Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών
Τομέας Συστημάτων Μετάδοσης
Πληροφορίας και Τεχνολογίας Υλικών

Ασφάλεια στο Διαδίκτυο των Ιατρικών Πραγμάτων (Security in the Internet of Medical Things)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΥΑΓΓΕΛΙΑ Α. ΣΤΑΘΟΠΟΥΛΟΥ

Επιβλέπων : Αθανάσιος Παναγόπουλος
Αναπληρωτής Καθηγητής Ε.Μ.Π.

Συνεπιβλέπων : Παναγιώτης Κοτζανικολάου
Επίκουρος Καθηγητής ΠΑ.ΠΕΙ.

Αθήνα, Οκτώβριος 2019

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών
Τομέας Συστημάτων Μετάδοσης
Πληροφορίας και Τεχνολογίας Υλικών

Ασφάλεια στο Διαδίκτυο των Ιατρικών Πραγμάτων (Security in the Internet of Medical Things)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΥΑΓΓΕΛΙΑ Α. ΣΤΑΘΟΠΟΥΛΟΥ

Επιβλέπων : Αθανάσιος Παναγόπουλος
Αναπληρωτής Καθηγητής Ε.Μ.Π.

Συνεπιβλέπων : Παναγιώτης Κοτζανικολάου
Επίκουρος Καθηγητής ΠΑ.ΠΕΙ.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 16η Οκτωβρίου 2019.

.....	.....	.....
Αθανάσιος Παναγόπουλος Αναπληρωτής Καθηγητής Ε.Μ.Π.	Γεώργιος Ματσόπουλος Καθηγητής Ε.Μ.Π.	Παναγιώτης Κοτζανικολάου Επίκουρος Καθηγητής ΠΑ.ΠΕΙ.

Αθήνα, Οκτώβριος 2019

Ευαγγελία Α. Σταθοπούλου

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Καθώς ο αριθμός των συσκευών (πραγμάτων) που συνδέονται με το Ίντερνετ (*Internet of things: IoT*) αυξάνεται, η επίτευξη ισχυρής ασφάλειας και ιδιωτικότητας (*Security & Privacy*) καθίσταται όλο και πιο δύσκολη. Με τη ευρεία χρήση ιατρικών συσκευών (*Internet of Medical Things: IoMT*), η ανάγκη για ασφάλεια και ιδιωτικότητα στον τομέα της ιατρικής θέτει ένα σοβαρό ζήτημα. Λόγω της κρισιμότητας και της ευαισθησίας των δεδομένων που συναντώνται στον τομέα της υγειονομικής περίθαλψης, η εξασφάλιση της ασφάλειας και της ιδιωτικότητας του Διαδικτύου για ιατρικά πράγματα (IoMT) καθίσταται όλο και πιο σημαντική. Οι περισσότερες συσκευές, εφαρμογές και υποδομές IoMT αναπτύχθηκαν χωρίς να έχει σημασία η ασφάλεια και πιθανότατα θα γίνουν στόχοι κακόβουλων. Η έλλειψη ασφάλειας στα IoMT όχι μόνο υπονομεύει την προστασία της ιδιωτικής ζωής των ασθενών, αλλά μπορεί επίσης να θέσει σε κίνδυνο τη ζωή των ασθενών. Στην παρούσα εργασία, παρουσιάζονται προβλήματα ασφάλειας της ειδικής αυτής κατηγορίας της τεχνολογία IoT αλλά και γενικότερα όλων των έξυπνων συσκευών που συνδέονται στο Διαδίκτυο. Παρουσιάζονται συχνές ευπάθειες που βρίσκουν σε εφαρμογές IoMT οι μηχανικοί και ερευνητές της ασφάλειας υπολογιστών καθώς και πρότυπα και πρακτικές που εφαρμόζονται για την οργανωμένη ανάπτυξη ασφαλών IoMT εφαρμογών. Επιδιώκεται επίσης μια προσέγγιση για την ποσοτικοποίηση των κινδύνων IoMT και την επίδειξη τρόπων μοντελοποίησης απειλών και αξιολόγησης των κινδύνων. Σαν πρακτική εφαρμογή όλων αυτών των μεθοδολογιών, αναπτύχθηκε το μοντέλο απειλών μιας πραγματικής συσκευής αντλίας έγχυσης φαρμάκων που αποτέλεσε και το αντικείμενο μελέτης μας. Στη συνέχεια, ακολούθησε η πειραματική αξιολόγηση ασφάλειας μέσω μιας σειράς δοκιμών. Οι εργασίες αυτές αποσκοπούν στην αύξηση της ευαισθητοποίησης για την ασφάλεια και την ιδιωτικότητα μεταξύ των ενδιαφερομένων μερών των IoMT, δίνοντάς τους την καθοδήγηση να εντοπίσουν και να ποσοτικοποιήσουν τους πιθανούς κινδύνους ασφάλειας των IoMT καθώς και να προβούν σε διαδικασίες ελέγχων ασφάλειας από τους αρμόδιους.

Λέξεις κλειδιά

Ίντερνετ των πραγμάτων, Ίντερνετ των ιατρικών πραγμάτων, έξυπνες ιατρικές συσκευές, μοντελοποίηση απειλών, ανάλυση κινδύνων, διαχείριση κινδύνων, πρότυπα, ιδιωτικότητα, ασφάλεια

Abstract

As the number of Internet of things (IoT) is increasing, achieving robust security and privacy is becoming increasingly difficult. With the widespread use of Internet of Medical Things (IoMT), the need for security and privacy in the medical field raises a serious issue. Due to the criticality and sensitivity of the data encountered in the healthcare sector, ensuring the safety and privacy of the Internet of IoMT is becoming increasingly important. Most IoMT devices, applications, and infrastructures have been developed without security, and will likely become target for hackers. The lack of security in IoMT not only undermines the privacy of patients, but can also endanger patients' lives. In the present work, security problems of this particular category of IoT technology and of all the smart devices connected to the Internet are presented. There are frequent vulnerabilities found in IoMT applications by computer security engineers and researchers as well as standards and practices applied to the organized development of secure IoMT applications. An approach is also sought to quantify IoMT risks and demonstrate ways of threat modeling and risk assessment. As a practical demonstration of all these methodologies, the threat model of a real infusion pump device has been developed and has been the subject of our study. Practical security evaluation was then followed by penetration testing. This work aims to raise awareness of security and privacy among IoMT stakeholders, giving them guidance to identify and quantify potential IoMT security risks and to conduct security auditing procedures by those who are expert in security.

Key words

IoT, IoMT, medical devices, threat modeling, risk assessment, risk management, penetration test, security assessment, privacy, smart medical systems, application security, cybersecurity, IoT security, hackers, medical device security, medical device vulnerabilities

Ευχαριστίες

Με την εκπόνηση της παρούσης διπλωματικής εργασίας ολοκληρώνεται ο κύκλος σπουδών μου στην Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Το όμορφο αυτό ταξίδι γνώσης έφτασε στο τέλος του και θα ήθελα πριν αναφερθώ στο περιεχόμενο της εργασίας να απευθύνω τις ευχαριστίες μου σε όλους όσους συνέβαλλαν σε αυτό το επίτευγμα. Αρχικά, θα ήθελα να ευχαριστήσω τον καθηγητή και επιβλέποντα της εργασίας αυτής κ.Αθανάσιο Παναγόπουλο, για την καθοδήγηση και τις συμβουλές του, δίνοντάς μου συνεχώς ευκαιρίες για προσπάθεια και βελτίωση. Ακόμα, θα ήθελα να πω ένα μεγάλο ευχαριστώ στον καθηγητή Παναγιώτη Κοτζανικολάου και τον κ.Δημήτριο Γλυνό, για την αδιάλειπτη βοήθεια που μου προσέφεραν και την προθυμία επίλυσης οποιουδήποτε ζητήματος που έδειξαν. Επίσης, οφείλω ένα τεράστιο ευχαριστώ στην οικογένειά μου και τους κοντινούς μου ανθρώπους, που με στήριξαν σε κάθε μου βήμα και μου έδωσαν τα εφόδια και την δυνατότητα να ολοκληρώσω τις σπουδές μου. Τέλος, θα ήθελα να ευχαριστήσω θερμά τους φίλους και συμφοιτητές μου, που με συνόδευσαν σε αυτό το δύσκολο μονοπάτι και ήταν πάντα δίπλα μου.

Ευαγγελία Α. Σταθοπούλου,

Αθήνα, 16η Οκτωβρίου 2019

Περιεχόμενα

Κατάλογος πινάκων

Κατάλογος σχημάτων

Ακρωνύμια

2FA Two-factor authentication. 32

3GPP The 3rd Generation Partnership Project. 35

ACL Access Control List. 49

AI Artificial Intelligence. 22, 23

API Application Pprogramming Interface. 39, 68

BLE Bluetooth Low Energy. 85

BSI The British Standards Institution. 52

CA Certificate Authority. 69

CEN The European Committee for Standardization (French: Comité Européen de Normalisation). 41

CIA Confidentiality Integrity Availability. 30, 31, 85

CMMI The Capability Maturity Model Integration. 40

CPS Cyber Physical Systems. 31

CPU Central Processing Unit. 62

CRAMM Central Communication and Telecommunication Agency Risk Analysis and Management Method. 52

CSRF Cross Site Request Forgery. 66

CT Computed Tomography. 26

CTS Cyber Transportation Systems. 31

CVE Common Vulnerabilities and Exposures. 64

DARPA Defense Advanced Research Projects Agency. 44

DDoS Distributed Denial of Service. 49

DML Level of Maturity Detection Level. 44, 45

DoS Denial of Service. 33, 34

DRM Digital Rights Management. 36

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives. 52

ECC Elliptic-curve Cryptography. 73

EMP Electromagnetic Pulse. 32

ENISA European Union Agency for Network and Information Security. 52

ETSI European Telecommunications Standards Institute. 41

FAIR Factor Analysis of Information Risk. 52

FDA U.S. Food and Drug Administration. 26, 40, 83, 84

GDPR The EU General Data Protection Regulation. 84

GLBA Gramm-Leach-Bliley Act. 52

GSM Global System for Mobile Communications. 53, 67, 76, 85, 86

GUI Graphical User Interface. 24

HF High Frequency. 72

HIPAA Health Insurance Portability and Accountability Act. 47, 52, 84

HTTP Hypertext Transfer Protocol. 63, 66, 70

IaaS Infrastructure-as-a-service. 24

IEC International Electrotechnical Commission. 40, 41

IEEE Institute of Electrical and Electronics Engineers. 41, 76

IMSI International Mobile Subscriber Identity. 86

IoMT Internet of Medical Things. 21–28

IoT Internet of Things. 21, 22, 28, 68, 76

IP Internet Protocol. 23

ISF Information Security Forum. 52

ISMS Information Security Management System. 52

ISO International Organization for Standardization. 41, 84

IT Information Technology. 48

ITIL Information Technology Infrastructure Library. 40

JSON JavaScript Object Notation. 71, 72

JTAG Join Test Action Group. 76, 77

LF Low Frequency. 72

M2M Machine to machine communication. 31, 33

MCU Microcontroller Unit. 76

MIT Massachusetts Institute of Technology. 38

MITM Man-in-the-middle. 85

MRI Magnetic Resonance Imaging. 26, 40

NCSC National Cyber Security Centre. 52

NFC Near-field Communication. 72, 76, 85

NIST National Institute of Standards and Technology. 49, 52

NSA National Security Agency. 44

OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation. 44

OWASP Open Web Application Security Project. 63

PASTA Process for Attack Simulation and Threat Analysis. 45

PCB Printed Circuit Board. 76

PCI DSS Payment Card Industry Data Security Standard. 47

PHI Personal Health Information. 25

RAID Redundant Array of Inexpensive Disks. 32

RFID Radio-frequency Identification. 12, 53, 55, 71, 72, 76

RSA Rivest-Shamir-Adleman algorithm. 72

RTM Real Time Medicine. 24, 26

RTOS Real-time operating system. 85

SDLC Software development life cycle. 46

SHA Secure Hash Algorithms. 72

SIEM Security Information and Event Management). 45

SQL Structured Query Language. 37, 66

SSL Secure Sockets Layer. 65, 68, 69, 77

STRIDE Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege. 44, 45

TAL Threat Agent Library. 57

TCP Transmission Control Protocol. 84

TLS Transport Layer Security. 68, 70

TMSI The Temporary Mobile Subscriber Identity. 35

TTP Tactics, Techniques and Procedures. 44, 45

UDP User Datagram Protocol. 84

USB Universal Serial Bus. 71

VAST Visual, Agile και Simple Threat Modeling. 46

WBAN Wireless Body Area Networks. 21

Wi-fi Wireless fidelity. 23, 40, 53, 67, 68, 76

WSN Wireless Sensor Network. 30, 35

X Energetic High-Frequency Electromagnetic Radiation. 26

XML Extensible Markup Language. 66

XSS Cross-site scripting. 37, 66

Κεφάλαιο 1

Εισαγωγή

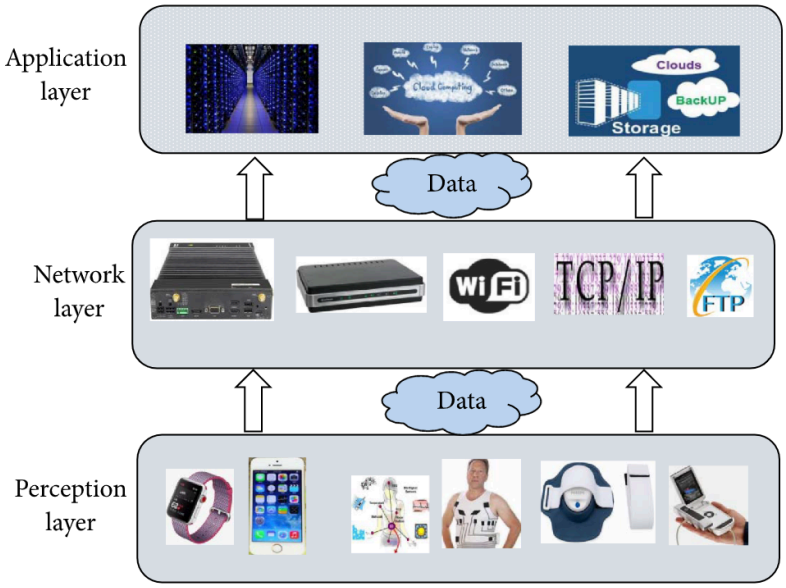
Το Διαδίκτυο των Ιατρικών πραγμάτων (*IoMT: Internet of Medical Things*) αναπτύσσεται γρήγορα σε όλη τη βιομηχανία της υγειονομικής περίθαλψη. Αυτές οι έξυπνες συσκευές όμως δημιουργούν σημαντικούς κινδύνους για την ασφάλεια.

Καθώς το Διαδίκτυο των πραγμάτων (*IoT: Internet of Things*) αυξάνεται σε δημοτικότητα, ο κλάδος της υγειονομικής περίθαλψης έχει λάβει γνώση. Για να αποκομίσουν αποδοτικότητα από πλευράς κόστους και να σώσουν τη ζωή των ασθενών, οι εταιρείες υγειονομικής περίθαλψης αξιοποιούν την τεχνολογία IoMT και ο ρόλος τους ως σημαντικός παράγοντας στην αγορά έξυπνων συσκευών θα συνεχίσει να αυξάνεται.

Ωστόσο, η ιατρική κοινότητα πρέπει να ανησυχεί για τα προβλήματα ασφάλειας στον τομέα της πληροφορικής όσο και για τους ανθρώπους, καθώς η τεχνολογία IoMT μπορεί να αφήσει τις ιατρικές επεμβάσεις και τα δεδομένα ασθενών ευάλωτα στο έγκλημα του κυβερνοχώρου. Στο πλαίσιο αυτό, η ασφάλεια δικτύων είναι περισσότερο αναγκαία από ποτέ, προκειμένου να προστατευθούν τόσο τα μέσα όσο και οι ζωές.

Το διαδίκτυο των ιατρικών πραγμάτων είναι η ομάδα των συσκευών που συνδέονται με το Διαδίκτυο, για την εκτέλεση των διαδικασιών και των υπηρεσιών που υποστηρίζουν την υγειονομική περίθαλψη. Το IoMT έχει αναδειχθεί ως μια νέα τεχνολογία για την ηλεκτρονική υγειονομική περίθαλψη που συλλέγει τις ζωτικές παραμέτρους του σώματος των ασθενών και παρακολουθεί τις παθολογικές τους λεπτομέρειες με μικρές φορητές συσκευές ή εμφυτεύσιμους αισθητήρες. Το IoMT έχει δείξει μεγάλο δυναμικό για την παροχή καλύτερης εγγύησης για την υγεία των ανθρώπων και υποστηρίζει ένα ευρύ φάσμα εφαρμογών από εμφυτεύσιμες ιατρικές συσκευές έως ασύρματο δίκτυο σώματος (WBAN-*Wireless Body Area Networks*).

Γενικά, η δομή IoMT αποτελείται από τρία επίπεδα: το στρώμα αντίληψης (*perception layer*), το στρώμα δικτύου (*network layer*) και το στρώμα εφαρμογής (*application layer*), όπως φαίνεται στο σχήμα 1.1. Το κύριο καθήκον του στρώματος αντίληψης είναι η συλλογή δεδομένων υγειονομικής περίθαλψης με μια ποικιλία συσκευών. Το στρώμα δικτύου, το οποίο αποτελείται από ενσύρματο και ασύρματο σύστημα και μεσαίο λογισμικό, επεξεργάζεται και μεταδίδει την είσοδο που λαμβάνεται από το στρώμα αντίληψης που υποστηρίζεται από τεχνολογικές πλατφόρμες. Τα καλά σχεδιασμένα πρωτόκολλα μεταφοράς όχι μόνο βελτιώνουν την αποδοτικότητα της μετάδοσης και μειώνουν την κατανάλωση ενέργειας, αλλά και διασφαλίζουν την ασφάλεια και την ιδιωτικότητα. Το στρώμα εφαρμογής ενσωματώνει τους πόρους ιατρικών πληροφοριών για την παροχή εξατομικευμένων ιατρικών υπηρεσιών και την ικανοποίηση των αναγκών των τελικών χρηστών, ανάλογα με την πραγματική κατάσταση του πληθυσμού-στόχου και τη ζήτηση υπηρεσιών.



Σχήμα 1.1: Δομή IoMT

1.1 Βασικά χαρακτηριστικά των IoMT

Τα IoMT (*Internet of Medical Things*) είναι μια υπο-αγορά του Διαδικτύου των Πραγμάτων (IoT), η οποία έχει επιφέρει μεγάλη εξέλιξη στην τεχνολογία των υπολογιστικών συστημάτων. Όπως το IoT αναφέρεται σε όλες τις συσκευές με δυνατότητα διασύνδεσης στο Διαδίκτυο (*Internet*), από τα έξυπνα αυτοκίνητα έως τις συσκευές κουζίνας, το IoMT περιλαμβάνει όλες τις ιατρικές εγαρμογές με συσκευές που διαθέτουν δυνατότητα σύνδεσης στο Διαδίκτυο.

Η τεχνολογία των IoMT επιτρέπει η κάθε ιατρική συσκευή να συλλέγει, να αναλύει και να στέλνει δεδομένα σε ολόκληρο τον Ιστό. Όχι μόνο οι ψηφιακές συσκευές, όπως οι οθόνες καρδιάς, μπορούν να συνδεθούν στο Διαδίκτυο, αλλά πλέον μπορούν και τα μη ψηφιακά αντικείμενα όπως τα νοσοκομειακά κρεβάτια ακόμα και τα χάπια.

Ουσιαστικά, η τεχνολογία IoMT επιτρέπει στον ιατρικό εξοπλισμό και στα προϊόντα υγειονομικής περίθαλψης να μοιράζονται δεδομένα σε πραγματικό χρόνο και με όλους όσους έχουν νόμιμη πρόσβαση στις πληροφορίες.

Τα IoMT έχουν βασιστεί σε μια σειρά τεχνολογιών, συμπεριλαμβανομένων των προηγμένων αισθητήρων, της συνδεσιμότητας των IoT και της τεχνητής νοημοσύνης (AI-*Artificial Intelligence*) πλέον.

Ιατρικοί αισθητήρες

Το μειούμενο κόστος της τεχνολογίας αισθητήρων επέτρεψε στους κατασκευαστές συσκευών IoMT να δημιουργήσουν οικονομικά συνδεδεμένα προϊόντα υγειονομικής περίθαλψης. Οι βιοαισθητήρες αποτελούν ένα υγιές κομμάτι της αγοράς προϊόντων IoMT, ενώ τα έσοδα της αγοράς αναμένεται να ξεπεράσουν τα 29 δισεκατομμύρια δολάρια μέχρι το 2024 [stat18]. Αυτές οι προηγμένες συσκευές βασίζονται σε ένα βιολογικό υλικό και αισθητήρα για την ανίχνευση χαρακτηριστικών του αίματος, της αναπνοής, του ιστού και άλλων τμημάτων του σώματος. Οι μη βιολογικοί ιατρικοί αισθητήρες μπορούν να μετρήσουν τη θερμοκρασία του σώματος, την κίνηση, την ηλεκτρική δραστηριότητα της καρδιάς και των μυών και άλλα χαρακτηριστικά του ασθενούς.

Συνδεσιμότητα IoT

Η ανίχνευση των παραγόντων υγείας ενός ασθενούς είναι μόνο ένα μέρος των IoMT. Προκειμένου τα δεδομένα να είναι χρήσιμα, πρέπει να είναι προσβάσιμα από υπολογιστές και ανθρώπους. Οι κατασκευαστές του IoMT χρησιμοποιούν μια τεράστια ποικιλία πρωτοκόλλων επικοινωνίας για να μεταφέρουν δεδομένα IoMT από ένα σημείο Α σε ένα σημείο Β. Ωστόσο, όλοι επιτυγχάνουν τον ίδιο στόχο - να στείλουν τα ιατρικά δεδομένα στο Διαδίκτυο. Έτσι, οποιοσδήποτε εξουσιοδοτημένος χρήστης ή υπολογιστής μπορεί να έχει πρόσβαση στα δεδομένα και να το χρησιμοποιήσει για να βοηθήσει στην παροχή φροντίδας στον ασθενή.

Είτε μια οθόνη παρακολούθησης της γλυκόζης στο σπίτι είτε μια οθόνη καρδιάς έκτακτης ανάγκης, οι συσκευές IoMT μεταδίδουν τα δεδομένα τους σε ένα κοντινό δίκτυο. Αυτό το πρώτο σημείο επαφής για μια συσκευή IoMT μπορεί να είναι μια οικιακή ασύρματη σύνδεση (Wi-fi), ένα δίκτυο κινητής τηλεφωνίας ή ένα νοσοκομειακό ιατρικό δίκτυο πληροφορικής. Τελικά, τα δεδομένα των IoMT συνήθως μπαίνουν σε μια βάση δεδομένων, η οποία είναι προσβάσιμη από το Διαδίκτυο. Δεδομένου ότι κάθε συσκευή IoMT έχει μια μοναδική διεύθυνση IP, υπάρχουν ελάχιστες πιθανότητες να μπερδευτούν τα δεδομένα από όλες τις συσκευές.

Τεχνητή Νοημοσύνη (AI)

Η τεχνητή νοημοσύνη έχει αρχίσει να παίζει όλο και σημαντικότερο ρόλο στην ανάπτυξη IoMT. Με τον αριθμό των συσκευών IoMT που θα φτάνουν τα 20 με 30 δισεκατομμύρια μέχρι το 2020, η ικανότητα επεξεργασίας όλων αυτών των δεδομένων είναι ζωτικής σημασίας για την επιτυχία της τεχνολογίας.

Τα λογισμικά τεχνητής νοημοσύνης (AI) είναι σε θέση να ταξινομούν έξυπνα ένα *torrent* δεδομένων από συσκευές IoMT και να παρέχουν στους ιατρούς μόνο δεδομένα που χρειάζονται την προσοχή τους. Καθώς η αγορά μεγαλώνει, η τεχνητή νοημοσύνη θα είναι ο σιωπηλός συνεργάτης που οι γιατροί θα έρθουν να επικαλεστούν για να είναι ενημερωμένοι.

1.2 Πλεονεκτήματα των IoMT

Η σύνδεση όλων των ”έξυπνων” ιατρικών συσκευών προσφέρει τεράστια πλεονεκτήματα από τα οποία επωφελούνται οι πάροχοι υγειονομικής περίθαλψης, οι ασφαλιστές και οι ασθενείς.

Προσιτότητα

Ένα από τα μεγαλύτερα οφέλη που προσφέρεται είναι η ικανότητα των γιατρών να έχουν πρόσβαση στα δεδομένα υγείας των ασθενών σε πραγματικό χρόνο. Αντί να χρειάζεται να γίνει επίσκεψη στο δωμάτιο του ασθενούς ή να κληθεί μια νοσοκόμα, ένας πολυάσχολος καρδιολόγος μπορεί να δει τις αναγνώσεις καρδιακού παλμού ενός ασθενούς απευθείας στο κινητό (*smartphone*) του. Οι γιατροί μπορούν ακόμη να δουν ιατρικές εικόνες αμέσως μόλις ληφθούν από το νοσοκομείο. Οι ασθενείς μπορούν να δουν τα δικά τους δεδομένα, χρησιμοποιώντας *online* πύλες ασθενών.

Χαμηλό κόστος και γρήγορη εφαρμογή ανά ασθενή

Εκτιμάται ότι τα IoMT θα εξοικονομήσουν 300 δισεκατομμύρια δολάρια στον κλάδο της υγειονομικής περίθαλψης. Δεδομένου ότι τα IoMT επιτρέπουν ταχύτερη πρόσβαση στα

δεδομένα των ασθενών, η λειτουργική αποτελεσματικότητα βελτιώνεται σημαντικά και επιτρέπει την πιο αποτελεσματική αξιοποίηση του χρόνου του ιατρικού προσωπικού.

Επιπλέον, ταχύτερη πρόσβαση σε δεδομένα σημαίνει ταχύτερη ανάλυση δεδομένων, ταχύτερη διάγνωση και θεραπεία. Όσο πιο γρήγορα οι ασθενείς μπορούν να λάβουν τη θεραπεία που χρειάζονται, τόσο νωρίτερα μπορούν να θεραπευτούν. Τα συστήματα RTM (*Real time medicine*) μειώνουν το κόστος επιτρέποντας στους ασθενείς να μένουν στο σπίτι και να μειώνουν τις επισκέψεις, ενώ παράλληλα η απομακρυσμένη παρακολούθηση επιτρέπει στους γιατρούς να ανιχνεύουν και να αντιμετωπίζουν προβλήματα πριν γίνουν πιο σοβαρά.

Οι συσκευές IoMT έχουν σχεδιαστεί για να είναι γρήγορες και εύκολες στην εφαρμογή τους. Μικροί, ασύρματοι αισθητήρες IoMT επιτρέπουν στους ασθενείς και τα υγιή άτομα να ελέγχουν τα δικά τους ζωτικά όργανα.

Βελτιωμένη απόδοση

Το κόστος δεν είναι το μόνο όφελος. Ο χρόνος αναμονής είναι το νούμερο ένα πρόβλημα των ασθενών σχετικά με τις ιατρικές επισκέψεις, πόσο μάλιστα όταν πρόκειται για κρούσματα εντατικής και έκτατης ανάγκης. Η βελτίωση της αποτελεσματικότητας καλυτερεύει την εμπειρία των ασθενών, η οποία θα πρέπει πάντα να αποτελεί κορυφαίο στόχο για τους παρόχους.

1.3 Προκλήσεις εφαρμογής των IoMT

Όπως και οι περισσότερες τεχνολογίες, τα IoMT φέρνουν τόσο πλεονεκτήματα όσο και μειονεκτήματα.

Υψηλό κόστος υποδομής

Ενώ η πτώση των τιμών των αισθητήρων και η μαζική παραγωγή συσκευών IoMT καθιστούν οικονομική την εφαρμογή τους, το κόστος κατασκευής της υποδομής IoMT είναι τεράστιο. Δίκτυα πληροφορικής IoMT, *blockchains* και πλατφόρμες νέφους (*cloud*) είναι όλα απαραίτητα για να γίνει σωστή υλοποίηση τους. Τα κόστη διανέμονται μεταξύ υλικού, υποδομής, εφαρμογών και εκπαίδευσης. Παράλληλα, η μετάβαση από τα παλαιότερα συστήματα στις ”έξυπνες” συσκευές απαιτεί χρόνο, προγραμματισμό και λεφτά.

Ενσωμάτωση στα υφιστάμενα δίκτυα

Πολλά υπάρχοντα νοσοκομειακά δίκτυα δεν είναι αρκετά ισχυρά ούτε αρκετά ασφαλή για να χειριστούν ένα πλήρως εφαρμοσμένο σύστημα IoMT. Προκειμένου οι ”έξυπνες” συσκευές να εισχωρήσουν στο ήδη υπάρχον δίκτυο, πρέπει αυτό και όλα τα υποστηρικτικά μέρη των εγκαταστάσεων να είναι γρήγορα, ασφαλή και με δυνατότητα κλιμάκωσης. Η μεταφορά διεπαφών GUI, αποθήκευσης και συγκεκριμένων διεργασιών δεδομένων σε περιβάλλον νέφους (*cloud*) μπορεί να μειώσει δραματικά το βάρος του παλαιού συστήματος πληροφορικής. Επιπλέον, όσο περισσότερα δεδομένα βρίσκονται στο *cloud*, τόσο λιγότερες είναι οι πιθανότητες παραβίασης τους. Καθώς η βιομηχανία IoMT αναβαθμίζεται, αναμένεται να διαδοθούν οι πλατφόρμες Υποδομής ως Υπηρεσία (IaaS-*Infrastructure-as-a-service*) που βασίζονται στην υγειονομική περίθαλψη για να εξυπηρετήσουν αυτήν την αγορά.

Έλλειψη τυποποίησης και νομικών κανονισμών

Η έλλειψη τυποποίησης μεταξύ των κατασκευαστών των IoMT είναι ένα μειονέκτημα. Με πολλά πρωτόκολλα επικοινωνιών, συσκευές από διαφορετικούς κατασκευαστές συχνά δεν είναι διαλειτουργικές. Ο συνδυασμός συσκευών με πολλαπλά πρότυπα στο ίδιο δίκτυο μειώνει σημαντικά την ασφάλεια και τη σταθερότητα του συστήματος.

Αν και γίνονται κάποιες προσπάθειες, όπως συμβαίνει και με άλλες τεχνολογίες, οι κατασκευαστές συνεχίζουν να κατασκευάζουν μη τυποποιημένα προϊόντα. Συγκεκριμένα, οι Η.Π.Α. υστερούν σε σχέση με την Ευρώπη σε νομοθετικές προσπάθειες για τα πρότυπα των IoMT. Ακόμη και στις χώρες όπου υπάρχει κοινωνικοποιημένη υγειονομική περίθαλψη, τα πρότυπα εκλείπουν. Στις Ηνωμένες Πολιτείες, η προηγούμενη κυβερνητική εποπτεία της υγειονομικής περίθαλψης κατευθύνθηκε προς τις εγκρίσεις φαρμάκων και διαδικασιών και τα δικαιώματα ιδιωτικής ζωής των ασθενών. Η τρέχουσα νομοθεσία των Η.Π.Α. μιλάει για τα πρότυπα για την ασφάλεια των πληροφοριών για την υγεία των ασθενών (PHI) και καθορίζει τι αποτελεί ιατρική συσκευή. Ειδικοί νόμοι που υποχρεώνουν τους κατασκευαστές να κατασκευάσουν διαλειτουργικά προϊόντα λείπουν πάρα πολύ. Η Ευρώπη έχει αρκετούς νόμους που ρυθμίζουν τα ιατροτεχνολογικά προϊόντα, αλλά κανένας δεν απαιτεί τυποποιήσεις. Υπάρχει επιτακτική ανάγκη για ωρίμανση των επιπέδων συνεργασίας των συμμετέχοντων στην βιομηχανία IoMT.

Ευπάθειες ασφάλειας

Τίποτα δεν παρεμποδίζει την υιοθέτηση της τεχνολογίας IoMT περισσότερο από ό,τι αφορά την ασφάλεια, αποτελώντας τη μεγαλύτερη απειλή για τη μακροπρόθεσμη βιωσιμότητα των λύσεων IoT στην υγειονομική περίθαλψη. Με εκατοντάδες εκατομμύρια ιατρικά αρχεία ασθενών που έχουν ήδη υποστεί βλάβη λόγω παραβιάσεων ιατρικών δεδομένων, η ασφάλεια πρέπει να είναι ίση με την ποιότητα της φροντίδας για τους στόχους της βιομηχανίας. Η επιτυχία των εγκληματιών στον κυβερνοχώρο πριν την είσοδο της τεχνολογίας των IoMT προκαλεί ανησυχίες για την εξασφάλιση της ασφάλειας όλων αυτών των ιατρικών δεδομένων στο διαδίκτυο. Χρειάζονται λύσεις με επίκεντρο την ασφάλεια και συνεχείς επενδύσεις στην τεχνολογία της προστασίας του κυβερνοχώρου. Αυτή τη στιγμή, η τεχνολογία *blockchain* προσφέρει το μοναδικό πλαίσιο αρκετά ισχυρό ώστε να ανταποκρίνεται στις προκλήσεις ασφαλείας των IoMT.

Βασικό χαρακτηριστικό των IoT και ειδικότερα των IoMT είναι οι σημαντικοί περιορισμοί που υπάρχουν σε επίπεδο υλικού και στην αρχιτεκτονική προκειμένου να συμβαδίζουν με την ανάγκη της φορητότητας και της υψηλής διαθεσιμότητας (*high availability*) . Η ανάγκη φορητότητας της συσκευής προσδιορίζει την αρχιτεκτονική που θα ακολουθηθεί κατά την σχεδίαση περιορίζοντας το μέγεθος καθώς και την ενεργειακή τροφοδοσία που αυτή θα έχει, περιορισμός που επηρεάζει τους μηχανισμούς ασφαλείας που μπορούν να εφαρμοστούν. Η ανάγκη υψηλής διαθεσιμότητας σχετίζεται άμεσα με την ανάγκη για χαμηλή κατανάλωση ενέργειας της συσκευής σε όλη τη διάρκεια λειτουργίας της. Η συνολικά καταναλισκώμενη ενέργεια εξαρτάται από πολλούς παράγοντες αρκετοί από τους οποίους έχουν άμεση αντανάκλαση στο επίπεδο ασφάλειας που μπορεί να προσφέρει η συσκευή.

1.4 Περιγραφή σεναρίων χρήσης IoMT

Η τεχνολογία IoMT βρίσκει πληθόρα εφαρμοφών στις μέρες μας. Όπως θα περίμενε κανείς, στα νοσοκομεία και τις κλινικές γίνεται η πιο συχνή χρήση των συσκευών IoMT, οι οποίες βελτιώνουν την ποιότητα της υγειονομικής περίθαλψης μειώνοντας ταυτόχρονα το κόστος κάτι που οι πάροχοι υπηρεσιών υγείας βρίσκουν πολύ ελκυστικό.

Εφαρμογές στις κλινικές και τα νοσοκομεία

Πέρα από τις εφαρμογές των IoMT στα νοσοκομεία και τις κλινικές για την παρακολούθηση ασθενών, εξοπλισμός όπως τα MRI, τα μηχανήματα ακτίνων X, οι σαρωτές CT μπορούν να παρακολουθούνται εξ αποστάσεως για θέματα επιδόσεων. Πολύ πριν το προσωπικό του νοσοκομείου διαπιστώσει κάποιο πρόβλημα, ο κατασκευαστής ή ο πωλητής υπηρεσιών μπορεί να εντοπίσει ζητήματα που απαιτούν διόρθωση. IoMT χρησιμοποιούνται και για απομακρυσμένη διάγνωση, προγνωστική συντήρηση και αναβάθμιση επιδόσεων στα προϊόντα απεικόνισης.

Εφαρμογές στο σπίτι

Σημαντικό αναφοράς, είναι η ιατρική τεχνολογία συνδεσιμότητας, που ονομάζεται επίσης τηλεϊατρική, επιτρέποντας οι υπηρεσίες υγειονομικής περίθαλψης να επεκταθούν πέρα από τα τείχη του νοσοκομείου, στο σπίτι. Η απομακρυσμένη παρακολούθηση ασθενών (RTM) επιτρέπει σε πολλούς ασθενείς που πάσχουν από χρόνια ασθένεια να αποφεύγουν τις συχνές επισκέψεις στο γιατρό. Οι καρδιακοί ασθενείς και οι διαβητικοί είναι παθόντες που μπορούν να ωφεληθούν από την τεχνολογία RTM. Οι φορητές συσκευές RTM μπορούν να παρακολουθούν την καρδιακή δραστηριότητα των ασθενών και τα επίπεδα γλυκόζης και να ειδοποιούν αυτόματα τον γιατρό όταν υπάρχει κάποιο πρόβλημα. Οι εικονικοί βοηθοί (*Virtual Assistants*) είναι μια πολύτιμη προσθήκη στο σπίτι για πολλούς ηλικιωμένους ασθενείς. Αυτές οι έξυπνες συσκευές αλληλεπιδρούν με τον ασθενή, υπενθυμίζοντάς τους να παίρνουν φάρμακα επιτρέποντας την πρόσβαση εξ αποστάσεως στην οικογένεια και στους γιατρούς.

