, εξωτερικές συσκευές και προγραμματιστές) όσο και τα αθέμιτα (ενεργοί και παθητικοί εισβολείς) θα έχουν συνδεσιμότητα δικτύου. Αυτό θα πρέπει να οδηγήσει στη δημιουργία επιτυχών λύσεων ασφάλειας για την πρόληψη συμβάντων. Συγκεκριμένα, σε κανονική λειτουργία η IMD είναι ευάλωτη σε διάφορες επιθέσεις. Οι επιτιθέμενοι θα μπορούσαν να βρίσκονται φυσικά σε μεγάλη απόσταση από την IMD και να χρησιμοποιούν τις δυνατότητες ασύρματης επικοινωνίας της — ίσως βασιζόμενοι σε μια κοντινή συσκευή μεσολάβησης — για να λαμβάνουν αιτήματα δεδομένων και να εκτελούν λειτουργίες ενημέρωσης. Οποιαδήποτε προτεινόμενη λύση πρέπει να εγγυάται βασικές ιδιότητες ασφάλειας και προστασίας προσωπικών δεδομένων σε αυτή την περίπτωση. Ωστόσο, κατά τη διάρκεια μιας έκτακτης ανάγκης το ιατρικό προσωπικό πρέπει να είναι σε θέση να έχει πρόσβαση στο εμφύτευμα γρήγορα και χωρίς περιορισμούς. Έτσι, ενώ η χρήση ισχυρών μέτρων ασφαλείας θα μπορούσε να παρέχει υψηλό επίπεδο προστασίας, μπορεί επίσης να θέσει σε κίνδυνο την ασφάλεια του ασθενούς κατά τη διάρκεια μιας κατάστασης έκτακτης ανάγκης. Ο συμβιβασμός μεταξύ ασφάλειας και προστασίας είναι μία από τις πιο κρίσιμες πτυχές στον σχεδιασμό μηχανισμών ασφαλείας για τα IMDs.

Διάρκεια Μπαταρίας κατά των Δυνατοτήτων των IMD Όπως προαναφέρθηκε, οι IMDs έχουν σοβαρούς περιορισμούς όσον αφορά την κατανάλωση ενέργειας, καθώς η παράταση της διάρκειας ζωής της μπαταρίας αποτελεί βασική προϋπόθεση. Με τη σειρά του, αυτό περιορίζει τον αριθμό των υπολογισμών και των επικοινωνιών που εμπλέκονται στις λειτουργίες ασφαλείας. Αυτό υποχρεώνει το σχεδιασμό νέων μηχανισμών ασφάλειας και προστασίας προσωπικών δεδομένων που δεν είναι πολύ απαιτητικοί όσον αφορά τον υπολογισμό, τις επικοινωνίες και την αποθήκευση. Ένα ενδιαφέρον γεγονός από την άποψη αυτή επισημάνθηκε [53]: η κατανάλωση ενέργειας αυξάνεται δραστικά εάν αυξηθεί το ποσοστό μεταφοράς δεδομένων. Έτσι, αν και μπορεί να φαίνεται αντιπαραγωγικό, είναι προτιμότερο να

βασίζεστε σε μεγάλες μεταδόσεις με πολύ χαμηλό ρυθμό bit παρά σε σύντομες ανταλλαγές δεδομένων με μεγάλη ταχύτητα.

Αρκετές λύσεις έχουν αντιμετωπίσει το πρόβλημα της εξοικονόμησης ή επαναφόρτισης της μπαταρίας των IMDs προκειμένου να παραταθεί ο χρόνος αντικατάστασης όσο το δυνατόν περισσότερο. Σαν παράδειγμα είναι η καινοτόμος λύση για την παροχή υψηλότερης νοημοσύνης στους νευροδιεγερτές. Η ιδέα είναι να παρασχεθεί στο εμφύτευμα η δυνατότητα πρόβλεψης των τρεμουλιασμάτων λόγω Πάρκινσον, έτσι ώστε μόνο εκείνη τη στιγμή να ενεργοποιείται μια διέγερση στον υποθάλαμο. Μόλις μειωθεί το τρεμούλιασμα, το εμφύτευμα σταματά τη διέγερση. Έξυπνες λύσεις όπως αυτές θα μπορούσαν να παρατείνουν τη διάρκεια ζωής της μπαταρίας.

Άλλες προσεγγίσεις έχουν προτείνει τεχνικές για την ασύρματη επαναφόρτισης της μπαταρίας . Ένα παράδειγμα [54] , όπου προτείνεται ένα πηνίο με παράλληλο πυκνωτή. Σε αυτό το σύστημα, το πηνίο εκπέμπει ενέργεια συνδέοντας ένα σήμα στη συχνότητα συντονισμού (300 Mhz εν προκειμένω). Τα συστήματα αυτά θα επέτρεπαν στις IMDs να λειτουργούν χωρίς μπαταρία, κάτι που θα ήταν ιδιαίτερα επιθυμητό, δεδομένου ότι η διαδικασία αντικατάστασης της μπαταρίας θα μπορούσε να αποφευχθεί.

Χρόνος Απόκρισης Εάν η αλληλεπίδραση με το εμφύτευμα διαρκεί πολύ λόγω των γενικών περιορισμών που επιβάλλονται από τους ελέγχους ασφαλείας, η προστασία του ασθενούς θα μπορούσε να τεθεί σε κίνδυνο. Οι έλεγχοι αυτοί θα πρέπει να αναλυθούν ώστε να διασφαλιστεί ότι ο χρόνος απόκρισης τους στη χειρότερη περίπτωση είναι εντός εύλογου εύρους.

Εν ολίγοις, οι τριβές μεταξύ της ασφάλειας (δηλαδή της διασφάλισης της πρόσβασης σε κρίσιμες συνθήκες) και της προστασίας (επιτρέποντας την πρόσβαση μόνο σε εξουσιοδοτημένα πρόσωπα), σε συνδυασμό με τους περιορισμούς που υπάρχουν στις τρέχουσες πλατφόρμες IMD, δημιουργούν μοναδικές προκλήσεις στην ανάπτυξη κατάλληλων μηχανισμών ασφαλείας για τα IMDs. Η προσαρμογή λύσεων που προτείνονται σε άλλα παρόμοια περιβάλλοντα (π.χ. ασύρματα δίκτυα αισθητήρων) δεν είναι απλή, καθώς ερωτήματα όπως ο τρόπος με τον οποίο πρέπει να συμπεριφέρονται οι μηχανισμοί ασφαλείας σε κατάσταση έκτακτης ανάγκης —και, το σημαντικότερο, η εγγύηση ότι η ύπαρξη αυτής της λειτουργίας δεν γίνεται καταχρηστικά από έναν εισβολέα— εξακολουθούν να αποτελούν ανοικτά προβλήματα.

2.5 Μέτρα Προστασίας

Σε αυτήν την ενότητα, αναφέρουμε διαφορετικούς μηχανισμούς ασφαλείας που έχουν προταθεί για την αποτροπή απειλών κατά της ασφάλειας των IMDs. Πολλές από αυτές τις προτάσεις αφορούν ρητά τους συμβιβασμούς και τις τριβές που συζητήθηκαν προηγουμένως, ενώ άλλες επικεντρώνονται απλώς στην εξουδετέρωση συγκεκριμένων επιθέσεων. Η πλειοψηφία αυτών είναι προληπτικοί και προσπαθούν να σταματήσουν τις επιθέσεις από το να συμβούν εξ αρχής, αν και έχουν επίσης προταθεί μηχανισμοί ανίχνευσης και διόρθωσης. Στην ιδανική περίπτωση, η συμπερίληψη μέτρων ασφαλείας δεν θα πρέπει να απαιτεί τροποποίηση της IMD, καθώς αυτό θα σήμαινε την αντικατάστασή της και, ως εκ τούτου, μια χειρουργική επέμβαση. Η εναλλακτική λύση θα ήταν η εφαρμογή λειτουργιών ασφαλείας σε εξωτερικές συσκευές ή ανεξάρτητες μονάδες του τσιπ της IMD. Σύμφωνα με αυτή την προσέγγιση, το λογισμικό που τρέχει στο εμφύτευμα θα χρησιμοποιηθεί αποκλειστικά για τη θεραπεία της ιατρικής κατάστασης του ασθενούς.

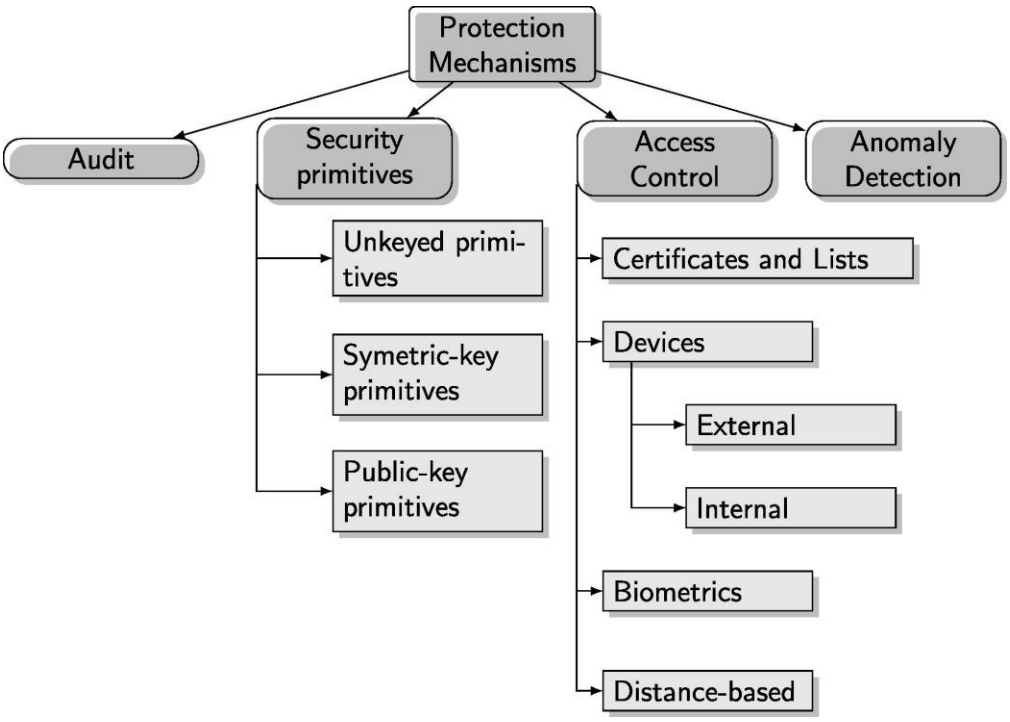

Figure 5 Μέτρα προστασίας [81]

Όπως προαναφέρθηκε, ένα σημαντικό πρόβλημα με τα περισσότερα μέτρα ασφαλείας είναι ότι θα μπορούσαν να θέσουν σε κίνδυνο την προστασία του ασθενούς σε καταστάσεις έκτακτης ανάγκης εάν δεν μπορούν να απενεργοποιηθούν εύκολα. Η χρήση κάποιας μορφής

κερκοπορτας(backdoor) για να παρακάμψει την ασφάλεια θα μπορούσε να είναι μια απλή λύση, αν και είναι πολύ εύκολα χειραγωγησιμη από έναν εισβολέα.

