Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Στην Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Αποδοτικοί Μηχανισμοί Ασφαλείας για το Διαδίκτυο των Πραγμάτων (IoT).

Αγορίτσα Κωστοπούλου

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Μάιος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Στην Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Αποδοτικοί Μηχανισμοί Ασφαλείας για το Διαδίκτυο των Πραγμάτων (IoT).

Αγορίτσα Κωστοπούλου

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2020

Περίληψη

Αντικείμενο της πτυχιακής εργασίας είναι η ανάπτυξη μίας μεθοδολογίας αντιμετώπισης ευπαθειών που μπορούν να εντοπιστούν σε ένα «έξυπνο νοσοκομείο». Αρχικά μέσα από την βιβλιογραφική έρευνα παρουσιάζουμε το οικοσύστημα του έξυπνου νοσοκομείου και τις σημαντικότερες απειλές που διατρέχουν από την ενσωμάτωση έξυπνων τεχνολογιών (Internet of Things). Κατόπιν προτείνουμε μία μεθοδολογία και εργαλεία που μπορούν να χρησιμοποιηθούν για τον εντοπισμό ευπαθειών σε ένα μικρό ιατρικό IoT δίκτυο. Ακολουθώντας τα βήματα της μεθοδολογίας και ενεργοποιώντας συγκεκριμένα εργαλεία, η μελέτη μας βοηθά να αναδείξουμε συγκεκριμένες ευπάθειες. Αναλύουμε τους πιθανούς τρόπους αντιμετώπισης των ευπαθειών, και υποβάλλουμε βασικές προτάσεις για την ενίσχυση της ασφάλειας των έξυπνων νοσοκομείων.

Summary

This thesis aims to propose a methodology for vulnerabilities management that can be identified in a 'smart hospital'. Initially, through a literature research, we present the smart hospital ecosystem and the major threats which are facing by the integration of smart technologies (Internet of Things). Then we propose a methodology and tools that can be used to identify vulnerabilities in a small medical IoT network. By following the steps of the methodology and activating specific tools, the study helps us identify specific vulnerabilities. We analyze possible ways to address these vulnerabilities, and make key suggestions to enhance the security of smart hospitals.

Ευχαριστίες

Πρώτα από όλους θα ήθελα να ευχαριστήσω τον επιβλέποντα Δρ. Νικόλαο Σκλάβο, Αναπληρωτή Καθηγητή του Τμήματος Μηχανικών Η/Υ και Πληροφορικής του Πανεπιστημίου Πατρών για την καθοδήγηση στις ερευνητικές μου αναζητήσεις, για τις πολύτιμες συμβουλές του και για την ενθάρρυνση που μου παρείχε καθ' όλη τη διάρκεια της διατριβής μου.

Επιπλέον, ευχαριστώ τους φίλους μου που με στήριξαν ψυχολογικά σε όλη τη διάρκεια της εκπόνησης της διατριβής μου και κυρίως κατά τη διάρκεια δύσκολων στιγμών.

Πάνω από όλα όμως, θα ήθελα να ευχαριστήσω την οικογένεια μου που είναι πάντα δίπλα μου σε όλη τη διάρκεια της ζωής μου και μου παρέχει αγάπη, κατανόηση, ανυπολόγιστη υποστήριξη και συμπαράσταση σε οτιδήποτε και αν επιχειρώ.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Τα τελευταία χρόνια έχουν προταθεί συστήματα που καλύπτουν μεγάλο φάσμα λειτουργιών στην υγειονομική περίθαλψη. Αυτά είναι τα λεγόμενα διάχυτα συστήματα (pervasive systems) και αντίστοιχα η διάχυτη υγειονομική περίθαλψη είναι εξαιρετικά πολύπλευρη, με πολλές εφαρμογές που επικεντρώνονται στη διαλειτουργικότητα με τα βασικά συστήματα ενός νοσοκομείου, την ασφάλεια, το απόρρητο των ευαίσθητων πληροφοριών και την εξυπηρέτηση των τελικών χρηστών [3].

Η έννοια του έξυπνου νοσοκομείου καθιερώνεται με την εισαγωγή στη ζωή μας του Ίντερνετ των πραγμάτων (Internet of Things - IoT) που μπορεί πλέον να υποστηρίξει σημαντικές λειτουργίες ενός νοσοκομείου. Επιπλέον η συνεργασία που απαιτείται μεταξύ διαφορετικών τμημάτων, οι πολυάριθμες διασυνδεδεμένες συσκευές και ταυτόχρονα οι απαιτήσεις για μεγαλύτερη ευελιξία αυξάνουν τη πολυπλοκότητα και τη δυναμική που ξεπερνούν κάθε οργανωτικά και διαχειριστικά όρια ενός παραδοσιακού νοσοκομείου. Λόγω του μεγάλου αριθμού των σημαντικών συσκευών από τις οποίες εξαρτώνται οι ζωές των ασθενών, ευαίσθητες προσωπικές πληροφορίες και οικονομικοί πόροι, η ασφάλεια των πληροφοριών αποτελεί βασικό ζήτημα για τα έξυπνα νοσοκομεία [4] , [31].

Ωστόσο, οι απειλές για τα έξυπνα νοσοκομεία δεν περιορίζονται σε κακόβουλες ενέργειες από την πλευρά της γενεσιουργούς αιτίας. Ανθρώπινα λάθη και αποτυχίες των συστημάτων καθώς και οι αποτυχίες τρίτων διαδραματίζουν επίσης σημαντικό ρόλο. Οι κίνδυνοι που προκύπτουν από αυτές τις απειλές και τα αντίστοιχα τρωτά σημεία (vulnerabilities) είναι συνήθως μετριασμένα από έναν συνδυασμό οργανωτικών και τεχνικών μέτρων ασφάλειας που λαμβάνουν τα έξυπνα νοσοκομεία και σύμφωνα με ορισμένες καλές πρακτικές στη διεθνή κοινότητα. Όσον αφορά τα οργανωτικά μέτρα που περιλαμβάνουν τη συμμόρφωση με τα πρότυπα, την κατάρτιση του προσωπικού και την ευαισθητοποίηση, η εφαρμογή μέτρων ασφάλειας με θεωρητικό υπόβαθρο και η χρήση κατευθυντήριων γραμμών και ορθών πρακτικών είναι ιδιαίτερα σημαντικές [5].

Τα σχετικά τεχνικά μέτρα περιλαμβάνουν την κατάτμηση του δικτύου, διαχείριση συσκευών και διαχείριση αλλαγών, παρακολούθηση δικτύου και ανίχνευση εισβολών. Ωστόσο, οι κατασκευαστές των συστημάτων πληροφοριών και οι συσκευές που χρησιμοποιούνται σε έξυπνα νοσοκομεία πρέπει να λάβουν ορισμένα μέτρα. Μεταξύ αυτών είναι, για παράδειγμα, η ενίσχυση της ασφάλειας στα προϊόντα από την αρχή της κατασκευής τους, η υιοθέτηση ασφαλών πρακτικών ανάπτυξης κώδικα και εκτεταμένων δοκιμών [6].

Το "Διαδίκτυο των πραγμάτων" είναι μια καινοτομία στον χώρο της Πληροφορικής και των Επικοινωνιών. Οι συσκευές, συστημικά μέσα και τα δίκτυα γίνονται αυτόνομα, πανταχού παρόντα και διασυνδεδεμένα. Όταν αυτή η τεχνολογική πρόοδος εφαρμόζεται και στην υγειονομική περίθαλψη, ένα από τους πιο παραδοσιακά κρίσιμους τομείς, τα αποτελέσματα είναι αξιοσημείωτα. Συνδεδεμένες ιατρικές συσκευές μπορούν να μεταμορφώσουν τον τρόπο με τον οποίο λειτουργεί η βιομηχανία της υγειονομικής περίθαλψης, τόσο εντός των νοσοκομείων όσο και μεταξύ των διαφόρων φορέων στον κλάδο της υγείας. [31]

Για παράδειγμα πλέον μια ηλεκτρονική συσκευή που συλλέγει πληροφορίες σχετικά με ζωτικά δεδομένα των ασθενών έχει μετατραπεί σε μία IoT συσκευή. Επίσης οι συσκευές μηχανικής υποστήριξης στην εντατική μπορούν πλέον να αντιδράσουν σε οποιαδήποτε αλλαγή της κατάστασης. Συνδεδεμένες ιατρικές συσκευές μπορούν να φέρουν αυξημένη ασφάλεια και αποτελεσματικότητα στην αντιμετώπιση των ασθενών, ιδιαίτερα εάν συνδέονται με κλινικά πληροφοριακά συστήματα. Όταν αυτό ισχύει για όλο το οικοσύστημα ενός οργανισμού στο χώρο της υγείας, γίνεται ένα "έξυπνο νοσοκομείο".

Ωστόσο, η αυξημένη ροή πληροφοριών εντός και μεταξύ των νοσοκομείων δημιουργεί κινδύνους που πρέπει να αντιμετωπιστούν από το προσωπικό που είναι υπεύθυνοι για την ασφάλεια (CIO, CISO κ.λπ.). Οι κίνδυνοι περιλαμβάνουν πιθανή βλάβη στην υγεία του ασθενούς ή απώλεια προσωπικών δεδομένων που αφορούν την υγεία και μπορούν όχι μόνο να προκληθούν από κακόβουλες ενέργειες, αλλά και από ανθρώπινα σφάλματα, σφάλματα σε ένα σύστημα ή τρίτο μέρος και φυσικά φαινόμενα. Καθώς το εύρος των επιθέσεων αυξάνεται με την εισαγωγή των συνδεδεμένων συσκευών, η δυναμική των επιθέσεων αυξάνεται εκθετικά [7].

1.1 Αντικείμενο της εργασίας

Αντικείμενο της πτυχιακής εργασίας είναι η ανάπτυξη μίας μεθοδολογίας αντιμετώπισης ευπαθειών που μπορούν να εντοπιστούν σε ένα «έξυπνο νοσοκομείο». Αφού γίνει μία ανασκόπηση της βιβλιογραφίας για την αρχιτεκτονική, τη δομή και τον τρόπο λειτουργίας ενός έξυπνου νοσοκομείου με βάση τις σύγχρονες τεχνολογικές εξελίξεις στο χώρο του IoT, επόμενος στόχος της προτεινόμενης μεθοδολογίας είναι να προτείνει συγκεκριμένα εργαλεία και διαδικασίες για τον εντοπισμό ευπαθειών στο παραπάνω οικοσύστημα. Ανάλογα με τη φύση των ευπαθειών η εργασία καλείται να προτείνει ένα φάσμα λύσεων που θα βοηθήσει το προσωπικό της ασφάλειας πληροφοριών σε ένα τέτοιο οργανισμό να καλύψει τις ευπάθειες και να θωρακίσει την ασφάλεια του με ακόμη περισσότερα μέτρα.

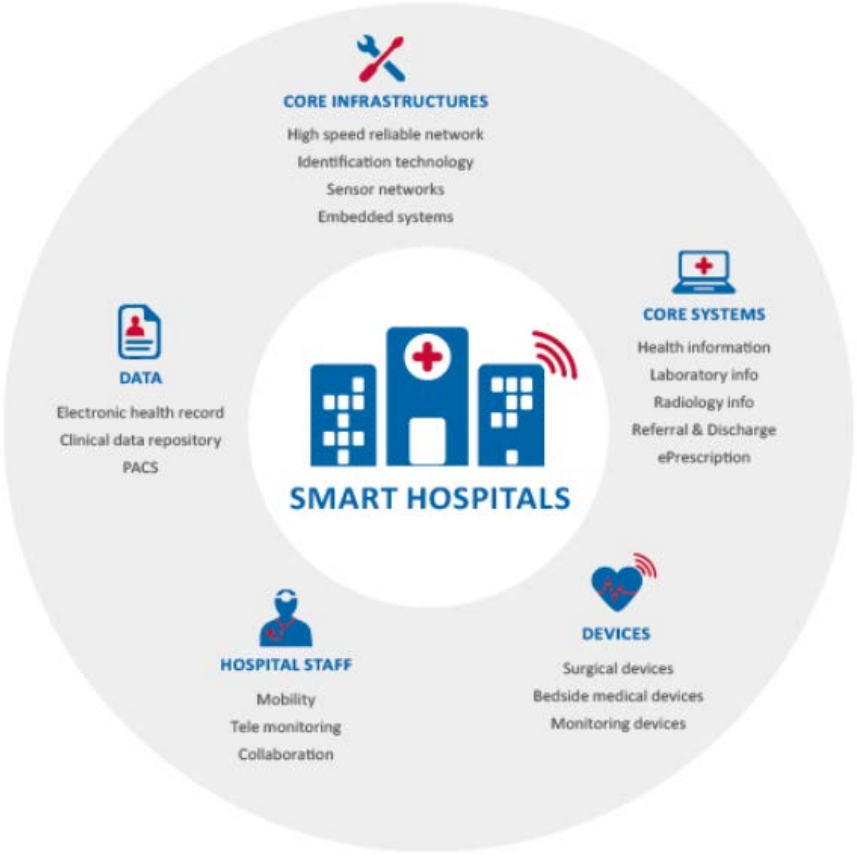
Στο κεφάλαιο 2 παρουσιάζεται μέσα από τη Βιβλιογραφία το οικοσύστημα του έξυπνου νοσοκομείου. Στη συνέχεια αναλύουμε κατηγορίες από ευπάθειες που έχουν καταγραφεί μέσα από μελέτες περίπτωσης άλλων ερευνητών. Στο κεφάλαιο 3 παρουσιάζουμε μία τυπική IoT αρχιτεκτονική Έξυπνου Νοσοκομείου. Η αρχιτεκτονική βασίζεται σε ένα μοντέλο τριών επιπέδων με πυρήνα τους τις Έξυπνες Ιατρικές Πύλες. Το κεφάλαιο 4 ορίζει τη μεθοδολογία και τα εργαλεία που θα χρησιμοποιήσουμε για τον εντοπισμό ευπαθειών σε μία υποθετική έξυπνη ιατρική πύλη που διαχειρίζεται τα δεδομένα από IoT συσκευές. Θα παρουσιάσουμε τα εργαλεία και τα βήματα εφαρμογής της μεθοδολογίας πάνω στις συγκεκριμένες έξυπνες συσκευές ως μελέτη περίπτωσης. Στο κεφάλαιο 5 θα παρουσιάσουμε τα αποτελέσματα και θα αναλύσουμε τους πιθανούς τρόπους αντιμετώπισης των πιθανών ευπαθειών. Το κεφάλαιο 6 ολοκληρώνει την πτυχιακή με τα συμπεράσματα.

Κεφάλαιο 2
Ανασκόπηση Βιβλιογραφίας

2.1 Έξυπνο νοσοκομείο

Οι βασικές συνιστώσες του παραδοσιακού νοσοκομείου απεικονίζονται στην εικόνα 2.1. Ως μία νέα εξέλιξη του παραδοσιακού νοσοκομείου, ο πρωταρχικός στόχος των έξυπνων νοσοκομείων είναι η βέλτιστη φροντίδα των ασθενών, αξιοποιώντας στο έπακρο τις προηγμένες τεχνολογίες πληροφορικής και τηλεπικοινωνιών [8]:

- Η διαθεσιμότητα όλων των σχετικών πληροφοριών όταν απαιτείται
- Η πρόσβαση σε τεχνογνωσία στο εσωτερικό και εξωτερικό του οργανισμού όταν απαιτείται και
- Αποδοτικές και αποτελεσματικές διαδικασίες χειρουργικής / διάγνωσης που διευκολύνουν την επίτευξη αυτού του στόχου με χαμηλό ποσοστό σφάλματος και κόστους.



Εικόνα 2.1. Οι βασικές συνιστώσες του παραδοσιακού νοσοκομείου [1].

Αυτό που καθιστά ένα νοσοκομείο έξυπνο είναι, ως εκ τούτου, η διαθεσιμότητα και η χρήση ουσιαστικά διασυνδεδεμένων συστημάτων και συσκευών που πετυχαίνουν μία συνολική ευφυΐα. Αν και τα παραδοσιακά ιατρικά συστήματα μπορούν πράγματι να αποτελέσουν αναπόσπαστο κομμάτι του ευφυούς συστήματος, η έμφαση στην παρούσα διατριβή δίνεται στις νέες τεχνολογίες, και ιδίως τα συστατικά στοιχεία του IoT.

Εικόνα 2.2. Οι στόχοι του έξυπνου νοσοκομείου (EN) [8]

Ανάλογα με τις τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) και την έκταση τους στη νέα γενιά ιατρικών υπηρεσιών επηρεάζουν αντίστοιχα τους στόχους καθώς και τις συναφείς προκλήσεις και ευκαιρίες [9]:

- Βελτιωμένες υπηρεσίες διάγνωσης / χειρουργικής: Οι ΤΠΕ δεν επιτρέπουν μόνο νέες μεθόδους θεραπείας (π.χ. τα ρομπότ μπορούν να εκτελούν επεμβάσεις μικροχειρουργικής, οι οποίες δεν μπορούν να γίνουν από τους κλινικούς ιατρούς), αλλά μπορούν επίσης να βελτιώσουν τις υπάρχουσες μεθόδους. Τα νοσοκομεία είναι ολοένα και πιο ικανά να εξάγουν δεδομένα ασθενών για να βοηθήσουν στη διάγνωση ή στην επιλογή της καλύτερης θεραπείας και οι εξελιγμένες λύσεις λογισμικού τους επιτρέπουν να βελτιώσουν τις εμπειρίες τους αναφορικά με τις διοικητικές διαδικασίες.

- Ροή ασθενών χωρίς εμπόδια/ενδιάμεσες διαδικασίες: Η αποτελεσματική υγειονομική περίθαλψη καθώς και η αποτελεσματική ροή ασθενών μπορούν να μειώσουν το χρόνο αναμονής και την ανακούφιση των ασθενών στη διάρκεια της διαμονής τους στο νοσοκομείο. Η μείωση των λαθών, η αύξηση των εσόδων και η τόνωση των ασθενών (και

των εργαζομένων) πετυχαίνουν τον στόχο της μεγαλύτερης ικανοποίησης ασθενών και εργαζομένων.

Οι ΤΠΕ μπορούν να χρησιμοποιηθούν για τον εντοπισμό, την ανάλυση και την επίλυση των σημείων συμφόρησης και με τον τρόπο αυτό να συμβάλουν αποτελεσματικά στην υγειονομική περίθαλψη και τη ροή των ασθενών. Σε έξυπνα νοσοκομεία, η αποτελεσματική υγειονομική περίθαλψη και η αποτελεσματική ροή ασθενών μπορεί, για παράδειγμα, να υποστηρίζονται από αυτόματες ενημερώσεις με ιατρικές πληροφορίες που εξάγονται από δικτυακές συσκευές και πληροφοριακά συστήματα. Η προκύπτουσα διαθεσιμότητα πληροφοριών για τους ασθενείς σε όλα τα στάδια - από την είσοδο στην έξοδο – και η βελτιστοποίηση της εισαγωγής, ο προγραμματισμός και άλλες διαδικασίες γύρω από αυτό οδηγούν στην ομαλή ροή των ασθενών μέσα στον οργανισμό.

- Απομακρυσμένη ιατρική περίθαλψη: Ένας από τους βασικούς στόχους της εισαγωγής συσκευών διαδικτύου στην υγειονομική περίθαλψη είναι η ικανότητα επέκτασης των νοσοκομειακών συνόρων και παροχή ιατρικής φροντίδας από απόσταση. Διάφορες ιατρικές συσκευές, π.χ. οι εμφυτεύσιμες συσκευές, οι φορητές συσκευές και άλλες κινητές συσκευές εισάγουν την ικανότητα να εκτελούν σε πραγματικό χρόνο παρακολούθηση ασθενών μέσω μέτρησης βασικών σημείων ζωτικής σημασίας και να καταστήσουν αυτές τις μετρήσεις άμεσα διαθέσιμες στο ιατρικό προσωπικό και τα απαραίτητα συστήματα μέσω δικτύου [10].

  Αυτές οι απομακρυσμένες δυνατότητες φροντίδας ασθενών είναι που επεκτείνονται με διάφορες ιατρικές συσκευές που προσφέρουν τη δυνατότητα δράσης (π.χ., χορήγηση ιατρικής δόσης) στον ασθενή ανάλογα με την κατάσταση ή μέσω των τηλεχειριστηρίων. Ως εκ τούτου, η εισαγωγή ασθενών στα νοσοκομεία μπορεί να περιορίζεται σε εκείνες τις περιπτώσεις που κρίνονται απαραίτητες, με αποτέλεσμα τη μείωση του κόστους περίθαλψης των ασθενών και τη βελτίωση της εμπειρίας των ασθενών, καθώς ο ασθενής μπορεί τώρα να λάβει θεραπεία από το δικό του σπίτι.

- Βελτιωμένη ασφάλεια των ασθενών: Η αύξηση της παροχής υγειονομικής περίθαλψης και η ροή των ασθενών αυξάνουν επίσης την προστασία του ασθενή και την κλινική του φροντίδα. Είναι σημαντικό, ωστόσο, ότι η παροχή υγειονομικής περίθαλψης και η ροή ασθενών δεν βελτιώνονται εις βάρος της υγείας του. Χωρίς αμφιβολία, σωστά χρησιμοποιούμενες συσκευές που συλλέγουν δεδομένα σχετικά με τα ζωτικά σημεία του

ασθενούς και τη φαρμακευτική του αγωγή, την παρακολούθηση των μηχανών υποστήριξης της ζωής του (πχ στην εντατική), μπορούν να οδηγήσουν σε αυξημένη ασφάλεια της ζωής του ασθενούς εάν συνδέονται στο δίκτυο και είναι σε θέση να παρέχουν έγκαιρη προειδοποίηση.

- Κυβερνοασφάλεια: αναφέρεται στην ικανότητα ενός νοσοκομείου να εξασφαλίζει τη διαθεσιμότητα και τη συνέχεια των υπηρεσιών της που βασίζονται σε ΤΠΕ. Η μεγαλύτερη διείσδυση των ΤΠΕ οδηγεί αναπόφευκτα σε μεγαλύτερη εξάρτηση από τις ΤΠΕ, η οποία με τη σειρά της αυξάνει τη σημασία της ασφάλειας των πληροφοριών για τα έξυπνα νοσοκομεία. Σε κάποιες ευρωπαϊκές χώρες, ο τομέας της υγείας θεωρείται μία κρίσιμη υποδομή που πρέπει να προστατεύεται ιδιαίτερα [6].

Οι φορείς στη φροντίδα υγείας, συμπεριλαμβανομένων των νοσοκομείων, πρέπει να προβλέπουν, να προετοιμάζονται και να ανταποκρίνονται και να προσαρμόζονται όχι μόνο σε μία σταδιακή αλλαγή αλλά και σε ξαφνικά γεγονότα. Σε έξυπνα νοσοκομεία, η επίτευξη αυτού του στόχου είναι πιο δύσκολη από ότι στα παραδοσιακά νοσοκομεία γιατί ο αριθμός των συσκευών ή συστημάτων που θα μπορούσαν να επηρεαστούν από τη μη διαθεσιμότητα μίας υπηρεσίας είναι πολύ υψηλότερη.

- Αξιοπιστία: Το να θεωρείται ένα ΕΝ αξιόπιστο και να έχει καλή φήμη αποτελεί ανταγωνιστικό ζήτημα ειδικά σε γεωγραφικές περιοχές όπου οι ασθενείς έχουν την επιλογή μεταξύ διαφορετικών παρόχων. Η αξιοπιστία επηρεάζει επίσης την τήρηση της φαρμακευτικής αγωγής και της συνέχειας της περίθαλψης, γεγονός που έχει σημασία για τα αποτελέσματα που μπορεί να επιτύχει ένα νοσοκομείο. Ένα ΕΝ που είναι στο προσκήνιο όσον αφορά τη χρήση των ΤΠΕ του παρέχει σαφώς μεγαλύτερη φήμη. Την ίδια στιγμή, η ασφάλεια των ασθενών και της ιδιωτικής τους ζωής δεν πρέπει να τίθενται σε κίνδυνο για να αποφευχθεί ακριβώς το αντίθετο αποτέλεσμα (της κακής φήμης).

2.2 Συστήματα/ Συσκευές Έξυπνου νοσοκομείου

Τα νοσοκομεία διαθέτουν ένα ευρύ φάσμα συστημάτων και συσκευών που είναι απαραίτητα για τη λειτουργία τους και επομένως πρέπει να προστατεύονται. Ενώ ορισμένα συστήματα των έξυπνων νοσοκομείων είναι επίσης διαθέσιμα στα παραδοσιακά νοσοκομεία, άλλα είναι μόνο διαθέσιμα σε ΕΝ δεδομένου ότι έχουν το χαρακτηριστικό της έξυπνης σύνδεσης και της

αυτόνομης λήψης αποφάσεων. Μεταξύ αυτών των συστημάτων και συσκευών είναι, για παράδειγμα, κινητές συσκευές τελικού χρήστη, συστήματα αναγνώρισης και διασυνδεδεμένα συστήματα κλινικής πληροφόρησης. Τα συγκεκριμένα στοιχεία (assets) που χαρακτηρίζουν τα έξυπνα νοσοκομεία παρουσιάζονται πιο αναλυτικά σε αυτή την ενότητα [11].

1. Τα στοιχεία ενός συστήματος απομακρυσμένης περίθαλψης ορίζουν ένα φάσμα τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) που επιτρέπουν στο ευφυές νοσοκομείο να επεκτείνει τα σύνορά του και να παρέχει υπηρεσίες υγειονομικής περίθαλψης σε ασθενείς σε απομακρυσμένες τοποθεσίες (π.χ. στο σπίτι):

    - ιατρικός εξοπλισμός για τηλε-παρακολούθηση και τηλε-διάγνωση (π.χ. μετρήσεις της αρτηριακής πίεσης, του καρδιακού ρυθμού, μετρήσεις γλυκόζης, ηλεκτροκαρδιογραφήματα και άλλες απομακρυσμένες φυσιολογικές μετρήσεις που στέλνουν σήματα κινδύνου εφόσον οι τιμές ξεπεράσουν κάποια όρια ελέγχου κ.λπ.), ο εξοπλισμός αυτός μπορεί να λάβει τη μορφή φορητών ή εμφυτεύσιμων συσκευών

    - ιατρικός εξοπλισμός για τη διανομή φαρμάκων (αυτοματοποιημένος εξοπλισμός δοσολογίας) ή για τη χορήγηση θεραπείας

    - τηλεϊατρικός εξοπλισμός, όπως κάμερες, αισθητήρες και συνδέσεις τηλεφώνου / διαδικτύου, ηλεκτρονικό σύστημα για τους ασθενείς να καταχωρούν οι ίδιες τις φυσιολογικές μετρήσεις τους (συμπεριλαμβανομένης της εφαρμογής στη πλευρά του ασθενούς, εάν υπάρχει)

2. Δίκτυα ιατρικών συσκευών των οποίων η εκτεταμένη χρήση τυπικά χαρακτηρίζει έξυπνα νοσοκομεία και επίσης επιτρέπει την απομακρυσμένη παρακολούθηση ασθενών, η οποία αποτελεί βασική υπηρεσία που μπορούν να προσφέρουν τα έξυπνα νοσοκομεία στη διαχείριση της υγειονομικής περίθαλψης σε ένα εθνικό επίπεδο σε σύγκριση με τα παραδοσιακά νοσοκομεία. Επιπλέον, οι σύγχρονες εμφυτεύσιμες συσκευές, όπως οι βηματοδότες, μπορούν να ενημερωθούν, μειώνοντας τον αριθμό των λόγων αντικατάστασης. Σταθερές καθώς και κινητές συσκευές έχουν επίσης χρησιμοποιηθεί σε μεγάλο βαθμό στα παραδοσιακά νοσοκομεία. Ωστόσο, στο περιβάλλον του ΕΝ, τα έξυπνα συνδεδεμένα στοιχεία ταυτοποίησης χρηστών και συστήματα κλινικών πληροφοριών αυξάνουν το επίπεδο αυτοματισμού και την ικανότητα λήψης αποφάσεων. Ορισμένα παραδείγματα αυτών των συστημάτων είναι [12]:

- κινητές συσκευές (π.χ. συσκευές μέτρησης γλυκόζης)

- φορητές εξωτερικές συσκευές (π.χ. φορητές αντλίες ινσουλίνης, μετρητές ασύρματης θερμοκρασίας)

- εμφυτεύσιμες συσκευές (π.χ. καρδιακοί βηματοδότες)

- σταθερές συσκευές (π.χ. τομογράφοι υπολογιστών (CT), μηχανήματα υποστήριξης ζωής, σταθμοί διανομής χημειοθεραπείας)

- υποστηρικτικές συσκευές (π.χ. βοηθητικά ρομπότ).

3. Τα συστήματα αναγνώρισης χρησιμοποιούνται για τον εντοπισμό και την ταυτοποίηση των ασθενών, του προσωπικού ή του νοσοκομειακού εξοπλισμού, όπως είναι τα κρεβάτια. Στα ΕΝ, οι βιομετρικοί σαρωτές διαβάζουν όχι μόνο τα συστήματα ταυτοποίησης αλλά και έξυπνα δικτυωμένες συσκευές και συστήματα πληροφοριών. Επιπλέον, τα συστήματα ασφαλείας κλειστού κυκλώματος διαδραματίζουν βασικό ρόλο όσον αφορά τον έλεγχο ταυτότητας - και στη συνέχεια επίσης την εξουσιοδότηση (π.χ. επιτρέποντας την πρόσβαση σε συγκεκριμένες ζώνες του κτιρίου) σε έξυπνες εφαρμογές του νοσοκομείου [13]. Παραδείγματα περιλαμβάνουν:

    - Στοιχεία συστημάτων ταυτοποίησης όπως ετικέτες, βραχιόλια, ετικέτες και έξυπνα διακριτικά (π.χ. με δυνατότητα υπερήχων)

    - Βιομετρικοί σαρωτές

    - Συστήματα RFID με υπηρεσίες εντοπισμού θέσης (στοιχεία λογισμικού) για την εκτίμηση και την παρακολούθηση της σχετικής κίνησης σε συστημικά στοιχεία / ασθενείς / προσωπικό κ.λπ.

    - CCTV (επιτήρηση βίντεο) με δυνατότητες αναγνώρισης / ελέγχου ταυτότητας

4. Εξοπλισμός δικτύωσης παρέχει τη ραχοκοκαλιά διασύνδεσης για την υποστήριξη των έξυπνων νοσοκομείων. Απαιτείται ο απαιτούμενος εξοπλισμός ο οποίος δε διαφέρει από τον τυποποιημένο εξοπλισμό που χρησιμοποιείται σε παραδοσιακό νοσοκομείο, αλλά

χαρακτηρίζεται από ορισμένα ενισχυμένα χαρακτηριστικά (π.χ. πρωτόκολλα δρομολόγησης, εύρος ζώνης). Παραδείγματα περιλαμβάνουν:

- Μέσα μετάδοσης
- Κάρτες διασύνδεσης δικτύου
- Συσκευές δικτύου κορμού (π.χ. κόμβοι, διακόπτες, δρομολογητές κ.λπ.)
- IoT Gateways που αναλύουν περαιτέρω τα δεδομένα που συλλέγονται από συσκευές και τα στέλνουν σε ένα κέντρο δεδομένων ή στο υπολογιστικό νέφος [4]

5. Κινητές συσκευές τελικού χρήστη είναι έξυπνα ενσωματωμένες σε έξυπνα νοσοκομεία για να παρέχουν τις σωστές πληροφορίες στο σωστό μέρος την κατάλληλη στιγμή και να διευκολυνθεί η κινητικότητα του προσωπικού και των ασθενών. Παραδείγματα περιλαμβάνουν:

   - Κινητές συσκευές τελικού χρήστη (π.χ. φορητοί υπολογιστές, tablet, smartphone, τηλεειδοποιητές)
   - Κινητές εφαρμογές για smartphone και tablet
   - Εφαρμογές συναγερμού και έκτακτης ανάγκης για κινητές συσκευές.