Εφαρμογές στο ανθρώπινο σώμα

Οι πρόοδοι στην τεχνολογία των βιοαισθητήρων καθιστούν εφικτές τις φορητές έξυπνες συσκευές που παρακολουθούν την υγεία του χρήστη. Οι αισθητήρες IoMT, είτε ενσωματωμένοι σε ενδύματα, προσαρμοσμένοι στο δέρμα ή εμφυτευμένοι στο σώμα επιτρέπουν την στενή παρακολούθηση των συνθηκών της υγείας των ασθενών ενώ παράλληλα δεν εμποδίζουν τις ελευθερίες του σώματος.

Παραδείγματα εφαρμογών IoMT

Ακολουθούν κάποια παραδείγματα εφαρμογών IoMT άξια αναφοράς:

- Το Abilify MyCite εγκρίθηκε τον Νοέμβριο από τις ΗΠΑ από την Υπηρεσία Τροφίμων και Φαρμάκων (FDA). Είναι ένα έξυπνο χάπι που περιέχει ένα δισκίο αριπιπραζόλης για τη θεραπεία της σχιζοφρένειας και έναν έξυπνο αισθητήρα. Όταν το χάπι εισέλθει στο στομάχι, ο αισθητήρας στέλνει ένα σήμα σε μια εφαρμογή *smartphone*, υποδεικνύοντας πότε το χάπι λήφθηκε. Η έγκριση ανοίγει το δρόμο για άλλα φάρμακα να περιέχουν παρόμοιους αισθητήρες.

- Το eVisit είναι μια πλατφόρμα τηλεϊατρικής που επιτρέπει στους γιατρούς να διεξάγουν εξετάσεις και να συνταγογραφούν φάρμακα για τους ασθενείς τους από απόσταση.
- Η Amiko.IO επικεντρώνεται στην παροχή προϊόντων για τη διαχείριση της αναπνευστικής νόσου, με μια πλατφόρμα με τεχνολογία τεχνητής νοημοσύνης.
- Το MoMe Kardia παρέχει απομακρυσμένη παρακολούθηση της καρδιακής αρρυθμίας.
- Το PillCamTM είναι μια σειρά καταπραϋντικών καψουλών που επιτρέπουν την απεικόνιση του οισοφάγου, του στομάχου, του λεπτού εντέρου και του παχέος εντέρου. Τα δεδομένα απεικόνισης μεταδίδονται σε έναν εξωτερικό θεατή για ανάλυση από τον ιατρό.

1.5 Στόχοι της εργασίας

Παρόλο που η πλειοψηφία των οργανισμών υγειονομικής περίθαλψης δεν αφιερώνουν επαρκείς πόρους για την προστασία της ασφάλειας και της ιδιωτικής ζωής, δεν υπάρχει αμφιβολία ότι η ασφάλεια και η προστασία της ιδιωτικής ζωής διαδραματίζουν βασικό ρόλο στα IoMT. Οι συσκευές IoMT παράγουν όλο και μεγαλύτερο όγκο όλο και διαφορετικών δεδομένων σε πραγματικό χρόνο, τα οποία είναι ιδιαίτερα ευαίσθητα. Αφενός, η καταστροφή της ασφάλειας του ιατρικού συστήματος ή του δικτύου θα μπορούσε να έχει καταστροφικές συνέπειες. Μάλιστα, δεδομένου ότι μία επιτυχής επίθεση ασφάλειας θα μπορούσε να προκαλέσει μέχρι και φυσική βλάβη ή διακύβευση της υγείας του ασθενούς, είναι προφανές ότι τέτοιες συσκευές είναι μεγάλης κρισιμότητας. Από την άλλη πλευρά, οι πληροφορίες προσωπικού απορρήτου του ασθενούς υπάρχουν σε όλα τα στάδια της συλλογής, της μετάδοσης, της αποθήκευσης στο νέφος και της αναδημοσίευσης τους.

Η επιτυχημένη ανάπτυξη των IoMT πρέπει να θεωρεί την ασφάλεια και την προστασία της ιδιωτικής ζωής βασικό παράγοντα. Στόχος της εργασίας μας, είναι να φανεί πόσο σημαντική είναι η ύπαρξη ασφάλειας και ιδιωτικότητας στις εφαρμογές IoMT παρουσιάζοντας κοινά προβλήματα σε IoMT αλλά και σε IoT γενικότερα, και πώς μπορεί να εξασφαλιστεί καλύτερα με ανάπτυξη αρχικών μοντέλων απειλών και ανάλυσης κινδύνων κατά το σχεδιασμό τους.

Κυρίως όμως θέλουμε να τονίσουμε την σημαντικότητα της πειραματικής ανάλυσης ασφάλειας ενός προϊόντος, δηλαδή της διαδικασίας προσπαθειών και δοκιμών παραβίασης και εκμετάλλευσης με κακόβουλο τρόπο των υπολογιστικών συστημάτων με σκοπό την έγκαιρη εύρεση ευπαθειών και τη διόρθωση τους από ειδικούς μηχανικούς ασφάλειας υπολογιστών πριν βγουν στην αγορά. Επισημαίνεται ότι παρ'όλο που οι έλεγχοι ασφάλειας αφορούν μια υπό ανάπτυξη συσκευή αντλίας έγχυσης φαρμάκων που είναι το αντικείμενο μελέτης μας, οι διαδικασίες καθώς και τα χαρακτηριστικά του υπολογιστικού συστήματος είναι παρόμοια με όλες τις IoMT εφαρμογές.

1.6 Δομή Εργασίας

Στην παρούσα διπλωματική εργασία ασχολούμαστε με την μοντελοποίηση απειλών και την πειραματική ανάλυση ασφάλειας ως δύο σημαντικά μέρη της κατασκευής διασυνδεδεμένων ιατρικών συσκευών για την εξασφάλιση της ασφάλειας και της ιδιωτικότητας. Στο Κεφάλαιο 2 εισάγουμε το θεωρητικό υπόβαθρο που απαιτείται για την κατανόηση αυτών που

αναφέρονται στη συνέχεια της εργασίας. Συνοπτικά, εξηγούμε τα προβλήματα ασφάλειας που υπάρχουν στις εφαρμογές IoT αλλά και πιο συγκεκριμένα στη συνέχεια όσων αφορά τις εφαρμογές των IoT στο χώρο της ιατρικής περίθαλψης. Επίσης, γίνεται αναφορά σε βασικές έννοιες που αφορούν το κομμάτι της Ασφάλειας των υπολογιστών καθώς και πρότυπα και πρακτικές ασφάλειας των IoMT. Το Κεφάλαιο 3 αφορά τις μεθοδολογίες μοντελοποίησης απειλών και αξιολόγησης κινδύνων, πρακτικές που είναι απαραίτητες για το σωστό σχεδιασμό ενός ασφαλούς υπολογιστικού συστήματος και προφανώς και στο σχεδιασμό IoMT καθώς συγκεντρώνει όλες τις απαιτήσεις ασφάλειας σε θεωρητικό επίπεδο. Όλο αυτό αποτελεί την εισαγωγή για το Κεφάλαιο 4 το οποίο ξεκινά με το μοντέλο απειλών που ανπτύχθηκε και κάποια μέτρα ασφάλειας που βρέθηκαν για το αντικείμενο μελέτης μας. Στη συνέχεια, παρουσιάζεται όλη η διαδικασία της πειραματικής αξιολόγησης ασφάλειας του αντικειένου μελέτης μας, καθώς και ευπάθειες που βρέθηκαν συνοδευόμενες με λύσεις ασφάλειας. Τέλος, στο Κεφάλαιο 5 καταγράφονται τα βασικά συμπεράσματα καθώς και μια σύντομη παρουσίαση της τρέχουσας κατάστασης σχετικά με την ασφάλεια στις διασυνδεδεμένες ιατρικές συσκευές, καταλήγοντας σε μελλοντικές κατευθύνσεις που αφορούν την πειραματική αξιολόγηση του αντικειμένου μελέτης.

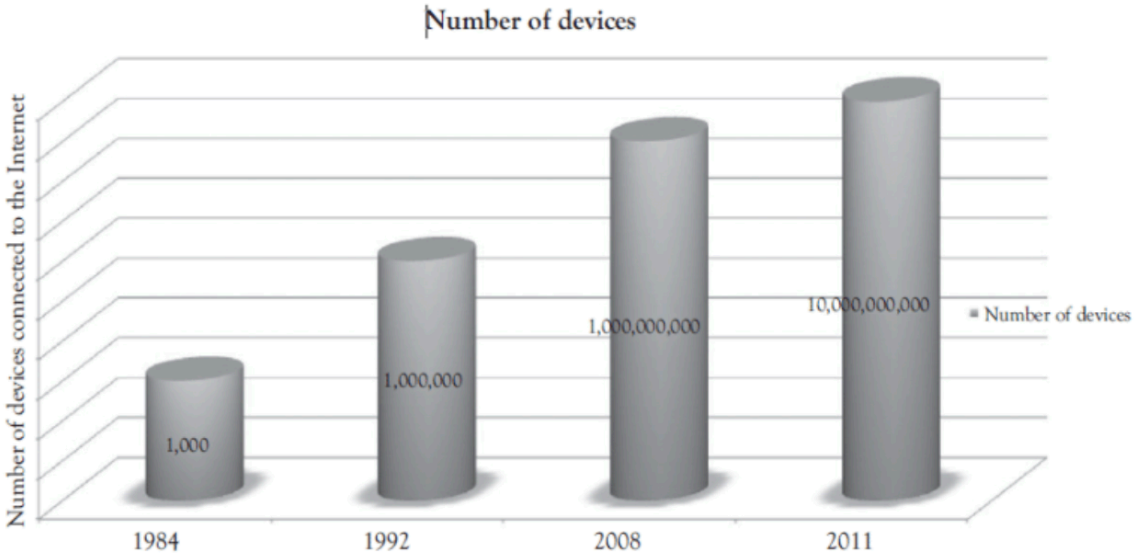
Κεφάλαιο 2

Προβλήματα ασφάλειας σε IoMT

Στο συγκεκριμένο κεφάλαιο στόχος είναι να καλύψουμε όλο το θεωρητικό υπόβαθρο σχετικά με την ασφάλεια στην τεχνολογία των IoT πάνω στο οποίο έχει βασιστεί και η πειραματική ανάλυση του 4ου κεφαλαίου. Λόγω του αντικειμένου της διπλωματικής που αφορά την ασφάλεια των ιατρικών διασυνδεδεμένων συσκευών θα αναφερθούμε αρχικά σε προβλήματα ασφάλειας των IoT γενικότερα και στη συνέχεια θα επεκταθούμε σε αυτά που συναντιούνται στις εφαρμογές του τομέα της πληροφορικής για τη βελτίωση του κλάδου της υγειονομικής περίθαλψης.

Το Ίντερνετ ιατρικών πραγμάτων (IoMT:*Internet of Medical Things*), γνωστό και ως IoT στον τομέα της υγείας, αναφέρεται στο σύνολο των ”έξυπνων” ιατρικών συσκευών και εφαρμογών που συνδέονται μέσω δικτύων. Πολλοί πάροχοι υγειονομικής περίθαλψης χρησιμοποιούν τις εφαρμογές IoMT για τη βελτίωση των θεραπειών, τη διαχείριση των ασθενειών, τη μείωση των λαθών, τη βελτίωση της εμπειρίας των ασθενών, τη διαχείριση των φαρμάκων και τη μείωση του γενικότερου κόστους. Σύμφωνα με έρευνα αγοράς [fore], το τμήμα της αγοράς της ιατρικής περίθαλψης για την υγειονομική περίθαλψη είναι έτοιμο να φτάσει τα 117 δισεκατομμύρια δολάρια μέχρι το 2020. Μια πορεία της αύξησης του αριθμού των συσκευών φαίνεται και στο σχήμα 2.1. Ωστόσο, η μεγάλη ποικιλία των ”έξυπνων συσκευών” στην υγειονομική περίθαλψη εισάγει νέους κινδύνους στην ασφάλεια των συστημάτων υγειονομικής περίθαλψης. Αυτό οφείλεται στους ακόλουθους λόγους:

1. Οι διασυνδεδεμένες ιατρικές συσκευές ανταλλάσσουν κυρίως ”ευαίσθητα” δεδομένα



Σχήμα 2.1: Αριθμός ”έξυπνων” ιατρικών συσκευών

ασθενών.

2. Προβλήματα πολυπλοκότητας και ασυμβατότητας προκύπτουν από την αλληλεπίδραση ενός μεγάλου αριθμού συσκευών και ετερογενών δικτύων που τα συνδέουν [Waur16].

3. Επειδή τα IoT είναι ένας νέος και αναδυόμενος τομέας, οι κατασκευαστές της υγειονομικής περίθαλψης βιάζονται να υιοθετήσουν τέτοιες λύσεις έξυπνων συστημάτων χωρίς να δίνουν τόση σημασία στην ασφάλεια. Λόγω αυτού, προκύπτουν νέα ζητήματα ασφάλειας που σχετίζονται με την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (CIA *triad*) που είναι το αντικείμενο του κλάδου ασφάλειας πληροφορικής (*information security*).

4. Δεδομένου ότι τα περισσότερα στοιχεία IoT μεταδίδουν και λαμβάνουν δεδομένα ασύρματα, αυτό επιφέρει στα IoMT κίνδυνους παραβιάσεων της ασφάλειας του ασύρματου δικτύου αισθητήρων (WSN - *Wireless Sensor Network*) [Mamt16].

5. Επιπλέον, σχεδόν όλες οι λύσεις IoMT περιλαμβάνουν εφαρμογές για τη λειτουργία, την παρακολούθηση και τον έλεγχο τους. Έτσι εισάγονται κίνδυνοι όπως οι παραβιάσεις της πιστοποίησης ταυτότητας (*authentication*) και της εξουσιοδότησης (*authorization*), καθώς και η συνολική ασφάλεια και διαθεσιμότητα (*availability*) και εξυπηρέτηση των αιτημάτων αποτελούν επίσης ανησυχίες [Jing14].

6. Ορισμένοι υπολογισμοί ασφαλείας καταναλώνουν σημαντικό μέρος των υπολογιστικών πόρων. Λόγω των περιορισμένων δυνατοτήτων (δηλαδή υπολογισμών και ισχύος) χαρακτηριστικό των ενσωματωμένων συσκευών όπως είναι και οι ασύρματοι αισθητήρες, πολλοί από αυτούς δεν έχουν υλοποίηση κρυπτογράφησης (στοιχείο απαραίτητο για τη διαφύλαξη του απορρήτου ”ευαίσθητων” δεδομένων). Αυτή η απουσία ισχυρής κρυπτογράφησης μέσω των ”έξυπνων” ιατρικών συσκευών ανοίγει πεδία προς ανακάλυψη και εκμετάλλευση από κακόβουλους επιτιθέμενους [Hoss15].

Ως εκ τούτου, η επιδίωξη ασφάλειας και ιδιωτικότητας στα IoMT έχει εξελιχθεί σε ζήτημα πρωταρχικής σημασίας για τον κλάδο της υγειονομικής περίθαλψης. Με βάση την κρισιμότητα του περιβάλλοντος υγείας, τέτοιοι κίνδυνοι ασφάλειας μπορούν να επιφέρουν καταστροφικές συνέπειες, όπως είναι μεταξύ άλλων η λάθος θεραπεία, η απώλεια ζωής, η κακή φήμη οργανισμών και οι οικονομικές απώλειες. Τα τελευταία έχουν επίπτωση και στις εταιρείες που εφευρεύουν τέτοιες συσκευές καθώς και τους οργανισμούς υγείας που τις χρησιμοποιούν. Γίνεται αντιληπτό, ότι υπάρχει επείγουσα ανάγκη να εντοπιστούν και να εκτιμηθούν οι κίνδυνοι των IoMT για να υποστηριχθεί καλύτερα η λήψη αποφάσεων κατά την υιοθέτηση ή το σχεδιασμό ενός ασφαλούς και αξιόπιστου IoMT.

2.1 Προβλήματα ασφάλειας των IoT

Ο όρος Διαδίκτυο των Πραγμάτων (IoT) που αναφέρεται σε μοναδικά αναγνωρίσιμα αντικείμενα, πράγματα σε μια διαδικτυακή δομή προτάθηκε για πρώτη φορά το 1998 [Webe10]. Τα τελευταία χρόνια, η έννοια του Διαδικτύου έχει γίνει ιδιαίτερα δημοφιλής μέσω μερικών αντιπροσωπευτικών εφαρμογών (π.χ., ανάγνωση ευφυών ηλεκτρικών μετρητών, παρακολούθηση θερμοκηπίου, παρακολούθηση μέσω τηλεϊατρικής και ευφυείς μεταφορές). Συνήθως, τα IoT έχουν βασικά στοιχεία, την ανίχνευση, την ετερογενή πρόσβαση, την επεξεργασία πληροφοριών, τις εφαρμογές και υπηρεσίες, καθώς και πρόσθετα στοιχεία όπως η

ασφάλεια και η ιδιωτικότητα. Σήμερα, τα IoT είναι συνδεδεμένα με τα έξυπνα συστήματα μεταφοράς (CTS-*Cyber Transportation Systems*), τα κυβερνο-φυσικά συστήματα (CPS-*Cyber Physical Systems*) και τις επικοινωνίες μηχανής προς μηχανή (M2M-*Machine to machine communication*) [Wan11]. Όσον αφορά την ασφάλεια, τα IoT αντιμετωπίζουν σοβαρές προκλήσεις. Οι λόγοι είναι οι εξής:

1. Τα IoT επεκτείνουν το διαδίκτυο μέσω των παραδοσιακών δικτύων, όπως το δίκτυο κινητής τηλεφωνίας και αισθητήρων κλπ.

2. Κάθε ”έξυπνη” συσκευή συνδέεται με αυτό το ”διαδίκτυο”

3. Όλες αυτές οι συσκευές επικοινωνούν μεταξύ τους.

Συνεπώς, προκύπτουν νέα προβλήματα ασφάλειας και προστασίας της ιδιωτικής ζωής. Μεγαλύτερη προσοχή πρέπει να δοθεί στα ερευνητικά θέματα σχετικά με την εμπιστευτικότητα, την αυθεντικότητα και την ακεραιότητα των δεδομένων των IoT.

Η ασφάλεια των πληροφοριών και του δικτύου πρέπει να είναι συνδυασμένη με έννοιες όπως είναι η αυθεντικοποίηση, η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Τα IoT έχουν εφαρμογή σε κρίσιμους τομείς της εθνικής οικονομίας, π.χ. στην ιατρική περίθαλψη και την υγειονομική περίθαλψη και στις ευφυείς μεταφορές, οπότε οι ανάγκες της ασφάλειας στο διαδίκτυο είναι υψηλότερες όσον αφορά τη διαθεσιμότητα και την αξιοπιστία.

CIA τριάδα

Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, γνωστή με το όνομα CIA *triad* (*Confidentiality, Integrity and Availability*), είναι ένα μοντέλο που έχει σχεδιαστεί για να καθοδηγεί πολιτικές για την ασφάλεια των πληροφοριών σε έναν οργανισμό. Το μοντέλο αναφέρεται επίσης μερικές φορές ως τριάδα AIC (διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα), προκειμένου να αποφευχθεί σύγχυση με την Κεντρική Υπηρεσία Πληροφοριών. Τα τρία αυτά στοιχεία της τριάδας θεωρούνται τα πιο κρίσιμα συστατικά για την εξασφάλιση της ασφάλειας οπότε είναι και το αντικείμενο της επιστήμης ασφάλειας υπολογιστών.

Γενικά, η εμπιστευτικότητα είναι ένα σύνολο κανόνων που περιορίζουν την πρόσβαση στις πληροφορίες μόνο για εξουσιοδοτημένα άτομα, η ακεραιότητα είναι η διασφάλιση ότι οι πληροφορίες είναι αξιόπιστες, ακριβείς και χωρίς να έχουν αλλοιωθεί και η διαθεσιμότητα αποτελεί εγγύηση για αξιόπιστη πρόσβαση των εξουσιοδοτημένων ατόμων στις πληροφορίες.

Εμπιστευτικότητα

Τα μέτρα που λαμβάνονται για την εξασφάλιση της εμπιστευτικότητας έχουν σχεδιαστεί για να αποτρέπουν την πρόσβαση σε ευαίσθητες πληροφορίες από μη εξουσιοδοτημένα άτομα, ενώ παράλληλα διασφαλίζουν ότι τα εξουσιοδοτημένα άτομα μπορούν πράγματι να τα αποκτήσουν. Η πρόσβαση πρέπει να περιορίζεται σε όσους έχουν εξουσιοδότηση για την προβολή των εν λόγω δεδομένων. Επίσης πολλές φορές τα δεδομένα αυτά ταξινομούνται ανάλογα με το μέγεθος και τον τύπο της ζημιάς που θα προκληθεί αν πέσουν σε λάθος άτομα. Με βάση αυτή την ταξινόμηση, μπορούν να εφαρμοστούν περισσότερο ή λιγότερο αυστηρά μέτρα.

Μερικές φορές, η διαφύλαξη του απορρήτου των δεδομένων μπορεί να απαιτεί ειδική εκπαίδευση που παρουσιάζει τους κινδύνους ασφαλείας που θα μπορούσαν να απειλήσουν αυτές τις πληροφορίες. Η εκπαίδευση μπορεί να βοηθήσει στην εξοικείωση των εξουσιοδοτημένων ατόμων με παράγοντες κινδύνου και τον τρόπο προστασίας τους. Σημαντική είναι η προβολή της σημασίας της ύπαρξης ισχυρών κωδικών πρόσβασης και της εφαρμογής των βέλτιστων πρακτικών που σχετίζονται με τον κωδικό πρόσβασης. Επίσης γνωρίζοντας για τις μεθόδους κοινωνικής μηχανικής (*social engineering*), είναι ένα βήμα για να αποφευχθούν επιθέσεις που στοχεύουν και εκμεταλλεύονται την καλή πρόθεση των χρηστών και μπορούν να οδηγήσουν σε καταστροφικά αποτελέσματα για τους ίδιους καθώς και για ολόκληρους οργανισμούς, εταιρείες και κυβερνήσεις.

Ένα καλό παράδειγμα μεθόδων που χρησιμοποιούνται για την εξασφάλιση της εμπιστευτικότητας είναι ο αριθμός λογαριασμού ή ο αριθμός δρομολόγησης κατά την ηλεκτρονική τραπεζική. Η κρυπτογράφηση δεδομένων είναι μια κοινή μέθοδος διασφάλισης της εμπιστευτικότητας. Τα αναγνωριστικά χρήστη και οι κωδικοί πρόσβασης αποτελούν μια τυπική διαδικασία. ο έλεγχος ταυτότητας δύο παραγόντων (2FA) έχει γίνει στις μέρες μας κανόνας. Άλλες επιλογές περιλαμβάνουν βιομετρικά στοιχεία επαλήθευσης και φυσικά κλειδιά ασφαλείας. Επιπλέον, οι χρήστες μπορούν να λάβουν προφυλάξεις για να ελαχιστοποιήσουν τον αριθμό των θέσεων όπου εμφανίζονται οι πληροφορίες και τον αριθμό των φορών που πραγματικά μεταδίδονται για να ολοκληρώσουν μια απαιτούμενη συναλλαγή. Επιπλέον μέτρα μπορούν να ληφθούν στην περίπτωση εξαιρετικά ευαίσθητων εγγράφων, όπως είναι η αποθήκευση μόνο σε υπολογιστές με κενό αέρα, συσκευές αποσύνδεσης ή, για εξαιρετικά ευαίσθητες πληροφορίες, μόνο σε έντυπη μορφή.

Ακεραιότητα

Η ακεραιότητα συνεπάγεται τη διατήρηση της συνέπειας, της ακρίβειας και της αξιοπιστίας των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους. Τα δεδομένα δεν πρέπει να μεταβάλλονται κατά τη διάρκεια ανταλλαγής τους και πρέπει να λαμβάνονται μέτρα ώστε τα δεδομένα να μην μπορούν να τροποποιηθούν από μη εξουσιοδοτημένα άτομα (παραβιάζοντας για παράδειγμα μαζί και την εμπιστευτικότητα). Αυτά τα μέτρα περιλαμβάνουν τα δικαιώματα αρχείων και τα στοιχεία ελέγχου πρόσβασης των χρηστών. Ο έλεγχος έκδοσης μπορεί να χρησιμοποιηθεί για την αποτροπή λανθασμένων αλλαγών ή τυχαίας διαγραφής από εξουσιοδοτημένους χρήστες. Επιπλέον, πρέπει να υπάρχουν ορισμένα μέσα για την ανίχνευση οποιωνδήποτε αλλαγών στα δεδομένα που ενδέχεται να προκύψουν ως αποτέλεσμα συμβάντων που δεν προκαλούνται από τον άνθρωπο, όπως από έναν ηλεκτρομαγνητικό παλμό (EMP) ή μια συντριβή του διακομιστή. Ορισμένα δεδομένα ενδέχεται να περιλαμβάνουν ποσά ελέγχου, ακόμη και κρυπτογραφικά αρχεία ελέγχου, για επαλήθευση της ακεραιότητας. Καλό είναι να υπάρχουν διαθέσιμα αντίγραφα ασφαλείας για την επαναφορά των επηρεαζόμενων δεδομένων στη σωστή τους κατάσταση.

Διαθεσιμότητα

Η διαθεσιμότητα εξασφαλίζεται καλύτερα με την αυστηρή διατήρηση όλων των πόρων, την εκτέλεση επισκευών υλικού αμέσως όταν χρειάζεται και τη διατήρηση ενός λειτουργικού περιβάλλοντος λειτουργικού συστήματος που λειτουργεί σωστά, χωρίς να γίνονται συγκρούσεις λογισμικού. Είναι επίσης σημαντικό να διατηρείται η τρέχουσα κατάσταση με όλες τις απαραίτητες αναβαθμίσεις του συστήματος. Η παροχή επαρκούς εύρους ζώνης επικοινωνίας και η πρόληψη της εμφάνισης σημείων συμφόρησης είναι εξίσου σημαντικές. Ο πλεονασμός, η αποτυχία, τα αρχεία RAID ακόμη και υψηλής διαθεσιμότητας μπορούν να μετριά-

σουν σοβαρές συνέπειες όταν προκύψουν ζητήματα υλικού. Η ταχεία και προσαρμοστική αποκατάσταση των καταστροφών είναι απαραίτητη για τα χειρότερα σενάρια. Η ικανότητα αυτή εξαρτάται από την ύπαρξη ενός ολοκληρωμένου σχεδίου αποκατάστασης καταστροφών. Η διασφάλιση κατά της απώλειας δεδομένων ή των διακοπών στις συνδέσεις πρέπει να προλαμβάνει απρόβλεπτα γεγονότα, όπως φυσικές καταστροφές και πυρκαγιές. Για να αποφευχθεί η απώλεια δεδομένων από τέτοια περιστατικά, ένα αντίγραφο ασφαλείας μπορεί να αποθηκευτεί σε μια γεωγραφικά απομονωμένη τοποθεσία, ίσως ακόμη και σε ένα πυρίμαχο, αδιάβροχο χρηματοκιβώτιο. Επιπλέον εξοπλισμός ή λογισμικό ασφαλείας, όπως είναι τα τείχη προστασίας και οι διακομιστές μεσολάβησης, μπορούν να προστατεύσουν ένα σύστημα από κακόβουλες ενέργειες όπως οι επιθέσεις DoS (*Denial of Service*) και οι εισβολές δικτύου.

Δοκιμή ασφάλειας ιστού είναι μια μέθοδος για την αξιολόγηση της ασφάλειας ενός συστήματος ή δικτύου υπολογιστών με τη μεθοδική επικύρωση και επαλήθευση της αποτελεσματικότητας των ελέγχων ασφάλειας εφαρμογών. Μια δοκιμή ασφαλείας εφαρμογών ιστού εστιάζει μόνο στην αξιολόγηση της ασφάλειας μιας εφαρμογής ιστού. Η διαδικασία περιλαμβάνει μια ενεργή ανάλυση της αίτησης για οποιεσδήποτε αδυναμίες, τεχνικές ατέλειες ή τρωτά σημεία. Τα τυχόν ζητήματα ασφάλειας που εντοπίζονται υποβάλλονται στον κάτοχο του συστήματος, μαζί με αξιολόγηση των επιπτώσεων, πρόταση για μετριασμό ή τεχνική λύση.

Ευπάθεια ονομάζεται ένα τρωτό σημείο, ένα ελάττωμα λογισμικού ή αδυναμία στο σχεδιασμό, την υλοποίηση, τη λειτουργία ή τη διαχείριση ενός συστήματος που θα μπορούσε να αξιοποιηθεί για να θέσει σε κίνδυνο τους στόχους ασφάλειας του συστήματος.

Απειλή θεωρείται ο,τιδήποτε (ένας κακόβουλος εξωτερικός επιτιθέμενος, ένας εσωτερικός χρήστης, μια αστάθεια του συστήματος κ.λπ.) που μπορεί να βλάψει τα περιουσιακά στοιχεία που ανήκουν σε μια εφαρμογή (πόροι αξίας, όπως τα δεδομένα σε μια βάση δεδομένων ή στο σύστημα αρχείων) εκμεταλλευόμενος ένα τρωτό σημείο.

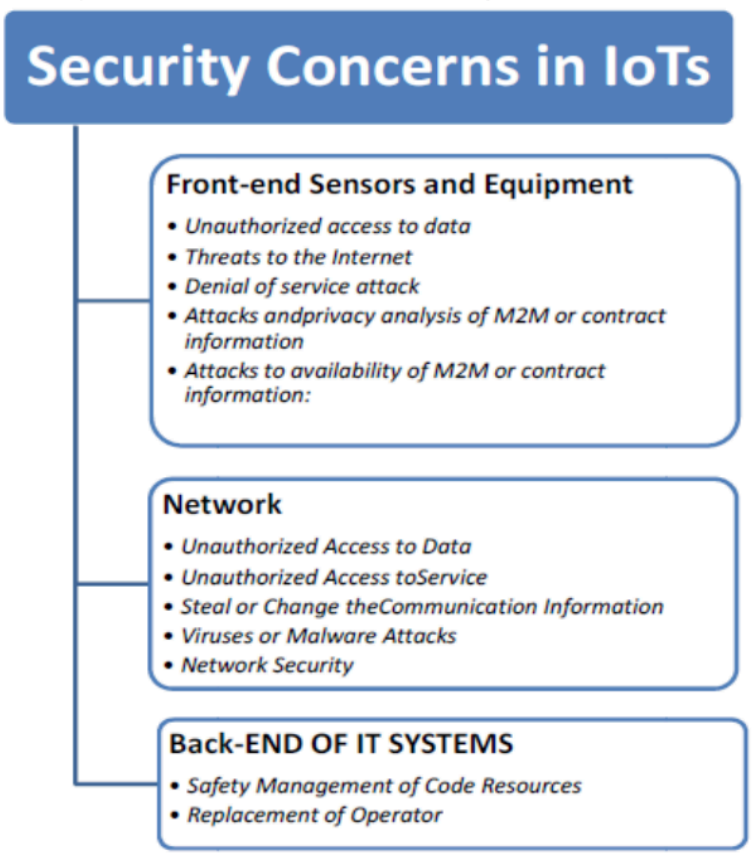
Τεστ ασφάλειας είναι γενικά μια σειρά δοκιμών που αποδεικνύουν ότι μια εφαρμογή πληροί τις απαιτήσεις ασφαλείας των ενδιαφερομένων.

Προβλήματα ασφάλειας

Παρόλο που η τεχνολογία IoT παρέχει βελτιώσεις στην αποδοτικότητα της κοινωνίας, δημιουργεί μια σειρά νέων προβλημάτων σχετικά με την παραβίαση της ιδιωτικής ζωής και την ασφάλεια των πληροφοριών [Jian]. Διάφορες απειλές παροουσιάζονται και στο σχήμα 2.2.

Αισθητήρες και εξοπλισμός

Οι αισθητήρες και ο εξοπλισμός γενικότερα λαμβάνουν δεδομένα και στη συνέχεια τα μεταδίδουν χρησιμοποιώντας μονάδες ή M2M συσκευές, επιτυγχάνοντας κατ ’αυτόν τον τρόπο υπηρεσίες δικτύωσης πολλαπλών αισθητήρων. Οι κόμβοι ως επί το πλείστον στερούνται παρακολούθησης. Ένας εισβολέας μπορεί εύκολα να έχει πρόσβαση σε αυτές τις συσκευές και να προκαλέσει ζημιές ή παράνομες ενέργειες σε αυτές. Πιθανές απειλές κατηγοροποιούνται σε μη εξουσιοδοτημένη πρόσβαση στα δεδομένα, απειλές κατά του Διαδικτύου και επιθέσεις άρνησης εξυπηρέτησης.



Σχήμα 2.2: Απειλές της ασφάλειας στα IoT

Δίκτυο

Το δίκτυο διαδραματίζει σημαντικό ρόλο παρέχοντας περισσότερο ολοκληρωμένη ικανότητα διασύνδεσης, αποτελεσματικότητα και αυθεντικότητα της σύνδεσης, καθώς και την αυθεντική ποιότητα των υπηρεσιών σε διαδικτυακές πύλες. Δεδομένου ότι ένας μεγάλος αριθμός συσκευών στέλνουν δεδομένα, εγκυμονούν οι κίνδυνοι συμφόρησης του δικτύου και επιθέσεων άρνησης εξυπηρέτησης (DoS).

Back-end συστήματα

Τα συστήματα τεχνολογίας *back-end* αποτελούν την πύλη, το μεσαίο λογισμικό στα οποία υπάρχουν υψηλές απαιτήσεις ασφάλειας. Η συγκέντρωση, εξέταση δεδομένων των αισθητήρων σε πραγματικό χρόνο ή ψευδο-πραγματικό χρόνο θέτει πολλούς κινδύνους. Η ασφάλεια του συστήματος διασύνδεσης IoT έχει ως επίκεντρο την προστασία προσωπικών δεδομένων, τους ελέγχους πρόσβασης, τον έλεγχο ταυτότητας χρηστών, την ασφάλεια του στρώματος επικοινωνίας, την ακεραιότητα των δεδομένων και την εμπιστευτικότητα και διαθεσιμότητα αυτών ανά πάσα στιγμή.

Προβληματισμοί για την προστασία της ιδιωτικότητας σε IoT

Το γλωσσάριο ασφάλειας του Διαδικτύου (*Internet*) [Shir00] ορίζει την ιδιωτικότητα ως ”το δικαίωμα μιας οντότητας (συνήθως ενός προσώπου), η οποία ενεργεί για δικό της λογαριασμό, να καθορίσει το βαθμό στον οποίο θα αλληλεπιδράσει με το περιβάλλον, συμπερι-

λαμβανομένου του βαθμού στον οποίο η οντότητα είναι πρόθυμη να μοιραστεί πληροφορίες για τον εαυτό του με άλλους".

Συνήθως στα IoT, οι συνδεδεμένες συκευές συλλέγουν δεδομένα από το περιβάλλον, στη συνέχεια μεταδίδονται οι συγκεντρωμένες πληροφορίες και συγκεκριμένα συμβάντα σε έναν διακομιστή που εκτελεί την εφαρμογή. Αυτό γίνεται με κινητή ή/και σταθερή επικοινωνία. Το απόρρητο των δεδομένων θα πρέπει να προστατεύεται στις συσκευές, κατά τη διάρκεια αποθήκευσης, της επικοινωνίας και της επεξεργασίας ώστε να μην διαρρεύσουν ευαίσθητες πληροφορίες [Chen12]. Η εξασφάλιση του ιδιωτικού απορρήτου των χρηστών και των δεδομένων τους έχει προσδιοριστεί ως μια από τις προκλήσεις που πρέπει να αντιμετωπιστούν στην τεχνολογία των IoT.

Απόρρητο δεδομένων στη συσκευή

Οι ευαίσθητες πληροφορίες ενδέχεται να διαρρεύσουν στην περίπτωση μη εξουσιοδοτημένου χειρισμού υλικού ή λογισμικού σε αυτές τις συσκευές. Για παράδειγμα, ένας εισβολέας μπορεί να "επαναπρογραμματίσει" μια κάμερα επιτήρησης, ώστε να μπορεί να αποστέλλει δεδομένα όχι μόνο στον νόμιμο διακομιστή, αλλά και στον ίδιο. Για να διασφαλιστεί η ασφάλεια των IoT χρειάζονται αξιόπιστες τεχνολογίες υπολογιστών, συμπεριλαμβανομένων των μηχανισμών επικύρωσης της ακεραιότητας της συσκευής, συσκευές ανθεκτικές σε παραβιάσεις και αξιόπιστα περιβάλλοντα εκτέλεσης κώδικα.