2.5.1 Έλεγχος

Ένας από τους απλούστερους μηχανισμούς ασφαλείας συνίσταται στη συνεχή καταγραφή όλων των προσβάσεων –εξουσιοδοτημένων ή μη– συμπεριλαμβανομένου και του ασθενούς. Πρόκειται για μέτρο που αποσκοπεί στη διευκόλυνση του εντοπισμού μη επιτρεπόμενων ενεργειών και αποτελεί πολύτιμη πηγή αποδεικτικών στοιχείων για τη λήψη επακόλουθων ενεργειών. Ως εκ τούτου, ο έλεγχος συμβάλλει στην καταπολέμηση των απειλών κατά της μη αμφισβήτησης. Επομενως, δεν εμποδίζει την εμφάνιση επιθέσεων, αλλά μπορεί να λειτουργήσει ως αποτρεπτικό στοιχείο εάν εφαρμοστεί κατάλληλα . Ως εκ τούτου, αυτού του είδους οι λύσεις θα πρέπει να συμπληρωθούν με κατάλληλους μηχανισμούς για τον εντοπισμό και τον αποκλεισμό τέτοιων επιθέσεων, καθώς και μέτρα για την αποτροπή τους (π.χ. κρυπτογραφικές λύσεις ή λύσεις ελέγχου πρόσβασης).

Το κύριο πρόβλημα που αντιμετωπίζουν οι προτάσεις ελέγχου είναι η περιορισμένη ποσότητα μνήμης που είναι διαθέσιμη στις IMDs. Για παράδειγμα, ολόκληρη η μνήμη ενός ICD είναι μικρότερη από 1 MB και περίπου το 75% αυτής της μνήμης χρησιμοποιείται για ιατρικές λειτουργίες. Σε αυτή την περίπτωση, μόνο μερικές εκατοντάδες kilobyte θα μπορούσαν να χρησιμοποιηθούν για συμβάντα καταγραφής, τα οποία είναι εξαιρετικά περιορισμένα. Μια πρόσθετη μνήμη θα μπορούσε να τοποθετηθεί στο τσιπ, αλλά αυτό θα αύξανε το μέγεθος της IMD, το οποίο δεν συνιστάται.

Για να αποφευχθεί η αύξηση της μνήμης των IMD, η εργασία καταγραφής μπορεί να βασιστεί σε μια εξωτερική συσκευή χωρίς περιορισμούς μνήμης και υπολογισμού. Ένα παράδειγμα στο πλαίσιο των συστημάτων RFID είναι το "RFID Guardian" [39] , το οποίο συλλέγει και αναλύει στοιχεία για όλα τα συμβάντα σε προκαθορισμένο εύρος. Μια παρόμοια προσέγγιση, που ονομάζεται MedMon, προτάθηκε πρόσφατα για εφαρμογές IMD και ηλεκτρονικής υγείας [55] .Οι δημιουργοί προτείνουν τη χρήση μιας εξωτερικής συσκευής που λειτουργεί ως οθόνη παρακολούθησης καταγράφοντας και αναλύοντας όλες τις επικοινωνίες από και προς την IMD. Τα δεδομένα αποθηκεύονται τοπικά στην εξωτερική συσκευή και θα μπορούσε να σημάνει συναγερμός για να ειδοποιηθεί ο ασθενής. Μια πιο δραστική λύση μπορεί να περιλαμβάνει τον αποκλεισμό του διαύλου επικοινωνίας εάν εντοπιστεί μια εισβολή.

2.5.2 Μέτρα Κρυπτογράφησης

Οι λύσεις ασφαλείας που βασίζονται στην κρυπτογράφηση εξαρτώνται σε μεγάλο βαθμό από κρυπτογραφικά πρότυπα, τα οποία μπορούν να κατηγοριοποιηθούν σε τρεις κύριες ομάδες [56] , όπως φαίνεται στο παραπάνω Σχήμα. Τα πρότυπα, όπως οι συναρτήσεις κατακερματισμού (hash functions) ή οι μονόδρομες μεταθέσεις (one-way permutations), είναι κρυπτογραφικά εργαλεία που δεν χρησιμοποιούν κανένα κλειδί. Μέσα στα κρυπτογραφικά εργαλεία που χρησιμοποιούν κλειδί μπορούμε να τις διακρίνουμε σε συμμετρικού και δημόσιου κλειδιού. Σε πρότυπα που χρησιμοποιείται συμμετρικό κλειδί, μοιράζεται ένα κλειδί μεταξύ των αξιόπιστων μερών . Ο τύπος των προτύπων σε αυτή την κατηγορία ποικίλλει, συμπεριλαμβανομένων συμμετρικών βασικών κρυπτογράφων (κρυπτογράφηση μπλοκ και ροής), κωδικών ελέγχου ταυτότητας μηνυμάτων (MACs), ακολουθιών ψευδοτυχαιοτητας και πρωτότυπων αναγνώρισης. Από την άλλη, οι κρυπτογράφοι δημόσιου κλειδιού και οι υπογραφές είναι δύο παραδείγματα προτύπων ασύμμετρων κλειδιών. Σε αυτόν τον τύπο αλγορίθμων χρησιμοποιούνται δύο κλειδιά, το ένα είναι δημόσιο και το άλλο πρέπει να κρατηθεί μυστικό.

Στο πλαίσιο των IMDs, τα κρυπτογραφικά μέτρα είναι αποτελεσματικοί μηχανισμοί για την προστασία του καναλιού ασύρματης επικοινωνίας και των αρχείων που είναι αποθηκευμένα στη συσκευή, από παραποίηση και αποκάλυψη πληροφοριών. Επιπλέον, τα κρυπτογραφικά πρωτόκολλα παρέχουν επίσης ένα μέσο για τον έλεγχο και τη διαχείριση των προσβάσεων στις IMD, παρέχοντας έτσι προστασία από την πλαστογράφηση και, σε ορισμένες περιπτώσεις, στις επιθέσεις με σκοπό την κλιμάκωση των προνομίων. Τόσο τα συμμετρικά [40] [57] όσο και τα συστήματα δημόσιου κλειδιού [78] έχουν προταθεί για τις εφαρμογές αυτές [59], αν και οι τελευταίες είναι σημαντικά ακριβότερες όσον αφορά την επικοινωνία, τον υπολογισμό και την κατανάλωση ενέργειας. Τα πρωτόκολλα που βασίζονται σε κρυπτογραφικά συστήματα δημόσιου κλειδιού συχνά ανταλλάσσουν μεγάλο αριθμό μηνυμάτων, γεγονός που τα καθιστά αρκετά απαιτητικά για ενέργεια, καθώς η αποστολή και η λήψη μηνυμάτων καταναλώνουν ενέργεια. Επιπλέον, οι κρυπτογράφοι δημόσιου κλειδιού οδηγούν σε πολύπλοκα κυκλώματα που καταναλώνουν υπερβολικούς πόρους (υλικό και μνήμη) και είναι αναποτελεσματικά όσον αφορά την κατανάλωση ενέργειας [60] [61] . Λόγω των περιορισμών πόρων που αναφέρονται παραπάνω για την τρέχουσα γενιά εμφυτευμάτων, οι λύσεις που βασίζονται σε συμμετρικές προσεγγίσεις-κλειδιά είναι η προτιμώμενη επιλογή. Τυποποιημένα πρωτόκολλα όπως αυτό που προτείνεται στο ISO/IEC 9798 βασίζονται στη χρήση συμμετρικών προτύπων (δηλ.

συμμετρική κρυπτογράφηση ή λειτουργία κατακερματισμού με χρήση κλειδιού) και τα κρυπτογραφημένα διακριτικά περιλαμβάνουν τυχαίους αριθμούς για να εγγυηθεί τη ανανέωση μεταξύ των αποστολών.

Οι συμμετρικοί κρυπτογραφικοί συνδυασμοί παρουσιάζουν αδυναμίες σχετικά με την διανομή κλειδιών. Σε γενικές γραμμές, οι IMD και άλλες εξουσιοδοτημένες συσκευές, όπως ο προγραμματιστής, πρέπει να μοιράζονται ένα κλειδί (ή ένα σύνολο κλειδιών) που χρησιμοποιείται για τη δημιουργία διακριτικών ελέγχου ταυτότητας για την απόκτηση πρόσβασης στις IMD και για την κρυπτογράφηση επικοινωνιών. Η καταλληλότητα ενός συγκεκριμένου βασικού συστήματος διανομής εξαρτάται από το είδος των IMD, τις αναμενόμενες αλληλεπιδράσεις με άλλα μέρη και άλλες παραδοχές σχετικά με το επιχειρησιακό περιβάλλον. Για παράδειγμα, εάν ο προγραμματιστής και η IMD θα έχουν μια μόνιμη σχέση, μπορεί να χρησιμοποιηθεί ένα προκαθορισμένο κλειδί. Αυτή η λύση μπορεί να ισχύει όταν ο προγραμματιστής είναι πάντα μια συσκευή που ανήκει στον ασθενή ή στον γιατρό. Σε αυτές τις περιπτώσεις, μια πρώτη προσέγγιση συνίσταται στην προ φόρτωση ενός κλειδιού στις εξουσιοδοτημένες συσκευές. Αυτό το κλειδί ενδέχεται να επαναδιαπραγματευτεί μεταξύ των σχετικών μερών κατά την πρώτη επικοινωνία για την ενημέρωση του. Τονίζουμε εδώ ότι αυτό είναι ζωτικής σημασίας για την προστασία αυτών των κλειδιών και εγγυάται ότι μόνο εξουσιοδοτημένοι φορείς (δηλαδή ο ασθενής και το προσωπικό υγειονομικής περίθαλψης) έχουν πρόσβαση σε αυτά .Τα κλειδιά αυτά θα χρησιμοποιηθούν για τη δημιουργία διαφόρων κρυπτογραφικών τμημάτων (tokens).