6. Τα διασυνδεδεμένα κλινικά πληροφοριακά συστήματα αναπτύσσονται σε έξυπνα νοσοκομεία από κοινού με ιατρικές συσκευές και συσκευές ταυτοποίησης για την παροχή έξυπνων διαδικασιών φροντίδας ασθενών από άκρο σε άκρο. Επιπλέον, το κλινικό δίκτυο, τα συστήματα πληροφοριών σε έξυπνα νοσοκομεία είναι όλο και περισσότερο σε θέση να λαμβάνουν αποφάσεις αυτόνομα. Παραδείγματα περιλαμβάνουν [3]:

   - Πληροφοριακά συστήματα νοσοκομείων (HIS)
   - Εργαστηριακά συστήματα πληροφοριών (LIS)
   - Συστήματα πληροφοριών ραδιολογίας (RIS)

- Σύστημα Πληροφοριών Φαρμακευτικής (PIS)
- Παθολογικό σύστημα πληροφοριών
- Σύστημα τραπεζών αίματος
- Συστήματα αρχειοθέτησης εικόνων και επικοινωνιών (PACS)
- Ερευνητικό πληροφοριακό σύστημα.

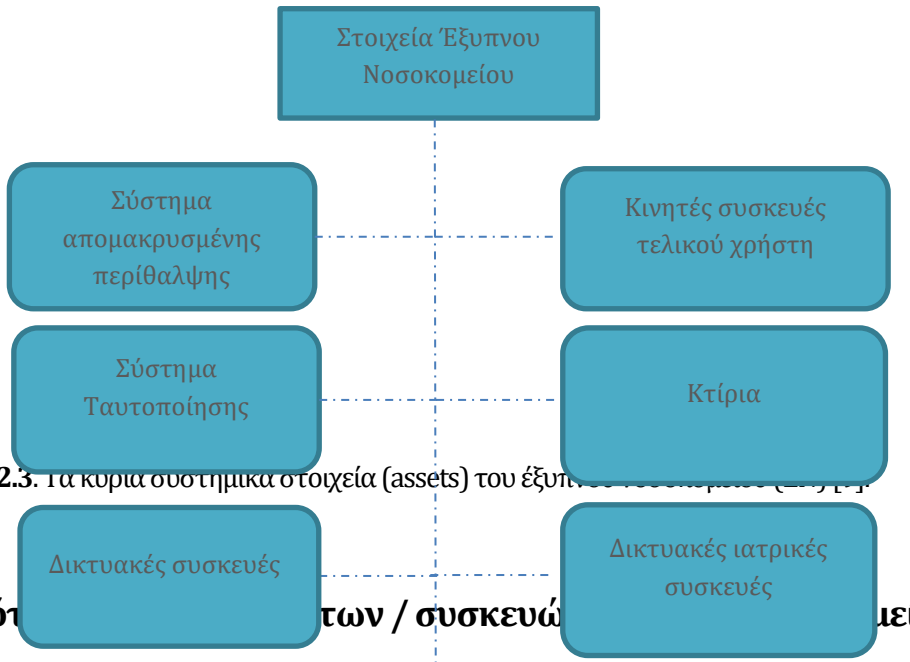
7. Τα δεδομένα θεωρούνται συχνά σημαντικά στοιχεία ενεργητικού από την άποψη της ασφάλειας των πληροφοριών. Κυρίως έξυπνες αποφάσεις που θα λάβει η συσκευή βασίζονται στην ανάλυση των συλλεγόμενων δεδομένων. Παραδείγματα περιλαμβάνουν:
    - Κλινικά και διοικητικά δεδομένα ασθενών (π.χ. ιατρικά αρχεία, αποτελέσματα δοκιμών, στοιχεία επικοινωνίας)
    - Οικονομικά, οργανωτικά και άλλα νοσοκομειακά δεδομένα
    - Στοιχεία έρευνας (π.χ. εκθέσεις κλινικών δοκιμών) και δεδομένα που προορίζονται για δευτερογενή χρήση
    - Δεδομένα προσωπικού
    - Παρακολούθηση καταγραφών
    - Στοιχεία προμηθευτών (π.χ. στοιχεία επικοινωνίας, προϊόντα που χρησιμοποιούνται).
8. Τα κτίρια και οι εγκαταστάσεις, συμπεριλαμβανομένων των έξυπνων διεργασιών που τελούν υπό τη διαχείριση και που διαχειρίζονται διάφορες λειτουργίες, είναι κρίσιμες για τη λειτουργία των έξυπνων νοσοκομείων. Ορισμένες κρίσιμες λειτουργίες που σχετίζονται με την ασφάλεια των ασθενών βασίζονται στις δυνατότητες των ευφυών συστημάτων διαχείρισης εγκαταστάσεων. Παραδείγματα περιλαμβάνουν:
    - Συστήματα ελέγχου ισχύος και κλιματισμού, συμπεριλαμβανομένων συστημάτων έξυπνου εξαερισμού

- Αισθητήρες θερμοκρασίας

- Ιατρική παροχή φυσικού αερίου

- Έξυπνες λειτουργίες και συστήματα διαχείρισης των δωματίων ασθενών, συμπεριλαμβανομένων έξυπνων πινακίδων, οθονών ασθενών, ιατρικών οθονών προσωπικού

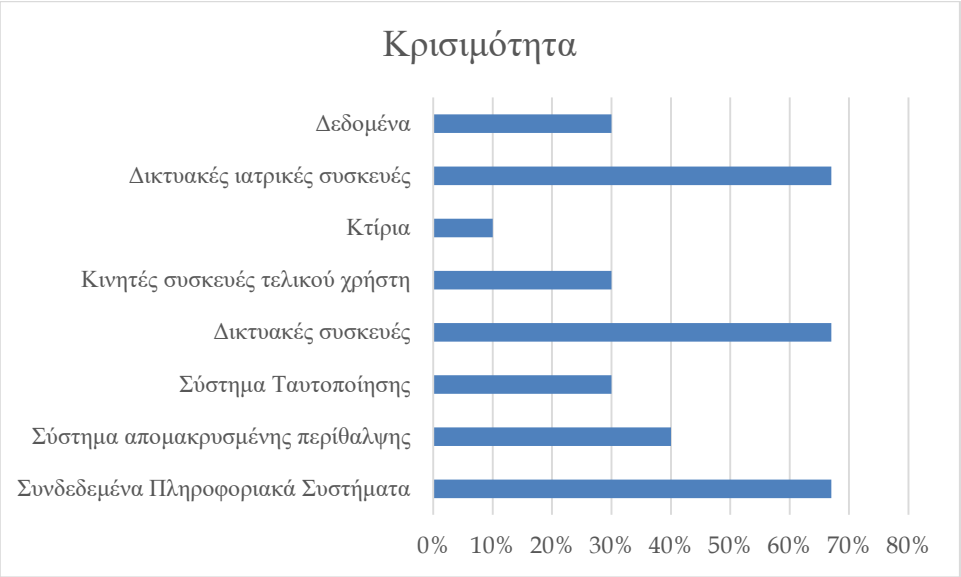
- Αυτοματοποιημένο σύστημα κλειδώματος θυρών, συμπεριλαμβανομένων έξυπνων κλειδαριών (π.χ. διασυνδεδεμένες κλειδαριές, ασύρματες κλειδαριές κ.λπ.), εφαρμογές κλειδώματος (π.χ. ξεκλείδωμα μέσω κινητής συσκευής) και διαχείριση κλειδώματος μέσω λογισμικού



Εικόνα 2.3. Τα κυρία συστημικά στοιχεία (assets) του έξυπ[illegible]

2.2.1 Κρισιμότ[illegible]των / συσκευώ[illegible]μείου

Στο περιβάλλον τ[illegible]ου, δεν έχουν όλα τα στοιχεία ενεργητικού την ίδια κρισιμότητα για τ[illegible] και προσφορά υπηρεσιών. Ένα συστημικό στοιχείο χαρακτηρίζεται ω[illegible]αδήποτε διακοπή [illegible]ς μεγάλο αντίκτυπο στη λειτουργία του συνολικού συστήματος αλλά κα[illegible]χεία που παρουσιάστηκαν στην παραπάνω ενότητα εκτιμήθηκαν μ[illegible] που θα μπορούσε να προκαλέσει η διακοπή της υπηρεσίας τους, δηλαδή η κρισιμότητα τους, μέσα από διάφορες έρευνες.



Εικόνα 2.4. Η κρισιμότητα των κύριων συστημικών στοιχείων (assets) του έξυπνου νοσοκομείου [1].

Τα πιο κρίσιμα έξυπνα στοιχεία ενεργητικού στο πλαίσιο ενός έξυπνου νοσοκομείου είναι τα διασυνδεδεμένα κλινικά πληροφοριακά συστήματα και οι συνδεδεμένες ιατρικές συσκευές. Αυτό μπορεί να εξηγηθεί από τον σημαντικό ρόλο που παίζουν στα έξυπνα νοσοκομεία. Η παρουσία έξυπνων συστημάτων κλινικής πληροφόρησης και ολοένα και πιο αυτόνομων ιατρικών συσκευών μεταξύ των πιο προφανών αλλαγών κατά τη διάρκεια του ψηφιακού μετασχηματισμού ενός νοσοκομείου σε ένα έξυπνο νοσοκομείο [3].

Η επίτευξη πολλών από τους βασικούς στόχους που συνδέονται με τα έξυπνα νοσοκομεία εξαρτώνται έντονα από τη διαθεσιμότητα αξιόπιστων και συνδεδεμένων συστημάτων κλινικής πληροφόρησης και ιατρικών συσκευών. Επιπλέον, προκειμένου να επιτευχθεί βελτιωμένη ιατρική περίθαλψη και βελτιωμένες διαγνωστικές δυνατότητες, τα εξαρτήματα και συσκευές του IoT αντικαθιστούν παλαιότερα συστήματα ζωτικής σημασίας για τη λειτουργία του νοσοκομείου. Αυτό το καθιστά άμεσα κρίσιμο όχι μόνο για την ασφάλεια του ασθενούς, αλλά και για τη συνολική λειτουργία του νοσοκομείου [6].

Ο εξοπλισμός δικτύωσης θεωρείται κρίσιμος δεδομένου ότι αποτελεί τη ραχοκοκαλιά του EN. Χωρίς μία αρχιτεκτονική ενός σταθερού δικτύου, οι αυξημένες δυνατότητες στο πλαίσιο εύρους ζώνης ή οι διαλειτουργικές λύσεις ανάμεσα στα στοιχεία του IoT δεν θα λειτουργούσαν σωστά. Πιο συγκεκριμένα, οι πληροφορίες που συλλέγονται από ιατρικές συσκευές ή από τα τελικά συστατικά χρειάζονται να αναλύονται και να συνδυάζονται με άλλες ιατρικές πληροφορίες. Αυτές

συνήθως αποθηκεύονται στα διασυνδεδεμένα κλινικά πληροφοριακά συστήματα του νοσοκομείου καθώς και από τρίτους [14].

Οι περισσότερες από τις αναλύσεις, ωστόσο, δεν διεξάγονται από τα ιατροτεχνολογικά προϊόντα ούτε από τα κλινικά συστήματα πληροφοριών, αλλά από ένα κεντρικό σύστημα το οποίο είναι εξοπλισμένο με την τεχνολογία για την αποτελεσματική συγκέντρωση και ανάλυση δεδομένων από διάφορες εσωτερικές και εξωτερικές πηγές. Η δικτύωση είναι απαραίτητη για τη λήψη των δεδομένων από τα συστήματα πληροφοριών και τις ιατρικές συσκευές στο σύστημα λήψης αποφάσεων (πχ οι ενδείξεις από βιομετρικά στοιχεία στην εντατική μπορούν να υποδεικνύουν την ανάγκη αναθεώρησης της συνταγής φαρμάκων) [14].

Ένας από τους κύριους στόχους του ΕΝ είναι να είναι σε θέση να προσφέρει υπηρεσίες απομακρυσμένης περίθαλψης. Για να επιτευχθεί αυτό τα νοσοκομειακά συστήματα πρέπει να συνδεθούν με τα συστήματα απομακρυσμένης περίθαλψης στο χώρο των ασθενών. Η δυσκολία που προκύπτει από αυτή τη ρύθμιση είναι ότι σε περίπτωση δυσλειτουργίας ή διακοπής η συσκευή / σύστημα θα αποκατασταθεί από τον αντίστοιχο προμηθευτή, καθώς δεν εμπίπτει στην ευθύνη του νοσοκομείου. Αυτό εξηγεί και τον χαμηλό βαθμό κρισιμότητας όπως εξηγήθηκε παραπάνω, παρά την σημασία των δεδομένων που συλλέγει αυτό το σύστημα για τη διάγνωση και τη συνταγογράφηση φαρμάκων.

Στη συνέχεια της κατάταξης βρίσκονται τα δεδομένα (στοιχεία έρευνας, αρχεία καταγραφής δεδομένων κ.λπ.), οι κινητές υπηρεσίες στο επίπεδο του τελικού χρήστη και τα συστήματα ταυτοποίησης. Αν και αυτά είναι πολύ σημαντικά στοιχεία για τη λειτουργία ενός έξυπνου νοσοκομείου, καθώς δεν υποστηρίζουν τον πυρήνα (η χρήση τους μπορεί να εκτείνεται από λόγους ευαισθητοποίησης έως απομακρυσμένη διάγνωση ή πρόσβαση) οποιαδήποτε διακοπή δεν θα προκαλούσε μεγάλη διακοπή στην παροχή των νοσοκομειακών υπηρεσιών.

Τελευταία στην κατάταξη έρχεται το κτίριο και οι εγκαταστάσεις. Σε αυτή την περίπτωση, η επίδραση μιας διακοπής – αν θα συμβεί - είναι πολύ μεγάλη, ωστόσο, καθώς η πιθανότητα είναι πολύ χαμηλή, έρχεται τελευταία στην κατάταξη. Ωστόσο, μελέτες έχουν δείξει ότι οι επιθέσεις στον κυβερνοχώρο που στοχεύουν τα συστήματα των εγκαταστάσεων (ρύθμιση του κλίματος, της ισχύς της παροχής, κλπ.) δεν είναι τόσο συνηθισμένες, διότι, αφενός, απαιτούν υψηλή τεχνογνωσία και πολυπλοκότητα και, από την άλλη πλευρά, το αποτέλεσμα δεν θα αποφέρει κανένα οικονομικό όφελος για τον κακόβουλο εισβολέα (όπως στην περίπτωση της ransomware επίθεσης).

2.3 Ευπάθειες Έξυπνου Νοσοκομείου

Σε αυτή την ενότητα περιγράφουμε λεπτομερώς τα πιο κοινά σημεία ευπάθειας που πρέπει να ληφθούν υπόψη από τα έξυπνα νοσοκομεία. Η λίστα δεν αποτελείται μόνο από τεχνικές ευπάθειες, αλλά επεκτείνεται σε οργανισμούς και σε κοινωνικές πτυχές. Οι απειλές συνήθως θα εκμεταλλευτούν τις ευπάθειες που συσχετίζονται με τα συστημικά στοιχεία και τους ανθρώπους στο τομέα των ΤΠΕ. Όσον αφορά τους ανθρώπους, οι πιο συναφείς ομάδες είναι το προσωπικό και η διοίκηση του οργανισμού. Καθώς το προσωπικό και η διοίκηση, αντίστοιχα, προμηθεύονται, διαχειρίζονται και λειτουργούν συστήματα και συσκευές ΤΠΕ, οι δύο ομάδες συνδέονται στενά [15].

Σε γενικές γραμμές, η ασφάλεια πρέπει να είναι πλήρης. Διαφορετικά, οι επιτιθέμενοι απλά εκμεταλλεύονται τον πιο αδύναμο σύνδεσμο. Υπάρχουν, ωστόσο, πολλές σοβαρές αδυναμίες που έρχονται με τη χρήση του IoT στην υγειονομική περίθαλψη που είναι δύσκολο να αντιμετωπιστούν. Ένα βασικό πρόβλημα των έξυπνων νοσοκομείων είναι ότι τα προσωπικά δεδομένα για την υγεία των ασθενών θεωρούνται ακόμη πιο πολύτιμες πληροφορίες για τους εισβολείς ακόμα και από οικονομικά στοιχεία. Εκτός από την πρόσβαση σε ευαίσθητες πληροφορίες, μπορεί επίσης να υπάρχει πρόσβαση σε συνταγογραφούμενα φάρμακα που θεωρούνται χρήσιμα από τους επιτιθέμενους [16], [32].

Κατά την εφαρμογή των λύσεων IoT επιλέγονται τα κατάλληλα συστατικά με βάση το χαμηλό τους κόστος και τις ειδικές τους δυνατότητες. Ωστόσο, οι δυνατότητες τους μπορεί να είναι κατώτερες των περιστάσεων όταν τα προστατευόμενα στοιχεία (assets) αφορούν την ανθρώπινη ζωή. Το κόστος της προστασίας της ζωής των ασθενών μπορεί να είναι ένα σημαντικό μέρος του κόστους ή ακόμη μεγαλύτερο από το κόστος των συστημικών στοιχείων. Ωστόσο, τα υπερβολικά ευάλωτα σημεία δεν διευκολύνουν μόνο κακόβουλες ενέργειες, αλλά μπορούν επίσης να αυξήσουν την πιθανότητα και τον αντίκτυπο των ανθρώπινων σφαλμάτων και των αποτυχιών του συστήματος.

Οι συσκευές IoT, συμπεριλαμβανομένων των δικτυωμένων ιατρικών συσκευών, είναι διασυνδεδεμένες σε μεγάλο βαθμό και έχουν τη δυνατότητα της αυτόματης σύνδεσης με άλλες συσκευές. Κατά συνέπεια, οι αποφάσεις που λαμβάνονται σε τοπικό επίπεδο για μία συγκεκριμένη συσκευή μπορεί να έχουν ευρύτερες επιπτώσεις. Σε πολλές περιπτώσεις, οι ιατρικές συσκευές σχεδιάστηκαν χωρίς να λαμβάνουν υπόψη ότι θα έπρεπε κάποια στιγμή να συνδεθούν με ένα δίκτυο. Η επικοινωνία μεταξύ έξυπνων συσκευών και συστημάτων παλαιού τύπου μπορεί

επίσης να δημιουργεί κενά και να δίνει χώρο στους κακόβουλους επιτιθέμενους να αποκτήσουν παράνομη πρόσβαση σε συστήματα και δεδομένα. Η εισαγωγή της νέας γενιάς συστημάτων εισάγει μια νέα επιφάνεια επίθεσης [17].

Οι συσκευές IoT διασκορπίζονται παντού στο νοσοκομείο (από τους αισθητήρες στα δωμάτια των ασθενών μέχρι το CCTV και τους RFID αναγνώστες που παρέχουν έλεγχο πρόσβασης. Αυτό σημαίνει ότι η φυσική ασφάλεια είναι πρακτικά αδύνατη για όλα τα συστημικά στοιχεία. Η προστασία της περιμέτρου ελαχιστοποιεί αυτήν την ευπάθεια, ωστόσο απαιτείται περισσότερη προστασία.

Ο σχεδιασμός των ιατρικών συσκευών δεν περιλαμβάνει την περιγραφή απειλών. Οι συσκευές είναι κατασκευασμένες με βάση τις προδιαγραφές για την "προοριζόμενη χρήση" τους. Η παραβίαση από τρίτο πρόσωπο και άλλα ατυχήματα που οφείλονται στο δίκτυο είναι περιπτώσεις "ακούσιας χρήσης". Αυτή η παραδοχή οδηγεί σε μια σειρά συστημικών τρωτών σημείων και κινδύνων σε όλο το περιβάλλον της υγειονομικής περίθαλψης.

Υπάρχει μια μαζική ανάπτυξη ομοιογενών συσκευών IoT, γεγονός που το κάνει να αξίζει τον κόπο να διερευνηθούν συγκεκριμένα μονοπάτια επίθεσης. Ενώ οι κατασκευαστές και οι εταιρείες ασφάλειας πρέπει να αφαιρέσουν όλες τις ευπάθειες οι εγκληματίες πρέπει να βρουν μόνο μία. Είναι σχεδόν αδύνατο να διορθωθούν όλες οι ευπάθειες για όλες τις συσκευές. Ταυτόχρονα, ωστόσο, αν μια συγκεκριμένη ευπαθής ομάδα απομακρυνθεί, συνήθως δεν είναι πολύ δύσκολο οι εισβολείς να βρουν μια άλλη βιώσιμη πορεία επίθεσης.

Ειδικά για τα ιατροτεχνολογικά προϊόντα, η διάρκεια ζωής τους είναι ένα πολύ σημαντικό μειονέκτημα που πρέπει να εξεταστεί. Τα νοσοκομεία δεν αλλάζουν σαρωτές CAT ή μηχανές μαγνητικής τομογραφίας κάθε 3 χρόνια και όταν αγοράζουν τις συσκευές μπορεί να είναι ήδη ξεπερασμένες οι τεχνολογίες τους (χρειάζονται σχεδόν 3 χρόνια από το σχεδιασμό έως τη δοκιμή και την παραγωγή ιατροτεχνολογικών προϊόντων που βασίζονται στην Ευρωπαϊκή νομοθεσία). Το ίδιο συμβαίνει και στην περίπτωση των έξυπνων νοσοκομείων, καθώς οι IoT συσκευές είναι μια υποδομή χτισμένη πάνω από την υφιστάμενη υποδομή.

Οι συσκευές IoT τρέχουν ενσωματωμένα λειτουργικά συστήματα και εφαρμογές με ελάχιστη αν υπάρχει δυνατότητα ανίχνευσης κακόβουλου λογισμικού ή πρόληψης. Το μικρό μέγεθος και η περιορισμένη ισχύς επεξεργασίας πολλών συνδεδεμένων συσκευών συχνά παρεμποδίζει μέτρα

όπως η κρυπτογράφηση ή άλλα ισχυρά μέτρα ασφαλείας. Επιπλέον, είναι συχνά δύσκολη ή αδύνατη η αναμόρφωση ή η αναβάθμιση των συσκευών. [35]

Υπάρχει ένα αυξανόμενο επίπεδο εξάρτησης από τις συσκευές IoT, οι οποίες δεν είναι γνωστές για την ανθεκτικότητα τους. Η εξάρτησή μας από τη συνδεδεμένη τεχνολογία αυξάνεται ταχύτερα από την ικανότητά μας να θωρακίσουμε την ασφάλεια της- σε τομείς στους οποίους κρίνεται η ανθρώπινη ζωή και η δημόσια ασφάλεια, θα πρέπει να υπάρχουν εγγυήσεις για ένα υψηλότερο επίπεδο φροντίδας και προστασίας. Αυτό ισχύει ιδιαίτερα για ορισμένες ιατρικές συσκευές που είναι ζωτικής σημασίας για την επιβίωση των ασθενών.

Ο πραγματικός χρήστης έχει ελάχιστη ή καθόλου εικόνα για την εσωτερική λειτουργία των συσκευών ή τις ακριβείς ροές δεδομένων που δημιουργούνται. Όσον αφορά τα ιατροτεχνολογικά προϊόντα, το κλινικό προσωπικό, το προσωπικό πληροφορικής και ο ασθενής έχουν ελάχιστη ή και καθόλου εικόνα για τα χαρακτηριστικά τους. Οι αποφάσεις διαχείρισης κινδύνου που μπορεί να έγιναν από τον κατασκευαστή δεν αποκαλύπτονται με κανέναν ουσιαστικό τρόπο στον πάροχο υγειονομικής περίθαλψης, ένα γιατρό ή ασθενή. Αυτό καθιστά δύσκολη την κατανόηση πιθανών απειλών και επομένως τη λήψη έγκαιρων μέτρων αντιμετώπισης του παραστατικού.

Συχνά δεν υπάρχει σαφής τρόπος ειδοποίησης του χρήστη όταν εμφανίζεται κάποιο πρόβλημα ασφαλείας. Αυτό μπορεί να οδηγήσει σε παραβίαση της ασφάλειας που παραμένει για πολύ καιρό πριν εντοπιστεί και αποκατασταθεί. Έχει ήδη αποδειχθεί, ωστόσο, ότι οι συμβατικές ιατρικές συσκευές λειτουργούν ως γέφυρες για την περαιτέρω διάδοση κακόβουλων προγραμμάτων στα νοσοκομεία. Στην υγειονομική περίθαλψη αυτό είναι ιδιαίτερα σημαντικό, επειδή οι παραδοσιακοί μηχανισμοί ασφαλείας μπορεί να αποτύχουν περισσότερο με το να αρνούνται πρόσβαση και μπορεί να θέσουν σε κίνδυνο την ασφάλεια των ασθενών περισσότερο από το να παρουσιάσουν κάποιο σφάλμα και να παρέχουν πλήρη πρόσβαση.

Ο έλεγχος πρόσβασης είναι πολύ σημαντικός στο περιβάλλον του έξυπνου νοσοκομείου, καθώς μπορεί να προκαλέσει την πρόσβαση σε μη εξουσιοδοτημένους χρήστες μέσω μιας τελικής συσκευής σε ένα κρίσιμο σύστημα. Το παραπάνω μπορεί να αφορά την εξουσιοδότηση του προσωπικού που χειρίζεται ιατροτεχνολογικά προϊόντα. Σε ορισμένες περιπτώσεις λείπει η "ανάγκη της εγρήγορσης" ή η κατανόηση των επιπτώσεων από την προοπτική της ασφάλειας στον κυβερνοχώρο.

Παρά το γεγονός ότι τα μέλη του προσωπικού είναι καλά εκπαιδευμένοι και έχουν επίγνωση των διάφορων κινδύνων, μπορούν να παρακάμπτουν μέτρα ασφαλείας, όπως πολιτικές και διαδικασίες, εάν τις θεωρούν άσκοπα ενοχλητικές ή επιβραδυντικές. Στο πλαίσιο του νοσοκομείου το κλινικό προσωπικό μπορεί να παρακάμψει τα μέτρα απλώς και μόνο λόγω πίεσης χρόνου ή λόγω συγκρούσεων με άλλους στόχους, συμπεριλαμβανομένης της αποτελεσματικής ροής υγειονομικής περίθαλψης / ασθενούς, η ευχάριστη εμπειρία ασθενούς ή προστασία της ιδιωτικής ζωής των ασθενών / εργαζομένων.

Σε ένα έξυπνο περιβάλλον, οι γιατροί ή οι ασθενείς μπορούν να χρησιμοποιήσουν προσωπικές συσκευές (κινητά, φορητά κ.λπ.). Σαφέστατα η έλλειψη σαφούς και αυστηρής πολιτικής σχετικά με τη χρήση προσωπικών συσκευών στο χώρο εργασίας μπορεί να είναι μεγάλη ευπάθεια. Η ενίσχυση των διαδικασιών που συμμορφώνονται με την πολιτική ασφάλειας των πληροφοριών του νοσοκομείου θα πρέπει να είναι υποχρεωτική για τη χρήση οποιασδήποτε εξωτερικής συσκευής. Σε πολλές περιπτώσεις, το τμήμα πληροφορικής δεν γνωρίζει καν ότι χρησιμοποιούνται τέτοια συστήματα ή συσκευές, ενώ σε άλλες περιπτώσεις, η επιχειρησιακή ανάγκη εισαγωγής ενός νέου συστήματος / συσκευής για την υποστήριξη της ιατρικής διαδικασίας δεν επιτρέπει επαρκή χρόνο για την κατάλληλη δοκιμή του εν λόγω συστήματος / συσκευής για συμμόρφωση προς τις απαιτήσεις του οργανισμού.

Λόγω κλινικών αναγκών είναι δυνατό να χρησιμοποιηθούν συστήματα ή συσκευές που δεν ανταποκρίνονται σε οργανωτικά ή βιομηχανικά πρότυπα. Σε αυτές τις περιπτώσεις, το τμήμα πληροφορικής γνωρίζει συνήθως τη χρήση του συστήματος ή της συσκευής. Πολλές συσκευές IoT που μπορούν να χρησιμοποιηθούν στο πλαίσιο της υγειονομικής περίθαλψης δεν ταιριάζουν με τα τρέχοντα οργανωτικά πρότυπα. Ιδιαίτερα όσον αφορά την εισαγωγή του IoT στο περιβάλλον των ΤΠΕ του οργανισμού, ο βαθμός διείσδυσης νέων συσκευών μπορεί συχνά να υπερβαίνει την ικανότητα του τμήματος IT να ακολουθεί τις κατάλληλες διαδικασίες διαχείρισης συστημάτων/συσκευών και διαχείρισης αλλαγών που να ενσωματώνουν τους ελέγχους ασφάλειας των νέων συστημάτων / συσκευών.

Από οργανωτική άποψη, πολύ σημαντική είναι η συμπεριφορά των χρηστών, η οποία είναι σημαντική ειδικότερα στην περίπτωση της υγειονομικής περίθαλψης. Ο πρωταρχικός στόχος είναι η ασφάλεια του ασθενούς και οι γιατροί λαμβάνουν όλες τις αποφάσεις που απαιτούνται επί τόπου για την επίτευξη αυτού του στόχου. Συχνά αυτό σημαίνει ότι μπορεί να ακολουθηθούν πρόχειρες, αυτοσχέδιες λύσεις. Σε ένα έξυπνο περιβάλλον, όπου ένας έλεγχος ασφαλείας είναι δύσκολο να εφαρμοστεί λόγω της φυσικής διασποράς του περιβάλλοντος, δεν θα πρέπει να

γίνονται αποδεκτές όποιες αυτοσχέδιες λύσεις θέτουν σε κίνδυνο το επίπεδο ασφάλειας. Αυτές οι λύσεις συχνά δεν τεκμηριώνονται ούτε δοκιμάζονται εκτεταμένα και αποτελούν βασική ευπάθεια.

Λόγω κλινικών αναγκών ή λόγω έλλειψης κατάλληλων διαδικασιών διαχείρισης των όποιων συστημικών ρυθμίσεων, οι ρυθμίσεις των συστημάτων ή συσκευών ενδέχεται να μην είναι σύμφωνες με οργανωτικά ή βιομηχανικά πρότυπα. Η έλλειψη ενός προτύπου κατά τη παραμετροποίηση παρόμοιων συσκευών έχει ως αποτέλεσμα ένα περιβάλλον ΤΠΕ όπου δεν υπάρχει κοινό σημείο αναφοράς και ειδικά όταν πρόκειται για ευπάθειες ασφαλείας, καθώς οι ίδιες συσκευές ενδέχεται να είναι εκτεθειμένες για διαφορετικούς λόγους, δυσχεραίνει τόσο την ανακάλυψη των τρωτών σημείων όσο και την εφαρμογή διορθωτικών μέτρων σε όλο τον οργανισμό.

Όλες οι παραπάνω περιπτώσεις ευπαθειών γενικά περιλαμβάνουν τεχνικές πτυχές που συσχετίζονται με τις τεχνολογίες Πληροφορικής/Επικοινωνιών (ΤΠΕ) και συσκευές . Σαφώς μερικές από τις ευπάθειες είναι πιο συναφή με ορισμένα συστήματα/συσκευές έναντι άλλων. Για παράδειγμα, ευπάθειες που συνδέονται με την έλλειψη κατάλληλου ελέγχου των πτυχών ασφάλειας (π.χ. μη υποστηριζόμενες ή μη τυποποιημένες συσκευές / συστήματα) σχετίζονται περισσότερο με δικτυακά συνδεδεμένες ιατρικές συσκευές ή κινητές συσκευές τελικού χρήστη. Λειτουργίες που σχετίζονται με το κτίριο όπως το σύστημα ρύθμισης της ισχύς του ρεύματος, του κλιματισμού ή το σύστημα κλειδώματος θυρών μπορεί επίσης να είναι ευάλωτες καθώς όλο και περισσότερο βασίζονται σε τεχνολογίες / συστήματα Πληροφορικής [18].