Επίσης πρέπει να προστατεύεται η τοποθεσία του κατόχου μιας συσκευής, να μην είναι αναγνωρίσιμη η φύση της συσκευής και τα επί μέρους στοιχεία της καθώς και σε περίπτωση κλοπής ή απώλειας της συσκευής, τα προσωπικά δεδομένα να μην μπορούν να υποκλαπούν. Το απόρρητο στο WSN (*Wireless Sensor Network*) επιτυγχάνεται με τη χρήση του αλγορίθμου *Multi-Routing Random Walk* [Zhou12] στους ασύρματους αισθητήρες.

Απόρρητο δεδομένων κατά την επικοινωνία

Για να διασφαλιστεί η εμπιστευτικότητα των δεδομένων κατά τη διάρκεια της μετάδοσης τους, η πιο κοινή πρακτική είναι η τεχνική της κρυπτογράφησης. Μερικές φορές προσθέτονται δεδομένα σε πακέτα που παρέχουν ως τρόπος ανίχνευσης, π.χ. αριθμός ακολουθίας, *IPsec- SecurityParameterIndex*, κ.λπ. Αυτά τα δεδομένα μπορεί να εκμεταλλεύονται για τον συνδυασμό των πακέτων με την ανάλυση της ίδιας κυκλοφορίας ροής. Χρήση ασφαλών πρωτοκόλλων επικοινωνίας είναι η κατάλληλη λύση[Gian13]. Κατά τη διάρκεια της επικοινωνίας μπορούν να αντικατασταθούν τα ψευδώνυμα σε περίπτωση που δεν είναι εφικτή η ταυτότητα της συσκευής ή χρηστών, προκειμένου να μειώνονται οι ευπάθειες. Ένα από τα μακροχρόνια παραδείγματα είναι η Προσωρινή Ταυτότητα Κινητού Συνδρομητή (TMSI). Οι συσκευές θα πρέπει να επικοινωνούν εάν και μόνο όταν είναι ανάγκη, για να αποφεύγεται η αποκάλυψη απορρήτου που προκαλείται από επικοινωνία. Σε επικοινωνίες τύπου μηχανής 3GPP, προκειμένου να αποφευχθεί η περιττή συλλογή πληροφοριών θέσης από το δίκτυο μετά από μια ορισμένη περίοδο αδράνειας οι συσκευές θα πρέπει να αποσυνδέονται από το δίκτυο.

Απορρήτο δεδομένων κατά την αποθήκευση

Για την προστασία της ιδιωτικότητας των πληροφοριών κατά την αποθήκευση τους, πρέπει να ληφθούν υπόψη:

- Πρέπει να υπάρχει μόνο η ελάχιστη δυνατή ποσότητα πληροφοριών που απαιτείται να αποθηκευτούν.

- Σε περίπτωση υποχρεωτικής κράτησης, διατηρούνται μόνο προσωπικά δεδομένα.
- Οι πληροφορίες εξάγονται μόνο όταν είναι ανάγκη.

Για να αποκρύπτεται η πραγματική ταυτότητα που συνδέεται με τα αποθηκευμένα δεδομένα πρέπει να χρησιμοποιείται ψευδωνυμοποίηση και ανωνυμοποίηση. Χωρίς να αποκαλύπτονται συγκεκριμένες εγγραφές, μια βάση δεδομένων μπορεί να επιτρέψει την πρόσβαση μόνο σε στατιστικά στοιχεία (άθροισμα, μέσος όρος, αριθμός κλπ.). Μια καλή τεχνική είναι η *differential privacy* [Hall13].

Απορρήτο δεδομένων κατά την επεξεργασία

Πρώτον, τα προσωπικά δεδομένα πρέπει να αντιμετωπίζονται με τρόπο που θα πρέπει να είναι ανάλογος με τον επιδιωκόμενο σκοπό. Δεύτερον, χωρίς ρητή αποδοχή και γνώση του ιδιοκτήτη δεδομένων, αυτά δεν πρέπει να γνωστοποιούνται ή να δίνονται σε τρίτους. Μελετώντας τα παραπάνω δύο σημεία, *Digital Rights Management* (DRM) συστήματα [Liu14] είναι τα πλέον κατάλληλα ώστε να ελέγχουν την κατανάλωση των εμπορικών μέσων ενημέρωσης και να βοηθούν κατά της παράνομης αναδιανομής δεδομένων. Ένα DRM σύστημα απαιτεί αξιόπιστες και ασφαλείς συσκευές να λειτουργούν αποτελεσματικά. Η άδεια του χρήστη και η επίγνωσή του είναι απαραίτητες για τη διανομή προσωπικών δεδομένων. Η ειδοποίηση του χρήστη βοηθάει στην αποφυγή παραβίασης της ιδιωτικότητας.

2.2 Προβλήματα ασφάλειας των IoMT

Κοινές αδυναμίες

Είναι σαφές ότι υπάρχει ένα πρόβλημα σχετικά με την ασφάλεια των υπολογιστικών συστημάτων IoMT, αλλά για να κατανοηθούν καλύτερα τα υποκείμενα ζητήματα είναι σημαντικό να δει κανείς ακριβώς τι είναι αυτά που οι ερευνητές της ασφάλειας βρίσκουν όταν εξετάζουν τα συστήματα για αδυναμίες. Μερικές φορές να είναι δύσκολο να υπάρχει σαφή εικόνα των ζητημάτων λόγω του βάθους και του εύρους των ελαττωμάτων που βρίσκονται απέναντι σε διαφορετικές συσκευές, αλλά γενικά συμπίπτουν όλα σε κοινές κατηγορίες. Αυτές συμπεριλαμβάνουν σφάλματα πηγαίου κώδικα, ελαττώματα στην υλοποίηση κρυπτογράφησης, ελλείψεις στο σχεδιασμό λογισμικού, απουσία μηχανισμών προστασίας από παραβιάσεις, ευπάθειες σε βιβλιοθήκες και προγράμματα άλλων που χρησιμοποιούνται ή ενσωματώνονται καθώς και λανθασμένες ρυθμίσεις δικτύου.

Σφάλματα πηγαίου κώδικα

Τέτοιες αδυναμίες προκύπτουν όταν υπάρχουν λάθη στον πηγαίο κώδικα ή στο *firmware* ενός υπολογιστικού συστήματος που μπορούν να επιτρέψουν σε επιτιθέμενους να δημιουργήσουν καταστάσεις σφάλματος που θα τους βοηθούν σε επιτυχείς επιθέσεις.

Για παράδειγμα, μια ευπάθεια που δημιουργεί συχνά δυνατότητα επιθέσεων απομακρυσμένης εκτέλεσης κώδικα είναι η ευπάθεια *buffer overflow*. Αυτό του είδους ελαττώματα τα συναντάμε όταν ο υποκείμενος κώδικας επιτρέπει το λογισμικό να προσπαθήσει να αποθηκεύσει περισσότερα δεδομένα από αυτά που γίνεται, σε προσωρινή περιοχή αποθήκευσης μνήμης *buffer*, γεγονός που δημιουργεί μια κατάσταση όπου η επιπλέον πληροφορία ξεχειλίζει σε άλλα προσωρινά δεδομένα, καταστρέφοντας αποτελεσματικά ή αντικαθιστώντας έγκυρα δεδομένα του *buffer*.

Ένας εισβολέας μπορεί να επωφεληθεί από αυτή την αδυναμία, και συμπεριλαμβάνοντας κακόβουλο κώδικα μέσα σε αυτά τα ”έξτρα” δεδομένα, να αναγκάσει το σύστημα να εκτελέσει ένα εντελώς νέο σύνολο εντολών. Τα τρωτά σημεία υπερχείλισης του *buffer* είναι μόνο ένα από τα πολλά είδη ελαττωμάτων αυτής της κατηγορίας που εμφανίζονται συχνά σε λογισμικό ιατρικών συσκευών. Άλλα κοινά ελαττώματα περιλαμβάνουν τρωτά σημεία όπου υπάρχει SQL *injection* και επιτρέπουν στους επιτιθέμενους, πληκτρολογώντας αποσπάσματα κώδικα σε πεδία εισαγωγής, να σπάσουν το σύστημα με τρόπο που προκαλείται δυσλειτουργία και διαρροή δεδομένων. Άλλα προβλήματα ασφάλειας μπορούν να ξεκινήσουν από τη χρήση αδύναμων κρυπτογραφικών αλγορίθμων ή από ακατάλληλους τρόπους επικύρωσης των πιστοποιητικών και τέλος από XSS(*cross site scripting*) προβλήματα μεταξύ ιστότοπων που δίνουν τη δυνατότητα εισαγωγής μικρών κομματιών κώδικα μέσα στην εφαρμογή με σκοπό την παράκαμψη στοιχείων ελέγχου ασφαλείας.

Απαιτήσεις σχεδιασμού λογισμικού

Οι αδυναμίες αυτής της κατηγορίας ξεκινάνε από λανθασμένες ρυθμίσεις λογισμικού και από λογισμικό που δεν σχεδιάστηκε σωστά. Ένα πρωταρχικό παράδειγμα αυτού είναι η κακή εφαρμογή της διαδικασίας αυθεντικοποίησης, ελέγχου ταυτότητας και απαίτησης κωδικού πρόσβασης.

Για παράδειγμα, ανάλυση που έγινε στο λογισμικό MDLink που σχεδιάσθηκε για αυτοματοποιημένους εξωτερικούς απινιδωτές κατέληξε ότι η εφαρμογή αποθήκευε με τέτοιο τρόπο τα αρχεία κωδικών πρόσβασης στο τοπικό σκληρό δίσκο, έτσι ώστε να είναι απλό να διαγραφτούν οι κωδικοί πρόσβασης όλων των χρηστών με αποτέλεσμα να παρακάμπτεται εξ ολοκλήρου η προστασία τους.[Hann11]

Η ερευνητική κοινότητα ανησυχεί ιδιαίτερα, γιατί συχνά σε πολλές ιατρικές συσκευές, βρίσκονται ενσωματωμένοι στον κώδικα του λογισμικού, κάποιοι κωδικοί πρόσβασης που αποτελούν «πίσω πόρτες» (*backdoors*) για τους κατασκευαστές ώστε να υπάρχει η δυνατότητα επαναφοράς σε κατάσταση συντήρησης και ρυθμίσεων (*administrative situations*). Σε πολλές περιπτώσεις, το λογισμικό έχει προγραμματιστεί κατά τέτοιο τρόπο ώστε αυτά τα διαπιστευτήρια δηλαδή οι κωδικοί να μην μπορούν ποτέ να αλλάξουν ή να καταργηθούν. Επιπρόσθετα, πληροφορίες σχετικά με αυτά τα διαπιστευτήρια μπορούν να βρεθούν εύκολα μέσα σε δημόσια διαθέσιμα λειτουργικά εγχειρίδια σχετικά με τις συσκευές. Έτσι το μόνο που θα χρειαζόταν για έναν εισβολέα είναι να πάρει στα χέρια του ένα τέτοιο εγχειρίδιο και να βρει τον τρόπο να προσπεράσει κάθε είδους ελέγχο πρόσβασης για τη συσκευή. Είναι εξαιρετικά διαδεδομένη πρακτική στον κόσμο των ιατρικών συσκευών. Για παράδειγμα, οι ερευνητές Rios και Terry McCorckle βρήκαν το 2013 ένα σύνολο 300 ιατρικών συσκευών σε 40 προμηθευτές που πλήττονταν από αυτήν την ευπάθεια, επιτρέποντας σε πιθανούς επιτιθέμενους έναν γρήγορο τρόπο για να αλλάξουν ρυθμίσεις καθώς και όλο το λογισμικό (*firmware*) σε αυτές τις συσκευές. Τέτοιες συσκευές ήταν χειρουργικές και αναισθησιολογικές συσκευές, ανεμιστήρες, αντλίες έγχυσης φαρμάκων, εξωτερικοί απινιδωτές, οργάνα παρακολούθησης ασθενών και εργαστηρίου, καθώς και εξοπλισμός αναλύσεων.[Team13]

Παρομοίως, προεπιλεγμένοι και αδύναμοι κωδικοί πρόσβασης που απαιτούνται για ρυθμίσεις λογισμικού (*firmware*) και δικτύου καθιστούν την παράκαμψη ελέγχων πρόσβασης όπου απαιτούνται. Ο Scott Erven, ερευνητής για θέματα ασφάλειας, γνωστός για τις ανακαλύψεις του για ευπάθειες σε ιατροτεχνολογικά προϊόντα, σχετίζεται με ένα τέτοιο παράδειγμα από μια παρουσίαση σε ορισμένες εξαντλητικές μελέτες που έκανε σε ιατρικά περιουσιακά στοιχεία στην Essentia Health, μια αλυσίδα ιατρικών εγκαταστάσεων, όταν εργάστηκε εκεί ως επικεφαλής ασφάλειας των πληροφοριών. Αναφέρει ότι βρήκαν δύο προμηθευτές απινι-

δωτών που χρησιμοποιούν μια στοίβα *Bluetooth* για τη σύνταξη ρυθμίσεων και τη διεξαγωγή δοκιμών σοκ κατά τον ασθενή μετά την εμφύτευση ή τη χειρουργική επέμβαση. Εντοπίστηκε ότι υπήρχαν προεπιλεγμένοι και αδύναμοι κωδικοί πρόσβασης στο *Bluetooth stack*, ώστε να είναι δυνατή η σύνδεση με τις συσκευές. «Είναι ένας απλός κωδικός πρόσβασης όπως ένα *iPhone PIN* που θα μπορούσε εύκολα κάποιος να μαντέψει» αναφέρει. [K]

Ένα άλλο κοινό και δυνητικά θανατηφόρο πρόβλημα στο σχεδιασμό λογισμικού είναι η απουσία κρυπτογράφησης στα δεδομένα όταν αυτά βρίσκονται σε ηρεμία εντός χώρου αποθήκευσης ή σε διαμετακόμιση μέσω πρωτοκόλλων επικοινωνίας όπως οι ασύρματες συνδέσεις. Στην τεκμηριωμένη ακαδημαϊκή έρευνα από τον Kevin Fu και την ομάδα του των συνεργαζόμενων ερευνητών το 2008-μια μελέτη που ήταν πρόδρομος για την επίδειξη παραβίασης της ασφάλειας βηματοδοτών του Barnaby Jack - υπογράμμισε τους ακραίους κινδύνους που δημιουργούν οι βηματοδότες που μεταδίδουν μη κρυπτογραφημένα δεδομένα με ασύρματα σήματα[Halp08].

Αυτή είναι μια όλο και πιο διαδεδομένη τάση που αφορά ιατρικές συσκευές καθώς έχουμε αύξηση των συσκευών που έχουν δυνατότητα ασύρματης διασύνδεσης. ”Οι ιατρικές συσκευές έχουν υιοθετήσει την ασύρματη τεχνολογία καθώς διευκολύνει την επικοινωνία με τις συσκευές προγραμματισμού που περνούν εντολές και ρυθμίσεις επεξεργασίας και την ανάκτηση δεδομένων των αισθητήρων”. ”Ενώ η ασύρματη επικοινωνία καθιστά την αλληλεπίδραση με ιατρικές συσκευές ευκολότερη και ασφαλέστερη για τους γιατρούς (για τις εμφυτευμένες συσκευές, οι βελόνες έπρεπε προηγουμένως να εισαχθούν σε ασθενείς για να μεταφέρουν σήματα), εισάγει σημαντικά προβλήματα στην ασφάλεια”, έγραψε ο Favyen Bastani και ο Tiffany Tang από το MIT. ”Η πλειοψηφία των ιατρικών συσκευών έχουν έλλειψη υλοποίησης κρυπτογράφησης και διαθέτουν ελάχιστους ή και καθόλου ελέγχους αυθεντικοποίησης για τις εντολές που λαμβάνουν, πράγμα που σημαίνει ότι οι πιθανοί επιτιθέμενοι μπορούν να κλέβουν εξ αποστάσεως ευαίσθητες πληροφορίες υγείας από τις συσκευές ή ακόμα και να ελέγχουν τη συσκευή δίνοντας ακόμα και θανατηφόρες εντολές. ”[Bast14]

Η πιο πρόσφατη έκθεση της MedSec σχετικά με την ευπάθεια του St. Jude δεν είχε πολλές τεχνικές λεπτομέρειες, αλλά αναφέρθηκε συγκεκριμένα ότι ένα από τα μεγάλα τρωτά σημεία που βρέθηκε ήταν στη χρήση πρωτόκολλων χωρίς έλεγχο ταυτότητας και χωρίς κρυπτογράφηση ακόμη και 8 χρόνια μετά την έρευνα του Fu και 4 χρόνια από τον Jack, οι βηματοδότες συνεχίζουν να βάζουν τους ασθενείς σε κίνδυνο εξ’ αιτίας της μη κρυπτογραφημένης ασύρματης επικοινωνίας.

Απουσία αποδείξεων για τις περιπτώσεις αλλαγών των δεδομένων (*tamper proofing*)

Η έκθεση MedSec έφερε στο φως ένα ακόμη υποσύνολο πολύ κοινών ελλατωμάτων σχεδίασης και εγγραφής κώδικα. Συγκεκριμένα, έγινε αναφορά στην απουσία μέτρων προστασίας από παραβίασεις σε όλο το υλικό (*hardware*), το λογισμικό (*firmware*) και τη στοίβα λογισμικού (*software stack*) μιας συσκευής. Η προστασία των συσκευών από αλλαγές, παραβιάσεις και από απλή αντίστροφη μηχανική ανάλυση (*reverse engineering*) είναι απαραίτητες με σκοπό να δυσκολέψουν πιθανούς επιτιθέμενους να καταφέρουν πλήρη έλεγχο της ιατρικής συσκευής. Οι κατασκευαστές πρέπει συνήθως να ακολουθούν μια σειρά από τυπικά βήματα για την αποφυγή παραβιάσεων των συσκευών, αυτά είναι:

- Προστασία της ταυτότητας του υλικού, όπως με την ανακάτωση δεδομένων και πληροφοριών (*obfuscation*) με τέτοιο τρόπο ώστε οι πιθανοί επιτιθέμενοι να μην μπορούν να βρουν χρήσιμα στοιχεία όταν ερευνούν συσκευές.

- Κρυπτογράφηση του δυαδικού ψηφιακού κώδικα ιδιοκτησίας και των εφαρμογών έτσι

ώστε να μην είναι εύκολο να εξαχθούν από έναν εισβολέα που επιδιώκει την αντίστροφη μηχανική ανάλυση (*reverse engineering*) για εύρεση εκμεταλλεύσιμων τρωτών σημείων στον κώδικα.

- Απενεργοποίηση των μηχανισμών εντοπισμού σφαλμάτων (*debugging*) και των μηχανισμών ανάπτυξης (*development*) σε συσκευές που βγαίνουν στην παραγωγή έτσι ώστε να μην είναι δυνατές αυθαίρετες αλλαγές στον κώδικα για τους πιθανούς επιτιθέμενους μόλις οι συσκευές κυκλοφορήσουν στην αγορά

- Προστασία των API (διεπαφών προγραμματισμού εφαρμογών) που συνδέουν τις συσκευές τελικού σημείου με το *back-end* (διακομιστές) ώστε να μην είναι δυνατή η εκμετάλλευση τους για πρόσβαση στον πηγαίο κώδικα.

Σύμφωνα με την MedSec, στην περίπτωση των Merlin @ home συσκευών που εξετάστηκαν, καμία από αυτές τις πρακτικές δεν ήταν σε ισχύ, έτσι ώστε αυτές οι συσκευές εγκυμονούσαν τεράστιους κινδύνους για την ασφάλεια με τρόπους που αψηφούν την λογική.

Ευπάθειες από εφαρμογές τρίτων κατασκευαστών (*third party vulnerabilities*)

Οι ευπάθειες δεν προκύπτουν μόνο από τα λάθη στο λογισμικό των κατασκευαστών αλλά και από προβλήματα ασφάλειας σε λογισμικό τρίτων κατασκευαστών που ενσωματώνεται στο σύνολο του πληροφοριακού συστήματος. Τέτοιες εφαρμογές μπορεί να είναι ολοκληρωμένες web εφαρμογές, υλικο λογισμικό (*firmware*) και πλατφόρμες λειτουργικών συστημάτων. Για παράδειγμα, κατασκευάζονται πολλές ιατρικές συσκευές νοσοκομείων με ειδικής κατασκευής λογισμικά που τρέχουν όμως σε εμπορικούς ηλεκτρονικούς υπολογιστές με *Windows*. Συχνά υποκείμενες αδυναμίες που εντοπίζονται στο λειτουργικό σύστημα των *Windows* μπορούν να προκαλέσουν αιφνίδια ελαττώματα σε ολόκληρη τη συσκευή που μπορούν να θέσουν την ασφάλεια των ασθενών και την ιδιωτικότητά τους σε κίνδυνο. Και, δυστυχώς, πολλές από τις συσκευές βασίζονται σε παλαιότερες, μη παρωχημένες και ευάλωτες εκδόσεις *Windows* που δεν υποστηρίζονται από ενημερώσεις και δεν μπορούν να προστατευθούν εύκολα από το χρήστη, διαταράσσοντας τη λειτουργικότητα της ίδιας της συσκευής. Ο Aaron Miri, διευθυντής του τμήματος πληροφοριών ενός ιατρικού κέντρου στο Ντάλας, πρόσφατα ανέφερε ένα συμβάν για να εξηγήσει πώς αυτό μπορεί να θέσει τους διαχειριστές των εγκαταστάσεων σε μια δέσμευση. Ανέφερε σε συνέντευξη του τον Απρίλιο του 2016 στο MedPage ότι είχαν λάβει τρία ολοκαίνουργια μηχανήματα για χορήγηση φαρμάκων. Τα τοποθέτησαν σε μια ολοκαίνουργια μονάδα που μόλις είχε φτιαχτεί, τα ενεργοποιήσαν και τα συνέδεσαν στο δίκτυο. Αμέσως τα συστήματα άρχισαν να υπολειτουργούν, καθώς ήταν σίγουρος ότι ήρθαν μολυσμένα με κακόβουλο λογισμικό από το εργοστάσιο επειδή το υποκείμενο τους λειτουργικό σύστημα ήταν *Windows XP*. Σε μια παρουσίαση που εξέτασε το δίκτυο μιας πολύ μεγάλης αμερικανικής οργάνωσης υγειονομικής περίθαλψης με πάνω από 12000 εργαζομένους, ο ερευνητής ασφάλειας Mark Collao συνεργάστηκε με τον Erven. Ο Collao σημείωσε ότι η εξάρτηση από τα *Windows XP*- λειτουργικό που δεν υποστηρίζεται πλέον από τη *Microsoft*- είναι πολύ συχνό φαινόμενο. ”Οι ιατρικές συσκευές εκτελούν τα πάντα σε *Windows XP* και πιθανώς δεν έχουν *antivirus* επειδή είναι κρίσιμα συστήματα ”, δήλωσε ο Collao. Ύστερα από την έρευνα βρήκαν λοιπόν, ότι η οργάνωση είχε περισσότερα από τα 68.000 ιατρικά συστήματα ευάλωτα σε επιθέσεις μέσω διαδικτύου λόγω πολλών διαφορετικών τρωτών σημείων. Μεταξύ των συσκευών αυτών περιλαμβάνονταν 21 συσκευές αναισθησίας, 488 καρδιολογίας, 67 πυρηνικής ιατρικής και 133 συστήματα έγχυσης, καθώς και 31 βηματοδότες, 97 σαρωτές μαγνητικής τομογραφίας και 323 μηχανές αρχειοθέτησης εικόνων και επικοινωνιών.[D15a]

Μη ασφαλείς ρυθμίσεις δικτύου και επικοινωνιών

Οι συσκευές που χρειάζονται παλιές εκδόσεις των *Windows* δεν υποστηρίζονται πλέον γιατί όχι μόνο η ίδια η συσκευή είναι ευάλωτη, αλλά συνήθως, αν χρησιμεύει ως σημείο στήριξης στο δίκτυο, καθιστά εύκολο για τους επιτιθέμενους να στοχεύουν και άλλες συσκευές.

Σε μια έκθεση του Ιουλίου 2015, οι ερευνητές της ασφάλειας ανέφεραν λεπτομερώς τον τρόπο με τον οποίο οι επιτιθέμενοι στοχεύουν τις ιατρικές συσκευές που βασίζονται στα *Windows* για να δημιουργήσουν πίσω πόρτες (*bachdoors*) που θα λειτουργούν ως ”βασικά σημεία εισόδου για τους επιτιθέμενους στα δίκτυα υγειονομικής περίθαλψης.”[D15b]

Αυτή η εξέλιξη συμβαδίζει με την έρευνα των Collao και Erven, η οποία εκτός από την ανάλυση που προαναφέρθηκε δημιούργησε επίσης ένα *honeypot* που μιμούνταν την πραγματική MRI και απινιδωτές που εκτίθενται στο Διαδίκτυο για να παρακολουθήσουν τι μπορεί να συμβεί. Σε χρονικό διάστημα 6 μηνών, διαπίστωσαν ότι οι συσκευές προσέλκυσαν πάνω από 55.000 επιτυχείς μη εξουσιοδοτημένες συνδέσεις και απορρόφησαν περίπου 300 φορτία κακόβουλου λογισμικού (*malware payloads*). Αυτό αποδεικνύει την πραγματική απειλή για αυτές τις συσκευές καθώς οι επιτιθέμενοι ήδη έχουν στοχεύσει τις συσκευές. Ο Collao δήλωσε ότι ”αυτές οι συσκευές είναι μέρος πλεόν όλο και περισσότερων νοσοκομείων καθώς υπάρχει δυνατότητα διασύνδεσης Wi-fi”.

2.3 Πρότυπα και βέλτιστες πρακτικές ασφάλειας για IoMT

Αυτή η ενότητα παρέχει μια επισκόπηση των προτύπων που ισχύουν για την υγειονομική περίθαλψη, και περιγράφει τις επιπτώσεις αυτών των προτύπων σχετικά με το σχεδιασμό συστημάτων. Συμπεριλαμβάνονται πρότυπα σχετικά με προϊόντα λογισμικού που πρόκειται να χρησιμοποιηθούν στην υγειονομική περίθαλψη, από χρήστες όπως οι νοσηλευτές, οι γιατροί, οι ασθενείς και οι φροντιστές. Τα παρουσιαζόμενα πρότυπα ισχύουν σε υποδομές, οι οποίες γενικά αναφέρονται ως ”δίκτυα ιατρικών δεδομένων”. Εξαιρέθηκαν πρότυπα που σχετίζονται μόνο με το σχεδιασμό και κατασκευή φυσικού εξοπλισμού. Επίσης εξαιρέθηκαν εθνικοί κανονισμοί για τα πρότυπα ανάπτυξης.

Επισκόπηση των προτύπων

Η ανάλυση των προτύπων δείχνει τέσσερις ομάδες τυποποιημένων πτυχών: ανάπτυξη ενός προϊόντος λογισμικού, διαλειτουργικότητα του προϊόντος με άλλα, η χρήση του από ανθρώπους και η ανθεκτικότητα και προστασία από βλάβες. Αυτές οι τέσσερις ομάδες ρυθμιζόμενων πτυχών εξασφαλίζουν επαρκή ποιότητα για το λογισμικό που χρησιμοποιείται σε κρίσιμα περιβάλλοντα.

Ανάπτυξη λογισμικού

Το IEC 62304 ρυθμίζει την ανάπτυξη λογισμικού για ιατρικές συσκευές. Προσθέτει τις πτυχές διαχείρισης του κινδύνου και της ποιότητας στις καθιερωμένες βέλτιστες πρακτικές που προτείνονται από πλαίσια (*frameworks*) όπως το CMMI και το ITIL και μοντέλα κύκλου ζωής ανάπτυξης όπως ο καταρράκτης (*waterfall* και το *agile*. Επίσης, περιορίζει την ανάπτυξη, τη συντήρηση, τη διαχείριση κινδύνου, τη διαχείριση των ρυθμίσεων και τις πρακτικές επίλυσης προβλημάτων βάσει αξιολόγησης της κρισιμότητας ασφάλειας του λογισμικού. Η συμμόρφωση με το πρότυπο IEC 62304 συμβάλλει στη συμμόρφωση με τον FDA.

Το πρότυπο ISO 13407 καθορίζει τις διαδικασίες σχεδιασμού διαδραστικών συστήματα από την άποψη της χρηστικότητας, και το ISO / TR 16982 καθορίζει τη χρήση μεθόδων μηχανικής χρηστικότητας ως μέρος τέτοιων αναπτυξιακών διαδικασιών. Το IEC 62366 ορίζει την αντίστοιχη διαδικασία που πρέπει να ακολουθηθεί για τις μηχανικές ιατρικές συσκευές. Περαιτέρω οδηγίες για την ανάπτυξη λογισμικού μπορούν να ληφθούν από άλλα πρότυπα IEEE και ISO / IEC, τα οποία ισχύουν για το λογισμικό γενικά και όχι για την υγειονομική περίθαλψη. Τέτοια πρότυπα είναι το IEEE Standard Glossary of Software Engineering Terminology 610.12 και το ISO / IEC 25010 για τις απαιτήσεις και την αξιολόγηση της ποιότητας συστημάτων και λογισμικού.

Διαλειτουργικότητα

Ένα προϊόν λογισμικού ενσωματωμένο σε ένα μια λύση πρέπει να μπορεί να επικοινωνεί με άλλα προϊόντα λογισμικού και ιατρικές συσκευές. Για να υπάρχει ανεξαρτησία από το κατασκευαστή αυτών των προϊόντων, το ISO / IEEE 11073 καθορίζει τον τρόπο που τα προϊόντα αλληλεπιδρούν. Πρόκειται για μια οικογένεια προτύπων που ορίζει τα πεδία εφαρμογής, όρους, μοντέλα πληροφοριών, τύπους συσκευών, εφαρμογές, τρόπους μεταφοράς δεδομένων και κωδικοποίησης τους. Το ETSI ES 202 975, έστω και αν δεν αφορά συγκεκριμένα τον τομέα της υγείας, περιορίζει περαιτέρω την επικοινωνία μέσω κειμένου, ομιλίας και βίντεο στα πλαίσια ενός δικτύου.

Οι πληροφορίες που έχουν ιδιαίτερη σημασία στον τομέα της περίθαλψης είναι το προφίλ του ασθενούς. Το CEN / TC 251 έχει αναπτύξει μια συλλογή προτύπων για την πληροφορική στον τομέα της υγείας για τη διαλειτουργικότητα. Το CEN / ISO 13606 έχει ιδιαίτερη σημασία, αφού διευκρινίζει τον τρόπο ηλεκτρονικών καταγραφών της υγείας. Διαμορφώνει ένα μοντέλο που επιτρέπει τη διαμόρφωση και τη συσσωμάτωση δηλώσεων σχετικά με τα αρχεία υγείας, ένα αρχέτυπο μοντέλο που καθορίζει τις έννοιες της υγείας και το νόημά τους, και επιτρέπει τον καθορισμό των κανόνων προστασίας δεδομένων που διέπουν την πρόσβαση στα δεδομένα υγείας. Το ISO / TS 19218 ορίζει πρακτικές κωδικοποίησης για την περιγραφή των ανεπιθύμητων συμβάντων που σχετίζονται με ιατρικές συσκευές. Το ISO 15225 ορίζει την ονοματολογία και δομή δεδομένων μιας ιατρικής συσκευής της ονοματολογίας για την ανταλλαγή δεδομένων που χρησιμοποιούνται από ρυθμιστικές αρχές.

Ευχρηστία

Πολλές εργασίες επένδυσαν στην τυποποίηση της αλληλεπίδρασης μεταξύ ανθρώπων και συστημάτων που βασίζονται σε λογισμικό με στόχο την απλούστευση της, και την αποτελεσματική υποστήριξη των χρηστών. Το πρότυπο ISO 9241 ορίζει τον σχεδιασμό των εισροών που επιτρέπουν στους χρήστες να αλληλεπιδρούν με το λογισμικό και τα συστήματα, τη διαδικασία αλληλεπίδρασης και το φυσικό πλαίσιο ως χώρο εργασίας στον οποίο οι χρήστες αλληλεπιδρούν με τα συστήματα.

Οι διεπαφές χρήστη λογισμικού χρησιμοποιούνται για να παρουσιάσουν μια μεγάλη ποικιλία της λειτουργικότητας και της ενημέρωσης των χρηστών. Το πρότυπο ISO 14915 θεσπίζει αρχές σχεδιασμού για την αλληλεπίδραση επαγγελματιών χρηστών με κείμενο, γραφικά, ήχο, κινούμενα σχέδια, βίντεο και μέσα που σχετίζονται με άλλες αισθητήριες λεπτομέρειες. Το IEC TR 61997 καθορίζει κατευθυντήριες γραμμές για διεπαφές πολυμέσων που χρησιμοποιούνται από το ευρύ κοινό χωρίς καμία ειδική προηγούμενη εκπαίδευση. Το ISO 15223 ορίζει τα σύμβολα και την ανάπτυξη τέτοιων συμβόλων για τη μετάδοση πληροφοριών σχετικά με την ασφαλή και αποτελεσματική χρήση των ιατροτεχνολογικών προϊόντων.

Ασφάλεια, ανθεκτικότητα και εμπιστοσύνη

Ένα νέο προϊόν λογισμικού μπορεί να παράγει νέα αξία, αλλά μπορεί και να βλάψει άτομα ή υπάρχοντες διεργασίες ή να εισάγει κινδύνους για τέτοιες βλάβες. Το ISO / TR 16142 παρέχει καθοδήγηση σχετικά με την επιλογή της ασφάλειας και των επιδόσεων που σχετίζονται με τα πρότυπα για τις ιατρικές συσκευές που επιτρέπουν την εμπιστοσύνη ότι το νέο προϊόν δεν θα προκαλέσει βλάβες.

Το IEC 80001 καθορίζει την προοπτική του παρόχου περίθαλψης καθορίζοντας τον τρόπο διαχείρισης της ασφάλειας και της αποτελεσματικότητας ενός ολοκληρωμένου συστήματος υγειονομικής περίθαλψης. Ορίζει τους ρόλους και τις ευθύνες και τις πολιτικές και διαδικασίες διαχείρισης του κινδύνου για τα ιατρικά δίκτυα πληροφοριών, την ενίσχυση και την αλλαγή αυτών. Η οικογένεια προτύπων ISO 27000 καθιερώνει λεξιλόγιο, απαιτήσεις και διαδικασίες για τη διαχείριση της ασφάλειας και των κινδύνων που συνδέονται με την ασφάλεια τέτοιων ολοκληρωμένων συστημάτων.

Η προοπτική του προμηθευτή προϊόντος καλύπτεται από το πρότυπο ISO 14971 που τώρα ενσωματώνεται στο IEC 80001. Το ISO 14971 καθορίζει τις πρακτικές διαχείρισης κινδύνων που πρέπει να ακολουθούνται από τους κατασκευαστές ιατρικών συσκευών. Το πρότυπο ISO 13485 ορίζει τις κανονιστικές απαιτήσεις για ιατρικές συσκευές, συμπεριλαμβανομένης της τεκμηρίωσης, της διαχείρισης, την υλοποίηση προϊόντων και τις διαδικασίες διασφάλισης της ποιότητας. Το IEC 60601 τυποποιεί τις πρακτικές ασφαλείας για εξοπλισμό ιατρικών ηλεκτρικών συσκευών.

Αντίκτυπος των Προτύπων

Τα παρουσιαζόμενα πρότυπα ενσωματώνονται σε πολλούς εθνικούς κανονισμούς, αποτελούν κοινή πρακτική του έμπειρους προμηθευτές προϊόντων λογισμικού και αποτελούν μέρος της ανάθεσης του σήματος για τα προϊόντα που προορίζονται για τον τομέα της ιατρικής περίθαλψης. Αυτό είναι επίσης σημαντικό για τη συμμόρφωση με την οδηγία περί ιατροτεχνολογικών προϊόντων (*Medical Devices Directive*) [Rega13].

Κεφάλαιο 3

Μοντελοποίηση απειλών (*threat modeling*) και κινδύνων (*risk assessment*) για IoMT

Στο συγκεκριμένο Κεφάλαιο στόχος είναι να παρουσιαστεί ολόκληρη η πορεία σκέψης η μελέτη και η υλοποίηση ενός υπολογιστικού συστήματος που δεν θα υπονομεύει την ασφάλεια και την ιδιωτικότητα των ανθρώπων. Στην αρχή, θα παρουσιαστούν οι υπάρχοντες μεθοδολογίες που εφαρμόζονται για την μοντελοποίηση απειλών και για την αξιολόγηση κινδύνων όσο αφορά τα πληροφοριακά συστήματα. Στη συνέχεια, θα παρουσιαστούν ποιες μεθοδολογίες εφαρμόζονται για την μοντελοποίηση απειλών και αξιολόγηση κινδύνων στα συνδεδεμένα συστήματα με συσκευές για υγειονομική περίθαλψη. Έτσι, θα γίνει μια θεωρητική εισαγωγή για το πρακτικό μέρος της εργασίας.