Άλλες λύσεις συστήνουν, τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται από τις IMD να μπορούν να αποθηκευτούν σε μια εξωτερική φορητή συσκευή, όπως μια έξυπνη συσκευή. Η εξωτερίκευση του κλειδιού συνεπάγεται σημαντικό κίνδυνο, καθώς η απώλεια μιας τέτοιας συσκευής (π.χ. εάν ο ασθενής υποστεί απώλειες ή ζημιά της έξυπνης συσκευής) θα καθιστούσε την IMD απρόσιτη ή/και θα διευκόλυνε την πρόσβαση σε μη εξουσιοδοτημένους χρήστες [64] .Μερικοί εισηγητές προτείνουν να τυπωθεί το κλειδί στο δέρμα του ασθενούς χρησιμοποιώντας υπεριώδη χρώση (δηλ. αόρατα τατουάζ) που μπορούν να διαβαστούν από το ιατρικό προσωπικό σε περίπτωση έκτακτης ανάγκης [65].

Στην περίπτωση σποραδικών επικοινωνιών με εξουσιοδοτημένες συσκευές που παρ' όλα αυτά δεν γνωρίζουν το κλειδί πρόσβασης, πρέπει να υποστηρίζεται ένα πρωτόκολλο αναγνώρισης . Η παροχή εμπιστευτικού διαύλου μεταξύ της IMD και του προγραμματιστή είναι ένας άλλος σημαντικός στόχος κατά τη χρήση κρυπτογραφικών λύσεων. Ορισμένες προσεγγίσεις

υποδηλώνουν την εκμετάλλευση της περιορισμένης κάλυψης του φυσικού στρώματος (Physical Layer) κατά τη φάση προετοιμασίας. Οι περισσότερες προτάσεις βασίζονται σε συμμετρικούς κρυπτογράφους [40] , και ορισμένες από αυτές ενσωματώνουν έναν βασικό μηχανισμό ενημέρωσης. Πρόσφατα, έχει προταθεί μια νέα αρχιτεκτονική IMD, που αξιολογείται σε ένα τεχνητό εμφύτευμα παγκρέατος. Σε αυτή την περίπτωση, το εμφύτευμα περιλαμβάνει δύο ξεχωριστούς πυρήνες (θεραπεία ασθένειας και εργασίες ασφαλείας) και η συνολική κάλυψη για την ασφάλεια σε τομείς υλικής και ενεργειακής κατανάλωσης είναι μηδαμινή [48].

Η χρήση τυποποιημένων κρυπτογραφικών λύσεων για την παροχή υπηρεσιών ασφαλείας σε IMD έχει δεχθεί κριτική, τόσο για λόγους χρηστικότητας όσο και για την έλλειψη αυστηρότητας στην ανάλυση πολλών προτάσεων [66] . Τα κύρια μειονεκτήματα που θα συνεπαγόταν την αποκλειστική χρήση αυτών των λύσεων είναι [67] :

Εναλλακτικότητα Η ενσωμάτωση κρυπτογραφικών μηχανισμών στη συσκευή σημαίνει ότι τα τρέχοντα εμφυτεύματα πρέπει να επανασχεδιαστούν και να αντικατασταθούν. Αυτό θα αναγκάσει τους ασθενείς να υποβληθούν σε χειρουργική επέμβαση μόνο για να αποκτήσουν μια πιο ασφαλή συσκευή, καθώς οι λειτουργίες θεραπείας δεν παρουσιάζουν κανένα πρόβλημα

Προστασία του Ασθενούς Η χρήση κρυπτογραφικών μέτρων που είναι ενσωματωμένα στη συσκευή δημιουργεί προβλήματα σε καταστάσεις έκτακτης ανάγκης στις οποίες η επικοινωνία με το IMD είναι απαραίτητη ακόμη και για μη εξουσιοδοτημένα μέλη (δηλαδή προγραμματιστές που δεν γνωρίζουν το κλειδί πρόσβασης).

Συντήρηση Καθώς εφαρμόζονται μέτρα ασφαλείας στη συσκευή, αυξάνεται ο όγκος του λογισμικού που είναι ενσωματωμένο στο εμφύτευμα, γεγονός που συνεπάγεται μεγαλύτερη πιθανότητα σφαλμάτων. Πολλοί εισηγητές υποστηρίζουν την ιδέα του περιορισμού όσο το δυνατόν περισσότερο του λογισμικού που εκτελείται στη συσκευή, διατηρώντας μόνο εκείνες τις απαραίτητες λειτουργίες για τη θεραπεία που σχεδιάστηκε.

2.5.3 Έλεγχος Πρόσβασης

Οι μηχανισμοί ελέγχου πρόσβασης αποτρέπουν μη εξουσιοδοτημένους χρήστες των λειτουργιών των IMD. Πριν προχωρήσει σε μια συγκεκριμένη ενέργεια (π.χ. πρόσβαση, ανάγνωση, επαναπρογραμματισμός κ.λπ.), τα δικαιώματα του αιτούντος αξιολογούνται με σκοπό να εκτιμηθεί εάν είναι εξουσιοδοτημένος να εκτελέσει τη συγκεκριμένη ενέργεια ή όχι.

Ειδικότερα, οι επιτρεπόμενες και απαγορευμένες λειτουργίες διέπονται από πολιτικές ελέγχου πρόσβασης που καθορίζουν ποιος μπορεί να κάνει τι, ενδεχομένως ανάλογα με το πλαίσιο στο οποίο πραγματοποιείται το αίτημα πρόσβασης. Σημειώστε ότι, ο έλεγχος πρόσβασης είναι πλήρως συμβατός με άλλα μέτρα ασφαλείας, όπως κρυπτογραφικά πρωτόκολλα για την προστασία του καναλιού επικοινωνίας. Επιπλέον, ο έλεγχος πρόσβασης απαιτεί γενικά προηγούμενη εξακρίβωση της γνησιότητας, καθώς οι αποφάσεις σχετικά με το αν μια πράξη επιτρέπεται ή όχι λαμβάνονται με βάση την ταυτότητα του αιτούντος, ο οποίος πρέπει να έχει προηγουμένως έχει ταυτοποιηθει. Παρακάτω περιγράφεται μια σειρά μοντέλων ελέγχου πρόσβασης που προτείνονται για IMDs και αναφέρονται τα κύρια πλεονεκτήματα και οι περιορισμούς τους.

2.5.4 Πιστοποιητικά και Λύσεις βάσει Λιστών

Υπάρχουν δύο κλασικοί μηχανισμοί ελέγχου ταυτότητας που προσαρμόζονται για IMDs [64] . Ο ένας βασίζεται σε λίστες ελέγχου πρόσβασης (ACL)—εφαρμογή μοντέλων ελέγχου πρόσβασης διακριτικής ευχέρειας με βάση τον πίνακα πρόσβασης—, ενώ ο δεύτερος βασίζεται σε υποδομή δημόσιου κλειδιού (PKI). Η ACL καθορίζει ποιες λειτουργίες έχει εξουσιοδοτηθεί να εκτελεί ένας χρήστης με έλεγχο ταυτότητας. Οι άδειες αυτές είναι μόνιμες μετά την προγραμματισμένη ACL. Έτσι, αν και μπορεί να επαναπρογραμματιστεί στο μέλλον, προορίζεται για την παροχή μόνιμης πρόσβασης σε ορισμένους χρήστες. Αντίθετα, στις λύσεις βασισμένες στο PKI, η σχέση μεταξύ της IMD και του χρήστη είναι παροδική. Συγκεκριμένα, ο χρήστης θα πρέπει να επαναλάβει τη διαδικασία απόκτησης του πιστοποιητικού του για έλεγχο ταυτότητας με την IMD σε κάθε νέα περίοδο λειτουργίας.

Προκειμένου να βελτιστοποιηθεί η κατανάλωση ενέργειας σε εκείνες τις περιπτώσεις όπου ο χρήστης επικοινωνεί συχνά με την IMD, οι προσεγγίσεις PKI και ACL μπορούν να συνδυαστούν. Για παράδειγμα, την πρώτη φορά που στον χρήστη γίνεται έλεγχος ταυτότητας με την IMD, θα χρησιμοποιήθει το πιστοποιητικό του. Μετά από αυτό, ο συγκεκριμένος χρήστης είναι εγγεγραμμένος στην ACL, καθώς η χρήση αυτής της προσέγγισης είναι πιο αποτελεσματική από την άποψη της κατανάλωσης ενέργειας από ό,τι οι λύσεις που βασίζονται σε PKI.

Ένα κρίσιμο σημείο είναι ότι το PKI και οι κατάλογοι πιστοποιητικών θα πρέπει να είναι δημόσια -και μόνιμα- προσβάσιμοι μέσω του Διαδικτύου. Για παράδειγμα, έναν ασθενή σε κατάσταση έκτακτης ανάγκης κατά την επίσκεψή του σε ξένη χώρα ή απλώς σε διαφορετικό

νοσοκομείο. Το ιατρικό προσωπικό θα πρέπει να είναι σε θέση να λάβει τα απαιτούμενα διαπιστευτήρια. Τα προβλήματα συνδεσιμότητας ή ελέγχου ταυτότητας με το PKI μπορεί να τους εμποδίσουν να αποκτήσουν τα απαιτούμενα διαπιστευτήρια για να τροποποιήσουν ή να απενεργοποιήσουν την IMD, το οποίο σε ορισμένες περιπτώσεις μπορεί να απειλήσει την προστασία του ασθενούς. Ως εκ τούτου, το απαραίτητο PKI είναι πολύ απαιτητικό λόγω μεγάλου αριθμού συμμετεχόντων και είναι πιθανή μια τεράστια σειρά επαναλήψεων.