2.3.1 Ταξινόμηση ευπαθειών

Οι βασικές αιτίες των απειλών που αντιμετωπίζουν τα έξυπνα νοσοκομεία είναι οι κακόβουλες ενέργειες, τα ανθρώπινα λάθη, τα σφάλματα σε διάφορα συστήματα του ΕΝ και φυσικά φαινόμενα [18].

Εικόνα 2.5. Ταξινόμηση των απειλών σε ένα Έξυπνο Νοσοκομείο [15].

1. Κακόβουλες ενέργειες

Οι κακόβουλες ενέργειες είναι σκόπιμες πράξεις από ένα άτομο ή έναν οργανισμό. Παρόλο που και οι δύο απειλούν έξυπνα νοσοκομεία, είναι σημαντικό να ξεχωρίσουμε τις κακόβουλες ενέργειες από άλλες εσκεμμένες ενέργειες που παρακάμπτουν τις πολιτικές και τις διαδικασίες χωρίς να υπάρχει όμως κακόβουλη πρόθεση. Ένα άτομο που εκτελεί μία κακόβουλη ενέργεια μπορεί να ανήκει στο ενεργητικό του νοσοκομείου ή να είναι εξωτερικός παράγοντας.

Το κακόβουλο λογισμικό είναι μία σημαντική απειλή για τα έξυπνα νοσοκομεία. Το λεγόμενο malware έχει το χαρακτηριστικό ότι μπορεί να επιτίθενται σε μεγάλο αριθμό οργανισμών με χαμηλή προσπάθεια. Ειδικά τα προγράμματα ransomware θεωρούνται σημαντική απειλή για τους οργανισμούς υγειονομικής περίθαλψης. Άλλες κατηγορίες κακόβουλου λογισμικού περιλαμβάνουν:

- αυτοαναπαραγόμενα προγράμματα («σκουλήκια»), τα οποία εξαπλώνονται μεταξύ υπολογιστών
- δούρειοι ίπποι που δρουν κρυφά
- οι ιοί, οι οποίοι εξαπλώνονται εσωτερικά
- τα rootkits, τα οποία κρύβουν τη μόλυνση
- τα exploit kits, τα οποία εκμεταλλεύονται τις ευπάθειες σε πελάτες για να μολύνουν τα συστήματα
- τα botnets, τα οποία θέτουν πολλά μολυσμένα συστήματα υπό έλεγχο και το
- spyware.

Τα κακόβουλα προγράμματα αποτελούν σοβαρή απειλή, καθώς μπορεί να μολύνουν ένα μεγάλο αριθμό συσκευών σε ένα έξυπνο νοσοκομείο (από σταθερές συσκευές και υπολογιστές μέχρι κινητές συσκευές τελικού χρήστη) και καταλήγουν σε μια ιδιαίτερα μεγάλη επιφάνεια επίθεσης [5].

Αντίστοιχα, μία εισβολή μπορεί να εκτελεστεί σε επίπεδο δικτύου ή συναλλαγής (μέσω web) ή σε επίπεδο συσκευής. Ειδικά η τελευταία περίπτωση έχει ιδιαίτερη σημασία στο πλαίσιο των έξυπνων νοσοκομείων. Η παραβίαση μίας ιατρικής συσκευής είναι μια άλλη κρίσιμη απειλή. Οι δικτυωμένες ιατρικές συσκευές μπορούν να επαναπρογραμματιστούν, επαναρυθμιστούν σύμφωνα με τις εντολές του εισβολέα ή ακόμα και να απενεργοποιηθούν. Επίσης, οι επιθέσεις κοινωνικής μηχανικής (π.χ. phishing) διαδραματίζουν ιδιαίτερο ρόλο στο πλαίσιο των έξυπνων νοσοκομείων. Οι κοινωνικές επιθέσεις είναι δημοφιλείς καθώς το ανθρώπινο στοιχείο είναι συνήθως ο πιο αδύναμος κρίκος στην υπεράσπιση ενός οργανισμού [15].

Η κλοπή συσκευών και δεδομένων σχετίζεται επίσης με τις κακόβουλες επιθέσεις. Είναι μια σπάνια επίθεση λαμβάνοντας υπόψη τον όγκο που μπορεί να έχει κάποιος ιατρικός εξοπλισμός. Ωστόσο, κατά την εισαγωγή αισθητήρων στα νοσοκομεία, ο όγκος δεν είναι πια πρόβλημα και αυξάνεται η πιθανότητα να επιτευχθεί αυτή η επίθεση. Αν δεν είναι όλες οι διασυνδεδεμένες συσκευές στη θέση τους αυτό ενδέχεται να οδηγήσει σε λανθασμένη συλλογή δεδομένων, λανθασμένη ανάλυση και έτσι σε λανθασμένες αποφάσεις.

Η απόκρυψη είναι μια επίθεση κατά των ραδιοσυχνοτήτων υψηλής συχνότητας RFID. Είναι ένας πολύ συγκεκριμένος τύπος επίθεσης, ωστόσο, δεδομένου ότι οι ετικέτες RFID χρησιμοποιούνται ευρύτερα στα έξυπνα νοσοκομεία (ετικέτες, αισθητήρες κ.λπ.), αυτό θα πρέπει να ληφθεί υπόψη καθώς η προστασία από αυτού του είδους τις επιθέσεις βασίζεται περισσότερο σε επενδύσεις υλικού.

Οι επιθέσεις άρνησης εξυπηρέτησης ενδέχεται να καταστήσουν ένα σύστημα ή μια υπηρεσία εντελώς μη διαθέσιμες, κάτι που θα μπορούσε ενδεχομένως να διαταράξει πλήρως τη διαδικασία φροντίδας των ασθενών. Δεδομένου ότι τα έξυπνα νοσοκομεία τείνουν να βασίζονται περισσότερο σε πόρους που βρίσκονται στο διαδίκτυο ή στο υπολογιστικό νέφος, μια επίθεση DoS μπορεί να οδηγήσει σε μη διαθεσιμότητα δεδομένων ασθενών (π.χ. εάν τα δεδομένα αποθηκεύονται σε μία Cloud υποδομή ή εάν η συλλογή τους βασίζεται στο Διαδίκτυο για λόγους φροντίδας ορισμένων ασθενών από απόσταση).

2. Ανθρώπινα λάθη

Τα ανθρώπινα λάθη προκύπτουν κατά τη διάρκεια της διαμόρφωσης ή λειτουργίας των συσκευών ή των συστημάτων Πληροφορικής ή της εκτέλεσης των λειτουργιών τους. Τα ανθρώπινα σφάλματα συχνά συνδέονται με ανεπαρκείς διαδικασίες ή ανεπαρκή εκπαίδευση [15]. Παραδείγματα περιλαμβάνουν:

- Σφάλματα κατά τη ρύθμιση κάποιου ιατρικού συστήματος που μπορεί να θέσει σε κίνδυνο τη λειτουργία του συστήματος ή την έκθεση του συστήματος σε κάποια κυβερνοαπειλή.

- Απουσία ή απώλεια καταγραφών για να επιτρέπεται ο κατάλληλος έλεγχος - π.χ. της πρόσβασης σε έξυπνους νοσοκομειακούς πόρους - και / ή τον εντοπισμό συμβάντων και την αξιολόγηση των διορθωτικών / βελτιωτικών ενεργειών

- Μη εξουσιοδοτημένη πρόσβασης ή η έλλειψη διαδικασιών πρόσβασης είναι σημαντικοί κίνδυνοι για τα έξυπνα νοσοκομεία, καθώς χειρίζονται ευαίσθητα δεδομένα ασθενών και το γεγονός ότι οι ιατρικές διαδικασίες περιλαμβάνουν ρόλους με υψηλού επιπέδου εξειδίκευσης σε διάφορους τομείς.

- Μη συμμόρφωση σε διάφορες πολιτικές και πρότυπα. Αυτό είναι ιδιαίτερα σημαντικό για τα έξυπνα νοσοκομεία που βασίζονται σε IoT και κινητές εφαρμογές που μπορούν να είναι προσβάσιμες / εγκατεστημένες (π.χ. ως εφαρμογές για κινητά) σε προσωπικές συσκευές που δεν έχουν εγκριθεί ρητά (και επομένως έχουν ελεγχθεί ή επαρκώς θωρακιστεί από πλευράς ασφάλειας) από το Τμήμα πληροφορικής του νοσοκομείου.

- Τα πιθανά λάθη του ιατρικού προσωπικού ή των ασθενών αποτελούν σοβαρή απειλή στην ασφάλεια του έξυπνου νοσοκομείου όπου υπάρχει μεγάλη εξάρτηση σε τεχνολογικές πληροφορικής. Για παράδειγμα, τέτοια σφάλματα μπορεί να οφείλονται σε κόπωση και κακή συγκέντρωση λόγω φόρτου εργασίας ή εφαρμογής πρόχειρων, αυτοσχέδιων λύσεων εξαιτίας άλλων πολιτικών και διαδικασιών που θεωρούνται υπερβολικά επίπονες ή χρονοβόρες (και ως εκ τούτου παρεμποδίζουν τη διαδικασία φροντίδας των ασθενών).

3. Σφάλματα σε επίπεδο συστήματος

Τα σφάλματα σε επίπεδο συστήματος είναι εξαιρετικά σημαντικά στο πλαίσιο της υγειονομικής περίθαλψης, ιδίως λόγω της αυξανόμενης πολυπλοκότητας και της δυναμικής των συστημάτων [18]. Τέτοιου είδους παραδείγματα περιλαμβάνουν:

- Αδυναμίες ενός λογισμικού που επηρεάζουν ή διακόπτουν εντελώς μια ιατρική (π.χ. αποτυχία ενός PACS) ή διοικητική διαδικασία (π.χ. μη διαθεσιμότητα των δεδομένων ασθενών)

- Ανεπαρκές υλικό και λογισμικό που μπορεί να είναι ιδιαίτερα σημαντικό για το πλήθος των συνδεδεμένων ιατρικών συσκευών σε ένα έξυπνο νοσοκομείο

- Η αστοχία της συσκευής ή απλώς η περιορισμένη / μειωμένη ικανότητα της μπορεί να επηρεάσει σοβαρά τις διαδικασίες που βασίζονται, π.χ. στη συλλογή δεδομένων ασθενών σε πραγματικό χρόνο, όπως συσκευές μέτρησης γλυκόζης.

- Ένα σφάλμα σε επίπεδο δικτύου μπορεί να έχει μεγάλες επιπτώσεις στη λειτουργία ενός δικτύου IoT συσκευών.

- Η ανεπαρκής συντήρηση μπορεί να προκαλέσει ανυπολόγιστα και ανεπίλυτα επιχειρησιακά προβλήματα, τόσο από την πλευρά της κυβερνο-ασφάλειας, αλλά και όσον αφορά τις λειτουργίες περίθαλψης των ασθενών.

- Η υπερφόρτωση μπορεί να οδηγήσει στη μη διαθεσιμότητα ενός συστήματος ή μιας υπηρεσίας.

- Η επικοινωνία μεταξύ του IoT δικτύου και του μη-IoT δικτύου μπορεί να επηρεαστεί, ιδίως καθώς το πρώτο μέρους του δικτύου αυξάνεται σε αριθμούς, τεχνολογία και πολυπλοκότητα ταχύτερα από το κύριο μέρος του δικτύου.

4. Σφάλματα τρίτων

Η αποτυχία της αλυσίδας εφοδιασμού βρίσκεται εκτός του άμεσου ελέγχου του ΕΝ, καθώς συνήθως επηρεάζεται ή εμπίπτει στην ευθύνη ενός τρίτου μέρους. Δεδομένου ότι τα έξυπνα νοσοκομεία εξαρτώνται όλο και περισσότερο από τρίτους, οι αποτυχίες τρίτων μερών μπορεί να έχουν σοβαρές συνέπειες για αυτούς. Παραδείγματα τρίτων των οποίων οι αποτυχίες θα είχαν αρνητικές επιπτώσεις στην λειτουργία έξυπνων νοσοκομείων περιλαμβάνουν:

- Οι πάροχοι υπηρεσιών Υπολογιστικού Νέφους (Cloud) που φιλοξενούν ιατρικά δεδομένα, εφαρμογές, συστήματα, διοικητικά δεδομένα, απομακρυσμένους ασθενείς, σημεία συλλογής δεδομένων - και άλλες εφαρμογές έξυπνης υγείας που βασίζονται στο Διαδίκτυο κλπ.

- Οι κατασκευαστές ιατρικών συσκευών σε περίπτωση αποτυχίας ή μη ευθύνης.

- Οι πάροχοι δικτυακών υπηρεσιών, όπως οι παροχείς υπηρεσιών διαδικτύου (ISPs), που υποστηρίζουν τη συνδεσιμότητα σε επίπεδο μητροπολιτικού δικτύου (WAN) και, επομένως, πρόσβαση σε δεδομένα νέφους, απομακρυσμένους ασθενείς, συστήματα που φιλοξενούνται εκτός του κέντρου δεδομένων του νοσοκομείου, συμπεριλαμβανομένων των εθνικών συστημάτων (π.χ. σύστημα ηλεκτρονικής συνταγογράφησης ή σύστημα ηλεκτρονικού φακέλου ασθενούς)

- Οι προμηθευτές ενέργειας.

5. Φυσικά φαινόμενα

Τα φυσικά φαινόμενα μπορεί επίσης να είναι η αιτία συμβάντων, ιδίως λόγω των καταστροφικών επιπτώσεών τους, ιδίως στις εγκαταστάσεις ευφυούς νοσοκομειακής περίθαλψης και στις υποδομές ΤΠΕ. Επιπλέον, φυσικά φαινόμενα (σεισμοί, πλημμύρες, πυρκαγιές) μπορεί να επηρεάζουν την παροχή υπηρεσιών απομακρυσμένης περίθαλψης ασθενών, ακόμη και αν ο αντίκτυπός τους δεν στοχεύει ή δεν έχει αντίκτυπο στο ίδιο το νοσοκομείο (π.χ. εάν η υποδομή του δικτύου επηρεαστεί από ένα σεισμό) . Τα παραδείγματα περιλαμβάνουν.

2.3.2 Προφίλ επιθέσεων

Το προφίλ των δυνητικών εισβολέων σε ένα έξυπνο νοσοκομείο διαφέρουν με βάση τους διαφορετικούς παράγοντες απειλών που ο καθένας τους ενεργοποιεί. Οι παράγοντες αυτοί μπορεί να είναι [19]:

- Απειλές εσωτερικών παραγόντων: Πρόκειται για προσωπικό του νοσοκομείου (οποιοσδήποτε ρόλος) με κακόβουλη πρόθεση. Αυτοί θα μπορούσαν να είναι γιατροί, νοσηλευτές, ή ακόμη και το διοικητικό προσωπικό που έχει κακόβουλη πρόθεση να βλάψει τα συστήματα Πληροφορικής/IoT του νοσοκομείου. Αυτά μπορεί να είναι ενδεχομένως οι πιο επικίνδυνοι παράγοντες.

- Ασθενείς /επισκέπτες με κακόβουλες προθέσεις: οι παράγοντες αυτοί αποτελούν μέρος του νοσοκομειακού οικοσυστήματος (κυρίως οι ασθενείς). Αυτοί μπορεί να έχουν κακόβουλη πρόθεση που σε συνδυασμό με την πρόσβαση που έχουν στα συστημικά μέρη και δεδομένα του έξυπνου νοσοκομείου, μπορούν να προκαλέσουν σημαντικές βλάβες.

- Απομακρυσμένοι εισβολείς: στην περίπτωση των έξυπνων νοσοκομείων, ένας από τους στόχους είναι η παροχή περίθαλψης από απόσταση. Έτσι η χρήση αυτού του εξοπλισμού για κακόβουλες ενέργειες θα μπορούσε να είναι ένα πιθανό σενάριο όταν ο εισβολέας δεν είναι φυσικά στο νοσοκομείο.

- Άλλες αιτίες: ένα τυχαίο σφάλμα σε κάποιο εξοπλισμό / λογισμικό ή εξαιτίας κάποιων περιβαλλοντικών συνθηκών, ή ακόμη και κάποιο εξωτερικό προσωπικό συντήρησης

μπορεί να προκαλέσει συμβάντα ασφαλείας, χωρίς να υπάρχει απαραίτητα κάποιος ενεργός εισβολέας.

Οι φορείς επίθεσης στα νοσοκομεία θα μπορούσαν να είναι [20]:

- Φυσική αλληλεπίδραση με IT συστήματα, σταθμούς εργασίας: Οι επιτιθέμενοι που είναι φυσικά παρόντες (ασθενείς ή γιατροί) μπορούν να αλληλεπιδρούν άμεσα με τις συσκευές στις οποίες έχουν πρόσβαση. Για παράδειγμα: συνδεδεμένες ιατρικές συσκευές ή διασυνδεδεμένα πληροφοριακά συστήματα των κλινικών.

- Ασύρματη επικοινωνία με τα μέσα πληροφορικής: μια πολύ κοινή τεχνική για την παρακολούθηση είναι η επίθεση εντός εύρους ασύρματων τεχνολογιών, συμπεριλαμβανομένων: συστημάτων αναγνώρισης ή κινητών συσκευών.

- Ενσύρματη επικοινωνία με IT συστήματα: Οι επιτιθέμενοι με ενσύρματες επικοινωνίες δικτύου (συμπεριλαμβανομένης της πρόσβασης στο Διαδίκτυο) μπορούν να αλληλεπιδράσουν με σχετικά IT συστήματα, συμπεριλαμβανομένων των υπηρεσιών cloud και online συστημάτων που παρέχουν υπηρεσίες σχετικά με τη συνταγογράφηση, τον ηλεκτρονικό φάκελο ασθενούς. Οι επιτιθέμενοι με φυσική παρουσία μπορεί να έχουν άμεση πρόσβαση στην δικτυακή υποδομή, με την οποία μπορούν να συνδεθούν για να επικοινωνούν με άλλες συνδεδεμένες έξυπνες συσκευές.

- Αλληλεπίδραση με το προσωπικό: Οι επιθέσεις κοινωνικής μηχανικής είναι πολύ συχνές στον τομέα της υγειονομικής περίθαλψης, και είναι συχνά το εφαλτήριο ransomware επιθέσεων. Αντί να στοχεύει άμεσα το σύστημα, ο επιτιθέμενος επικεντρώνεται σε κάποιο γιατρό / νοσοκόμα ή ασθενή (χρήστη με προνομιακή πρόσβαση). Επιθέσεις τύπου CSRF ή XSS και οι επιθέσεις της κοινωνικής μηχανικής περιλαμβάνουν την εξαπάτηση του τελικού χρήστη έτσι ώστε να πραγματοποιεί εντολές για λογαριασμό τους.

2.4 Τεχνολογίες IoT

2.4.1 Εισαγωγή

Το διαδίκτυο των πραγμάτων περιλαμβάνει πλέον δισεκατομμύρια μικρές συσκευές που σκοπός τους είναι να ανιχνεύουν, συλλέγουν, αποστέλλουν δεδομένα και να εκτελούν εντολές που δέχονται μέσω διαδικτύου. Τέτοιες πληροφορίες μπορεί να περιλαμβάνουν την τοποθεσία, τη λίστα επαφών, τα μοτίβα περιήγησης και τις πληροφορίες για την υγεία και την φυσικής μας κατάσταση. Η ανίχνευση, η συλλογή και η διάδοση δεδομένων γίνεται μέσω από τυποποιημένα ασύρματα πρωτόκολλα επικοινωνίας. Οι συσκευές λαμβάνουν ερεθίσματα από το περιβάλλον και μπορούν επίσης να προσαρμόζονται σε αυτό ή να ενημερώνουν τους ανθρώπους για τη λήψη προσωποποιημένων αποφάσεων.

Μέχρι τώρα τα πρότυπα ανάπτυξης αυτών των συσκευών εστιάσανε στη διευκόλυνση χρήσης τους μέσα από τις ανάγκες, και προτιμήσεις των χρηστών ή έστω να χειρίζονται καταστάσεις έκτακτης ανάγκης (π.χ. άμεση ενημέρωση για μία φωτιά σε ένα σπίτι ή μία περιοχή). Από την άλλη πλευρά, τα μέχρι τώρα πρότυπα δεν εστιάσανε αρκετά στην ασφάλεια και την προστασία των προσωπικών δεδομένων που διακινούνται μέσα από αυτά. Αν δεν λαμβάνονται επιπρόσθετα μέτρα, ακόμη και μέσα σε ένα ιδιωτικό χώρο (πχ ένα σπίτι, μία κλινική) προσωπικά δεδομένα μπορεί να γίνουν προσβάσιμα σε κακόβουλα τρίτα μέρη ή εισβολείς.

Αλλά και οι ίδιοι κατασκευαστές των IoT συσκευών απειλούνται από απώλεια βιομηχανικών μυστικών ή εσόδων. Ο εισβολέας μπορεί να υποκλέψει στοιχεία σχετικά με το λογισμικό διαχείρισης του υλικού ή μπορεί να διαρρεύσει την παραβίαση της ασφάλειας του συστήματος προκαλώντας ζημία στην εμπορική φήμη του κατασκευαστή. Καθώς οι συσκευές χρησιμοποιούνται σε πολλούς τομείς και με διάχυτο τρόπο, η εμφάνιση και εκμετάλλευση μπορεί για κάποιους τομείς να είναι λιγότερο ή περισσότερο καταστροφικές.

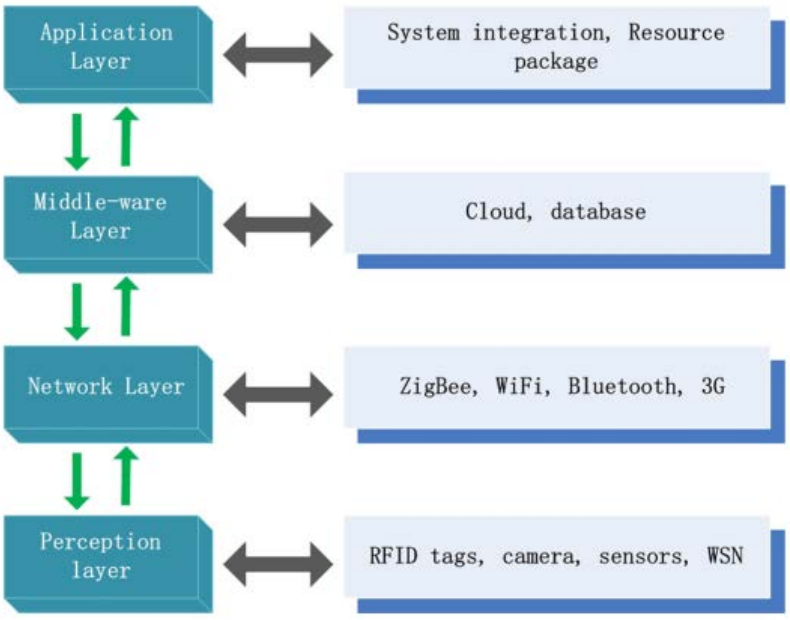
Πράγματι, έχουν υπάρξει αναφορές για κακόβουλες επιθέσεις είτε απευθείας στις συσκευές ή τις εφαρμογές διαχείρισης τους είτε σε ένα κινητό τηλέφωνο ή σε ένα web διακομιστή. Μία συνήθης τακτική τους είναι να εμφυτεύσουν κακόβουλο κώδικα και να υποκλέπτουν προσωπικά δεδομένα των χρηστών [26]. Οι επιθέσεις σε IoT συσκευές που χρησιμοποιούνται ως ιατρικά μηχανήματα υποστήριξης μπορεί να απειλήσουν σοβαρά την ζωή του ασθενούς. Το ίδιο

σημαντικές είναι οι επιπτώσεις αν οι επιθέσεις γίνουν στη παραγωγή μίας βιομηχανικής μονάδας ή στο λογισμικό κινούμενων οχημάτων.

2.4.2 IoT αρχιτεκτονική

Η αρχιτεκτονική του IoT απλώνεται σε τρία τουλάχιστον επίπεδα. Τα τρία πρώτα περιλαμβάνουν το επίπεδο εφαρμογής, επίπεδο δικτύου και το επίπεδο συλλογής δεδομένων (perception layer). Σε κάθε επίπεδο μπορεί να χρησιμοποιηθούν διαφορετικές τεχνολογίες τόσο από τη πλευρά της φύσης κατασκευής και λειτουργίας τους, όσο και ως προς την εξάρτηση από διαφορετικούς τηλεπικοινωνιακούς, ηλεκτρικούς και άλλους περιορισμούς. Αυτό καθιστά τη διαχείρισή τους μια δύσκολη και πολύπλοκη διαδικασία.

Για να αντιμετωπιστεί αυτή η πρόκληση, πρόσφατα έχει εισαχθεί ένα ενδιάμεσο επίπεδο διαχείρισης (middleware) ή όπως θα δούμε σε επόμενο κεφάλαιο, προστίθενται πύλες (gateways) ως διακομιστές μεσολάβησης για τη παροχή διαφορετικών υπηρεσιών αλλά προστατεύοντας τις εσωτερικές τεχνολογίες. Το ενδιάμεσο επίπεδο (διακομιστής ή λογισμικό) συλλέγει πληροφορίες από τα κάτω επίπεδα και τα αποθηκεύει σε ένα μόνιμο μέσο (πχ βάση δεδομένων) είτε στο τοπικό δίκτυο ή στο υπολογιστικό νέφος. Επίσης, μπορεί να επεξεργάζεται ή να αναλύει τα δεδομένα για σκοπούς τρίτων. Στην παρακάτω εικόνα περιγράφεται μία τέτοια αρχιτεκτονική με τις αντίστοιχες τεχνολογίες σε κάθε επίπεδο.



Εικόνα 2.6. IoT Αρχιτεκτονική [25]

Η ασφάλεια των αποθηκευτικών μέσων ή η ασφαλής επικοινωνία με την υποδομή στο υπολογιστικό νέφος είναι τα καίρια ζητήματα στο επίπεδο του μεσαίου λογισμικού από πλευράς ασφάλειας. Το δε επίπεδο της εφαρμογής υλοποιεί διαφορετικές εφαρμογές για διαφορετικά σενάρια. Αξιοποιεί τα αποτελέσματα της ανάλυσης ή επεξεργασίας του ενδιάμεσου επιπέδου παρέχοντας επιπλέον πληροφορίες στον τελικό χρήστη. Και σε αυτό το επίπεδο έχουν καταγραφεί κενά ασφαλείας με αποτέλεσμα την κακόβουλη πρόσβαση σε δεδομένα, ή αλλοίωση των δεδομένων [20], [30]

Αυτό το επίπεδο είναι υπεύθυνο για τη συνδεσιμότητα της υποδομής του IoT. Επίσης, συλλέγει δεδομένα από το επίπεδο συλλογής δεδομένων και τα μεταδίδει στο ανώτερο στρώμα. Το μέσο μετάδοσης μπορεί να είναι ενσύρματο ή ασύρματο και οι κύριες τεχνολογίες που χρησιμοποιούνται είναι το ZigBee, το WiFi, το Bluetooth, το 4/5G και άλλες. Οι επιθέσεις στο επίπεδο του δικτύου εστιάζουν στην άρνηση εξυπηρέτησης (Denial of Service) και την μεσολάβηση στην ανταλλαγή πληροφοριών (Man-in-the-middle attack) μεταξύ των συσκευών [27].

Επίσης, το επίπεδο συλλογής δεδομένων μπορεί να συλλέγει δεδομένα μέσα από συστήματα ή πρωτόκολλα αισθητήρων. Για παράδειγμα, δεδομένα που είναι διαθέσιμα από ετικέτες RFID (ενημερώνονται από τους αντίστοιχους σαρωτές), εικόνες/δεδομένα κίνησης από, δεδομένα του περιβάλλοντος από τους αισθητήρες, είναι ορισμένα παραδείγματα. Οι τεχνολογίες σε αυτό το επίπεδο εκτίθενται σε διάφορους κινδύνους πέρα από κυβερνοεπιθέσεις (πχ φυσικές καταστροφές, κακόβουλες ενέργειες). Αυτό μπορεί να επηρεάσει την λειτουργία ολόκληρης της αρχιτεκτονικής εφόσον υπάρχει σημαντική εξάρτηση στη συλλογή δεδομένων [27].

2.4.3 Απαιτήσεις ασφάλειας

Η ασφάλεια στον τομέα του IoT εξετάζεται μέσα από τις σύγχρονες προκλήσεις που καλούνται να αντιμετωπίσουν οι εκατοντάδες κατασκευαστές τέτοιων τεχνολογιών [35]:

- περιορισμοί στην επικοινωνία
- περιορισμοί στο φυσικό περιβάλλον
- ανεπαρκής προστασία των δεδομένων και πληροφοριών.

Στη πρώτη περίπτωση, οι εφαρμογές του IoT καθίσταται ευάλωτες σε μια σειρά κενών ασφαλείας εξαιτίας των διαφορετικών πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται για την μετάδοση σημαντικών δεδομένων. Ανάλογα το μέσο επικοινωνίας, καθίσταται μοναδική και η εκδοχή της εκάστοτε ευπάθειας. Ειδικά τα ασύρματα πρωτόκολλα επικοινωνίας είναι πιο ευάλωτα σε επιθέσεις (πχ υποκλοπή μη κρυπτογραφημένων πακέτων δεδομένων, αλλοίωση σήματος, άρνηση εξυπηρέτησης, καθυστέρηση μετάδοσης, εμφύτευση κώδικα στον κόμβο ασύρματης δρομολόγησης). Σε ασύρματα δίκτυα αισθητήρων μεγάλης κλίμακας που ενδεχομένως να εμπλέκονται ασύρματες τεχνολογίες χαμηλού, μεσαίου και μεγάλου εύρους ζώνης ή εμβέλειας μετάδοσης η επίθεση σε ένα κόμβο μπορεί να επηρεάσει τη λειτουργία όλου του συστήματος.

Στη δεύτερη περίπτωση, το φυσικό περιβάλλον θέτει τους δικούς του περιορισμούς και απαιτήσεις όσον αφορά και τη φυσική ασφάλεια του εξοπλισμού. Αν εισβολείς έχουν φυσική πρόσβαση τότε μπορούν απευθείας να αποκτήσουν πληροφορίες από τις συσκευές ή να πετύχουν κλωνοποίηση τους για υποκλοπή των δεδομένων ή ακόμα και καταστροφή των συσκευών. Επίσης, οι σχεδιαστές τους πρέπει να λάβουν υπόψη τις απαιτήσεις σε κατανάλωση ενέργειας ή σε ισχύ. Οι εισβολείς μπορεί να εκμεταλλευτούν αυτούς τους περιορισμούς και να πραγματοποιήσουν επιθέσεις όπως Άρνηση Εξυπηρέτησης. Προκύπτει επίσης, ότι εξαιτίας των παραπάνω περιορισμών, οι κατασκευαστές δεν δύναται να αναπτύξουν πιο αποτελεσματικούς μηχανισμούς ασφάλειας πάνω σε αυτές τις συσκευές.