3.1 Επισκόπηση μεθοδολογιών ασφάλειας για μοντελοποίηση απειλών και αξιολόγηση κινδύνων

Η ασφάλεια των πληροφοριακών συστημάτων μπορεί να χωριστεί σε δύο κατηγορίες, της εξωτερικής και της εσωτερικής ασφάλειας. Η εσωτερική ασφάλεια είναι το κύριο ζήτημα για ένα ασφαλές σύστημα και εξαρτάται από το σχεδιασμό και την ενσωμάτωση χαρακτηριστικών ασφαλείας κατά τη διάρκεια του. Αυτή η διαδικασία περιλαμβάνει τον εντοπισμό των απειλών ασφάλειας για τα συστήματα, τον προσδιορισμό των κατάλληλων μέτρων αντιμετώπισης και την ενσωμάτωσή τους στο σχεδιασμό. Για τον εντοπισμό των απαιτήσεων ασφαλείας των συστημάτων λογισμικού, έχουν αναπτυχθεί πολλές τεχνικές.

Η μοντελοποίηση απειλών αποτελεί μία από τις προσεγγίσεις για τον εντοπισμό των απαιτήσεων ασφάλειας. Η μοντελοποίηση απειλών καθιστά δυνατό τον εντοπισμό όλων των πιθανών απειλών για ένα σύστημα και ως εκ τούτου βοηθά τους σχεδιαστές λογισμικού στον περισσότερο ασφαλή και αξιόπιστο σχεδιασμό. Τα τελευταία χρόνια έχουν αναπτυχθεί πολλές μεθοδολογίες που θα αναλύσουμε παρακάτω.

3.1.1 Μοντελοποίηση απειλών

Η μοντελοποίηση απειλών είναι μια διαδικασία με την οποία μπορούν να προσδιοριστούν, να απαριθμηθούν και να ταξινομηθούν με βάση την προτεραιότητα, οι δυνητικές απειλές, όπως είναι οι δομικές αδυναμίες - όλες από την άποψη ενός υποθετικού επιτιθέμενου. Στόχος της μοντελοποίησης απειλών είναι να παρέχει μια συστηματική ανάλυση του προφίλ του πιθανού επιτιθέμενου, των πιθανότερων φορέων επίθεσης και των περιουσιακών στοιχείων που επιθυμεί περισσότερο ένας εισβολέας. Η προσομοίωση απειλών απαντά σε ερωτήσεις όπως ”Πού είναι τα περιουσιακά στοιχεία υψηλής αξίας;”, ”Πού είμαι πιο ευάλωτος σε επίθεση;”, ”Ποιες είναι οι σημαντικότερες απειλές;” και ”Υπάρχει διάνυσμα επίθεσης

που μπορεί να περάσει απαρατήρητο;". Εννοιολογικά, οι περισσότεροι άνθρωποι ενσωματώνουν κάποια μορφή μοντελοποίησης απειλών στην καθημερινότητά τους και δεν το συνειδητοποιούν.

Λίγο μετά την κοινή χρήση υπολογιστών που έκανε το ντεμπούτο του στις αρχές της δεκαετίας του 1960, τα άτομα άρχισαν να αναζητούν τρόπους εκμετάλλευσης των ευπαθειών ασφαλείας για προσωπικό κέρδος[McMi12]. Ως αποτέλεσμα, οι μηχανικοί και οι επιστήμονες υπολογιστών άρχισαν σύντομα να αναπτύσσουν έννοιες σχεδίασης απειλών για συστήματα τεχνολογίας πληροφοριών.

Οι πρώτες μεθοδολογίες μοντελοποίησης απειλών βασισμένες σε τεχνολογίες πληροφορικής βασίστηκαν στην έννοια των αρχιτεκτονικών μοντέλων [Shos14] που παρουσιάστηκε αρχικά από τον Christopher Alexander το 1977. Το 1988 ο Robert Barnard ανέπτυξε και διαμόρφωσε επιτυχώς το πρώτο προφίλ για έναν εισβολέα συστήματος πληροφορικής.

Το 1994, ο Edward Amoroso ανέπτυξε την έννοια του "δένδρου απειλής" στο βιβλίο του, "Βασικές αρχές της τεχνολογίας ασφάλειας υπολογιστών" [Amor94]. Η έννοια του δέντρου απειλών βασίστηκε στα διαγράμματα αποφάσεων. Τα δέντρα απειλών παριστάνουν γραφικά πώς μπορεί να εκμεταλλευτεί κακόβουλα μια πιθανή απειλή για ένα σύστημα πληροφορικής.

Ανεξάρτητα, παρόμοια δουλειά διεξήχθη από την NSA και τη DARPA σε μια δομημένη γραφική αναπαράσταση του τρόπου με τον οποίο θα μπορούσαν να γίνουν συγκεκριμένες επιθέσεις εναντίον συστημάτων πληροφορικής. Το 1998, ο Bruce Schneier δημοσίευσε την ανάλυσή του σχετικά με τους κινδύνους στον κυβερνοχώρο χρησιμοποιώντας δέντρα επίθεσης στην εργασία του με τίτλο «*Towards a Secure System Engineering Methodology*». [Salt98]

Το έγγραφο αποδείχθηκε να έχει σημαντική συμβολή στην εξέλιξη της προσομοίωσης απειλών για τα συστήματα πληροφορικής. Στην ανάλυση του Schneier, ο στόχος του εισβολέα παρουσιάζεται ως ένας "ριζικός κόμβος", με τα δυνητικά μέσα επίτευξης του στόχου να παρουσιάζονται ως "κόμβοι φύλλων". Η χρήση του δέντρου προσβολής με τον τρόπο αυτό επέτρεψε στους επαγγελματίες του κυβερνοχώρου να υπολογίζουν συστηματικά πολλαπλούς τρόπους επίθεσης ενάντια σε οποιονδήποτε στόχο έχει οριστεί.

Το 1999, οι επαγγελματίες της *Microsoft* για την ασφάλεια στον κυβερνοχώρο, Loren Kohnfelder και Praerit Garg, ανέπτυξαν ένα μοντέλο για να εξετάσουν τις επιθέσεις που σχετίζονται με το περιβάλλον ανάπτυξης των *Microsoft Windows*. (STRIDE *Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege*)[Scan15]. Η προκύπτουσα μνημονική ονομασία βοηθά τους επαγγελματίες ασφαλείας να καθορίζουν συστηματικά πώς ένας δυνητικός εισβολέας θα μπορούσε να χρησιμοποιήσει οποιαδήποτε απειλή από αυτές που περιλαμβάνονται στο STRIDE.

Το 2003, εισήχθη η μέθοδος OCTAVE [Albe02] (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), μια μεθοδολογία μοντελοποίησης απειλών κατά των επιχειρήσεων, με έμφαση στη διαχείριση κινδύνων οργανισμών.

Το 2004, ο Frank Swiderski και ο Window Snyder έγραψαν "Μοντελοποίηση απειλών" στον Τύπο της *Microsoft*. Σε αυτό ανέπτυξαν την έννοια της χρήσης μοντέλων απειλών για τη δημιουργία ασφαλών εφαρμογών. [Swid04]

Το 2014, ο Ryan Stillions εξέφρασε την άποψη ότι οι απειλές στον κυβερνοχώρο θα πρέπει να εκφράζονται με διαφορετικά σημασιολογικά επίπεδα και πρότειναν το μοντέλο DML (*Level of Maturity Detection Level*) [Mavr17]. Μια επίθεση είναι μια παράσταση ενός σεναρίου απειλής που προκαλείται από έναν συγκεκριμένο εισβολέα με συγκεκριμένο στόχο στο μυαλό και μια στρατηγική για την επίτευξη αυτού του στόχου. Ο στόχος και η στρατηγική αντιπροσωπεύουν τα υψηλότερα σημασιολογικά επίπεδα του μοντέλου DML. Αυτό ακολουθείται από το TTP (*Tactics, Techniques and Procedures*) που αντιπροσωπεύουν ενδιάμεσα

σημασιολογικά επίπεδα. Τα χαμηλότερα σημασιολογικά επίπεδα του μοντέλου DML είναι τα εργαλεία που χρησιμοποιούνται από τους επιτιθέμενους, τους κεντρικούς υπολογιστές και τα αντικείμενα που παρατηρούνται στο δίκτυο όπως τα πακέτα και τα ωφέλιμα φορτία και τέλος οι ατομικοί δείκτες όπως οι διευθύνσεις IP στο χαμηλότερο σημασιολογικό επίπεδο. Τα τρέχοντα εργαλεία SIEM (*security information and event management*) τυπικά παρέχουν μόνο δείκτες στα χαμηλότερα σημασιολογικά επίπεδα. Συνεπώς, υπάρχει ανάγκη ανάπτυξης εργαλείων SIEM που να παρέχουν δείκτες απειλών σε υψηλότερα σημασιολογικά επίπεδα [Brom16].

3.1.2 Μεθοδολογίες μοντελοποίησης απειλών

Εννοιολογικά, μια πρακτική μοντελοποίησης απειλών απορρέει από μια μεθοδολογία. Υπάρχουν πολλές μέθοδοι μοντελοποίησης απειλών για υλοποίηση. Τυπικά, η μοντελοποίηση απειλών έχει εφαρμοστεί χρησιμοποιώντας μία από τις τρεις προσεγγίσεις ανεξάρτητα, προσανατολισμένη στο ενεργητικό, επίκεντρο του εισβολέα και επικεντρωμένη στο λογισμικό. Με βάση το δημοσιευμένο περιεχομένου, οι τέσσερις μεθοδολογίες που αναφέρονται παρακάτω είναι οι πιο γνωστές.

Μεθοδολογία STRIDE

Η προσέγγιση STRIDE για τη μοντελοποίηση απειλών εισήχθη το 1999 στη *Microsoft*, παρέχοντας ένα μνημονικό για τους προγραμματιστές να βρουν «απειλές για τα προϊόντα μας» [Kohn]. STRIDE, TTP και Asset / entry ήταν μεταξύ των προσεγγίσεων μοντελοποίησης απειλών που αναπτύχθηκαν και δημοσιεύθηκαν από τη *Microsoft*. Οι αναφορές ως «μεθοδολογία της *Microsoft*» συνήθως αφορούν την μεθοδολογία STRIDE και τα διαγράμματα ροής δεδομένων.

Μεθοδολογία P.A.S.T.A.

Η διαδικασία προσομοίωσης επίθεσης και ανάλυσης απειλών (PASTA - *Process for Attack Simulation and Threat Analysis*) είναι μια μεθοδολογία επικεντρωμένη σε κινδύνους επτά σταδίων.[Uced15] Παρέχει μια διαδικασία επτά σταδίων για την ευθυγράμμιση των επιχειρηματικών στόχων και των τεχνικών απαιτήσεων, λαμβάνοντας υπόψη τα ζητήματα συμμόρφωσης και την επιχειρηματική ανάλυση. Σκοπός της μεθόδου είναι να παρέχει μια δυναμική αναγνώριση απειλών, απαρίθμηση και διαδικασία βαθμολόγησης. Μόλις ολοκληρωθεί το μοντέλο απειλής, οι εμπειρογνώμονες στον τομέα της ασφάλειας αναπτύσσουν μια λεπτομερή ανάλυση των εντοπισμένων απειλών. Τέλος, ορίζονται οι κατάλληλοι έλεγχοι ασφαλείας. Αυτή η μεθοδολογία αποσκοπεί να παρέχει μια επίκεντρο του εισβολέα μια εικόνα της εφαρμογής και της υποδομής από την οπτική των πιθανών επιτιθέμενων, από την οποία οι υπερασπιστές της ασφάλειας να μπορούν να αναπτύξουν μια στρατηγική αντιμετώπισης των στοιχείων του πληροφοριακού συστήματος.

Μεθοδολογία Trike

Το επίκεντρο της μεθοδολογίας Trike [Sait05] είναι μοντέλα απειλών ως εργαλείο διαχείρισης κινδύνου. Στο πλαίσιο αυτό, τα μοντέλα απειλών χρησιμοποιούνται για την ικανοποίηση της διαδικασίας ελέγχου της ασφάλειας. Τα μοντέλα απειλών βασίζονται σε ένα ”μοντέλο απαιτήσεων”. Το μοντέλο απαιτήσεων καθορίζει το ”αποδεκτό” επίπεδο κινδύνου που έχει οριστεί από τους συμμετέχοντες σε κάθε κατηγορία περιουσιακών στοιχείων. Η

ανάλυση του μοντέλου των απαιτήσεων δίνει ένα μοντέλο απειλής από το οποίο απαριθμούνται οι απειλές και αποδίδονται τα επίπεδα κινδύνου. Το ολοκληρωμένο μοντέλο απειλών χρησιμοποιείται για την κατασκευή ενός μοντέλου κινδύνου που βασίζεται σε περιουσιακά στοιχεία, ρόλους, ενέργειες και έτσι υπολογίζεται η έκθεση κινδύνου.

Μεθοδολογία VAST

Το VAST είναι ένα αρκτικόλεξο για *Visual, Agile και Simple Threat Modeling* [Agar16]. Η βασική αρχή αυτής της μεθοδολογίας είναι η ανάγκη κλιμάκωσης της διαδικασίας μοντελοποίησης απειλών σε ολόκληρη την υποδομή και ολόκληρο το SDLC (*Software development life cycle*) και την ενσωμάτωσή της σε μια Agile μεθοδολογία ανάπτυξης λογισμικού. Η μεθοδολογία επιδιώκει να παράσχει αποτελέσματα για τις ανάγκες των διαφόρων ενδιαφερομένων, δηλαδή των αρχιτεκτόνων εφαρμογών και προγραμματιστών, των μηχανικών ασφαλείας και των άλλων ανώτερων στελεχών. Η μεθοδολογία παρέχει ένα μοναδικό σχήμα οπτικοποίησης εφαρμογών και υποδομών, έτσι ώστε η δημιουργία και η χρήση μοντέλων απειλής να μην απαιτούν τεχνική γνώση για τα θέματα ασφαλείας.

3.1.3 Ανάλυση κινδύνων

Η ασφάλεια στον κυβερνοχώρο αφορά αποκλειστικά την κατανόηση, τη διαχείριση, τον έλεγχο και τον μετριασμό του κινδύνου για τα κρίσιμα στοιχεία ενός οργανισμού.

Για να ξεκινήσει μια αξιολόγηση κινδύνων ασφαλείας στον χώρο της πληροφορικής, πρέπει να απαντηθούν τρία σημαντικά ερωτήματα:

1. Ποια είναι τα σημαντικά στοιχεία τεχνολογίας της επιχείρησής - δηλαδή τα δεδομένα των οποίων η έκθεση θα είχε σημαντικό αντίκτυπο στις επιχειρηματικές δραστηριότητες;

2. Ποιες είναι οι πέντε κορυφαίες επιχειρηματικές διαδικασίες που χρησιμοποιούν ή απαιτούν αυτές τις πληροφορίες;

3. Ποιες απειλές θα μπορούσαν να επηρεάσουν την ικανότητα αυτών των επιχειρηματικών λειτουργιών να λειτουργούν;

Μόλις γίνει αντιληπτό τι πρέπει να προστατευτεί, μπορεί να ξεκινήσει η ανάπτυξη στρατηγικών. Πριν να εφαρμοστούν λύσεις για τη μείωση των κινδύνων, πρέπει να απαντηθούν περαιτέρω ερωτήσεις.

- Ποιος είναι ο κίνδυνος που θα μειωθεί;

- Είναι ο κίνδυνος ασφαλείας υψηλότερης προτεραιότητας;

- Γίνεται να μειωθεί με πλέον οικονομικά αποδοτικό τρόπο;

Αυτές οι ερωτήσεις καταλήγουν στο τι είναι κίνδυνος. Ο **κίνδυνος** είναι μια επιχειρησιακή ιδέα - είναι αν η πιθανότητα οικονομικής απώλειας για τον οργανισμό είναι υψηλή, μεσαία, χαμηλή ή μηδενική. Τρεις παράγοντες προσδιορίζουν τον κινδύνο: ποια είναι η απειλή, πόσο ευάλωτο είναι το σύστημα και ποια είναι η σημασία του περιουσιακού στοιχείου που μπορεί να καταστραφεί ή να μην είναι διαθέσιμο. Έτσι, ο κίνδυνος μπορεί να οριστεί ως εξής:

Κίνδυνος = Απειλή x Ευπάθεια x Περιουσιακό στοιχείο

Παρόλο που ο κίνδυνος παρουσιάζεται εδώ ως μαθηματικός τύπος, δεν πρόκειται για αριθμούς αλλά για ένα λογικό κατασκεύασμα. Για παράδειγμα, στην περίπτωση αξιολόγησης ενός κινδύνου που σχετίζεται με την απειλή των χάκερ που θέτουν σε κίνδυνο ένα συγκεκριμένο σύστημα. Εάν το δίκτυό είναι πολύ ευάλωτο (ίσως επειδή δεν υπάρχει τείχος προστασίας και δεν υπάρχει λύση αντιμετώπισης ιών) και το περιουσιακό στοιχείο είναι κρίσιμο, ο κίνδυνος είναι υψηλός. Ωστόσο, αν έχει καλή περιμετρική άμυνα και η ευπάθειά είναι χαμηλής σοβαρότητας, και παρόλο που το περιουσιακό στοιχείο είναι ακόμα κρίσιμο, ο κίνδυνος θα είναι μέτριος.

Εάν οποιοσδήποτε από τους παράγοντες είναι μηδέν, ακόμη και αν οι άλλοι παράγοντες είναι υψηλοί ή κρίσιμοι, ο κίνδυνος είναι μηδενικός. Ο κίνδυνος συνεπάγεται αβεβαιότητα. Αν κάτι είναι εγγυημένο να συμβεί, δεν υπάρχει κίνδυνος. Ακολουθούν ορισμένοι τρόποι με τους οποίους μπορεί ένας οργανισμός να υποστεί οικονομική ζημιά:

Απώλεια δεδομένων

Αν μια επιχείρηση υποστεί κλοπή εμπορικών μυστικών μπορεί να καταστραφεί από τους ανταγωνιστές της. Από την άλλη, κλοπή των πληροφοριών των πελατών θα μπορούσε να οδηγήσει σε απώλεια εμπιστοσύνης προς την επιχείρηση και φθοράς των πελατών.

Διακοπή συστήματος ή εφαρμογής

Εάν ένα σύστημα αποτυγχάνει να εκτελέσει την κύρια λειτουργία του, οι πελάτες ενδέχεται να μην είναι σε θέση να πραγματοποιήσουν παραγγελίες, οι εργαζόμενοι μπορεί να μην είναι σε θέση να κάνουν τις δουλειές τους ή να επικοινωνήσουν και ούτω καθεξής.

Νομικές συνέπειες

Εάν κλαπούν δεδομένα από τις βάσεις δεδομένων της επιχείρησης, ακόμη και αν αυτά τα δεδομένα δεν είναι ιδιαίτερα πολύτιμα, η εταιρεία μπορεί να υποστεί πρόστιμα και άλλα νομικά έξοδα επειδή απέτυχε να συμμορφωθεί με τις απαιτήσεις ασφάλειας των δεδομένων HIPAA, PCI DSS ή άλλων κανονισμών.

Η διαδικασία αξιολόγησης κινδύνων στον τομέα της τεχνολογίας πληροφοριών ακολουθεί τα παρακάτω βήματα.

1. Εντοπισμός και προτεραιότητα περιουσιακών στοιχείων

   Τα στοιχεία ενεργητικού περιλαμβάνουν διακομιστές, πληροφορίες επικοινωνίας με τους πελάτες, έγγραφα ευαίσθητων συνεργατών, εμπορικά μυστικά και ούτω καθεξής. Αυτό που ένας τεχνικός πιστεύει ότι είναι πολύτιμο μπορεί να μην θεωρείται πολύτιμο για την επιχείρηση. Επομένως, πρέπει να υπάρχει συνεργασία με τη διοίκηση για να δημιουργηθεί μια λίστα με όλα τα πολύτιμα περιουσιακά στοιχεία. Για κάθε στοιχείο, συγκεντρώνονται οι ακόλουθες πληροφορίες, ανάλογα με την περίπτωση:

   - Λογισμικό
   - Συσκευές, εξαρτήματα
   - Δεδομένα
   - Διεπαφές
   - Χρήστες
   - Υποστήριξη προσωπικού

- Αποστολή ή σκοπός
- Κριτική
- Λειτουργικές απαιτήσεις
- Πολιτικές ασφαλείας IT
- Αρχιτεκτονική ασφάλειας IT
- Τοπολογία δικτύου
- Προστασία αποθήκευσης πληροφοριών
- Ροή πληροφοριών
- Τεχνικοί έλεγχοι ασφαλείας
- Περιβάλλον φυσικής ασφάλειας
- Περιβαλλοντική ασφάλεια

Επειδή οι περισσότεροι οργανισμοί έχουν περιορισμένο προϋπολογισμό για την εκτίμηση κινδύνου, θα πρέπει πιθανότατα να περιορίζεται η ανάλυση σε περιουσιακά στοιχεία κρίσιμης σημασίας. Συνεπώς, πρέπει να ορίζεται ένα πρότυπο για τον προσδιορισμό της σημασίας κάθε στοιχείου. Τα κοινά κριτήρια περιλαμβάνουν τη νομισματική αξία του περιουσιακού στοιχείου, τη νομική υπόσταση και τη σημασία του οργανισμού. Μόλις το πρότυπο εγκριθεί από τη διοίκηση και ενσωματωθεί επισήμως στην πολιτική ασφάλειας αξιολόγησης κινδύνου, μπορεί να χρησιμοποιηθεί για την ταξινόμηση κάθε στοιχείου που θεωρείται κρίσιμο, σημαντικό ή μικρό.

2. Εντοπισμός απειλών

   Μια απειλή είναι κάτι που θα μπορούσε να εκμεταλλευτεί μια ευπάθεια για να παραβιάσει την ασφάλεια και να προκαλέσει βλάβη στον οργανισμό σας. Πέρα από τους χάκερς και τα κακόβουλα λογισμικά, υπάρχουν και άλλοι τύποι απειλών:

   - Φυσικές καταστροφές.

     Πλημμύρες, τυφώνες, σεισμοί, πυρκαγιές και άλλες φυσικές καταστροφές μπορούν να καταστρέψουν πολύ περισσότερο από έναν χάκερ. Μπορεί να χαθούν όχι μόνο τα δεδομένα, αλλά διακομιστές και συσκευές. Όταν αποφασίζεται για το πού θα στεγαστούν οι διακομιστές, πρέπει να υπολογίζεται και η πιθανότητα μιας φυσικής καταστροφής. Για παράδειγμα, ένας διακομιστής δεν πρέπει να τοποθετείται στον πρώτο όροφο αν η περιοχή έχει υψηλό κίνδυνο πλημμυρών.

   - Αποτυχία συστήματος.

     Η πιθανότητα βλάβης του συστήματος εξαρτάται από την ποιότητα του υπολογιστή. Για σχετικά νέο, υψηλής ποιότητας εξοπλισμό, η πιθανότητα βλάβης του συστήματος είναι χαμηλή. Αλλά εάν ο εξοπλισμός είναι παλαιός ή από έναν πωλητή χωρίς όνομα, η πιθανότητα αποτυχίας είναι πολύ υψηλότερη. Ως εκ τούτου, είναι σοφό ο εξοπλισμός να είναι υψηλής ποιότητας ή τουλάχιστον να προσφέρεται καλή υποστήριξη.

   - Τυχαία ανθρώπινη παρέμβαση.

     Αυτή η απειλή είναι πάντα υψηλή, ανεξάρτητα από την επιχείρηση. Οποιοσδήποτε μπορεί να κάνει λάθη, όπως η κατά λάθος διαγραφή σημαντικών αρχείων, κάνοντας κλικ σε συνδέσμους κακόβουλου λογισμικού ή τυχαία φυσική καταστροφή ενός εξοπλισμού. Επομένως, θα πρέπει να δημιουργούνται αντίγραφα

ασφαλείας των δεδομένων, των ρυθμίσεων του συστήματος, των ACL (*Access Control Lists*) και άλλων πληροφοριών διαμόρφωσης, και να παρακολουθούνται προσεκτικά όλες οι αλλαγές στα κρίσιμα συστήματα.

- Κακόβουλοι άνθρωποι.

  Υπάρχουν τρεις τύποι κακόβουλων συμπεριφορών:

  – Η παρεμβολή είναι όταν κάποιος προκαλεί ζημιά στην επιχείρησή, διαγράφοντας δεδομένα, σχεδιάζοντας μια κατανεμημένη άρνηση παροχής υπηρεσιών (DDoS) στον ιστότοπό, κλέβοντας φυσικά έναν υπολογιστή ή διακομιστή κλπ.
  – Η παρακολούθηση είναι κλασσική επίθεση, όπου κλέβουν τα δεδομένα της επιχείρησης.
  – Η πλαστοπροσωπία είναι κατάχρηση των διαπιστευτηρίων κάποιου άλλου, τα οποία αποκτώνται συχνά μέσω επιθέσεων *social engineering* ή επιθέσεων *brute-force* ή αγοράζονται στο σκοτεινό ιστό.

3. Προσδιορισμός ευπαθειών

   Στην συνέχεια, πρέπει να βρεθούν τα τρωτά σημεία. Ένα θέμα ευπάθειας είναι μια αδυναμία που μια απειλή μπορεί να εκμεταλλευτεί για να παραβιάσει την ασφάλεια και να βλάψει την εταιρεία. Οι ευπάθειες μπορούν να εντοπιστούν μέσω της ανάλυσης ευπάθειας, των εκθέσεων ελέγχου, της βάσης δεδομένων ευπάθειας NIST, των δεδομένων πωλητών, των ομάδων αντιμετώπισης των περιστατικών (*incident response teams*) και της ανάλυσης ασφάλειας λογισμικού συστήματος.

   Η δοκιμή του συστήματος πληροφορικής είναι επίσης ένα σημαντικό εργαλείο για τον εντοπισμό τρωτών σημείων. Οι δοκιμές μπορούν να περιλαμβάνουν τα εξής:

   - Διαδικασίες δοκιμής και αξιολόγησης της ασφάλειας πληροφοριών (*security test and evaluation*)
   - Τεχνικές δοκιμής διείσδυσης (*penetration testing techniques*)
   - Αυτοματοποιημένα εργαλεία σάρωσης ευπαθειών (*Automated vulnerability scanning tools*)

4. Ανάλυση των ελέγχων

   Αναλύοντας τα στοιχεία ελέγχου που βρίσκονται είτε στη θέση τους είτε στο στάδιο του σχεδιασμού ελαχιστοποιούνται ή εξαλείφονται οι πιθανότητες ότι μια απειλή θα εκμεταλλευτεί την ευπάθεια του συστήματος. Οι έλεγχοι μπορούν να υλοποιηθούν με τεχνικά μέσα, όπως υλικό ή λογισμικό ηλεκτρονικών υπολογιστών, κρυπτογράφηση, μηχανισμούς ανίχνευσης εισβολής και υποσυστήματα αναγνώρισης και ελέγχου ταυτότητας. Οι μη τεχνικοί έλεγχοι περιλαμβάνουν πολιτικές ασφάλειας, διοικητικές ενέργειες και φυσικούς και περιβαλλοντικούς μηχανισμούς.

   Τόσο οι τεχνικοί όσο και οι μη τεχνικοί έλεγχοι μπορούν περαιτέρω να ταξινομηθούν ως εξής. Οι προληπτικοί έλεγχοι προσπαθούν να προβλέψουν και να σταματήσουν τις επιθέσεις. Παραδείγματα προληπτικών τεχνικών ελέγχων είναι συσκευές κρυπτογράφησης και ελέγχου ταυτότητας. Όμως υπάρχουν και οι έλεγχοι που χρησιμοποιούνται για την ανεύρεση επιθέσεων ή συμβάντων με μέσα όπως τα διαγράμματα ελέγχου και τα συστήματα ανίχνευσης εισβολής (*intrusion detection systems*).

5. Προσδιορισμός της πιθανότητας συμβάντος

   Η πιθανότητα εκμετάλλευσης μιας ευπάθειας, αξιολογείται λαμβάνοντας υπόψη το είδος της ευπάθειας, την ικανότητα και την παρακίνηση της πηγής απειλής και την ύπαρξη και αποτελεσματικότητα των ελέγχων που υάρχουν. Αντί για αριθμητική βαθμολογία, πολλοί οργανισμοί χρησιμοποιούν τις κατηγορίες υψηλής, μεσαίας και χαμηλής για να εκτιμήσουν την πιθανότητα επίθεσης ή άλλης ανεπιθύμητης ενέργειας.

6. Αξιολόγηση του αντίκτυπου μια απειλής

   Η ανάλυση αντίκτυπου πρέπει να περιλαμβάνει τους ακόλουθους παράγοντες:

   - Η αποστολή του συστήματος, συμπεριλαμβανομένων των διαδικασιών που εφαρμόζονται από το σύστημα
   - Η κρισιμότητα του συστήματος, που καθορίζεται από την αξία του και την αξία των δεδομένων στον οργανισμό
   - Η ευαισθησία του συστήματος και των δεδομένων του

   Οι πληροφορίες που απαιτούνται για τη διεξαγωγή ανάλυσης αντικτύπου μπορούν να ληφθούν από τα υπάρχοντα οργανωτικά έγγραφα, συμπεριλαμβανομένης της ανάλυσης των επιπτώσεων στις επιχειρήσεις (*business impact analysis*). Το παρόν έγγραφο χρησιμοποιεί είτε ποσοτικά είτε ποιοτικά μέσα για τον προσδιορισμό του αντίκτυπου που θα προκαλούσε ο συμβιβασμός ή η βλάβη στα πληροφοριακά στοιχεία του οργανισμού.

   Μια επίθεση ή ένα ανεπιθύμητο συμβάν μπορεί να οδηγήσει σε συμβιβασμό ή απώλεια εμπιστευτικότητας του συστήματος πληροφοριών, ακεραιότητας και διαθεσιμότητας. Όπως και με τον προσδιορισμό της πιθανότητας, ο αντίκτυπος στο σύστημα μπορεί να εκτιμηθεί ποιοτικά ως υψηλός, μεσαίος ή χαμηλός.

   Τα ακόλουθα πρόσθετα στοιχεία πρέπει να περιλαμβάνονται στην ανάλυση αντίκτυπου:

   - Η εκτιμώμενη συχνότητα της εκμετάλλευσης μιας απειλής σε μια ετήσια βάση
   - Το κατά προσέγγιση κόστος καθενός από αυτά τα περιστατικά
   - Παράγοντας βάρους που βασίζεται στη σχετική επίδραση μιας συγκεκριμένης απειλής που εκμεταλλεύεται μια συγκεκριμένη ευπάθεια

7. Προτεραιότητα στους κινδύνους ασφάλειας πληροφοριών

   Για κάθε ζεύγος απειλών / ευπάθειας, καθορίζεται το επίπεδο κινδύνου για το σύστημα πληροφορικής, με βάση τα ακόλουθα:

   - Η πιθανότητα ότι η απειλή θα εκμεταλλευτεί την ευπάθεια
   - Ο αντίκτυπος μιας επιτυχούς εκμετάλλευσης της ευπάθειας
   - Η επάρκεια των υφιστάμενων ή προγραμματισμένων ελέγχων ασφάλειας του συστήματος πληροφοριών για την εξάλειψη ή τη μείωση του κινδύνου

8. Προτεινόμενοι έλεγχοι

   Χρησιμοποιώντας το επίπεδο κινδύνου ως βάση, καθορίζονται οι ενέργειες που πρέπει να αποφασιστούν από τα ανώτερα στελέχη και άλλα υπεύθυνα άτομα για να μετριάσουν τον κίνδυνο. Ακολουθούν ορισμένες γενικές οδηγίες για κάθε επίπεδο κινδύνου:

Υψηλό - Θα πρέπει να αναπτυχθεί το συντομότερο δυνατόν ένα σχέδιο διορθωτικών μέτρων.
Μέσο - Πρέπει να αναπτυχθεί ένα σχέδιο διορθωτικών μέτρων εντός εύλογου χρονικού διαστήματος.
Χαμηλό - Η ομάδα πρέπει να αποφασίσει εάν θα δεχτεί τον κίνδυνο ή θα εφαρμόσει διορθωτικές ενέργειες. Κατά την ανάπτυξη ελέγχων για τον μετριασμό κάθε κινδύνου, πρέπει να εξεταστούν:

- Οργανωτικές πολιτικές
- Ανάλυση κόστους-οφέλους
- Επιχειρησιακές επιπτώσεις
- Σκοπιμότητα
- Εφαρμοστέοι κανονισμοί
- Η συνολική αποτελεσματικότητα των συνιστώμενων ελέγχων
- Ασφάλεια και αξιοπιστία

9. Καταγραφή των αποτελεσμάτων

   Το τελευταίο βήμα στη διαδικασία εκτίμησης κινδύνων είναι η εκπόνηση μιας έκθεσης αξιολόγησης κινδύνου για τη στήριξη της διαχείρισης κατά τη λήψη των κατάλληλων αποφάσεων σχετικά με τον προϋπολογισμό, τις πολιτικές, τις διαδικασίες και ούτω καθεξής. Για κάθε απειλή, η αναφορά θα πρέπει να περιγράφει τις αντίστοιχες ευπάθειες, τα περιουσιακά στοιχεία σε κίνδυνο, τον αντίκτυπο στην υποδομή πληροφορικής, την πιθανότητα εμφάνισης και τις συστάσεις ελέγχου.

   Μπορεί να χρησιμοποιηθεί μια αναφορά αξιολόγησης κινδύνων (*risk assessment report*) για να εντοπιστούν τα βασικά βήματα αποκατάστασης που θα μειώσουν τους πολλαπλούς κινδύνους. Είναι σημαντικό να δίνεται σημασία στους επιχειρηματικούς λόγους για κάθε εφαρμογή βελτίωσης.

   Έχοντας καλύτερη εικόνα για το πώς λειτουργεί η επιχείρηση και η υποδομής της και πώς μπορεί να λειτουργήσει καλύτερα, γίνεται να δημιουργηθεί μια πολιτική εκτίμησης κινδύνων που καθορίζει τι πρέπει να κάνει ο οργανισμός (σε ετήσια βάση σε πολλές περιπτώσεις), τον τρόπο αντιμετώπισης και μετριασμού του κινδύνου (για παράδειγμα, ένα ελάχιστο αποδεκτό παράθυρο ευπάθειας) και τον τρόπο με τον οποίο ο οργανισμός πρέπει να πραγματοποιήσει μεταγενέστερη επιχείρηση αξιολόγησης των κινδύνων για τις συνιστώσες της υποδομής πληροφορικής και άλλων περιουσιακών στοιχείων.

   Οι διαδικασίες αξιολόγησης κινδύνων ασφάλειας των πληροφοριών και διαχείρισης επιχειρηματικών κινδύνων αποτελούν την καρδιά της ασφάλειας υπολογιστών. Αυτές οι διαδικασίες καθορίζουν τους κανόνες και τις κατευθυντήριες γραμμές για το σύνολο της διαχείρισης της ασφάλειας των πληροφοριών, παρέχοντας απαντήσεις στο ποιες απειλές και τρωτά σημεία μπορούν να προκαλέσουν οικονομική βλάβη στην επιχείρησή μας και πώς πρέπει να μετριαστούν.

3.1.4 Μεθοδολογίες Αξιολόγησης κινδύνων

Είναι πολύ δύσκολο να περιγράψουμε τις περισσότερες από τις μεθόδους που υποστηρίζουν τουλάχιστον εν μέρει τη διαδικασία διαχείρισης κινδύνων στον τομέα της πληροφορικής. Προσπάθειες προς αυτή την κατεύθυνση έγιναν από:

- Ινστιτούτο NIST. Η περιγραφή των αυτοματοποιημένων πακέτων διαχείρισης κινδύνων που εξέτασε το εργαστήριο έρευνας διαχείρισης κινδύνων NIST / NCSC, που ενημερώθηκε το 1991

- Ο ENISA (*European Union Agency for Network and Information Security*) το 2006. Στο διαδίκτυο είναι διαθέσιμη μια λίστα μεθόδων και εργαλείων. Μεταξύ αυτών οι πιο ευρέως χρησιμοποιούμενες είναι:

  – Το CRAMM που αναπτύχθηκε από τη βρετανική κυβέρνηση είναι σύμφωνο με το πρότυπο ISO / IEC 17799, τον νόμο Gramm-Leach-Bliley Act(GLBA) και τον HIPAA (*Health Insurance Portability and Accountability Act*).

  – Το EBIOS που αναπτύχθηκε από τη γαλλική κυβέρνηση συμμορφώνεται με τα βασικά πρότυπα ασφαλείας: ISO / IEC 27001, ISO / IEC 13335, ISO / IEC 15408, ISO / IEC 17799 και ISO / IEC 21287.

  – Πρότυπο ορθής πρακτικής που αναπτύχθηκε από το φόρουμ ασφάλειας πληροφοριών (ISF – *Information Security Forum*).

  – Το Mehari αναπτύχθηκε από το Clusif Club de la Sécurité de l'Information Français .

  – TIK IT Risk Framework που αναπτύχθηκε από το ινστιτούτο IT Risk.

  – Το Octave (*Operationally Critical Threat Asset and Vulnerability Evaluation*)που αναπτύχθηκε από το Πανεπιστήμιο Carnegie Mellon και το Ινστιτούτο μηχανικών λογισμικού (*Software Engineering Institute*) το οποίο ορίζει μια στρατηγική αξιολόγησης και σχεδιασμού για την ασφάλεια με βάση τον κίνδυνο.