2.5.5 Εξουσιοδότηση Πρόσβασης σε Εξωτερικές Συσκευές

Ορισμένοι εισηγητές πρότειναν να κάνουν χρήση μιας εξωτερικής συσκευής για τον έλεγχο των προσβάσεων στην IMD. Τέτοιες συσκευές δεν θα εμφυτεύονται στο σώμα του ασθενούς και ένα μέρος ή όλες οι λειτουργίες ασφαλείας θα ανατεθούν σε αυτές. Αυτό παρουσιάζει πολλά οφέλη. Από τη μία πλευρά, η IMD θα εξοικονομήσει διάρκεια ζωής της μπαταρίας, καθώς οι υπολογισμοί που σχετίζονται με την ασφάλεια θα εκτελούνται εξωτερικά. Από την άλλη, μια μεμονωμένη συσκευή μπορεί να ενσωματώσει ορισμένες δυνατότητες ασφαλείας, όπως έλεγχο, διαχείριση κλειδιών, έλεγχο ταυτότητας και έλεγχο πρόσβασης. Επιπλέον, καθώς οι περισσότερες από αυτές τις δυνατότητες λειτουργούν στο φυσικό στρώμα, άλλα είδη λύσεων μπορούν να χρησιμοποιηθούν σε υψηλότερα στρώματα.

Γενικά, ο ρόλος της εξωτερικής συσκευής είναι να ενεργεί ως διαμεσολαβητής μεταξύ του προγραμματιστή και της IMD. Όταν ο προγραμματιστής πρέπει να έχει πρόσβαση στην IMD, αποκτά πρώτα πρόσβαση στην εξωτερική συσκευή και στη συνέχεια επικοινωνεί με την IMD. Μια λύση βασισμένη σε εξωτερικές συσκευές ονομάζεται "Cloaker" [68] . Η IMD ελέγχει περιοδικά την ύπαρξη του Cloaker. Ενώ ανιχνεύεται, η IMD παραμένει σιωπηλή. Ως εκ τούτου, ο Cloaker θα παρέχει ασφάλεια στον ασθενή όσο το διατηρεί . Αλλιώς οι επικοινωνίες με την IMD είναι πλήρως ανοικτές σε όλους τους χρήστες. Χρησιμοποιώντας αυτή την προσέγγιση, σε κατάσταση έκτακτης ανάγκης θα ήταν αρκετό να αφαιρεθεί ο Cloaker από τον ασθενή για να αποκτηθεί πλήρης πρόσβαση στη συσκευή.

Προσδιορίζονται δύο διαφορετικές δυνατότητες:

1. Ο Cloaker θα μεσολαβούσε σε όλες τις ανταλλαγές μέχρι την IMD και ο προγραμματιστής να ολοκληρώσει με επιτυχία μια ανταλλαγή κλειδιών. Μετά από αυτό, και τα δύο μέρη επικοινωνούν απευθείας μεταξύ τους μέσω ενός ασφαλούς

καναλιού που έχει δημιουργηθεί χρησιμοποιώντας το κοινόχρηστο κλειδί. Η εξωτερική συσκευή δεν συμμετέχει σε τέτοιες επικοινωνίες.

2. Μια διαφορετική δυνατότητα είναι η εμπλοκή του Cloaker σε όλες τις επικοινωνίες μεταξύ της IMD και του προγραμματιστή. Σε αυτή την περίπτωση, όλα τα πακέτα περνούν από αυτό, γεγονός που θα επέτρεπε την καταγραφή τους (για παράδειγμα, για μια επακόλουθη εγκληματολογική ανάλυση) και ακόμη και την εφαρμογή λειτουργιών φιλτραρίσματος και ανίχνευσης επιθέσεων. Ωστόσο,σε αυτή τη ρύθμιση ο Cloaker είναι ηυστατη μορφή διαμεσολάβησης, οπότε οποιαδήποτε δυσλειτουργία ή υποβάθμιση της απόδοσης θα επηρεάσει τη διαθεσιμότητα της IMD.

Οι μηχανισμοί ασφαλείας προσφέρονται μόνο σε κανονική λειτουργία και η προστασία του ασθενούς είναι εγγυημένη σε συνθήκες έκτακτης ανάγκης. Ωστόσο, εξακολουθούν να υπάρχουν ορισμένα ανοικτά ζητήματα που δεν έχουν δρομολογηθεί προς επίλυση :

- Η συνεχής ανίχνευση του Cloaker από την IMD δεν είναι ελάσσονος σημασίας. Στην πρώτη περίπτωση, η IMD στέλνει ένα μήνυμα "γεια" στον Cloaker κάθε φορά που εντοπίζεται ένα εισερχόμενο μήνυμα. Ένας άλλος, πιο περιοριστικός τρόπος αποτελείται από την IMD που στέλνει περιοδικά μηνύματα "γεια" στον Cloaker για να ελέγξει την ύπαρξη του. Το αποτέλεσμα αποθηκεύεται σε ένα μόνο bit που υποδεικνύει αν ο Cloaker υπάρχει ή όχι.

- Και τα δύο συστήματα που αναφέρονται ανωτέρω είναι αναποτελεσματικά όσον αφορά την κατανάλωση ενέργειας, ως αποτέλεσμα των μηνυμάτων που ανταλλάσσονται για τον έλεγχο της ύπαρξης της εξωτερικής συσκευής. Η πρώτη λύση αποφεύγει τη συνεχή ροή αιτημάτων προς τον Cloaker, αλλά καθιστά το σύστημα πιο ευάλωτο, καθώς ο επιτιθέμενος γνωρίζει την ακριβή ώρα κατά την οποία θα ερωτηθεί ο Cloaker. Έτσι, ο επιτιθέμενος θα μπορούσε να στείλει ένα ψεύτικο αίτημα στον Cloaker και στη συνέχεια να τον υποδυθεί. Αντίθετα, η δεύτερη προσέγγιση είναι πολύ πιο ασφαλής, αλλά απαιτεί από την IMD να ελέγχει συνεχώς την ύπαρξη του Cloaker.

Μια άλλη λύση που βασίζεται σε εξωτερικές συσκευές είναι ο "RFID Guardian" [39] .Ο RFID Guardian καταχωρεί όλες τις συσκευές στο χώρο εποπτείας του, διαχειρίζεται κλειδιά, ελέγχει τους προγραμματιστές που ζητούν πρόσβαση στην IMD και αποκλείει όλους τους μη εξουσιοδοτημένους χρήστες. Χρησιμοποιώντας αυτή την προσέγγιση, εντοπίζονται όλες οι

συσκευές στη περιοχή του Guardian (δηλαδή περίπου 1 ή 2 μέτρα) και τα διορθωτικά μέτρα θα μπορούσαν να εφαρμοστούν εάν χρειαστεί. Αν και η λύση προτάθηκε αρχικά στο πλαίσιο συστημάτων RFID, η προσέγγιση μπορεί εύκολα να προσαρμοστεί στις IMDs.

Άλλες προσεγγίσεις βασίζονται στη χρήση hardware tokens. Υπάρχει μια μεγάλη ποικιλία από αυτές τις συσκευές, συμπεριλαμβανομένων των αποσυνδεδεμένων και συνδεδεμένων tokens, των έξυπνων καρτών, των bluetooth tokens κ.λπ. Σε αυτήν την περίπτωση, η συσκευή αποθηκεύει έναν κωδικό πρόσβασης που είναι κοινόχρηστος με την IMD. Το ιατρικό προσωπικό θα χρησιμοποιήσει αυτό το κλειδί για να έχει πρόσβαση στο εμφύτευμα. Το κύριο μειονέκτημα είναι το ίδιο όπως και στις άλλες λύσεις που βασίζονται σε εξωτερικές συσκευές: εάν το token χαθεί ή ο ασθενής ξεχάσει να το έχει μαζί τους σε κατάσταση έκτακτης ανάγκης,η IMD δεν θα είναι προσβάσιμη [69].

Συμπερασματικά, το κύριο πλεονέκτημα των λύσεων που βασίζονται σε εξωτερικές συσκευές είναι ότι προσφέρουν υψηλό επίπεδο προστασίας από μη εξουσιοδοτημένες εντολές. Η IMD δεν θα ανταποκριθεί σε κακόβουλες εντολές ή επιθέσεις επαναπρογραμματισμού για την εκφορτιση της μπαταρίας. Τα κύρια μειονεκτήματά τους περιλαμβάνουν:

- Εάν ο ασθενής ξεχάσει την εξωτερική συσκευή, η IMD θα ανταποκριθεί σε όλα τα εισερχόμενα (εξουσιοδοτημένα ή μη) αιτήματα, τα οποία είναι απαραίτητα μόνο σε κατάσταση έκτακτης ανάγκης.

- Οι λύσεις αυτές δεν λαμβάνουν γενικά υπόψη σενάρια στα οποία η η εξωτερική συσκευή αντικαθίσταται από μια κακόβουλη. Σε αυτή την περίπτωση, η ασφάλεια και η προστασία της ιδιωτικής ζωής της IMD θα διακυβεύονταν σε μεγάλο βαθμό.

- Η εξωτερική συσκευή είναι πλήρως ορατή σε εξωτερικούς χρήστες , οι οποίοι μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες σχετικά με την ιατρική κατάσταση του ασθενούς.

- Αυτές οι λύσεις συχνά προϋποθέτουν ότι η εξωτερική συσκευή είναι αξιόπιστη. Ωστόσο, αυτή μπορεί να παραβιαστεί ή να ενεργήσει κακόβουλα. Για παράδειγμα, τα πακέτα μπορούν να τροποποιηθούν (π.χ. τροποποιονταςορισμένα bits), να διακοπούν ή να αποκλειστούν, γεγονός που θα καθιστούσε εκτός λειτουργίας την επικοινωνία με την IMD.