Στη τρίτη περίπτωση, οι εισβολείς αξιοποιούν συχνά την έλλειψη μηχανισμών ταυτοποίησης και ελέγχου δικαιωμάτων πρόσβασης στις επιμέρους τεχνολογίες. Έτσι ένας εισβολέας μπορεί να αποκτήσει πρόσβαση και να τροποποιήσει από απόσταση τα όποια δεδομένα διακινούνται από τη συσκευή. Αυτό γίνεται σε συνδυασμό με την έλλειψη εγρήγορσης και ενημέρωσης των τελικών χρηστών που μπορεί να λάβουν κάποιο κακόβουλο μήνυμα στην αλληλογραφία τους που επιτρέπει στον εισβολέα να εμφυτεύσει πρόγραμμα ελέγχου της συσκευής και συνεπώς και όποιας IoT συσκευής στο δίκτυο. Έτσι το απόρρητο των δεδομένων των χρηστών παραβιάζεται λόγω της έλλειψης μηχανισμών ταυτοποίησης στην είσοδο των χρηστών. Επιπλέον, εκμεταλλευόμενοι σφάλματα στο πρόγραμμα, οι εισβολείς μπορούν να εισάγουν κακόβουλο κώδικα στο σύστημα και να εξάγουν δεδομένα. [35]

Επιπρόσθετες απαιτήσεις παρουσιάζονται στον παρακάτω πίνακα.

Χαρακτηριστικό ποιότητας	**Περιγραφή ασφάλειας IoT**
Ακεραιότητα δεδομένων	Η ακεραιότητα των δεδομένων εξασφαλίζει την ακεραιότητα, την αξιοπιστία και την ορθότητα των δεδομένων και επιβεβαιώνει ότι τα δεδομένα δεν έχουν τροποποιηθεί και καταστραφεί.
Εμπιστευτικότητα δεδομένων	Το απόρρητο των δεδομένων στοχεύει στην απόκρυψη δεδομένων από μη εξουσιοδοτημένα άτομα, προστατεύοντας έτσι το απόρρητο και τα ευαίσθητα δεδομένα των χρηστών χωρίς να αυτά να αποκτώνται από τους επιτιθέμενους. Μόνο οι νόμιμοι χρήστες μπορούν να έχουν πρόσβαση στις πληροφορίες.
Διαθεσιμότητα δεδομένων	Η διαθεσιμότητα δεδομένων χρησιμοποιείται για να βεβαιωθεί ότι οι πόροι (π.χ. δεδομένα και υπηρεσίες) είναι διαθέσιμοι.
Ταυτοποίηση	Ο έλεγχος ταυτότητας ορίζει την επαλήθευση και τη διαφοροποίηση των χρηστών με τα απαραίτητα στοιχεία ταυτοποίησης προκειμένου να έχουν πρόσβαση σε διάφορες οντότητες. Τα πρωτόκολλα ελέγχου ταυτότητας διαδραματίζουν σημαντικό ρόλο στην αμοιβαία επικοινωνία μεταξύ διαφορετικών οντοτήτων.
Εξουσιοδότηση	Η εξουσιοδότηση ορίζει τη διαδικασία χορήγησης, άρνησης και περιορισμού της πρόσβασης σε οντότητες. Το σύστημα αδειοδότησης εκτελεί διαφορετικές λειτουργίες σύμφωνα με διαφορετικές οντότητες.

Πίνακας 2.1. Απαιτήσεις ασφάλειας στο πεδίο του IoT [32]

Ακεραιότητα δεδομένων

Μηχανισμοί όπως κώδικας επαλήθευσης μηνυμάτων (MAC), ψηφιακή υπογραφή και έλεγχος εκδόσεων χρησιμοποιούνται για την εξασφάλιση της ακεραιότητας των δεδομένων.

Εμπιστευτικότητα δεδομένων

Υπάρχουν πολλοί τρόποι για να διασφαλιστεί η εμπιστευτικότητα των δεδομένων. Οι συνήθεις μέθοδοι περιλαμβάνουν έλεγχο πρόσβασης και κρυπτογράφηση δεδομένων. Ωστόσο, λόγω των περιορισμένων πόρων σε συσκευές IoT ή σε ενσωματωμένες συσκευές, δεν μπορεί να εφαρμοστεί πλήρως ένα εξελιγμένο σύστημα κρυπτογράφησης δεδομένων και ελέγχου ταυτότητας, επομένως δεν μπορεί να προσφέρει επαρκή προστασία.

Διαθεσιμότητα δεδομένων

Η διαθεσιμότητα πληροφοριακών πόρων είναι κρίσιμη για τους χρήστες και αυτό είναι ένα σημαντικό βήμα για την εξασφάλιση της ποιότητας των υπηρεσιών (QoS). Ο στόχος μίας επίθεσης άρνησης εξυπηρέτησης (DoS) είναι να καταστούν οι πόροι μη διαθέσιμοι στους χρήστες. Ένας αποτελεσματικός τρόπος διασφάλισης της διαθεσιμότητας των δεδομένων είναι η παροχή πολλαπλών διαδρομών για τη μετάδοση δεδομένων, ενισχύοντας έτσι την ικανότητα ανίχνευσης επίθεσης. Όταν μια διαδρομή δεν είναι διαθέσιμη, άλλες διαδρομές μπορούν επίσης να παρέχουν υπηρεσίες για να εξασφαλίσουν το QoS.

Έλεγχος ταυτότητας και εξουσιοδότηση

Ένας μηχανισμός ταυτοποίησης και εξουσιοδότησης συνιστούν την πρώτη υπερασπιστική γραμμή κατά μίας εισβολής. Οι επιτιθέμενοι συχνά εκμεταλλεύονται τις ευπάθειες στον έλεγχο ταυτότητας και της εξουσιοδότησης πρόσβασης στο σύστημα. Για παράδειγμα, στις IoT συσκευές ο εισβολέας μπορεί να παραβιάσει το απόρρητο του χρήστη λόγω της έλλειψης αποτελεσματικής προστασίας για την είσοδο του χρήστη. Επιπλέον, οι επιτιθέμενοι μπορούν να παρακάμψουν τους μηχανισμούς ελέγχου ταυτότητας και εξουσιοδότησης και μπορούν να εκτελέσουν κακόβουλη λειτουργία σε έξυπνες συσκευές.

Ο συνηθέστερος τρόπος επίλυσης αυτών των προβλημάτων είναι η υιοθέτηση ενός συστηματικού παραδείγματος ελέγχου πρόσβασης, όπως ο έλεγχος πρόσβασης βάσει ρόλων

(RBAC). Μια οντότητα μπορεί να παίξει πολλαπλούς ρόλους και κάθε ρόλος έχει διαφορετικές λειτουργίες. Το σύστημα διαχειρίζεται πρόσβαση και άδεια ανάλογα με το ρόλο.

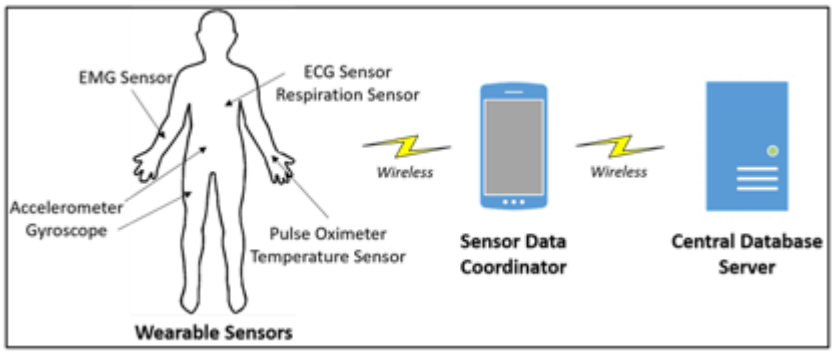
Υπάρχουν διάφοροι τρόποι για να ξεκινήσει μια επίθεση σε ένα IoT δίκτυο. Για παράδειγμα, οι επιθέσεις μπορούν να ξεκινήσουν από το επίπεδο λογισμικού και το επίπεδο υλικού. Ένας εισβολέας μπορεί φυσικά να έχει πρόσβαση στο σύστημα για να τροποποιήσει τα δεδομένα και ακόμα και αν έχει προκύψει έκτακτης ανάγκης, δεν θα ενεργοποιήσει κάποιον πραγματικό μηχανισμό σήμανσης συναγερμού. Επιπλέον, ένας εισβολέας μπορεί να τροποποιήσει την τιμή εμφάνισης για να καθυστερήσει την ανθρώπινη αντίδραση σε περίπτωση έκτακτης ανάγκης.

Από το επίπεδο του λογισμικού, οι επιτιθέμενοι μπορούν επίσης να εκμεταλλευτούν τα τρωτά σημεία του προγράμματος, όπως εμφύτευση κάποιου κώδικα. Επιπλέον, ο εισβολέας μπορεί να χρησιμοποιήσει τα τρωτά σημεία του πρωτοκόλλου επικοινωνίας. Επομένως, στο σχεδιασμό των μηχανισμών ασφαλείας στο IoT δίκτυο, πρέπει να εξετάσουμε όχι μόνο συγκεκριμένες μεθόδους επίθεσης αλλά και την ενσωμάτωση ποικίλων μεθόδων επίθεσης, για την υλοποίηση μίας πιο ολοκληρωμένης προοπτικής αντιμετώπισης ζητημάτων στην ασφάλεια του διαδικτύου των πραγμάτων. [31] , [34]

Κεφάλαιο 3
Αρχιτεκτονική Έξυπνου Νοσοκομείου

Όπως αναφέραμε παραπάνω, οι σύγχρονες εξελίξεις στις Τεχνολογίες Πληροφορικής και Επικοινωνιών όπως το Διαδίκτυο των Πραγμάτων (Internet-of-Things -IoT) επιτρέπει την ανάπτυξη καινοτόμων λύσεων υγειονομικής περίθαλψης αξιοποιώντας τις δυνατότητες που προσφέρει η τεχνητή νοημοσύνη. Η ιατρική φροντίδα μπορεί να παρέχεται όχι μόνο στο χώρο μίας υγειονομικής μονάδας αλλά και στο σπίτι ή στο γραφείο. Οι τεχνολογίες IoT μπορούν να δημιουργήσουν ένα σημείο διασύνδεσης ανάμεσα σε έξυπνα σπίτια και νοσοκομεία, έτσι ώστε διαφορετικά δίκτυα αισθητήρων να υποστηρίξουν νέους τρόπους διάγνωσης και ιατρικής φροντίδας μέσω του Διαδικτύου.

Στο κεφάλαιο αυτό παρουσιάζουμε την έννοια της Έξυπνης Ιατρικής Πύλης (ΕΙΠ). Μία τέτοια αρχιτεκτονική καλείται να επιτρέψει τη διασύνδεση πολλών απομακρυσμένων κέντρων ιατρικής περίθαλψης, και συστημάτων έξυπνων σπιτιών (πχ για ανθρώπους με αναπηρίες) για να μπορεί να αντιμετωπίσει διάφορες προκλήσεις όπως η κινητικότητα, η ενεργειακή απόδοση, η επεκτασιμότητα, αξιοπιστία αλλά και η ασφάλεια.

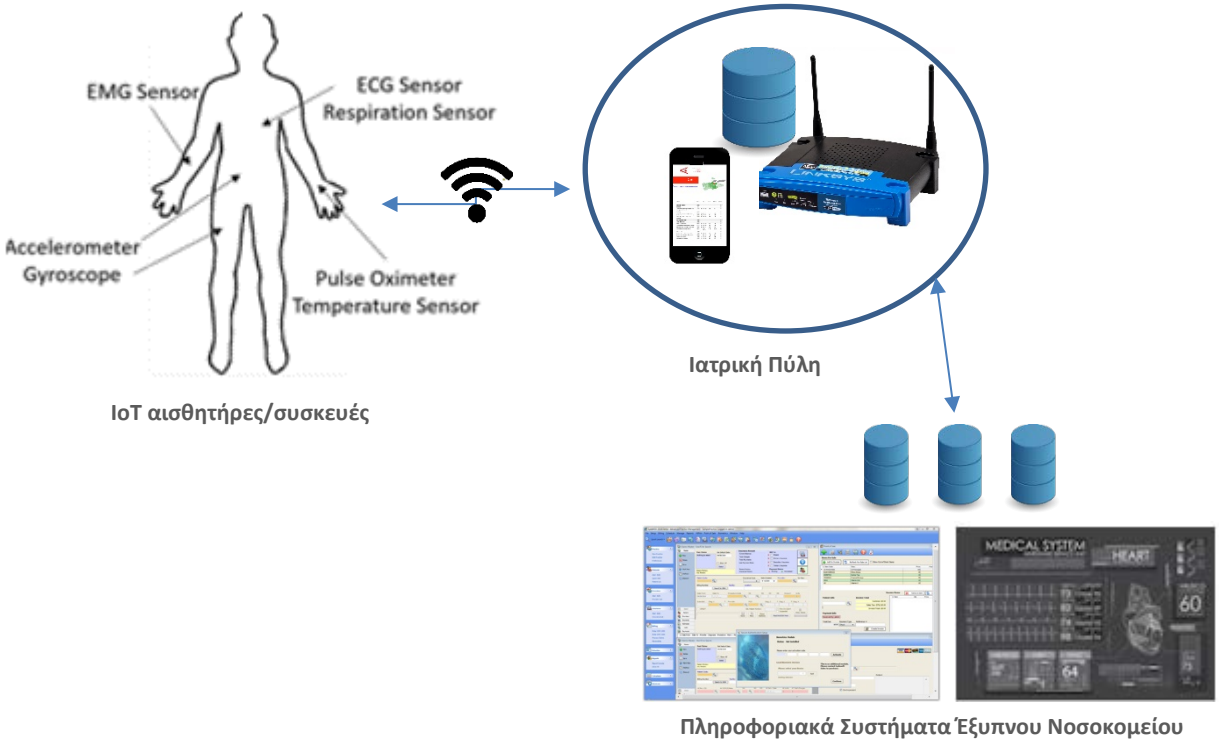


Εικόνα 3.1. Σύστημα απομακρυσμένης παρακολούθησης ασθενούς

Τα παραδοσιακά συστήματα απομακρυσμένης παρακολούθησης (Εικόνα 3.1) εξελίσσονται σε σύγχρονα οικοσυστήματα στα οποία οι ιατρικές αισθητήρες μεταδίδουν τα δεδομένα στις δικτυακές υπηρεσίες και βάσεις δεδομένων του έξυπνου νοσοκομείου μέσω IoT υποδομής.

Η Εικόνα 3.2 επεξηγεί τις βασικές συνιστώσες μίας τέτοιας αρχιτεκτονικής η οποία περιλαμβάνει τρία κύρια συστατικά:

i) δίκτυο αισθητήρων και IoT συσκευών που αντλούν δεδομένα από τον ασθενή
ii) Ιατρικές πύλες συνδεδεμένες στο Διαδίκτυο, και
iii) Πληροφοριακά Συστήματα του Έξυπνου Νοσοκομείου είτε σε φυσικές υπολογιστικές υποδομές ή στο υπολογιστικό νέφος.



Εικόνα 3.2. Σύστημα απομακρυσμένης παρακολούθησης ασθενούς -IoT αρχιτεκτονική

3.1 IoT Αρχιτεκτονική – βασικές λειτουργίες

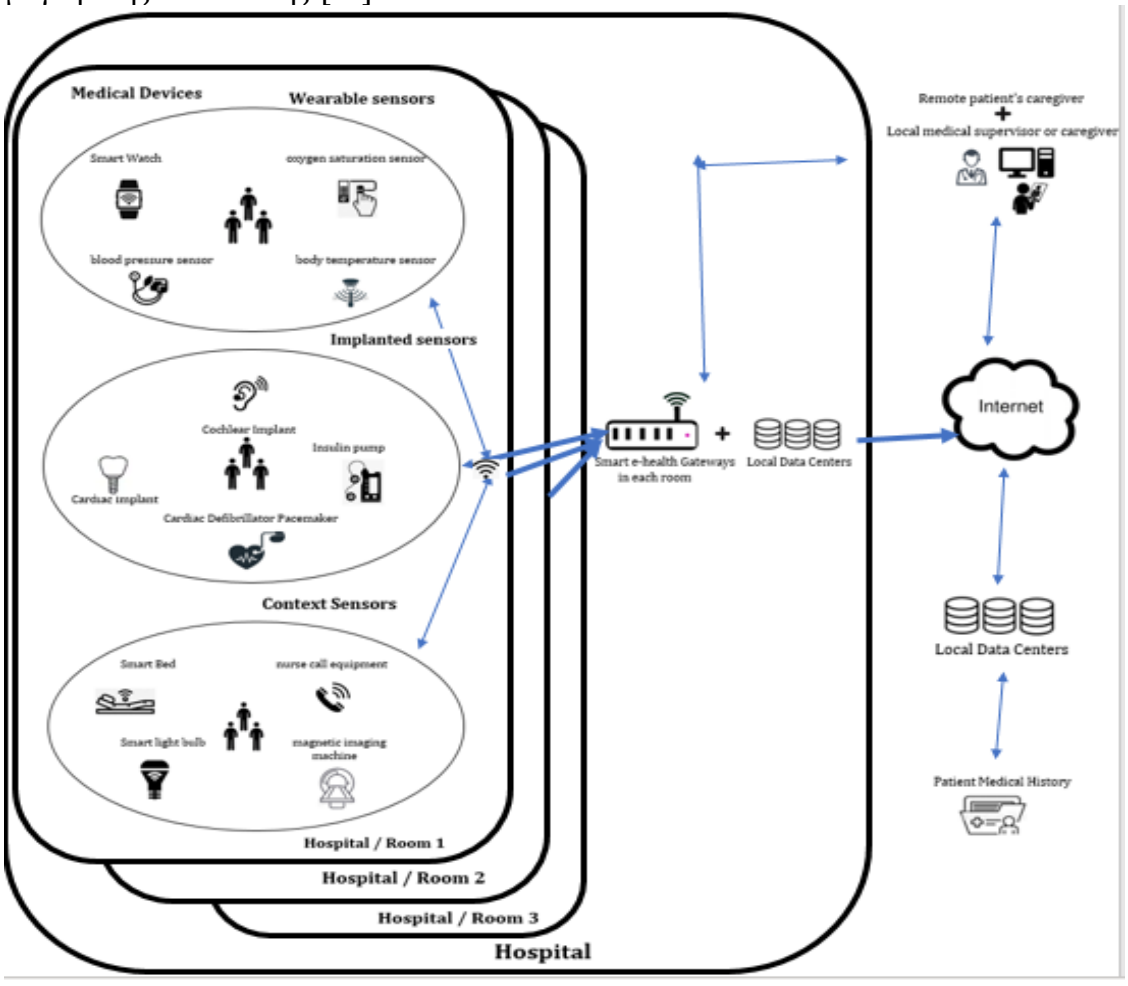
Το δίκτυο IoT συσκευών/αισθητήρων περιλαμβάνει συσκευές που μπορούν να λαμβάνουν αδιάλειπτα δεδομένα για την θερμοκρασία σώματος, πίεση αίματος, επίπεδα οξυγόνου, κατάσταση ύπνου, φυσική κατάσταση ασθενούς (πχ αν έχει πέσει στο πάτωμα). Τα δεδομένα αυτά μεταδίδονται ασύρματα σε μία ιατρική πύλη (που μπορεί να βρίσκεται σε μία συσκευή έξυπνου τηλεφώνου ή ένα έξυπνο δρομολογητή σπιτιού ή κλινικής μονάδας) και κατόπιν στη κεντρική υποδομή του έξυπνου νοσοκομείου. Η ιατρική πύλη αναλαμβάνει την επεξεργασία των

δεδομένων/σημάτων, την δημιουργία ενημερώσεων βάσει των δεδομένων, σύνθεση και φιλτράρισμα δεδομένων σε μία ολοκληρωμένη ιατρική εικόνα ενός ασθενούς.

Η κεντρική μονάδα του Έξυπνου Νοσοκομείου αναλαμβάνει την αποθήκευση των δεδομένων που λαμβάνει από τις πύλες, την παροχή λειτουργιών ανάλυσης των δεδομένων και λήψης αποφάσεων αναφορικά με τη φροντίδα ασθενών στις επιμέρους κλινικές μονάδες εντός του φυσικού χώρου του νοσοκομείου ή σε απομακρυσμένους χώρους. Τα κατάλληλα πληροφοριακά συστήματα κατευθύνουν τις φαρμακευτικές αγωγές και την άμεση παροχή ιατρικής φροντίδας με κεντρικοποιημένο τρόπο.

Οι εφαρμογές και σχετικές γραφικές διεπαφές των Πληροφοριακών Συστημάτων θα πρέπει να παρέχουν υπηρεσίες σε διάφορους ενδιαφερόμενους μέσω μίας τέτοιας πλατφόρμας. Τα δεδομένα που παράγονται από τους αισθητήρες που συνδέονται με τους χρήστες μπορούν με αυτό το τρόπο να διατίθενται σε φροντιστές, μέλη της οικογένειας και εξουσιοδοτημένα μέρη που πρέπει να έχουν τον έλεγχο και ενημέρωση για ζωτικά δεδομένα από οπουδήποτε και ανά πάσα στιγμή.

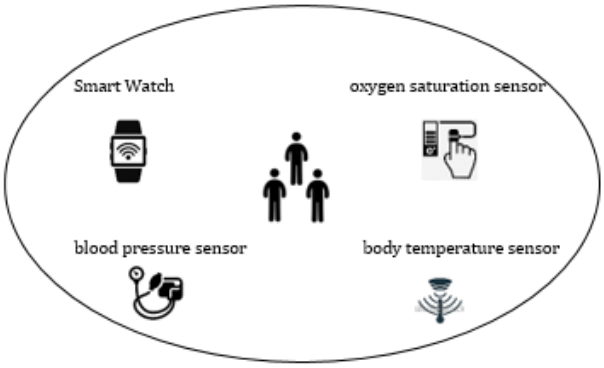
Η Εικόνα 3.3 δείχνει λεπτομερώς τις κύριες συνιστώσες ενός Έξυπνου Νοσοκομείου βασισμένου σε τεχνολογίες IoT. Το σύστημα μπορεί να οργανωθεί με κατανεμημένο τρόπο σε τρία επίπεδα για χρήση σε έξυπνα νοσοκομεία. Όπως αναφέραμε παραπάνω, οι πληροφορίες για την υγεία των ασθενών καταγράφονται από αισθητήρες που φοριούνται στο σώμα ή εμφυτεύονται ή παρακολουθούνται με άλλους τρόπους (πχ αναγνώριση προσώπου), με τους οποίους ο ασθενής είναι εξοπλισμένος για ατομική ιατρική παρακολούθηση μέσα από πολλαπλούς παραμέτρους. Επιπλέον, τα δεδομένα υγείας μπορούν να συμπληρωθούν με πληροφορίες από τους αισθητήρες περιβάλλοντος όπως το έξυπνο κρεβάτι, η έξυπνη λάμπα, εξοπλισμός κλήσης νοσοκόμας, μηχανή μαγνητικής απεικόνισης. [34]



Εικόνα 3.3. Προτεινόμενη IoT αρχιτεκτονική του Έξυπνου Νοσοκομείου [28]

Η λήψη επιπλέον στοιχείων που αφορούν το περιβάλλον επιτρέπει την αναγνώριση ασυνήθιστων μοτίβων και τη δημιουργία πιο ακριβή συμπερασμάτων σχετικά με την κατάσταση του ασθενούς. Άλλοι αισθητήρες και ενεργοποιητές (π.χ. ιατρικός εξοπλισμός) μπορούν επίσης να συνδεθούν με συστήματα μετάδοσης δεδομένων σε ιατρικές υπηρεσίες όπως εικόνες υψηλής ανάλυσης (π.χ. απεικονιστικά μηχανήματα, απεικόνιση αποτελεσμάτων μαγνητικού τομογράφου). Οι ιατρικές συσκευές που χρησιμοποιούνται για διάφορες εφαρμογές υγειονομικής περίθαλψης, μπορούν να υποδιαιρεθούν σε 3 μεγάλες ομάδες: Φορητοί Αισθητήρες, Εμφυτεύσιμοι Αισθητήρες και Αισθητήρες Περιβάλλοντος. Η αρχιτεκτονική ενός τέτοιου συστήματος περιλαμβάνει το ακόλουθα κύρια συστατικά [28]:

1. Φορητοί εξωτερικοί αισθητήρες: Υποστηρίζεται από πανταχού παρόντες λειτουργίες ταυτοποίησης, παρακολούθησης και επικοινωνίας, λήψης ιατρικών και άλλων δεδομένων από το σώμα του ασθενούς Τα δεδομένα μεταδίδονται στη συνέχεια στην πύλη μέσω πρωτοκόλλων ασύρματης επικοινωνίας όπως Bluetooth, Wi-Fi, ZigBee. Οι συσκευές αυτές είναι βιοαισθητήρες που παρακολουθούν φυσιολογικά δεδομένα με ασύρματη επικοινωνία, οι οποίες μπορούν να χρησιμοποιηθούν για παρακολούθηση τηλεϊατρικής και νοσηλείας. Για παράδειγμα, παρακολουθούν την αρτηριακή πίεση, τη θερμοκρασία, τη συνεχή γλυκόζη, το επίπεδο οξυγόνου.



Εικόνα 3.3.1: Φορητοί Αισθητήρες

Παρατηρούμε πως οι φορητοί αισθητήρες αποτελούνται από:

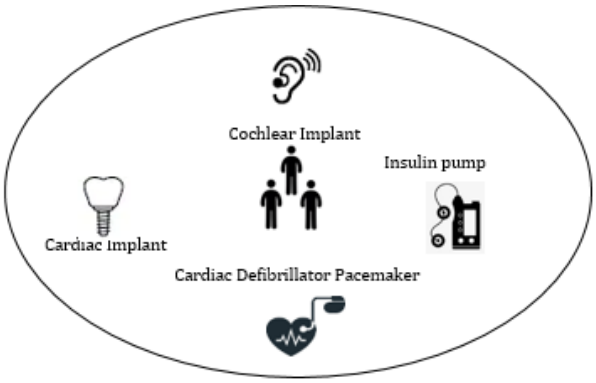
- Έξυπνο Ρολόι: Τα έξυπνα ρολόγια έχουν τη δυνατότητα να υποστηρίξουν την

υγεία των ασθενών στην καθημερινή ζωή. Δίνει τη δυνατότητα της αυτό-παρακολούθησης της προσωπικής τους δραστηριότητας.

- Αισθητήρας Αρτηριακής Πίεσης: Σχεδιασμένος για τη μέτρηση της πίεσης του ανθρώπου. Είναι συσκευή, της οποίας η οθόνη παρέχει ασύρματα ακριβείς μετρήσεις αρτηριακής πίεσης και καρδιακού ρυθμού με άμεση ανατροφοδότηση σχετικά με το πλήρες ιστορικό του ασθενή.

- Αισθητήρας Κορεσμού Οξυγόνου: Χρησιμοποιείται για τη μέτρηση των επιπέδων οξυγόνου στο αίμα ή του κορεσμού οξυγόνου στο αίμα του ασθενή. Οι πληροφορίες λαμβάνονται ασύρματα στη συσκευή που έχει το νοσηλευτικό προσωπικό.

- Αισθητήρας Θερμοκρασίας Σώματος : Συσκευή που προορίζεται για απομακρυσμένη παρακολούθηση της θερμοκρασίας του σώματος έως και 100 ώρες συνεχούς χρήσης. Οι πληροφορίες αποστέλλονται ασύρματα σε μια συσκευή αποθήκευσης ή μεταδίδονται απευθείας στο smartphone Bluetooth ανάλογα με την προβλεπόμενη εφαρμογή. Το smartphone μπορεί να χρησιμοποιηθεί για την οπτικοποίηση της μέτρησης για τον πελάτη ή τον ασθενή ή για την αποθήκευση εγγραφών στο cloud. Τώρα οι πάροχοι φροντίδας μπορούν να έχουν πρόσβαση σε δεδομένα από απόσταση και να ακολουθούν ορισμένες προϋποθέσεις.



Εικόνα 3.3.2: Εμφυτεύσιμοι Αισθητήρες

Παρατηρούμε πως οι Εμφυτεύσιμοι αισθητήρες αποτελούνται από:

- Κοχλιακό εμφύτευμα :Συσκευή που συνδέεται με την μπαταρία του επεξεργαστή

ήχου Naída CI Q90, μετατρέποντας αποτελεσματικά το κοχλιακό εμφύτευμα σε ασύρματο ακουστικό Bluetooth. Δεδομένου, ότι οι ασθενείς κοχλιακού εμφυτεύματος έχουν τη δυνατότητα να απαντούν απευθείας σε τηλεφωνικές κλήσεις και να μεταδίδουν ήχο στη συσκευή ακοής τους.

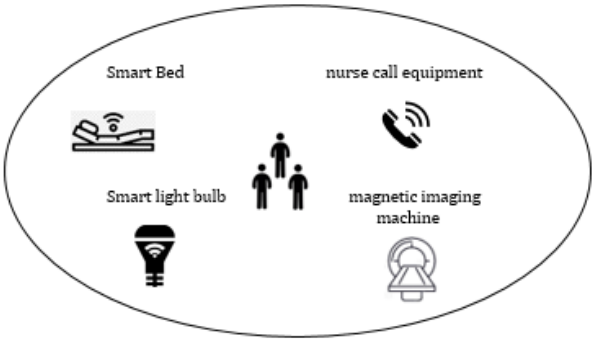
- Καρδιακό εμφύτευμα / Καρδιακός απινιδωτής βηματοδότης: Είναι μια μικρή συσκευή με μπαταρία τοποθετημένη στο στήθος του ασθενούς για την παρακολούθηση του καρδιακού του ρυθμού και την ανίχνευση ακανόνιστων καρδιακών παλμών. Οι πληροφορίες της συσκευής αποστέλλονται αυτόματα ασύρματα ICD ή χειροκίνητα από τον ασθενή. Η απομακρυσμένη παρακολούθηση είναι ένας τρόπος για την εμφυτευμένη καρδιακή συσκευή να επικοινωνεί με τον γιατρό ή την κλινική χρησιμοποιώντας μια μικρή οθόνη, μειώνοντας ενδεχομένως τον αριθμό των φορών που πρέπει να επισκεφτεί ο ασθενής την κλινική για έλεγχο εμφυτευμένης καρδιακής συσκευής.

Το ICD επικοινωνεί με έναν ασύρματο πομπό (Home Monitor) σε ακτίνα 3m, ο οποίος συνήθως τοποθετείται κοντά στο κρεβάτι του ασθενούς. Τα δεδομένα αυτά αποστέλλονται μέσω ενός αναλογικού σταθερού τηλεφώνου, το οποίο μπορεί να χρησιμοποιηθεί μόνο στη χώρα διαμονής του ασθενούς.

Επιπλέον, για σκοπούς απομακρυσμένης παρακολούθησης, η ανίχνευση ενός συμβάντος όπως η μη φυσιολογική αντίσταση μολύβδου θα προκαλέσει αμέσως το ICD να επιχειρήσει επικοινωνία με το Home Monitor με επαναλαμβανόμενες προσπάθειες κάθε 3 ώρες κατά τη διάρκεια 3 ημερών σε περίπτωση αδυναμίας επικοινωνίας, και μετά από ηχητικές ειδοποιήσεις.

- Αντλίες ινσουλίνης: Μικρή συσκευή που παρέχει ινσουλίνη για τη θεραπεία του διαβήτη. Μπορεί να χρησιμοποιηθεί ως αυτόνομη αντλία ινσουλίνης ή να ενσωματωθεί στο σύστημα συνεχούς παρακολούθησης γλυκόζης (CGM). Η συνεχής παρακολούθηση της γλυκόζης (CGM- Continuous Glucose Monitoring) είναι μια μέθοδος παρακολούθησης των επιπέδων γλυκόζης καθ' όλη τη διάρκεια της ημέρας και της νύχτας. Τα συστήματα CGM λαμβάνουν μετρήσεις γλυκόζης σε τακτά χρονικά διαστήματα, 24 ώρες την ημέρα και μεταφράζουν τις μετρήσεις σε δυναμικά δεδομένα, δημιουργώντας κατεύθυνση γλυκόζης και ρυθμό αλλαγής. Η εμφυτεύσιμη αντλία δίνει τη δυνατότητα

μιας ταχύτερης και αποτελεσματικής δράσης ινσουλίνης.