  – IT-Grundschutz (Εγχειρίδιο προστασίας στον τομές της πληροφορικής) που αναπτύχθηκε από την Ομοσπονδιακή Υπηρεσία Ασφάλειας Πληροφοριών (BSI) (Γερμανία). Το IT-Grundschutz παρέχει μια μέθοδο για έναν οργανισμό σχετικά με τη δημιουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Περιλαμβάνει τόσο γενικές συστάσεις ασφαλείας IT για την καθιέρωση μιας εφαρμόσιμης διαδικασίας ασφάλειας στον τομέα της πληροφορικής όσο και λεπτομερείς τεχνικές συστάσεις για την επίτευξη του απαιτούμενου επιπέδου ασφάλειας για συγκεκριμένο τομέα.

Η έκθεση Enisa [Mari06] ταξινόμησε τις διάφορες μεθόδους όσον αφορά την πληρότητα, την ελεύθερη διαθεσιμότητα, την υποστήριξη εργαλείων. Οι μέθοδοι EBIOS, ISF, IT-Grundschutz καλύπτουν βαθιά όλες τις πτυχές (προσδιορισμός κινδύνου, ανάλυση κινδύνου, αξιολόγηση κινδύνου, εκτίμηση κινδύνου, αντιμετώπιση κινδύνου, αποδοχή κινδύνου, επικοινωνία κινδύνου). Το EBIOS και το IT-Grundschutz είναι τα μόνα ελεύθερα διαθέσιμα και μόνο το EBIOS διαθέτει ένα εργαλείο ανοιχτού κώδικα για να το υποστηρίξει.

Το βασικό έγγραφο FAIR (*Factor Analysis of Information Risk* – 2006) [Freu14], περιγράφει ότι οι περισσότερες από τις παραπάνω μεθόδους δεν ορίζουν αυστηρά τον κινδύνο και τους παράγοντες τους. Το FAIR δεν είναι ξεχωριστή μέθοδος αντιμετώπισης της διαχείρισης κινδύνου, αλλά συμπληρώνει τις υπάρχουσες μεθοδολογίες.

Κεφάλαιο 4

Πειραματική ανάλυση - Ανάλυση ασφάλειας

Στην αρχή του κεφαλαίου θα γίνει μια καταγραφή των απειλών που αφορούν το αντικείμενο της πειραματικής μελέτης (*case study*) και παρουσίαση ενός μοντέλου απειλών σαν εισαγωγή του πρακτικού μέρους όπου ακολουθεί και περιγραφεί τον πειραματικό έλεγχο για την επιβεβαίωση ικανοποίησης απαιτήσεων ασφάλειας.

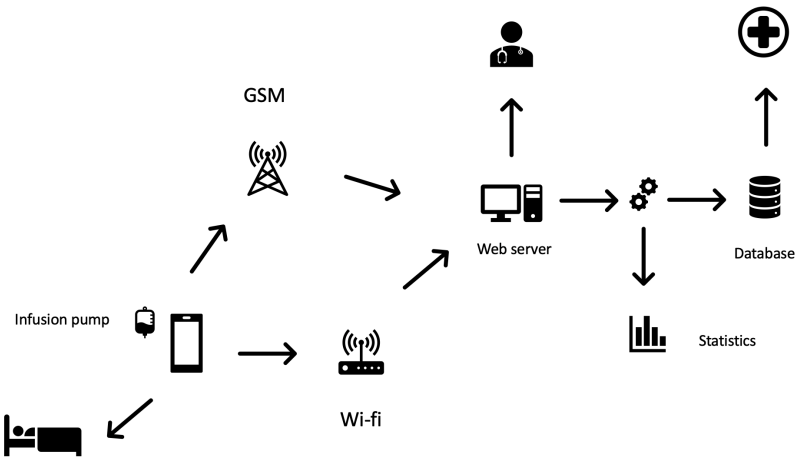
Το αντικείμενο μελέτης μας πρόκειται για μια ιατρική συσκευή αντλίας έγχυσης φαρμάκων που είναι σε στάδιο ανάπτυξης και δεν είναι διαθέσιμη στην αγορά. Τα τελευταία χρόνια, πολλές έρευνες και παρουσιάσεις στον χώρο της ασφάλειας των IoMT έχουν δείξει πόσο εύκολα επιτιθέμενοι μπορούν να θέσουν σε κίνδυνο όλους τους τύπους συσκευών, συμπεριλαμβανομένων των αντλίων έγχυσης, των βηματοδοτών, των απινιδωτών και παρόμοιων προσωπικών ιατρικών συσκευών που συνδέονται με το διαδίκτυο, και είναι απαραίτητες για τις ζωές των ασθενών[Kher16]. Αυτό συμβαίνει επειδή οι επιτιθέμενοι μπορούν να ελέγξουν τα σήματα που στέλνονται και λαμβάνονται από αυτές τις συσκευές και στη συνέχεια μπορούν να ενεργήσουν κακόβουλα με διάφορους τρόπους, όπως, να επηρεάσουν τις τιμές των μετοχών του κατασκευαστή, να ζητήσουν λύτρα από το νοσοκομείο, τον ιατρικό προμηθευτή ή το άτομο και μπορεί ακόμη και να επιλέξουν να βλάψουν τον ασθενή σωματικά.

Οι εμπλεκόμενοι ρόλοι στο σύστημα αναφέρονται σε κάθε οντότητα φυσική ή μη που έχει την δυνατότητα να αλληλεπιδρά με την συσκευή και να διαμορφώνει, να καθορίζει ή να επηρεάζει την λειτουργία της. Έχουμε έτσι δύο κατηγορίες, τους ανθρώπινους ρόλους και τους ρόλους συστήματος. Οι ρόλοι του συστήματος περιλαμβάνουν την ιατρική συσκευή έγχυσης, την ηλεκτρονική πλατφόρμα του παρόχου της ιατρικής συσκευής στην οποία περιλαμβάνονται οι θεραπείες ασθενών, τις βιβλιοθήκες φαρμάκων, τον μηχανισμό φόρτωσης βιβλιοθηκών (*drug libraries*) και τον μηχανισμό συντήρησης της συσκευής, τις ετικέτες και το μηχανισμό ανάγνωσης RFID ετικετών, το σύστημα πληροφοριών του νοσοκομείου. Οι ανθρώπινοι ρόλοι είναι οι ασθενείς, οι ενδονοσοκομειακούς χρήστες (γιατροί, νοσηλευτές μιας νοσοκομειακής μονάδας που έχουν την ευθύνη για τον χειρισμό της αντλίας έγχυσης, οι τεχνικοί (οι νοσοκομειακοί τεχνικοί, οι γενικοί τεχνικοί και οι τεχνικοί του προμηθευτή), ο διαχειριστής καθώς και ο μηχανικός ανάπτυξης (*developer*) του προμηθευτή.

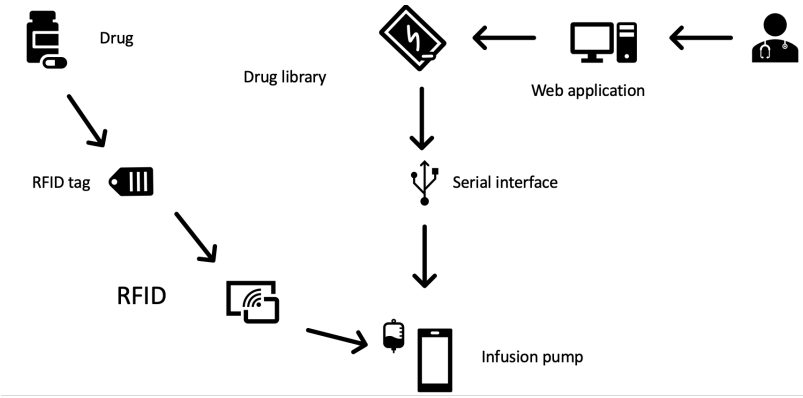
Αρχιτεκτονική του συστήματος

Το συνολικό σύστημα που επιλέχθηκε ως αντικείμενο μελέτης αποτελείται από τις υπό ανάπτυξη αντλίες έγχυσης φαρμάκων που έχουν δυνατότητα διασύνδεσης με την ηλεκτρονική πλατφόρμα του παρόχου με δύο τρόπους όπως φαίνεται στο σχήμα 4.1. Είτε με σύνδεση Wi-fi είτε με GSM επικοινωνία.

Μέσω του λογισμικού της ηλεκτρονικής πλατφόρμα επιτρέπεται η απομακρυσμένη παρακολούθηση των θεραπειών εγχύσεων που εκτελούνται με τις αντλίες έγχυσης σε πραγματικό χρόνο. Συλλέγονται και παρουσιάζονται στατιστικά στοιχεία. Καθώς και δημιουργούνται οι βιβλιοθήκες φαρμάκων και θεραπειών.



Σχήμα 4.1: Συνδεσιμότητα αντλίας έγχυσης



Σχήμα 4.2: Προγραμματισμός βιβλιοθηκών

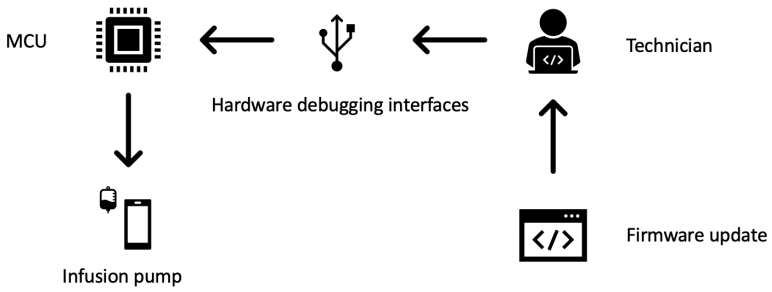
Η υπό ανάπτυξη αντλία έγχυσης έχει τη δυνατότητα να συνδεθεί τοπικά με τα κάτωθι περιφερειακά/συσκευές:

- *Administration set* (παροχή φαρμάκου στον ασθενή)
- Τροφοδοτικό
- *Bolus Handset* (παροχή δόσεων φαρμάκου στον ασθενή κατ'επίκληση)

Όσων αφορά τον προγραμματισμό των βιβλιοθηκών φαρμάκων στη συσκευή, αυτός γίνεται είτε μέσω σειριακής θύρας και τη βοήθεια ειδικού λογισμικού είτε με ανάγνωση RFID ετικετών όπως παρουσιάζονται και στο σχήμα 4.2.

Η αντλία έγχυσης αποτελείται από τις εξής υπομονάδες:

- Περισταλτικός μηχανισμός έγχυσης
- Ηλεκτρικός κινητήρας
- Επεξεργαστές
- Λογισμικό Επεξεργαστών
- Μονάδα διεπαφής χρήστη



Σχήμα 4.3: Ενημέρωση λογισμικού αντλίας έγχυσης

- Μονάδα ελέγχου ηλεκτρικής ισχύος
- Αισθητήρα παρακολούθησης έγχυσης
- Αισθητήρες παρακολούθησης πίεσης, αέρα
- Αισθητήρα ταυτοποίησης μέσω ραδιοσυχνοτήτων (RFID)

Τέλος, για την ενημέρωση του λογισμικού της συσκευής έχει επιλεχθεί ο τρόπος μέσω διεπαφών της συσκευής (*hardware debugging interfaces*) όπως παρουσιάζεται στο σχήμα 4.3. Επιλέχθηκε αυτός ο μηχανισμός ώστε να αποφευχθεί η λήψη εντολών και νέου λογισμικού πάνω από το Ίντερνετ. Αυτό μειώνει σημαντικά τις δυνατότητες και τις ευκολίες όλου του συστήματος αλλά εξασφαλίζει ότι δεν υπάρχουν οι κίνδυνοι αλλοίωσης του υλικολογιμσικού (*firmware*) κατά τη διαδικασία ενημέρωσης και απομακρυσμένου ελέγχου της συσκευής (*remote code execution*).

Περιορισμοί

Ένα βασικό χαρακτηριστικό των διασυνδεδεμένων συσκευών (IoT) και των διασυνδεδεμένων ιατρικών συσκευών (IoMT) ειδικότερα είναι οι σημαντικοί περιορισμοί που υπάρχουν στο επίπεδο του υλικού και στην αρχιτεκτονική προκειμένου αυτές να συμβαδίζουν με την ανάγκη της φορητότητας και της υψηλής διαθεσιμότητας (*high availability*).

Η ανάγκη φορητότητας της συσκευής προσδιορίζει την αρχιτεκτονική που θα ακολουθηθεί κατά την σχεδίαση περιορίζοντας το μέγεθος καθώς και την ενεργειακή τροφοδοσία που αυτή θα έχει. Ο συγκεκριμένος περιορισμός επηρεάζει τους μηχανισμούς ασφαλείας που μπορούν να εφαρμοστούν.

Η ανάγκη υψηλής διαθεσιμότητας σχετίζεται άμεσα με την ανάγκη για χαμηλή κατανάλωση ενέργειας της συσκευής σε όλη τη διάρκεια λειτουργίας της. Η συνολικά καταναλισκώμενη ενέργεια εξαρτάται από πολλούς παράγοντες αρκετοί από τους οποίους έχουν άμεση αντανάκλαση στο επίπεδο ασφάλειας που μπορεί να προσφέρει η συσκευή.

4.1 Μοντέλο απειλών αντικειμένου μελέτης - *case study*

Κατά τη διάρκεια της πειραματικής ανάλυσης του αντικειμένου ιατρικής περίθαλψης που επιλέχθηκε, έγινε μια σειρά από δοκιμές και προσπάθειες παραβίασης της ασφάλειας του υπολογιστικού συστήματος με σκοπό την εύρεση αδυναμιών ώστε να προταθούν λύσεις

αντιμετώπισης τους. Πρώτα όμως θα παρουσιαστεί ένα μοντέλο απειλών για να περιγραφούν κάποιες μέτρα ασφάλειας του συστήματος που χρειάζονται.

Το μοντέλο απειλών προσωποποιεί τους βασικούς πράκτορες που μπορούν να επηρεάσουν το IoMT σύστημα, τους εν γένει κινδύνους στους οποίους τέτοιου τύπου συστήματα είναι ευάλωτα, τις αντίστοιχες απειλές και τον τύπο των μέτρων ασφάλειας που πρέπει να εφαρμοστούν.

Για τις ανάγκες της εργασίας αναπτύχθηκε ένα μοντέλο βασισμένο σε πράκτορες (*agent-centric model*), που επιτρέπει την αποτελεσματική μοντελοποίηση των απειλών.

Ο **πράκτορας** μιας απειλής (*threat agent*) θεωρείται το υποκείμενο που δημιουργεί τον κίνδυνο σε ένα συγκεκριμένο στοιχείο του συστήματος. Οι πράκτορες έχουν κάποια χαρακτηριστικά που επιτρέπουν μια συγκεκριμένη συμπεριφορά δεδομένων κάποιων κανόνων (π.χ. ένας εσωτερικός εχθρός, ένας απογοητευμένος υπάλληλος).

Τα μοντέλα απειλών που είναι βασισμένα στους πράκτορες εκκινούν την διερεύνηση των απειλών από τα υποκείμενα και τις δυνατότητές τους σε σχέση με το σύστημα και την λειτουργία του, και δεν επικεντρώνονται αποκλειστικά στα στοιχεία του πληροφοριακού συστήματος.

Απειλή (*threat*) είναι μία πιθανή ενέργεια ενός πράκτορα σε ένα στοιχείο του πληροφοριακού συστήματος που μπορεί να επηρεάσει την ακεραιότητα, την διαθεσιμότητα ή την εμπιστευτικότητα αυτού ή άλλων στοιχείων.

Για το συγκεκριμένο μοντέλο απειλών **στοιχεία του πληροφοριακού συστήματος** (*assets*) είναι όλα τα μέρη που συμμετέχουν ή καθορίζουν τη λειτουργία του συστήματος δηλαδή τα υπολογιστικά συστήματα, οι δικτυακές πύλες, οι περιφερειακές συσκευές, το λογισμικό, τα δεδομένα κ.ά.

Στοιχεία πληροφοριακού συστήματος

Τα στοιχεία πληροφοριακού συστήματος είναι τα παρακάτω:

- Έξυπνη Ιατρική Συσκευή: Πρόκειται για την ίδια την ιατρική συσκευή, δηλαδή την υπό ανάπτυξη αντλία έγχυσης. Διαθέτει επαναπρογραμματίσιμο λογισμικό καθώς και δυνατότητα δικτυακής διασύνδεσης.

- Ηλεκτρονική Πλατφόρμα: Πρόκειται για το σύστημα μέσω του οποίου γίνεται η απομακρυσμένη διαχείριση των ιατρικών συσκευών από το ιατρικό προσωπικό και/ή τεχνικό προσωπικό.

- Μέσο Διασύνδεσης: Πρόκειται για μία δικτυακή πύλη (*gateway*) που μέσω αυτής γίνεται η διασύνδεση της ιατρικής συσκευής και της ηλεκτρονικής πλατφόρμας.

- Περιφερειακές Συσκευές: Αναφέρεται σε κάθε περιφερειακή συσκευή, όπως ο μηχανισμός ανάγνωσης ετικετών RFID. Κάθε περιφερειακή συσκευή περιλαμβάνει πέρα από την ίδια την συσκευή και το λογισμικό που χρειάζεται για την χρήση της.

Τα επιμέρους στοιχεία που παρουσιάζονται είναι συνήθως τα στοιχεία πληροφοριακού συστήματος κάθε IoMT εφαρμογής με ”έξυπνες συσκευές” και κάθε ένα τέτοιο στοιχείο μπορεί να αποτελεί αντικείμενο μίας ή περισσότερων απειλών από κάποιον πράκτορα.

Για τον προσδιορισμό των πρακτόρων χρησιμοποιήθηκε ως αναφορά η Βιβλιοθήκη Πρακτόρων Απειλών της INTEL (*INTEL Threat Agent Library*) [Case07]. Η βιβλιοθήκη αυτή έχει μια περιγραφή των ανθρώπων που θα μπορούσαν να απειλούν ένα πληροφοριακό σύστημα και είναι μια καλή επιλογή για αναφορά για το μοντέλο απειλών μας.

Τα χαρακτηριστικά βάσει των οποίων προσδιορίζονται οι πράκτορες σύμφωνα με το την βιβλιοθήκη TAL είναι τα παρακάτω:

- Πρόθεση
- Πρόσβαση
- Αποτέλεσμα
- Όρια
- Πόροι
- Επίπεδο Δεξιοτήτων
- Σκοπός
- Ορατότητα

Τα χαρακτηριστικά αυτά προσδιορίζουν την απάντηση στις παρακάτω βασικές ερωτήσεις.

- Ποιος είναι ο πράκτορας;
- Από πού ο πράκτορας απειλεί κάποιο στοιχείο του συστήματος;
- Γιατί έχει κίνητρο ο πράκτορας;
- Πώς θα επηρεάσει ο πράκτορας τον οργανισμό;
- Έχει ο πράκτορας κάποια όρια στις πράξεις του;
- Είναι βιώσιμη η απειλή; Χρειάζεται εκτεταμένη χρηματοδότηση για τις ενέργειες του πράκτορα;
- Πόσο εύκολο είναι; Χρειάζεται κάποιο επίπεδο δεξιοτήτων για τις ενέργειες του πράκτορα;
- Πρόκειται ο πράκτορας να αναγνωριστεί από τις πράξεις του;
- Θα είναι δυνατόν να εντοπιστεί μια τρέχουσα επίθεση;

Εξέταση των προτύπων της INTEL TAL

Καθένας από τους πράκτορες που περιγράφει η INTEL βιβλιοθήκη πρακτόρων κινδύνων (*Threat Agent Library*), ελέγχθηκε ως προς την συμβατότητα με τα χαρακτηριστικά που αναγνωρίσθηκαν στο πληροφοριακό σύστημα της αντλίας έγχυσης. Στην ανάλυση μας δεν παρουσιάζονται πράκτορες των οποίων οι απειλές μπορούν να αντιμετωπιστούν εξ ολοκλήρου μέσω λειτουργικών διαδικασιών γιατί θέλουμε να επικεντρωθούμε στα τεχνολογικά μέσα ασφάλειας.

Έτσι, δημιουργήθηκε ο πίνακας 4.1 πρακτόρων ο οποίος περιλαμβάνει όλους τους πράκτορες οι οποίοι είναι συμβατοί με τα χαρακτηριστικά του συστήματος της αντλίας έγχυσης.

Εχθρική πρόσθεση							
Πράκτορας	Πρόσβαση	Αποτέλεσμα	Όρια	Πόροι	Επίπεδο δεξιοτή-των	Σκοπός	Ορατότητα
Απατεώνας ασθενής	Εξωτερική (βασική)	Απόκτηση/Κλοπή, Προσβολή	Εκτός νόμου (μεγάλης κλίμακας)	Άτομο	Ελάχιστες	Αντιγραφή Βλάβη	Μυστικός
Απατεώνας γιατρός	Εξωτερική (εκτεταμένη)	Απόκτηση/Κλοπή, Επιχειρηματικό πλεονέκτημα, Προσβολή	Εκτός νόμου (μεγάλης κλίμακας)	Άτομο	Λειτουργι	Αντιγραφή Βλάβη	Μυστικός
Αδιάκριτος γιατρός	Εξωτερική (εκτεταμένη)	Απόκτηση/Κλοπή	Κώδικας Δεοντολογίας	Άτομο	Λειτουργι	Αντιγραφή	Μυστικός
Απατεώνας τεχνικός	Εσωτερική	Απόκτηση/Κλοπή, Επιχειρηματικό πλεονέκτημα	Εκτός νόμου (μεγάλης κλίμακας)	Άτομο	Ειδήμων	Αντιγραφή	Μυστικός
Ανταγωνιστής	Εξωτερική (βασική)	Βλάβη, Επιχειρηματικό Πλεονέκτημα, Τεχνικό Πλεονέκτημα	Εκτός νόμου (μικρής κλίμακας)	Οργανισ	Ειδήμων	Αντιγραφή	Κρυφός
Κλέφτης ιατρικών δεδομένων	Εξωτερική (βασική)	Απόκτηση/Κλοπή	Νομικά	Άτομο	Λειτουργι	Αντιγραφή Από-σπαση	Μυστικός
Σκανδαλοθήρ	Εξωτερική (βασική)	Βλάβη, Προσβολή	Εκτός νόμου (μικρής κλίμακας)	Άτομο	Λειτουργι	Αδιάφορο	Φανερός
Τρομοκράτης	Εξωτερική (βασική)	Βλάβη, Προσβολή	Εκτός νόμου (μεγάλης κλίμακας)	Σύλλογο	Ειδήμων	Καταστρο Βλάβη, Από-σπαση	Κρυφός
Προμηθευτής	Εξωτερική	Απόκτηση/Κλοπή, Επιχειρηματικό πλεονέκτημα	Εκτός νόμου (μικρής κλίμακας)	Οργανισ	Ειδήμων	Αντιγραφή	Μυστικός

Πίνακας 4.1: Συμβατοί πράκτορες με τα χαρακτηριστικά του συστήματος

Έξυπνη Ιατρική Συσκευή	
1	Μεταβολή του firmware της συσκευής
2	Αντιγραφή του firmware της συσκευής
3	Κλοπή δεδομένων υγείας ασθενών από την συσκευή
4	Μεταβολή των ιατρικών δεδομένων στη συσκευή
5	Μεταβολή θεραπειών στην συσκευή
6	Παροχή θεραπείας χωρίς νόμιμη άδεια

Πίνακας 4.2: Απειλές για την έξυπνη ιατρική συσκευή

Απειλές

Από κάθε πράκτορα μπορούν να ξεκινούν μια ή περισσότερες απειλές στο σύστημα και στα στοιχεία του συστήματος, χρησιμοποιώντας κάθε φορά διαφορετική τεχνική παρείσδυσης για να πετύχει τον σκοπό του. Παρακάτω θα αναφερθούν πιθανές απειλές που αφορούν κάθε στοιχείο του συστήματος που προσδιορίσαμε καθώς και μέτρα ασφάλειας που απαιτούνται ώστε να παραμένει ασφαλές το σύστημα.

Στον πίνακα 4.2 παρουσιάζονται απειλές με κέντρο την έξυπνη ιατρική συσκευή.

Ηλεκτρονική Πλατφόρμα	
1	Χρήση της ηλεκτρονικής πλατφόρμας χωρίς νόμιμη άδεια (Ανταγωνιστής, Απατεώνας Ασθενής, Απατεώνας Ιατρός, Απατεώνας Τεχνικός)
1	Αντιγραφή του λογισμικού της ηλεκτρονικής πλατφόρμας (Ανταγωνιστής)
3	Αντιγραφή του λειτουργικού της συσκευής μέσω της ηλεκτρονικής πλατφόρμας
4	Κλοπή δεδομένων υγείας ασθενών μέσω της ηλεκτρονικής πλατφόρμας
5	Μεταβολή των δεδομένων υγείας στην ηλεκτρονική πλατφόρμα
6	Μεταβολή των θεραπειών στην ηλεκτρονική πλατφόρμα
7	Μη εξουσιοδοτημένη πρόσβαση σε επιχειρησιακά δεδομένα χρηστών της ηλεκτρονικής πλατφόρμας
8	Μεταβολή του λογισμικού της ηλεκτρονικής πλατφόρμας
9	Μεταβολή του υλικολογισμικο μέσω της ηλεκτρονικής πλατφόρμας

Πίνακας 4.3: Απειλές για την ηλεκτρονική πλατφόρμα

Μέσο Διασύνδεσης	
1	Κλοπή δεδομένων υγείας ασθενών μέσω των μέσων διασύνδεσης
2	Μεταβολή δεδομένων υγείας ασθενών μέσω των μέσων διασύνδεσης
3	Μεταβολή των θεραπειών μέσω των μέσων διασύνδεσης
4	Μη εξουσιοδοτημένη πρόσβαση σε επιχειρησιακά δεδομένα χρηστών του συστήματος μέσω των μέσων διασύνδεσης

Πίνακας 4.4: Απειλές για το μέσο διασύνδεσης

Περιφερειακές Συσκευές	
1	Πλαστογραφία δεδομένων από τις περιφερειακές συσκευές

Πίνακας 4.5: Απειλές για τις περιφερειακές συσκευές

Στον πίνακα 4.3 παρουσιάζονται οι απειλές με κέντρο την ηλεκτρονική πλατφόρμα του παρόχου.

Στον πίνακα 4.4 παρουσιάζονται απειλές που μπορούν να προκύψουν με κέντρο το μέσο διασύνδεσης των συσκευών με την ηλεκτρονική πλατφόρμα.

Στον πίνακα 4.5 παροουσιάζονται απειλές που μπορούν να προκύψουν με κέντρο τις περιφερειακές συσκευές.

Μέτρα ασφάλειας για το σύστημα ιατρικής συσκευής αντλίας έγχυσης

Από αυτές τις απειλές προκύπτουν κάποιες απαιτήσεις ασφάλειας για το σύστημα που αφορούν τεχνικά μέσα και όχι εφαρμογή διαδικασιών (π.χ. εκπαίδευση προσωπικού) που κατευθύνουν και τους μηχανικούς ασφάλειας για το ποια είναι οι απαραίτητοι έλεγχοι αξιολόγησης της ασφάλειας. Λαμβάνοντας υπόψη τις απειλές που περιγράφηκαν και τα πρότυπα και τις οδηγίες ασφάλειας που υπάρχουν μπορούμε να προσδιορίσουμε κάποιες μέτρα ασφάλειας για ιατρικές συσκευές αντλιών έγχυσης φαρμάκου. Λαμβάνοντας υπόψη τα πρότυπα διαχείρισης ασφάλειας, όπως το ISO27001, τα μέτρα ασφάλειας αφορούν τέσσερις γενικές κατηγορίες: της Εμπιστευτικότητας (*Confidentiality*), της *Ακεραιότητας* (Integrity), της Δια-

θεσιμότητας (*Availability*) και της Αυθεντικοποίησης (*Authentication*). Οι κατηγορίες αυτές αφορούν τις διεθνώς αναγνωρισμένες πρακτικές για τον καθορισμό απαιτήσεων ασφάλειας.

Εμπιστευτικότητα

Η εμπιστευτικότητα αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένη αποκάλυψη τους. Ο τρόπος με τον οποίο οι πληροφορίες που αποθηκεύονται ή μεταδίδονται στο δίκτυο πρέπει να θεωρούνται έμπιστοι.

Κάποιος με φυσική πρόσβαση στη συσκευή πρέπει να μην μπορεί να έχει πρόσβαση στο υλικολογισμικό. Το υλικολογισμικό πρέπει να προστατεύεται και από υποκλοπή και όταν ταξιδεύει στα μέσα διασύνδεσης στο πλαίσιο μιας ρουτίνας ανανέωσης υλικολογισμικού για παράδειγμα (*firmware update*).

Τα ευαίσθητα προσωπικά δεδομένα που αποθηκεύονται ή επεξεργάζονται πρέπει να είναι κρυπτογραφημένα ώστε να αποφευχθεί η πρόσβαση σε αυτά από μη εξουσιοδοτημένους χρήστες δηλαδή να υπάρχει εμπιστευτικότητα κατά την αποθήκευση και επεξεργασία ευαίσθητων προσωπικών δεδομένων και στη συσκευή αλλά και στην ηλεκτρονική πλατφόρμα. Προφανώς, τα δεδομένα αυτά πρέπει να είναι κρυπτογραφημένα και κατά την μετάδοση τους μέσω δικτύου. Με βάση την ιδιωτικότητα, ο πάροχος των υπηρεσιών της συσκευής και οι εξωτερικοί χρήστες δεν πρέπει να έχουν πρόσβαση στα προσωπικά δεδομένα που αποθηκεύονται ή μεταδίδονται από αυτήν.

Τέλος, απαιτείται ένα κρυπτογραφικό κλειδί που να σχετίζεται με μοναδική συσκευή και να αποθηκεύεται με ασφαλές τρόπο σε αυτή ώστε να αποφευχθεί η υποκλοπή και η χρήση του από μη εξουσιοδοτημένους χρήστες.

Ακεραιότητα

Η ακεραιότητα αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένη μεταβολή, τροποποίηση ή διαγραφής τους, οι απαιτήσεις ακεραιότητας είναι αυτές που υπαγορεύουν τις πολιτικές που σχετίζονται με τον τρόπο με τον οποίο οι πληροφορίες θα μεταβάλλονται ανάλογα με την εξουσιοδότηση που παρέχεται.

Σχετικά με τη συσκευή πρέπει να λειτουργεί με βάση τον τύπο λειτουργίας που έχει οριστεί κάθε φορά για τον ασθενή και εντός του χρονικού πλαισίου. Σχετικοί έλεγχοι θα πρέπει να γίνουν στο λογισμικό και να προστατευτούν κατάλληλα από χρήστες που έχουν είτε φυσική πρόσβαση είτε λογική πρόσβαση στη συσκευή. Κατά την ανανέωση του λειτουργικού της συσκευής πρέπει να εξασφαλίζεται απόδειξη ότι το περιεχόμενο του δεν έχει αλλοιωθεί.

Σχετικά με τα ιατρικά δεδομένα, πρέπει να υπάρχει τρόπος απόδειξης ότι δεν έχουν μεταβληθεί και όταν αυτά στέλνονται στο δίκτυο να μένουν αμετάβλητα και να αφορούν όντως τον ασθενή με τον οποίο σχετίζεται η συσκευή. Οι παράμετροι λειτουργίας της συσκευής ορίζουν τον τρόπο έγχυσης, την ποσότητα του φαρμάκου κλπ. Υπάρχουν διεθνείς κανονισμοί οι οποίοι καθορίζουν το «ασφαλές» πεδίο τιμών των παραμέτρων αυτών, το οποίο δεν θα πρέπει να επηρεαστεί και να μεταβληθεί από οποιονδήποτε είτε με φυσική πρόσβαση στη συσκευή είτε απομακρυσμένα.

Διαθεσιμότητα

Η διαθεσιμότητα αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης στις πληροφορίες και στις υπηρεσίες της συσκευής χωρίς εμπόδια και καθυστερήσεις, οι απαιτήσεις διαθεσιμότητας είναι αυτές που υπαγορεύουν τις πολιτικές που σχετίζονται με τον τρόπο με

τον οποίο οι πληροφορίες και οι υπηρεσίες της συσκευής θα παραμένουν διαθέσιμες στους χρήστες ανάλογα με την εξουσιοδότηση που παρέχεται.

Η πιο σημαντική απαίτηση σχετικά με τη διαθεσιμότητα είναι οι ιατρικές συσκευές να είναι άμεσα και πάντα έτοιμες για λειτουργία καθώς οι θεραπείες μπορεί να υποβοηθούν κρίσιμα περιστατικά ασθενών. Γι'αυτόν τον λόγο, οι μηχανισμοί διαχείρισης ισχύος των συσκευών πρέπει να προστατεύονται από επιθέσεις εξάντλησης της μπαταρίας. Επίσης χρειάζονται μηχανισμοί ελαχιστοποίησης της κατανάλωσης ενέργειας και να απενεργοποιούνται τμήματα της συσκευής (CPU, *Communication modules*) όταν δεν χρησιμοποιούνται για να αυξάνεται η διάρκεια αυτονομίας της συσκευής. Τέλος, αν υπάρχει υλοποίηση κρυπτογράφησης, αυτή πρέπει να γίνεται γρήγορα και να απαιτεί όσο το δυνατόν λιγότερους πόρους.

Αυθεντικοποιήση

Η αυθεντικοποίηση αφορά την διαδικασία επιβεβαίωσης της ταυτότητας μιας οντότητας στο σύστημα και οι απαιτήσεις αυθεντικοποίησης σχετίζονται με τον τρόπο που μια οντότητα αυθεντικοποιείται προκειμένου να αποκτήσει πρόσβαση στο σύστημα και να εκτελέσει ενέργειες ανάλογα με τα δικαιώματα που κατέχει.

Η συσκευή πρέπει να υποστηρίζει έναν μηχανισμό ταυτοποίησης και αυθεντικοποίησής της (*device identification and authentication*), στον οποίον να λαμβάνονται υπόψη μοναδικά φυσικά χαρακτηριστικά της συσκευής. Διαφορετικά, θα είναι εύκολο για κακόβουλους χρήστες να υποκλέψουν την ταυτότητα μίας πραγματικής συσκευής (*identity replication, identity spoofing*) ή να υλοποιήσουν μία επίθεση ενδιάμεσου (*man-in-the-middle attack*). Πρέπει να υπάρχει διαβαθμισμένη αυθεντικοποίηση στους χρήστες και όσων αφορά την πρόσβαση στος φυσικές θύρες διαχείρισης της συσκευής (*debugging ports*), και όσων αφορά την χρήση της ηλεκτρονικής πλατφόρμας και των επιμέρους λειτουργιών της καθώς και στην ίδια συσκευή. Η ύπαρξη κωδικών διαφορετικών ανάλογα με τις λειτουργίες της συσκευής, καθώς και η λήξη της συνεδρίας (*session*) ύστερα από μεγάλο χρονικό διάστημα που η συσκευή είναι ανενεργή, είναι σημαντικά μέτρα για αποφυγή χρήσης της συσκευής από μη εξουσιοδοτημένους χρήστες. Η συσκευή πρέπει να αυθεντικοποιείται στο δίκτυο ώστε να αποφευχθεί η πιθανότητα να παρουσιαστεί μια άλλη συσκευή σαν έμπιστη στο σύστημα. Χρειάζεται να εξετάζονται τα διαπιστευτήρια των συστημάτων με τα οποία επικοινωνεί η συσκευή προτού αποστείλει οποιαδήποτε δεδομένα σε αυτά.

Κατά τον προγραμματισμό της συσκευής με βιβλιοθήκες θεραπειών πρέπει να αποδεικνύεται η αυθεντικότητα τους. Όσων αφορά τα δεδομένα από τις συσκευές πρέπει να αποδεικνύεται ότι αφορούν όντως την συσκευή και τον ασθενή για τους οποίους αναφέρονται. Τέλος, το λογισμικό διαχείρισης συσκευών θα πρέπει να είναι προσβάσιμο ως μεταγλωτισμένος κώδικας ή ως πηγαίος κώδικας, μόνο σε αυθεντικοποιημένους διαχειριστές του συστήματος.

4.2 Πειραματική αξιολόγηση ασφάλειας και προτεινόμενα μέτρα ασφάλειας - *case study*

4.2.1 Αξιολόγηση της ηλεκτρονικής πλατφόρμας του παρόχου των ιατρικών συσκευών

Ένα μεγάλο μέρος των τεστ που έγιναν για την εύρεση αδυναμιών του ολικού συστήματος αποτελεί η αξιολόγηση της ηλεκτρονικής πλατφόρμας του παρόχου, δηλαδή την εφαρμογή ιστού (*web application*)[Hasa19]. Ως βοήθεια για την οργανωμένη και ολοκληρωμένη ανάλυση ασφάλειας χρησιμοποιήθηκε ο οδηγός του οργανισμού OWASP (Open Web Application Security Project)[1]. Ο OWASP είναι ένας παγκόσμιος φιλανθρωπικός οργανισμός μη κερδοσκοπικού χαρακτήρα που επικεντρώνεται στη βελτίωση της ασφάλειας του λογισμικού. Σκοπός του *project* είναι να καταστεί η ασφάλεια του λογισμικού ορατή, έτσι ώστε τα άτομα και οι οργανώσεις να μπορούν να λαμβάνουν τεκμηριωμένες αποφάσεις. Έτσι παρέχει αμερόληπτες, πρακτικές πληροφορίες σχετικά με την ασφάλεια εφαρμογών σε ιδιώτες, εταιρείες, πανεπιστήμια, κυβερνητικές υπηρεσίες και άλλους οργανισμούς παγκοσμίως. Η προσέγγιση του OWASP είναι ανοικτή και συνεργατική αφού κάθε εμπειρογνώμονας ασφάλειας μπορεί να συμμετάσχει με την εμπειρία του στο έργο και πραγματοποιείται *brainstorming* πριν από τη σύνταξη των άρθρων, ώστε η ομάδα να μοιραστεί ιδέες και να αναπτύξει μια συλλογική εικόνα του έργου. Έχει δημιουργηθεί έτσι μια καθορισμένη μεθοδολογία. Γενικότερα, είναι σημαντικό να ακολουθείται μια μεθοδολογία για να δοκιμαστούν όσο είναι δυνατόν όλες οι γνωστές ευπάθειες.

Οι δοκιμές χωρίζονται σε δύο φάσεις. Η πρώτη φάση είναι η παθητική λειτουργία κατά την οποία ο μηχανικός ασφάλειας προσπαθεί να κατανοήσει τη λογική της εφαρμογής και τα μέρη της. Διάφορα εργαλεία μπορούν να χρησιμοποιηθούν για τη συλλογή πληροφοριών. Το πιο σημαντικό και απαραίτητο εργαλείο για τέτοιου είδους τεστ είναι ένας διακομιστής HTTP μεσολαβητής ο οποίος χρησιμοποιείται για την παρακολούθηση όλων των αιτήσεων HTTP και απαντήσεων. Στο τέλος αυτής της φάσης, ο ελεγκτής θα πρέπει να κατανοεί όλα τα σημεία πρόσβασης (πύλες) της εφαρμογής (π.χ. κεφαλίδες HTTP, παραμέτρους και *cookies*). Η δεύτερη φάση περιλαμβάνει την ενεργή ανάλυση δηλαδή μια σειρά από διάφορα τεστ για τον εντοπισμό ευπαθειών.

- Συλλογή πληροφοριών (*Information Gathering*)
- Δοκιμές διαχείρισης διαμόρφωσης και ανάπτυξης (*Configuration and Deployment Management Testing*)
- Δοκιμές διαχείρισης ταυτότητας (*Identity Management Testing*)
- Δοκιμές ελέγχου ταυτότητας (*Authentication Testing*)
- Εξέταση εξουσιοδότησης (*Authorization Testing*)
- Δοκιμές διαχείρισης συνόδων συνδέσεων (*Session Management Testing*)
- Έλεγχοι επικύρωσης τιμών εισόδου (*Input Validation Testing*)
- Χειρισμός σφαλμάτων (*Error Handling*)

[1] https://www.owasp.org/index.php/Main_Page

- Κρυπτογραφία (*Cryptography*)
- Δοκιμές επιχειρηματικής λογικής των εφαρμογών (*Business Logic Testing*)
- Δοκιμές επιθέσεων από πλευράς του πελάτη (*Client Side Testing*)

Σχετικά με το πρώτο μέρος των δοκιμών, την συλλογή πληροφοριών δηλαδή, έγινε το λεγόμενο *Web Server Fingerprint*. Η αποτύπωση του τύπου του διακομιστή είναι πολύ σημαντική καθώς υπάρχουν πολλοί και διαφορετικοί προμηθευτές διακομιστών ιστού στην αγορά σήμερα. Η γνώση της έκδοσης και του τύπου ενός διαδικτυακού εξυπηρετητή που λειτουργεί επιτρέπει στους δοκιμαστές να προσδιορίζουν γνωστά σημεία ευπάθειας και τα κατάλληλα εκμεταλλεύσιμα που θα χρησιμοποιήθουν κατά τη διάρκεια των δοκιμών. Ένα σημαντικό βήμα στη δοκιμή για τις ευπάθειες σε εφαρμογές διαδικτύου είναι να βρεθούν ποιες συγκεκριμένες εφαρμογές φιλοξενούνται σε έναν διακομιστή ιστού καθώς και να γίνει κατανοητή η αναπτυχθείσα διαμόρφωση του διακομιστή που φιλοξενεί την εφαρμογή ιστού.

Πολλές εφαρμογές έχουν γνωστές ευπάθειες και γνωστές στρατηγικές επίθεσης που μπορούν να αξιοποιηθούν από επιτιθέμενους προκειμένου να αποκτήσουν απομακρυσμένο έλεγχο ή να εκμεταλλευτούν δεδομένα. Επιπλέον, πολλές εφαρμογές είναι συχνά εσφαλμένες ή μη ενημερωμένες, λόγω της αντίληψης ότι χρησιμοποιούνται μόνο ”εσωτερικά” και ως εκ τούτου δεν υπάρχει απειλή.

Σε αυτό το στάδιο βρέθηκε ότι η έκδοση της βάσης δεδομένων που χρησιμοποιείται είναι παλαιότερη, μη ενημερωμένη έκδοση, για την οποία υπάρχουν γνωστές στο κοινό δημοσιευμένες ευπάθειες που μπορεί κάποιος εύκολα να βρει στο Διαδίκτυο στους καταλόγους με τα CVEs (Common Vulnerabilities and Exposures) [2] και αναλόγως να τις χρησιμοποιήσει για επιθέσεις στην εφαρμογή και τον οργανισμό. Η γνώση του τύπου *web framework* μπορεί επίσης να προσφέρει ένα μεγάλο πλεονέκτημα και να οδηγήσει στην εύρεση γνωστών τρωτών σημείων της έκδοσης που χρησιμοποιήθηκε.

Η απαρίθμηση της εφαρμογής και των σημείων εισόδου της εφαρμογής είναι ένας βασικός πρόδρομος προτού να διεξαχθούν ενδελεχείς έλεγχοι, καθώς επιτρέπει στον εξεταστή να εντοπίσει πιθανές περιοχές αδυναμίας. Στόχος της δοκιμής είναι η κατανόηση του τρόπου με τον οποίο διαμορφώνονται τα αιτήματα και οι τυπικές απαντήσεις από την εφαρμογή.

Αφού αναγνωρίστηκε πλήρως η υποδομή της πλατφόρμας, έγινε επικύρωση των ρόλων των χρηστών του συστήματος, καθώς και αν υπάρχουν οι κατάλληλοι έλεγχοι πρόσβασης σε λειτουργίες και δεδομένα.

Βεβαιώθηκε ότι οι απαιτήσεις ταυτότητας για την εγγραφή χρήστη είναι ευθυγραμμισμένες με τις απαιτήσεις των επιχείρησης και της ασφάλειας. Επαληθεύθηκε η διαδικασία εγγραφής νέου χρήστη και ποιου ρόλου χρήστες έχουν όντως το δικαίωμα να δημιουργούν νέους χρήστες και τι ρόλου.

Συχνά, οι εφαρμογές ιστού αποκαλύπτουν πότε υπάρχει ένα όνομα χρήστη στο σύστημα, είτε ως συνέπεια κακής διαμόρφωσης είτε ως σχεδιαστική απόφαση. Για παράδειγμα, μερικές φορές, όταν υποβάλλονται λάθος διαπιστευτήρια (*credentials*), επιστρέφεται ως απάντηση ένα μήνυμα που αναφέρει ότι είτε το όνομα χρήστη υπάρχει στο σύστημα είτε ο παρεχόμενος κωδικός πρόσβασης είναι λάθος. Οι πληροφορίες που λαμβάνονται μπορούν να χρησιμοποιηθούν από έναν εισβολέα για να αποκτήσουν μια λίστα χρηστών στο σύστημα. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για να επιτεθούν στην εφαρμογή ιστού. Έτσι, επιβεβαιώθηκε ότι δεν είναι δυνατή η συλλογή ενός συνόλου έγκυρων ονομάτων χρηστών με την αλληλεπίδραση με το μηχανισμό ελέγχου ταυτότητας της εφαρμογής (*user enumeration*

[2] https://cve.mitre.org/

or user fingerprinting). Στη συνέχεια ελέγχθηκε ότι έχει γίνει υλοποίηση μηχανισμού αντιμετώπισης *brute-force* επιθέσεων, δηλαδή ότι δεν είναι δυνατόν ένας επιτιθέμενος έχοντας γνώση ενός έγκυρου ονόματος χρήστη (*username*) να βρει τον αντίστοιχο κωδικό πρόσβασης.

Στη συνέχεια, ελέγχθηκε αν όλη η επικοινωνία με τον διακομιστή γίνεται πάνω από ασφαλές κανάλι, δηλαδή γίνεται χρήση SSL επικοινωνίας και τα διαπιστευτήρια ή ευαίσθητα δεδομένα δεν στέλνονται ως καθαρό κείμενο (*clear text*) αναγνώσιμο από άνθρωπο. Σε αυτό το σημείο ελέγχθηκε με αυτόματα εργαλεία αν η επικοινωνία με τον διακομιστή μέσω SSL πάσχει από γνωστές ευπάθειες και δεν βρέθηκε κάποιο λάθος.

Επιπρόσθετα, αξιολογήθηκε η υλοποίηση της λειτουργίας αλλαγής κωδικού (*change password functionality*), η λειτουργία ανάκτησης πρόσβασης στις περιπτώσεις που κάποιος έχει ξεχάσει τον κωδικό (*forgot password functionality*) ή αν έχει απενεργοποιηθεί ο λογαριασμός του (*locked account*). Γενικά, δεν βρέθηκε κάποιος τρόπος με τον οποίο κάποιος να προσπεράσει τον μηχανισμό αυθεντικοποίησης και να πάρει πρόσβαση σε δεδομένα για τα οποία δεν έχει εξουσιοδότηση. Η πολιτική δημιουργίας κωδικού ήταν σωστά επιλεγμένη (απαιτήσεις για το μήκος, την πολυπλοκότητα, την επαναχρησιμοποίηση και τη γήρανση των κωδικών) αποκλείοντας το γεγονός κάποιος νόμιμος χρήστης να θέσει έναν αδύνατο κωδικό πρόσβασης (*weak password*) με αποτέλεσμα να είναι δύσκολο και πολύπλοκο από μαθηματικής άποψης κάποιος κακόβουλος να τον βρει ή να τον μαντέψει.

Ένα άλλο συχνό πρόβλημα είναι η αποθήκευση τοπικά σε έναν υπολογιστή, δεδομένων που σχετίζονται με την εφαρμογή. Τα προγράμματα περιήγησης μπορούν να αποθηκεύουν πληροφορίες για σκοπούς αποθήκευσης και ιστορικού και για τη βελτίωση της απόδοσης, έτσι ώστε οι πληροφορίες που εμφανίζονται στο παρελθόν να μην χρειάζεται να φορτωθούν ξανά. Εάν εμφανίζονται ευαίσθητες πληροφορίες στον χρήστη (όπως η διεύθυνση, ο αριθμός κοινωνικής ασφάλισης ή το όνομα χρήστη), τότε αυτές οι πληροφορίες θα μπορούσαν να αποθηκευτούν για σκοπούς προσωρινής αποθήκευσης ή ιστορικού και επομένως να ανακτηθούν μέσω της εξέτασης της προσωρινής μνήμης του προγράμματος περιήγησης πατώντας το πλήκτρο ”Πίσω” του προγράμματος περιήγησης. Επομένως έγιναν αντίστοιχοι έλεγχοι για την επιβεβαίωση ότι δεν υπάρχει δυνατότητα διαρροής διαπιστευτηρίων και ευαίσθητων δεδομένων σε τρίτους μέσω της προσωρινής αποθήκευσης τους.

Ακολούθησαν έλεγχοι για παραβίαση του σχήματος εξουσιοδότησης και για την εύρεση ευπαθειών αύξησης των προνομίων (*privilege escalation*). Για κάθε συγκεκριμένο ρόλο που κατέχει ο δοκιμαστής κατά τη διάρκεια της αξιολόγησης, για κάθε λειτουργία και αίτημα εκτέλεσης της εφαρμογής κατά τη διάρκεια της φάσης μετά την αυθεντικοποίηση, είναι απαραίτητο να επαληθεύεται αν είναι δυνατή η πρόσβαση σε αυτόν τον πόρο ακόμα και αν ο χρήστης δεν έχει πιστοποιηθεί. Αν είναι πιθανό κάποιος χρήστης να έχει πρόσβαση σε δεδομένα άλλων χρηστών που δεν θα έπρεπε ή αν είναι δυνατή η πρόσβαση σε πόρους μετά την αποσύνδεση ή ακόμα και αν είναι δυνατή η πρόσβαση σε λειτουργίες και πόρους που πρέπει να είναι προσβάσιμοι σε ένα χρήστη που κατέχει διαφορετικό ρόλο με περισσότερα προνόμια. Για παράδειγμα, στην εφαρμογή που εξετάστηκε, ελέγχθηκε αν είναι δυνατό ένας απλός χρήστης να κάνει μια ενέργεια που κανονικά μπορεί μόνο ένας χρήστης διαχειριστής (*admin user*).

Οι μη ασφαλείς αναφορές άμεσων αντικειμένων (*insecure direct object reference*) ως ευπάθεια εμφανίζονται όταν μια εφαρμογή παρέχει άμεση πρόσβαση σε αντικείμενα βάσει εισόδου που παρέχεται από τον χρήστη. Ως αποτέλεσμα αυτής της ευπάθειας, οι επιτιθέμενοι μπορούν να παρακάμψουν την εξουσιοδότηση και να αποκτήσουν άμεση πρόσβαση σε πόρους του συστήματος, για παράδειγμα αρχεία βάσεων δεδομένων, τροποποιώντας την τιμή εισόδου. Αυτό μπορεί να συμβεί αν δεν γίνονται επαρκείς έλεγχοι εξουσιοδότησης.

Συγκεκριμένα στην εφαρμογή του αντικειμένου μελέτης μπορούσε να γίνει μετατρέποντας σειριοποιημένα δεδομένα (*serialized data*) που στέλνονταν σαν μέρος αιτημάτων σε κάποια σημεία της εφαρμογής.

Σε επόμενο στάδιο, ελέγχθηκε πλήρως η υλοποίηση σχετικά με τη διαχείριση συνόδων συνδέσεων (*session management*) για ευπάθειες τύπου *session fixation* (επίθεση κατά την οποία μπορεί κάποιος να ορίσει το cookie ενός νόμιμου χρήστη με μια γνωστή τιμή πριν την διαδικασία αυθεντικοποιήσης και αν αυτή δεν αλλάξει να έχει πρόσβαση στο λογαριασμό του) ή για την έλλειψη σημαντικών cookie χαρακτηριστικών όπως είναι το *"secure flag"* και το *"HttpOnly flag"* όπως αυτά ορίζονται κανονικά στο πεδίο της παραμέτρου *set-cookie* των HTTP αιτημάτων. Επίσης, συλλέχθηκαν πολλά *cookies* για να μπορεί να εφαρμοστεί αντίστροφη μηχανική στον αλγόριθμο με τον οποίον αυτά παράγονται και να εξακριβωθεί αν όντως δημιουργούνται με ασφαλές, τυχαίο τρόπο και δεν μπορούν να προβλεφθούν από επιτιθέμενους. Τα cookies είχαν εύλογο χρόνο λήξης ορισμένο, δηλαδή έπαυαν να είναι έγκυρα μετά από συγκεκριμένο χρονικό διάστημα καθώς και μετά από πολλή ώρα έλλειψης δραστηριότητας του χρήστη και δεν μπορούσαν να επαναχρησιμοποιηθούν. Τέλος, υπήρχε λειτουργία αποσύνδεσης, και ήταν σωστά υλοποιημένη ώστε να ακυρώνονται τα αντίστοιχα *session cookies* της σύνδεσης από τη μεριά του διακομιστή και να θεωρούνται μη έγκυρα.

Εν συνεχεία, επιβεβαιώθηκε ότι δεν είναι δυνατό να εφαρμοστεί το CSRF που είναι μια επίθεση που αναγκάζει έναν τελικό χρήστη να εκτελέσει ανεπιθύμητες ενέργειες σε μια εφαρμογή στο διαδίκτυο στην οποία είναι ήδη πιστοποιημένος. Με λίγη βοήθεια της κοινωνικής μηχανικής (*social engineering*) (όπως αποστολή συνδέσμου μέσω ηλεκτρονικού ταχυδρομείου ή συνομιλίας), ένας εισβολέας μπορεί να αναγκάσει τους χρήστες μιας διαδικτυακής εφαρμογής να εκτελέσουν ενέργειες της επιλογής του εισβολέα εκμεταλλευόμενος την έλλειψη υλοποίησης μηχανισμού αποκλεισμού CSRF.

Ακολούθησαν έλεγχοι για επικύρωση των τιμών εισόδου. Οι πιο συνηθισμένες αδυναμίες ασφάλειας εφαρμογών ιστού ξεκινούν από την αποτυχία να επικυρωθεί σωστά η είσοδος που προέρχεται από τη μεριά του ππελάτη (*client side*) ή από τον διακομιστή (*server side*) πριν αυτή χρησιμοποιηθεί. Αυτή η αδυναμία οδηγεί σε σχεδόν όλες τις σημαντικές ευπάθειες στις εφαρμογές ιστού, όπως είναι το XSS, το SQL *injection*, επιθέσεις συστήματος αρχείων (*file system attacks*), όπως είναι *path traversal* και *file inclusion*, καθώς και ευπάθειες υπερχείλισης του *buffer* (*buffer overflow*). Τα δεδομένα από μια εξωτερική οντότητα ή πελάτη δεν πρέπει ποτέ να είναι αξιόπιστα αλλά να ελέγχονται πλήρως, διότι μπορούν να αλλοιωθούν αυθαίρετα από έναν εισβολέα.

Παρουσιάζονται κάποιες σημαντικές κατηγορίες επιθέσεων λόγω έλλειψης επικύρωσης τιμών εισόδου που δοκιμάστηκαν αλλά δεν ήταν επιτυχημένες:

- XSS (Stored XSS, DOM XSS)
- SQL Injection
- XML injection
- Path traversal
- Server Side Injection

Μια σημαντική πτυχή της ανάπτυξης ασφαλών εφαρμογών είναι η αποφυγή διαρροής πληροφοριών λόγω κακής διαχείρισης σφαλμάτων. Τα μηνύματα σφάλματος δίνουν σε έναν εισβολέα μεγάλη εικόνα για την εσωτερική λειτουργία μιας εφαρμογής. Ο σκοπός της αναθεώρησης του κώδικα χειρισμού σφαλμάτων είναι να διασφαλιστεί ότι όταν η εφαρμογή

αποτυγχάνει κάτω από όλες τις πιθανές συνθήκες σφάλματος, αναμενόμενες και μη αναμενόμενες, δεν εμφανίζονται ευαίσθητες πληροφορίες στο χρήστη.

Μια κατηγορία ευπαθειών είναι τα επιχειρησιακής λογικής (*business logic*) λάθη. Τα αυτοματοποιημένα εργαλεία δυσκολεύονται να κατανοήσουν το πλαίσιο και τον σκοπό μιας εφαρμογής, επομένως εναπόκειται στους μηχανικούς ασφάλειας να πραγματοποιήσουν ελέγχους για να βρουν λογικά λάθη που έχουν κάνει αυτοί που ανέπτυξαν το λογισμικό.

Στις ιατρικές εφαρμογές, υπάρχουν αναγκαστικά αποθηκευμένα πολλά ευαίσθητα ιατρικά δεδομένα, που είναι συσχετισμένα με ασθενείς και αποτελούν πολύτιμο στόχο για τους υποκλέπτες δεδομένων που τα πουλάνε σε ασφαλιστικές ή σε όποιους οργανισμούς ενδιαφέρονται, για το προσωπικό οικονομικό όφελος τους. Οπότε, έπρεπε να ελεγχθεί αν αυτά τα δεδομένα αποθηκεύονται στη βάση δεδομένων με ασφαλές τρόπο. Ύστερα από ανάλογους ελέγχους διαπιστώθηκε ότι όντως όσα δεδομένα αφορούν ασθενείς ήταν κρυπτογραφημένα και με ασφαλές αλγόριθμο. Έτσι, και να βρει κάποιος πρόσβαση στη βάση δεδομένων δεν θα μπορεί να καταλάβει τα δεδομένα.

Κατά την αναζήτηση των δεδομένων στη βάση όμως, βρέθηκε ότι τα συνθηματικά των χρηστών που απαιτούνται για τη διαδικασία ελέγχου ταυτότητας αποθηκεύονται σε ακατάλληλη μορφή *hash*. Λεπτομερέστερα, οι *hashed* τιμές δημιουργήθηκαν χωρίς χρήση *salt*. Στην κρυπτογραφία, ένα *salt* είναι μια τυχαία τιμή που χρησιμοποιείται ως πρόσθετη είσοδος σε μια λειτουργία μονής κατεύθυνσης που κάνει *hashed* τα δεδομένα (έναν κωδικό πρόσβασης ή μια φράση πρόσβασης). Τα *salt* χρησιμοποιούνται για την προστασία των κωδικών πρόσβασης κατά τη αποθήκευση και ένα νέο *salt* παράγεται για κάθε κωδικό πρόσβασης. Η τεχνική χρήσης *salt* χρησιμοποιείται ως μέτρο προστασίας ενάντια σε επιθέσεις κατακερματισμού.

Το γεγονός ότι οι κωδικοί πρόσβασης δεν έχουν *salt*, δίνει στον επιτιθέμενο τη δυνατότητα να χρησιμοποιεί πίνακες αναζήτησης με υπολογισμένα *hashes* για να επιταχύνει τη διαδικασία εύρεσης των κωδικών από τα *hashes*. Επιπλέον, η έλλειψη *salt* έχει ως αποτέλεσμα χρήστες με πανομοιότυπους κωδικούς πρόσβασης, να έχουν ταυτόσημα *hashes* στη βάση δεδομένων. Με αυτόν τον τρόπο βρέθηκε και η αδυναμία στην περίπτωση του αντικειμένου μελέτης μας. Ένας αντίπαλος που έχει πρόσβαση στα δεδομένα της βάσης δεδομένων μπορεί να είναι σε θέση να σπάσει εύκολα και να ανακτήσει τους αρχικούς κωδικούς πρόσβασης των χρηστών. Στην περίπτωση που οι κωδικοί επαναχρησιμοποιούνται σε εφαρμογές / υπηρεσίες τρίτων, υπάρχει επίσης ο κίνδυνος ο επιτιθέμενος να αποκτήσει πρόσβαση σε αυτές τις υπηρεσίες.

4.2.2 Αξιολόγηση της επικοινωνίας μεταξύ των ιατρικών συσκευών και του διακομιστή

Σχετικά με την επικοινωνία των ιατρικών συσκευών με τον διακομιστή (*web server*) υπάρχουν δύο τρόποι, ο ένας είναι μέσω GSM επικοινωνίας και ο άλλος μέσω Wi-fi. Είναι σημαντικό να σημειωθεί ότι ο διακομιστής δεν στέλνει δεδομένα στις ιατρικές συσκευές για λόγους ασφάλειας. Μόνο λαμβάνει. Έτσι αποφεύγονται οποιουδήποτε είδους επιθέσεις όπως είναι η απομακρυσμένη εκτέλεση κώδικα (*remote code execution*) στις συσκευές που θα μπορούσε να θέσει σε κίνδυνο την συνολική λειτουργία της συσκευής χωρίς να χρειάζεται καν ο επιτιθέμενος να βρίσκεται φυσικά στον ίδιο χώρο. Τέτοιες επιθέσεις θα μπορούσαν να πραγματοποιηθούν με την εκμετάλλευση τύπου ευπαθειών υπερχείλισης όπως είναι το *buffer overflow*, *stack overflow* και *heap overflow* στον κώδικα της συσκευής. Αυτό σίγουρα μειώνει τις δυνατότητες για λειτουργίες και ευκολίες που θα μπορούσαν να υπάρχουν, αλλά εξασφαλίζει περισσότερη ασφάλεια.

Τα δεδομένα που στέλνουν οι συσκευές στον διακομιστή είναι κυρίως στατιστικά στοι-

χεία, πληροφορίες για το πότε γίνεται έγχυση (αν υπάρχει σύνδεση σε ζωντανό χρόνο) ποια θεραπεία δίνεται και τυχόν προειδοποιήσεις (*alarms*) που ξεκινούν είτε από τεχνικά σφάλματα στις συσκευές είτε από τις απαντήσεις του ασθενή σε διάφορες ερωτήσεις σχετικά με την κατάσταση του. Υπάρχει δηλαδή μια σειρά από ερωτήσεις που μπορεί ο ασθενής να απαντήσει ανάλογα με το πώς νιώθει (αδιαθεσία, πόνος, κ.ά.).

Η επικοινωνία των συσκευών με τον διακομιστή είναι κρυπτογραφημένη. Σαν επιπλέον μέτρο ασφάλειας έχει υλοποιηθεί αυθεντικοποιήση πελάτη (*client authentication*) για να μπορεί ο διακομιστής να διαβεβαιώνει την αυθεντικότητα των ιατρικών συσκευών.

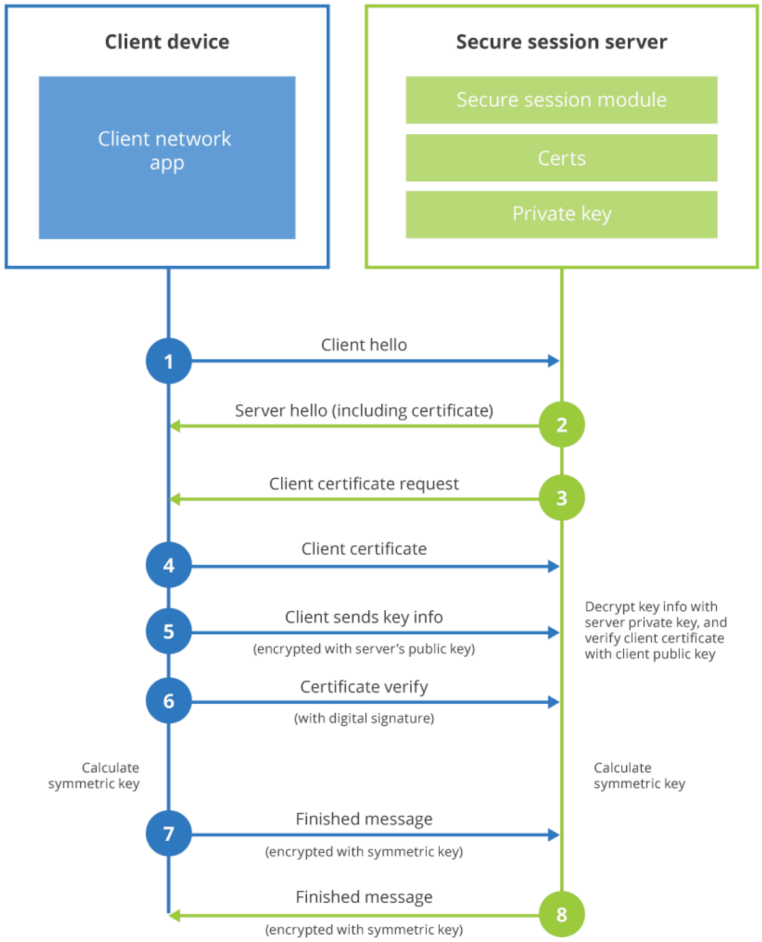
Σε μια παραδοσιακή χειραψία TLS (TLS *handshake*), ο πελάτης επικυρώνει τον διακομιστή (*server*) και ο διακομιστής δεν γνωρίζει πολλά για τον πελάτη (*client*). Όμως, όταν εφαρμόζεται TLS με πιστοποίηση πελάτη (*client authentication*), ο διακομιστής επιβεβαιώνει επιπλέον εάν ο πελάτης που συνδέεται με αυτό είναι ο εξουσιοδοτημένος να συνδεθεί. Ο έλεγχος ταυτότητας πελάτη TLS είναι χρήσιμος ειδικά σε περιπτώσεις όπου ένας διακομιστής παρακολουθεί πολλούς πελάτες, όπως σε IoT εφαρμογές όπου ανταλλάσσονται ασφαλείς πληροφορίες. Στο αντικείμενο μελέτη μας, εκδίδεται ένα μοναδικό πιστοποιητικό πελάτη ανά συσκευή αποκλείοντας έτσι συνδέσεις όπου ο πελάτης δεν παρουσιάζει πιστοποιητικό υπογεγραμμένο από την αρχή πιστοποίησης της εταιρείας.

Τα πιστοποιητικά πελατών προσφέρουν ένα επίπεδο ασφάλειας που δεν μπορούν να παρέχουν τα κλειδιά API. Εάν ένα κλειδί API γίνει *compromised* μπορεί να επαναχρησιμοποιηθεί για να άλλα έγκυρα αξιόπιστα αιτήματα στην υποδομή *backend*. Ωστόσο, το ιδιωτικό κλειδί του πιστοποιητικού πελάτη χρησιμοποιείται για τη δημιουργία ψηφιακής υπογραφής σε κάθε σύνδεση TLS και έτσι ακόμα και αν το πιστοποιητικό εκτεθεί εν μέσω σύνδεσης, δεν είναι δυνατά νέα αιτήματα με αυτό.

Σε μια χειραψία με έλεγχο ταυτότητας πελάτη TLS, ο διακομιστής αναμένει από τον πελάτη να παρουσιάσει ένα πιστοποιητικό και αποστέλλει στον πελάτη ένα αίτημα πιστοποιητικού πελάτη μαζί με το *hello server*. Στη συνέχεια, κατά την ανταλλαγή κλειδιών ο πελάτης αποστέλλει επίσης το πιστοποιητικό του. Στη συνέχεια, το πιστοποιητικό πελάτη χρησιμοποιείται για την υπογραφή της χειραψίας TLS και η ψηφιακή υπογραφή αποστέλλεται στον διακομιστή για επαλήθευση. Όλη η διαδικασία παρουσιάζεται στο σχήμα 4.4:

Για να καταλήξουμε στο συμπέρασμα ότι η επικοινωνία των συσκευών με τον διακομιστή μέσω Wi-fi εξασφαλίζει όντως την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα του συστήματος, πρέπει να ελεγχθούν κάποιοι παράγοντες όπως για παράδειγμα η ισχύς του εκδότη του πιστοποιητικού, τους αλγορίθμους που υποστηρίζονται για υπογραφή, λεπτομέρειες του πρωτοκόλλου, σουίτες κρυπτογράφησης και αν είναι δυνατόν να πετύχουν γνωστές TLS επιθέσεις όπως είναι οι POODLE (*Padding Oracle On Downgraded Legacy Encryption*), BEAST (*Browser Exploit Against SSL/TLS*), CRIME (*Compression Ratio Info-leak Made Easy*), BREACH (*Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext*).

Ένας διακομιστής με δυνατότητα SSL ακολουθεί τα παρακάτω βήματα για να πιστοποιήσει την ταυτότητα ενός χρήστη. Ελέγχει αν το δημόσιο κλειδί του χρήστη επικυρώνει την ψηφιακή υπογραφή του χρήστη. Αν ναι, ο διακομιστής έχει διαπιστώσει ότι το δημόσιο κλειδί που δηλώνεται ότι ανήκει στη συσκευή αντιστοιχεί στο ιδιωτικό κλειδί που χρησιμοποιείται για τη δημιουργία της υπογραφής και ότι τα δεδομένα δεν έχουν αλλοιωθεί από τότε που υπογράφηκε. Σε αυτό το σημείο, ωστόσο, η σύνδεση μεταξύ του δημόσιου κλειδιού και του *Domain Name* που καθορίζεται στο πιστοποιητικό δεν έχει ακόμη καθοριστεί. Το πιστοποιητικό ενδέχεται να έχει δημιουργηθεί από κάποιον που επιχειρεί να υποδηλώσει τον χρήστη. Για να επικυρώσετε τη σύνδεση μεταξύ του δημόσιου κλειδιού και του *Domain Name*, ο διακομιστής θα πρέπει να ελέγξει αν η σημερινή ημερομηνία είναι εντός της περιόδου ισχύος.



Σχήμα 4.4: Διαδικασία Client Authentication

Σαν επόμενο βήμα ελέγχει αν η CA (Certificate Authority) που έχει εκδώσει το πιστοποιητικό είναι αξιόπιστη Αρχή Πιστοποιητικών (CA). Κάθε διακομιστής με δυνατότητα SSL διατηρεί μια λίστα αξιόπιστων πιστοποιητικών CA, η οποία καθορίζει ποια πιστοποιητικά δέχεται ο διακομιστής. Εάν η διεύθυνση Domain Name της CA που εκδίδει αντιστοιχεί στο Domain Name μιας από τη λίστα αξιόπιστων CA. Εάν η CA που εκδίδει δεν είναι στη λίστα, ο πελάτης δεν έχει πιστοποιηθεί, εκτός εάν ο διακομιστής μπορεί να επαληθεύσει μια αλυσίδα πιστοποιητικών που τελειώνει σε μια CA που είναι αξιόπιστη ή μη αξιόπιστη στους οργανισμούς τους ελέγχοντας τις λίστες των πιστοποιητικών CA που διατηρούν οι πελάτες και οι διακομιστές. Σε αυτή την περίπτωση ο διακομιστής χρησιμοποιεί το δημόσιο κλειδί από το πιστοποιητικό της CA (το οποίο βρήκε στη λίστα με αξιόπιστες CA στο προηγούμενο βήμα) για να επικυρώσει την ψηφιακή υπογραφή της CA στο πιστοποιητικό που παρουσιάζεται. Εάν οι πληροφορίες στο πιστοποιητικό έχουν αλλάξει από τότε που υπογράφηκε από την CA ή εάν το δημόσιο κλειδί στο πιστοποιητικό της CA δεν αντιστοιχεί στο ιδιωτικό κλειδί που χρησιμοποιείται από την CA για την υπογραφή του πιστοποιητικού, ο διακομιστής δεν θα πιστοποιήσει την ταυτότητα του χρήστη . Σε αυτό το σημείο, το πρωτόκολλο SSL επιτρέπει στον διακομιστή να εξετάσει τον πελάτη που έχει πιστοποιηθεί και να συνεχίσει τη σύνδεση.

Για τον έλεγχο όλων των παραπάνω βοήθησε το *script* testssl.sh που έχει αναπτυχθεί για αυτόν τον σκοπό. Ο διακομιστής και στις δύο θύρες που ακούει (*web application* και για

την επικοινωνία με τις συσκευές) υποστηρίζει μέχρι το TLS v1.2 και δεν πάσχει από κάποια ευπάθεια.

Στη συνέχεια της πειραματικής ανάλυσης, λόγω πρόσβασης στον εκτελέσιμο κώδικα της εφαρμογής της ηλεκτρονικής πλατφόρμας, έγινε *decompilation* του με αποτέλεσμα ένα κώδικα πολύ κοντά στον κώδικα που αρχικά οι προγραμματιστές της εφαρμογής είχαν γράψει. Παρατηρώντας και αναλύοντας τον πηγαίο κώδικα (*source code audit*) εντοπίστηκε και αναλύθηκε το πρωτόκολλο επικοινωνίας των ιατρικών συσκευών με το διακομιστή. Για την υλοποίηση της επικοινωνίας δεν χρησιμοποιήθηκε το HTTP πρωτόκολλο αλλά χρησιμοποιήθηκε ένα δυαδικής μορφής δικό τους (*custom*) πρωτόκολλο που μπορεί να μεταβιβάσει αιτήματα διακομιστή μεσολάβησης από ένα διακομιστή ιστού σε ένα διακομιστή εφαρμογών που βρίσκεται πίσω από τον διακομιστή ιστού.

Η συσκευή δεν έχει καμία πληροφορία σχετικά με το ποιον ασθενή είναι συσχετισμένη, αλλά αυτό μπορεί ορθά να βρεθεί μόνο στην ηλεκτρονική πλατφόρμα. Επίσης αυτό σημαίνει ότι όσο ευπαθής και να είναι η επικοινωνία των συσκευών με τον διακομιστή, από τη στιγμή που δεν μεταφέρεται οποιαδήποτε πληροφορία που να συσχετίζει τα ιατρικά δεδομένα με κάποιον ασθενή, δεν υπάρχει κίνδυνος για υποκλοπή δεδομένων μέσω παραβίασης του δικτύου.

Παρατηρήθηκε κατά την επικοινωνία της συσκευής με το διακομιστή, ότι γίνεται κάποιου είδους αυθεντικοποίηση. Εντοπίστηκε πρόβλημα στη διαδικασία αυθεντικοποίησης της συσκευής στον διακομιστή. Συγκεκριμένα, είναι δυνατό να συμβεί επιτυχημένη επίθεση *identity spoofing* στην οποία θα αναφερθούμε παρακάτω.

Κάθε συσκευή χαρακτηρίζεται από έναν μοναδικό σειριακό αριθμό (*unique identifier*) για να διακρίνεται από τις υπόλοιπες. Κατά τη διαδικασία της αυθεντικοποίησης που προείπαμε, η κάθε συσκευή έστελνε τον *unique identifier* της και αναλόγως αν ο διακομιστής μπορούσε να βρει εγγραφή στη βάση με αυτόν τον αριθμό αναλόγως δεχόταν την σύνδεση με τη συσκευή ή όχι.

Εδώ υπήρχαν τρία λογικά λάθη. Αρχικά, οι *unique identifiers* δεν είχαν παραχθεί με τυχαιότητα, και αυτό τους καθιστά εύκολα προβλέψιμους. Το ότι δεν είχαν την απαραίτητη τυχαιότητα, επιτρέπει το ενδεχόμενο κάποιος επιτιθέμενος να βρει προβλέποντας έγκυρους σειριακούς αριθμούς των συσκευών που είναι εγγεγραμμένοι στη βάση δεδομένων.

Επιπρόσθετα, παρατηρήθηκε ότι αν αποσταλεί σειριακός αριθμός που δεν είναι εγγεγραμμένος στην ηλεκτρονική πλατφόρμα, Ο διακομιστής αποκρίνεται με διαφορετικό αναγνωριστικό εντολής εάν η συσκευή είναι καταχωρημένη σε οργανισμούς της εφαρμογής ή όχι. Έτσι, προβλέποντας και δοκιμάζοντας διάφορους σειριακούς αριθμούς για να γίνει σύνδεση στον διακομιστή, είναι δυνατή η απαρίθμηση των εγγεγραμμένων συσκευών και η περαιτέρω εκμετάλλευση της ευπάθειας κατά την αυθεντικοποίηση.

Ύστερα από δοκιμές, έγινε επιτυχημένη επίθεση *identity spoofing*. Δηλαδή, αν κάποιος κακόβουλος επηρεάσει την επικοινωνία της συσκευής με τον διακομιστή και αλλάξει τον σειριακό αριθμό της συσκευής που αποστέλλεται, ο διακομιστής θα νομίζει ότι τα στέλνει άλλη συσκευή από αυτή που πραγματικά στέλνει τα δεδομένα. Ένας εισβολέας με φυσική πρόσβαση σε μια συσκευή μπορεί να εξαγάγει το ιδιωτικό κλειδί που χρησιμοποιήθηκε για τη χειραψία TLS για να ξεκινήσει ένα ασφαλές κανάλι επικοινωνίας και έπειτα να στείλει μηνύματα χρησιμοποιώντας ψευδή σειριακούς αριθμούς. Από τη στιγμή που κάθε συσκευή είναι συσχετισμένη με έναν ασθενή κάθε φορά στην ηλεκτρονική πλατφόρμα, υπάρχει ο κίνδυνος απώλειας ανθρώπινης ζωής καθώς το ιατρικό προσωπικό θα νομίζει ότι η θεραπεία χορηγείται στο σωστό πρόσωπο. Η ευπάθεια που βρέθηκε σε συνδυασμό με το γεγονός ότι οι σειριακοί αριθμοί είναι εύκολα προβλέψιμοι καθιστούν το σύστημα αυθεντικοποίησης ανασφαλές.

Για την αντιμετώπιση των παραπάνω έπρεπε οι σειριακοί αριθμοί είναι παραγόμενοι με σωστή τυχαιότητα εξασφαλίζοντας το να μην είναι προβλέψιμοι και να μην αποτελούν το χαρακτηριστικό που απαιτείται για τη διαδικασία της αυθεντικοποιήσης. Κάθε φορά που δημιουργείται μια νέα σύνδεση, ο διακομιστής πρέπει να ανακτά το πιστοποιητικό της συσκευής και να ελέγχει διασταυρωμένα τον παρεχόμενο αριθμό σειράς εντός της κεφαλίδας του μηνύματος για να επικυρώσει την αυθεντικότητα του σειριακού αριθμού. Τέλος, έτσι θα λυθεί και το πρόβλημα της απαρίθμησης των εγγεγραμμένων συσκευών.

4.2.3 Αξιολόγηση του μηχανισμού φόρτωσης των βιβλιοθηκών

Από τη στιγμή που ο κατασκευαστής επέλεξε οι συσκευές να μην δέχονται δεδομένα από τον διακομιστή για τους λόγους που παρουσιάσαμε παραπάνω, οι μηχανισμοί φόρτωσης των βιβλιοθηκών με τις θεραπείες και τα φάρμακα στις συσκευές έγχυσης είναι δύο. Ο ένας τρόπος είναι η επιλογή θεραπειών μέσω ανάγνωσης ετικετών (*tags*) τεχνολογίας RFID με τη βοήθεια ειδικού μικροτσίπ που βρίσκεται ενσωματωμένο στην συσκευή, στον οποίο έγινε εκτενή ανάλυση για αδυναμίες η οποία παρουσιάζεται παρακάτω. Ο δεύτερος τρόπος είναι μέσω ειδικής USB θύρας που καταλήγει σε ειδική σειριακή υποδοχή (πατέντα του κατασκευαστή) και με τη βοήθεια ειδικού λογισμικού από υπολογιστή. Είναι σημαντικό να σημειωθεί σε αυτό το σημείο, ότι το γεγονός ότι η θύρα και το σειριακό καλώδιο είναι πατέντα του κατασκευαστή και αυτό δεν μπορεί να αποκτηθεί από οποιονδήποτε στην αγορά αλλά μόνο από ειδική παραγγελία στον κατασκευαστή προσθέτει ένα έξτρα επίπεδο ασφαλείας. Στο σενάριο δηλαδή που κάποιος έχει φυσική πρόσβαση στις ιατρικές συσκευές και στο λογισμικό φόρτωσης βιβλιοθηκών στο χώρο ενός νοσοκομείου παραδείγματος χάριν, να μην είναι σε θέση να εκμεταλλευτεί κάποιο τυχόν κενό ασφαλείας από τη στιγμή που δεν έχει στην κατοχή του και το ειδικό καλώδιο.

Σχετικά με τη μορφή των αρχείων που φορτώνονται στις συσκευές, η λήψη τους γίνεται τοπικά από τον υπολογιστή μέσω της πλατφόρμας του παρόχου μέσα στην οποία γίνεται και η δημιουργία τους. Εξετάζοντας ένα τέτοιο αρχείο, παρατηρήθηκε ότι περιέχει ένα αντικείμενο JSON με τις παραμέτρους της βιβλιοθήκης με τις θεραπείες και τις δοσολογίες των φαρμάκων. Στο τέλος κάθε αρχείου υπάρχει μια τιμή που είναι *digest* των περιεχομένων του αρχείου. Για την ανίχνευση τροποποιημένων δεδομένων χρησιμοποιείται ένα *digest* ή ένα *one-way hash*. Με λίγα λόγια, ένα *digest* μήνυμα είναι ένα αποτύπωμα των δεδομένων. Αν τα δεδομένα αλλάξουν, το αποτύπωμα (*digest* ή *hash*) αλλάζει με τρόπους που δεν γίνεται να προβλεφθούν. Αυτές οι τιμές όμως προστατεύουν τα δεδομένα μόνο από τυχαία φθορά.

Η *hashed* τιμή αυτή χρησιμεύει στον έλεγχο για το αν τα περιεχόμενα του αρχείου αλλοιώθηκαν ή αλλάχτηκαν κατά τη λήψη του αρχείου και ο έλεγχος γίνεται με επαναυπολογισμό της τιμής και σύγκρισης της με την ήδη υπάρχουσα. Αν τα δεδομένα έχουν αλλοιωθεί η τιμές θα είναι διαφορετικές. Το πρόβλημα με την λογική αυτού του ελέγχου είναι ότι οποιοσδήποτε κακόβουλος που έχει πρόσβαση στα αρχεία με τις βιβλιοθήκες, χωρίς κανέναν έλεγχο εξουσιοδότησης μπορεί να τα πάρει να τα μεταβάλλει και απλά υπολογίζοντας ξανά το *hash* του νέου JSON και αντικαθιστώντας το, τα αρχεία να συνεχίζουν να είναι έγκυρα. Αυτό είναι πρόβλημα ζωτικής σημασίας αν για παράδειγμα αλλαχτούν οι επιτρεπόμενες δοσολογίες σε φάρμακα όπως είναι η μορφίνη ή μειώνοντας τη δοσολογία σε φάρμακα που είναι απαραίτητα σε καθημερινή βάση για τη συνέχεια της ζωής ασθενών.

Συνίσταται τα αρχεία βιβλιοθηκών φαρμάκων να συνοδεύονται από έναν κωδικό επαλήθευσης που να αποδεικνύει την αυθεντικότητα και την ακεραιότητα του αρχείου. Είναι απαραίτητο έτσι να εφαρμοστεί μια μέθοδος υπογραφής. Η υπογραφή θα πρέπει να δημιουρ-

γείται με κρυπτογραφικά ασφαλές τρόπο, ώστε ο παραλήπτης του αρχείου (η συσκευή) να μπορεί να επικυρώνει για να εξασφαλίζει την αυθεντικότητα του αρχείου εμποδίζοντας μη εξουσιοδοτημένα άτομα να δημιουργήσουν έγκυρα αρχεία. RS256 (υπογραφή RSA με SHA-256) προτείνεται. Πιο συγκεκριμένα, ο συνθέτης της βιβλιοθήκης φαρμάκων (διακομιστής ιστού) και ο κάτοχος του ιδιωτικού κλειδιού (*private key*) θα υπογράφουν τα αρχεία αντλιών και οι συσκευές που διαθέτουν το δημόσιο κλειδί (*public key*) θα μπορούν να επαληθεύουν ότι οι βιβλιοθήκες έχουν δημιουργηθεί από το διακομιστή. Ένας άλλος μηχανισμός ασφάλειας είναι κάθε φορά που προγραμματίζεται μια βιβλιοθήκη στις συσκευές να χρειάζεται πρώτα ένας κωδικός, αποτρέποντας έτσι μη εξουσιοδοτημένα άτομα να φορτώσουν βιβλιοθήκες στις συσκευές.

Στη συνέχεια έγιναν δοκιμές με κακόμορφα JSON με σκοπό το σπάσιμο (*crash*) του λογισμικού των συσκευών (*firmware*).

4.2.4 Αξιολόγηση των RFID ετικετών και του μηχανισμού ανάγνωσης τους

Ένας τρόπος επιλογής θεραπείας για την αντλία έγχυσης είναι μέσω ανάγνωσης RFID ετικετών από τη συσκευή. Το σύστημα ανάγνωσης RFID ετικετών από την συσκευή αποτελείται από τον ενσωματωμένο στη συσκευή δέκτη και από τις ειδικές ετικέτες που εκτυπώνονται με σκοπό την ενημέρωση των θεραπειών. Σχετικά με τον εκτυπωτή των ετικετών, δεν υπήρχε πρόσβαση, οπότε και δεν υπήρχε τρός ανάλυσης ασφάλειας.

Ο δέκτης είναι μια ενσωματωμένη αναλογική συσκευή εμπρόσθιας λήψης και πλαισίωσης δεδομένων για ένα σύστημα 13.56MHz RFID και (NFC). Οι ενσωματωμένες επιλογές προγραμματισμού καθιστούν αυτή τη συσκευή κατάλληλη για ένα ευρύ φάσμα εφαρμογών για συστήματα εγγύτητας. Μπορεί να εκτελεστεί σε μία από τις τρεις λειτουργίες: RFID και NFC *Reader*, NFC *Peer* ή *Emulation Card* και διαμορφώνεται επιλέγοντας το επιθυμητό πρωτόκολλο στους καταχωρητές ελέγχου. Η άμεση πρόσβαση σε όλους τους καταχωρητές ελέγχου επιτρέπει τη λεπτομερή ρύθμιση διαφόρων παραμέτρων του αναγνώστη, όπως απαιτείται κάθε φορά.

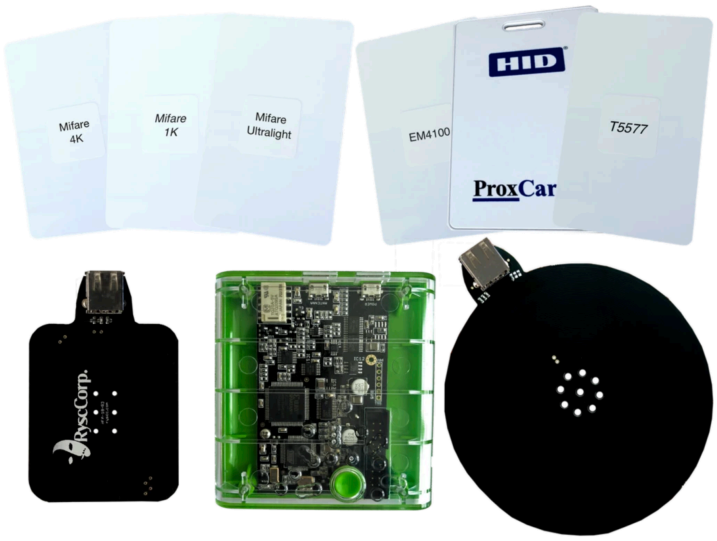
Για να αξιολογηθούν οι συγκεκριμένες ετικέτες χρειάστηκε ειδικό *hardware* το Proxmark3 kit όπως παρουσιάζεται στο σχήμα 4.5 και το ανάλογο λογισμικό και *firmware* ανοιχτού κώδικα που έχει αναπτυχθεί για τεστ ασφάλειας της επικοινωνίας NFC.

Το Proxmark3 kit συμπεριλαμβάνει LF (*low frequency*) κεραία, HF (*high frequency*) κεραία μαζί με καλώδια και κάρτες διαφόρων τύπων για τις δοκιμές. Στην συγκεκριμένη αξιολόγηση, χρειάστηκε η HF κεραία των 13.56 MHz καθώς τέτοιας συχνότητας είναι οι ετικέτες. Από την ανάλυση βρέθηκε ότι οι ετικέτες είναι τύπου NTAG213 με 144 bytes μνήμη προς χρήση (*user memory*) και μοιάζουν με αυτή του σχήματος 4.6[3].

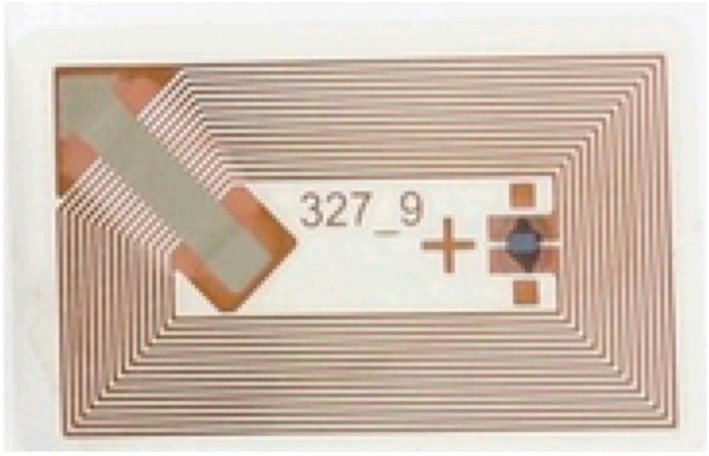
```
proxmark3> hf search

Waiting for a response from the proxmark...
You can cancel this operation by pressing the pm3 button
 UID : 04 b2 f7 6a fc 59 80
ATQA : 00 44
 SAK : 00 [2]
Tagtype: 00000100
```

[3] https://www.nfc-tag-shop.de/en/nfc-sticker/clear-nfc-tags/145/nfc-sticker-midas-12-x-19-mm-ntag-213-180-byte-transparent



Σχήμα 4.5: Σύνολο εργαλείων Proxmark3kit



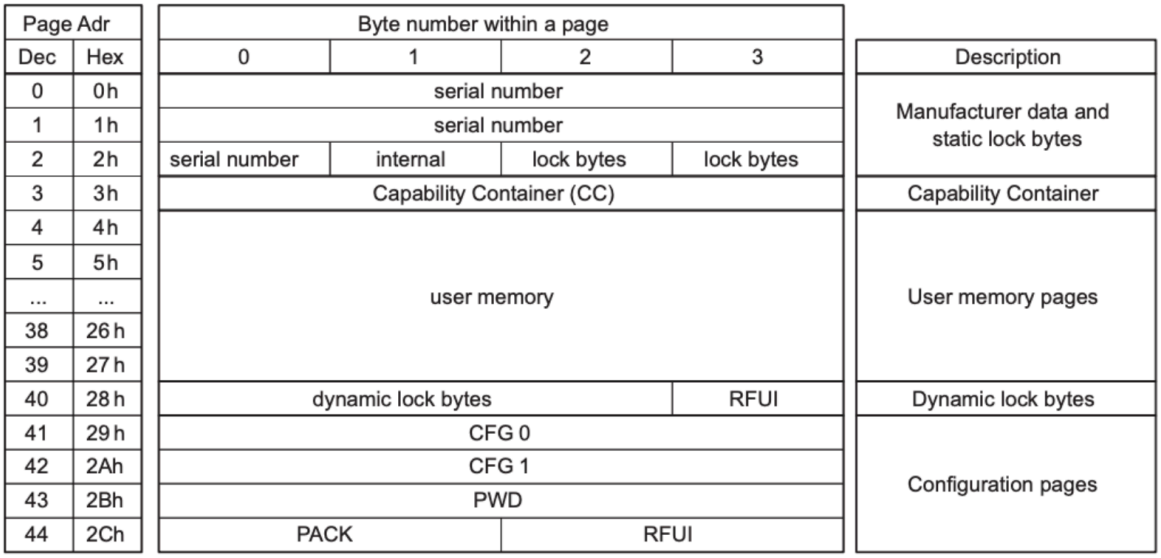
Σχήμα 4.6: RFID ετικέτα

```
TYPE : NTAG 213 144bytes (NT2H1311G0DU)
MANUFACTURER : NXP Semiconductors Germany
proprietary non iso14443-4 card found, RATS not supported
No chinese magic backdoor command detected

Valid ISO14443A Tag Found - Quiting Search
```

Τα χαρακτηριστικά που αναφέρονται επίσημα από τα έγγραφα για τον συγκεκριμένο τύπο ετικέτας σχετικά με την ασφάλεια είναι τα παρακάτω.

- Manufacturer programmed 7-byte UID for each device
- Preprogrammed Capability container with one-time programmable bits
- Field programmable read-only locking function
- ECC-based originality signature



Σχήμα 4.7: Οργάνωση μνήμης NTAG213 ετικετών

- 32-bit password protection to prevent unauthorized memory operations

Αυτή η σειρά ετικετών δεν υποστηρίζει κρυπτογράφηση, αλλά διαθέτει έναν μηχανισμό με κωδικό προστασίας πρόσβασης των 32-*bit* και την ικανότητα ορισμού ορίου αποτυχημένων προσπαθειών για κωδικό πρόσβασης. Επιπλέον, παρέχει μηχανισμό για την προστασία της μνήμης δεδομένων χρήστη καθιστώντας την να είναι μόνο αναγνώσιμη και όχι εγγράψιμη. Η οργάνωση της μνήμης τους είναι αυτή που φαίνεται στο σχήμα 4.7.

```
proxmark3> hf mfu info
Tagtype: 00000100

--- Tag Information ---------
-------------------------------------------------------------

      TYPE : NTAG 213 144bytes (NT2H1311G0DU)
       UID : xx xx xx xx xx xx xx
    UID[0] : 04, NXP Semiconductors Germany
      BCC0 : C9, Ok
      BCC1 : 4F, Ok
  Internal : 48, default
      Lock : 00 00          (binary 00000000 00000000)
OneTimePad : e1 10 12 00    (binary 11100001 11100001 11100001 11100001)

--- NDEF Message
Capability Container: e1 10 12 00
  E1 : NDEF Magic Number
  10 : version 1.0 supported by tag
  12 : Physical Memory Size: 152 bytes
  12 : NDEF Memory Size: 144 bytes
  00 : Read access granted without any security / Write access granted wi

--- Tag Signature
```

```
IC signature public key name  : NXP NTAG21x (2013)
IC signature public key value : ...

     Elliptic curve parameters : secp128r1
            Tag ECC Signature : ...

--- Tag Version
       Raw bytes : 00 04 04 02 01 00 0f 03
       Vendor ID : 04, NXP Semiconductors Germany
    Product type : 04, NTAG
 Product subtype : 02, 50pF
   Major version : 01
   Minor version : 00
            Size : 0F, (256 <-> 128 bytes)
   Protocol type : 03

--- Tag Configuration
  cfg0 [41/0x29] : 04 00 00 ff
                   - pages don't need authentication
                   - strong modulation mode disabled
  cfg1 [42/0x2A] : 00 05 00 00
                   - Unlimited password attempts
                   - user configuration writeable
                   - write access is protected with password
                   - 05, Virtual Card Type Identifier is  default
  PWD  [43/0x2B] : 00 00 00 00 - (cannot be read)
  PACK [44/0x2C] : 00 00       - (cannot be read)
  RFU  [44/0x2C] :       00 00 - (cannot be read)

--- Known EV1/NTAG passwords.
 Found a default password: ff ff ff ff  || Pack: 00 00
```

Όπως παρουσιάζουν τα αποτελέσματα παραπάνω υπάρχουν δύο σημαντικά σημεία που πρέπει να αναλυθούν.

Αρχικά, παρατηρείται ότι τα *bytes* κλειδώματος (*lock bytes*) είχαν τιμή 0. Παράλληλα, βρέθηκε ότι χρησιμοποιείται προκαθορισμένος κωδικός ο οποίος κανονικά απαιτείται για την ανάγνωση της ετικέτας. Από τη στιγμή που έχει χρησιμοποιηθεί τύπος ετικετών που προσφέρει μηχανισμό προστασίας της μνήμης από μη εξουσιοδοτημένα άτομα, θα έπρεπε να οριστεί ένας κωδικός που να μην είναι προβλέψιμος ούτε ανιχνέυσιμος από τέτοιου είδους εξοπλισμό ή με μια απλή αναζήτηση στο Διαδίκτυο. Διαφορετικά, κάποιος που έχει φυσική πρόσβαση στις ετικέτες θα μπορούσε με τα κατάλληλα μέσα να διαβάσει το περιεχόμενο της μνήμης των ετικετών.

Σαν απόδειξη του παραπάνω ευρήματος, έγινε ανάγνωση του περιεχόμενου της μνήμης με τη χρήση του κωδικού *ffffffff*. Παρ'όλα αυτά ο ορισμός ενός πολύπλοκου κωδικού θα καθιστούσε δύσκολη την λειτουργικότητα της επικοινωνίας RFID από τη στιγμή που πολλά άτομα (γιατροί, νοσοκόμοι, ιατρικό προσωπικό) θα έπρεπε να γνωρίζουν και να θυμούνται πολλούς και διάφορους κωδικούς.

Σε συνέχεια του πρώτου ευρήματος φάνηκε ξεκάθαρα ότι τα *lock bytes* έχουν όντως τιμή 0. Αυτό σημαίνει ότι δεν αξιοποιήθηκε ο μηχανισμός κλειδώματος της μνήμης ενάντια στην

εγγραφή της. Ως προς απόδειξη αυτού, έγινε εγγραφή του περιεχομένου κάποιων *blocks* της μνήμης με κακόβουλα δεδομένα.

Επιπρόσθετα, ύστερα από την ανάγνωση επιβεβαιώθηκε ότι δεν υπάρχει υλοποιημένη κρυπτογράφηση από τη στιγμή που το περιεχόμενο είναι *plain text* και αναγνώσιμο από τον άνθρωπο. Αυτό ήταν αναμενόμενο από τη στιγμή που ο συγκεκριμένος τύπος ετικετών που επιλέχθηκε δεν υποστηρίζει κρυπτογράφηση. Παρ' όλα αυτά υπάρχει παρόμοιος τύπος ετικετών που υποστηρίζει, χαρακτηριστικό που θα εξασφάλιζε την εμπιστευτικότητα των δεδομένων καθώς και θα λειτουργούσε ως ανασταλτικός παράγοντας στην μεταβολή των περιεχόμενων των ετικετών. Δεν έχει νόημα να υπήρχε κρυπτογράφηση επειδή θα ήταν χρονοβόρο για το λειτουργικό της αντλίας έγχυσης να αποκρυπτογραφεί τα δεδομένα κάτι που εμποδίζει την άμεση διαθεσιμότητα του συστήματος που είναι πρωταρχική απαίτηση στον τομέα της ιαρικής περίθαλψης.

Συνολικά, ο συνδυασμός των τριών ευρημάτων καθιστούν το σύστημα επιλογής φαρμάκων με ανάγνωση RFID ετικετών ευπαθές και αναξιόπιστο με επιπτώσεις στην εμπιστευτικότητα και την ακεραιότητα του καθώς και θέτοντας σε κίνδυνο συσκευές που είναι ζωτικής σημασίας για τους ανθρώπους όπως αναφέρθηκε και παραπάνω.

4.2.5 Αξιολόγηση του υλικού μέρους των ιατρικών συσκευών

Σχετικά με τα υλικά μέρη των ιατρικών συσκευών έγινε χαρτογράφηση των επί μέρους εξαρτημάτων για την αναγνώριση των κυκλωμάτων και γενικότερα την κατανόηση της επικοινωνίας των διάφορων ολοκληρωμένων κυκλωμάτων (*chips*) μεταξύ τους. Τέτοιου είδους IoT συσκευές αποτελούνται από μικροελεγκτές (MCUs – *MicroController Units*), περιφεριακά όπως είναι οι διάφοροι αισθητήρες, η οθόνη, *buzzer*. Σημαντικά εξαρτήματα είναι και τα *modules* για Wi-fi και GSM επικοινωνία καθώς και το ολοκληρωμένο κύκλωμα για NFC επικοινωνία.

Βρέθηκε μία ευπάθεια που συναντάται πάρα πολύ συχνά σε IoT εφαρμογές και αφορά το υλικό μέρος (*hardware*) σχετικά με την επαφή JTAG. Το JTAG [Vish18] είναι ένα πρότυπο IEEE που αναπτύχθηκε στη δεκαετία του 1990 για την αποσφαλμάτωση, την ενημέρωση και την αποθήκευση λογισικού στα ολοκληρωμένα κυκλώματα (*firmware* στο τσιπ και ακόμα, σήμερα αυτό το πρότυπο χρησιμοποιείται ευρέως στη βιομηχανία. Συνήθως, οι κόμβοι IoT είναι μικρές ενσωματωμένες συσκευές που έχουν ένα πρόγραμμα που τρέχει συνεχώς σε έναν βρόχο που ονομάζεται υλικολογισμό (*firmware*).

Αυτά τα προγράμματα εφαρμογών εγγράφονται απευθείας στο ολοκληρωμένο κύκλωμα μέσω σειριακής ή *JTAG debugging* διεπαφής. Οι κατασκευαστές διατηρούν τη θύρα JTAG στην πλακέτα PCB για να ελέγχουν και να επικυρώνουν αν κάθε ηλεκτρονικό μέρος είναι κατάλληλα τοποθετημένο ή όχι, καθώς και για αναβάθμιση του υλικολογισμικού στο μέλλον. Υπάρχουν πολλοί JTAG *debuggers* διαθέσιμοι στην αγορά που κοστίζουν από δέκα έως μερικές εκατοντάδες δολάρια, πράγμα που καθιστά ακόμη πιο εύκολο για τους εισβολείς να έχουν πρόσβαση στα εσωτερικά του ολοκληρωμένου κυκλώματος και του υλικολογισμικού. Οι κατασκευαστές προϊόντων IoT πρέπει να διαφυλλάσσουν όχι μόνο την ασφαλή μετάδοση δεδομένων μεταξύ πολλαπλών συσκευών αλλά και την ασφάλεια τους κατά των επιθέσεων που μπορούν να γίνουν έχοντας φυσική πρόσβαση, απενεργοποιώντας τη λειτουργία της θύρας JTAG και οποιωνδήποτε *debugging* διεπαφών υπάρχουν.

Στην συγκεκριμένη ιατρική εφαρμογή, όχι μόνο δεν είναι απενεργοποιημένη η θύρα αλλά είναι και εκτεθειμένη σε εμφανές και εύκολα προσβάσιμο σημείο για λόγους ενημερώσεων του λειτουργικού (*firmware*). Συγκεκριμένα, αυτός είναι ο μηχανισμός που επιλέχθηκε για ενημερώσεις, από τη στιγμή που έχει αποτραπεί οποιοσδήποτε τρόπος αποστολής δεδομέ-

νων στη συσκευή μέσω δικτύου. Παρ'όλη την ευκολία λειτουργίας αφήνει ένα σοβαρό κενό ασφαλείας για το σύστημα. Ένας επιτιθέμενος με φυσική πρόσβαση στη συσκευή μπορεί να αποσπάσει όλο το λειτουργικό (που μπορεί να χρησιμεύσει στην ανάλυση του κώδικα), να αποσπάσει ευαίσθητες πληροφορίες (*sensitive data*) καθώς και να περάσει μολυσμένο λογισμικό (*malware*) ή αλλαγμένο με τέτοιο τρόπο προς όφελος του.

Τέλος, είναι σημαντικό αν έχουν απενεργοποιηθεί όλες οι διεπαφές από τις οποίες κάποιος θα μπορούσε να υποκλέψει δεδομένα ή να πάρει και να μεταβάλλει το λειτουργικό, να εξασφαλισθεί και η δυνατότητα ελέγχου της υλικής ακεραιότητας της συσκευής. Δεν εντοπίστηκε μηχανισμός πρόληψης παραβιάσεων κατά τη διάρκεια αυτής της διαδικασίας αφού η συσκευή αποσυναρμολογήθηκε σε μεμονωμένα μέρη από τα οποία ξανασυναρμολογήθηκε μια πλήρως λειτουργική συσκευή.

Η δυνατότητα παραβίασης του υλικού της συσκευής χωρίς επιπτώσεις στη λειτουργία του μπορεί να επιτρέψει σε έναν εισβολέα να χρησιμοποιήσει μεθόδους χαμηλού επιπέδου για την εξαγωγή μυστικών από την αποθήκευση της συσκευής, όπως το πιστοποιητικό SSL πελάτη. Με αυτές τις πληροφορίες, ένας εισβολέας μπορεί να δημιουργήσει πλαστά γεγονότα στο διακομιστή. Η δυνατότητα παραβίασης της συσκευής χωρίς να αφήνει κανένα στοιχείο μπορεί να επιτρέψει σε έναν αντίπαλο (σε οποιοδήποτε στάδιο, ακόμη και στην αλυσίδα εφοδιασμού) να επηρεάσει τη θεραπεία των ασθενών, χωρίς να ανιχνεύεται από διαδικασίες διασφάλισης ποιότητας.

Είναι καλό να υιοθετηθούν μηχανισμοί πρόληψης των παραβιάσεων που θα ενεργοποιήσουν την ασφαλή διαγραφή πληροφοριών (όπως το πιστοποιητικό *SSL* πελάτη) κατά το άνοιγμα του περιβλήματος. Επιπλέον, συνιστάται να κατασκευαστεί ένα περίβλημα που να προστατεύει τη συσκευή από παραβιάσεις.

4.2.6 Αξιολόγηση του λογισμικού των ιατρικών συσκευών

Για την αξιολόγηση του λογισμικού (*firmware*) των ιατρικών συσκευών, είναι αναγκαίο πρώτα να βρεθεί ένας τρόπος να εξαχθεί ώστε να μπορεί να αναλυθεί περαιτέρω με ειδικό λογισμικό και τεχνική *reverse engineering*. Στους περισσότερους σύγχρονους μικροϋπολογιστές ή μικροελεγκτές υπάρχει θύρα JTAG μέσα από την οποία υπάρχει δυνατότητα εξαγωγής του λογισμικό της συσκευής. Για να γίνει το εκτελέσιμο αναγνώσιμο από τον άνθρωπο φορτώνεται σε ειδικό πρόγραμμα το IDA. Κατά την φόρτωση του καθορίζει κάποιος τι είδους *binary* (τύπος επεξεργαστή ή μικροελεγκτή, αρχιτεκτονική) είναι καθώς και πόσο είναι το μέγεθος του και μια οργάνωση της μνήμης (*memory mapping*).

Έτσι, με μια απλή αναζήτηση των εγγράφων δεδομένων (*datasheets*) του συγκεκριμένου μοντέλου μικροελεγκτή ή επεξεργαστή κάθε φορά, βρίσκεται ο πίνακας που απεικονίζει σε διευθύνσεις την οργάνωση της μνήμης όπως φαίνεται στο παρακάτω παράδειγμα 4.8.

Από αυτά τα δεδομένα φαίνεται σε ποιες διευθύνσεις βρίσκεται ο κύριος κώδικας (*main code* και πόσο είναι το μέγεθος του. Σκοπός της τεχνικής *reverse engineering* είναι να βρεθεί η κύρια συνάρτηση του προγράμματος (*main function* και βήμα βήμα να προβλεθεί η λειτουργία του αρχικού κώδικα που γράφτηκε πριν γίνει τη διαδικασία του *compilation*.

Σε αυτά τα ειδικά προγράμματα που αναλαμβάνουν το *disassembling* του κώδικα, άμα δεν γίνει αυτόματη αναγνώριση, χρειάζεται να οριστεί από τον χρήστη το λεγόμενο σημείο εισόδου (*entry point*) δηλαδή το σημείο από το οποίο αρχίζει να τρέχει ο κώδικας. Για να γίνει ο εντοπισμός αυτού του σημείου χρειάζεται να βρεθούν οι διευθύνσεις των διακοπών (*interrupt vectors*. Κάθε διεύθυνση ενός *interrupt vector* δείχνει τη διεύθυνση που βρίσκεται κάθε φορά ο κώδικας του αντίστοιχου χειριστή διακοπών (*interrupt handler*. Ένα παράδειγμα ενός τέτοιου πίνακα παρουσιάζεται στο παρακάτω σχήμα 4.9:

Memory (flash)	Total Size	384KB	512KB	384KB	512KB
Main: interrupt vector		00FFFFh to 00FF80h	00FFFFh to 00FF80h	00FFFFh to 00FF80h	00FFFFh to 00FF80h
Main: code memory	Bank 3	N/A	128KB 087FFFh to 068000h	N/A	128KB 087FFFh to 068000h
	Bank 2	128KB 067FFFh to 048000h	128KB 067FFFh-48000h	128KB 067FFFh to 048000h	128KB 067FFFh-48000h
	Bank 1	128KB 047FFFh to 028000h	128KB 047FFFh to 028000h	128KB 047FFFh to 028000h	128KB 047FFFh to 028000h
	Bank 0	128KB 027FFFh to 008000h	128KB 027FFFh to 008000h	128KB 027FFFh to 008000h	128KB 027FFFh to 008000h
MID support software (ROM)	Total Size	1KB 006FFFh to 006C00h	1KB 006FFFh to 006C00h	1KB 006FFFh to 006C00h	1KB 006FFFh to 006C00h
RAM	Sector 3	16KB 0FBFFFh to 0F8000h	16KB 0FBFFFh to 0F8000h	16KB 0FBFFFh to 0F8000h	16KB 0FBFFFh to 0F8000h
	Sector 2	N/A	16KB 0F7FFFh to 0F4000h	N/A	16KB 0F7FFFh to 0F4000h
	Sector 1	N/A	16KB 0F3FFFh to 0F0000h	N/A	16KB 0F3FFFh to 0F0000h
	Sector 0	16KB 0063FFh to 002400h (mirrored at address range 0FFFFFh to 0FC000h)	16KB 0063FFh to 002400h (mirrored at address range 0FFFFFh to 0FC000h)	16KB 0063FFh to 002400h (mirrored at address range 0FFFFFh to 0FC000h)	16KB 0063FFh to 002400h (mirrored at address range 0FFFFFh to 0FC000h)
RAM[2]	Sector 7	2KB 0023FFh to 001C00h	2KB 0023FFh to 001C00h	N/A	N/A
USB RAM[3]	Sector 7	N/A	N/A	2KB 0023FFh to 001C00h	2KB 0023FFh to 001C00h
Information memory (flash)	Info A	128 B 0019FFh to 001980h	128 B 0019FFh to 001980h	128 B 0019FFh to 001980h	128 B 0019FFh to 001980h
	Info B	128 B 00197Fh to 001900h	128 B 00197Fh to 001900h	128 B 00197Fh to 001900h	128 B 00197Fh to 001900h
	Info C	128 B 0018FFh to 001880h	128 B 0018FFh to 001880h	128 B 0018FFh to 001880h	128 B 0018FFh to 001880h
	Info D	128 B 00187Fh to 001800h	128 B 00187Fh to 001800h	128 B 00187Fh to 001800h	128 B 00187Fh to 001800h
Bootloader (BSL) memory (flash)	BSL 3	512 B 0017FFh to 001600h	512 B 0017FFh to 001600h	512 B 0017FFh to 001600h	512 B 0017FFh to 001600h
	BSL 2	512 B 0015FFh to 001400h	512 B 0015FFh to 001400h	512 B 0015FFh to 001400h	512 B 0015FFh to 001400h
	BSL 1	512 B 0013FFh to 001200h	512 B 0013FFh to 001200h	512 B 0013FFh to 001200h	512 B 0013FFh to 001200h
	BSL 0	512 B 0011FFh to 001000h	512 B 0011FFh to 001000h	512 B 0011FFh to 001000h	512 B 0011FFh to 001000h
Peripherals	Size	4KB 000FFFh to 000000h	4KB 000FFFh to 000000h	4KB 000FFFh to 000000h	4KB 000FFFh to 000000h

Σχήμα 4.8: Οργάνωση μνήμης μικροελεγκτή

Σε τέτοιου είδους αναλύσεις, η διακοπή (*interrupt*) που μας ενδιαφέρει περισσότερο είναι το *System Reset*. Είναι κατανοητό ότι όταν δίνεται εντολή επανακίνησης (*reset*) σε μια συσκευή ξεκινάει ξανά από την αρχή τη λειτουργίας της. Οπότε από εκεί που βρίσκεται ο *reset interrupt handler* μπορούμε να οδηγηθούμε στη διεύθυνση όπου ξεκινάει και ο κώδικας.

INTERRUPT SOURCE	INTERRUPT FLAG	SYSTEM INTERRUPT	WORD ADDRESS	PRIORITY
System Reset Power up, External Reset Watchdog time-out, key violation Flash memory key violation	WDTIFG, KEYV (SYSRSTIV)(1) (2)	Reset	0FFFEh	63, highest
System NMI PMM Vacant memory access JTAG mailbox	SVMLIFG, SVMHIFG, DLYLIFG, DLYHIFG, SVMLVLRIFG, SVMHVLRIFG, VMAIFG, JMBINIFG, JMBOUTIFG (SYSSNIV)(1)	(Non)maskable	0FFFCh	62
User NMI NMI Oscillator fault Flash memory access violation	NMIIFG, OFIFG, ACCVIFG, BUSIFG (SYSUNIV)(1) (2)	(Non)maskable	0FFFAh	61
Comp_B	Comparator B interrupt flags (CBIV)(1) (3)	Maskable	0FFF8h	60
Timer TB0	TB0CCR0 CCIFG0 (3)	Maskable	0FFF6h	59
Timer TB0	TB0CCR1 CCIFG1 to TB0CCR6 CCIFG6, TB0IFG (TB0IV)(1) (3)	Maskable	0FFF4h	58
Watchdog interval timer mode	WDTIFG	Maskable	0FFF2h	57
USCI_A0 receive or transmit	UCA0RXIFG, UCA0TXIFG (UCA0IV)(1) (3)	Maskable	0FFF0h	56
USCI_B0 receive or transmit	UCB0RXIFG, UCB0TXIFG (UCB0IV)(1) (3)	Maskable	0FFEEh	55
ADC12_A	ADC12IFG0 to ADC12IFG15 (ADC12IV)(1) (3)	Maskable	0FFECh	54
Timer TA0	TA0CCR0 CCIFG0(3)	Maskable	0FFEAh	53
Timer TA0	TA0CCR1 CCIFG1 to TA0CCR4 CCIFG4, TA0IFG (TA0IV)(1) (3)	Maskable	0FFE8h	52
USB_UBM(4)	USB interrupts (USBIV)(1) (3)	Maskable	0FFE6h	51
LDO-PWR (5)	LDOOFFIFG, LDOONIFG, LDOOVLIFG			
DMA	DMA0IFG, DMA1IFG, DMA2IFG, DMA3IFG, DMA4IFG, DMA5IFG (DMAIV)(1) (3)	Maskable	0FFE4h	50
Timer TA1	TA1CCR0 CCIFG0(3)	Maskable	0FFE2h	49
Timer TA1	TA1CCR1 CCIFG1 to TA1CCR2 CCIFG2, TA1IFG (TA1IV)(1) (3)	Maskable	0FFE0h	48
I/O Port P1	P1IFG.0 to P1IFG.7 (P1IV)(1)(3)	Maskable	0FFDEh	47
USCI_A1 receive or transmit	UCA1RXIFG, UCA1TXIFG (UCA1IV)(1) (3)	Maskable	0FFDCh	46
USCI_B1 receive or transmit	UCB1RXIFG, UCB1TXIFG (UCB1IV)(1) (3)	Maskable	0FFDAh	45
I/O port P2	P2IFG.0 to P2IFG.7 (P2IV)(1) (3)	Maskable	0FFD8h	44
LCD_B(6)	LCD_B Interrupt Flags (LCDBIV)(1)	Maskable	0FFD6h	43
RTC_B	RTCRDYIFG, RTCTEVIFG, RTCAIFG, RT0PSIFG, RT1PSIFG, RTCOFIFG (RTCIV)(1) (3)	Maskable	0FFD4h	42
DAC12_A	DAC12_0IFG, DAC12_1IFG(1) (3)	Maskable	0FFD2h	41
Timer TA2	TA2CCR0 CCIFG0(3)	Maskable	0FFD0h	40
Timer TA2	TA2CCR1 CCIFG1 to TA2CCR2 CCIFG2, TA2IFG (TA2IV)(1) (3)	Maskable	0FFCEh	39

Σχήμα 4.9: Διευθύνσεις διακοπών μικροελεγκτή

4.3 Μέτρα ασφάλειας για τον σχεδιασμό μιας ”έξυπνης” ιατρικής συσκευής

Εξετάζοντας τα αρχικά αίτια (*root causes*) είναι σαφές ότι υπάρχει μακρύς δρόμος μπροστά για την βιομηχανία της υγειονομικής περίθαλψης για να αντιμετωπίσει το εύρος και την κλίμακα των ζητημάτων ασφάλειας στις προβληματικές ιατρικές συσκευές. Δεν υπάρχει συγκεκριμένος τρόπος γιατί τα αίτια πίσω από τις αδυναμίες είναι πολλά και πολύπλοκα. Πολλά από αυτά συνδέονται με το γεγονός ότι ο τρόπος κατασκευής ιατρικών συσκευών καθιερώθηκε προτού εισαχθεί η τεχνολογία του Διαδικτύου των πραγμάτων.

Ένας μεγάλος αριθμός συσκευών σχεδιάστηκαν αρχικά για να μην είναι συνδεδεμένα στο εσωτερικό νοσοκομειακό δίκτυο πόσο μάλιστα στο Διαδίκτυο. Ως εκ τούτου, οι προγραμματιστές που δούλευαν πάνω σε αυτές τις συσκευές σπάνια ανησυχούσαν για την ύπαρξη τρωτών σημείων που θα μπορούσαν να αξιοποιηθούν από απομακρυσμένους εισβολείς. Επειδή πολλά είδη τέτοιων συσκευών αναπτύσσονται με επαναληπτικό τρόπο, δηλαδή με νέες εκ-

δόσεις που βασίζονται στο σκελετό του λογισμικού των παλαιότερων, είναι προφανές ότι όλες οι ευπάθειες και τα λάθη λογισμικού και ρυθμίσεων κληρονομούνται και πολλές φορές οι επιπτώσεις φανερώνονται στις νέες συσκευές.

Ελαττώματα λογισμικού εμφανίζουν όμως ακόμα και οι νέες εξελιγμένες συσκευές, επειδή παρόλο που οι κίνδυνοι έχουν γίνει πλέον γνωστοί, πολλοί κατασκευαστές δεν έχουν την πρακτική ή τη συνήθεια να φροντίζουν για κορυφαία ασφάλεια κατά τη διάρκεια της διαδικασίας ανάπτυξης. Επιπλέον, λόγω της ταχύτητας της καινοτομίας και του ανταγωνισμού για νέες βελτιώσεις, οι κατασκευαστές εστιάζουν περισσότερο στο να βγάλουν γρήγορα προϊόντα στην παραγωγή αντί να πάρουν χρόνο να φροντίσουν για την ασφάλεια κατά τη διαδικασία της ανάπτυξης. Και ακόμη και για εκείνους τους κατασκευαστές που έχουν κατανοήσει τους κινδύνους και έχουν αρχίσει να βελτιώνουν τις πρακτικές ασφαλείας, τέτοιο είδος αλλαγής απαιτεί χρόνο.

Ανεξαρτήτως αυτού, πρέπει να ληφθούν μέτρα για χάρη της ασφάλειας των ασθενών και των ιατρικών εγκαταστάσεων. Μερικά από τα πιο σημαντικά βήματα που πρέπει να γίνουν είναι:

Δημιουργία ασφαλούς κύκλου ζωής ανάπτυξης

Οι κατασκευαστές πρέπει να αναπτύσσουν κώδικα έχοντας πάντα όλες τις πρακτικές ασφάλειας στο μυαλό τους, να φροντίζουν να γίνονται πρακτικές δοκιμές ασφαλείας κατά την ανάπτυξη και αφού βγουν στην αγορά, προγράμματα διαχείρισης ευπαθειών μπορούν να βοηθήσουν στην αντιμετώπιση του προβλήματος.

Ανάπτυξη συσκευών που να αποδεικνύουν γεγονότα παραβιάσεων

Είναι σημαντικό, ιδιαίτερα για τις προσωπικές ιατρικές συσκευές που είναι άμεσα διαθέσιμες στην αγορά, να υπάρχει προστασία από παραβιάσεις. Οι ερευνητές της ασφάλειας τονίζουν ότι οι πρακτικές της προστασίας του δυαδικού κώδικα, της απόκρυψης πληροφοριών υλικού και της προστασίας από οι δραστηριότητες αποσφαλμάτωσης (debugging activities) θα πρέπει να θεωρούνται και να είναι τυποποιημένα μέτρα ασφαλείας.

Εστιάζοντας στην κρυπτογράφηση

Η κρυπτογράφηση των ευαίσθητων δεδομένων και των επικοινωνιών είναι από τα πιο προφανή μέτρα για τη βελτίωση της ασφάλειας των ιατρικών συσκευών. Αλλά, μια κακή εφαρμογή της κρυπτογράφησης είναι σχεδόν το ίδιο επικίνδυνο όσο το να μην υπάρχει καμία. Άρα, για πλήρη αξιοποίηση της κρυπτογράφησης πρέπει να υπάρχει μεγάλη προσοχή στην εφαρμογή πρωτοκόλλων κρυπτογράφησης, να υπάρχουν σταθερές πρακτικές αποθήκευσης κωδικών πρόσβασης και να χρησιμοποιούνται οι πιο ενημερωμένοι κρυπτογραφικοί αλγόριθμοι.

Προστασία των κρυπτογραφικών κλειδιών

Η προστασία των κρυπτογραφικών κλειδιών είναι πολύ σημαντική γιατί ακόμα και οι πιο ενημερωμένοι αλγόριθμοι κρυπτογράφησης δεν έχουν σημασία εάν οι επιτιθέμενοι βρουν έναν τρόπο να έχουν πρόσβαση στα κρυπτογραφικά κλειδιά που χρειάζονται για τη διαδικασία αποκρυπτογράφησης. Οι περισσότερες εφαρμογές έχουν κλειδιά που δεν είναι σωστά ασφαλισμένα.

Αλλαγή αντιμετώπισης της ερευνητικής κοινότητας ασφαλείας

Πολλές φορές οι κατασκευαστές ιατρικών συσκευών αντί να ευχαριστούν τους ερευνητές της ασφάλειας, προσπαθούν να τους μηνύσουν και να θάψουν τα ευρήματα σχετικά με τις αδυναμίες. Θα ήταν καλύτερο οι κατασκευαστές να αναπτύσσουν επίσημες διαδικασίες γνωστοποίησης της ασφάλειας, αλλά και να πληρώνουν ανεξάρτητους ερευνητές για να τους βρουν πολύτιμες λεπτομέρειες για κρίσιμες ευπάθειες που εντοπίζονται στις συσκευές.

Βελτίωση των ενημερώσεων λογισμικού και του ελέγχου ρυθμίσεων μετά την αγορά

Τέλος, οι ιατρικές εγκαταστάσεις χρειάζονται κατασκευαστές που να φροντίζουν για τις

βέλτιστες πρακτικές ασφάλειας στα μηχανήματα που θα συνδεθούν σε σώματα ασθενών ή στα δίκτυα υγειονομικών εγκαταστάσεων. Αυτό απαιτεί και τη δημιουργία πιο ορθολογικών διαδικασιών ενημέρωσης λογισμικού για τις συσκευές καθώς και να επιτρέπεται στους χρήστες να ελέγχουν περισσότερο τον τρόπο με τον οποίο οι συσκευές ρυθμίζονται γιατί πρέπει να μην υπάρχουν πια hardcoded κωδικοί πρόσβασης που δεν γίνεται να αλλάξουν

Κεφάλαιο 5

Συμπεράσματα και Ανοικτά προβλήματα

Σε αυτό το Κεφάλαιο θα παρουσιάσουμε συνοπτικά τα συμπεράσματα στα οποία καταλήξαμε μέσω της ενασχόλησης μας με τα προβλήματα ασφάλειας στις διασυνδεδεμένες ιατρικές συσκευές. Επιπλέον, θα προτείνουμε μελλοντικές κατευθύνσεις ώστε να βελτιωθεί περισσότερο ο σχεδιασμός έξυπνων ιατρικών συσκευών και να συνεισφέρουμε περαιτέρω στην εξασφάλιση της ασφάλειας στον τομέα της υγειονομικής περίθαλψης.

5.1 Αξιολόγηση της τρέχουσας κατάστασης

Τα ζητήματα ασφάλειας του κυβερνοχώρου που αντιμετωπίζει ο τομέας της υγείας το 2019 δεν διαφέρουν πολύ από τα τελευταία χρόνια. Αν και οι επιθέσεις γίνονται όλο και πιο πολύπλοκες λόγω των τεχνολογικών εξελίξεων, τα ποσοστά επιτυχίας τους δεν έχουν μειωθεί. Οι περισσότεροι πάροχοι υγειονομικής περίθαλψης αγωνίζονται να καλύψουν τις απαιτήσεις ασφάλειας αν και οι προϋπολογισμοί είναι περιορισμένοι παράλληλα με ύπαρξη μεγάλων ελλείψεων σε πόρους και ανθρώπινο δυναμικό. Οι ειδικοί τονίζουν ότι ο κλάδος θα αντιμετωπίζει σχεδόν καθημερινά κρούσματα παραβιάσεων.

Μια έρευνα διαπίστωσε ότι από 370 οργανώσεις που χρησιμοποιούν λύσεις IoMT, περίπου το 35% υπέστη τουλάχιστον μία επίθεση στον κυβερνοχώρο το 2016. Η έλλειψη ενημέρωσης σχετικά με την ασφάλεια των χρηστών της IoMT αποτελεί βασικό παράγοντα για τα θέματα ασφάλειας στο IoMT. Σύμφωνα με πρόσφατη έρευνα, μόνο το 17% των κατασκευαστών συνδεδεμένων ιατρικών συσκευών και το 15% των επαγγελματιών του τομέα της ιατρικής γνωρίζουν πιθανά ζητήματα ασφάλειας και λαμβάνουν σοβαρά μέτρα για την πρόληψή τους [syno17]. Αυτό θα μπορούσε να εξηγήσει και το γεγονός ότι οι περισσότερες από 36.000 συσκευές που σχετίζονται με την υγειονομική περίθαλψη στις Ηνωμένες Πολιτείες μπορεί να τις βρει κάποιος εύκολα στο Shodan, μια μηχανή αναζήτησης για IoT συσκευές [Newm17].

Επιπλέον, ενώ έτσι και αλλιώς υπάρχει έλλειψη προτύπων ασφάλειας σχετικά με την τεχνολογία IoT, χρειάζονται επιπλέον προσπάθειες για την ρύθμιση και την διασφάλιση της ασφάλειας σχετικά με τα IoMT. Σε αντίθεση με άλλους τομείς, η ασφάλεια στον ιατρικό τομέα είναι ζωτικής σημασίας λόγω της ευαισθησίας των ιατρικών δεδομένων και της κρίσιμης φύσης των ενεργειών. Η αμερικανική Υπηρεσία Τροφίμων και Φαρμάκων (FDA) πραγματοποιεί βήματα για τη διασφάλιση των ιατρικών συσκευών. Ωστόσο, μόνο το 10% αυτών των συσκευών είναι ταξινομημένα σύμφωνα με την κατηγορία III του FDA, η οποία περιλαμβάνει συσκευές σχεδιασμένες να υποστηρίζουν ή να διατηρούν τη ζωή (π.χ., βηματοδότες) [Haml17]. Παρ’ όλα αυτά, η απειλή της υγείας των ασθενών δεν είναι η μόνη συνέπεια των επιθέσεων κατά των IoMT, καθώς αυτές οι επιθέσεις μπορούν επίσης να έχουν αρνητικές επιπτώσεις στο απόρρητο των ιατρικών δεδομένων, τη φήμη του εμπορικού σήματος, τη συνέχεια της επιχείρησης και τη χρηματοοικονομική σταθερότητα ενός οργανισμού.

Επιπλέον, υπάρχει έλλειψη συναίνεσης μεταξύ των ενδιαφερομένων στις οργανώσεις υγειονομικής περίθαλψης σχετικά με τις απαιτήσεις ασφάλειας[Jala18]. Αυτή η διαφωνία και η έλλειψη γνώσης σχετικά με τις πρακτικές ασφάλειας αφήνει τους υπεύθυνους αβέβαιους σχετικά με τα χαρακτηριστικά ασφαλείας που σχετίζονται με τις αποφάσεις τους. Αυτοί που εφαρμόζουν την τεχνολογία IoMT συνήθως υποχρεώνονται να αποδεχθούν τις προεπιλεγμένες εγγυήσεις ασφαλείας. Θα πρέπει οι ίδιοι να είναι σε θέση να μετρήσουν και να επαληθεύσουν την ασφάλεια και να παίρνουν καλές επιστημονικές αποφάσεις. Είναι επίσης σημαντικό να δοθεί η δυνατότητα στους υιοθετούντες να επιλέξουν τα χαρακτηριστικά ασφαλείας βάσει των απαιτήσεων τους (π.χ. προτεραιότητες), διότι οι στόχοι ασφαλείας δεν εξαρτώνται μόνο από το σενάριο, αλλά και από τα περιουσιακά στοιχεία και την ανοχή σε κινδύνους.

Λόγω της ταχείας εξέλιξης των τεχνολογιών IoMT, υπάρχει ανάγκη να εισαχθεί ένα δομημένο ποσοτικό μοντέλο που είναι επεκτάσιμο και προσφέρει ευκαιρίες για βελτίωση της ασφάλειας. Με βάση αυτό, οι υιοθετούντες θα προσδιορίζουν τις προτεραιότητές τους στον τομέα της ασφάλειας, οι οποίες αντικατοπτρίζουν τους στόχους ασφαλείας τους και τις αξιοποιούν για να ταξινομήσουν τις μελλοντικές λύσεις όσον αφορά την ασφάλεια. Η μέθοδος πρέπει να χρησιμοποιεί μια λίστα λεπτομερών κριτηρίων ασφαλείας που συλλέγονται με την εξέταση των ελέγχων ασφαλείας που δημοσιεύονται από εξειδικευμένες οργανώσεις όπως ο OWASP, οι Διεθνείς Οργανισμοί Τυποποίησης (ISO) και ο FDA μεταξύ άλλων.

Συμόρφωση με HIPAA και GDPR

Πλέον οποιοσδήποτε οργανισμός που εμπλέκεται με ιατρικά αρχεία στις Η.Π.Α. έχει καθήκον να είναι συμβατός με την HIPAA (*Health Insurance Portability and Accountability Act*) και να προστατεύσει τα εμπιστευτικά δεδομένα ασθενών από το να μοιράζονται ή να έχουν σε αυτά πρόσβαση μη εξουσιοδοτημένοι χρήστες. Η συμμόρφωση με την HIPAA απαιτεί από τους οργανισμούς υγειονομικής περίθαλψης των Η.Π.Α. να εφαρμόσουν κατάλληλες τεχνικές για να διασφαλίσουν την προστασία των δεδομένων τους και προσφέρει ένα σταθερό σημείο αναφοράς για κάθε οργανισμό στον κλάδο της υγειονομικής περίθαλψης παγκοσμίως. Οι εταιρείες που δεν συμμορφώνονται μπορεί να αντιμετωπίσουν σημαντικό πρόστιμο.

5.2 Συμπεράσματα

Στην εργασία μας, παρουσιάσαμε ένα μοντέλο απειλών με σκοπό την κατηγοριοποίηση των κινδύνων και τη διαχείριση τους απαριθμώντας τις ανάλογες απαιτήσεις ασφάλειας. Μπορεί όλη η ανάλυση κινδύνων να έγινε με βάση το αντικείμενο μελέτης μας, όμως όλα αυτά που παρουσιάστηκαν είναι προβλήματα που συναντώνται σε όλες τις IoMT εφαρμογές και προφανώς σε όλες τις αντλίες έγχυσης.

Η μοντελοποίηση απειλών και η διαχείριση κινδύνων είναι πολύ σημαντική καθώς προσφέρει μια ολοκληρωμένη εικόνα των θεμάτων ασφάλειας που πρέπει να προσέξουν οι κατασκευαστές IoMT. Παρ'όλα αυτά, αυτό είναι μόνο το πρώτο βήμα, που πρέπει πάντα να ακολουθείται από ελέγχους και δοκιμές από ειδικούς του τομέα της ασφάλειας υπολογιστών.

Η κύρια διαφορά στις δοκιμές διείσδυσης σε IoT είναι η ποικιλομορφία που συναντάται. Με τις παραδοσιακές δοκιμές, ο μηχανικός ασφάλειας αντιμετωπίζει συνήθως συστήματα *Windows* ή *Linux* x86 / x64-bits, γνωστά πρωτόκολλα και εφαρμογές TCP / UDP. Αλλά, όταν έχει να εξετάσει IoT εφαρμογές, αντιμετωπίζει νέες αρχιτεκτονικές που είναι ασυνήθιστες για τους περισσότερους (*ARM, MIPS, SuperH, PowerPC*). Διαφορετικά πρωτόκολλα

επικοινωνίας όπως το *ZigBee*, το SDR (*Software Defined Radio*), το BLE (*Bluetooth Low Energy*), το NFC (*Near Field Communication*), το οποίο απαιτεί νέες γνώσεις και εργαλεία για τη δοκιμή τους. Σε πολλές εφαρμογές υπάρχουν λειτουργικά συστήματα σε πραγματικό χρόνο (RTOS) (τα οποία είναι πολύ συνηθισμένα σε αντλίες έγχυσης) απαιτούν από τον ελεγκτή διείσδυσης να δημιουργήσει νέα εργαλεία από την αρχή για να υποστηρίξει αυτό το είδος τεχνολογίας. Και σίγουρα χρειάζονται πολύ καλές γνώσεις από ολους τους τομείς της πληροφορικής, δηλαδή γνώσεις για δίκτυα, GSM επικοινωνία, λειτουργικά συστήματα, υλικού (*hardware*), βάσεις δεδομένων και ανάπτυξης εφαρμογών ιστού (*web applications*) και προφανώς αρχιτεκτονικής μικροεπεξεργαστών και μικροελεγκτών.

Τέλος, τα οφέλη από τις δοκιμές περιλαμβάνουν την ενίσχυση της ασφάλειας των συσκευών, την προστασία από μη εξουσιοδοτημένη χρήση, την αποφυγή της αύξησης των προνομίων, τη μείωση του κινδύνου πλήρης κατοχής ενός συστήματος, την καλύτερη προστασία του ιδιωτικού απορρήτου και των δεδομένων, και την αποφυγή επιθέσεων MITM. Μπορεί η εξασφάλιση ασφάλειας να είναι σημαντική για όλες τις εφαρμογές του τομέα της πληροφορικής, αλλά όταν οι επιπτώσεις επιτυχημένων επιθέσεων σε IoMT είναι η παραβίαση της ιδιωτικότητας δεδομένων υγείας και ο κίνδυνος απώλειας ανθρώπινων ζωών, είναι κατανοητό πώς αυτό είναι πρωταρχικής σημασίας.

5.3 Μελλοντικές κατευθύνσεις

Σε αυτή την Ενότητα προτείνουμε πιθανές επεκτάσεις για ακόμα καλύτερη αξιολόγηση απειλών και κινδύνων σχετικά με το αντικείμενο μελέτης της εργασίας δηλαδή την αντλία έγχυσης, βοηθώντας έτσι γενικότερα στην εξέλιξη των δοκιμών αξιολόγησης της ασφάλειας που απαιτούναι για να βγουν στην παραγωγή οι μελλοντικές έξυπνες ιατρικές συσκευές αλλά και για να προληφθούν μέτρα ασφάλειας πριν το σχεδιασμό τους.

5.3.1 Αξιολόγηση της GSM επικοινωνίας

Όπως έχει αναφερθεί ο ένας τρόπος επικοινωνίας των συσκευών αντλίας έγχυσης με τον διακομιστή της ηλεκτρονικής πλατφόρμας είναι και με GSM επικοινωνία μέσω της διεπαφής που υπάρχει στην συσκευή. Υπάρχουν σενάρια επίθεσης με εκμετάλλευση του GSM δικτύου τα οποία δεν δοκιμάστηκαν και είναι απαραίτητο να ελεγχθούν.

Μια σοβαρή επίθεση είναι η πλαστογράφηση του σταθμού βάσης (*base station spoofing*) που μπορεί να επιτρέψει σε απομακρυσμένους επιτιθέμενους να δημιουργούν και να μιμούνται έναν σταθμό βάσης. Η επίθεση εκμεταλλεύεται ένα ελάττωμα εξακρίβωσης ταυτότητας στο πρότυπο GSM το οποίο επιτρέπει στο ψεύτικο σταθμό βάσης (*Rogue base station*) να ενεργεί ως ο ”άνθρωπος στη μέση” (*man-in-the-middle*) και να λαμβάνει κάθε κίνηση που αποστέλλεται μέσω του δικτύου GSM. Ένας άλλος τρόπος είναι με χρήση πινάκων ουρανίου τόξου (*rainbow tables*). Ένας προ-συντάκτης πίνακας των *hashes* που χρησιμοποιούνται συνήθως για να σπάσουν κωδικούς πρόσβασης. Στην περίπτωση του αλγορίθμου A5, αυτοί οι πίνακες είναι διαθέσιμοι δημόσια και κακόβουλοι χρήστες μπορούν να τις χρησιμοποιήσουν για να αποκτήσουν πρόσβαση στις εσωτερικές λειτουργίες ενός συστήματος που βασίζεται στο *GSM*.

Η πλαστογράφηση σταθμών βάσης εγκυμονεί σημαντικά προβλήματα ασφαλείας γύρω από την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (CIA) καθώς επηρεάζει όλες τις πτυχές του τριγώνου.

Επιπλέον, είναι καλό να ελεγχθεί αν υπάρχει δυνατότητα κρυπτογράφησης. Υπάρχει ο κίνδυνος εάν ο εισβολέας τροποποιήσει τα μηνύματα για να υποδείξει ότι ο σταθμός δεν

υποστηρίζει πρωτόκολλα κρυπτογράφησης, ο σταθμός θα υποβαθμίσει όλες τις επικοινωνίες σε αυτό το κανάλι σε μη κρυπτογραφημένο. Το πρότυπο GSM δηλώνει ότι οι κινητές συσκευές πρέπει να εμφανίζουν ένα μήνυμα με απενεργοποίηση κρυπτογράφησης, εάν η κρυπτογράφηση μεταξύ του σταθμού βάσης και του συνδρομητή κινητής τηλεφωνίας είναι απενεργοποιημένη. Όμως είναι πολύ συνηθισμένο για τους μεταφορείς και τις εταιρείες τηλεφωνίας να απενεργοποιήσουν αυτή την εγκατάσταση, καθώς πολλοί σταθμοί ενδέχεται να μην υποστηρίζουν την κρυπτογράφηση του GSM εξαιτίας πιθανών κακών υλοποιήσεων υλικού.

Τέλος, είναι καλό να εξεταστεί αν το σύστημα πάσχει από αδυναμίες σχετικές με την διεθνή ταυτότητα συνδρομητή κινητής τηλεφωνίας (*International mobile subscriber identity*) όπως είναι τα *IMSI bypassing* και *IMSI catching*. Μια περαιτέρω ευπάθεια σε συστήματα GSM είναι το βασικό υλικολογισμικό που χρησιμοποιείται στην συγκεκριμένη συσκευή και η εκμετάλλευση αδυναμιών στον κώδικά του[Pann15].

5.3.2 Αξιολόγηση διαχείρισης ισχύος

Πολλές φορές, η ασφάλεια των συσκευών που απαιτούν περοιρισμένη ισχύ έρχεται σε δεύτερη μοίρα σε σχέση με την ανάγκη για διαθεσιμότητα. Η ισχύς της μπαταρίας είναι ένας σημαντικός πόρος στην ασύρματη τεχνολογία, ειδικά για μικρές, κινητές συσκευές όπως είναι τα IoMT. Αυτό εισάγει στους σχεδιαστές το περίπλοκο πρόβλημα της επιλογής περισσότερης ασφάλειας σε βάρος της μεγαλύτερης χρήσης ενέργειας και δυνητικά λιγότερης διαθεσιμότητας υπηρεσιών.

Οι Stajano και Anderson [Staj01] πρότειναν την ιδέα των επιθέσεων εξάντλησης ενέργειας από το 1999. Μια αναδυόμενη κατηγορία επιθέσεων, η εξάντληση της μπαταρίας και η άρνηση του ύπνου αντιπροσωπεύουν κακόβουλες καταστάσεις όπου εξαντλείται η μπαταρία της συσκευής και ο χρήστης στερείται την πρόσβαση σε πληροφορίες. Δεδομένου ότι οι σχεδιαστές συστημάτων συσκευών με ενεργειακή ισχύ ενσωματώνουν διαχείριση ενέργειας, οι επιθέσεις που αναφέραμε επιδιώκουν να εκμεταλλευτούν το σύστημα διαχείρισης και ισχύος και να εμποδίσουν τη λειτουργία των συσκευών. Είναι σημαντικό να εξεταστεί αν είναι δυνατό να εφαμοστούν τέτοιου είδους επιθέσεις, ειδικά στο αντικείμενο μελέτης μας που πρόκειται για ζωτικής σημασίας ιατρική συσκευή που απαιτεί υψηλή διαθεσμότητα.

Βιβλιογραφία

[Agar16] Anurag Agarwal, "VAST Methodology: Visual, Agile, and Simple Threat Modeling.", 2016.

[Albe02] Christopher J. Alberts and Audrey Dorofee, *Managing Information Security Risks: The Octave Approach*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

[Amor94] Edward G. Amoroso, *Fundamentals of Computer Security Technology*, Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1994.

[Bast14] Tang T. Bastani F, "Improving security of wireless communication in medical devices.", December 2014.

[Brom16] Siri Bromander, Audun Jøsang and Martin Eian, "Semantic Cyberthreat Modelling", in *STIDS*, 2016.

[Case07] Timothy Casey, "Threat Agent Library Helps Identify Information Security Risks", 09 2007.

[Chen12] Yi Cheng, Mats Naslund, Göran Selander and Eva Fogelstrom, "Privacy in machine-to-machine communications A state-of-the-art survey", pp. 75–79, 11 2012.

[D15a] Pauli D., "Thousands of "directly hackable" hospital devices exposed online.", September 2015.

[D15b] Storm D., "Hackers hijacking medical devices to create backdoors in hospital networks.", June 2015.

[fore] "Big Data in Internet of Things (IoT):Key Trends, Opportunities and Market Forecasts 2015 - 2020".

[Freu14] Jack Freund and Jack Jones, *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, Newton, MA, USA, 1st edition, 2014.

[Gian13] M. Giannikos, K. Kokoli, N. Fotiou, G. F. Marias and G. C. Polyzos, "Towards secure and context-aware information lookup for the Internet of Things", in *2013 International Conference on Computing, Networking and Communications (ICNC 2013)*, pp. 632–636, Los Alamitos, CA, USA, jan 2013, IEEE Computer Society.

[Hall13] Rob Hall, Alessandro Rinaldo and Larry Wasserman, "Differential Privacy for Functions and Functional Data", *J. Mach. Learn. Res.*, vol. 14, no. 1, pp. 703–727, February 2013.

[Halp08] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses", in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pp. 129–142, May 2008.

[Haml17] James H. Hamlyn-Harris, "Three reasons why pacemakers are vulnerable to hacking", 9 2017.

[Hann11] Steve Hanna, Rolf Rolles, Andres Molina-Markham, Pongsin Poosankam, Jeremiah Blocki, Kevin Fu and Dawn Xiaodong Song, "Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices", in *HealthSec*, 2011.

[Hasa19] Ashikali Hasan and Dr. Divyakant Meva, "Web Application Safety by Penetration Testing", vol. 3, pp. 159–163, 01 2019.

[Hoss15] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", in *2015 IEEE World Congress on Services*, pp. 21–28, June 2015.

[Jala18] Kaiser-J.P. Jalali, M.S., "Cybersecurity in hospitals: a systematic, organizational perspective.", 2018.

[Jian] Du Jiang and Chao ShiWei, "A study of information security for M2M of IOT".

[Jing14] Qi Jing, Athanasios Vasilakos, Jiafu Wan, Jingwei Lu and Dechao Qiu, "Security of the Internet of Things: Perspectives and challenges", *Wireless Networks*, vol. 20, pp. 2481–2501, 11 2014.

[K] Zetter K., "It's insanely easy to hack hospital equipment.".

[Kher16] Mandeep Khera, "Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications", *Journal of Diabetes Science and Technology*, vol. 11, p. 1932296816677576, 12 2016.

[Kohn] Loren Kohnfelder and Praerit Garg, "Threats to our products".

[Liu14] Enqiang Liu, Zengliang Liu and Fei Shao, "Digital Rights Management and Access Control in Multimedia Social Networks", *Advances in Intelligent Systems and Computing*, vol. 238, pp. 257–266, 01 2014.

[Mamt16] Mamta and S. Prakash, "An overview of healthcare perspective based security issues in Wireless Sensor Networks", in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 870–875, March 2016.

[Mari06] L. Marinos, "Risk management and risk assessment at ENISA: issues and challenges", in *First International Conference on Availability, Reliability and Security (ARES'06)*, pp. 2 pp.–3, April 2006.

[Mavr17] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence", in *2017 European Intelligence and Security Informatics Conference (EISIC)*, pp. 91–98, Sep. 2017.

[McMi12] Robert McMillan, "The World's First Computer Password? It Was Useless Too", *Wired Business*, 2012.

[Newm17] Lily Hay Newman, "Medical Devices Are the Next Security Nightmare", 2 2017.

[Pann15] Mandeep Pannu, Robert Bird, Bob Gill and Kiran Patel, "Investigating Vulnerabilities in GSM Security", 10 2015.

[Rega13] Gilbert Regan, Fergal Mc Caffery, Kevin Mc Daid and Derek Flood, "Medical Device Standards' Requirements for Traceability During the Software Development Lifecycle and Implementation of a Traceability Assessment Model", *Comput. Stand. Interfaces*, vol. 36, no. 1, pp. 3–9, November 2013.

[Sait05] Paul Saitta, B. J. Larcom and Michael J. Eddington, "Trike v . 1 Methodology Document [Draft]", 2005.

[Salt98] Chris Salter, O. Sami Saydjari, Bruce Schneier and Jim Wallner, "Toward a Secure System Engineering Methodolgy", in *Proceedings of the 1998 Workshop on New Security Paradigms*, NSPW '98, pp. 2–10, New York, NY, USA, 1998, ACM.

[Scan15] Riccardo Scandariato, Kim Wuyts and Wouter Joosen, "A Descriptive Study of Microsoft's Threat Modeling Technique", *Requir. Eng.*, vol. 20, no. 2, pp. 163–180, June 2015.

[Shir00] Dr. Rob Shirey, "Internet Security Glossary", RFC 2828, May 2000.

[Shos14] Adam Shostack, *Threat Modeling: Designing for Security*, Wiley Publishing, 1st edition, 2014.

[Staj01] Frank Stajano, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", 10 2001.

[stat18] "Biosensors Market outlook will register 8% CAGR to overtake $29 billion by 2024", August 2018.

[Swid04] Frank Swiderski and Window Snyder, *Threat Modeling*, Microsoft Press, Redmond, WA, USA, 2004.

[syno17] "Synopsys and Ponemon Study Highlights Critical Security Deficiencies in Medical Devices", 5 2017.

[Team13] The Industrial Control Systems Cyber Emergency Response Team., "Medical devices hardcoded passwords.", 2013.

[Uced15] Tony UcedaVelez and Marco M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*, Wiley Publishing, 1st edition, 2015.

[Vish18] Gopal Vishwakarma and Wonjun Lee, “Exploiting JTAG and Its Mitigation in IOT: A Survey”, *Future Internet*, vol. 10, no. 12, 2018.

[Wan11] Jiafu Wan, Hehua Yan, Hui Suo and Fang Li, “Advances in Cyber-Physical Systems Research”, *TIIS*, vol. 5, pp. 1891–1908, 01 2011.

[Waur16] P. Waurzyniac, “Securing Manufacturing Data in the Cloud”, Jun 2016.

[Webe10] Rolf H. Weber, “Internet of Things – New security and privacy challenges”, *Computer Law Security Review*, vol. 26, no. 1, pp. 23 – 30, 2010.

[Zhou12] L. Zhou, Q. Wen and H. Zhang, “Preserving Sensor Location Privacy in Internet of Things”, in *2012 Fourth International Conference on Computational and Information Sciences*, pp. 856–859, Aug 2012.