2.5.6 Εντοπισμός Δυσλειτουργιών

Η διαθεσιμότητα των λειτουργιών IMD είναι ζωτικής σημασίας, καθώς η θεραπεία – ακόμη και η ζωή του ασθενούς – μπορεί να τεθεί σε κίνδυνο. Εάν εντοπιστεί επίθεση, ο ασθενής μπορεί να ενημερωθεί (π.χ. με μηχανισμό ειδοποίησης) ή η συσκευή μπορεί να καταστεί μη προσβάσιμη μέσω απενεργοποίησης των επικοινωνιών (ή εμπλοκής του καναλιού) ενώ οι ιατρικές λειτουργίες παραμένουν ενεργές. Η δυσκολία πρόληψης αυτού του είδους επιθέσεων προκύπτει κυρίως από τη χρήση του ασύρματου διαύλου επικοινωνίας. Η επικοινωνία μεταξύ της IMD και του χρήστη ξεκινά από την πιστοποίηση από την IMD. Εάν ο χρήστης δεν περάσει το βήμα ελέγχου ταυτότητας, διακόπτεται η επικοινωνία. Αυτό καταναλώνει πόρους στην IMD και, ως εκ τούτου, μπορεί να αξιοποιηθεί από έναν εισβολέα ο οποίος, για παράδειγμα, προσπαθεί επανειλημμένα να επικοινωνήσει με την IMD. Το αποτέλεσμα θα ήταν μια επίθεση άρνηση υπηρεσίας κατά την οποία η μπαταρία θα μπορούσε να μειωθεί δραστικά και η μνήμη/αποθήκευση θα μπορούσε επίσης να επηρεαστεί. Σε κάθε έλεγχο ταυτότητας, ορισμένοι καταχωρητες χρησιμοποιούνται για την αποθήκευση παραμέτρων ασφαλείας, όπως tokens και αρχεία καταγραφής (logs) .Σε γενικές γραμμές, αυτού του είδους οι επιθέσεις είναι γνωστές ως επιθέσεις εξάντλησης πόρων (Resource Depletion - RD) και επικεντρώνονται στη κατανάλωση των πόρων της IMD [70] . Είναι πολύ εύκολο να εφαρμοστούν και οι συνέπειές τους μπορεί να είναι πολύ επιβλαβείς, καθώς η διάρκεια ζωής της μπαταρίας της IMD θα μπορούσε να μειωθεί από αρκετά χρόνια σε λίγες εβδομάδες μόνο με την αποστολή εικονικών αιτημάτων.

Οι τυποποιημένες κρυπτογραφικές λύσεις δεν εμποδίζουν αυτές τις επιθέσεις και οι υπάρχουσες μελέτες σχετικά με τις επιθέσεις RD σε δίκτυα αισθητήρων [71] δεν ισχύουν άμεσα για τις IMDs, καθώς τα εμφυτεύματα έχουν πιο αυστηρούς περιορισμούς πόρων. Επιπλέον, υπάρχει μια δυσκολία στην προσθήκη νέων πόρων καθώς το εμφύτευμα βρίσκεται μέσα στο σώμα, κάτι που δεν συμβαίνει με τα δίκτυα αισθητήρων. Αυτό παρακινεί την ανάγκη σχεδιασμού λύσεων που λαμβάνουν υπόψη το γεγονός ότι αυτές οι συσκευές θα χρησιμοποιηθούν μέσα σε ένα ανθρώπινο σώμα.

Στο πλαίσιο των IMDs, η συνδυασμένη χρήση συστημάτων ανάλυσης προτύπων/συμπεριφοράς και ειδοποίησης είναι η πιο ευρέως χρησιμοποιούμενη λύση για την αντιμετώπιση επιθέσεων RD. Τα συστήματα ειδοποίησης ενημερώνουν τον ασθενή μέσω σήματος συναγερμού (π.χ. ήχου ή κραδασμού) όταν συμβαίνουν συγκεκριμένα γεγονότα, όπως όταν η IMD καθιερώνει επικοινωνία με εξωτερική συσκευή [40] ή όταν ορισμένες

βιοϊατρικές παράμετροι κινούνται εκτός φυσιολογικού εύρους [72] .Τέτοιοι συναγερμοί είναι μόνο ενημερωτικοί. Έτσι, η ειδοποίηση δεν εμποδίζει την εμφάνιση επιθέσεων, αν και η ειδοποίηση του ασθενούς μπορεί να είναι πολύτιμη για να τον ενημερώσει για μη αναμενόμενη επικοινωνία. Ένα σημαντικό μειονέκτημα αυτών των λύσεων είναι ότι δεν λειτουργούν σωστά σε θορυβώδη περιβάλλοντα. Εκτός αυτού, οι συναγερμοί έχουν μια σχετική κατανάλωση ενέργειας που δεν πρέπει να παραβλέπεται. Όπως και στην περίπτωση του ελέγχου, οι μηχανισμοί ειδοποίησης από μόνοι τους είναι ανεπαρκείς και θα πρέπει να συμπληρώνονται και με άλλες λύσεις.

Αξιοποιώντας το γεγονός ότι οι ασύρματες επικοινωνίες μεταξύ μιας IMD και ενός χρήστη ακολουθούν ένα σύνολο μοτίβων (π.χ. συχνότητα, εντοπισμός, συνθήκες ασθενούς κ.λπ.), προτείνεται ως λύση [73] , ένας μηχανισμός, ενάντια στις επιθέσεις RD, με ένα μέσο ποσοστό ανίχνευσης πάνω από 90%. Το σύστημα χρησιμοποιεί Support Vector Machine (SVM), η οποία υποτίθεται ότι λειτουργεί στο τηλέφωνο του ασθενούς. Αναλυτικά, εξετάζονται πέντε παράμετροι δεδομένων εισόδου για να πραγματοποιηθεί ανίχνευση:

1. Ο τύπος δράσης του χρήστη (δηλαδή, η ενέργεια ή οι ενέργειες που μπορεί να εκτελέσει στην IMD, όπου το σύνολο των ενεργειών εξαρτάται από τον τύπο του εμφυτεύματος)

2. Το χρονικό διάστημα της ίδιας ενέργειας του χρήστη

3. Η τοποθεσία (π.χ. σπίτι ή νοσοκομείο)

4. Η ώρα , και

5. Η ημέρα (π.χ. εβδομαδιαία ή σαββατοκύριακο)

Ο classifier θα καθορίσει αν ένα μοτίβο είναι έγκυρο ή όχι. Για παράδειγμα, εάν ένα συγκεκριμένο είδος αιτήματος αποστέλλεται πάντα από το γραφείο του γιατρού, μια προσπάθεια του ίδιου αιτήματος από διαφορετική τοποθεσία θα σημάνει συναγερμό. Το συνολικό σύστημα λειτουργεί ως εξής.

Κάθε φορά που ο χρήστης προσπαθεί να επικοινωνήσει με την IMD, ο τελευταίος στέλνει ένα μήνυμα στο κινητό τηλέφωνο του ασθενούς με το μοτίβο πρόσβασης. Το τηλέφωνο εκτελεί

τον αλγόριθμο ταξινόμησης και επιστρέφει μια απάντηση που αποστέλλεται πίσω στην IMD. Ανάλογα με την απάντηση αυτή, είναι δυνατές τρεις ενέργειες:

1. Ο input vector θεωρείται νόμιμος. Σε αυτή την περίπτωση το κινητό στέλνει ένα "1" (αληθές) στην IMD και η επικοινωνία με τον χρήστη συνεχίζεται.

2. Ο input vector δεν αντιστοιχεί σε κάποιο από τα επιτρεπόμενα μοτίβα, και σε αυτή την περίπτωση το τηλέφωνο στέλνει ένα "0" (ψευδές). Το αίτημα μπορεί να προέρχεται από έναν εισβολέα και η IMD τίθεται σε κατάσταση αναστολής λειτουργίας για την αποφυγή επιθέσεων RD

3. Εάν είναι ασαφές ότι ο input vector είναι νόμιμος ή πρόκειται για κακόβουλη επίθεση ενεργοποιείται συναγερμός (π.χ. ηχητικός συναγερμός) για την ενημέρωση του ασθενούς, ο οποίος πρέπει να αποφασίσει εάν επιτρέπεται η επικοινωνία.

Η λύση αυτή [73] έχει τρία κύρια μειονεκτήματα . Πρώτον, το σύστημα υποθέτει ότι η IMD είναι πάντα σε κανονική λειτουργία και δεν λαμβάνει υπόψη τις συνθήκες έκτακτης ανάγκης κατά τις οποίες τα νομιμοποιημένα πρότυπα πρόσβασης μπορούν να είναι παραποιημένα. Σε αυτή την περίπτωση, η πρόσβαση στην IMD θα απορριφθεί, γεγονός που θα μπορούσε να έχει σοβαρές συνέπειες στη νυγεια του ασθενούς. Δεύτερον, η λυσηαυτη φέρει ορισμένα μειονεκτήματα από τα συστήματα που βασίζουν την ασφάλειά της σε μια εξωτερική συσκευή —το κινητό τηλέφωνο, στην προκειμένη περίπτωση. Τέλος, αλλά εξίσου σημαντικό,είναι στην ευθύνη του ασθενουςη λήψη απόφασης, σε περίπτωση που το SVM δεν μπορεί να ταξινομήσει τα δεδομένα εισόδου.

Εναλλακτικά αντί να χρησιμοποιηθούν μοτίβα, έχει προταθεί [74] ένα σύστημα για την ανίχνευση κακόβουλης χρήσης μιας αντλίας ινσουλίνης. Συγκεκριμένα, η χορήγηση δόσεων ινσουλίνης ανιχνεύεται με την παρακολούθηση των ακουστικών ήχων του εντέρου. Τα συμβάντα καταγράφονται και στη συνέχεια χρησιμοποιούνται για τον έλεγχο της σωστής λειτουργίας του συστήματος. Επιπλέον, το σύστημα βασίζεται στη χρήση εξωτερικής συσκευής που απαιτείται για τη μέτρηση των κοιλιακών ήχων.

Μια νέα αμυντική μέθοδος για τις IMDs που βασίζεται στην ασύρματη παρακολούθηση και την ανίχνευση ανωμαλιών έχει προταθει [55]. Οι εισηγητές προτείνουν τη χρήση ενός μόνιτορ ιατρικής ασφάλειας, που ονομάζεται MedMon, το οποίο κρυφακούει τις επικοινωνίες προς και από την IMD. Στη συνέχεια, η επικοινωνία που καταγράφεται μεταβιβάζεται για ανάλυση σε

ένα σύστημα ανίχνευσης ανωμαλιών πολλαπλών επιπέδων. Εάν εντοπιστεί κακόβουλη συναλλαγή, ο χρήστης μπορεί να ενημερωθεί (passive response) ή εναλλακτικά το σύστημα μπορεί να καταστήσει την IMD μη προσβάσιμη μέσω active jamming. Το jamming αναφέρεται στη μετάδοση ραδιοσημάτων με σκοπό την παρεμπόδιση των επικοινωνιών στο κανάλι μειώνοντας την αναλογία σήματος προς θόρυβο. Σε αυτή την περίπτωση, το jamming χρησιμοποιείται για την προστασία της IMD από το να είναι προσβάσιμη στον εισβολέα. Το κύριο μειονέκτημα αυτής της πρότασης είναι ότι ολόκληρη η ασφάλεια βρίσκεται σε μια εξωτερική συσκευή, αλλά έχει το πλεονέκτημα ότι εφαρμόζεται σε υπάρχουσες συσκευές χωρίς καμία τροποποίηση. Σύμφωνα με το MedMon, προτάθηκε πρόσφατα ένα σύστημα για τον εντοπισμό ενεργών επιθέσεων,με τη χρήση εξωτερικής συσκευής μεσολάβησης εξοπλισμένη με διάφορες κεραίες που απαιτειτην ύπαρξη εξουσιοδοτημένων χρηστών/προγραμματιστών με βάση τη θέση τους [75]. Οι θέσεις υπολογίζονται μέσω τεχνικών τριγωνισμού. Η πρόταση φαίνεται αποτελεσματική για στατικά σενάρια, αλλά όχι για δυναμικά.