Εικόνα 3.3.3: Αισθητήρες Περιβάλλοντος

Παρατηρούμε πως οι αισθητήρες Περιβάλλοντος αποτελούνται από:

- Έξυπνο Κρεβάτι: Χρησιμοποιεί αισθητήρες και άλλες τεχνολογίες για τη συλλογή δεδομένων σχετικά με τον τρόπο που κοιμάται ο ασθενής. Οι πληροφορίες αυτές συμβάλλουν για να αυτορυθμιστεί και να βελτιώσει τον ύπνο του ασθενή. Ορισμένα έξυπνα κρεβάτια παρέχουν επίσης τις πληροφορίες ύπνου στη συσκευή κινητού του ασθενή, όπου μπορεί να αναφέρει πόσο καλά κοιμάται και προσφέρει συμβουλές για τον καλύτερο ύπνο.

- Έξυπνη Λάμπα: Έχει τη δυνατότητα δυναμικής αλλαγής χρωματισμού. Η εναλλαγή από ένα απαλό χρώμα σε ένα πιο σκούρο χρώμα είναι ένδειξη αύξησης της θερμοκρασίας στο δωμάτιο του ασθενούς (πληροφορία περιβάλλοντος).

- Εξοπλισμός κλήσης Νοσοκόμας: Η τεχνολογία προχωράει ραγδαία και κατέστη δυνατή την ασύρματη συσκευή κλήσης νοσοκόμας χωρίς την ανάγκη καλωδίωσης. Δίνει τη δυνατότητα στον ασθενή να επικοινωνεί άμεσα με το νοσηλευτικό προσωπικό. Η συσκευή αυτή λειτουργεί σε συνδυασμό με τη χρήση συσκευών VoIP που έχουν οι εργαζόμενοι για να λαμβάνουν έγκαιρα τα μηνύματα κειμένου ή φωνητικά μηνύματα που στέλνουν οι ασθενείς.

- Μηχανή μαγνητικής απεικόνισης: Χρησιμοποιεί αισθητήρες για να καταγράψει

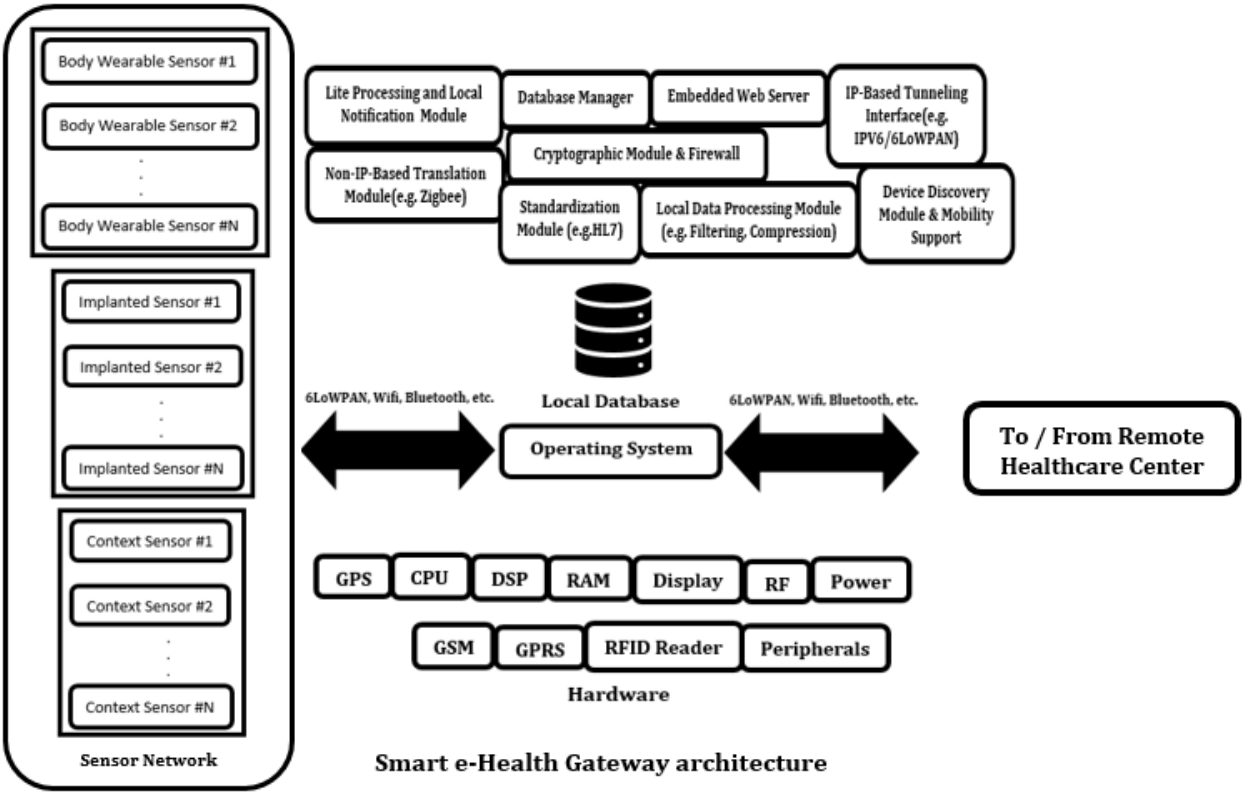
λεπτομερείς εικόνες τμημάτων του σώματος, συμπεριλαμβανομένου του εγκεφάλου.

2. Δίκτυο Έξυπνων Ιατρικών Πυλών: Αυτό το επίπεδο είναι η σύνθεση πολλαπλών γεωγραφικά κατανεμημένων έξυπνων πυλών ηλεκτρονικής υγείας. Κάθε πύλη, η οποία υποστηρίζει διαφορετικά πρωτόκολλα επικοινωνίας, ενεργεί ως ένα δυναμικό σημείο επαφής μεταξύ ενός δικτύου αισθητήρων (μιας κλινικής μονάδας) και του τοπικού δικτυακού πόρου (πχ τοπικού switch στον όροφο της κλινικής). Λαμβάνει δεδομένα από διαφορετικά υπο-δίκτυα, εκτελεί μετατροπή δεδομένων μεταξύ πρωτοκόλλων και παρέχει άλλες υψηλότερες υπηρεσίες επιπέδου, όπως συγκέντρωση δεδομένων και διαλογή δεδομένων σε πιο αφηρημένες δομές. Η πύλη στην άκρη του δικτύου συχνά εκτελεί απλώς βασικές λειτουργίες, όπως μετάφραση μεταξύ των πρωτοκόλλων που χρησιμοποιούνται στο Διαδίκτυο και των δικτύων αισθητήρων. Αυτές οι πύλες έχουν ευεργετική γνώση και εποικοδομητικό έλεγχο τόσο στο δίκτυο αισθητήρων όσο και στα δεδομένα που θα μεταδοθούν μέσω του Διαδικτύου. Προσφέρουν αρκετές υπηρεσίες υψηλότερου επιπέδου όπως τοπική αποθήκευση, τοπική επεξεργασία δεδομένων σε πραγματικό χρόνο, ενσωματωμένη εξόρυξη δεδομένων. Λόγω του περιορισμού του εύρους ζώνης του δικτύου και της ευαισθησίας του, βασικά δεδομένα στην υγειονομική περίθαλψη, η συμπίεση δεδομένων θεωρείται ως μια κατάλληλη δυνατότητα για Έξυπνες Πύλες Υγείας ως μία από τις υπηρεσίες που παρέχονται από τη μονάδα τοπικής επεξεργασίας δεδομένων.

3. Κεντρικό Πληροφοριακό Σύστημα Έξυπνου Νοσοκομείου: Το κεντρικοποιημένο σύστημα λειτουργεί σε φυσικές υπολογιστικές υποδομές ή στο υπολογιστικό νέφος και υποστηρίζει τη μετάδοση, και αποθήκευση δεδομένων για την υποστήριξη λειτουργιών ανάλυσης δεδομένων και λήψης αποφάσεων. Παρέχει γραφικές διεπαφές τελικού χρήστη για οπτική απεικόνιση και ανατροφοδότηση δεδομένων. Τα ιατρικά δεδομένα που συλλέγονται αποτελούν μία τεράστια δεξαμενή δεδομένων για στατιστικές μελέτες και επιδημιολογικές ιατρικές έρευνες. Συγκεκριμένα, τα δεδομένα αποστέλλονται απευθείας στο υπολογιστικό νέφος ή στον τοπικό ιατρό επόπτη, ο οποίος τα εξετάζει και τα αποθηκεύει στο υπολογιστικό νέφος. Στη συνέχεια, μεταφέρονται τα αρχεία στα τοπικά κέντρα δεδομένων και αποθηκεύεται το ιατρικό ιστορικό των ασθενών.

3.2 Αρχιτεκτονική Ιατρική Πύλης – βασικά χαρακτηριστικά

Η Εικόνα 3.4 παρουσιάζει μια εννοιολογική αρχιτεκτονική της έξυπνης ιατρικής πύλης που χρησιμοποιεί μια τοπική μονάδα επεξεργασίας για τη συλλογή, συμπίεση, συγχώνευση και ανάλυση δεδομένων. [34]



Εικόνα 3.4. Αρχιτεκτονική ιατρικής πύλης [28]

Ορισμένα από αυτά τα χαρακτηριστικά περιλαμβάνουν:

1. Φιλτράρισμα δεδομένων: Η ΕΙΠ αντιμετωπίζει το πρόβλημα του θορύβου που μπορεί να παρουσιαστεί κατά τη συλλογή δεδομένων από τους επιμέρους αισθητήρες. Καθώς διασυνδέεται με τους αισθητήρες απευθείας, λαμβάνει ψηφιακά σήματα μέσω διαφόρων πρωτοκόλλων επικοινωνίας και εφαρμόζει συγκεκριμένες τεχνικές αφαίρεσης θορύβου.

2. Συμπίεση δεδομένων: η ΕΙΠ καλείται να εφαρμόζει τόσο συμπίεση με απώλειες όσο και χωρίς απώλειες δεδομένων. Σε πολλές περιπτώσεις η μέθοδος συμπίεσης δεδομένων με απώλειες είναι περισσότερο χρήσιμη εξαιτίας των περιορισμένων πόρων σε ορισμένους αισθητήρες όπως η διάρκεια ζωής της μπαταρίας, και η διαθέσιμη επεξεργαστική ισχύς.

Ωστόσο, για εφαρμογές όπως η παρακολούθηση ηλεκτροκαρδιογραφημάτων (ΗΚΓ) σε πραγματικό χρόνο, είναι επιθυμητό να εφαρμόζεται συμπίεση χωρίς απώλειες για να διασφαλιστεί ότι όλα τα χαρακτηριστικά των σημάτων είναι αξιοποιήσιμα προς ανάλυση με υψηλή ακρίβεια.

3. Σύνθεση δεδομένων: Η σύνθεση δεδομένων μπορεί να πραγματοποιηθεί για διαφορετικούς λόγους όπως για την δημιουργία νέων δομών πληροφοριών σε ένα επιπλέον αφαιρετικό επίπεδο. Για παράδειγμα, η διαφορά θερμοκρασίας μεταξύ σώματος και περιβάλλοντος είναι μια πληροφορία που περιλαμβάνει τις τιμές από δύο διαφορετικούς αισθητήρες. Επιπλέον, είναι ωφέλιμο να λαμβάνονται (ανταγωνιστικές) τιμές από διαφορετικούς αισθητήρες για μία μόνο παράμετρο από διαφορετικές πηγές μόνο και μόνο για τη βελτίωση της ακρίβειας και της συνέπειας των αποτελεσμάτων σε περίπτωση σφάλματος σε ένα από τους αισθητήρες. Τέλος, παρέχονται ολοκληρωμένες πληροφορίες σχετικά με την ιατρική κατάσταση ενός ασθενούς για ζωτικά σήματα συνθέτοντας δεδομένα από διαφορετικές πηγές.

4. Ανάλυση δεδομένων: η λειτουργία αυτή είναι χρήσιμη επιτρέποντας τον εντοπισμό ή τη πρόβλεψη καταστάσεων έκτακτων αναγκών σε τοπικό επίπεδο. Για παράδειγμα, σε περίπτωση ανίχνευσης πτώσης ενός ηλικιωμένου ατόμου, η ΕΙΠ στέλνει την σχετική ένδειξη στο κεντρικό σύστημα μαζί με τις υπόλοιπες παραμέτρους και αναμένει τη τελική επιβεβαίωση από το κεντρικό σύστημα. Με αυτό το τρόπο το σύστημα του ΕΝ αντιδρά σε μία κατάσταση έκτακτης ανάγκης γρηγορότερα και πιο αξιόπιστα και μικραίνει το χρόνο απόκρισης σε κρίσιμες αποφάσεις.

   Επιπλέον, η τοπική ανάλυση και ανατροφοδότηση δεδομένων από τις IoT συσκευές και αισθητήρες βελτιώνει την αξιοπιστία του συστήματος σε περίπτωση μη διαθεσιμότητας του Διαδικτύου. Ειδικά στη περίπτωση μακροχρόνιας απομακρυσμένης παρακολούθησης ατόμων που αντιμετωπίζουν χρόνιες ασθένειες, η αποσύνδεση στο Διαδίκτυο μπορεί να συμβεί συχνά. Σε αυτή τη περίπτωση, η ΕΙΠ υποστηρίζει την τοπική επεξεργασία των δεδομένων. Επιπλέον, είναι δυνατή η τοπική αποθήκευση των δεδομένων σε επίπεδο ΕΙΠ και ο συγχρονισμός με το κεντρικό σύστημα σε δεύτερο χρόνο.

5. Προσαρμοστικότητα: κάποιες σημαντικές παράμετροι θα πρέπει να ρυθμίζονται ανάλογα με τη περίπτωση χρήσης. Η μετάδοση δεδομένων πρέπει να συντονίζεται σύμφωνα με έκτακτες ανάγκες όπως επίσης και ο ρυθμός μετάδοσης δεδομένων από και προς

διάφορους αισθητήρες. Για παράδειγμα, κατά τη μακροπρόθεσμη παρακολούθηση ενός ασθενής που πάσχει από μία καρδιαγγειακή νόσο, το σύστημα πρέπει να μάθει να αυξάνει το ρυθμό ανάγνωσης τιμών για παραμέτρους που σχετίζονται με την καρδιά κατά την ανίχνευση μίας μη φυσιολογικής ένδειξης.

6. Αποστολή προειδοποιήσεων: Η αποστολή τέτοιων μηνυμάτων είναι επίσης απαραίτητο χαρακτηριστικό μίας ΕΙΠ. Η ΕΙΠ πρέπει συχνά να ενημερώνει και να προειδοποιεί τις ιατρικές ομάδες, τους φροντιστές και τον ασθενή για καταστάσεις έκτακτης ανάγκης. Οποιαδήποτε αποτυχία στην υπηρεσία γνωστοποίησης μπορεί να προκαλέσει σοβαρά προβλήματα σε ασθενείς και ιατρικές θεραπείες. Μια πύλη έχει περιορισμένους πόρους και μπορεί να ειδοποιήσει μόνο μέσω συγκεκριμένων μέσων. Ωστόσο, το πλεονέκτημα τους είναι ότι οι πύλες ενεργούν ανεξάρτητα (π.χ. μέσω του τοπικού δικτύου ή GSM) ακόμη και κατά τη διάρκεια μη διαθεσιμότητας του διακομιστή στο πίσω μέρος, για μεγιστοποίηση της αξιοπιστίας του συστήματος και για να διασφαλιστεί ότι οι χρήστες μπορούν να λαμβάνουν κρίσιμες ειδοποιήσεις σε πραγματικό χρόνο.

7. Υποστήριξη Ανακάλυψης Συσκευών και Κινητικότητας: Η ανακάλυψη συσκευών έχει αναφερθεί στη διαλειτουργικότητα της συσκευής από την άποψη των αισθητήρων που ενεργοποιούνται μετά από ένα συγκεκριμένο χρονικό όριο και προσπάθεια εγγραφής στο δίκτυο. Σε σχέση με την κινητικότητα ενός ασθενούς από το ένα μέρος στο άλλο, η ανακάλυψη συσκευών αποτελεί τον κύριο ρόλο στην ανακάλυψη της πύλης προορισμού και στην παράδοση όλων των απαραίτητων πληροφοριών. Καθορίζει την πύλη προορισμού από τους αισθητήρες περιβάλλοντος και άλλες σχετικές πληροφορίες. ξεκινά τη διαπραγμάτευση έως παράδοση και ολοκλήρωση της ομαλής μετάβασης στο επόμενο. Συνοχή δεδομένων μεταξύ των προηγούμενων και των νέων πυλών διατηρεί τη χρήση του κοινόχρηστου διακομιστή cloud που είναι συνδεδεμένος σε όλες τις πύλες.

3.3 Ασφάλεια

Λαμβάνοντας υπόψη τις παραπάνω λειτουργίες σε επίπεδο IoT αρχιτεκτονικής καθώς και τις βασικές λειτουργίες σε επίπεδο ΕΙΠ, η ασφάλεια είναι μία από τις βασικότερες απαιτήσεις σε ένα τέτοιο οικοσύστημα. Επιμέρους συστατικά ή εφαρμογές μπορεί να έχουν σοβαρές ευπάθειες κρίνοντας τα ως μη ασφαλή. Για να ενισχυθεί η ασφάλεια λαμβάνονται

διάφορα μέτρα. Ένα από αυτά είναι η ενσωμάτωση τοίχους προστασίας. Το τοίχος προστασίας χρησιμοποιείται για τη διαμόρφωση ενός συνόλου κανόνων για το ποια πακέτα δεδομένων επιτρέπονται να ληφθούν ή να αποσταλούν. Οι πίνακες διαμορφώνονται έτσι ώστε να παραχωρούν δικαιώματα σε ορισμένες θύρες για επικοινωνία, ενώ άλλες θύρες έχουν αποκλειστεί για αποτροπή περιττής κίνησης.

Καθώς η πύλη μπορεί επίσης να λειτουργήσει ως ενσωματωμένος ιστός διακομιστή κατά τη μη διαθεσιμότητα του δικτύου (του κεντρικού συστήματος) ή όποτε χρειάζεται, μπορεί να επικοινωνήσει πάνω από το ασφαλές πρωτόκολλο HTTPS και να ελέγξει τη ταυτότητα των επιμέρους κόμβων αισθητήρων για τη διατήρηση της εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας του συστήματος.

Πέρα του τοίχους προστασίας λαμβάνονται υπόψη και επιπλέον μέτρα όπως η κρυπτογράφηση των δεδομένων πριν την μετάδοση τους. Επιπλέον, εφαρμόζονται σύγχρονες τεχνικές ελέγχου ταυτότητας και εξουσιοδότησης σε επίπεδο ΕΙΠ. Η προσέγγιση αυτή λαμβάνει υπόψη την επεξεργαστική ισχύ μιας έξυπνης πύλης, συνεπώς μπορεί να εκτελέσει εργασίες που σχετίζονται με την ασφάλεια. Κάτι τέτοιο δεν θα μπορούσε να γίνει αρκετά αποδοτικό σε επίπεδο IoT συσκευών καθώς διαθέτουν περιορισμένους πόρους [29].

Η παραβίαση του πρωτοκόλλου κρυπτογράφησης ή του μηχανισμού ταυτοποίησης μπορεί να οδηγήσει σε ορισμένους κινδύνους για τους ασθενείς, εάν ο εισβολέας καταφέρει να αποκτήσει πρόσβαση στα δεδομένα που συλλέγονται από τους αισθητήρες και ενδεχομένως τα αλλοιώσει. Τόσο η ΕΙΠ όσο οι εφαρμογές/υπο-συστήματα του κεντρικού πληροφοριακού συστήματος του ΕΝ πρέπει να διαθέτουν ισχυρούς μηχανισμούς έγκρισης πρόσβασης των χρηστών σε δεδομένα και λειτουργίες. Εάν ο μηχανισμός ελέγχου ταυτότητας δεν είναι αρκετά ισχυρός, τότε οι εισβολείς μπορούν να εκμεταλλευτούν αυτή την αδυναμία.

Εάν ένας αισθητήρας είναι συνδεδεμένος με έναν ασθενή, με αυτόν τον τρόπο, μπορεί να έχει ολέθριες συνέπειες και μπορεί να οδηγήσει σε απώλεια ζωής ενός ασθενούς. Έτσι, είναι πολύ σημαντικό αυτές οι συσκευές να διατηρούνται ασφαλείς. Οι IoT αισθητήρες που χρησιμοποιούνται σε ιατρικά συστήματα για την υποστήριξη ασθενών συνεχώς καταγράφουν τα δεδομένα σχετικά με τις επισκέψεις στο νοσοκομείο, τη κατάσταση της υγείας των ασθενών και αναλύουν τα δεδομένα σε πραγματικό χρόνο. Αν αυτά ενσωματώνονται επιπρόσθετα με μια παραδοσιακή πληροφοριακή υποδομή που χρησιμοποιείται στο νοσοκομείο, τότε δημιουργούνται περισσότερες προκλήσεις για την ασφάλεια. Επιπλέον, η παραπάνω

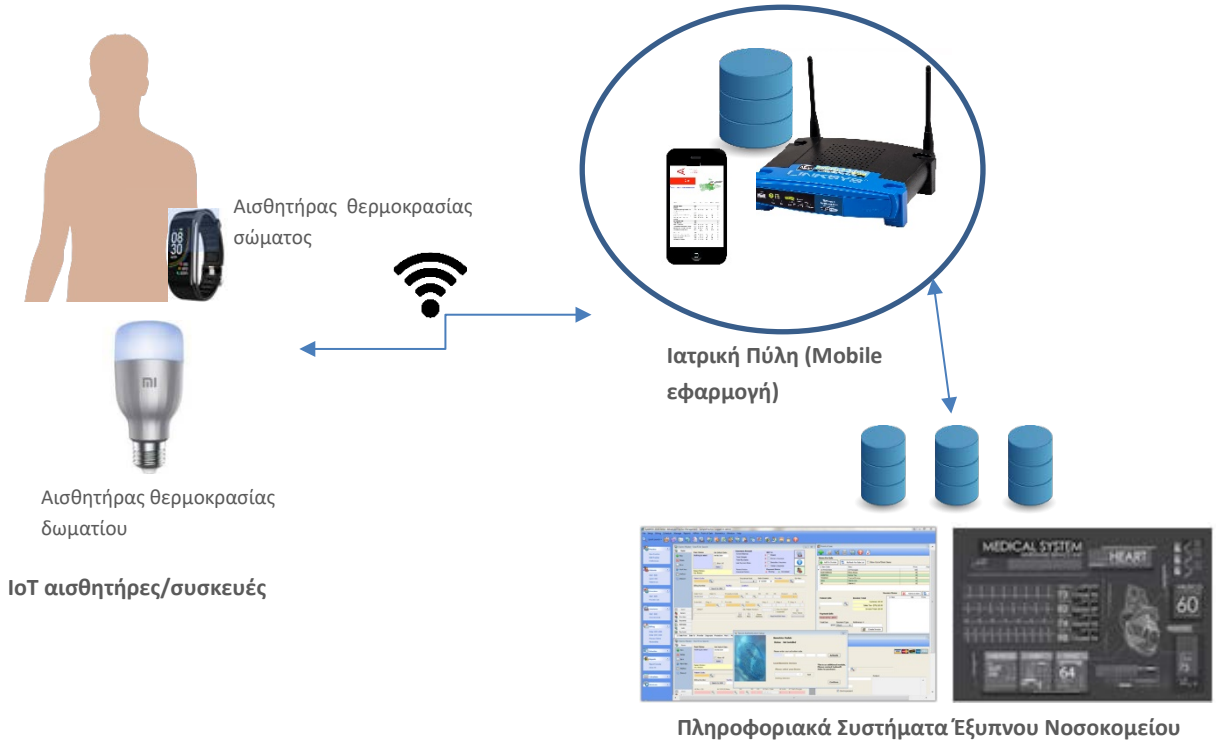
αρχιτεκτονική θεωρεί ότι οι έξυπνες πύλες είναι αποκεντρωμένες και δεν είναι απαραίτητα στον ίδιο χώρο. Αυτό καθιστά ακόμη πιο δύσκολη την πρόβλεψη και τον μετριασμό των απειλών ασφαλείας και την προστασία από κακόβουλες προθέσεις αν δεν ληφθούν μέτρα εξαρχής.

Και αντίστροφα, η κρίσιμη υποδομή νοσοκομείων και συστημάτων υγειονομικής περίθαλψης βασίζεται σε συσκευές αισθητήρων και συστήματα ελέγχου που ενδεχομένως να είναι ευάλωτα σε απειλές κατά της ασφάλειας. Εάν αυτές οι απειλές δεν αντιμετωπιστούν σωστά, τότε μπορεί κακόβουλοι παράγοντες να αποκτήσουν πρόσβαση σε τοπικές ή απομακρυσμένες έξυπνες πύλες και στη συνέχεια σε αισθητήρες παρακολούθησης. Και αυτό μπορεί να έχει σοβαρές επιπτώσεις στους ασθενείς καθώς ο εισβολέας αποκτά πρόσβαση στο σύστημα παρακολούθησης του ασθενούς και μπορεί να ελέγξει τις ιατρικές συσκευές, οι οποίες μπορούν να επηρεάσουν την ασφάλεια του ασθενούς.

Οι τελευταίες εξελίξεις σε IoT τεχνολογίες για έξυπνα νοσοκομεία περιλαμβάνουν ενσωματωμένα συστήματα ασφαλείας, ανίχνευση εισβολών και ασφάλεια αισθητήρων τύπου PLC. Ωστόσο, το γεγονός παραμένει ότι τα πρωτόκολλα IoT εξακολουθούν να μην διαθέτουν επαρκή χαρακτηριστικά που απαιτούνται για την προστασία των συστημάτων από έξυπνες απειλές στον κυβερνοχώρο. Η χρήση μεθόδων ταυτοποίησης για τη πρόσβαση των χρηστών σε δεδομένα μέσω ΕΙΠ καθώς και μέσω επιπρόσθετων παραγόντων ταυτοποίησης (πχ μέσω κινητού τηλεφώνου) μπορεί να βοηθήσει στην αντιμετώπιση τέτοιων απειλών.

Κεφάλαιο 4
Μεθοδολογία εντοπισμού ευπαθειών - Μελέτη Περίπτωσης

Έχοντας υπόψη την αρχιτεκτονική του έξυπνου νοσοκομείου που βασίζεται σε έξυπνες πύλες διαχείρισης IoT συσκευών (Εικόνα 3.3), εφαρμόζουμε μία μεθοδολογία ανίχνευσης ευπαθειών σε ένα μέρος της IoT αρχιτεκτονικής του έξυπνου νοσοκομείου. Το μέρος της αρχιτεκτονικής προς προσομοίωση επιθέσεων απεικονίζεται στην παρακάτω εικόνα.



Εικόνα 4.1. Σύστημα απομακρυσμένης παρακολούθησης ασθενούς -IoT αρχιτεκτονική με 2 αισθητήρες (θερμοκρασίας σώματος, IoT συσκευή θερμοκρασίας δωματίου) [33]

Η υποθετική αρχιτεκτονική περιλαμβάνει τα ακόλουθα συστατικά μέρη:

1. Ένα αισθητήρα θερμοκρασίας σώματος[1] με δυνατότητα λήψης δεδομένων από το σώμα του ασθενούς και μετάδοση των δεδομένων στην ΕΙΠ.

2. Ένα αισθητήρα θερμοκρασίας δωματίου. Η θερμοκρασία δωματίου καταγράφεται από μία έξυπνη λάμπα[2] που βρίσκεται στη διάθεση μας: καθώς η λάμπα έχει τη δυνατότητα δυναμικής αλλαγής χρωματισμού, η εναλλαγή από ένα απαλό χρώμα σε ένα πιο σκούρο χρώμα είναι ένδειξη αύξησης της θερμοκρασίας στο δωμάτιο του ασθενούς (πληροφορία περιβάλλοντος). Η τιμή αυτής της παραμέτρου θα μπορεί να συγκριθεί με τη τιμή της θερμοκρασίας του σώματος για πιο ακριβή συμπεράσματα ως προς την αύξηση της θερμοκρασίας του ασθενούς.

3. Μία εφαρμογή εγκατεστημένη σε κινητό τηλέφωνο που έχει το ρόλο της ΕΙΠ. [33] Συγκεκριμένα,

    a. Αναλαμβάνει την ανακάλυψη ιατρικών (IoT) συσκευών και αισθητήρων – όπως οι παραπάνω- στο τοπικό δίκτυο και την καταχώρηση τους στο δίκτυο του ΕΝ (device discovery function).

    b. Λαμβάνει δεδομένα από τις συσκευές μέσω ασύρματου δικτύου και προχωρά σε τοπική επεξεργασία και ανάλυση πριν την αποστολή τους στον απομακρυσμένο διακομιστή του κεντρικού συστήματος του IoT (data preprocessing, data cryptography).

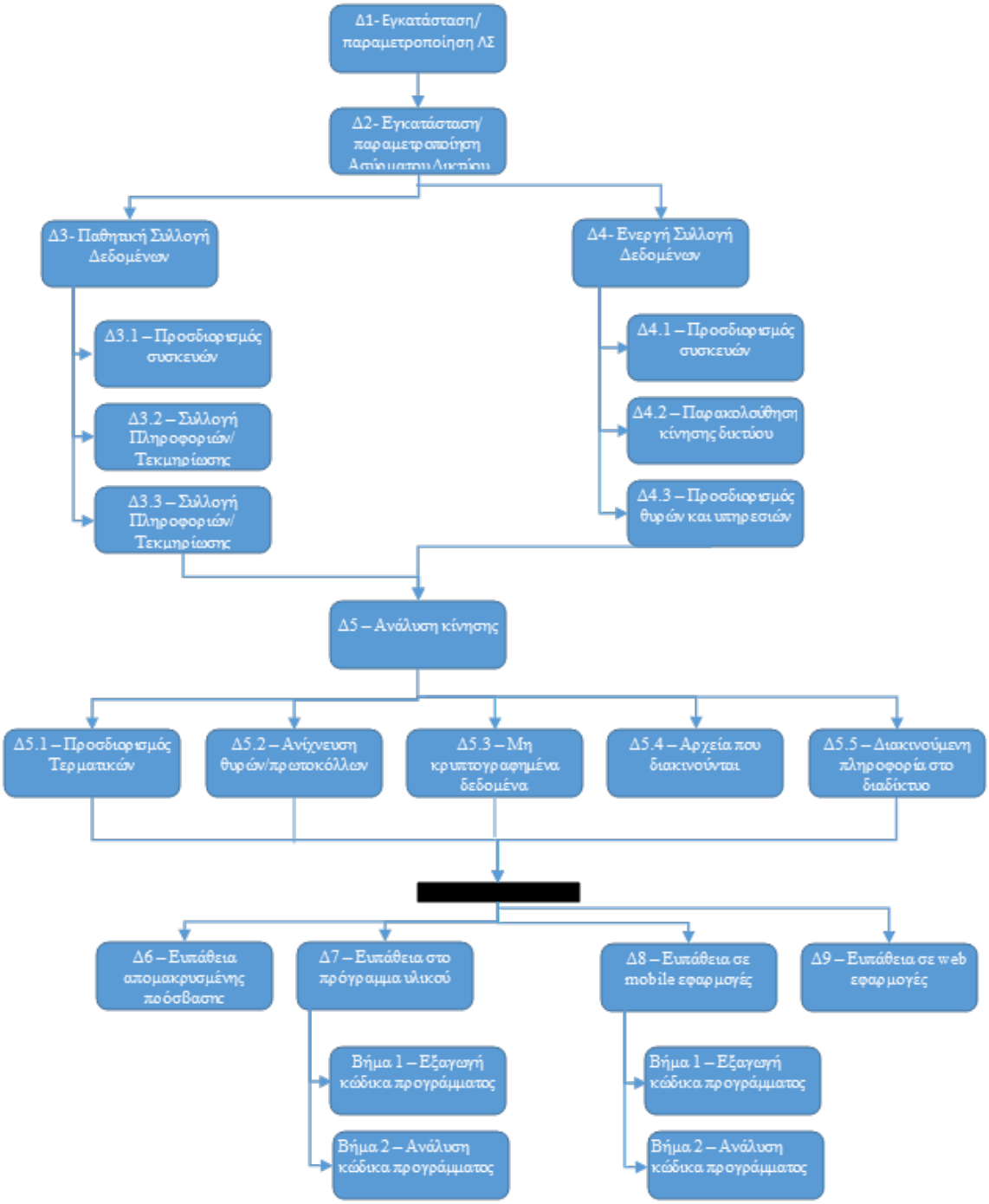
    c. Ενεργεί επάνω στις συσκευές ζητώντας να προσαρμόσουν το ρυθμό μετάδοσης δεδομένων αν το κρίνουν απαραίτητο (adaptivity).

Σημείωση: για λόγους συντόμευσης εφαρμογής της μεθοδολογίας δεν δίνονται περισσότερες λεπτομέρειες για το κεντρικό σύστημα του ΕΝ. Επικεντρωνόμαστε στην ανίχνευση ευπαθειών στον αισθητήρα θερμοκρασίας περιβάλλοντος και στη mobile εφαρμογή που προσομοιώνει τη λειτουργία της ΕΙΠ.

[1] https://www.banggood.com/Bakeey-C6T-Body-Temperature-Heart-Rate-Blood-Oxygen-Monitor-Brightness-Control-Weather-Display-Fitness-Tracker-Smart-Watch-p-1658043.html?rmmds=buy&ID=230&cur_warehouse=CN

[2] https://www.mi.com/us/yeelight-led-light-bulb

Το παρακάτω διάγραμμα παρουσιάζει τη ροή διαδικασιών και βημάτων της προτεινόμενης μεθοδολογίας.

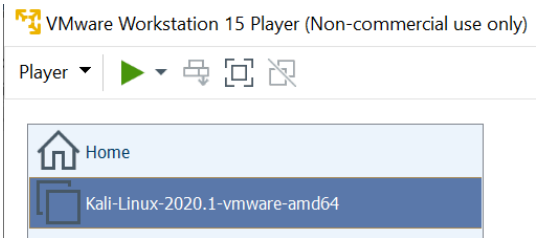


Εικόνα 4. 2. Προτεινόμενη μεθοδολογία – σύνολο διαδικασιών και βημάτων

Όλες οι διαδικασίες και τα στάδια στο ίδιο επίπεδο μπορούν να εκτελεστούν παράλληλα, αλλά μόνο εφόσον όλα έχουν εκτελεστεί μπορούμε να προχωρήσουμε στο επόμενο επίπεδο. Αν κάποια διαδικασία δεν μπορεί να εκτελεστεί για κάποιο λόγο (π.χ. η συσκευή δεν διαθέτει web εφαρμογή) τότε αγνοείται μαζί με τις υπο-εργασίες και βήματα.

4.1 Διαδικασία: Δ1- Εγκατάσταση/ παραμετροποίηση ΛΣ

Εγκαθιστούμε σε εικονικό μηχάνημα το λειτουργικό σύστημα (ΛΣ) Kali Linux[3] . Το τελευταίο αποτελεί το κατεξοχήν ΛΣ για την εγκατάσταση εργαλείων και την πραγματοποίηση επιθέσεων «καλού σκοπού» (ethical hacking). [32]



4.2 Διαδικασία: Δ2- Εγκατάσταση/ παραμετροποίηση Ασύρματου Δικτύου

Το δίκτυο της ΕΙΠ περιλαμβάνει ένα wifi router στο οποίο συνδέονται οι αισθητήρες και το κινητό τηλέφωνο (smart phone) στο οποίο εγκαθιστούμε την εφαρμογή Xiaomi Home App (προσομοίωση λειτουργίας ΕΙΠ). [33]

4.3 Διαδικασία: Δ3- Παθητική Συλλογή Δεδομένων

Αυτό το στάδιο επικεντρώνεται στη συλλογή πληροφοριών σχετικά με την έξυπνη IoT συσκευή και το οικοσύστημα της. Σε αυτό το στάδιο δεν γίνεται κάποια επικοινωνία με την IoT συσκευή ή το οικοσύστημά της. Αντίθετα, εστιάζουμε στο να συλλέξουμε πληροφορίες που είναι ευρύτερα διαθέσιμες. Το στάδιο αυτό χωρίζεται σε τρεις διαδικασίες:

[3] https://www.kali.org

1. **Δ3.1 – Προσδιορισμός συσκευών**

Συλλέγουμε περισσότερες πληροφορίες σχετικά με τις συσκευές όπως το εμπορικό σήμα, το μοντέλο και τον κατασκευαστή. Εάν είναι δυνατόν, η συσκευή μπορεί να αποσυναρμολογηθεί προκειμένου να εντοπιστούν τυχόν αριθμοί εξαρτημάτων, λογότυπα ή άλλες επιγραφές.

2. **Δ3.2 – Συλλογή Πληροφοριών/ Τεκμηρίωσης**

Όσο περισσότερες πληροφορίες συλλέγουμε για μια συσκευή, τόσο μεγαλύτερες οι πιθανότητες να κατανοήσουμε τον τρόπο λειτουργίας της και πώς αλληλεπιδρά με το οικοσύστημα της. Αναζητούμε εγχειρίδια χρήστη, τεκμηρίωση κώδικα/προγραμματιστικής βιβλιοθήκης (API) [4], τεκμηρίωση ανοιχτού κώδικα (αν υπάρχει), και αρχεία εγκατάστασης λογισμικού[5].

3. **Δ3.3 – Συλλογή Πληροφοριών/ Τεκμηρίωσης**

Οι περισσότερες συσκευές IoT χρησιμοποιούν μια εφαρμογή κινητού τηλεφώνου προκειμένου να ελέγχουν και να συλλέγουν δεδομένα από αυτές. Στο λειτουργικό σύστημα Android είναι δυνατή η απόκτηση μιας εφαρμογής απευθείας από ένα online αποθετήριο όπως ένα από τα παρακάτω:

- Google Play (http://play.google.com)
- APKmirror (https://www.apkmirror.com/)
- Aptoide (https://pt.aptoide.com/)

Στη περίπτωση μας κατεβάζουμε την εφαρμογή Mi Home (έκδοση 5.6.65) από το πρώτο αποθετήριο.

4.1 Διαδικασία: Δ4 – Ενεργή Συλλογή Δεδομένων

Η διαδικασία της ενεργής συλλογής πληροφοριών σημαίνει τη συλλογή πληροφοριών σχετικά με τη συσκευή IoT και το περιβάλλον του έξυπνου ιατρικού δικτύου. Αυτό γίνεται μέσω της παρακολούθησης του δικτύου και της μεταφοράς δεδομένων σε αυτό. Το στάδιο αυτό χωρίζεται σε τρεις υποενότητες.

[4] https://www.yeelight.com/en_US/developer
[5] https://www.yeelight.com/download/Yeelight_Inter-Operation_Spec.pdf

1. Δ4.1 – Προσδιορισμός συσκευών

Αυτή η διαδικασία αφορά τον εντοπισμό των IP διευθύνσεων των συσκευών και MAC διευθύνσεων στο δίκτυο. Εάν η παραμετροποίηση της συσκευής γίνεται μέσω του WiFi δικτύου θα πρέπει να προσπαθήσουμε να συνδεθούμε σε αυτό. Μερικές συσκευές εκθέτουν διαφορετικές δικτυακές πόρτες ή υπηρεσίες. Ένα εργαλείο που μπορεί να χρησιμοποιηθεί για τον εντοπισμό της διεύθυνσης IP και MAC της συσκευής είναι το Netdiscover[6].

Συμβάλλει στη συλλογή όλων των διευθύνσεων IP, παρέχοντας έτσι τη δυνατότητα να γίνονται επιθέσεις σε αυτά τα μηχανήματα που έχουν συγκεντρωθεί από το Netdiscover.

Χρήση: netdiscover [-i συσκευή] [-r εύρος | -p] [-s χρόνος] [-n κόμβος] [-c υπολογισμός] [-f] [-S]

Παράμετροι	Σημασία
-i συσκευή	: η συσκευή δικτύου σας
-r εύρος	: σάρωση συγκεκριμένου εύρους αντί για αυτόματη σάρωση. 192.168.6.0/24,/16,/8
-p παθητική λειτουργία:	: παίρνει μέρος σε δίκτυα όπως αυτά που έχουν διανομέα ως συσκευή σύνδεσης
- s χρόνος	: χρόνος για ύπνο μεταξύ κάθε αιτήματος arp (χιλιοστά του δευτερολέπτου)
-n κόμβος	: τελευταία οκτάδα ip που χρησιμοποιήθηκε για σάρωση (από 2 έως 253)
-c υπολογισμός	: αριθμός φορών για την αποστολή κάθε αιτήματος ARP (απώλεια πακέτων)
-f	: ενεργοποίηση γρήγορης σάρωσης
-S	: ενεργοποίηση καταστολής χρόνου ύπνου μεταξύ κάθε αιτήματος

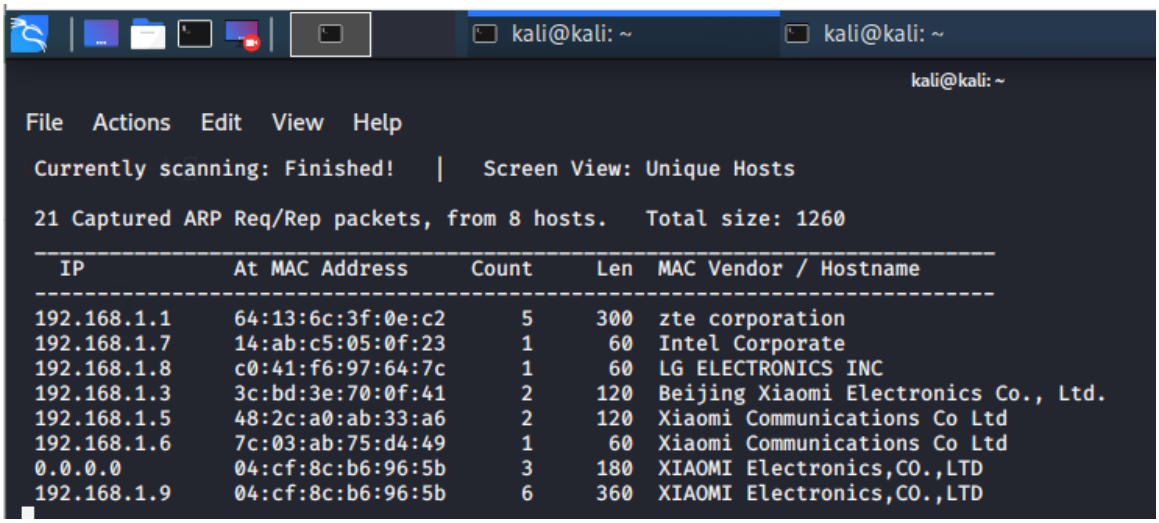
Πράγματι, χρησιμοποιώντας το εργαλείο στο ιατρικό δίκτυο 192.168.1.1 μέσα από το Kali εντοπίζουμε την IP, και τη MAC διεύθυνση της IoT συσκευής εκτελώντας την εντολή:

netdiscover –r 192.168.1.1/24

[6] https: //github.com/alexxy/netdiscover

επιστρέφοντας:

- IP: 192.168.1.9
- MAC Address: 04:cf:8c:b6:96:5b



2. Δ4.2 – Παρακολούθηση κίνησης δικτύου

Καταγράφοντας τις εισερχόμενες και εξερχόμενες επικοινωνίες προς και από τη συσκευή και το περιβάλλον της, μπορούμε να εξαγάγουμε πολύτιμες πληροφορίες που μπορούν να αξιοποιηθούν σε μεταγενέστερο στάδιο. Καθώς ορισμένες συσκευές IoT πραγματοποιούν διαφορετικές επικοινωνίες σύμφωνα με την κατάστασή τους, είναι σημαντικό να καταγραφθεί η κίνηση στο δίκτυο που αφορά αυτή τη συσκευή σε διαφορετικές καταστάσεις όπως:

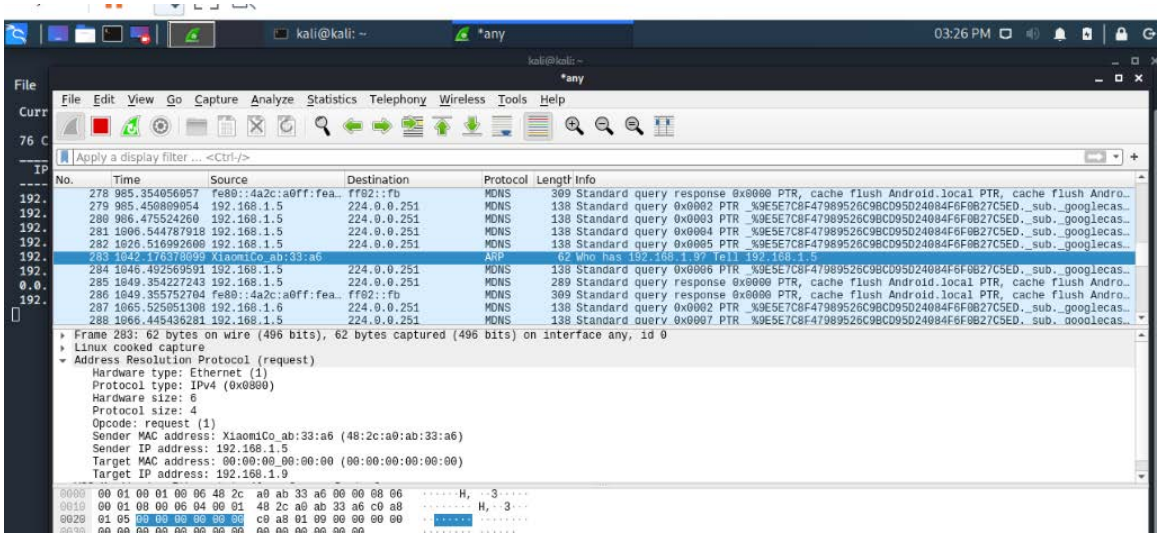
- Εκκίνηση, κατάσταση στην οποία δεν πραγματοποιείται κάποια ρύθμιση και η συσκευή τίθεται σε κατάσταση αναμονής.
- Επικοινωνία με mobile, και web εφαρμογές.
- Κατά την ενημέρωση του λογισμικού διαχείρισης του υλικού.
- Χωρίς σύνδεση στο διαδίκτυο.

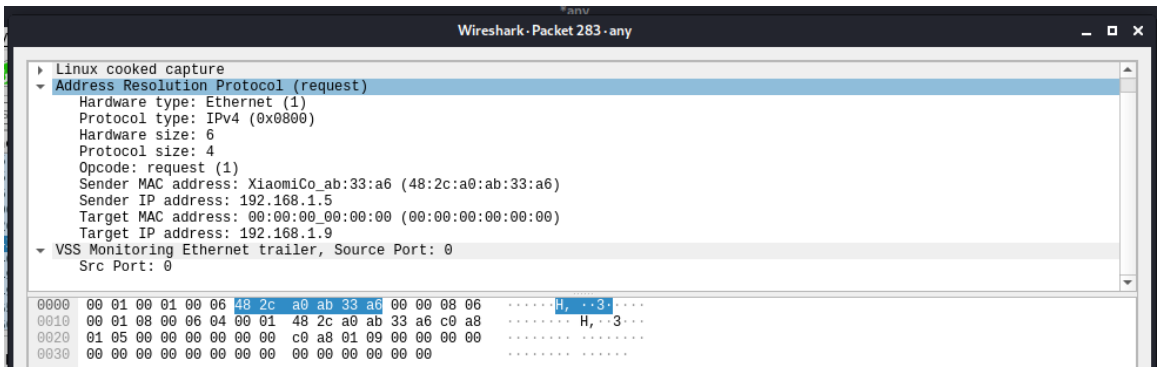
Η αποτύπωση της κίνησης στο δίκτυο μπορεί να γίνει με το εργαλείο Wireshark[7].

Είναι ένα ελεύθερο και ανοιχτού κώδικα λογισμικό ανάλυσης πρωτοκόλλων δικτύου υπολογιστών. Χρησιμοποιείται για ανάλυση δικτύου, παρακολούθηση δικτύου, εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα.

[7] https://www.wireshark.org/

Παρακολουθώντας την κίνηση στο δίκτυο 192.168.1.1 (εικόνα παρακάτω) παρατηρούμε την επικοινωνία ανάμεσα στην IP της συσκευής (192.168.1.9) και μία άλλη συσκευή (IP: 192.168.1.5). Επομένως επιβεβαιώνεται ο παραπάνω κανόνας της αποτύπωσης της κίνησης κατά την επικοινωνία της IoT συσκευής με κάποια mobile, ή web εφαρμογή. Αυτό θα επιτρέψει την αναζήτηση σε επόμενο στάδιο των δικτυακών θυρών, υπηρεσιών που τρέχουν στις πόρτες αυτές και εφαρμογών.





3. Δ4.3 – Προσδιορισμός θυρών και υπηρεσιών

Το τελικό βήμα αυτής της διαδικασίας περιλαμβάνει την προσπάθεια απαρίθμησης των δικτυακών θυρών που είναι ανοιχτές στη συσκευή και του προσδιορισμού των υπηρεσιών που εκθέτουν. Ορισμένες συσκευές έχουν δεκάδες ανοικτές δικτυακές πόρτες που εκθέτουν υπηρεσίες όπως το SSH ή το Telnet. Ένα τέτοιο εργαλείο για αυτή τη διαδικασία είναι το Nmap[8].

[8] https://nmap.org/

Είναι ένα ανοικτό εργαλείο πηγής για την εξερεύνηση του δικτύου και τον έλεγχο της ασφάλειας που αρχικά γράφτηκε από τον Gordon Lyon (γνωστός επίσης με το ψευδώνυμο Fyodor Vaskovich).

Λειτουργεί ως σαρωτής ασφαλείας και χρησιμοποιείται για να ανακαλύψει κεντρικούς υπολογιστές και τις υπηρεσίες σε ένα δίκτυο υπολογιστών, δημιουργώντας έτσι ένα "χάρτη" του δικτύου. Η λειτουργία του παρέχει στο χρήστη μια αναλυτική εικόνα προς ελέγχου δικτύου φανερώνοντας πιθανά προβλήματα και ελλείψεις ασφάλειας.

Παράμετροι	Σημασία
-sS	: προεπιλεγμένη παράμετρος σάρωσης, καθορίζει τον τρόπο με τον οποίο θα σαρώσει το Nmap
-T χρονικό διάστημα	: κυμαίνεται από 0 έως 5, με το 0 να είναι το πιο αργό και λιγότερο επεμβατικό και το 5 να είναι το ταχύτερο και πιο εμφανές
-iL εισαγωγή λίστας στόχου	: δίνει τη δυνατότητα αποθήκευσης στόχων και την επανάληψη των σαρώσεων σε μεταγενέστερο χρόνο
-F	: σάρωση μόνο τις 100 πιο συχνά χρησιμοποιούμενες θύρες αντί για τις 1000 θύρες
--open	: ανίχνευση ανοικτών δικτυακών θυρών σε ένα συγκεκριμένο μηχάνημα
-sV	: λήψη λεπτομερειών πληροφοριών σχετικά με τις υπηρεσίες που εκτελούνται σε ένα μηχάνημα.
-p	: καθορίζει συγκεκριμένες θύρες για σάρωση
-A	: συλλέγει επιθετικά όσο περισσότερες πληροφορίες μπορεί

Εκτελώντας την εντολή nmap –p1–65535 192.168.1.16 ανιχνεύεται μία ανοιχτή πόρτα στην IoT συσκευή (η 56130).

```
kali@kali:~$ nmap -p1-65535 192.168.1.16
Port 56130 is open
```

Σημείωση: καθώς το παραπάνω βήμα εκτελέστηκε σε διαφορετική χρονική στιγμή από το 1ο και το 2ο βήμα παραπάνω, η συσκευή άλλαξε IP (από 192.168.1.9 σε 192.168.1.16). Σε κάθε περίπτωση αυτό δεν επηρεάζει τη διαδικασία.

4.2 Δ5 – Ανάλυση κίνησης

Αξιοποιώντας τη πληροφορία που συλλέξαμε μέσω των παραπάνω διαδικασιών προχωράμε σε ανάλυση της κίνησης στο δίκτυο. Στόχος αυτής της ανάλυσης είναι να καθορίσουμε τον τρόπο με τον οποίο οι διάφορες συσκευές και εφαρμογές στο δικτυακό περιβάλλον αλληλεπιδρούν μεταξύ τους και τι είδους πληροφορίες αποστέλλονται και λαμβάνονται. Τα παρακάτω βήματα είναι οι βασικές πτυχές για την συλλογή πληροφοριών σε αυτό το στάδιο:

1. Ταυτοποίηση τελικού σημείου: Προσδιορισμός διεύθυνσης IP, δικτυακού τομέα και τοποθεσίας όλων των τελικών σημείων.
2. Θύρες και πρωτόκολλα: Τι θύρες δικτύου και πρωτόκολλα χρησιμοποιήθηκαν.
3. Δεδομένα που αποστέλλονται χωρίς κρυπτογράφηση.
4. Αρχεία που ανταλλάσσονται.
5. Πληροφορίες που αποστέλλονται στο Διαδίκτυο.

Η ανάλυση της κίνησης στο δίκτυο σε πραγματικό χρόνο γίνεται χρησιμοποιώντας το εργαλείο Wireshark.

4.3 Δ6 – Ευπάθεια απομακρυσμένης πρόσβασης

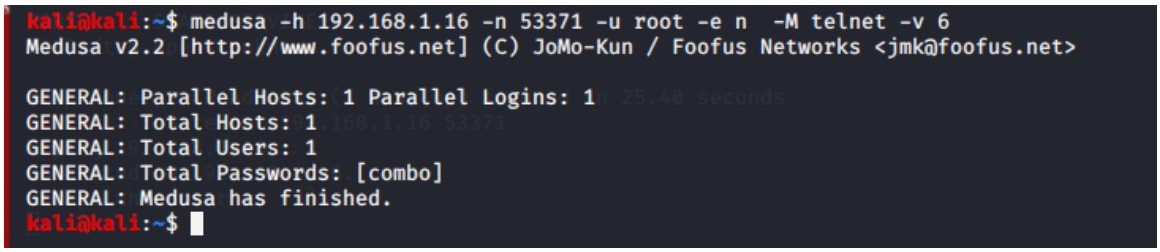
Ορισμένες συσκευές IoT διαθέτουν πρωτόκολλο απομακρυσμένης πρόσβασης, όπως Telnet ή SSH. Οι πιο κοινές επιθέσεις σε αυτές τις υπηρεσίες είναι Brute Force ή Dictionary επιθέσεις [2]. Για να ελεγχθεί εάν η υπηρεσία απομακρυσμένης πρόσβασης είναι ευάλωτη σε οποιαδήποτε από τις προαναφερθείσες επιθέσεις μπορεί να χρησιμοποιηθεί κάποιο εργαλείο όπως το Medusa[9].

Εκτελώντας την εντολή medusa –h 192.168.1.16 –n 53371 –u root –e n –M telnet –v 6

- h: όνομα ή IP υπολογιστή
- n: πόρτα η οποία είναι ανοιχτή στη συσκευή
- u: κωδικός χρήστη που δοκιμάζουμε
- e: n (δηλώνουμε ότι δεν θα χρησιμοποιηθεί κωδικός πρόσβασης)
- M: πρωτόκολλο απομακρυσμένης πρόσβασης

[9] https://github.com/jmk-foofus/medusa

- v: επίπεδο πληροφόρησης κατά την επιστροφή αποτελεσμάτων (επιλέγουμε το πιο αναλυτικό – επίπεδο 6)



Η παραπάνω δοκιμή επιβεβαιώνει ότι η συσκευή δεν απαιτεί διαδικασία ταυτοποίησης για την πρόσβαση στις υπηρεσίες. Αυτό δίνει τη δυνατότητα σε κάποιον εισβολέα που γνωρίζει τη προγραμματιστική βιβλιοθήκη της συσκευής να αποστείλει εντολές στη συσκευή και να μεταβάλλει τη συμπεριφορά της.

4.4 Δ7 – Ευπάθεια στο πρόγραμμα υλικού

Η εξερεύνηση του προγράμματος διαχείρισης υλικού μίας συσκευής IoT είναι από τους πιο σημαντικούς τρόπους εντοπισμούς τρωτών σημείων. Ορισμένες από αυτές τις συσκευές διαθέτουν μια περιορισμένη έκδοση του λειτουργικού συστήματος Linux, ενώ η δομή των αρχείων και οι υπηρεσίες είναι πολύ παρόμοιες με αυτές ενός επιτραπέζιου υπολογιστή. Ένα από τα πιο κοινά ευρήματα που συνήθως διαπιστώνεται είναι η έκθεση ευαίσθητων δεδομένων όπως οι κωδικοί σύνδεσης. Προτείνεται η εκτέλεση των παρακάτω βημάτων, προκειμένου να προσδιοριστούν ευαίσθητες πληροφορίες στο λογισμικό.

1. **Βήμα 1 – Εξαγωγή κώδικα προγράμματος**

Στόχος αυτής της διαδικασίας είναι η εξαγωγή του προγράμματος υλικού από την εικόνα του λογισμικού, τυπικά θα είναι ένα αρχείο τύπου binary. Ορισμένοι κατασκευαστές διαθέτουν αυτά τα αρχεία για λήψη από τους ιστοτόπους τους, ή μπορούμε να τα αποκτήσουμε καταγράφοντας τη μεταφορά δεδομένων στο δίκτυο, για παράδειγμα κατά τη διάρκεια ενημέρωσης της τρέχουσας έκδοσης του λογισμικού. Αν κάποιος αποκτήσει φυσική πρόσβαση στη συσκευή, τότε θα μπορεί να εξάγει το λογισμικό απευθείας από τον φάκελο σημείο αποθήκευσης (σύμφωνα με τη δομή αρχείων του).

Ένα τέτοιο πρόγραμμα που επιτρέπει την εξαγωγή φακέλων από το πρόγραμμα υλικού είναι το binwalk[10].

Παράμετροι	Σημασία
-B	: Σάρωση αρχείων προορισμού για κοινές υπογραφές αρχείων
-R	: Σάρωση αρχείων προορισμού για την καθορισμένη ακολουθία byte
-I	: Εμφάνιση αποτελεσμάτων επισημασμένα ως μη έγκυρα
-e	: Αυτόματη εξαγωγή γνωστών τύπων αρχείων
-j	: Περιορισμός του μεγέθους κάθε εξαγόμενου αρχείου
-r	: Διαγραφή σκαλισμένων αρχείων μετά την εξαγωγή

Σε αυτή τη μελέτη περίπτωσης δοκιμάσαμε τα παραπάνω προκειμένου να αποκτήσουμε πρόσβαση στον κώδικα του προγράμματος υλικού ωστόσο ούτε το πρόγραμμα ήταν διαθέσιμο στο διαδίκτυο ούτε μπορέσαμε να αποτυπώσουμε συγκεκριμένες λεπτομέρειες κατά την διαδικασία ενημέρωσης του λογισμικού στην IoT συσκευή.

2. Βήμα 2 – Ανάλυση κώδικα προγράμματος

Εφόσον είχαμε πρόσβαση στα αρχεία του λογισμικού, θα μπορούσαμε να αρχίσουμε να αναζητάμε πληροφορίες που μπορούν να μας βοηθήσουν να εντοπίσουμε μερικά τρωτά σημεία και να μελετήσουμε τη συμπεριφορά της συσκευής. Οι πληροφορίες που πρέπει να αναζητήσουμε είναι οι ακόλουθες:

- Πιστοποιητικά σύνδεσης - Όνομα χρήστη και κωδικός πρόσβασης που έχουν δηλωθεί στον κώδικα.
- Backdoors - Συνήθως υπηρεσίες Telnet ή SSH.
- URLs - Αποθηκευτικοί χώροι του υλικολογισμικού ή πηγαίου κώδικα, συνδέσεις σε web, ή cloud υπηρεσίες χωρίς ταυτοποίηση.
- Κλειδιά κρυπτογράφησης - συμμετρικά κλειδιά στο πηγαίο κώδικα ή σε έναν φάκελο.
- Αλγόριθμοι κωδικοποίησης- Πληροφορίες σχετικά με τους αλγορίθμους κρυπτογράφησης που εφαρμόζονται που μπορούν να βοηθήσουν στην αποκρυπτογράφηση των επικοινωνιών.

[10] https://github.com/ReFirmLabs/binwalk

- Μηχανισμοί ταυτοποίησης - Λεπτομέρειες σχετικά με τη προγραμματιστική βιβλιοθήκη, την web εφαρμογή ή άλλες διαδικασίες ταυτοποίησης.

Το Firmwalker[11] είναι ένα εργαλείο που αναζητά συγκεκριμένες λέξεις στον κώδικα του προγράμματος (όπως "password" ή "admin"), επεκτάσεις, τύπους αρχείων, IP και email διευθύνσεις και άλλα. Ωστόσο όπως αναφέρθηκε παραπάνω, η αξιοποίηση αυτού του εργαλείου δεν ήταν εφικτή καθώς δεν πετύχαμε πρόσβαση στο πρόγραμμα του υλικού.

4.5 Δ8 – Ευπάθεια σε mobile εφαρμογές

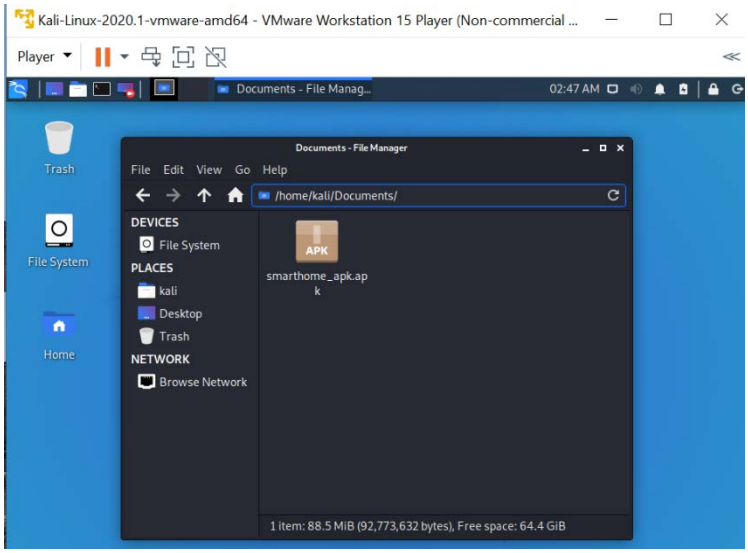
Ορισμένες εφαρμογές για κινητά τηλέφωνα εκθέτουν επίσης ευαίσθητες πληροφορίες που μπορεί να βοηθήσει στην εξερεύνηση άλλων τρωτών σημείων στη συσκευή ή στο δίκτυο. Εκτός αυτού, οι ίδιες οι εφαρμογές μπορούν να έχουν τρωτά σημεία. Προκειμένου να γίνει μια ανάλυση ανίχνευσης ευπαθειών σε αυτές τις εφαρμογές απαιτείται απόκτηση γνώσης σχετικά με το λειτουργικό σύστημα (πχ Android) και τις εφαρμογές σε αυτό. Αλλά ακόμη και χωρίς αυτές τις γνώσεις μπορούμε να χρησιμοποιήσουμε εργαλεία για τον εντοπισμό ευπαθειών. Αυτή η διαδικασία περιλαμβάνει δύο βήματα για τον εντοπισμό ευπαθειών.

1. **Βήμα 1 – Εξαγωγή κώδικα προγράμματος**

Ο πηγαίος κώδικας εφαρμογών Android εξάγεται συνήθως από το αρχείο εγκατάστασής του τύπου APK. Αυτό το αρχείο μπορεί να ληφθεί από ένα από τα αποθετήρια που αναφέραμε στην Διαδικασία 3.3. Κατόπιν τα αρχεία με τον πηγαίο κώδικα έτσι όπως σχηματίστηκε με αντίστροφο τρόπο από τις java classes (reverse engineering) είναι διαθέσιμα προς ανάλυση. Για την εξαγωγή του πηγαίου κώδικα μπορεί να χρησιμοποιηθεί το εργαλείο QARK11. Το εργαλείο αυτό αναλαμβάνει όχι μόνο την εξαγωγή του πηγαίου κώδικα, αλλά και την ανάλυση τυχόν ευπαθειών όπως θα δούμε στο επόμενο βήμα.

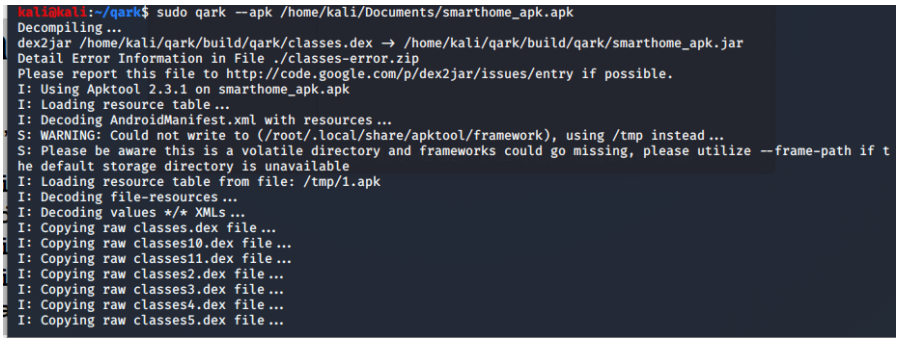
Στη συγκεκριμένη μελέτη περίπτωσης κατεβάζουμε από το αποθετήριο της google το αρχείο εγκατάστασης του Xiaomi Mi SmartHome. Η εφαρμογή αυτή διαχειρίζεται μέσω κινητού όλες τις Xiaomi IoT συσκευές που εγκαθίστανται σε ένα wifi δίκτυο. Το αρχείο αντιγράφεται στο Kali Linux για να αναλυθεί από το Qark.

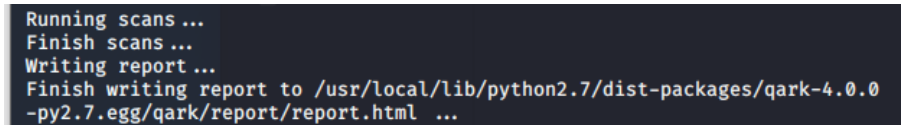
[11] https://github.com/craigz28/



Στη συνέχεια εγκαθιστούμε το εργαλείο Qark στο Kali Linux.

Το εργαλείο εκτελείται έχοντας ως παράμετρο το μονοπάτι του αρχείου εγκατάστασης της Xiaomi Smart Home εφαρμογής. Αφού κάνει εξαγωγή του πηγαίου κώδικα στη συνέχεια κάνει ανάλυση του δημιουργώντας μία αναφορά που αναλύεται παρακάτω.





2. Βήμα 2 – Ανάλυση κώδικα προγράμματος

Η διαδικασία ανάλυσης του πηγαίου κώδικα εφαρμογών σε κινητό τηλέφωνο έχει δύο στόχους:

a. να κατανοήσουν καλύτερα την αλληλεπίδραση των διαφόρων συσκευών ή εφαρμογών στο ιατρικό δίκτυο και
b. να εντοπίσουν σημεία ευπάθειας στην εφαρμογή.

Αυτή η διαδικασία είναι πολύ παρόμοια με αυτή που χρησιμοποιήθηκε στο βήμα 2 της προηγούμενης διαδικασίας. Όπως αναφέρθηκε παραπάνω, η χρήση του QARK συμβάλλει στην στατική ανάλυση του κώδικα για τον εντοπισμό ευπαθειών.

Πράγματι στην αναφορά καταγράφηκαν 6.929 ευπάθειες όπως παρουσιάζεται στον παρακάτω πίνακα. Δίπλα στη συχνότητα εμφάνισης της κάθε ευπάθειας καταγράφεται επίσης ο βαθμό σπουδαιότητας της εκάστοτε ευπάθειες. Παρατηρούμε ότι σε σύνολο 24 περιπτώσεων ευπαθειών, οι 15 είναι πολύ σημαντικές. Τυχόν εκμετάλλευση τους μπορεί να θέσουν σε κίνδυνο τη λειτουργία και διαχείριση των IoT συσκευών, και την διαρροή δεδομένων από το κινητό τηλέφωνο.

Ευπάθεια	**Αριθμός εμφανίσεων**	**Βαθμός σπουδαιότητας ευπάθειας**
Potential API Key found	3330	Μεσαία
Logging found	2534	Μεσαία
Hardcoded HTTP url found	764	Υψηλή
Insecure functions found	48	Υψηλή
Phone number or IMEI detected	44	Υψηλή
Exported tags	33	Χαμηλή
Potientially vulnerable check permission function called	29	Υψηλή
launchMode=singleTask found	27	Υψηλή
Javascript enabled in Webview	19	Υψηλή
Webview enables file access	18	Υψηλή
Webview enables content access	18	Υψηλή
External storage used	17	Υψηλή
Broadcast sent without receiverPermission	16	Υψηλή
Webview enables DOM Storage	9	Υψηλή
Random number generator is seeded with SecureSeed	5	Χαμηλή
Empty certificate method	5	Υψηλή
Ordered broadcast sent with receiverPermission with minimum SDK under 21	3	Υψηλή
BaseURL set for Webview	2	Μεσαία
Custom permissions are enabled in the manifest	2	Μεσαία
Protected Exported Tags	2	Μεσαία
Broadcast sent with receiverPermission with minimum SDK under 21	1	Υψηλή
Exported Tag With Permission	1	Μεσαία
Backup is allowed in manifest	1	Μεσαία

android:allowTaskReparenting='true' found	1	Υψηλή

Πίνακας 4. 1. Ευπάθειες που καταγράφηκαν με το εργαλείο Qark στη mobile εφαρμογή

Η αναλυτική περιγραφή των ευπαθειών δίνεται στο αρχείο που επισυνάπτεται στο παράρτημα Α'.

4.6 Δ9 – Ευπάθεια σε web εφαρμογές

Οι web εφαρμογές εξακολουθούν να υπάρχουν σε ορισμένες συσκευές IoT. Και σε αυτές μπορούν να εντοπιστούν ευπάθειες με τα ίδια εργαλεία που χρησιμοποιούνται για κοινούς ιστότοπους ή εφαρμογές ιστού. IoT εφαρμογές ιστού που εκτίθενται στο διαδίκτυο αποτελούν σοβαρή απειλή για το υπόλοιπο μέρος του δικτύου όταν δεν είναι σωστά θωρακισμένες όσον αφορά την ασφάλεια τους. Για παράδειγμα, μία από τις μεγαλύτερες απειλές για την ασφάλεια του έξυπνου δικτύου στο σπίτι είναι οι αυτοματοποιημένες επιθέσεις. Σε αυτή τη περίπτωση, μπορούμε να χρησιμοποιήσουμε ένα από αυτά τα εργαλεία αυτόματης σάρωσης για να εντοπίσουμε ορισμένες από τις ευπάθειες των web εφαρμογών όπως το OWASP ZAP[12].

Καθώς ο αισθητήρας θερμοκρασίας περιβάλλοντος δεν διαθέτει web εφαρμογή, η χρήση του παραπάνω εργαλείου κρίθηκε μη απαραίτητη.

Κεφάλαιο 5
Τρόποι αντιμετώπισης απειλών

Στον τομέα της Υγείας, το Διαδίκτυο των Πραγμάτων θα πρέπει να είναι σε θέσει να αντιμετωπίσει τις απειλές και τις ευπάθειες που περιέχουν οι συσκευές του έξυπνου Νοσοκομείου. Οι τρόποι αντιμετώπισης αναφέρονται παρακάτω:

- Αλλαγή Κωδικών Πρόσβασης: Οι χρήστες οφείλουν να αποσυνδέονται κάθε φορά από τις εφαρμογές καθώς υπάρχει κίνδυνος να εντοπιστούν ευπάθειες. Επίσης, η τακτική αλλαγή των κωδικών πρόσβασης θα μπορούσε να προστατεύσει τους χρήστες από πιθανές επιθέσεις.
- Έλεγχος Πρόσβασης: Θα πρέπει να εφαρμόζεται σωστά ο περιορισμός σε ό,τι επιτρέπεται να κάνουν οι χρήστες με έλεγχο ταυτότητας. Με τον τρόπο αυτό, οι κακόβουλοι χρήστες δε θα μπορούν να εκμεταλλευτούν αυτές τις λεπτομέρειες για να αποκτήσουν πρόσβαση σε εξουσιοδοτημένες λειτουργίες, να αποκτήσουν πρόσβαση σε λογαριασμούς άλλων χρηστών, να προβάλλουν ευαίσθητα αρχεία, να τροποποιήσουν τα δεδομένα άλλων χρηστών, να αλλάξουν δικαιώματα πρόσβασης ή των κωδικό πρόσβασης των χρηστών.
- Κρυπτογράφηση: Τα ευαίσθητα δεδομένα από τις εφαρμογές ιστού (web applications) και APIs (applications programming interface) θα πρέπει να έχουν ασφάλεια ειδική, να υπάρχει κάποιος αλγόριθμος κρυπτογράφησης, με αποτέλεσμα να τηρείται η ακεραιότητα των αρχείων και η ιδιωτικότητα που αποτελούν σημαντικές πτυχές για την ασφάλεια του διαδικτύου των πραγμάτων.

Όπως είδαμε και στο προηγούμενο κεφάλαιο οι ευπάθειες που είναι πιθανότερο να αξιοποιηθούν μέσω επιθέσεων σε ένα IoT δίκτυο είναι οι εξής:

- μη πραγματοποίηση επαρκών ενημερώσεων ασφαλείας

- μη ασφαλής διαδικασία ταυτοποίησης κατά την πρόσβαση σε web και mobile εφαρμογές διαχείρισης του IoT εξοπλισμού

- άλλες ευπάθειες στον κώδικα των web και mobile εφαρμογών

- έκθεση μη ασφαλών υπηρεσιών στο διαδίκτυο

- μη ασφαλείς δικτυακές επικοινωνίες

Η προτεινόμενη μεθοδολογία και το παράδειγμα του μικρού ιατρικού IoT δικτύου (ΕΙΠ) ανέδειξαν με απλό τρόπο τα διάφορα προβλήματα προκειμένου οι ιδέες πίσω από αυτή τη μεθοδολογία να γίνουνε κατανοητές. Καθώς βρισκόμαστε στο ξεκίνημα της εποχής της IoT τεχνολογίας και οι κατασκευαστές εξακολουθούν να συζητούν για το πρότυπο τυποποίησης των αρχιτεκτονικών και τεχνολογιών, δεν υπάρχει μία καθολική μεθοδολογία για τον εντοπισμό ευπαθειών σε IoT συστήματα.

Παρόλα αυτά, αν οι σχεδιαστές τέτοιων συστημάτων έχουν μια γενική αντίληψη των ιδεών, των προκλήσεων, των σημερινών αρχιτεκτονικών, όπως και των απειλών, ή ευπαθειών που έχουν να αντιμετωπίσουν, τότε η προτεινόμενη μέθοδος καθίσταται ευκολότερη στην εφαρμογή της. Μπορεί να προσαρμόζεται στις διαφορετικές και μελλοντικές έξυπνες υπηρεσίες που θα αναπτύσσονται στο πλαίσιο ενός έξυπνου νοσοκομείου. Κατόπιν χρειάζονται μία σειρά από μέτρα που καλούνται να υλοποιήσουν για να αυξήσουν το επίπεδο ασφάλειας (εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας) στο οικοσύστημα έξυπνων συσκευών του νοσοκομείου. Τα μέτρα αυτά προτείνονται παρακάτω.

5.1 Διακομιστές μεσολάβησης

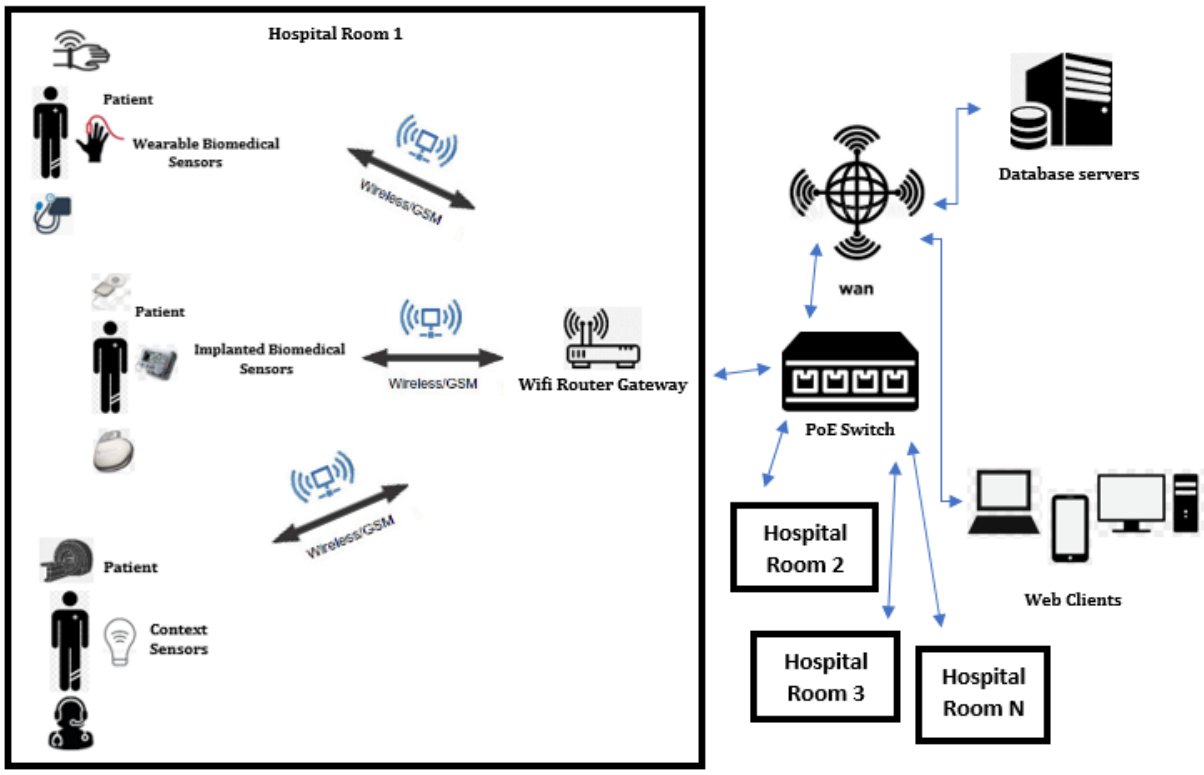
Στην παραπάνω διαδικασία ανίχνευσης ευπαθειών εντοπίστηκε μία σημαντική ευπάθεια όσον αφορά την έλλειψη μηχανισμού ταυτοποίησης κατά την πρόσβαση στη διεπαφή (API) της IoT συσκευής. Το πρόβλημα αυτό έχει αναφερθεί σε διάφορες τεχνολογίες IoT και αναμφισβήτητα αποκτά μεγαλύτερη βαρύτητα εφόσον τέτοιες συσκευές διακινούν ιατρικά δεδομένα [15].

Η μη ύπαρξη κοινών στρατηγικών και προτύπων για τον έλεγχο του σχεδιασμού και της εκτέλεσης αλγορίθμων στο Διαδίκτυο των Πραγμάτων, καθιστά δύσκολο τον έλεγχο της ασφάλειας. Είναι σημαντικό για τον τομέα του IoT να έχει μια νέα αρχιτεκτονική που να

υποστηρίζει μεν την εσωτερική αυτονομία των συσκευών αλλά να υπάρχει δε μια κεντρική μονάδα που να βοηθά να αντιμετωπιστεί η όποια ετερογένεια διαφόρων συσκευών, λογισμικών και πρωτοκόλλων.

Στον ερευνητικό χώρο προτείνεται μία τέτοια αρχιτεκτονική που ονομάζεται Secure Mediation GateWay (SMGW). Η χρήση ενδιάμεσων πυλών μπορεί πλέον να υποστηρίξει κάθε είδους κατανεμημένες υποδομές που είναι εντελώς ετερογενείς ως προς τη φύση και τη λειτουργία τους (πχ μπορεί να περιλαμβάνουν τηλεπικοινωνιακούς, ηλεκτρικούς, ιατρικούς κόμβους, κλπ) [22]. Η έρευνα σε αυτή τη κατεύθυνση επιβεβαιώνει την δική μας προτεινόμενη αρχιτεκτονική ως προς την χρήση έξυπνων ιατρικών πυλών στο κεφάλαιο 3.

Πράγματι, στην αρχιτεκτονική του συστήματος ενός έξυπνου νοσοκομείου θα πρέπει να ενσωματωθούν έξυπνες πύλες (gateways). Καμία επικοινωνία προς και από τους συνδεμένους IoT τερματικούς κόμβους δεν θα πρέπει να γίνεται χωρίς τη διαμεσολάβηση της συγκεκριμένης πύλης. Η πύλη επίσης ελέγχει αν η εφαρμογή ή η υπηρεσία (ή χρήστης) έχει ταυτοποιηθεί πριν αποκτήσει πρόσβαση (και με ποια δικαιώματα). Ένα τέτοιο παράδειγμα δίνεται στην παρακάτω εικόνα.



Εικόνα 5.1. Αρχιτεκτονική ενός Συστήματος Παρακολούθησης Για Εφαρμογές Υγειονομικής περίθαλψης που βασίζεται σε IoT και Έξυπνες Πύλες διαχείρισης των παρεχόμενων υπηρεσιών [21]

Σε ένα τέτοιο σύστημα, οι πληροφορίες που σχετίζονται με την υγεία του ασθενή καταγράφονται με αισθητήρες, είτε είναι φορητοί ή εμφυτευμένοι στο σώμα του ασθενούς. Έτσι εξασφαλίζεται η παρακολούθηση πολλαπλών παραμέτρων για την υγεία του είτε στην κλινική ή στο σπίτι του. Αυτά τα δεδομένα υγείας μπορούν να επεκταθούν με επιπλέον πληροφορίες (π.χ. ημερομηνία, ώρα, τοποθεσία και θερμοκρασία) που επιτρέπει τον εντοπισμό ασυνήθιστων διακυμάνσεων όσον αφορά την υγεία του. οι αισθητήρες συνδέονται με την πύλη που λαμβάνει τα δεδομένα και προωθεί σχετικές πληροφορίες σε διακομιστή, βάση δεδομένων ή απευθείας σε πελάτη Ιστού.

Εκτός από την απομακρυσμένη παρακολούθηση ασθενών, ένα έξυπνο σύστημα οικοδόμησης είναι ενσωματωμένο που αποτελείται από κόμβους IoT που χρησιμοποιούνται για αυτοματισμό κτιρίων. Αυτά περιλαμβάνουν τον παραδοσιακό φωτισμό, τη δημόσια διεύθυνση, τον έλεγχο πρόσβασης, καθώς και συσκευές ασύρματες φορητές ή εμφυτεύσιμες (συγκεκριμένα χειριστήρια δίπλα στο κρεβάτι) και συσκευές αισθητήρες περιβάλλοντος όπως ο εξοπλισμός κλήσης νοσοκόμας, το έξυπνο ρολόι και η έξυπνη λάμπα. Το οραματιζόμενο σύστημα είναι ενεργειακά αποδοτικό αξιοποιώντας τις δυνατότητες PoE της πύλης, η οποία επιτρέπει την άμεση ενεργοποίηση ενεργοποιητών και αισθητήρων χωρίς να επαναλαμβάνεται σε διαφορετικό δίκτυο τροφοδοσίας ή πρίζες AC. Το πίσω μέρος του συστήματος αποτελείται από τα δύο υπόλοιπα στοιχεία, τον διακόπτη με δυνατότητα PoE και μια πλατφόρμα cloud computing που περιλαμβάνει εκπομπές, αποθήκες δεδομένων και διακομιστές ανάλυσης Big Data, και πελάτες στο Web ως γραφικό περιβάλλον εργασίας χρήστη για τελική οπτικοποίηση. [21].

Σε μία τέτοια αρχιτεκτονική η αξιοπιστία της πληροφορίας που διακινείται από το δίκτυο των ιατρικών (IoT) αισθητήρων είναι πολύ σημαντική καθώς τα βιο-ιατρικά και τα συναφή σήματα συλλαμβάνονται από το σώμα του ασθενούς ή το δωμάτιο και πρέπει να μεταδοθούν για την έγκαιρη διάγνωση της ιατρικής κατάστασης και την υποστήριξη της όποιας θεραπείας. Οι ιατρικοί αισθητήρες συλλαμβάνουν σήματα από το σώμα που χρησιμοποιείται για τη θεραπεία και τη διάγνωση μιας ιατρικής κατάστασης. Παραδείγματα είναι τα σήματα ECG, EMG και EEG για την ανάλυση της καρδιάς, των μυών και των εγκεφαλικών καταστάσεων. Οι συσκευές αυτές μπορεί να είναι αισθητήρας πίεσης αίματος, αισθητήρας οξυγόνου. Το σήμα θα πρέπει να μεταδίδεται στην πύλη μέσω ασύρματων ή ενσύρματων πρωτοκόλλων επικοινωνίας (πχ όπως Serial, SPI, Bluetooth, Wi-Fi ή IEEE 802.15.4). Τα δεδομένα θα πρέπει να μεταδοθούν στη βασική πληροφοριακή υποδομή ή κάποια υποδομή στο υπολογιστικό νέφος που περιλαμβάνει βάσεις δεδομένων και εξυπηρετητές ανάκτησης και ανάλυσης δεδομένων [22].

Καθώς οι διαφορετικές κατασκευαστές των IoT τεχνολογιών δεν έχουν καταλήξει σε ένα κοινό πρωτόκολλο ταυτοποίησης /πιστοποίησης για τη πρόσβαση στα δεδομένα που παράγονται, θα πρέπει αυτό να γίνεται κεντρικοποιημένα από την ενδιάμεση πύλη. Έτσι θα εξασφαλίζεται η ασφαλή μετάδοση τους στις απομακρυσμένες βάσεις δεδομένων όπου διατρέχουν ήδη συγκεκριμένες διαδικασίας αναγνώρισης του χρήστη που έχει πρόσβαση σε διαβαθμισμένα δεδομένα του ασθενή (π.χ. ταυτότητα ή τύπο αίματος, DNA, ιστορικό, δημόσια δεδομένα χρήσιμα για στατιστική και επιδημιολογική ιατρική έρευνα).

Η αρχιτεκτονική θα πρέπει να λαμβάνει υπόψη της την ύπαρξη κατανεμημένων έξυπνων πυλών, για παράδειγμα με βάση ένα ορισμένο αριθμό IoT συσκευών ανά πύλη ή ανά τοποθεσία. Αυτό διασφαλίζει την πραγματοποίηση ελέγχου ταυτότητας και εξουσιοδότησης τοπικών και απομακρυσμένων τελικών χρηστών για την πρόσβαση τους στους διάφορους αισθητήρες. Επιπλέον σε αυτή την αρχιτεκτονική, εάν ένας εισβολέας επιχειρήσει μία επίθεση τύπου Denial of Service (DoS) με σκοπό να θέσει σε κίνδυνο τη λειτουργία μίας πύλης και των δεδομένων που ενδεχομένως αποθηκεύει προσωρινά, η κατανεμημένη αρχιτεκτονική θα απομονώσει το πρόβλημα σε ένα μόνο κόμβο.

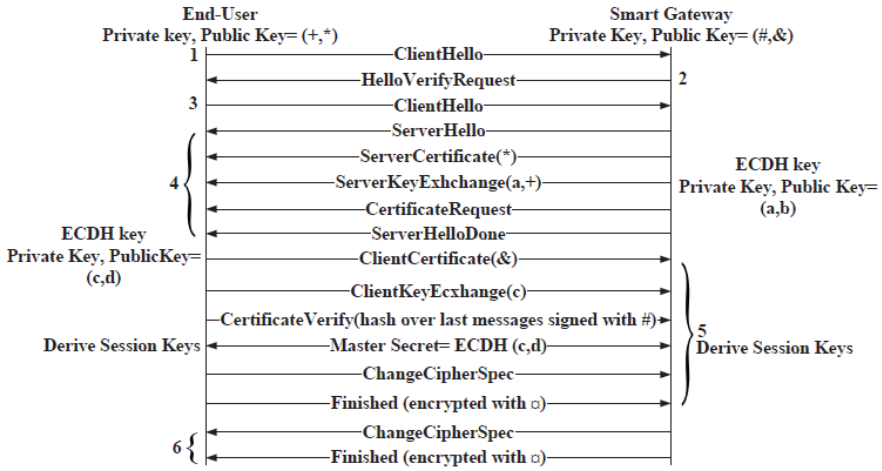
Η κύρια ευθύνη της έξυπνης πύλης είναι να μεσολαβήσει ανάμεσα στις IoT συσκευές και τον απομακρυσμένο τελικό χρήστη. Για την διαμόρφωση ενός ολοκληρωμένου πλαισίου ασφαλείας που να καλύπτει ακόμα και τα απομακρυσμένα σημεία ιατρικής παρακολούθησης, η έξυπνη πύλη πρέπει να ενεργεί για λογαριασμό όλων των ιατρικών (IoT) συσκευών. Δεδομένου ότι οι πύλες έχουν μια τοπική βάση δεδομένων, μπορούν να αποθηκεύουν προσωρινά τις πληροφορίες των ιατρικών αισθητήρων και να παρέχουν δυνατότητες επεξεργασίας και ανάκτησης των δεδομένων ως ένας ενσωματωμένος διακομιστής της εκάστοτε συσκευής.

Η πύλη περιέχει επίσης ένα Διακομιστή WebSocket για ροή δεδομένων απευθείας σε εφαρμογές ιστού ή για διασύνδεση με άλλους διακομιστές μετάδοσης. Η σύνδεση WebSocket βασίζεται σε TLS / SSL για την παροχή κρυπτογραφημένων, ασφαλών επικοινωνιών πελάτη και διακομιστή από άκρο σε άκρο. Η πύλη έχει σχεδιαστεί για να είναι χαμηλού κόστους, ώστε να αναπτύσσεται μαζικά κατά μήκος ενός νοσοκομείου (π.χ. μία πύλη σε κάθε δωμάτιο ή για κάθε κρεβάτι), έτσι ώστε οι ασύρματοι αισθητήρες χαμηλής ισχύος να ωφελούνται από τη μικρή περιοχή κάλυψης. Η πύλη λαμβάνει εντολές μέσω Διαδικτύου για την εκτέλεση διαφορετικών εργασιών, όπως έναρξη ροής δεδομένων αισθητήρων που περιλαμβάνουν επεξεργασία και μετάδοση μέσω της διεπαφής WebSocket.

5.2 Μηχανισμοί Εξουσιοδότησης

Το προτεινόμενο μοντέλο της χρήσης ενδιάμεσων διακομιστών εξασφαλίζει επιπλέον ότι μπορούν να χρησιμοποιηθούν διαθέσιμα πρωτόκολλα ασφάλειας για την διαδικασία πιστοποίησης και εξουσιοδότησης της πρόσβασης τοπικών και απομακρυσμένων χρηστών σε ιατρικό εξοπλισμό. Δεύτερον, παρέχει ένα βελτιωμένο επίπεδο ασφάλειας σε ιατρικές (IoT) συσκευές που έχουν περιορισμένους πόρους υλικού και λογισμικού για ασφαλή επικοινωνία με απομακρυσμένα κέντρα υγειονομικής περίθαλψης.

Για παράδειγμα, στο [21] προτείνεται η ταυτοποίηση ενός απομακρυσμένου χρήστη για την πρόσβαση του σε μία IoT συσκευή μέσω πρωτοκόλλου ασφαλείας που υλοποιεί η ενδιάμεση πύλη. Το πρωτόκολλο ασφαλείας βασίζεται στο Internet Protocol (IP), και ονομάζεται Datagram Transport Layer Security (DTLS). Όπως φαίνεται και στην παρακάτω εικόνα, επιτρέπει την αμοιβαία ανταλλαγή πιστοποιητικών (handshake). Η διαδικασία ξεκινά με ένα μήνυμα ClientHello, το οποίο περιλαμβάνει τις παραμέτρους ασφαλείας της σύνδεσης που χρησιμοποιούνται αργότερα κατά τη διάρκεια της χειραψίας για τον υπολογισμό του πρωτεύοντος μυστικού κλειδιού (master secret). Βάσει περαιτέρω διαπραγμάτευσης των υπολοίπων παραμέτρων, η πύλη κοινοποιεί το δημόσιο κλειδί στον χρήστη για τη συγκεκριμένη συνεδρία. [30]



Εικόνα 5.2. Αμοιβαία ανταλλαγή πιστοποιητικών μεταξύ τελικού χρήστη και έξυπνης πύλης βάσει πρωτοκόλλου DTLS [21]

5.3 Διαχείριση Ταυτότητας Χρηστών και Συσκευών

Η διαχείριση της ταυτότητας στο IoT δίκτυο πραγματοποιείται με ανταλλαγή πληροφοριών εντοπισμού των συσκευών τη πρώτη φορά της σύνδεσης τους στο δίκτυο. Όπως είδαμε στο προηγούμενο κεφάλαιο, αυτή η διαδικασία είναι ευάλωτη σε επιθέσεις τύπου Man-in-the-middle είτε απευθείας ή μέσω της mobile εφαρμογής διαχείρισης της. Μία τέτοια ευπάθεια μπορεί να απειλήσει ολόκληρη τη δομή του IoT δικτύου. Ως εκ τούτου, πρέπει να υπάρχει κάποια προκαθορισμένη οντότητα διαχείρισης της ταυτότητας των χρηστών και των συσκευών που να εποπτεύει την διαδικασία επικοινωνίας μεταξύ τους εφαρμόζοντας πρωτόκολλα ανταλλαγής κρυπτογραφημένων μηνυμάτων και άλλων τεχνικών για την πρόληψη της κλοπής ταυτότητας.

Ένας άλλος προτεινόμενος μηχανισμός περιλαμβάνει το Identity Authentication and Capability based Access Control (IACAC). Το πρωτόκολλο αυτό συνδυάζει ένα μηχανισμό ταυτοποίησης αλλά και ελέγχου πρόσβασης προκειμένου να διασφαλίζεται ο έλεγχος της ταυτότητας τόσο του χρήστη όσο και της IoT συσκευής. Υλοποιεί μία διαδικασία ταυτοποίησης βάσει δημόσιου κλειδιού και εξαλείφει τον κίνδυνο για επιθέσεις τύπου Man-in-the-Middle καθώς ενσωματώνει χρονοσήμανση στα μηνύματα ταυτοποίησης μεταξύ των μηνυμάτων. Η χρονοσήμανση χρησιμοποιείται ως ο κώδικας ελέγχου της ταυτότητας των μηνυμάτων [21] , [30].

Το πρωτόκολλο λειτουργεί σε τρία στάδια.

1. δημιουργείται ένα μυστικό κλειδί με βάση τον Elliptical Curve Cryptography-Diffie Hellman αλγόριθμο (ECCDH)

2. δημιουργείται ένα κωδικοποιημένο αναγνωριστικό με βάση πρωτόκολλα κρυπτογράφησης μονής κατεύθυνσης και αμοιβαίας πιστοποίησης και,

3. υλοποιείται έλεγχος πρόσβασης.

Το κοινόχρηστο μυστικό κλειδί αρχικοποιείται από τον συνδυασμό ενός δημόσιου κλειδιού και ενός μυστικού κωδικού. Μετά την ταυτοποίηση του χρήστη, ενεργοποιείται ο μηχανισμός ελέγχου των δικαιωμάτων πρόσβασης σε κάθε συσκευή. Το επίπεδο πρόσβασης είναι ένας τυχαίος αριθμός που περιλαμβάνει το αναγνωριστικό της συσκευής και τα δικαιώματα πρόσβασης και εκχωρείται στα δικαιώματα πρόσβασης του συγκεκριμένου χρήστη. Το IACAC πρωτόκολλο δεν εμποδίζει αποτελεσματικά επιθέσεις τύπου Denial-of-Service (DoS), μπορεί όμως να τις εξαλείφει.

5.4 Επίπεδο συνεδριών (Session layer)

Σύμφωνα με τους περισσότερους ερευνητές, η αρχιτεκτονική τριών επιπέδων του IoT δεν περιλαμβάνει το άνοιγμα, το κλείσιμο και τη διοργάνωση μιας συνεδρίας ανάμεσα σε δύο συσκευές. Επομένως, υπάρχει ανάγκη για νέους μηχανισμούς που μπορούν να αντιμετωπίσουν αυτά τα προβλήματα και μπορούν να απλοποιήσουν την αλληλεπίδραση μεταξύ των συσκευών. Ένα αφηρημένο επίπεδο συνεδριών θα πρέπει να περιέχει ένα πρόσθετο επίπεδο στην αρχιτεκτονική του διαδικτύου, το οποίο μπορεί να καθορίσει συγκεκριμένα τις συνδέσεις, τις υποχρεώσεις και τις συνεδρίες επικοινωνίας μεταξύ διαφορετικών συσκευών [24].

5.5 Ενημέρωση των χρηστών

Ένα άλλο σημαντικό μέτρο για την ασφάλεια και την εύρυθμη λειτουργία της IoT υποδομής στον ιατρικό χώρο είναι η ευαισθητοποίηση και η εγρήγορση του ιατρικού προσωπικού, καθώς είναι οι βασικοί χρήστες του IoT εξοπλισμού. Η πρόσβαση σε IoT συσκευές χωρίς κωδικό πρόσβασης ή με ένα κοινό κωδικό και γνωστό από τις εργοστασιακές ρυθμίσεις της συσκευής είναι ορισμένες απειλές που διευκολύνουν ακόμη περισσότερο τους κακόβουλους χρήστες [23].

Κεφάλαιο 6
Συμπεράσματα

Στη σύγχρονη ψηφιακή εποχή, το Διαδίκτυο των Πραγμάτων αποτελεί ένα νέο στάδιο της ψηφιακής επανάστασης που συμβάλει στην επέκταση της Κοινωνίας της Πληροφορίας και της Γνώσης. Πολλοί τομείς της Κοινωνίας, της Πληροφορίας και της Γνώσης χρησιμοποιούν ή θα χρησιμοποιήσουν το Διαδίκτυο των Πραγμάτων για τη βελτίωση υφιστάμενων διαδικασιών ή τη διαμόρφωση νέων και καινοτόμων υπηρεσιών (έξυπνο σπίτι, έξυπνο νοσοκομείο, έξυπνα αυτοκίνητα, έξυπνες πόλεις, έξυπνη βιομηχανία, ενέργεια, υγεία). Η ευρεία χρήση συσκευών στο Διαδίκτυο των Πραγμάτων έχει διαδραματίσει σημαντικό ρόλο στην καθημερινή ζωή των ατόμων και εγγυάται την βελτίωση πολλών μορφών των ψηφιακών εφαρμογών.

Το πλαίσιο ανάπτυξης και λειτουργίας των IoT τεχνολογιών, και ιδιαίτερα στον ιατρικό τομέα, είναι ευαίσθητο σε επιθέσεις σε κάθε επίπεδο της αρχιτεκτονικής τους. Ως εκ τούτου, υπάρχουν πολλές απειλές ασφάλειας και απαιτήσεις που πρέπει να αντιμετωπιστούν στο μέλλον. Η τρέχουσα ερευνητική δραστηριότητα στο πεδίο των IoT τεχνολογιών επικεντρώνεται κυρίως στα πρωτόκολλα ελέγχου ταυτότητας και πρόσβασης. Ωστόσο με τη ταχεία ανάπτυξη της τεχνολογίας είναι απαραίτητο να εδραιωθούν νέα πρωτόκολλα δικτύωσης όπως το IPv6 και το 5G για να επιτευχθεί η επέκταση της τοπολογίας του Διαδικτύου αλλά και η αξιοποίηση μηχανισμών ασφάλειας στα πιο κάτω επίπεδα.

Πράγματι θα πρέπει να αντιμετωπιστούν σημαντικά ζητήματα στο επίπεδο της ασφάλειας αν επιζητείται η μεταμόρφωση των ιατρικών υποδομών σε έξυπνα και ευέλικτα ιατρικά οικοσυστήματα. Αν βελτιωθούν τα πρωτόκολλα και οι αλγόριθμοι προστασίας των δεδομένων, η εμπιστευτικότητα, η πιστοποίηση ταυτότητας, η πρόσβαση, ο έλεγχος, η ασφάλεια από άκρο σε άκρο, η διαχείριση εμπιστοσύνης, υπάρχουν κοινές πολιτικές και πρότυπα, οι IoT τεχνολογίες θα μπορούν να μετασχηματίσουν το έξυπνο νοσοκομείο στο εγγύς μέλλον.

Όπως ανέδειξε η προτεινόμενη μεθοδολογία εντοπισμού απειλών σε ένα IoT δίκτυο, υπάρχει ανάγκη για νέα πρωτόκολλα ταυτοποίησης, δημιουργίας αναγνωριστικών για την πρόσβαση σε

ιατρικά δεδομένα μέσω αυτών των συσκευών. Οι ασύρματες τεχνολογίες σε επίπεδο λογισμικού και υλικού θα πρέπει να εξελιχθούν για να επιλύσουν τις ανοικτές σε ερευνητικό επίπεδο απειλές όπως τα ετερογενή πρότυπα για διαφορετικές συσκευές, την εφαρμογή κλειδιών διαχείρισης και δημιουργίας ταυτότητας, καθώς και ενσωμάτωση κόμβων διαχείρισης εμπιστοσύνης.

Από την βιβλιογραφική έρευνα, καθώς και τα συμπεράσματα των σεναρίων επίθεσης που πραγματοποιήθηκαν, η παρούσα διατριβή προτείνει βασικές προτάσεις για την ενίσχυση της ασφάλειας των έξυπνων νοσοκομείων. Τα νοσοκομεία πρέπει να:

- δημιουργήσουν ένα αποτελεσματικό πλαίσιο εταιρικής διακυβέρνησης για την ασφάλεια στον κυβερνοχώρο
- εφαρμόσουν μέτρα ασφάλειας με βάση τις πιο πρόσφατες τεχνολογίες
- παρέχουν συγκεκριμένες απαιτήσεις ασφάλειας των πληροφοριών για τον IoT εξοπλισμό του νοσοκομείου
- επενδύσουν σε τεχνολογίες ανάλυσης δεδομένων (πακέτων) σε επίπεδο δικτύου
- δημιουργήσουν έναν μηχανισμό κοινής ασφάλειας πληροφοριών μεταξύ των νοσοκομείων
- διεξάγουν εκτιμήσεις κινδύνου και αξιολογήσεις ευπάθειας
- εκτελέσουν δοκιμές διείσδυσης και ελέγχους
- να υποστηρίζουν το άνοιγμα διαύλων · Υποστήριξη πλατφορμών επικοινωνίας με πολλούς φορείς (ISACs)

Από την άλλη πλευρά οι κατασκευαστές θα πρέπει να κάνουν ενέργειες από τη πλευρά τους για να ενισχύσουν το επίπεδο της ασφάλειας πληροφοριών στα έξυπνα νοσοκομεία. Οι κατασκευαστές ή πάροχοι υπηρεσιών ασφάλειας θα πρέπει να:

1. ενσωματώσουν την ασφάλεια στα υπάρχοντα συστήματα διασφάλισης της ποιότητας

2. να βοηθήσουν τη συμμετοχή τρίτων (πχ οργανισμών υγειονομικής περίθαλψης) στις διαδικασίες δοκιμών

3. να εξετάσουν την εφαρμογή σχετικού νομοθετικού πλαισίου στη ρύθμισης των ιατρικών συσκευών ειδικά σε αυτές που λειτουργούν σε κρίσιμα τμήματα

4. να υποστηρίξουν την καθιέρωση προτύπων ασφάλειας πληροφοριών στην υγειονομική περίθαλψη

Στη δεύτερη περίπτωση, η εφαρμογή της προτεινόμενης μεθοδολογίας και εργαλείων σε ένα έξυπνο ιατρικό δίκτυο που περιλάμβανε μία έξυπνη λάμπα (Xiaomi Smart Bulb- Yeelight) οδήγησε με επιτυχία σε χρήσιμα συμπεράσματα:

1. Η παθητική (Δ3) καθώς και η ενεργή συλλογή δεδομένων (Δ4) με τη χρήση αντίστοιχων εργαλείων οδήγησε στην αποτύπωση πληροφοριών που αξιοποιήθηκαν στην ανάλυση της δικτυακής κίνησης και λειτουργίας της συσκευής σε πραγματικό χρόνο.

2. Εντοπίστηκε ευπάθεια σχετικά με την απομακρυσμένη πρόσβαση στη συσκευή λόγω έλλειψης ισχυρού μηχανισμού ταυτοποίησης πριν τη χρησιμοποίηση των υπηρεσιών της (Δ6).

3. Εντοπίστηκαν 6.930 ευπάθειες στον κώδικα της mobile εφαρμογής (Δ8) που ομαδοποιήθηκαν σε 24 κατηγορίες και 15 από αυτές ταξινομήθηκαν ως υψηλής σημασίας.

Σημειώνεται επίσης ότι δεν μπορέσαμε να αξιοποιήσουμε τα εργαλεία και τα αποτελέσματα των διαδικασιών ανάλυσης ευπαθειών στο πρόγραμμα υλικού (Δ7) και σε web εφαρμογές (Δ9). Ωστόσο η οι διαδικασίες και τα εργαλεία είναι διαθέσιμα για μελλοντική αξιοποίηση μέσω της προτεινόμενης μεθοδολογίας.

Αντίστοιχα οι προγραμματιστές των mobile και web εφαρμογών θα πρέπει να κάνουν χρήση των παραπάνω ευρημάτων για να διορθώσουν τις ευπάθειες στον κώδικα. Η αναφορά που δημιουργήθηκε από τη προτεινόμενη μεθοδολογία θα πρέπει να είναι διαθέσιμη κατόπιν στον κατασκευαστή προκειμένου να σχεδιάσει τις απαραίτητες διορθωτικές κινήσεις (patch management procedures– mitigation actions) στην εφαρμογή. Επαναλαμβάνοντας την εκτέλεση

της ανάλυσης του κώδικα – μετά τις διορθωτικές κινήσεις τους – θα μπορούν να επιβεβαιώσουν τη μείωση των ευπαθειών σε αυτόν.

Βιβλιογραφία

[1] Julio Mayol, Bjorn Kabisch. «Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures NOVEMBER 2016 Smart Hospitals About ENISA». European Union Agency For Network And Information Security, ISBN 978-92-9204-181-6, doi: 10.2824/28801, November 2016.

[2] Cho, J.-S., Yeo, S.-S., & Kim, S. Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value. Comput Commun, 391–397. 2011.

[3] Ilias Maglogiannis and Stathes Hadjiefthymiades. Pervasive Electronic Services in Health Care. Pervasive Information Systems. Chapter 8. Eds. Taylor Francis. 2016

[4] S. Pinto, J. Cabral and T. Gomes, "We-care: An IoT-based health care system for elderly people," 2017 IEEE International Conference on Industrial Technology (ICIT), Toronto, ON, 2017, pp. 1378-1383.

[5] Lauren Elizabeth Branch. Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective. Phd. West Virginia University, 2018.

[6] Kimberly A. Cook and Alexandra Block. Improving Health Care Cybersecurity. Risk Management (Vol. 64, Issue 11)

[7] Mohamed Shakeel, P., Baskar, S., Sarma Dhulipala, V.R. et al. Maintaining Security and Privacy in Health Care System Using Learning Based Deep-Q-Networks. J Med Syst 42, 186 (2018). https://doi.org/10.1007/s10916-018-1045-z

[8] J. Naveen Ananda Kumar and S. Suresh, "A Proposal of smart hospital management using hybrid Cloud, IoT, ML, and AI," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 1082-1085.

[9] Oksana Ilyashenko, Igor Ilin, Dmitry Kurapeev. Smart Hospital concept and its implementation capabilities based on the incentive extension. SHS Web of Conf. 44 00040 (2018).

[10] S.A. Hosseinpour, M.R. Delavar, H. Hasani Baferani. A WEB-BASED SMART TELECARE SYSTEM FOR EARLY DIAGNOSIS OF HEART ATTACK. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLII-4/W18, 2019 GeoSpatial Conference 2019 – Joint Conferences of SMPR and GI Research, 12–14 October 2019, Karaj, Iran

[11] Cáceres C., Rosário J.M., Amaya D. (2019) Proposal of a Smart Hospital Based on Internet of Things (IoT) Concept. In: Lepore N., Brieva J., Romero E., Racoceanu D., Joskowicz L. (eds) Processing and Analysis of Biomedical Information. SaMBa 2018. Lecture Notes in Computer Science, vol 11379. Springer, Cham

[12] H. Zhang, J. Li, B. Wen, Y. Xun and J. Liu, "Connecting Intelligent Things in Smart Hospitals Using NB-IoT," in IEEE INTERNET OF THINGS JOURNAL, vol. 5, no. 3, pp. 1550-1560, June 2018.

[13] Moro Visconti, Roberto and Martiniello, Laura, Smart Hospitals and Patient-Centered Governance (March 21, 2019). Moro Visconti, R., & Martiniello, L. (2019). Smart hospitals and patient-centered governance. Corporate Ownership & Control, 16(2).

[14] P. Luo, H. Chao and S. Wu, "Robustness of IoT Gateway Deployment in Smart Hospitals," 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 2019, pp. 1-6.

[15] George G., Thampi S.M. (2019) Securing Smart Healthcare Systems from Vulnerability Exploitation. In: Wang G., El Saddik A., Lai X., Martinez Perez G., Choo KK. (eds) Smart City and Informatization. iSCI 2019. Communications in Computer and Information Science, vol 1122. Springer, Singapore

[16] George, G., Thampi, S.M.: A graph-based security framework for securing industrial IoT networks from vulnerability exploitations. IEEE Access 6, 43586–43601 (2018)

[17] Simpson, A.K., Roesner, F., Kohno, T.: Securing vulnerable home IoT devices with an in-hub security manager. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 551–556. IEEE (2017)

[18] S. Safavi, A. M. Meer, E. Keneth Joel Melanie and Z. Shukur, "Cyber Vulnerabilities on Smart Healthcare, Review and Solutions," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-5.

[19] Sethuraman, S.C., Vijayakumar, V. & Walczak, S. Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. J Med Syst 44, 29 (2020). https://doi.org/10.1007/s10916-019-1489-9

[20] A. Djenna and D. Eddine Saïdouni, "Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure," 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018, pp. 1-4.

[21] S. R. Moosavi, T. N. Gia, Amir-Mohammad Rahmani, E. Nigussie, S. Virtanen , J. Isoaho, H. Tenhunen. SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. 6th International Conference on Ambient Systems, Networks and Technologies (ANT 2015). Procedia Computer Science 52 (2015) 452 – 459 . ScienceDirect.

[22] M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5, 86-97, 2012.

[23] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172, 2014.

[24] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

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

[26] Arias, O., Ly, K., & Jin, Y. (2017). Smart Sensors at the IoT Frontier. The Security and privacy in IoT era, 2017, pp. 351–378.

[27] Zhang, W., & Qu, B. (2013). Security architecture of the Internet of Things oriented to perceptual layer. Int J Comput, Consum Control (IJ3C), pp. 37-45).

[28] Amir M. Rahmani, Tuan Nguyen Gia, Behailu Negash, Arman Anzanpour, Iman Azimi, Mingzhe Jiang, Pasi Liljeberg, Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach, Future Generation Computer Systems, Volume 78, Part 2, 2018, Pages 641-658.

[29] Zhou, W., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. University of Chinese Academy of Sciences.

[30] Zeadally, Sherali & Das, Ashok Kumar & Sklavos, Nicolas. (2020). Cryptographic Technologies and Protocol Standards for Internet of Things, Internet of Things: Engineering Cyber Physical Human Systems, Elsevier Science Press.

[31] S.Theodorou & N.Sklavos. (2019). Blockchain Based Security & Privacy in Smart Cities, Chapter in the Book: Smart Cities Cybersecurity and Privacy, editors Danda B. Rawat, Kayhan Z. Ghafoor, Elsevier Press, ISBN: 9780128150320

[32] P.Spanaki & N. Sklavos. (2018). Cloud Computing: Security Issues and Establishing Virtual Cloud Environment via Vagrant to Secure Cloud Hosts, Chapter in the Book: Computer and Network Security Essentials, editor Kevin Daimi, Springer, ISBN: 978-3-319-58423-2

[33] E. Isa & N. Sklavos. (2017). Smart Home Automation: GSM Security System Design & Implementations, proceedings of the 3rd Pan-Hellinic Conference on Electronics and Telecommunications (PACET' 15), Ioannina, Greece, May 8-9, 2015, Selected Paper, journal of Engineering Science and Technology Review, Vol 10, Issue 3

[34] N. Sklavos & I. D. Zaharakis. (2016). Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations, proceedings of 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaca, Cyprus, November 21-23

[35] N. Sklavos & P. Souras. (2006). Economic Models and Approaches in Information Security for Computer Networks, International Journal of Networks Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January 2006, pp 14-20

Παράρτημα Α

Αναφορά Αποτελεσμάτων

<html>

<head><title>Temporary Report Template</title></head>

<body>

<h1>Issues</h1>

<h2>INFO Potential API Key found</h2>

Please confirm and investigate for potential API keys to determine severity.

File: <a
href="file:///home/kali/qark/build/qark/AndroidManifest.xml">/home/kali/qark/build/qark/
AndroidManifest.xml::

<h2>WARNING Logging found</h2>

Logs are detected. This may allow potential leakage of information from Android applications. Logs should never be compiled into an application except during development. Reference: https://developer.android.com/reference/android/util/Log.html

File: <a
href="file:///home/kali/qark/build/qark/procyon/com/xiaomi/youpin/common/util/Process
Utils.java">/home/kali/qark/build/qark/procyon/com/xiaomi/youpin/common/util/ProcessU
tils.java:54:17

<h2>WARNING Webview enables content access</h2>

While not a vulnerability by itself, it appears this app does not explicitly disable Content Provider access from WebViews. If the WebViews take in untrusted input, this can allow for data theft. To validate this vulnerability, load the following local file in this WebView: file://qark/poc/html/WV_CPA_WARNING.html

File: /home/kali/qark/build/qark/cfr/com/alipay/sdk/auth/c.java:29:13

<h2>WARNING Broadcast sent without receiverPermission</h2>

A broadcast, sendBroadcast which does not specify the receiverPermission. This means any application on the device can receive this broadcast. You should investigate this for potential data leakage.

File: /home/kali/qark/build/qark/fernflower/com/xiaomi/miot/support/monitor/MiotMonitorClient.java:97:59

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://push.buy.test.mi.com/, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/cfr/com/mi/global/shop/ShopApp.java:533:0

<h2>INFO Protected Exported Tags</h2>

The receiver com.xiaomi.jr.antifraud.por.MaskedPhoneNumHelper$SimStateReceive is exported, but the associated Intents can only be sent by SYSTEM level apps. They could still potentially be vulnerable, if the Intent carries data that is tainted (2nd order injection)

File: /home/kali/qark/build/qark/AndroidManifest.xml

<h2>INFO Exported Tag With Permission</h2>

The service com.xiaomi.assemble.control.COSPushMessageService tag is exported and protected by a permission, but the permission can be obtained by malicious apps installed prior to this one. More info: https://github.com/commonsguy/cwac-security/blob/master/PERMS.md. Failing to protect service tags could leave them vulnerable to attack by malicious apps. The service tags should be reviewed for vulnerabilities, such as injection and information leakage.

File: /home/kali/qark/build/qark/AndroidManifest.xml

<h2>WARNING Ordered broadcast sent with receiverPermission with minimum SDK under 21</h2>

A broadcast, sendOrderedBroadcast which specifies the receiverPermission, but may still be vulnerable to interception, due to the permission squatting vulnerability in API levels before 21. This means any application, installed prior to the expected receiver(s) on the device can potentially receive this broadcast. You should investigate this for potential data leakage.

File: /home/kali/qark/build/qark/fernflower/android/support/v4/content/pm/ShortcutManagerCompat.java:79:13

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://localhost/, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/cfr/retrofit2/Response.java:59:0

<h2>INFO Potential API Key found</h2>

Please confirm and investigate the API key to determine its severity.

File: /home/kali/qark/build/qark/lib/armeabi-v7a/libxmediaplayerv7.so:2954:0

<h2>WARNING Webview enables DOM Storage</h2>

DOM Storage enabled for this WebView, there is a potential for caching sensitive information.

File: /home/kali/qark/build/qark/cfr/com/alipay/sdk/widget/WebViewWindow.java:178:9

<h2>WARNING Insecure functions found</h2>

The Content provider API provides a method call. The framework does no permission checking on this entry into the content provider besides the basic ability for the application to get access to the provider at all. Any implementation of this method must do its own permission checks on incoming calls to make sure they are allowed. Failure to do so will allow unauthorized components to interact with the content provider. Reference: https://bitbucket.org/secure-it-i/android-app-vulnerability-benchmarks/src/d5305b9481df3502e60e98fa352d5f58e4a69044/ICC/WeakChecksOnDynamicInvocation-InformationExposure/?at=master

File: /home/kali/qark/build/qark/fernflower/com/alipay/zoloz/android/phone/mrpc/core/RpcCaller.java:4:4

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://ns.adobe.com/xap/1.0/sType/Version, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/procyon/com/adobe/xmp/XMPConst.java:37:0

<h2>WARNING Custom permissions are enabled in the manifest</h2>

This permission can be obtained by malicious apps installed prior to this one, without the proper signature. Applicable to Android Devices prior to L (Lollipop). More info: https://github.com/commonsguy/cwac-security/blob/master/PERMS.md

File: /home/kali/qark/build/qark/AndroidManifest.xml

<h2>WARNING launchMode=singleTask found</h2>

This results in AMS either resuming the earlier activity or loads it in a task with same affinity or the activity is started as a new task. This may result in Task Poisoning. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-ren-chuangang.pdf

File: /home/kali/qark/build/qark/AndroidManifest.xml::

<h2>WARNING Random number generator is seeded with SecureSeed</h2>

Specifying a fixed seed will cause a predictable sequence of numbers. This may be useful for testing, but not for secure use

File: /home/kali/qark/build/qark/cfr/cn/tongdun/android/core/q9qq99qg9qqgqg9gqgg9/gqg9qq9gqq9q9q.java

<h2>WARNING Logging found</h2>

Logs are detected. This may allow potential leakage of information from Android applications. Logs should never be compiled into an application except during development. Reference: https://developer.android.com/reference/android/util/Log.html

File: /home/kali/qark/build/qark/cfr/com/xiaomi/smarthome/framework/log/LogUtil.java:122:17

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://ns.adobe.com/xap/1.0/mm/, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/cfr/com/adobe/xmp/impl/XMPSchemaRegistryImpl.java:76:0

<h2>WARNING BaseURL set for Webview</h2>

This webView sets the BaseURL. You should verify that this is only loading content from this domain. Loading content from a domain you do not control, or using plain-text HTTP, leaves this vulnerable to injection attacks against the BaseURL domain.

File: /home/kali/qark/build/qark/procyon/bolts/WebViewAppLinkResolver.java:409:17

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://ns.adobe.com/photoshop/1.0/, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/cfr/com/adobe/xmp/impl/Utils.java:206:0

<h2>WARNING Logging found</h2>

Logs are detected. This may allow potential leakage of information from Android applications. Logs should never be compiled into an application except during development. Reference: https://developer.android.com/reference/android/util/Log.html

File: /home/kali/qark/build/qark/procyon/com/alipay/zoloz/a/b.java:24:13

<h2>WARNING Potientially vulnerable check permission function called</h2>

Be careful with use of Check permission function

App maybe vulnerable to Privilege escalation or Confused Deputy Attack. This function can grant access to malicious application, lacking the appropriate permission, by assuming your applications permissions. This means a malicious application, without appropriate permissions, can bypass its permission check by using your applicationpermission to get access to otherwise denied resources. Use - checkCallingPermission instead. Reference: https://developer.android.com/reference/android/content/Context.html

File: <a href="file:///home/kali/qark/build/qark/procyon/com/alipay/mobile/security/bio/utils/Per

missionHelper.java">/home/kali/qark/build/qark/procyon/com/alipay/mobile/security/bio/utils/PermissionHelper.java

<h2>INFO Potential API Key found</h2>

Please confirm and investigate the API key to determine its severity.

File: /home/kali/qark/build/qark/lib/armeabi-v7a/libDToken.so:4969:0

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://m.alipay.com/?action=h5quit, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/cfr/com/alipay/sdk/cons/a.java:23:0

<h2>WARNING Webview enables file access</h2>

File system access is enabled in this WebView. If untrusted data is used to specify the URL opened by this WebView, a malicious app or site may be able to read your app's private files, if it returns the response to them. To validate this vulnerability, load the following local file in this WebView: qark/poc/html/FILE_SYS_WARN.html

File: /home/kali/qark/build/qark/procyon/com/alipay/sdk/auth/c.java:22:19

<h2>WARNING Exported tags</h2>

The receiver com.xiaomi.smarthome.framework.account.MiAccountChangeReceiver is exported, but not protected by any permissions. Failing to protect receiver tags could leave them vulnerable

to attack by malicious apps. The receiver tags should be reviewed for vulnerabilities, such as injection and information leakage.

File: /home/kali/qark/build/qark/AndroidManifest.xml

<h2>WARNING Webview enables content access</h2>

While not a vulnerability by itself, it appears this app does not explicitly disable Content Provider access from WebViews. If the WebViews take in untrusted input, this can allow for data theft. To validate this vulnerability, load the following local file in this WebView: file://qark/poc/html/WV_CPA_WARNING.html

File: /home/kali/qark/build/qark/procyon/com/alipay/sdk/auth/c.java:22:19

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://139.224.138.243/gateway/identification/simulate/face/initialize, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/procyon/com/alipay/mobile/security/bio/workspace/Env.java:42:0

<h2>WARNING External storage used</h2>

Reading files stored on {storage_location} makes it vulnerable to data injection attacks. Note that this code does no error checking and there is no security enforced with these files. For example, any application holding WRITE_EXTERNAL_STORAGE can write to these files. Reference: https://developer.android.com/reference/android/content/Context.html

File: /home/kali/qark/build/qark/procyon/android/support/v4/content/FileProvider.java:155:54

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://ns.adobe.com/png/1.0/, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/cfr/com/adobe/xmp/impl/XMPSchemaRegistryImpl.java:159:0

<h2>INFO Potential API Key found</h2>

Please confirm and investigate the API key to determine its severity.

File: /home/kali/qark/build/qark/lib/armeabi-v7a/libxmediaplayerv7.so:545:0

<h2>WARNING launchMode=singleTask found</h2>

This results in AMS either resuming the earlier activity or loads it in a task with same affinity or the activity is started as a new task. This may result in Task Poisoning. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-ren-chuangang.pdf

File: /home/kali/qark/build/qark/AndroidManifest.xml::

<h2>WARNING Insecure functions found</h2>

The Content provider API provides a method call. The framework does no permission checking on this entry into the content provider besides the basic ability for the application to get access to the provider at all. Any implementation of this method must do its own permission checks on incoming calls to make sure they are allowed. Failure to do so will allow unauthorized components to interact with the content provider. Reference: https://bitbucket.org/secure-it-i/android-app-vulnerability-benchmarks/src/d5305b9481df3502e60e98fa352d5f58e4a69044/ICC/WeakChecksOnDynamicInvocation-InformationExposure/?at=master

<h2>INFO Phone number or IMEI detected</h2>

Access of phone number or IMEI, is detected. Avoid storing or transmitting this data.

File: /home/kali/qark/build/qark/fernflower/com/alipay/deviceid/module/x/class_605.java

<h2>WARNING Backup is allowed in manifest</h2>

Backups enabled: Potential for data theft via local attacks via adb backup, if the device has USB debugging enabled (not common). More info: http://developer.android.com/reference/android/R.attr.html#allowBackup

File: /home/kali/qark/build/qark/AndroidManifest.xml

<h2>WARNING Empty certificate method</h2>

Instance of checkServerTrusted, with empty body found. This means this application is likely vulnerable to Man-In-The-Middle attacks. This can be confirmed using the free version of Burpsuite. Simply set the Android device's proxy to use Burpsuite via the network settings, but DO NOT install the Portswigger CA certificate on the device. If you still see traffic in the proxy, the app

is vulnerable. Note: You need to ensure you exercise this code path. If you are unsure, make sure you click through each part of the application which makes network requests. You may need to toggle the proxy on/off to get past sections that do validate certificates properly in order to reach the vulnerable code. This proves that it will accept certificates from any CA. You should always validate your configuration by visiting an HTTPS site in the native browser and verifying you receive a certificate warning. For details, please see: https://developer.android.com/training/articles/security-ssl.html

File: /home/kali/qark/build/qark/cfr/cn/tongdun/android/core/g9q9q9g9/q9qq99qg9qqgqg9gqgg9.java:25:12

<h2>INFO Hardcoded HTTP url found</h2>

Application contains hardcoded HTTP url: http://ns.adobe.com/xap/1.0/sType/ManifestItem, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.

File: /home/kali/qark/build/qark/cfr/com/adobe/xmp/XMPConst.java:41:0

<h2>WARNING Webview enables file access</h2>

File system access is enabled in this WebView. If untrusted data is used to specify the URL opened by this WebView, a malicious app or site may be able to read your app's private files, if it returns the response to them. To validate this vulnerability, load the following local file in this WebView: qark/poc/html/FILE_SYS_WARN.html

File: /home/kali/qark/build/qark/fernflower/com/xiaomi/jr/web/webkit/XiaomiWebLoginProcessor.java:31:7

<h2>WARNING android:allowTaskReparenting='true' found</h2>

This allows an existing activity to be reparented to a new native task i.e task having the same affinity as the activity. This may lead to UI spoofing attack on this application.https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-ren-chuangang.pdf

File: /home/kali/qark/build/qark/AndroidManifest.xml::

<h2>WARNING Javascript enabled in Webview</h2>

While not a vulnerability by itself, it appears this app has JavaScript enabled in the WebView: If this is not expressly necessary, you should disable it, to prevent the possibility of XSS (cross-site scripting) attacks. More info: http://developer.android.com/guide/practices/security.html To validate this vulnerability, load the following local file in this WebView: qark/poc/html/JS_WARNING.html

</body>

</html>