3 MITM & Replay Attack on WiFi Bulb

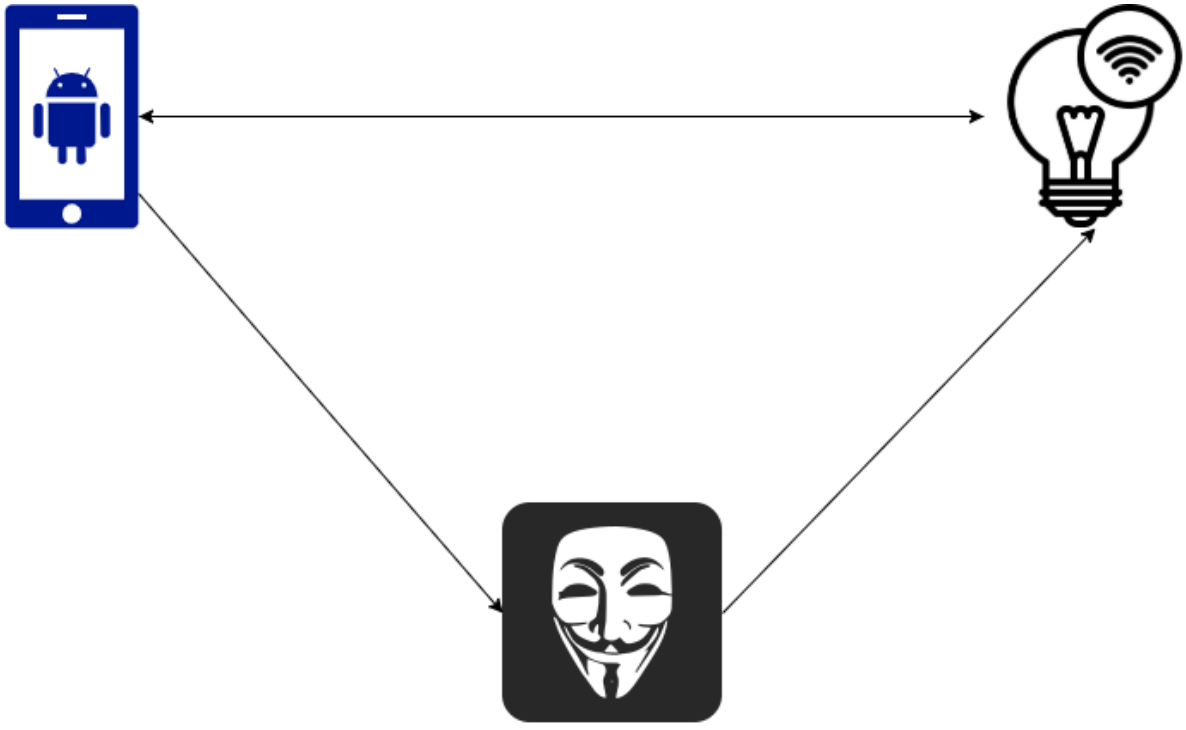

Figure 6 Επίθεση σε WiFi λάμπα

Σκοπός της συγκεκριμένης επίθεσης ήταν η καταγραφή πακέτων διαχείρισης της λάμπας και η επανεκπομή αυτών από μη εξουσιοδοτημένη συσκευή για τη διαχείριση της λάμπας. Για να επιτευχθεί αυτό έγινε χρήση μιας λάμπας Bulb, μιας συσκευής android και ενός φορητού υπολογιστή. Για να επιτευχθεί η επίθεση έγινε χρήση εργαλείων ανοιχτού κώδικα τα οποία είναι διαθέσιμα στην έκδοση Kali Linux. Συγκεκριμένα χρησιμοποιήθηκαν arspoof, tcpreplay και Wireshark.

Για να πραγματοποιήσω την επίθεση χρησιμοποίησα το arpspoof ώστε να "εξαπατήσω" τις δύο συσκευές με βάση τη δική μου από την οποία ήθελα να περάσω τη κίνηση. Με τη χρήση του εργαλείου αυτού η κίνηση άρχισε να περνάει από τη δική μου συσκευή και στη συνέχεια να τη προωθώ στην αντίστοιχη.

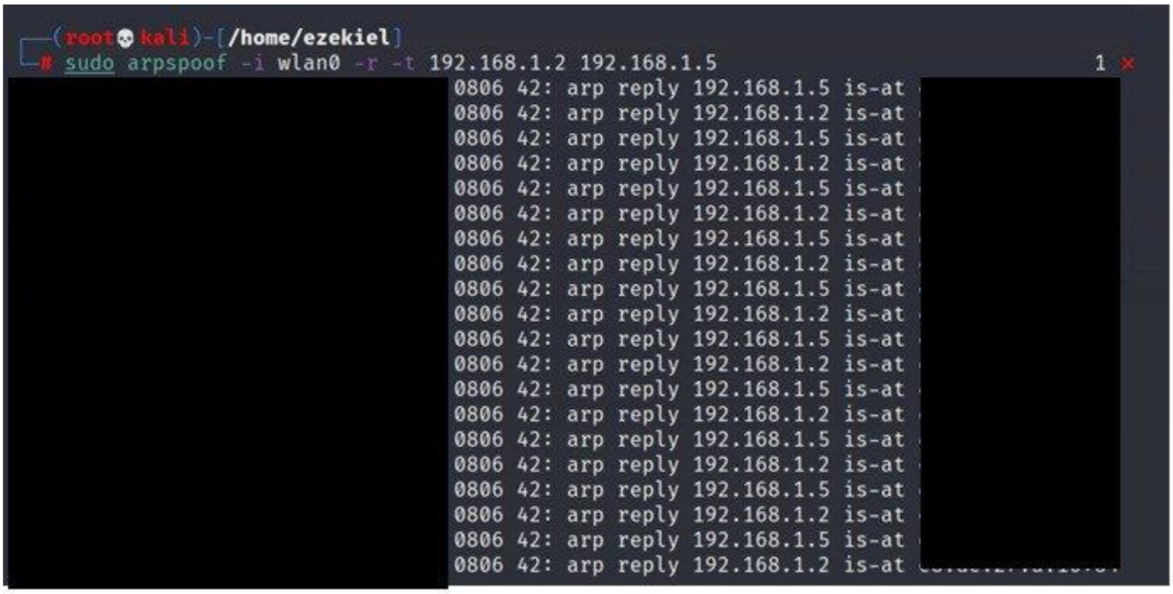

Figure 7 Χρήση του arpspoof για προώθηση πακέτων

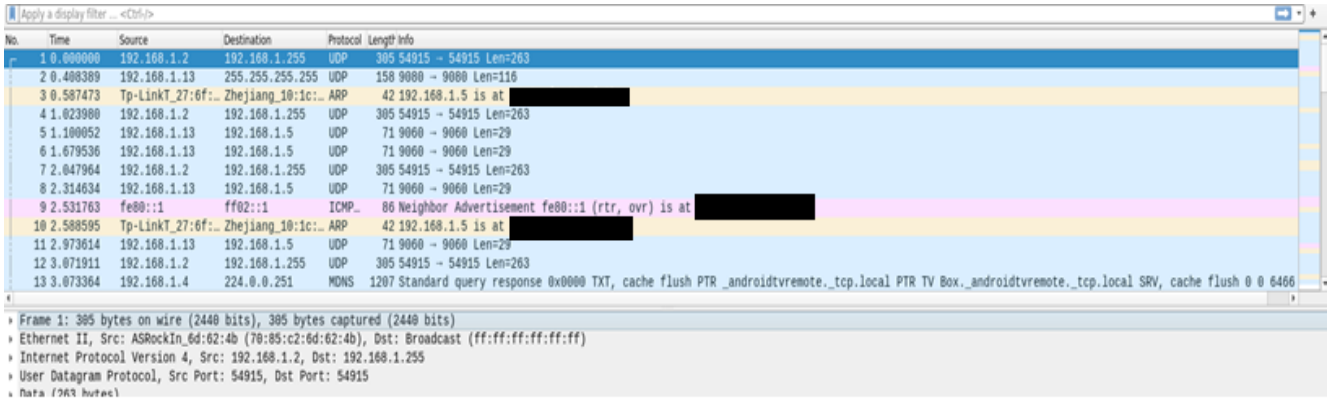

Figure 8 Καταγραφή πακέτων με την χρήση του Wireshark

Στην συνέχεια με την βοήθεια του Wireshark κατέγραψα την επικοινωνία μεταξύ της συσκευής Android και της λάμπας. Παρατήρησα πως εκτός από τα DNS και ARP υπήρχαν και αρκετά UDP. Σε συνδυασμό με την προηγούμενη παρατήρηση κατάλαβα πως τα πακέτα UDP πρέπει να ήταν για την διαχείριση της λάμπας.

Τέλος χρησιμοποίησα το tcpreplay για να κάνω επανεκπομπή των πακέτων στη λάμπα και να τη χειριστώ από το laptop. Η επίθεση πέτυχε με την λάμπα να αναβοσβήνει με μεγάλη συχνότητα μέχρι να ολοκληρωθεί η επανεκπομπή των πακέτων που είχαν καταγραφεί.

```
┌──(root💀kali)-[/home/ezekiel]
└─# tcpreplay -i wlan0 replayattack.pcap
tcpreplay: Symbol `pcap_version' has different size in shared object, consider re-linking
^C User interrupt ...
sendpacket_abort
Actual: 41 packets (6932 bytes) sent in 10.22 seconds
Rated: 678.2 Bps, 0.005 Mbps, 4.01 pps
Flows: 5 flows, 0.48 fps, 31 flow packets, 10 non-flow
Statistics for network device: wlan0
        Successful packets:        40
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

Figure 9 Επανεκπομπή πακέτων με την χρήση του tcpreplay

4 Συμπεράσματα

Τα εμφυτεύσιμα ιατροτεχνολογικά προϊόντα αποδεδειγμένα βελτιώνουν την ποιότητα ζωής των ασθενών και, σε ορισμένες περιπτώσεις, διαδραματίζουν σημαντικό ρόλο στη υγεία τους. Η νέα γενιά των IMDs ενσωματώνει όλο και περισσότερες δυνατότητες πληροφορικής και επικοινωνίας. Σε αυτή τη διπλωματική, υποστηρίχθηκε ότι η πρόοδος σε νέα και πιο έξυπνα μοντέλα IMDs πρέπει να ενσωματώνουν λύσεις ασφαλείας , προκειμένου να παρέχουν στον ασθενή ασφάλεια και προστασία. Παρουσιάστηκε μια ολοκληρωμένη επισκόπηση των κύριων προβλημάτων ασφάλειας που σχετίζονται με τις νεότερες IMDs και συζητήθηκε πώς, σε ορισμένες περιπτώσεις, η υγεία του ασθενούς μπορεί να απειληθεί σοβαρά από έναν κακόβουλο εισβολέα. Ως εκ τούτου, είναι προφανές ότι οι μηχανισμοί ασφαλείας πρέπει να ειναι ενσωματωμένες σε αυτές τις συσκευές.

Δεδομένων των τριβών μεταξύ των διαφόρων στόχων ασφάλειας και των λύσεων που έχουν προταθεί μέχρι στιγμής, δεν είναι σαφές ποια θα ήταν η βέλτιστη επιλογή. Το ερώτημα παραμένει ανοιχτό . Πολλές προτάσεις παρέχουν ένα αρκετά υψηλό επίπεδο ασφάλειας, αλλά απαιτούν πάρα πολλούς πόρους (π.χ. μνήμη ή υπολογισμό), οι οποίοι είναι ανέφικτοι λαμβάνοντας υπόψη την ανάγκη εξοικονόμησης διάρκειας ζωής της μπαταρίας . Εναλλακτικά, οι απλούστερες και λιγότερο απαιτητικές λύσεις είναι συχνά ευάλωτες σε επιθέσεις ως συνέπεια των αδύναμων σχεδιασμών τους.

Μελλοντικά , τα ιατρικά εμφυτεύματα ανοίγουν την πόρτα σε άλλους τύπους συσκευών για να βελτιώσουν τις ανθρώπινες ικανότητες, όπως η μνήμη ή η αντίληψη. Αυτό φαίνεται σίγουρα πολυ αισιόδοξο , αλλα κάπως ετσι οι βηματοδότες και οι νευροδιεγερτές θεωρήθηκαν μια ανέφικτη εξέλιξη πριν από την εφαρμογή τους . Ο τομέας της ασφάλειας των συστημάτων πρέπει να είναι έτοιμος να προσαρμόσει και να ενσωματώσει λύσεις για αυτό το νέο περιβάλλον στην φάση του σχεδιασμού, αποφεύγοντας την προσέγγιση <<ανάπτυξη και μετά ενημέρωση >> πρακτική που έχει επιφέρει καταστροφικά αποτελέσματα στο Διαδίκτυο.

Βιβλιογραφία – Αναφορές - Διαδικτυακές Πηγές

[1] Asare P, Broman D, Lee EA, Torngren M, Sunder SS. Cyberphysical systems [Online]; 2012. Available from: http://cyberphysicalsystems.org/. [Accessed 24 December 2016].

[2] Ali S, Anwar RW, Hussain OK. Cyber security for cyber physical systems: a trust-based approach. J Theor Appl Inf Technol 2015;71(2):144–52.

[3] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui and K. P. Chow, "Security Issues and Challenges for Cyber Physical System," 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, 2010, pp. 733-738, doi: 10.1109/GreenCom-CPSCom.2010.36.

[4] Zhang, B.Z., Ma, X.X., Qin, Z.G. Security architecture on the trusting internet of things (2011) J. Electr. Sci. Technol., 9 (4), pp. 364-367

[5] Lu T, Lin J, Zhao L, Li Y, Peng Y. A security architecture in cyberphysical systems: security theories, analysis, simulation and application fields. Int J Secur Appl 2015;9(7):1–16.

[6] U. Sendler Industrie 4.0 – Beherrschung der Industriellen Komplexität mit SysLM (Systems Lifecycle Management) Ind. 4.0, Springer Berlin Heidelb., pp. 1–19 (2013)

[7] NIST Cyber-physical systems: situation analysis of current trends, technologies, and challenges Natl. Inst. Stand. Technol (NIST), Columbia, Maryland (2012)

[8] Jing Q., A.V. Vasilakos, Wan J. Security of the internet of things: perspectives and challenges Wirel Netw, 20 (8) (2014), pp. 2481-2501

[9] L. Vegh, L. Miclea Enhancing security in cyber-physical systems through cryptographic and steganographic techniques Autom. Qual. Testing, Robot. Int. Conf. IEEE, pp. 1–6 (2014)

[10] M.A. Bhabad, P.G. Scholar Internet of things: architecture, security issues and countermeasures Int J Comput Appl, 125 (14) (2015)

[11] R. Khan, S.U. Khan, R. Zaheer, S. Khan FUTURE Internet: the Internet of Things architecture, possible applications and key challenges 10th Int. Conf. Front. Inf. Technol., pp. 257–260 (2012)

[12] Q. Shafi Cyber physical systems security: a brief survey Comput. Sci. Its Appl. (ICCSA), 12th Int. Conf. IEEE, pp. 146–150 (2012)

[13] Peng Y., Lu T., Liu J., Gao Y., Guo X., Xie F. Cyber-physical system risk assessment Ninth Int. Conf. Intell. Inf. Hiding Multimed. Signal Process., pp. 442–447 (2013)

[14] A.M. Gamundani An impact review on Internet of Things attacks Int. Conf. Emerg. Trends Networks Comput. Commun., pp. 114–118 (2015)

[15] J.S. Kumar, D.R. Patel A survey on internet of things: security and privacy issues Int J Comput Appl, 90 (11) (2014), pp. 20-26

[16] Wu M., Lu T., Ling F., Du H. Research on the architecture of Internet of Things Proc. 3rd Int. Conf. Adv. Comput. Theory Eng., pp. 20–22 (2010)

[17] Zhao K., Ge L. A survey on the Internet of Things security Ninth Int. Conf. Comput. Intell. Secur., pp. 663–667 (2013)

[18] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan Internet of Things (IoT) security: current status, challenges and prospective measures 10th Int. Conf. Internet Technol. Secur. Trans. IEEE, pp. 336–341 (2015)

[19] Cárdenas A., Amin S., Lin Z.-S., Huang Y., Huang C.-Y., Sastry S., Attacks against process control systems: risk assessment, detection, and response, Proc. 6th ACM Symp. Information, Comput. Commun. Secur. ACM, pp. 355–366, 2011.

[20] C. Konstantinou, M. Maniatakos, F. Saqib, Hu S., J. Plusquellic, Jin Y. Cyber-physical systems: a security perspective 20th IEEE Eur. Test Symp., pp. 1–8 (2015)

[21] S. Raza Lightweight security solutions for the Internet of Things Mälardalen University Press Dissertations, Mälardalen University, Västerås, Sweden (2013)

[22] J. Weiss Control system cyber vulnerabilities and potential mitigation of risk for utilities White Pap. Juniper Networks, Inc. (2010)

[23] Hu W., J. Oberg, J. Barrientos, Mu D., R. Kastner Expanding gate level information flow tracking for multilevel security IEEE Embed Syst Lett, 5 (2) (2013), pp. 25-28

[24] R. Mitchell, Chen I. A survey of intrusion detection techniques for cyber-physical systems ACM Comput Surv, 46 (4) (2014), pp. 1-29

[25] Gou Q., Yan L., Liu Y., Li Y. Construction and strategies in IoT security system Proc. - IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCom., pp. 1129–1132(2013)

[26] Suo H., Wan J., Zou C., Liu J. Security in the internet of things: a review Int Conf Comput Sci Electron Eng IEEE, 3 (2012), pp. 648-651

[27] J. Kao, R. Marculescu Eavesdropping minimization via transmission power control in ad-hoc wireless networks Sens Ad Hoc Commun Netw, 2 (2006), pp. 707-714

[28] J.G. Webster Design of Cardiac Pacemakers IEEE Press (1995)

[29] R.N. Simons, D.G. Hall, F.A. Miranda, Rf telheidu2011emetry system for an implantable bio-mems sensor, in: IEEE MTT-S International Microwave Symposium Digest, vol. 3, 2004, pp. 1433–1436.

[30] R.T. Lukins, S. Tisch, B. Jonker The latest evidence on target selection in deep brain stimulation for Parkinsons disease J. Clin. Neurosci., 21 (1) (2014), pp. 22-27

[31] T.J. Lamer Treatment of cancer-related pain: when orally administered medications fail Mayo Clin. Proc., 69 (5) (1994), pp. 473-480

[32] S. Cherukuri, K.K. Venkatasubramanian, S.K.S. Gupta, BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, in: Proc. of International Conference on Parallel Processing Workshops, 2003, pp. 432–439.

[33] T. Drew, M. Gini Implantable medical devices as agents and part of multiagent systems Proc. of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS '06, ACM (2006), pp. 1534-1541

[34] K.K. Venkatasubramanian, S.K.S. Gupta, Security for pervasive health monitoring sensor applications, In: Proceedings of 4th International Conference on Intelligent Sensing and Information Processing (ICISIP), 2006, pp. 197–202.

[35] M. Salajegheh, A. Molina, K. Fu Privacy of home telemedicine: encryption is not enough J. Med. Dev., 3 (2) (2009)

[36] S. Patel, K. Lorincz, R. Hughes, N. Huggins, J.H. Growdon, M. Welsh, P. Bonato, Analysis of feature space for monitoring persons with parkinson's disease with application to a wireless wearable sensor system, in: 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS), 2007, pp. 6290–6293.

[37] V. Shnayder, B.-r. Chen, K. Lorincz, T.R.F. Fulford Jones, M. Welsh Sensor networks for medical care Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, SenSys '05, ACM (2005) pp. 314–314

[38] S. Xiao, A. Dhamdhere, V. Sivaraman, A. Burdett Transmission power control in body area sensor networks for healthcare monitoring IEEE J. Sel. Areas Commun., 27 (1) (2009), pp. 37-48

[39] M.R. Rieback, B. Crispo, A.S. Tanenbaum, Is your cat infected with a computer virus? in: Fourth Annual IEEE International Conference on Pervasive Computing and Communications, March 2006, pp. 179–189.

[40] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W.H. Maisel, Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses, in: Proc. of the 29th Annual IEEE Symposium on Security and Privacy, 2008, pp. 129–142.

[41] K. Fotopoulou, B.W. Flynn, Optimum antenna coil structure for inductive powering of passive RFID tags, in: IEEE International Conference on RFID, 2007, pp. 71–77.

[42] D. Arney, K.K. Venkatasubramanian, O. Sokolsky, I. Lee, Biomedical devices and systems security, in: Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2011, pp. 2376–2379.

[43] J.A. Hansen, N.M. Hansen A taxonomy of vulnerabilities in implantable medical devices Proc. of the Second Annual Workshop on Security and Privacy in Medical and Home-care Systems, SPIMACS '10, ACM, New York, USA (2010), pp. 13-20

[44] H. Zhu, R. Xu, J. Yuan, High speed intra-body communication for personal health care, in: Annual International Conference of the IEEE Engineering in Medicine and Biology Society, September 2009, pp. 709–712

[45] Medtronic, Parkison's Disease. <http://www.medtronic.eu/your-health/parkinsons-disease/device/our-dbs-therapy-products/activaRC/index.htm> (consulted on Feburary 2014).

[46] V. S Mallela, V. Ilankumaran, N.S. Rao Trends in cardiac pacemaker batteries J. Indian Pac. Electrophys., 4 (4) (2004), pp. 201-212

[47] C.W. Israel, S.S. Barold Pacemaker systems as implantable cardiac rhythm monitors Am. J. Cardiol., 88 (4) (2001), pp. 442-445

[48] C. Strydis, R.M. Seepers, P. Peris-Lopez, D. Siskos, I. Sourdis A system architecture, processor, and communication protocol for secure implants ACM Trans. Archit. Code Optimiz., 10 (4) (2013), pp. 57:1-57:23

[49] S. Park, Y. Kim, B. Urgaonkar, J. Lee, E. Seo A comprehensive study of energy efficiency and performance of flash-based {SSD} J. Syst. Architect., 57 (4) (2011), pp. 354-365

[50] C. Sandner, R. Amirtharajah, Power management, in: IEEE Custom Integrated Circuits Conference, September 2013, pp. 1–1.

[51] J.H. Schulman, Stimulating and sensing network inside the human body, in: International Workshop on Wearable and Implantable Body Sensor Networks, April 2006, pp. 95–98.

[52] Texas Instruments, Msp430f156, 16-bit Ultra-low-power MCU. <http://www.ti.com/lit/ds/symlink/msp430f156.pdf>.

[53] D. Panescu Emerging technologies [wireless communication systems for implantable medical devices] IEEE Eng. Med. Biol. Mag., 27 (2) (2008), pp. 96-101

[54] D. Wu, K. Warwick, Z. Ma, M.N. Gasson, J.G. Burgess, S. Pan, T.Z. Aziz Prediction of parkinson's disease tremor onset using a radial basis function neural network based on particle swarm optimization Int. J. Neural Syst., 20 (02) (2010), pp. 109-116

[55] M. Zhang, A. Raghunathan, N.K. Jha MedMon: securing medical devices through wireless monitoring and anomaly detection IEEE Trans. Biomed. Circ. Syst., 7 (6) (2013), pp. 871-881

[56] A.J. Menezes, S.A. Vanstone, P.C.V. Oorschot Handbook of Applied Cryptography (first ed.), CRC Press, Inc. (1996)

[57] S. Hosseini-Khayat, A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices, in: 5th International Symposium on Medical Information Communication Technology (ISMICT), March 2011, pp. 6–9.

[58] M.H. Eldefrawy, M.K. Khan, K. Alghathbar, A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography, in: 2010 International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID), 2010, pp. 1–6.

[59] K. Singh, V. Muthukkumarasamy, Authenticated key establishment protocols for a home health care system, in: 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007, pp. 353–358.

[60] F. Furbass, J. Wolkerstorfer, ECC processor with low die size for RFID applications, in: IEEE International Symposium on Circuits and Systems, 2007, pp. 1835–1838.

[61] Y.K. Lee, K. Sakiyama, L. Batina, I. Verbauwhede Elliptic-curve-based security processor for RFID IEEE Trans. Comput., 57 (11) (2008), pp. 1514-1527

[62] ISO, Information Technology – Security Techniques – Entity Authentication – Part 2: Mechanisms using Symmetric Encipherment Algorithms, ISO/IEC 9798-2:2008, International Standard, second ed., 1999.

[63] L. Seltzer, Securing Your Private Keys as Best Practice for Code Signing Certificates, 2013. <https://www.symantec.com/content/en/us/enterprise/white_papers/b-securing-your-private-keys-csc-wp.pdf>.

[64] E. Freudenthal, R. Spring, L. Estevez, Practical techniques for limiting disclosure of RF-equipped medical devices, in: IEEE Engineering in Medicine and Biology Workshop, 2007, pp. 82–85.

[65] S. Schechter, Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices, 2004. <http://research.microsoft.com/apps/pubs/default.aspx?id=12213>.

[66] M. Rostami, W. Burleson, F. Koushanfar, A. Juels Balancing security and utility in medical devices? Proceedings of the 50th Annual Design Automation Conference, DAC '13, ACM (2013), pp. 13:1-13:6

[67] S. Gollakota, H. Al Hassanieh, B. Ransford, D. Katabi, K. Fu, IMD Shield: Secure Implantable Medical Devices, 2011. <http://groups.csail.mit.edu/netmit/IMDShield/>.

[68] T. Denning, K. Fu, T. Kohno Absence makes the heart grow fonder: new directions for implantable medical device security Proceedings of the 3rd Conference on Hot Topics in Security, HOTSEC'08, USENIX Association (2008), pp. 5:1-5:7

[69] S. Bergamasco, M. Bon, P. Inchingolo, Medical data protection with a new generation of hardware authentication tokens, 2001.

[70] F. Hu, Q. Sun, Y. Wu, M. Guo, J. Lu, J. Li, D.J. Gay, J.K. Garner, A.L. Poellnitz, Implantable medical devices: architecture and design, in: Telehealthcare Computing and Engineering: Principles and Design, first ed., 2013, pp. 359–406 (Chapter 14).

[71] D.R. Raymond, S.F. Midkiff Denial-of-service in wireless sensor networks: attacks and defenses IEEE Pervasive Comput., 7 (1) (2008), pp. 74-81

[72] Dexcom, Seven Plus CGM System. <http://www.dexcom.com/seven-plus>. (consulted on Feburary 2014).

[73] X. Hei, X. Du, J. Wu, F. Hu, Defending resource depletion attacks on implantable medical devices, in: Proc. of IEEE Global Telecommunications Conference (GLOBECOM), 2010, pp. 1–5.

[74] N. Henry, N. Paul, N. McFarlane, Using bowel sounds to create a forensically-aware insulin pump system, in: Workshop on Health Information Technologies, HealthTech, USENIX, 2013, pp. 1–10.

[75] M. Darji, B. Trivedi Detection of active attacks on wireless IMDs using proxy device and localization information Security in Computing and Communications, Communications in Computer and Information Science, vol. 467, Springer, Berlin Heidelberg (2014), pp. 353-362

[76] Lu T., Xu B., Guo X., Zhao L., Xie F. A new multilevel framework for cyber-physical system security pp. 2–3 (2013)

[77] Kune DF, Backes J, Clark SS, et al. Ghost talk: mitigating EMI signal injection attacks against analog sensors. Proc. - IEEE Symp. Secur. Priv. 2013

[78] M.H. Eldefrawy, M.K. Khan, K. Alghathbar, A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography, in: 2010 International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID), 2010, pp. 1–6.

[79] Figure 3 Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador, Security and privacy issues in implantable medical devices: A comprehensive survey, Journal of Biomedical Informatics, Volume 55, 2015, Pages 272-289, ISSN 1532-0464, https://doi.org/10.1016/j.jbi.2015.04.007.

[80] Graphical Abstract Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador, Security and privacy issues in implantable medical devices: A comprehensive survey, Journal of Biomedical Informatics, Volume 55, 2015, Pages 272-289, ISSN 1532-0464, https://doi.org/10.1016/j.jbi.2015.04.007.

[81] Figure 5 Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador, Security and privacy issues in implantable medical devices: A comprehensive survey, Journal of Biomedical

Informatics, Volume 55, 2015, Pages 272-289, ISSN 1532-0464, https://doi.org/10.1016/j.jbi.2015.04.007.

[82] Table 1 Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador, Security and privacy issues in implantable medical devices: A comprehensive survey, Journal of Biomedical Informatics, Volume 55, 2015, Pages 272-289, ISSN 1532-0464, https://doi.org/10.1016/j.jbi.2015.04.007.

[83] Figure 1 Tabassum, Aliya & Safi, Zeineb & AlKhater, Wadha & Shikfa, Abdullatif. (2018). Cybersecurity Issues in Implanted Medical Devices. 1-9. 10.1109/COMAPP.2018.8460454.

[84] Figure 1 Yosef Ashibani, Qusay H. Mahmoud, Cyber physical systems security: Analysis, challenges and solutions, Computers & Security, Volume 68, 2017, Pages 81-97, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.04.005.

[85] https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%B9%CE%B8%CE%AD%CF%83%CE%B5%CE%B9%CF%82_%CE%AC%CF%81%CE%BD%CE%B7%CF%83%CE%B7%CF%82_%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%B9%CF%8E%CE%BD

[86] https://www.investopedia.com/terms/e/eavesdropping-attack.asp

[87] https://el.wikipedia.org/wiki/Spoofing

[88] https://en.wikipedia.org/wiki/Replay_attack

[89] https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle