Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Απεικόνιση και Προτεραιοποίηση Επικινδυνοτήτων Ψηφιακής Υγείας (eHealth) Σχετικά με την Ασφάλεια των Ασθενών

Ελευθέριος Ελευθεριάδης

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

Μάιος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Απεικόνιση και Προτεραιοποίηση Επικινδυνοτήτων Ψηφιακής Υγείας (eHealth) Σχετικά με την Ασφάλεια των Ασθενών

Ελευθέριος Ελευθεριάδης

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

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 2023

Περίληψη

Η ψηφιακή υγεία (eHealth) αφορά σε ένα διαρκώς αυξανόμενο εύρος ιατρικών υπηρεσιών. Βασίζεται και ενισχύεται από τις ραγδαίες τεχνολογικές εξελίξεις στο πλαίσιο των τηλεπικοινωνιών και της πληροφορικής, καθιστώντας δυνατή την αποκεντρωμένη υλοποίηση παροχής ιατρικών υπηρεσιών. Η επέκταση αυτή συνεπάγεται όμως και την επέκταση της επιφάνειας επίθεσης σε υπηρεσίες και συστήματα τα οποία ενδέχεται να συνδέονται πλέον άμεσα με την φυσική ασφάλεια των ασθενών. Παρά την κρισιμότητα των επιπτώσεων από ενδεχόμενες κυβερνοεπιθέσεις στην υγεία των ασθενών στο πλαίσιο της ψηφιακής υγείας, δεν υπάρχει κάποιο ευρέως υιοθετημένο πλαίσιο για την αναγνώριση και την διαχείριση των σχετικών απειλών και επιπτώσεων στην υγεία των ασθενών.

Η παρούσα μεταπτυχιακή διατριβή αποσκοπεί στην ανάπτυξη ενός πλαισίου για την οργανωμένη απεικόνιση και προτεραιοποίηση των επικινδυνοτήτων που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας σχετικά με την ασφάλεια των ασθενών, επιδοτώντας έτσι την αποτελεσματική διαχείρισή τους.

Αφού μελετήθηκε η σχετική βιβλιογραφία, εντοπίστηκαν οι σχετικές κωδικοποιήσεις των ενδεχόμενων κυβερνοεπιθέσεων που απαντώνται στο πλαίσιο της ψηφιακής υγείας και συσχετίστηκαν με ζητήματα προστασίας της υγείας και της ζωής των ασθενών που θα μπορούσαν να προκληθούν από αυτές. Εν συνεχεία προχωρήσαμε σε αξιοποίηση των σχετικών προτύπων και πρακτικών για την ανάπτυξη ενός πλαισίου για την οργανωμένη απεικόνιση και προτεραιοποίηση των επικινδυνοτήτων που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας σχετικά με την ασφάλεια των ασθενών, όπως επίσης και της σχετικής εφαρμογής για την υλοποίησή του, η οποία και λειτουργεί στο πλαίσιο μιας προσέγγισης αυτοματοποιημένου υπολογισμού επικινδυνότητας.

Τέλος, παρουσιάζεται και σχολιάζεται η λειτουργικότητα της εφαρμογής στο πλαίσιο ενός ενδεικτικού υπολογιστικού συστήματος, για το οποίο και υπολογίζεται τόσο η επιμέρους τιμή για το εκάστοτε συστατικό όσο και η συνολική τιμή επικινδυνότητας, εξαρτώμενη πάντα από τον βαθμό εξάρτησης μεταξύ ψηφιακής υποδομής και πτυχών ασφάλειας που ορίζει ο χρήστης.

Summary

Digital health (eHealth) refers to an ever-increasing range of medical services. It is based on and enhanced by rapid technological developments in telecommunications and information technology, thus enabling the decentralized delivery of medical services. Such an expansion however also implies an expansion of the attack surface of systems and services that may now be directly linked to the physical safety of patients. Despite the criticality of the impact of potential cyberattacks on patient health in the context of digital health, there is no widely adopted framework for identifying and managing the associated threats and impacts on patient health.

This Master's thesis aims to develop a framework for the organized visualization and prioritization of the risks that characterize digital health systems linked to patient safety, thereby promoting their effective management.

After reviewing the relevant literature, the relevant codifications of potential cyberattacks encountered in the context of digital health were identified and correlated with issues related to the protection of patients' health and lives that could be caused by them. We then proceeded to leverage relevant standards and practices to develop a framework for the organized mapping and prioritisation of the patient safety-related risks that characterize digital health systems, as well as the associated application for its implementation, which operates in the context of an automated risk calculation approach.

Finally, the functionality of the application is presented and commented on in the context of an illustrative computing system, for which both the individual value for each component and the overall risk value are calculated, always depending on the degree of dependency between digital infrastructure and user-defined security aspects.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

1.1. Κίνητρο έρευνας

Η ψηφιακή υγεία (eHealth) αφορά σε ένα διαρκώς αυξανόμενο εύρος ιατρικών υπηρεσιών. Βασίζεται και ενισχύεται από τις ραγδαίες τεχνολογικές εξελίξεις στο πλαίσιο των τηλεπικοινωνιών και της πληροφορικής, καθιστώντας έτσι, για παράδειγμα στο πλαίσιο της τηλεϊατρικής, δυνατή την απομακρυσμένη ιατρική παρακολούθηση και επέμβαση με ποικίλους τρόπους. Εγγενής σε μια τέτοιου τύπου αποκεντρωμένη υλοποίηση της παροχής ιατρικών υπηρεσιών είναι όμως και η επέκταση της επιφάνειας επίθεσης σε υπηρεσίες και συστήματα τα οποία συνδέονται πλέον άμεσα με την φυσική ασφάλεια των ασθενών. Η δημιουργία ενός κοινού πλαισίου για την έγκαιρη αναγνώριση και διαχείριση των κινδύνων που απορρέουν από ένα τέτοιο μοντέλο είναι απαραίτητη για την ασφαλή εκμετάλλευση των ευκαιριών που προσφέρονται από αυτό.

1.2. Περιγραφή προβλήματος

Παρά τις επιπτώσεις ενδεχόμενων κυβερνοεπιθέσεων στην υγεία και την ζωή των ασθενών στο πλαίσιο της ψηφιακής υγείας, δεν υπάρχει κάποιο ευρέως υιοθετημένο πλαίσιο για την αναγνώριση και την διαχείριση των σχετικών απειλών και επιπτώσεων στην υγεία των ασθενών. Η παρούσα μεταπτυχιακή διατριβή αποσκοπεί στην ανάπτυξη ενός πλαισίου για την οργανωμένη απεικόνιση και προτεραιοποίηση των επικινδυνοτήτων κυβερνοασφάλειας που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας σχετικά με την ασφάλεια των ασθενών, επιδοτώντας έτσι την αποτελεσματική διαχείρισή τους.

1.3. Ερευνητικά ερωτήματα

Με βάση υπόβαθρο της έρευνας, τα κίνητρά μας και την περιγραφή του προβλήματος τα ερευνητικά μας ερωτήματα ορίζονται ως εξής:

1. Ποιες είναι οι επικινδυνότητες κυβερνοασφάλειας που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας;

2. Ποιες είναι οι επικινδυνότητες για την ασφάλεια των ασθενών, ως αποτέλεσμα της εξάρτησης των διεργασιών υγείας από τα ψηφιακά συστήματα που τις υποστηρίζουν;

3. Πώς μπορούν να μετρηθούν και να προτεραιοποιηθούν οι επικινδυνότητες αυτές ως προς τις επιπτώσεις τους στην υγεία και την ζωή των ασθενών;

1.4. Δομή μεταπτυχιακής εργασίας

Η δομή της μεταπτυχιακής εργασίας είναι η εξής:

Στο **κεφάλαιο 2** θα παρουσιαστεί το θεωρητικό υπόβαθρο και η σχετική βιβλιογραφία της παρούσας μεταπτυχιακής εργασίας.

Στο **κεφάλαιο 3** θα προσδιοριστεί το περιβάλλον της ψηφιακής υγείας και το τρόπος ταξινόμησης των επικινδυνοτήτων κυβερνοασφάλειας που εντοπίστηκαν.

Στο **κεφάλαιο 4** θα παρουσιαστούν οι επικινδυνότητες κυβερνοασφάλειας που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας, όπως αυτές εντοπίστηκαν κατόπιν μελέτης της σχετικής βιβλιογραφίας.

Στο **κεφάλαιο 5** παρουσιάζονται οι επιπτώσεις των επικινδυνοτήτων κυβερνοασφάλειας στην ασφάλεια των ασθενών και διερευνάται ο συνδετικός κρίκος ανάμεσα στα δυο.

Στο **κεφάλαιο 6** παρουσιάζεται η προσέγγιση της μεθοδολογίας ARES για τον αυτόματο υπολογισμό επικινδυνοτήτων κυβερνοασφάλειας και στη συνέχεια παρουσιάζεται η προτεινόμενη προσέγγιση για τον υπολογισμό επικινδυνοτήτων για την υγεία των ασθενών ως αποτέλεσμα της εξάρτησης των σχετικών διεργασιών υγείας από την ψηφιακή υποδομή.

Στο **κεφάλαιο 7** παρουσιάζεται το λογισμικό που αναπτύχθηκε για να επιτύχει μια αυτοματοποιημένη εκτίμηση των επικινδυνοτήτων βάσει της προσέγγισης που παρουσιάστηκε στο κεφάλαιο 6, ενώ πραγματοποιείται μια δοκιμαστική λειτουργία του και σχολιάζονται οι περιορισμοί του.

Η μεταπτυχιακή εργασία τελειώνει με τον επίλογο του **κεφαλαίου 8**.

1.5. Μεθοδολογία

Στο πλαίσιο της παρούσας μεταπτυχιακής διατριβής υιοθετήσαμε μια ποιοτική προσέγγιση για την ανάλυση των υφιστάμενων αναφορών στη βιβλιογραφία. Η μεθοδολογία που ακολουθήθηκε ήταν η εξής: αρχικά χρησιμοποιήθηκαν οι βάσεις δεδομένων IEEE Xplore, Google Scholar, PubMed, Elsevier, ACM, arXiv και SpringerLink, ξεκινώντας από το 2010 και χρησιμοποιώντας διαφορετικές λέξεις-κλειδιά σχετικές με την ψηφιακή υγεία και την ασφάλεια των ασθενών σε κάθε βάση δεδομένων έτσι ώστε να εντοπιστούν τα άρθρα με σχετικό περιεχόμενο. Η αναζήτηση πραγματοποιήθηκε μέσω της χρήσης και του συνδυασμού ομάδων λέξεων-κλειδιών.

Η πρώτη ομάδα περιλαμβάνει λέξεις – κλειδιά που σχετίζονται με “information security” με λέξεις κλειδιά “security”, “privacy”, “encryption”, “hacking”, “confidentiality”, “integrity”, “availability”, “attacks”, “threats”. Η δεύτερη ομάδα περιλαμβάνει λέξεις – κλειδιά που σχετίζονται με “patient safety” με λέξεις κλειδιά “safety”, “patient safety”, “lack of care”, “lack of access”.

Η τρίτη ομάδα περιλαμβάνει λέξεις κλειδιά που σχετίζονται με “Healthcare”, με τις λέξεις κλειδιά “healthcare”, “eHealth”, “medical device”, “implantable device”, “patient data”.

Κατόπιν μελέτης της βιβλιογραφίας κωδικοποιήθηκαν οι ενδεχόμενες κυβερνοεπιθέσεις που απαντώνται στο πλαίσιο της ψηφιακής υγείας καθώς επίσης και τα ζητήματα προστασίας της υγείας και της ζωής των ασθενών από αυτές. Έπειτα προχωρήσαμε σε αξιοποίηση των σχετικών προτύπων και πρακτικών για την ανάπτυξη ενός πλαισίου και σχετικής εφαρμογής για την οργανωμένη απεικόνιση και προτεραιοποίηση των επικινδυνοτήτων που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας σχετικά με την ασφάλεια των ασθενών.

Κεφάλαιο 2
Ανασκόπηση βιβλιογραφίας και υπόβαθρο

Στο πλαίσιο κεφαλαίου 2 θα παρουσιαστούν τα κεντρικά άρθρα που μελετήθηκαν στο (2.1.) και θα περιγραφεί το σχετικό για την μεταπτυχιακή εργασία υπόβαθρο (2.2.).

2.1. Ανασκόπηση βιβλιογραφίας

Η ανασκόπηση της σχετικής βιβλιογραφίας επικεντρώνεται στον εντοπισμό των επικινδυνοτήτων που χαρακτηρίζουν συστήματα ψηφιακής υγείας, με τις περισσότερες πηγές να αναφέρονται σε ζητήματα ασφάλειας ιατρικών συσκευών, στην μεταχείριση του προβλήματος σύγκλισης σιγουριάς και ασφάλειας κατά την εκτίμηση των επικινδυνοτήτων αυτών και τέλος στην διαδικασία προτεραιοποίησης των επικινδυνοτήτων που εντοπίστηκαν.

Στο πλαίσιο εντοπισμού των επικινδυνοτήτων που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας οι περισσότερες πηγές αναφέρονται σε επιθέσεις σε συσκευές της γενικότερης κατηγορίας του Διαδικτύου των Ιατρικών Πραγμάτων (Internet of Medical Things – IoMT/IoTM) [7, 9, 13, 16, 22, 25, 26, 46, 82], συμπεριλαμβανομένων των ιατρικών συσκευών [3, 4, 5, 15, 23, 67, 83], με ελάχιστες πηγές να ασχολούνται με τις επικινδυνότητες που αφορούν γενικά σε πληροφοριακά συστήματα του χώρου της (ψηφιακής) υγείας [1, 2, 6, 8]. Υιοθετούνται διαφορετικοί τρόποι ταξινόμησης των επιθέσεων που εντοπίζονται, είτε βάσει της πτυχής ασφάλειας στην οποία και αφορούν [5, 13, 22, 26], είτε βάσει τοπολογίας [1, 2, 3, 8, 9, 23, 83], είτε βάσει της στρώσης του πρωτοκόλου επικοινωνίας TCP/IP στην οποία αφορά η επίθεση [7, 15, 16, 82]. Μερικές πηγές δεν χρησιμοποιούν κάποια συγκεκριμένη μέθοδο ταξινόμησης [4, 6, 25, 46, 67].

Κεντρικές πηγές σε στο πλαίσιο εντοπισμού επικινδυνοτήτων που χαρακτηρίζουν την γενικότερη κατηγορία ιατρικών συσκευών είναι η δουλειά των Yaqoob et al. [4], Papaioannou et al.

[22], Batista et al. [9] και Newaz et al. [2]. Οι Yaqoob et al. [4] ασχολήθηκαν ενδελεχώς με ζητήματα ασφάλειας στο πλαίσιο ιατρικών συσκευών, ενώ οι Papaioannou et al. [22] παρουσιάζουν μια πλήρη ταξινόμηση υφιστάμενων αλλά και δυνητικών απειλών και πιθανών αντιμέτρων. Οι Batista et al. [9] μελετούν έξυπνους αισθητήρες στο πλαίσιο της ψηφιακής υγείας και παρουσιάζουν μια ταξινόμηση απειλών υψηλού επιπέδου, η οποία και επιδοτεί την κατανόηση της συσχέτισης των επιμέρους στοιχείων πληροφοριακών συστημάτων στο χώρο της υγείας ως προς τις επιθέσεις που τα απειλούν. Τέλος, η δουλειά των Newaz et al. [2] καθιστά την πιο ενδελεχή πηγή που εντοπίστηκε. Στο άρθρο αυτό παρουσιάζονται οι απαιτήσεις ασφάλειας και παρουσιάζεται ένα μοντέλο επίθεσης το οποίο περιλαμβάνει τους πιθανούς τύπους επιθέσεων, τους στόχους του επιτιθέμενου και τις δυνατότητες του. Οι συγγραφείς αξιολογούν τις επιθέσεις που εντοπίστηκαν εξηγώντας τις ενδελεχώς, παρουσιάζοντας πολλαπλά παραδείγματα από τον χώρο της ψηφιακής υγείας και συνυπολογίζοντας χαρακτηριστικά όπως την προσέγγιση της εκάστοτε επίθεσης και την πολυπλοκότητα της.

Ο Piggin [62] ασχολείται με τα γενικότερα ζητήματα ασφάλειας που ανακύπτουν στο πλαίσιο ιατρικών συσκευών και ασχολείται ιδιαίτερα με το ζήτημα της σύγκλισης σιγουριάς και ασφάλειας, ζήτημα με το οποίο ασχολείται τόσο η Skierka [67] αλλά και οι Lisova et al. [66], οι οποίοι και συγκρίνουν τις προτάσεις που εντοπίζονται στην βιβλιογραφία κατά την εκτίμηση κινδύνων σε περιπτώσεις που επιχειρείται η διενέργεια της σχετικής διαδικασίας τόσο υπό το πρίσμα της σιγουριάς όσο και υπό το πρίσμα της ασφάλειας, σχολιάζοντας ενδελεχώς την κάθε προτεινόμενη προσέγγιση.

Οι Battles και Lilford [61] παρουσιάζουν έναν τρόπο οργάνωσης της έρευνας σχετικά με την ασφάλεια των ασθενών, απαγκιστρωμένη από ζητήματα κυβερνοασφάλειας και βασισμένη στην προσέγγιση του Donabedian [74], όπως αυτή εξελίχθηκε από τους Reason [74, 75], Rasmussen [77] και τον Van der Schaaf [78].

Στο πλαίσιο προτεραιοποίησης των επικινδυνοτήτων που εντοπίστηκαν, κεντρική δουλειά είναι αυτή των Dimitriades et al. [79]. Το άρθρο παρουσιάζει την προσέγγιση ARES (Automated Risk Estimation in Smart Sensor Environments), η οποία και αναπτύχθηκε με σκοπό την αυτοματοποιημένη εκτίμηση κινδύνου σε υπολογιστικά συστήματα και μέρη αυτών, βασιζόμενη στην δημιουργία μιας αλυσίδας ιχνηλάτησης των ευπαθειών του εκάστοτε υπολογιστικού

συστήματος, των ασθενειών που σχετίζονται με τις ευπάθειες αυτές και τέλος τους τύπους επιθέσεων που εκμεταλλεύονται τις ασθένειες που εντοπίστηκαν.

2.2. Υπόβαθρο

Στο πλαίσιο του υποβάθρου θα ξεκινήσουμε με την παρουσίαση του κεντρικού μοντέλου απαιτήσεων κυβερνοασφάλειας, το τρίπτυχο εμπιστευτικότητας (Confidentiality), ακεραιότητας (Integrity) και διαθεσιμότητας (Availability) – το λεγόμενο τρίπτυχο CIA (3.2.1.), θα προχωρήσουμε στην σύντομη παρουσίαση του πλαισίου και της σημασίας της διαδικασίας εκτίμησης κινδύνων (3.2.2.) και τέλος των – σημαντικών για την προσέγγιση που θα παρουσιαστεί στο πλαίσιο του κεφαλαίου 7 – κοινών προτύπων ασφάλειας για τον υπολογισμό κινδύνου στο πλαίσιο της ψηφιακής υγείας (3.2.3.).

2.2.1. Τρίπτυχο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας

Για να καθορίσουμε τις απαιτήσεις ασφάλειας συστημάτων ψηφιακής υγείας θα πρέπει αρχικά να εξετάσουμε τις επιταγές της ασφάλειας πληροφοριών, ο πυρήνας της οποίας περιστρέφεται γύρω από την προστασία του τριπτύχου της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας [80]. Η εμπιστευτικότητα αφορά στην αποτροπή ή την ελαχιστοποίηση αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένα άτομα. Η ακεραιότητα αφορά στην προστασία της αξιοπιστίας και ορθότητας των πληροφοριών, ενώ διαθεσιμότητα σημαίνει πως εξουσιοδοτημένοι χρήστες αποκτούν έγκαιρη και αδιάκοπη πρόσβαση στο εκάστοτε αντικείμενο και πως οι υποδομές που την υποστηρίζουν είναι λειτουργικές.

Αν εξετάσουμε το τρίπτυχο αυτό ως προς την αντιστοίχηση της προστασίας που επιδιώκει ως προς την ασφάλεια των ασθενών, παρατηρούμε πως και οι τρεις πτυχές του διατηρούν την σημασία τους:

1. Στο πλαίσιο της εμπιστευτικότητας εμπίπτει η ευρύτερη κατηγορία δεδομένων υγείας των ασθενών, η οποία και ρυθμιστικά προστατεύεται τόσο από την Health Insurance Portability and Accountability Act (HIPPA) όσο και το General Data Protection Regulation (GDPR). Ιδιαιτέρως σχετικά είναι σε αυτό το πλαίσιο δεδομένα από αισθητήρες [9]. Άμεσα σχετικά με την φυσική ασφάλεια του ασθενή, δεδομένης της σύνδεσης ιατρικών αποφάσεων οι οποίες και την επηρεάζουν, είναι τα δεδομένα της πρώτης κατηγορίας, τα οποία και προσφέρουν πολλαπλές δυνατότητες στο πλαίσιο της

αποκεντρωμένης υγειονομικής περίθαλψης, είτε με την μορφή της αυτοπαρακολούθησης είτε με την μορφή της αποκεντρωμένης παρακολούθησης της υγείας των ασθενών και την έγκαιρη ανίχνευση πιθανών ιατρικών επιπλοκών. Παρά την σημασία εξασφάλισης της εμπιστευτικότητας τέτοιου τύπου δεδομένων όμως, και υπό το πρίσμα της προστασίας της φυσικής ασφάλειας του ασθενή, η εμπιστευτικότητα κατέχει μια καθαρά υποστηρικτική θέση μιας και η απώλειά της δεν καθορίζει τις σχετικές ιατρικές αποφάσεις, ενέργειες, ή παραλείψεις.

2. Κεντρικό ρόλο στην φυσική ασφάλεια του ασθενή παίζει όμως η ακεραιότητα των πληροφοριών. Βασιζόμενοι στο παράδειγμα των ανθρωποκεντρικών αισθητήρων, και δεδομένης της χρήσης δεδομένων που πηγάζουν από αυτούς από ιατρικές συσκευές οι οποίες και μπορούν να προκαλέσουν άμεσα ζημιά στην υγεία ή και να απειλήσουν την ζωή των ασθενών όπως στην περίπτωση αντλιών έκχυσης ή βηματοδοτών [67], η εξασφάλιση της αξιοπιστίας και της ορθότητας των δεδομένων στα οποία βασίζονται οι ιατρικές αποφάσεις, ενέργειες, ή παραλείψεις, έστω και αυτοματοποιημένα, είναι καθοριστική.

3. Αντιστοίχως σημαντική για την φυσική ασφάλεια των ασθενών είναι και η διαθεσιμότητα των συστημάτων ψηφιακής υγείας, είτε πρόκειται για κάποια ιατρική συσκευή είτε και “απλά” για τρόπο επικοινωνίας με τον θεράποντα γιατρό. Σημαντικό σε αυτό το πλαίσιο είναι πως η ζημιά στην υγεία ή η απειλή για την ζωή δεν είναι απαραίτητο να προκαλείται άμεσα από την έλλειψη διαθεσιμότητας, όπως θα δούμε παρακάτω.

2.2.2. Πλαίσιο και σημασία της διαδικασίας εκτίμησης και διαχείρισης κινδύνων

Ο κίνδυνος, σύμφωνα με τον οργανισμό NIST [88] περιγράφει το εύρος απειλών τις οποίες αντιμετωπίζει μια οντότητα και θα πρέπει, ιδανικά, να διατηρείται σε αποδεκτά επίπεδα ώστε να εξυπηρετεί το επίπεδο ασφαλείας που κρίνεται ως απαραίτητο από τον εκάστοτε οργανισμό. Αυτό πραγματοποιείται μέσω της διαδικασίας διαχείρισης κινδύνων, στο πλαίσιο της οποίας αναγνωρίζεται, εκτιμάται και διατηρείται το επίπεδο κινδύνου στα επιθυμητά επίπεδα.

Σύμφωνα με τον οργανισμό NIST [88], κάθε μεθοδολογία εκτίμησης κινδύνου περιλαμβάνει τυπικά τα εξής:

1. μια διεργασία εκτίμησης του κινδύνου (risk assessment process),

2. ένα μοντέλο κινδύνου, στο οποίο καθορίζεται η σχετική ορολογία και προσδιορίζονται οι διάφοροι παράγοντες κινδύνου και οι μεταξύ τους σχέσεις,

3. μια μεθοδολογία υπολογισμού, στο πλαίσιο της οποίας καθορίζεται το εύρος τιμών του εκάστοτε παράγοντα κινδύνου. Τυπικά, σε αυτό το σημείο απαντώνται τρία είδη μεθοδολογιών, ποιοτικές, ποσοτικές και ανάμεικτες.

4. Μια μεθοδολογία ανάλυσης των κινδύνων. Σε αυτό το πλαίσιο απαντώνται τρεις κύριες προσεγγίσεις, οι οποίες είτε εστιάζουν στο εκάστοτε αγαθό και τις επιπτώσεις σε αυτό (asset/impact oriented) είτε εστιάζουν στις σχετικές απειλές, από τις οποίες πηγάζουν ενδεχόμενες επιθέσεις (threat oriented) είτε εστιάζουν στις ευπάθειες που απαντώνται στο εκάστοτε αγαθό (vulnerability oriented).

2.2.3. Κοινά πρότυπα ασφάλειας

Τα κοινά πρότυπα ασφάλειας περιγράφουν τα βασικά, κοινά στοιχεία τα οποία και χρησιμοποιούνται για την εκτίμηση και διαχείριση κινδύνων, και οποία βασίζονται σε σχετικά εγχειρήματα διαφόρων οργανισμών.

1. CPE (Common Platform Enumeration) [91], αφορά σε σύστημα ή μέθοδο ονοματοδοσίας κάθε στοιχείου (λογισμικού και υλικού) της εκάστοτε υπολογιστικής ή δικτυακής υποδομής.

2. CVE (Common Vulnerability and Exposures) [94], αφορούν σε σύστημα περιγραφής μια γνωστής, εκμεταλλεύσιμης ευπάθειας σε λογισμικό ή υλικό. Κάθε CVE εμπεριέχει πλειάδα πληροφοριών (άλλες υποχρεωτικά και άλλες όχι) σχετικά με την ευπάθεια, μεταξύ των οποίων ένα μοναδικό χαρακτηριστικό αριθμό, μια περιγραφή, μια δημόσια αναφορά, μια αναφορά στο στοιχείο της εκάστοτε υπολογιστικής ή δικτυακής υποδομής κάνοντας χρήση του συστήματος ονοματοδοσίας CPE, μια αναφορά σε σχετικές αδυναμίες και περιγραφή της σοβαρότητάς της.

3. CWE (Common Weakness Enumeration) [93], αφορούν σε σύστημα περιγραφής ενδεχόμενων ασθενειών ή ελαττωμάτων στην αρχιτεκτονική, στον σχεδιασμό ή στον κώδικα λογισμικού που καθιστά δυνατή την εκάστοτε ευπάθεια (CVE).

4. CAPEC (Common Attack Pattern Enumeration and Classification) [92], αφορούν σε ένα εμπεριστατωμένο λεξικό και απόπειρα ταξινόμησης όλων των γνωστών απειλών ασφαλείας. Κάθε CAPEC περιγράφει τα κοινά χαρακτηριστικά μιας κυβερνοαπειλής, επιδοτώντας έτσι την κατανόηση της. Χρησιμοποιούν μια ποιοτική προσέγγιση βαθμονόμησης της πιθανότητας και της επίδρασης σε μια κλίμακα πέντε επιπέδων, η οποία κυμαίνεται από πολύ χαμηλή έως πολύ υψηλή. Τέλος κάθε CAPEC καταγράφει και τις αδυναμίες (CWEs) που καθιστούν δυνατή την σχετική επίθεση.

5. CVSS (Common Vulnerability Scoring System) [90], το οποίο και αφορά σε σύστημα βαθμονόμησης ευπαθειών το οποίο και επιδοτεί την επικοινωνία των χαρακτηριστικών τους, μερικά από τα οποία πρέπει να συμπεριλαμβάνονται και άλλα τα οποία είναι προαιρετικά. Συχνά περιλαμβάνεται στο πλαίσιο του εκάστοτε CVE.

Κεφάλαιο 3
Πλαίσιο μελέτης ασφάλειας συστημάτων ψηφιακής υγείας

Στο πλαίσιο του κεφαλαίου 3 θα παρουσιαστεί το πλαίσιο μελέτης της ασφάλειας των συστημάτων ψηφιακής υγείας με βάση μιας συστηματικής μελέτης της σχετικής βιβλιογραφίας. Αφού αρχικά προσδιορίσουμε τα προβλήματα που εντοπίστηκαν στο πλαίσιο αυτής της διαδικασίας (3.1.) και προσδιορίσουμε το περιβάλλον της ψηφιακής υγείας (3.2.), θα περιγράψουμε την μέθοδο ταξινόμησης των απειλών την οποία θα υιοθετήσουμε (3.3.).

3.1. Το πρόβλημα στο πλαίσιο των προσεγγίσεων της βιβλιογραφίας

Στο πλαίσιο αξιολόγησης της βιβλιογραφίας παρατηρείται μια βαθιά σύγχυση των εννοιών απειλή (threat), επίθεση (attack) στην οποία μπορεί να οδηγήσει η εκάστοτε απειλή, ευπάθεια (vulnerability) και επίπτωση (impact), κάτι που με την σειρά του σημαίνει πως οι κατηγοριοποιήσεις που απαντώνται πάσχουν από μια ανάμειξη των παραπάνω όρων στο πλαίσιο παρουσίασης σχετικών απειλών. Χαρακτηριστικά, στην βιβλιογραφία που εξετάστηκε, θα πρέπει να απορρίψουμε τα εξής:

1. Η περίπτωση του διακομιστή Dropbear SSH [1] και των προβλημάτων που μπορεί να δημιουργήσει δεν αφορά σε απειλή αλλά σε ευπάθεια του διακομιστή dropbear SSH.

2. Η εξάντληση μπαταρίας (Battery Depletion) [2, 3, 4] παρουσιάζεται ως επίθεση ενώ ουσιαστικά καθιστά επίπτωση κάποιας επίθεσης όπως θα δούμε παρακάτω.

3. Η διαρροή δεδομένων (Data Breach) παρουσιάζεται ως επίθεση [5] ενώ καθιστά επίπτωση επίθεσης, συγκεκριμένα με την μορφή κατάλυσης της εμπιστευτικότητας.

4. Η κοινοποίηση μηνυμάτων (Message Disclosure) παρουσιάζεται ως ξεχωριστό παράδειγμα της κατηγορίας διαρροής δεδομένων [4, 6]. Όπως και πάλι, αφορά σε επίπτωση επίθεσης, συγκεκριμένα με την μορφή κατάλυσης της εμπιστευτικότητας.

5. Η εκμετάλλευση ασθενών μεθόδων αυθεντικοποίησης (Weak Authentication Schemes Exploitation) [2] αφορά σε αόριστη περιγραφή εκμετάλλευσης της σχετικής ευπάθειας (Weak Authentication, CWE – 1390) και δεν καθιστά περιγραφή συγκεκριμένης επίθεσης.

6. Η μη εξουσιοδοτημένη πρόσβαση (Unauthorized Access) [4, 6] δεν καθιστά επίθεση αλλά αντίκτυπο επιτυχημένης επίθεσης.

7. Η επίθεση σε υπολογιστικό νέφος το οποίο καθιστά υποδομή ως υπηρεσία (IaaS Cloud Attack) [7] περιγράφει ένα κομμάτι της επιφάνειας επίθεσης αναγνωρίζοντάς το ως πιθανό στόχο και όχι κάποιον συγκεκριμένο τύπο επίθεσης.

8. Η αναβάθμιση προνομίων (Privilege Escalation) [2] δεν περιγράφει επίθεση αλλά επίπτωση επιτυχημένης επίθεσης η οποία και οδηγεί στην κατάσταση που περιγράφεται.

9. Η παραβίαση κόμβου (Compromised Node) [6] δεν καθιστά περιγραφή συγκεκριμένης επίθεσης αλλά περιγραφή του αντικτύπου επιτυχημένης επίθεσης σε κάποιον κόμβο.

10. Τα παρωχημένα/παλαιωμένα λειτουργικά συστήματα (Outdated Operating Systems) [2, 7] περιγράφουν αδυναμία (Use of Unmaintained Third Party Components, CWE – 1104), δηλαδή μια συνθήκη εγγύτερη μιας ευπάθειας, η οποία *μπορεί να οδηγήσει* σε κάποια σχετική επίθεση, όπως για παράδειγμα σάρωση για ευπαθές λογισμικό (Scanning for Vulnerable Software, CAPEC – 310), χωρίς όμως η ίδια να συνιστά επίθεση.

Δεδομένης αυτής της σύγχυσης, η οποία πέραν της ανάμειξης ανόμοιων εννοιών οδηγεί και στον επανειλημμένο χαρακτηρισμό της ίδιας απειλής ή επίθεσης με διαφορετικούς τρόπους, προτείνουμε την χρήση των ονομάτων των σχετικών με την εκάστοτε επίθεση CAPEC για την ονομασία της, με υποστηρικτική περιγραφή της επίθεσης – και ενδεχομένως την χρήση περισσότερων CAPEC – αν κάτι τέτοιο είναι απαραίτητο. Μια τέτοια προσέγγιση καθιστά δυνατή την χρήση μιας κοινής ορολογίας για την επικοινωνία πιθανών επιθέσεων, ενώ ταυτόχρονα

προσφέρεται η δυνατότητα επιστροφής στο εκάστοτε CAPEC για εξερεύνηση σχετικών αδυναμιών (CWE) ή και άλλων CAPEC τα οποία μπορούν να προηγηθούν η να ακολουθήσουν επιτυχή εκμετάλλευση του εξεταζόμενου.

Αν, για παράδειγμα, θέλουμε να περιγράψουμε την επικινδυνότητα εισβολής κατόπιν χρήσης συνθηματικού (Password Intrusion) για την περίπτωση που θέλουμε να αναφερθούμε στην απειλή επίθεσης εξαντλητικής αναζήτησης και μετέπειτα χρήσης του συνθηματικού που ανακτήθηκε μπορούμε να αναφερθούμε στα CAPEC – 49 (επίθεση εξαντλητικής αναζήτησης) για την ανάκτηση του συνθηματικού, το οποίο ατομικά δεν συνεπάγεται πρόσβαση στο εκάστοτε σύστημα, και στο CAPEC – 560, το οποίο και περιγράφει την χρήση γνωστών διαπιστευτηρίων (use of known domain credentials), για την χρήση του συνθηματικού και την απόκτηση σχετικής πρόσβασης.

3.2. Καθορισμός του περιβάλλοντος της ψηφιακής υγείας

Επόμενο βήμα είναι ο προσδιορισμός του περιβάλλοντος της ψηφιακής υγείας ως προς τα συστατικά στοιχεία του. Η περιγραφή μας αφορά συνεπώς στον προσδιορισμό της επιφάνειας επίθεσης που απαντάται στο πλαίσιο της ψηφιακής υγείας.

Αν προσεγγίσουμε τα γενικότερα συστατικά στοιχεία του περιβάλλοντος της ψηφιακής υγείας, παρατηρούμε πως μπορούμε να τα οργανώσουμε στις εξής τέσσερις κατηγορίες [8]:

1. Δεδομένα ψηφιακής υγείας (eHealth data), δηλαδή το σύνολο των πληροφοριών οι οποίες και σχετίζονται με το γενικότερο πλαίσιο της ψηφιακής υγείας. Στην κατηγορία αυτή ανήκουν δεδομένα τα οποία πηγάζουν από ανθρωποκεντρικούς αισθητήρες, από αισθητήρες περιβάλλοντος αλλά και ο προσωπικός φάκελος υγείας (Personal Health Record – PHR) του εκάστοτε ασθενή.

   Τα ανθρωποκεντρικά δεδομένα αφορούν στον άνθρωπο και προέρχονται, στο πλαίσιο που μεταχειριζόμαστε εδώ, από ανθρωποκεντρικούς αισθητήρες. Πρόκειται για ιατρικά δεδομένα, όπως βιοσήματα (δηλαδή φυσιολογικές παραμέτρους), δεδομένα σχετικά με την κατάσταση και τις συνθήκες υγείας. Επιπλέον, αισθητήρες που συλλέγουν τη θέση ή τις κινήσεις του σώματος των χρηστών τους παράγουν δεδομένα που μπορούν να χρησιμοποιηθούν για τον εντοπισμό του εκάστοτε ασθενή [9].

Τα δεδομένα περιβάλλοντος στο πλαίσιο της υγείας αφορούν σε δεδομένα σχετικά με περιβαλλοντικές παραμέτρους (π.χ. ατμοσφαιρική πίεση, θερμοκρασία κ.ο.κ.). Οι πληροφορίες αυτές σπάνια χρησιμοποιούνται για ατομικές αποφάσεις στο πλαίσιο της υγειονομικής περίθαλψης, παίζουν όμως σημαντικό ρόλο στο πλαίσιο της ψηφιακής υγείας για την βελτίωση της ευεξίας των ανθρώπων [9].

Η αλλοίωση ανθρωποκεντρικών δεδομένων μπορεί, δεδομένης της βαρύτητας των ατομικών ιατρικών αποφάσεων, να οδηγήσει σε ζημιά υψηλής βαρύτητας, ενώ η αλλοίωση δεδομένων περιβάλλοντος μπορεί να οδηγήσει σε μικρότερες ζημιές μεγαλύτερης κλίμακας [9].

Το αυξημένο ενδιαφέρον για την στοχοποίηση δεδομένων ψηφιακής υγείας αντικατοπτρίζεται και από το κόστος τους στην μαύρη αγορά, όπου η αξία ενός φακέλου υγείας ασθενούς ήδη το 2016 προσέγγιζε τα 50$, ενώ ένας αριθμός κοινωνικής ασφάλισης κοστολογούνταν σε 3$ και ο αριθμός μιας πιστωτικής κάρτας σε 1,50$ [10].

2. Ιατρικές συσκευές (Medical Devices), οι οποίες, εφόσον μπορούν να συνδεθούν στο διαδίκτυο ανήκουν στην γενικότερη κατηγορία του διαδικτύου των ιατρικών πραγμάτων (Internet of Medical Things – IoTM/mIOT), καθιστούν "ιατροτεχνολογικά προϊόντα", τα οποία σύμφωνα με το Άρθρο 2 του Κανονισμού της Ευρωπαϊκής Ένωσης 2017/745 [95] ορίζονται ως "κάθε όργανο, συσκευή, εξοπλισμός, λογισμικό, εμφύτευμα, αντιδραστήριο, υλικό ή άλλο αντικείμενο το οποίο προορίζεται από τον κατασκευαστή να χρησιμοποιηθεί, μόνο του ή σε συνδυασμό, στον άνθρωπο για έναν ή περισσότερους από τους ακόλουθους συγκεκριμένους ιατρικούς σκοπούς:

— διάγνωση, πρόληψη, παρακολούθηση, πρόβλεψη, πρόγνωση, θεραπεία ή ανακούφιση ασθένειας,

— διάγνωση, παρακολούθηση, θεραπεία, ανακούφιση ή επανόρθωση τραύματος ή αναπηρίας,

— διερεύνηση, αντικατάσταση ή τροποποίηση της ανατομίας ή μιας φυσιολογικής ή παθολογικής λειτουργίας ή κατάστασης,

— παροχή πληροφοριών χάρη σε in vitro εξέταση δειγμάτων, προερχόμενων από το ανθρώπινο σώμα, συμπεριλαμβανομένων της αιμοδοσίας και της δωρεάς οργάνων και ιστών, και του οποίου η κύρια επιδιωκόμενη δράση, εντός ή επί του ανθρώπινου σώματος, δεν επιτυγχάνεται με φαρμακολογικά ή ανοσολογικά μέσα ούτε μέσω του μεταβολισμού αλλά του οποίου η λειτουργία μπορεί να υποβοηθείται από τέτοια μέσα."

Ενδιαφέρον σε αυτό το πλαίσιο είναι πως σύμφωνα με το σημείο 19 του Προοιμίου του ίδιου Κανονισμού [95], το ίδιο το λογισμικό, όταν προορίζεται από τον κατασκευαστή για να χρησιμοποιηθεί ειδικά για μία ή περισσότερες από τις ιατρικές χρήσεις που περιέχονται στον ορισμό του ιατροτεχνολογικού προϊόντος, αποτελεί και *το ίδιο* ιατροτεχνολογικό προϊόν.

Εστιάζοντας σε συστήματα του διαδικτύου των πραγμάτων (Internet of Things – IoT) – ή του διαδικτύου των ιατρικών πραγμάτων (medical Internet of Things – mIoT), παρατηρούμε πως οι επικινδυνότητες χωρίζονται σε τυπικές ευπάθειες οποιουδήποτε συστήματος συνδεδεμένου στο διαδίκτυο – όπως για παράδειγμα καταχρηστικά ανοιχτές θύρες (ports), ύπαρξη ευπαθειών λογισμικού κ.ο.κ. και σε ευπάθειες που αφορούν "αποκλειστικά" συστήματα IoT, δεδομένων των χαρακτηριστικών, των τεχνολογιών και των πρωτοκόλλων που αυτά χρησιμοποιούν – όπως για παράδειγμα ελλείψεις/περιορισμούς λόγω του τυπικά μικρού μεγέθους, το οποίο και δεν επιτρέπει π.χ. την υλοποίηση ασύμμετρης κρυπτογραφίας ή, μια άλλη χαρακτηριστική συνθήκη για συστήματα IoT, την χρήση ενσωματωμένων (embedded) λειτουργικών συστημάτων, τα οποία και δεν σχεδιάζονται με (τουλάχιστον κεντρικό) στόχο σχεδιασμού την ασφάλεια [11].

Παρά την διαρκώς αυξανόμενη υιοθέτησή τους, οι τεχνολογίες IoT δεν έχουν ωριμάσει ακόμα, κάτι που είναι ιδιαίτερα ορατό στο πλαίσιο του επιπέδου ασφάλειας που επιτυγχάνουν [12]: δεδομένης της μεγάλης επιφάνειας επίθεσης, το τοπίο απειλών IoT είναι διαρκώς αυξανόμενο. Επιπλέον, καθώς οι συσκευές έχουν περιορισμένους πόρους και είναι σχεδιασμένες με σκοπό την ελάχιστη κατανάλωση κατά την παροχή των υπηρεσιών τους και μάλιστα με το ελάχιστο δυνατό κόστος, η ασφάλεια συχνά παραμελείται στον κύκλο της ανάπτυξής τους. Το εύρος διαθέσιμων λειτουργικών συστημάτων και εκδόσεων υλικολογισμικού (firmware) καθιστά δύσκολη την ανάπτυξη

“αγνωστικών” της εκάστοτε τεχνολογίας και αρχιτεκτονικής λύσεων ασφάλειας - οι οποίες με την σειρά τους θα πρέπει να είναι και επεκτάσιμες αλλά και εύκολα εφαρμόσιμες, κάτι εγγενώς δύσκολο σε περίπτωση του Διαδικτύου των Πραγμάτων.

3. Ιατρικά Δίκτυα (Medical Networks), κατηγορία που περιλαμβάνει κάθε τύπο δικτύου που μεταδίδει δεδομένα ηλεκτρονικής υγείας, όπως η επικοινωνία στο πλαίσιο του διαδικτύου των ιατρικών πραγμάτων και τα ασύρματα δίκτυα περιοχής σώματος (Wireless Body Area Networks - WBAN).

4. Υπολογιστικό Νέφος (Edge/Fog/Cloud), το οποίο και τυπικά χρησιμοποιείται ως ασφαλής χώρος αποθήκευσης δεδομένων ηλεκτρονικής υγείας.

3.3. Μέθοδος ταξινόμησης απειλών

Αν υιοθετήσουμε τον ορισμό της επιφάνειας επίθεσης ως το σύνολο των σημείων εντός των ορίων ενός συστήματος, ενός στοιχείου συστήματος ή ενός περιβάλλοντος όπου ένας επιτιθέμενος μπορεί να προσπαθήσει να εισέλθει, να καταφέρει να επενεργήσει ή να εξάγει δεδομένα από το εν λόγω σύστημα, στοιχείο συστήματος ή περιβάλλον [97], η επιφάνεια επίθεσης και οι πιθανές απειλές που απαντώνται είναι στενά συνυφασμένες καθώς εξελίσσονται παράλληλα, σε σημείο που πολλές φορές καταλήγουν να αλληλοκαθορίζονται. Στην βιβλιογραφία που εξετάστηκε απαντώνται οι εξής προσεγγίσεις ταξινόμησης απειλών και επιθέσεων:

1. Σύμφωνα με την φύση της επίθεσης, αν πρόκειται δηλαδή για ενεργητική ή παθητική [13]. Στο πλαίσιο παθητικών επιθέσεων ο επιτιθέμενος παρακολουθεί και συλλέγει πληροφορίες για το σύστημα, τις οποίες εκμεταλλεύεται σε ένα επόμενο στάδιο στο πλαίσιο περαιτέρω επιθέσεων. Τέτοιου τύπου ενέργειες λειτουργούν ουσιαστικά προπαρασκευαστικά, χωρίς να προκαλούν άμεσα ζημιά στο σύστημα – στόχο, κάτι που με την σειρά του οδηγεί στο να μην γίνονται αντιληπτές από τον οργανισμό – θύμα. Το άλλο άκρο, οι ενεργητικές επιθέσεις, αποσκοπούν στην τροποποίηση ή άμεση ζημίωση του συστήματος μέσω της εισαγωγής, αλλοίωσης ή καταστροφής δεδομένων ή υπηρεσιών. Το αντίξοο αποτέλεσμα μιας ενεργής επίθεσης γίνεται πολύ πιο εύκολα αντιληπτό από το θύμα.

2. Σύμφωνα με την πηγή της επίθεσης ως προς τον οργανισμό/σύστημα – στόχο, αν πρόκειται δηλαδή για εσωτερική ή εξωτερική [13]. Αν η επίθεση πηγάζει από κάποια εσωτερική απειλή, πρόκειται για εσωτερική επίθεση. Αντιθέτως, επιθέσεις που ξεκινούν εκτός των "ορίων" του οργανισμού/συστήματος καθιστούν εξωτερικές επιθέσεις.

3. Σύμφωνα με την μέθοδο εκτέλεσης της επίθεσης [14], αν πρόκειται δηλαδή για φυσικές μεθόδους, μεθόδους που βασίζονται σε λογισμικό ή μεθόδους παράπλευρου καναλιού (side-channel methods). Οι φυσικές μέθοδοι αφορούν σε περιπτώσεις που ο επιτιθέμενος έχει την δυνατότητα να έχει φυσική, μη εξουσιοδοτημένη πρόσβαση στο κυβερνο-φυσικό σύστημα. Μέθοδοι που βασίζονται σε λογισμικό στηρίζονται στην εκμετάλλευση ευπαθειών λογισμικού, λειτουργικών συστημάτων, (διαδικτυακών) εφαρμογών και πρωτοκόλλων έτσι ώστε να αποκτηθεί με αυτόν τον τρόπο μη εξουσιοδοτημένη πρόσβαση. Οι μέθοδοι παράπλευρου καναλιού βασίζονται στην παρατήρηση των έμμεσων φυσικών επιπτώσεων λειτουργίας των συστημάτων με σκοπό την απόκτηση πληροφοριών σχετικών με την λειτουργία τους.

4. Σύμφωνα με την στρώση του πρωτοκόλλου επικοινωνίας TCP/IP (αντιστοίχως μπορεί να χρησιμοποιηθεί και το μοντέλο OSI) στην οποία αφορά η επίθεση [7, 15, 16, 82], δηλαδή στα στρώματα εφαρμογής, μεταφοράς, δικτύου και το στρώμα διασύνδεσης δικτύου. Οι επιτιθέμενοι μπορούν να στοχοποιήσουν οποιαδήποτε από τις στρώσεις της στοίβας TCP/IP κατά την αναζήτηση και εκμετάλλευση ευπαθειών.

5. Σύμφωνα με την πτυχή ασφάλειας (CIA) της προσβολής την οποία και αφορούν [5, 13, 22, 26].

6. Σύμφωνα με τους εμπλεκόμενους φορείς σε συστήματα ψηφιακής υγείας ή σύμφωνα με την κατηγορία συστατικών πληροφοριακού συστήματος [1, 2, 3, 8, 9, 23, 83], δηλαδή κατηγοριοποίηση σε κόμβους, επικοινωνίες, νοσοκομειακά πληροφοριακά συστήματα και χρήστες.

Αντί να προσεγγίσουμε την περιγραφή του περιβάλλοντος της ψηφιακής υγείας αποκλειστικά ως προς την τυπική αρχιτεκτονική του, τα πρωτόκολλα που χρησιμοποιούνται ή ως προς τα συστατικά στοιχεία του, η προσέγγιση που επιδοτεί τον σκοπό μας, την ανάπτυξη δηλαδή ενός πλαισίου για την οργανωμένη απεικόνιση και προτεραιοποίηση των επικινδυνοτήτων που

χαρακτηρίζουν τα συστήματα ψηφιακής υγείας, είναι μια κατηγοριοποίηση των πιθανών επιθέσεων σύμφωνα με την τελευταία προσέγγιση ταξινόμησης, την οργάνωση δηλαδή των επιθέσεων ανάλογα με το αν αφορούν κόμβους, επικοινωνίες, νοσοκομειακά πληροφοριακά συστήματα ή χρήστες. Κατά αυτόν τον τρόπο απεικονίζεται με σαφήνεια, σε αντίθεση με δισ-διάστατες προσεγγίσεις σύμφωνα με την φύση ή την πηγή της εκάστοτε επίθεσης, το στοιχείο του περιβάλλοντος στο οποίο αναφερόμαστε και αυτό χωρίς την ανάγκη προσφυγής σε στοίβες πρωτοκόλλων επικοινωνίας, ενώ ταυτόχρονα αποφεύγεται και η ασαφής κατηγο-ριοποίηση σύμφωνα με την μέθοδο εκτέλεσης της εκάστοτε επίθεσης.

Κεφάλαιο 4
Απειλές για συστήματα ψηφιακής υγείας

Στο πλαίσιο του κεφαλαίου 4 θα προχωρήσουμε στην παρουσίαση των απειλών και επιθέσεων που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας, οι οποίες εντοπίστηκαν στην βιβλιογραφία, εναρμονισμένων πλέον με την βάση γνώσεων του εγχειρήματος CAPEC του οργανισμού MITRE. Δεδομένης της επιλογής μας σχετικά με την μέθοδο ταξινόμησης απειλών (3.3.), την κατηγοριοποίηση δηλαδή των πιθανών επιθέσεων ανάλογα με το αν αφορούν κόμβους, επικοινωνίες, νοσοκομειακά πληροφοριακά συστήματα ή χρήστες, τα ευρήματά μας κατόπιν μελέτης της βιβλιογραφίας μπορούν να παρουσιαστούν συνδυαστικά και οργανωμένα σύμφωνα με τα συστατικά πληροφοριακού συστήματος που αφορούν ως εξής:

1. Απειλές και επιθέσεις σχετικές με κόμβους:
    1.1. Κακόβουλο λογισμικό (4.1.)
    1.2. Εισβολή κατόπιν χρήσης συνθηματικού (4.3.)
    1.3. Επιθέσεις παράπλευρου καναλιού (4.10)
    1.4. Επιθέσεις τροποποίησης κατά την κατασκευή/διανομή (4.11.)
    1.5. Επιθέσεις τροποποίησης υλικολογισμικού (4.12.)
2. Απειλές και επιθέσεις σχετικές με επικοινωνίες
    2.1. Επιθέσεις δρομολόγησης (4.2.)

2.2. Επιθέσεις πλαστοπροσωπίας/πλαστογράφησης ταυτότητας (4.4.)

2.3. Επιθέσεις πλαστοπροσωπίας μέσω κλωνοποίησης συσκευής (4.5.)

2.4. Επιθέσεις υποκλοπής/ “Sniffing” (4.6.)

2.5. Επιθέσεις τύπου Man-in-The Middle (MiTM) (4.7.)

2.6. Επιθέσεις παραποίησης/τροποποίηση μηνυμάτων (4.8.)

2.7. Επιθέσεις πλημμύρας/επανειλημμένης σύνδεση (4.9.)

2.8. Επιθέσεις σχετικές με το πρωτόκολλο Bluetooth (4.14.)

3. Απειλές και επιθέσεις σχετικές με νοσοκομειακά πληροφοριακά συστήματα

3.1. Κακόβουλο λογισμικό (4.1.)

3.2. Εισβολή κατόπιν χρήσης συνθηματικού (4.3.)

3.3. Απειλές διεπαφών οικοσυστήματος (4.13.)

4. Απειλές και επιθέσεις σχετικές με χρήστες

4.1. Επιθέσεις κοινωνικής μηχανικής (4.15) και

4.2. επιθέσεις ηλεκτρονικού ψαρέματος (phishing) (4.15.)

4.1. Κακόβουλο λογισμικό

Κακόβουλο λογισμικό (malware) ορίζεται από τον οργανισμό NIST [89] ως το λογισμικό ή υλικολογισμικό που προορίζεται για την εκτέλεση κάποιας μη εξουσιοδοτημένης διαδικασίας, η οποία έχει δυσμενείς επιπτώσεις στην εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος πληροφοριών. Συμπεριλαμβάνει τις κατηγορίας ιός (virus), σκουλήκι (worm), δούρειος ίππος (trojan horse ή εν συντομία trojan) ή άλλη οντότητα που βασίζεται σε

κώδικα και μολύνει ένα κεντρικό σύστημα. Το spyware, λογισμικό που αποσκοπεί την παρακολούθηση, και ορισμένες μορφές adware, λογισμικό που επιδοτεί κακόβουλη διαφήμιση, αποτελούν επίσης παραδείγματα κακόβουλου κώδικα. Συνεπώς στην γενικότερη κατηγορία κακόβουλου λογισμικού ανήκει κάθε τύπου κώδικας που αναπτύσσεται με κακόβουλες προθέσεις, με απώτερο σκοπό την εγκατάσταση και εκτέλεση στο σύστημα – στόχο, προκαλώντας έτσι κάποιο αποτέλεσμα που επιδοτεί το σχέδιο του κακόβουλου τρίτου, χωρίς, σε αυτό το πλαίσιο, να είναι απαραίτητο να προκαλεί *το ίδιο* την ζημιά η οποία και αποσκοπείται.

Η κατηγορία κακόβουλου λογισμικού χαρακτηρίζεται ως τοπική εκτέλεση κώδικα σύμφωνα με το CAPEC – 549. Η γενικότερη χρήση κακόβουλου λογισμικού μπορεί να είναι μέρος κάποιας επίθεσης συμπερίληψης κώδικα (code inclusion, CAPEC – 175) η οποία μπορεί να εκτελεστεί τοπικά (CAPEC – 251) ή απομακρυσμένα (CAPEC – 253), όπως για παράδειγμα στην περίπτωση διανομής μέσω της λεγόμενης επιμόλυνσης "νερόλακκου" (waterhole attack) στην οποία θα επιστρέψουμε παρακάτω, ή, εναλλακτικά, ως μέρος επίθεσης στην ακεραιότητα του λογισμικού (software integrity attack, CAPEC – 184), η οποία και περιλαμβάνει, μεταξύ άλλων, το "κατέβασμα" κακόβουλου λογισμικού (malicious software download, CAPEC – 185) και την κακόβουλη επικαιροποίηση υπάρχοντος λογισμικού (malicious software update, CAPEC – 186). Η οικογένεια κακόβουλου λογισμικού απαντάται πολλαπλές φορές στο πλαίσιο της βιβλιογραφίας [2, 5, 21, 22, 23], όπου και υπογραμμίζεται η επικινδυνότητα της για συστήματα στο χώρο της υγείας.

4.1.1. Πηγή του κώδικα κακόβουλου λογισμικού

Ο κώδικας δεν είναι απαραίτητο να έχει δημιουργηθεί από τον επιτιθέμενο. Μπορεί να αγοραστεί αλλά και να αποκτηθεί άνευ κόστους από το διαδίκτυο. Ανάλογα με την πολυπλοκότητα της επίθεσης υπάρχει όμως πιθανότητα να χρησιμοποιηθούν πληροφορίες που έχουν συλλεχθεί για το σύστημα – στόχο με σκοπό την ανάπτυξη *στοχευμένου* κακόβουλου λογισμικού (targeted malware), όπως προδίδει το CAPEC – 542 με το ίδιο όνομα.

4.1.2. Αποτελέσματα εκτέλεσης κακόβουλου κώδικα

Το εύρος των επιπτώσεων που σχετίζονται με την εκτέλεση κακόβουλου κώδικα σε κάποιο σύστημα περιορίζεται αποκλειστικά από τις δυνατότητες του συστήματος και τις προθέσεις του κακόβουλου τρίτου, όπως αυτές εν μέρει αντικατοπτρίζονται από τις δυνατότητες του εκάστοτε κακόβουλου κώδικα. Κάποιο σύστημα που έχει μολυνθεί με κακόβουλο λογισμικό

μπορεί παραδειγματικά να αντιμετωπίζει προβλήματα με την λειτουργικότητά του, όπως για παράδειγμα καθυστερήσεις ή τυχαία περιστατικά απενεργοποίησης. Στο άλλο άκρο, η μόλυνση με κακόβουλο λογισμικό μπορεί να συνεπάγεται την ολοκληρωτική απώλεια των δεδομένων αποθηκευμένων στο σύστημα, όπως στην περίπτωση ransomware, ή την ενσωμάτωση του συστήματος ως "σκλάβο" σε κάποιο botnet, επικινδυνότητα που απαντάται ιδιαίτερα σε κόμβους του διαδικτύου των πραγμάτων (IoT).

4.1.3. Τρόπος διανομής κακόβουλου λογισμικού

Οι τρόποι διανομής κακόβουλου λογισμικού είναι πολλές φορές στενά συνυφασμένοι με την διαδικασία επιμόλυνσης. Αν ο κακόβουλος τρίτος έχει αποκτήσει κάποιου τύπου πρόσβαση στο σύστημα, η οποία και του δίνει την δυνατότητα να εκτελέσει κώδικα, μπορεί να χρησιμοποιήσει κάποιο οικείο αποθηκευτικό μέσο όπως π.χ. USB ή CD για την επιμόλυνση. Ο συνηθέστερος, όμως, τρόπος διανομής του κακόβουλου λογισμικού είναι μέσω της χρήσης μεθόδων κοινωνικής μηχανικής, απειλή στην οποία θα επιστρέψουμε παρακάτω, και ιδιαίτερα μέσω:

1. μηνυμάτων ηλεκτρονικού ψαρέματος (phishing) σε όλες του τις εκφάνσεις[1], όπου το θύμα λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου με ενσωματωμένο σύνδεσμο (URL) ή συνημμένο αρχείο που περιέχει ένα πρόγραμμα λήψης (downloader). Όταν ο χρήστης διαδρά με τον σύνδεσμο ή με το πρόγραμμα λήψης, ενεργοποιείται ο σχετικός μηχανισμός, ο οποίος με την σειρά του "κατεβάζει" το εκάστοτε κακόβουλο λογισμικού μέσω σύνδεσης με έναν (τυπικά κακόβουλο) ιστότοπο όπου αυτός φιλοξενείται [20].

2. επιμόλυνσης "νερόλακκου" (watering hole attacks). Η χρήση του "νερόλακκου" παραπέμπει στο φαινόμενο που παρατηρείται στην φύση, όπου η πανίδα συγκεντρώνεται σε νερόλακκους. Αντιστοίχως, στην ψηφιακή έκδοση της επίθεσης, ο επιτιθέμενος παραβιάζει έναν ιστότοπο – τον "νερόλακκο" στην περίπτωσή μας – που είναι πιθανό να δέχεται συχνές επισκέψεις από μια συγκεκριμένη ομάδα-στόχο, αντί για να επιτεθεί *άμεσα* στην ομάδα-στόχο (μια μορφή "spear-phishing", που καθιστά περίπτωση στοχευμένου ηλεκτρονικού ψαρέματος και στην οποία θα επιστρέψουμε παρακάτω, άνευ χρήσης ηλεκτρονικού ταχυδρομείου [20]) [89]. Η παραβίαση του ιστότοπου – νε-

1 Δηλαδή συμπεριλαμβανομένων των μεθόδων "spear phishing" και "whaling", στις οποίες θα επιστρέψουμε παρακάτω.

ρόλακκου συνεπάγεται και την εμφύτευση κακόβουλου κώδικα σε αυτόν. Όταν ο χρήστης διαδρά με το εκάστοτε επιθυμητό αντικείμενο της ιστοσελίδας, ανακατευθύνεται σε κακόβουλους ή παραβιασμένους διακομιστές και καλείται να εγκαταστήσει νέο λογισμικό ή ενδεχομένως να προβεί σε (εδώ κακόβουλη) ενημέρωση υπάρχοντος λογισμικού [20].

3. χρήση προγραμμάτων τύπου Δούρειου Ίππου, δηλαδή κακόβουλα προγράμματα λογισμικού που μεταμφιέζονται – ή συνήθως ενσωματώνονται – σε χρήσιμα εργαλεία, εφαρμογές ή παιχνίδια. Εφαρμογές τέτοιου τύπου περιέχουν δύο φορτία: αφενός την λειτουργικότητα που αναζητούσε εξαρχής ο χρήστης (οι εφαρμογές δηλαδή λειτουργούν) και ένα δεύτερο φορτίο, αυτήν τη φορά κακόβουλο, το οποίο είτε "περιορίζεται" σε τοπική εκτέλεση είτε εγκαθιδρύει σύνδεση με κάποιον κακόβουλο ιστότοπο και "κατεβάζει" περισσότερο κακόβουλο λογισμικό (λειτουργεί δηλαδή ως "dropper") [20].

4.1.4. Τυπικές επιπτώσεις

Οι επιπτώσεις της οικογένειας κακόβουλου λογισμικού μπορούν να οδηγήσουν, ανάλογα με την εκάστοτε υλοποίηση, στην κατάλυση και των τριών πτυχών ασφάλειας.

4.1.5. Παραδείγματα από τον χώρο της υγείας

Διάφορα παραδείγματα χρήσης κακόβουλου λογισμικού παρουσιάζουν οι Newaz et al. [2] στον χώρο της υγείας, όπως για παράδειγμα την χρήση του – σχετικά παλιού – κακόβουλου λογισμικού Conficker, μέσω του οποίου καθίσταται δυνατή η απομακρυσμένη εκτέλεση κώδικα εκ μέρους του κακόβουλου τρίτου και το οποίο εντοπίστηκε σε 104 συσκευές στο πλαίσιο ενός νοσοκομείου (James A. Haley Veteran's Hospital στην Τάμπα, Φλόριντα), συμπεριλαμβανομένων μηχανημάτων ακτίνων Χ, μηχανημάτων μαστογραφίας και καμερών γάμμα. Ένα άλλο παράδειγμα είναι το κακόβουλο λογισμικό ονόματος "Kwampirs", το οποίο και καθιστά δυνατή, μεταξύ άλλων, την πρόκληση καθυστέρησης στην διαδικασία πρόσβασης σε πληροφορίες που φιλοξενεί ο σχετικός εξοπλισμός [19]. Πολλά είναι και τα παραδείγματα περιστατικών επιτυχούς μόλυνσης με κακόβουλο λογισμικό τύπου ransomware, με πιο χαρακτηριστική την περίπτωση του ransomware „WannaCry", από το οποίο και μολύνθηκαν περίπου 50 νοσοκομεία στο Ηνωμένο Βασίλειο το 2017, με πολλά από αυτά να απενεργοποιούν προληπτικά τα συστήματά τους. Σε αντίστοιχα περιστατικά μόλυνσης με Ransomware ο μέσος χρόνος αποκατάστασης περιορισμένης πρόσβασης στα συστήματα είναι περίπου 12

μέρες, με την πλήρη πρόσβαση να αποκαθίσταται σε περίπου 6 εβδομάδες [18]. Αυτή η συνθήκη αντικατοπτρίζει και την εγγενή επικινδυνότητα κακόβουλου λογισμικού σε περιπτώσεις πέραν της άμεσης πρόκλησης βλάβης σε άτομα, η οποία και έγκειται στην αλλοιωμένη η καθυστερημένη παροχή ιατρικής φροντίδας, γεγονός που επιβεβαιώνεται και από την πρόσφατη έρευνα του ινστιτούτου Ponemon, σύμφωνα με την οποία καθυστερήσεις βασιζόμενες σε ransomware δύνανται να οδηγήσουν έμμεσα σε βλάβη στην υγεία των ασθενών [17].

4.2. Επιθέσεις δρομολόγησης

4.2.1. Περιγραφή

Μια άλλη κατηγορία επιθέσεων, η οποία και απαντάται στην βιβλιογραφία συνήθως στο πλαίσιο ιατρικών συσκευών ή συσκευών στο πλαίσιο του (ιατρικού) διαδικτύου των πραγμάτων, είναι η οικογένεια επιθέσεων δρομολόγησης (η οποία απαντάται και ως ξεχωριστή επίθεση και όχι ως οικογένεια, όπως π.χ. στον Algarni, [6]), οι οποίες και ανταποκρίνονται στην επικινδυνότητα χειραγώγησης υποδομών (Infrastructure manipulation, CAPEC – 161), σύμφωνα με την οποία ο κακόβουλος τρίτος εκμεταλλεύεται χαρακτηριστικά της υποδομής ενός δικτύου προκειμένου:

1. να διαπράξει περαιτέρω επιθέσεις ή

2. να συλλέξει πληροφορίες σχετικά με κόμβους του δικτύου ή

3. να επιφέρει αλλαγή στη συνήθη ροή πληροφοριών μεταξύ των κόμβων αυτών.

Τις περισσότερες φορές, αυτό περιλαμβάνει τη χειραγώγηση της δρομολόγησης των μηνυμάτων στο πλαίσιο του δικτύου, έτσι ώστε, αντί να φτάνουν στον αρχικό προορισμό τους, να ανακατευθύνονται προς μια οντότητα που επιλέγει ο κακόβουλος τρίτος, συνήθως έναν διακομιστή που ελέγχεται από αυτόν, να προωθούνται επιλεκτικά ή και να απορρίπτονται. Οι επιθέσεις που απαντώνται σε αυτήν την κατηγορία είναι επιθέσεις τύπου “Sybil” [22, 25, 26], επιθέσεις τύπου “Wormhole” [25, 26] με τις υποκατηγορίες “Black Hole” [6, 25, 26] και ”Grey Hole” [6, 25, 26], επιθέσεις τύπου “Sinkhole” [25] και τέλος επίθεση δηλητηρίασης του πίνακα ARP (ARP table poisoning/ARP Cache Poisoning) [7], η οποία ανήκει σε υπο-κατηγορία του CAPEC – 161, αυτήν της δηλητηρίασης cache, CAPEC – 141.

Οι επιθέσεις τύπου “Sybil” παίρνουν το όνομα τους από την Sybil Dorsett [24], η οποία και έπασχε από διασχιστική διαταραχή ταυτότητας ή διαταραχή πολλαπλής προσωπικότητας και αντικατοπτρίζουν το χαρακτηριστικό πολλαπλών ψηφιακών προσωπικοτήτων, δηλαδή την κατασκευή πολλαπλών ψεύτικων ταυτοτήτων (κόμβους “Sybil”) στο πλαίσιο του εκάστοτε δικτύου, αποσκοπώντας την συμμετοχή σε κατανεμημένους αλγόριθμους [25] και κατ’ επέκταση την απόκτηση της εμπιστοσύνης του δικτύου π.χ. μέσω τροποποίησης των πινάκων δρομολόγησης [6], έτσι ώστε, σε ένα δεύτερο επίπεδο, να καταστήσουν δυνατές επιθέσεις τύπου Denial of Service (DoS) ή επιθέσεις πλημμύρας (Flooding) [22, 25, 26].

Στην περίπτωση της επίθεσης τύπου “Wormhole” [25, 26], η επίθεση εκτελείται μέσω της τροποποίησης των πινάκων δρομολόγησης, προωθώντας την κυκλοφορία σε κόμβους ελεγχόμενους από τον κακόβουλο τρίτο [25]. Η επίθεση προϋποθέτει δύο η περισσότερους κακόβουλους κόμβους, στρατηγικά τοποθετημένους στο δίκτυο. Ο επιτιθέμενος διοχετεύει τα μηνύματα που λαμβάνει σε ένα τμήμα του δικτύου μέσω μιας σύνδεσης χαμηλής καθυστέρησης (latency). Τα μηνύματα αναπαράγονται σε ένα άλλο τμήμα του δικτύου. Η επίθεση λειτουργεί πείθοντας κόμβους που απέχουν συνήθως πολλά άλματα (hops) από τον εκάστοτε προορισμό πως απέχουν μόνο ένα ή δύο άλματα μέσω κάποιου κακόβουλου κόμβου, ο οποίος παρουσιάζεται έτσι ως ιδιαίτερα “ελκυστικός”. Εάν το τελικό σημείο είναι σχετικά μακριά από τον εκάστοτε προορισμό, οι περισσότεροι κόμβοι θα προσπαθήσουν να χρησιμοποιήσουν τον κακόβουλο κόμβο για προώθηση των πακέτων τους, τα οποία στην συνέχεια μπορούν να προωθηθούν επιλεκτικά σε κάποιον από τους κακόβουλους κόμβους για περαιτέρω προώθηση ή να συλληφθούν για υποκλοπή πριν προωθηθούν [27]. Οι υποκατηγορίες [6, 25, 26] “Black Hole” και “Gray Hole” αφορούν στην μεταχείριση των πακέτων – θυμάτων της επίθεσης. Στην περίπτωση επίθεσης τύπου “Black Hole”, τα πακέτα απορρίπτονται συνολικά ή επιλεκτικά [25]. Στην περίπτωση επίθεσης τύπου “Gray Hole” η απόρριψη ή προώθηση εκτελείται και πάλι είτε επιλεκτικά είτε σε τυχαία χρονικά διαστήματα [28]. Επιθέσεις της γενικότερης κατηγορίας “Wormhole” έχουν πολλές ομοιότητες με τις επιθέσεις της κατηγορίας “Sinkhole” [27].

Στην περίπτωση επιθέσεων τύπου “Sinkhole” [25], ο επιτιθέμενος και πάλι χειραγωγεί τους γειτονικούς κόμβους για να προσελκύσει σχεδόν όλη την κυκλοφορία από μια συγκεκριμένη περιοχή του δικτύου μέσω ενός κακόβουλου κόμβου, παρουσιάζοντάς τον και πάλι ως ιδιαίτερα “ελκυστικό”, δημιουργώντας έτσι μια καταβόθρα (Sinkhole) πακέτων. Η συνθήκη αυτή

οδηγεί στην δρομολόγηση όλων των πακέτων στον κακόβουλο κόμβο, κάτι μου με την σειρά του καθιστά δυνατή την υποκλοπή και την επιλεκτική προώθηση ή και απόρριψη μηνυμάτων [29].

Τέλος, η δηλητηρίαση του πίνακα ARP [7] καθιστά υποκατηγορία της μεγαλύτερης οικογένειας επιθέσεων τύπου Man-in-The Middle (MiTM), στην οποία θα επιστρέψουμε παρακάτω. Στο πλαίσιο της επίθεσης ο κακόβουλος τρίτος εκμεταλλεύεται τη λειτουργικότητα των τεχνολογιών προσωρινής αποθήκευσης (cache) για να προκαλέσει την προσωρινή αποθήκευση συγκεκριμένων δεδομένων που εξυπηρετούν τους στόχους του, εδώ τροποποιημένων δεδομένων σχετικών με το πρωτόκολλο ARP. Αποτέλεσμα της επίθεσης είναι μια κατάσταση όπου η κυκλοφορία η οποία προορίζεται για συγκεκριμένους κόμβους στο τοπικό δίκτυο θα κατευθύνεται σε προορισμό της επιλογής του επιτιθέμενου.

4.2.2. Τυπικές επιπτώσεις

Οι επιπτώσεις της οικογένειας επιθέσεων δρομολόγησης μπορούν να οδηγήσουν, ανάλογα με την περίπτωση, στην κατάλυση και των τριών πτυχών ασφάλειας.

4.3. Εισβολή κατόπιν χρήσης συνθηματικού

4.3.1. Περιγραφή

Μια άλλη κατηγορία επικινδυνοτήτων που απαντάται είναι η εισβολή κατόπιν χρήσης συνθηματικού (password intrusion). Σκοπός του συνθηματικού είναι η αυθεντικοποίηση (authentication), δηλαδή η επιβεβαίωση της ταυτότητας του εκάστοτε χρήστη πριν του επιτραπεί η πρόσβαση στο εκάστοτε αγαθό. Αυτό μπορεί να επιτευχθεί με την “επίδειξη” τριών παραγόντων: κάτι που ο χρήστης γνωρίζει (π.χ. συνθηματικό), κάτι που ο χρήστης έχει στην κατοχή του (π.χ. κλειδί) η κάτι που ο χρήστης είναι, δηλαδή κάποιο βιομετρικό χαρακτηριστικό του (π.χ. ίριδα) [30].

Τυπικά, η αυθεντικοποίηση λαμβάνει χώρα μέσω διαδικτυακών εφαρμογών. Αφού ο χρήστης εισάγει στα πεδία τα διαπιστευτήρια (credentials), αυτά μεταφέρονται (ιδανικά μέσω κάποιου ασφαλούς πρωτοκόλλου, π.χ. HTTPS) στην εκάστοτε υπηρεσία. Στο πλαίσιο αυτής της διαδικασίας, οι πληροφορίες δεν μεταφέρονται σε αναγνωρίσιμη μορφή (plaintext), αλλά

κατακερματίζονται βάσει κάποιου αλγορίθμου (π.χ. SHA-256) ή συνάρτησης. Αποτέλεσμα είναι μια "σύνοψη" (hash) σταθερού μεγέθους. Αφού φτάσουν στην υπηρεσία, συγκρίνονται με την βάση δεδομένων της, στην οποία βρίσκονται αποθηκευμένες οι αποδεκτές "συνόψεις". Αν οι τιμές είναι ίδιες αποκτάται πρόσβαση στην υπηρεσία [31].

Καθώς μια σύνοψη δεν είναι αναστρέψιμη, η διαδικασία ανάκτησης περιστρέφεται γύρω από τον κατακερματισμό υποψήφιων συνθηματικών και την σύγκρισή τους με την σύνοψη του συνθηματικού του οποίου η ανάκτηση αποπειράται [32]. Αυτό συμβαίνει είτε με την τυφλή, διαδοχική και χρονοβόρα απόπειρα χρήσης όλων των πιθανών αλφαριθμητικών συνδυασμών (επίθεση εξαντλητικής αναζήτησης – brute force attack, CAPEC – 49), είτε μέσω της χρήσης λεξικών (dictionary attack, CAPEC - 16), δηλαδή λιστών συνθηματικών, οι οποίες μπορεί να προέρχονται από διαρροές πραγματικών συνθηματικών ή και να δημιουργηθούν από τον ίδιο τον επιτιθέμενο. Η επίσπευση της διαδικασίας μπορεί επίσης να επιτευχθεί μέσω πινάκων ουράνιου τόξου (rainbow tables, CAPEC – 55), δηλαδή λεξικών όπου πέραν των πιθανών συνθηματικών σε αναγνωρίσιμη μορφή περιέχεται και η σύνοψή τους [33]. Εναλλακτικά, ο επιτιθέμενος μπορεί να προσπαθήσει να χρησιμοποιήσει συχνά ή προεπιλεγμένα ονόματα χρήστη και συνθηματικά (Try Common or Default Usernames and Passwords, CAPEC – 70) ή και να δοκιμάσει έναν μικρό κατάλογο (π.χ. 3-5) συχνών ή αναμενόμενων συνθηματικών, τα οποία και συνάδουν με πολιτική πολυπλοκότητας του στόχου, εφόσον κάτι τέτοιο είναι γνωστό, έναντι ενός συγκεκριμένου καταλόγου λογαριασμών χρηστών (Password Spraying, CAPEC-565). Επιτυχής ανάκτηση του συνθηματικού και μετέπειτα χρήση του συνεπάγεται χρήση γνωστών διαπιστευτηρίων (use of known domain credentials, CAPEC – 560) και, εφόσον λείπουν μέτρα προστασίας όπως, π.χ. αυθεντικοποίηση πολλαπλών παραγόντων, πρόσβαση στο εκάστοτε σύστημα.

4.3.2. Τυπικές επιπτώσεις

Οι περιπτώσεις εισβολής κατόπιν χρήσης συνθηματικού οδηγούν τυπικά στην κατάλυση της εμπιστευτικότητας, της ακεραιότητας και ελλείψει σχετικών δικλείδων ασφάλειας και στην κατάλυση της διαθεσιμότητας μέσω περιορισμού της εξουσιοδοτημένης πρόσβασης του αρχικού χρήστη. Σε περίπτωση που ανακτηθεί συνθηματικό λογαριασμού που χαίρει ιδιαίτερων προνομίων, σχετική εισβολή μπορεί να οδηγήσει σε κατάλυση της διαθεσιμότητας ευρύτερης κλίμακας.

4.4. Επιθέσεις πλαστοπροσωπίας/πλαστογράφησης ταυτότητας

4.4.1. Περιγραφή

Η απειλή, η οποία και απαντάται στην βιβλιογραφία ως πλαστοπροσωπία (impersonation, [2]) είτε (και) ως πλαστογράφηση ταυτότητας (forgery, [22]) περιγράφει την περίπτωση που ο κακόβουλος τρίτος κρύβεται ως αυθεντικοποιημένος, "νόμιμος" χρήστης στο δίκτυο [2, 22]. Πρόκειται για εκφάνσεις της πλαστογράφησης ταυτότητας/πλαστοπροσωπίας (identity spoofing, CAPEC – 151), η οποία και αναφέρεται στην ανάληψη της ταυτότητας κάποιας άλλης οντότητας (ανθρώπινης ή μη) και στη συνέχεια της χρήσης αυτής της ταυτότητας για την επίτευξη ενός, εδώ κακόβουλου, στόχου.

4.4.2. Παράδειγμα από τον χώρο της υγείας

Ως παράδειγμα αναφέρεται από τους Newaz et al. [2] η εκμετάλλευση της ανασφαλούς επικοινωνίας ανάμεσα στην συσκευή παρακολούθησης γλυκόζης και του συστήματος χορήγησης ινσουλίνης για τη εξώρυξη του προσωπικού αριθμού αυθεντικοποίησης (Personal Identification Number – PIN), ο οποίος και σε ένα δεύτερο στάδιο χρησιμοποιήθηκε με αποτέλεσμα ο κακόβουλος τρίτος να λάβει την "θέση" του ασθενή.

4.4.3. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας οδηγούν σε κατάλυση της εμπιστευτικότητας και της ακεραιότητας.

4.5. Πλαστοπροσωπία μέσω κλωνοποίησης συσκευής

Η απειλή κλωνοποιημένων συσκευών αφορά σε ένα συνονθύλευμα επιθέσεων δικτύου, υλικού και πλαστοπροσωπίας.

4.5.1. Περιγραφή

Η επίθεση περιγράφει την περίπτωση πλαστοπροσωπίας σε επίπεδο υλικού, με απώτερο σκοπό την εκτέλεση περαιτέρω κακόβουλων ενεργειών στο εκάστοτε περιβάλλον [22]. Τυπικά ακολουθεί την κατάληψη κάποιου έγκυρου/"νόμιμου" κόμβου και την εξόρυξη τυπικά

κρυπτογραφημένων πληροφοριών από αυτόν, ενδεχομένως μέσω κάποιας επίθεσης παράπλευρου καναλιού (στην οποία θα επιστρέψουμε παρακάτω). Οι πληροφορίες αυτές χρησιμοποιούνται για την δημιουργία περισσότερων κλώνων στο δίκτυο, οι οποίοι με την σειρά τους μπορούν να χρησιμοποιηθούν στο πλαίσιο περαιτέρω επιθέσεων. Σε αντίθεση με τις επιθέσεις τύπου Sybil, τις οποίες μεταχειριστήκαμε παραπάνω, στην περίπτωση της κλωνοποίησης συσκευής κάθε κόμβος έχει μόνο μια ταυτότητα.

4.5.2. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας οδηγούν, όπως και στην περίπτωση πλαστοπροσωπίας/πλαστογράφησης ταυτότητας σε κατάλυση της εμπιστευτικότητας και της ακεραιότητας.

4.6. Επιθέσεις τύπου “Sniffing”

Η απειλή επιθέσεων τύπου “Sniffing” [4, 27], κατηγορία που περιλαμβάνει και την ανάλυση κυκλοφορίας δικτύου (traffic analysis [22]) αφορά στην χρήση υλικού και λογισμικού για την συλλογή της κυκλοφορίας του εκάστοτε δικτύου.

4.6.1. Οριοθέτηση της επίθεσης

Στο πλαίσιο της ανάλυσης ή αναχαίτισης κυκλοφορίας δικτύου (Interception, CAPEC – 117) η ενέργεια του κακόβουλου τρίτου περιορίζεται στην (παθητική) παρακολούθηση μιας ροής δεδομένων, η οποία μπορεί να ξεκινήσει από τον ίδιο τον τρίτο, από και προς το σύστημα-στόχο με αποκλειστικό σκοπό την συλλογή πληροφοριών. Σε αντίθεση με την απειλή τύπου “Man-in-The Middle” (CAPEC – 94), στην οποία θα επιστρέψουμε παρακάτω, ο επιτιθέμενος τοποθετείται ανάμεσα σε δύο τρίτες οντότητες αλλά δεν παραποιεί το περιεχόμενο των μηνυμάτων που ανταλλάσσονται και κατ’ επέκταση δεν προωθεί τα μηνύματα στον παραλήπτη. Η διαφορά με επιθέσεις τύπου “Sniffing” έγκειται στο ότι στην περίπτωση της αναχαίτισης κυκλοφορίας δικτύου ο επιτιθέμενος απλώς παρακολουθεί την επικοινωνία με απώτερο σκοπό τον προσδιορισμό της θέσης των βασικών κόμβων, της δομής δρομολόγησης, ή και του τρόπου συμπεριφοράς των σχετικών εφαρμογών, χωρίς να τον ενδιαφέρει το περιεχόμενο της. Αντιθέτως, στην περίπτωση του “Sniffing”, στόχος είναι το περιεχόμενο των μηνυμάτων [34].

4.6.2. Η ιδιαιτερότητα της κατηγορίας "υποκλοπή"

Στο πλαίσιο της βιβλιογραφίας η ίδια συμπεριφορά που ορίσαμε ως sniffing χαρακτηρίζεται και ως υποκλοπή (eavesdropping, CAPEC – 651). Κάτι τέτοιο, με την προσέγγισή μας εδώ, δεν μπορεί να ισχύει, καθώς υποκλοπή υπό την έννοια του CAPEC – 651 δεν πραγματοποιείται σε κανάλι επικοινωνίας που βασίζεται σε δίκτυο (π.χ. κίνηση IP). Αντίθετα, αφορά στην ακρόαση της ακατέργαστης ηχητικής πηγής μιας συνομιλίας (π.χ. κείμενο, ήχο, βίντεο) μεταξύ δύο ή περισσότερων μερών μέσω λογισμικού (π.χ. μικροφώνου και εφαρμογής καταγραφής ήχου), υλικού (π.χ. εξοπλισμού καταγραφής) ή φυσικών μέσων (π.χ. φυσική εγγύτητα). Παρόλα αυτά, η κατηγορία της υποκλοπής όπως αυτή νοείται από την βιβλιογραφία καθιστά την πιο σχολιασμένη απειλή [2, 3, 4, 5, 6, 21, 22, 23].

4.6.3. Παραδείγματα από τον χώρο της υγείας

Παραδείγματα από τον χώρο της υγείας δίνουν οι Newaz et al. [2], κατά τους οποίους διάφορες ιατρικές και φορητές συσκευές, όπως τα όργανα μέτρησης της αρτηριακής πίεσης και τα έξυπνα ρολόγια, πάσχουν από ευπάθειες που επιτρέπουν σε κάποιον κακόβουλο τρίτο να "υποκλέψει" ευαίσθητα δεδομένα προσωπικού χαρακτήρα αλλά και οι Yaqoob et al. [4], οι οποίοι απαριθμούν διάφορες ιατρικές συσκευές ευπαθείς σε τέτοιου τύπου επίθεση, όπως για παράδειγμα ένα οικιακό καρδιολογικό σύστημα παρακολούθησης, εξαιτίας ελλιπούς κρυπτογράφησης και σχετικής προστασίας στο πλαίσιο των πρωτοκόλλων επικοινωνίας.

4.6.4. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας καθιστούν τυπικά απειλή της εμπιστευτικότητας.

4.7. Επιθέσεις τύπου "Man-in-The Middle"

Μια άλλη κεντρική απειλή είναι οι επιθέσεις τύπου "Man-in-the-Middle" [2, 4, 22].

4.7.1. Περιγραφή

Περιγράφουν την περίπτωση που ο κακόβουλος τρίτος στοχοποιεί στην επικοινωνία μεταξύ δύο κόμβων προκειμένου να παραποιήσει ή να αποκτήσει πρόσβαση δεδομένα από την επικοινωνία τους. Τυπικά περιλαμβάνει την τοποθέτηση του αντιπάλου στο κανάλι επικοινωνίας μεταξύ των δύο κόμβων, με τα δεδομένα να περνούν πρώτα από τον αντίπαλο, ο οποίος και έχει την δυνατότητα να τα παρατηρήσει ή να τα τροποποιήσει, προτού τα προωθήσει στον

προοριζόμενο παραλήπτη. Αυτή η παρείσφρηση είναι συνήθως διαφανής, καθιστώντας τον εντοπισμό ενδεχόμενης αλλοίωσης ή διαρροής των επικοινωνιών δύσκολη. Οι επιθέσεις αυτές διαφέρουν από τις επιθέσεις της κατηγορίας "Sniffing" (CAPEC-157), δεδομένου ότι οι επιθέσεις τύπου "Man-in-The Middle" περιλαμβάνουν και την τροποποίηση της επικοινωνίας πριν την προώθησή της στον προβλεπόμενο παραλήπτη. Οι επιθέσεις επανάληψης (Replay Attacks) οι οποίες επίσης απαντώνται ως ξεχωριστή κατηγορία στην βιβλιογραφία [4, 6] και περιγράφουν την περίπτωση που ο κακόβουλος τρίτος επαναλαμβάνει ή καθυστερεί μια έγκυρη μετάδοση δεδομένων, είναι σύμφωνα με την θεώρηση μας στο πλαίσιο της παρούσας μεταπτυχιακής διατριβής μέρος των επιθέσεων τύπου "Man-in-The Middle".

4.7.2. Παραδείγματα από τον χώρο της υγείας

Στην βιβλιογραφία απαντώνται διάφορα παραδείγματα από τον χώρο της υγείας. Οι Hei et al. [35] παρουσίασαν μια επίθεση τύπου "Man-in-The Middle" όπου ο επιτιθέμενος παραβίασε την ασύρματη επικοινωνία μεταξύ μιας αντλίας ινσουλίνης και μιας συσκευής USB. Καθώς η επικοινωνία προς την αντλία ινσουλίνης δεν ήταν κρυπτογραφημένη, ο εισβολέας κατάφερε να προκαλέσει σήμα υπερδοσολογίας και σήμα χρόνιας υπερδοσολογίας. Το σήμα υπερδοσολογίας χορήγησε μια πολύ μεγάλη δόση άμεσα στον ασθενή, ενώ η χρόνια υπερδοσολογία οδήγησε στην χορήγηση επιπλέον δόσεων του φαρμάκου, για ευρύτερο χρονικό διάστημα.

Οι Paoletti et al. [36] παρουσίασαν μια τυπική προσέγγιση για την εκτέλεση επιθέσεων επαναπρογραμματισμού σε συσκευές κατηγορίας εμφυτεύσιμων καρδιομετατροπέων-απινιδωτών (Implantable cardioverter-defibrillators – ICDs). Οι ερευνητές επικεντρώθηκαν στο λογισμικό του ICD που υλοποιεί έναν αλγόριθμο διάκρισης για τον εντοπισμό περιστατικών αρρυθμίας βάσει ανάλυσης του καρδιακού ρυθμού του ασθενή. Η παραποίηση του αλγορίθμου διάκρισης σε αυτήν την περίπτωση συνεπάγεται και την πρόκληση ακατάλληλης θεραπείας ή και την παντελή έλλειψη χορήγησής της. Για την εκτέλεση αυτής της επίθεσης, ο κακόβουλος τρίτος πρέπει βέβαια να γνωρίζει το μοντέλο ICD του θύματος, ώστε να μπορεί να επιλέξει και κατ' επέκταση να τροποποιήσει τον αλγόριθμο διάκρισης που χρησιμοποιείται στην εκάστοτε περίπτωση.

4.7.3. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας καθιστούν απειλή για την εμπιστευτικότητα και την ακεραιότητα.

4.8. Επιθέσεις τύπου παραποίησης/τροποποίησης μηνυμάτων

Η απειλή παραποίησης/τροποποίησης μηνυμάτων αφορούν εδώ παραλλαγές επιθέσεων που αποσκοπούν την παραποίηση/τροποποίηση μηνυμάτων μεταξύ ιατρικών συσκευών και του εκάστοτε παρόχου υγειονομικής περίθαλψης [4, 5, 6, 22].

4.8.1. Περιγραφή

Η επίθεση αναφέρεται στην πλαστογράφηση περιεχομένου (Content spoofing, CAPEC-148), κατά την οποία ο κακόβουλος τρίτος τροποποιεί το περιεχόμενο ώστε να περιέχει κάτι διαφορετικό από αυτό που σκόπευε ο αρχικός δημιουργός/αποστολέας, διατηρώντας παράλληλα αμετάβλητη τη φαινομενική πηγή του εν λόγω περιεχομένου. Θα μπορούσε να παρουσιαστεί και ως το τελευταίο βήμα μιας επίθεσης τύπου "Man-in-The Middle" που είδαμε παραπάνω, χωρίς να συνδέεται άμεσα με την εν λόγω κατηγορία, καθώς εδώ το περιεχόμενο μπορεί να τροποποιηθεί μεν κατά τη μεταφορά (π.χ. υποκλοπή και τροποποίηση ενός μηνύματος μεταξύ αποστολέα και παραλήπτη) αλλά μπορεί να τροποποιηθεί και στην πηγή. Ο κακόβουλος τρίτος τυπικά προσπαθεί να αποκρύψει το γεγονός ότι το περιεχόμενο έχει τροποποιηθεί.

4.8.2. Παραδείγματα από τον χώρο της υγείας

Πολλαπλά παραδείγματα από τον χώρο της υγείας δίνουν οι Yaqoob et al. [4], οι οποίοι και απαριθμούν πιθανούς στόχους τέτοιας τύπου επίθεσης, με τις ιατρικές συσκευές (εμφυτεύσιμες και μη) να είναι στο επίκεντρο.

4.8.2. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας καθιστούν σημαντική απειλή για την εμπιστευτικότητα και ιδιαιτέρως την ακεραιότητα.

4.9. Επιθέσεις πλημμύρας/επανειλημμένης σύνδεσης

Η απειλή επιθέσεων πλημμύρας (Flooding, CAPEC - 125)/επανειλημμένης σύνδεσης (Sustained Client Engagement, CAPEC – 227) αφορούν σε επιθέσεις που είναι γνωστές ως επιθέσεις τύπου Denial of Service (DoS) και απαντώνται συχνά στην βιβλιογραφία [1, 3, 4, 5, 22, 23, 25, 26].

4.9.1. Περιγραφή

Οι επιθέσεις πλημμύρας αφορούν στην περίπτωση που ο κακόβουλος τρίτος καταναλώνει τους πόρους ενός στόχου μέσω αποστολής μεγάλου αριθμού αιτημάτων στο σύστημα – στόχο. Αυτός ο τύπος επίθεσης εκθέτει σε γενικές γραμμές μια αδυναμία του συστήματος – στόχου στον περιορισμό του ρυθμού ή της ροής των σχετικών αιτημάτων. Όταν η επίθεση αυτή είναι επιτυχής, εμποδίζει τους νόμιμους χρήστες από την αδιάκοπη πρόσβαση στην σχετική υπηρεσία και μπορεί να προκαλέσει έως και κατάρρευση του στόχου, καταλύοντας έτσι την διαθεσιμότητα του στόχου. Καθοριστικός για τις προοπτικές επιτυχίας επιθέσεων πλημμύρας είναι ο αριθμός των αιτημάτων που μπορεί να πραγματοποιήσει ο αντίπαλος σε μια δεδομένη χρονική περίοδο – όσο μεγαλύτερος είναι αυτός ο αριθμός, τόσο πιο πιθανό είναι να επιτύχει μια επίθεση εναντίον ενός συγκεκριμένου στόχου.

Στην περίπτωση επίθεσης επανειλημμένης σύνδεσης ο κακόβουλος τρίτος επιχειρεί να προκαλέσει και πάλι την κατάλυση της διαθεσιμότητας του εκάστοτε πόρου επιχειρώντας επανειλημμένα σύνδεση με αυτόν, σε μια προσπάθεια να τον κρατήσει δεσμευμένο για όσο το δυνατόν μεγαλύτερο διάστημα. Ο κύριος στόχος του κακόβουλου τρίτου δεν είναι να καταρρεύσει ή να κατακλύσει τον πόρο – στόχο, συμπεριφορά που θα ήταν ευκόλως ανιχνεύσιμη, αλλά έγκειται στην επανειλημμένη εκτέλεση ενεργειών ή στην κατάχρηση αλγοριθμικών ατελειών έτσι ώστε ο πόρος να παραμένει δεσμευμένος σε αλληλεπίδραση με τον κακόβουλο τρίτο και συνεπώς να μην είναι διαθέσιμος σε κάποιον άλλο, νόμιμο χρήστη. Ο βαθμός επιτυχίας της επίθεσης εξαρτάται από την ικανότητα του αντιπάλου να διατηρήσει τα αιτήματα σε βάθος χρόνου με όγκο που υπερβαίνει την κανονική χρήση από τους νόμιμους χρήστες, καθώς και από άλλες δυνάμει παθολογικές συνθήκες, όπως η (αν-)ικανότητα του στόχου να μετατοπίσει το φορτίο ή να αποκτήσει πρόσθετους πόρους για να αντιμετωπίσει την απόπειρα εξάντλησης. Αυτή η επίθεση διαφέρει από μια επίθεση πλημμύρας καθώς δεν εξαρτάται εξ ολοκλήρου από τον μεγάλο όγκο αιτημάτων.

4.9.2. Παραδείγματα από τον χώρο της υγείας

Ενδιαφέροντα παραδείγματα για τον χώρο της υγείας παρουσιάζουν συγκεντρωτικά οι Newaz et al. [2]:

- Μια συσκευή τύπου εμφυτεύσιμου καρδιομετατροπέα-απινιδωτή (Implantable cardioverter-defibrillator – ICD), για παράδειγμα, παραμένει σε κατάσταση αναμονής

για 5 λεπτά μετά την ενεργοποίηση, παρόλο που δεν υπάρχει ενεργή συνεδρία επικοινωνίας. Αυτός ο χρόνος αναμονής μπορεί να αξιοποιηθεί με την έναρξη ψευδών συνεδριών επικοινωνίας διατηρώντας έτσι το ICD σε κατάσταση αναμονής για μεγαλύτερο χρονικό διάστημα [37].

- Οι Ransford et al. ανέφεραν μια επίθεση σε συσκευές τύπου εμφυτεύσιμων καρδιακών ηλεκτρονικών συσκευών (Cardiac Implantable Electronic Devices – CIEDs), κατά την οποία οι επιτιθέμενοι στέλνουν προσεκτικά κατασκευασμένα πακέτα για να διαταράξουν τη συνδεσιμότητα ραδιοεπικοινωνία μιας συσκευής CIED, με αποτέλεσμα να σταματήσει η λειτουργία της συσκευής [38].

Επιθέσεις αυτής της κατηγορίας είναι, δεδομένης της εξαναγκαστικής διατήρησης του στόχου σε "ενεργή" κατάσταση, συχνά στενά συνυφασμένες και με την εξάντληση της μπαταρίας που τυπικά απαντάται σε ιατρικές συσκευές:

- Οι Raymond et al. [39] παρουσίασαν μια επίθεση "άρνησης ύπνου" (sleep deprivation), η οποία εκμεταλλεύεται το γεγονός πως επανειλημμένες απόπειρες αυθεντικοποίησης εμποδίζουν την ιατρική συσκευή από την εκκίνηση της τη διαδικασίας απενεργοποίησης, η οποία και προβλέπεται σε περίπτωση αποτυχημένης απόπειρας αυθεντικοποίησης, οδηγώντας έτσι στην εξάντληση της διάρκειας ζωής της μπαταρίας.

- Οι Hei et al. [40] παρουσίασαν μια επίθεση εξάντλησης της μπαταρίας σε εμφυτεύσιμη ιατρική συσκευή (Implantable Medical Device – IMD) εκμεταλλευόμενοι την ασύρματη επικοινωνία μεταξύ της συσκευής IMD και της συσκευής προγραμματιστή. Καθώς η συσκευή προγραμματιστή πρέπει να αυθεντικοποιηθεί στην συσκευή IMD, μια μη εξουσιοδοτημένη συσκευή προγραμματιστή μπορεί να στείλει επανειλημμένα αιτήματα αυθεντικοποίησης, εξαντλώντας έτσι την μπαταρία της συσκευής IMD.

4.9.3. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας καθιστούν απειλή για την διαθεσιμότητα.

4.10. Επιθέσεις παράπλευρου καναλιού

Η απειλή επιθέσεων παράπλευρου καναλιού (Side Channel Attacks) απαντώνται συχνά στην βιβλιογραφία [2, 3, 4, 21, 25].

4.10.1. Περιγραφή

Εξαρτάται από το αν ο κακόβουλος τρίτος έχει φυσική πρόσβαση στον εκάστοτε κόμβο – αν αυτή υπάρχει, μπορεί και να συνεπάγεται την δυνατότητα της εξόρυξης δεδομένων από αυτόν (λεγόμενη επίθεση πλάγιου καναλιού (Hardware Fault Injection / Side Channel Attack, CAPEC-624) με διάφορους τρόπους όπως εξέταση της ηλεκτρομαγνητικής δραστηριότητας γύρω από την εκάστοτε συσκευή, αναλύοντας τον χρονισμό κατανάλωσης ενέργειας ή κίνησης δεδομένων. Ενώ οι περισσότερες επιθέσεις αποσκοπούν στην εκμετάλλευση ευπαθειών των αλγορίθμων και πρωτοκόλλων που χρησιμοποιούνται από τον εκάστοτε κόμβο, οι οικογένεια επιθέσεων παράπλευρου καναλιού εστιάζουν στην εκμετάλλευση των στην εκμετάλλευση των φυσικών επιδράσεων των υπολογιστικών συσκευών κατά την κανονική λειτουργία τους για την εξαγωγή ευαίσθητων πληροφοριών, όπως για παράδειγμα κρυπτογραφικών κλειδιών και συνθηματικών [41]. Η διαρροή των σχετικών πληροφοριών μπορεί να συμβεί μέσω φυσικών παράπλευρων σημάτων, όπως στην περίπτωση ανάλυσης χρονισμού (timing analysis) (δηλ. ο χρόνος που απαιτείται για την εκτέλεση υπολογισμών), ανάλυση ισχύος (δηλ. τις διακυμάνσεις στην κατανάλωση ισχύος για την εκτέλεση υπολογισμών), ηλεκτρομαγνητική εκπομπή (δηλ. την ακτινοβολία που εκπέμπεται από το σύστημα για την εκτέλεση υπολογισμών) αλλά και μέσω ακουστικής ανάλυσης (δηλαδή ανάλυσης των ήχων που παράγονται κατά τη διάρκεια υπολογισμών) [15].

Οι επιθέσεις πλάγιου καναλιού καθιστούν δυνατές επιθέσεις αντίστροφης μηχανικής (reverse engineering, CAPEC – 188), κατά τις οποίες αφού ο κακόβουλος τρίτος ανακαλύψει ή εξορύξει την δομή, την λειτουργία και τη σύνθεση ενός αντικειμένου, ενός πόρου ή ενός συστήματος χρησιμοποιώντας τακτικές όπως οι επιθέσεις πλάγιου καναλιού, επιχειρεί να αντιγράψει ή να "επανασχεδιάσει" κάποια πτυχή της λειτουργίας του. Οι τεχνικές αντίστροφης μηχανικής μπορούν να εφαρμοστούν σε μηχανικά αντικείμενα, ηλεκτρονικές συσκευές ή λογισμικό, αν και η μεθοδολογία και οι τεχνικές που εμπλέκονται σε κάθε τύπο ανάλυσης διαφέρουν σημαντικά.

Συνδυαστικά, επιθέσεις τέτοιου τύπου μπορούν να οδηγήσουν σε αυτό που περιγράφεται στην βιβλιογραφία ως αλλοίωση αισθητήρα (sensor spoofing) [2, 4, 5], όπου ο κακόβουλος τρίτος μεταβάλλει το φυσικό περιβάλλον του αισθητήρα με τρόπο ώστε ένα ιατρικό σύστημα να συμπεριφέρεται με τρόπο που απέχει από τον σχεδιασμό του. Ενώ η αλλοίωση καθιστά έκφανση επίθεσης παράπλευρου καναλιού, η γνώση για τον ακριβή τρόπο λειτουργίας του αισθητήρα πολλές φορές πηγάζει από επιθέσεις αντίστροφης μηχανικής.

4.10.2. Παραδείγματα από τον χώρο της υγείας

Οι Zhang et al. [42] ανέφεραν μια επίθεση διαφορικής ανάλυσης ισχύος που μπορεί να εξάγει μυστικά κλειδιά από ιδιαιτέρως "θορυβώδη" κανάλια σε μια συσκευή παρακολούθησης καρδιακού ρυθμού η οποία χρησιμοποιεί συμμετρική κρυπτογράφηση. Η χρήση του αλγορίθμου AES για την κρυπτογράφηση του αποτελέσματος της μέτρησης καρδιακών παλμών πριν από τη προώθηση των δεδομένων. Ο κακόβουλος τρίτος μπορεί να ανακτήσει το μυστικό κλειδί που χρησιμοποιείται αναλύοντας τον τρέχοντα ρυθμό κατανάλωσης κατά τη μέτρηση των καρδιακών παλμών του ασθενή. Εάν το ίδιο κλειδί χρησιμοποιείται στο ίδιο μοντέλο όλων των συσκευών παρακολούθησης του καρδιακού ρυθμού, ο κακόβουλος τρίτος μπορεί να δημοσιοποιήσει το (κοινό) μυστικό κλειδί και έτσι να καταστήσει την κρυπτογραφική προστασία αναποτελεσματική για μεγάλο αριθμό συσκευών.

Ένα παράδειγμα αλλοίωσης αισθητήρα δίνουν οι Park et al. [43] στην περίπτωση αισθητήρα υπέρυθρης πτώσης (infrared drop – ID), ενσωματωμένου σε αντλία έγχυσης. Οι ερευνητές έδειξαν ότι ένας κακόβουλος τρίτος θα μπορούσε να εισάγει ένα *εξωτερικό* σήμα ισχύος για να να μπλοκάρει την απόκριση του αισθητήρα στις περιβαλλοντικές αλλαγές, με αποτέλεσμα την υπερ- ή υποδοσολογία φαρμάκου στον ασθενή. Η υπερδοσολογία οδήγησε στην έγχυση περίπου 333% της αρχικής δόσης του φαρμάκου, ενώ η υποδοσολογία οδήγησε σε έγχυση δόσης μειωμένης κατά 45% σε σχέση με την δόση σε κανονική λειτουργία.

4.10.3. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας καθιστούν απειλή για την εμπιστευτικότητα και την ακεραιότητα.

4.11. Επιθέσεις τροποποίησης κατά την κατασκευή/διανομή

Αυτή η οικογένεια απειλών εμφανίζεται στην βιβλιογραφία ως δούρειος ίππος υλικού (hardware trojan) [2, 21], όπου και περιγράφεται ως εισαγωγή δούρειου ίππου (μιας μορφής κακόβουλου λογισμικού, όπως είδαμε παραπάνω) στο υλικό της εκάστοτε συσκευής, με τον οργανισμό FDA να έχει δημοσιεύσει πολλαπλές αναφορές σχετικά με την συγκεκριμένη οικογένεια απειλών [2].

4.11.1. Περιγραφή

Πρόκειται για την περίπτωση τροποποίησης κατά την κατασκευή (Modification During Manufacture, CAPEC – 438) ή κατά την διανομή (Modification During Distribution, CAPEC – 439) συνήθως είτε με την μορφή εμφύτευσης κακόβουλου κώδικα κατά τον προγραμματισμό του ημιαγωγού (malicious code implanted during chip manufacture, CAPEC – 672) είτε μέσω της εμφύτευσης κακόβουλου λογισμικού κατά την διαδικασία διανομής (malicious software implanted, CAPEC – 523). Περιγράφει την περίπτωση όπου ο κακόβουλος τρίτος τροποποιεί μια τεχνολογία, ένα προϊόν ή ένα εξάρτημα κατά τη διάρκεια κάποιου σταδίου της κατασκευής ή της διανομής του με σκοπό την πραγματοποίηση επίθεσης εναντίον κάποιας οντότητας που εμπλέκεται με κάποιον τρόπο στον κύκλο ζωής της αλυσίδας εφοδιασμού (supply chain). Δεδομένης της ενδεχόμενης πρόσβασης του κακόβουλου τρίτου στην διαδικασία σύνθεσης του λογισμικού, στο σχεδιασμό και τη συναρμολόγηση του υλικού, στο υλικολογισμικό ή στους βασικούς μηχανισμούς σχεδιασμού, έχει απεριόριστες δυνατότητες να επιτύχει την όποια κακόβουλη τροποποίηση. Η επικίνδυνη αυτή κατάσταση εντείνεται καθώς πολλές φορές η κατασκευή βασικών εξαρτημάτων ανατίθεται σε εξωτερικούς συνεργάτες, ενώ το τελικό προϊόν συναρμολογείται από τον κύριο κατασκευαστή, επεκτείνοντας έτσι τα σημεία όπου ο κακόβουλος τρίτος μπορεί να παρεισφρήσει στην διαδικασία.

4.11.2. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας καθιστούν απειλή για την ακεραιότητα αλλά και την διαθεσιμότητα εξαιτίας της αναξιόπιστης λειτουργίας.

4.12. Επιθέσεις τροποποίησης υλικολογισμικού

Η απειλή επιθέσεων τροποποίησης υλικολογισμικού απαντάται τυπικά σε ιατρικές συσκευές [2, 4].

4.12.1. Περιγραφή

Η επίθεση αφορά στην τροποποίηση του υλικολογισμικού, η οποία με την σειρά της οδηγεί σε αλλαγή του τρόπου συμπεριφοράς της συσκευής [2, 4]. Ο κακόβουλος τρίτος μπορεί να επιτύχει την τροποποίηση του υλικολογισμικού με δυο τρόπους:

1. μέσω της επιμόλυνσης του συστήματος – στόχου με κακόβουλο λογισμικό το οποίο και έχει την δυνατότητα να τροποποιήσει το υλικολογισμικό (Altered Component Firmware, CAPEC – 638), προσέγγιση που συνήθως αφορά στο υλικό.

2. Εναλλακτικά, ένας κακόβουλος τρίτος με πρόσβαση στον μηχανισμό λήψης και ενημέρωσης λογισμικού του συστήματος μπορεί να στείλει κακόβουλα τροποποιημένο υλικολογισμικό / BIOS είτε άμεσα στο θύμα είτε στον προμηθευτή του θύματος (Altered Installed BIOS, CAPEC – 532).

Σε αυτό το πλαίσιο, ανεξάρτητα από την ύπαρξη σχετικών απειλών, θα πρέπει να τονιστεί πως καίριο πρόβλημα σε επίπεδο αδυναμίας είναι η χρήση υλικολογισμικού το οποίο και αναπτύσσεται από την εκάστοτε εταιρία για εφαρμογή στην εκάστοτε συσκευή διαδικτύου των (ιατρικών) πραγμάτων [12]. Αυτό σημαίνει πως πολλές φορές γίνονται αλλαγές π.χ. στον πυρήνα (kernel) του εκάστοτε ενσωματωμένου (embedded) λειτουργικού συστήματος, κάτι που καθιστά την ανανέωσή του δύσκολη, καθώς κάθε ανανέωση θα πρέπει να αναπτύσσεται από την εκάστοτε εταιρία – εγχείρημα δύσκολο δεδομένης της έκτασης που μπορεί να έχουν οι αλλαγές. Αυτό πολλές φορές οδηγεί στο να παραλείπονται ανανεώσεις του υλικολογισμικού, συνθήκη που επιτρέπει την ύπαρξη ευπαθειών λογισμικού για μεγάλα χρονικά διαστήματα. Επιπλέον, το γεγονός ότι σε τέτοιες περιπτώσεις ο κώδικας είναι ιδιόκτητος (proprietary) της εκάστοτε εταιρίας σημαίνει πως ευπάθειες μπορούν να περάσουν απαρατήρητες και πως, ουσιαστικά, η ασφάλεια του συστήματος εξαρτάται σχεδόν αποκλειστικά από την ικανότητα, τους πόρους και το χρονικό διάστημα υποστήριξης που προσφέρει η εταιρεία που το παρήγαγε.

4.12.3. Παραδείγματα από τον χώρο της υγείας

Στο πλαίσιο της υγείας, οι Hanna et al. [44] εξέτασαν έναν αυτόματο εξωτερικό απινιδωτή (AED) και εντόπισαν τέσσερεις ευπάθειες, συμπεριλαμβανομένου ενός μηχανισμού ενημέρωσης λογισμικού που δεν απορρίπτει υλικολογισμικό του οποίου η αυθεντικότητα δεν είναι εξακριβωμένη. Οι Rios et al. [45] πάλι έδειξαν ότι είναι δυνατή η ενημέρωση μη επαληθευμένου υλικολογισμικού μιας οικιακής συσκευής παρακολούθησης που είναι συνδεδεμένη με ένα ICD.

4.12.4. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας μπορούν, ανάλογα με την περίπτωση, να οδηγήσουν στην κατάλυση και των τριών πτυχών ασφάλειας.

4.13. Απειλές διεπαφών οικοσυστήματος

Στο πλαίσιο της ψηφιακής υγείας χρησιμοποιούνται πολλές φορές διεπαφές web, backend API, cloud και mobile, οι οποίες και πλήττονται συχνά από τα “αποτελέσματα” ανασφαλούς ή λανθασμένου προγραμματισμού αλλά και από επιθέσεις που εκτελούνται λόγω του τρόπου λειτουργίας των διαδικτυακών εφαρμογών.

4.13.1. Περιγραφή

Στην οικογένεια αυτή ανήκουν απειλές όπως Cross Site Scripting (XSS, CAPEC – 63), SQL Injection (CAPEC – 66) ή session hijacking (CAPEC – 593) [7]. Η ακριβής χαρτογράφηση καθίσταται δύσκολη, καθώς η απάντηση συγκεκριμένων απειλών σε αυτό το πλαίσιο εξαρτάται άμεσα από την υλοποίηση της εκάστοτε διαδικτυακής εφαρμογής.

4.13.2. Τυπικές επιπτώσεις

Δεδομένου του εύρους τους, απειλές αυτής της κατηγορίας μπορούν, ανάλογα με την περίπτωση, να οδηγήσουν στην κατάλυση και των τριών πτυχών ασφάλειας.

4.14. Απειλές σχετικές με το πρωτόκολλο Bluetooth

4.14.1. Περιγραφή

Στο πλαίσιο της βιβλιογραφίας απαντώνται αναφορές σε επιθέσεις στο πλαίσιο του πρωτοκόλλου Bluetooth [2, 46] με τους Zubair et al. [46] να παρουσιάζουν μια εκτενή λίστα πιθανών επιθέσεων. Ενδιαφέρουσες σε αυτό το πλαίσιο είναι οι εξής:

1. Επίθεση που οι Zubair et al. ονομάζουν MAC spoofing, η οποία απαντάται ως επίθεση πλαστοπροσωπίας Bluetooth (Bluetooth Impersonation AttackS (BIAS), CAPEC – 667), η οποία αφορά την περίπτωση που ο κακόβουλος τρίτος μεταμφιέζει την διεύθυνση MAC της συσκευής τους με δυνατότητες Bluetooth ως κάποια για την οποία υπάρχει μια ενεργή, έμπιστη σύνδεση και αυθεντικοποιείται επιτυχώς, παρεισφρέοντας έτσι στην επικοινωνία μεταξύ του θύματος και μιας άλλης οντότητας.

2. Επίθεση διαπραγμάτευσης κλειδιού Bluetooth (Key Negotiation of Bluetooth Attack (KNOB), CAPEC – 668), στο πλαίσιο της οποίας ο κακόβουλος τρίτος εκμεταλλεύεται ένα ελάττωμα στη διαπραγμάτευση κλειδιών Bluetooth, το οποίο του επιτρέπει να αποκρυπτογραφήσει πληροφορίες που ανταλλάσσονται μεταξύ δύο συσκευών που επικοινωνούν μέσω Bluetooth, αλλά και να τροποποιήσει τα πακέτα που ανταλλάσσονται (συγκεκριμένα τα bits εντροπίας) μεταξύ των δύο συσκευών κατά τη διαδικασία ελέγχου ταυτότητας.

3. Επίθεση τύπου “BlueSmacking” (CAPEC – 666), η οποία και ουσιαστικά αποτελεί μορφή επίθεσης πλημμύρας, η οποία εδώ εκτελείται μέσω του πρωτοκόλλου L2CAP (το οποίο και χρησιμοποιείται στο πλαίσιο της στοίβας πρωτοκόλλου Bluetooth), και η οποία, όπως οι “τυπικές” επιθέσεις πλημμύρας οδηγεί σε κατάσταση τύπου Denial of Service (DoS).

4.14.2. Τυπικές επιπτώσεις

Επιθέσεις αυτής της κατηγορίας μπορούν και πάλι, ανάλογα με την περίπτωση, να οδηγήσουν στην κατάλυση και των τριών πτυχών ασφάλειας.

4.15. Ομάδα απειλών κοινωνικής μηχανικής

Ο ασθενέστερος κρίκος στην αλυσίδα ασφάλειας κάθε συστήματος είναι ο άνθρωπος – χρήστης [47]. Αυτή η αναπόφευκτη παθολογική κατάσταση καθιστά ιστορικά, με ένα από τα πρώιμα λογοτεχνικά – μυθολογικά παραδείγματα που απαντάται στην ομηρική Ιλιάδα με την μορφή του Δούρειου Ίππου [48, 49], μια εκμεταλλεύσιμη διαπίστωση κακόβουλων τρίτων ή δυνάμει επιτιθέμενων, οι οποίοι και πολλές φορές επιχειρούν να διεισδύσουν στο εκάστοτε σύστημα – στόχο εκμεταλλευόμενοι κατά κόρον ψυχολογικά τους χρήστες του και κατ' επέκταση τις ελλιπείς γνώσεις τους σχετικά με ζητήματα ασφάλειας σε αντίθεση με την αμιγώς τεχνολογική προσέγγιση αναζήτησης ευπαθειών στην υποδομή, το δίκτυο και τους κόμβους του συστήματος – στόχου.

4.15.1. Εννοιολογική προσέγγιση και σχολιασμός

Η οικογένεια απειλών που ταυτίζεται με μια τέτοιου τύπου ανθρωποκεντρική προσέγγιση είναι οι επιθέσεις κοινωνικής μηχανικής. Αν ανατρέξουμε στο Λεξικό της Κοινής Νεοελληνικής [98], ο όρος "κοινωνική" αναφέρεται στις σχέσεις των ανθρώπων μεταξύ τους μέσα στην κοινωνία, ενώ "μηχανική" ορίζεται ως κλάδος της φυσικής που μελετά την κίνηση των σωμάτων. Αν συνδυάσουμε τους δύο όρους, κοινωνική μηχανική θα μπορούσε να οριστεί ως η επιστήμη της χειραγώγησης ανθρώπων για να προχωρήσουν σε κάποια "κίνηση", δηλαδή, σε αυτό το πλαίσιο σε κάποια ενέργεια η παράλειψη. Την κακόβουλη κατεύθυνση μιας τέτοιας χειραγώγησης υιοθετεί το γλωσσάριο του NIST [89] στο σχετικό λήμμα του, όπου και ορίζει την κοινωνική μηχανική ως την "απόπειρα εξαπάτησης κάποιου ατόμου ώστε να αποκαλύψει πληροφορίες (π.χ. συνθηματικά), οι οποίες μπορούν να χρησιμοποιηθούν για επιθέσεις σε συστήματα ή δίκτυα".

Στην εννοιολογική προσέγγιση του NIST παρατηρούνται ωστόσο, κατά τη γνώμη μας, δυο ελλείψεις: αφενός ο ορισμός του περιορίζει το αποτέλεσμα στην εκμαίευση πληροφοριών με σκοπό την ενδεχόμενη χρήση τους στο πλαίσιο περαιτέρω επιθέσεων και αφετέρου εντατικοποιεί την επενέργεια στο θύμα σε "απόπειρα εξαπάτησης". Ενώ μια τέτοια προσέγγιση ίσως καθιστά την τυπική έκφανση επιθέσεων κοινωνικής μηχανικής, το εύρος τους είναι πολύ μεγαλύτερο καθώς μπορεί να περιλαμβάνει, πέραν της συλλογής πληροφοριών, την απόκτηση πρόσβασης στο εκάστοτε σύστημα ή την παρακίνηση του χρήση στο να προβεί σε κάποια ενέργεια, π.χ. στην χρήση κάποιου εξωτερικού αποθηκευτικού μέσου [50] ή και παράλειψη.

Ενδιαφέρουσα είναι επιπλέον η επιλογή της μεθόδου, εδώ ο περιορισμός στην "εξαπάτηση", έννοια που προσάπτεται στην αντίληψη του θύματος και όχι στο συμφέρον του. Μια τέτοιου τύπου διάκριση είναι σημαντική, καθώς τα συμφέροντα του εκάστοτε χρήστη πολλές φορές δεν είναι απαραιτήτως παράλληλα με αυτά του οργανισμού. Συνεπώς, πολλές φορές η κοινωνική μηχανική είναι μέθοδος που λειτουργεί και ως εκκολαπτήριο εσωτερικών απειλών, είτε μέσω ιδεολογικής επιρροής, χρηματικού οφέλους ή εκβιασμού. Άλλες φορές πάλι περιορίζεται στην οπλοποίηση του – έστω αφελούς – χρήστη ως – πολλές φορές άδολου – εργαλείου το οποίο και επιφέρει το εκάστοτε αντίξοο αποτέλεσμα.

Θα μπορούσαμε λοιπόν να επεκτείνουμε τον ορισμό του NIST ως εξής: "Κοινωνική μηχανική είναι η πράξη ψυχολογικής επενέργειας στον χρήστη κάποιου συστήματος με απώτερο σκοπό την χειραγώγηση του στο να προβεί σε κάποια ενέργεια ή παράλειψη, η οποία και δεν ανταποκρίνεται απαραίτητα στα συμφέροντά του [51].

4.15.2. Επιθέσεις ηλεκτρονικού ψαρέματος

Η πιο συνηθισμένη τεχνική κοινωνικής μηχανικής είναι επιθέσεις τύπου ηλεκτρονικού ψαρέματος (phishing) σε όλες του τις εκφάνσεις [9]. Σε επίπεδο ορολογίας απαντώνται και πάλι διαφορετικές προτάσεις, με το γλωσσάρι του NIST να ορίζει (ή, κατά την άποψη του συγγραφέα εδώ να περιορίζει) το phishing ως την εξαπάτηση χρηστών με σκοπό την αποκάλυψη ευαίσθητων προσωπικών δεδομένων μέσω παραπλανητικών ηλεκτρονικών μέσων [89]. Η χαρτογράφηση του οργανισμού MITRE στο πλαίσιο του εγχειρήματος CAPEC συμφωνεί με τον περιορισμό του phishing στην εκμαίευση πληροφοριών και το διαχωρίζει από άλλες σχετικές δραστηριότητες, τις οποίες και οργανώνει σε επιπλέον κατηγορίες όπως π.χ. επιθέσεις ακεραιότητας λογισμικού (CAPEC-184) ή παραποίηση ενεργειών (CAPEC-173). Εδώ θα ακολουθήσουμε την αντίληψη του phishing όπως αυτή απαντάται στο κύριο εγχείρημα του οργανισμού MITRE, την βάση γνώσεων ATT&CK [95], σύμφωνα με την οποία το phishing αποσκοπεί στην πρόσβαση στα συστήματα των θυμάτων, με όλες τις μορφές phishing να καθιστούν ηλεκτρονικά διανεμόμενη κοινωνική μηχανική.

4.15.3. Περιγραφή της τεχνικής

Πρόκειται για τεχνική, η οποία πρωτίστως στηρίζεται στην παραποίηση ταυτότητας (identity spoofing) κάποιας πραγματικής, εμπιστεύσιμης, όχι απαραίτητα φυσικής οντότητας εκ μέρους του κακόβουλου τρίτου και στην μετέπειτα χρήση της ταυτότητας αυτής για πετύχει τον

εκάστοτε κακόβουλο σκοπό του [52], π.χ. μέσω της κατασκευής μηνυμάτων τα οποία φαίνεται να πηγάζουν από κάποιον εμπιστεύσιμο τρίτο. Εναλλακτικά, ο κακόβουλος τρίτος μπορεί να αναχαιτίσει πραγματικά μηνύματα και να παραποιήσει την ταυτότητα του αποστολέα σε αυτήν του κακόβουλου τρίτου, χωρίς όμως να μεταβάλλει το περιεχόμενο τους, κάτι που απαντάται για παράδειγμα στο πλαίσιο απόπειρας εκμαίευσης έγκυρων στοιχείων αυθεντικοποίησης από τον χρήστη, όπως είδαμε παραπάνω, ή κατά την διαδικασία εγκαθίδρυσης μιας σχέσης εμπιστοσύνης με αυτόν.

Σε ένα δεύτερο στάδιο – το οποίο μπορεί να είναι μέρος του ίδιου μηνύματος – ο κακόβουλος τρίτος επιχειρεί:

1. να μεταμφιέσει κάποια κακόβουλη πράξη (π.χ. κάποιον σύνδεσμο που οδηγεί σε ιστοσελίδα που ελέγχεται από τον κακόβουλο τρίτο) και να εξαπατήσει τον χρήστη στο να προχωρήσει σε αυτήν, πιστεύοντας πως πράττει κάτι άλλο. Η εξαπάτηση πραγματοποιείται είτε κοινωνικά, δηλαδή λεκτικά μέσω του μηνύματος ή στηρίζεται στην φυσική τάση του αφελούς σε θέματα ασφάλειας χρήστη να δράσει με έναν συγκεκριμένο τρόπο (π.χ. να κατεβάσει/ανοίξει κάποιο αρχείο σχετικό με δεδομένα οικονομικού χαρακτήρα), είτε μέσω τεχνικών μέσων, π.χ. μέσω της χρήσης μεθόδων όπως το “clickjacking”, όπου το θύμα νομίζει πως διαδρά με μια συγκεκριμένη επιφάνεια ενώ στην πραγματικότητα διαδρά με μια διαφανή/αόρατη στρώση η οποία οδηγεί και σε διαφορετικά αποτελέσματα.

2. να προχωρήσει στην εκμαίευση πληροφοριών από το θύμα. Η επιτυχία αυτής της προσέγγισης βασίζεται στην σωστή προετοιμασία της επίθεσης, με ικανοποιητική συλλογή πληροφοριών ανοικτών (η όχι) πηγών τόσο σχετικά με το θύμα όσο και με το περιβάλλον του και τον οργανισμό στον οποίο εργάζεται. Η ποιότητα των πληροφοριών παίζει σημαντικό ρόλο στις πιθανότητες επιτυχίας της επίθεσης.

Στο πλαίσιο και των δύο προσεγγίσεων μπορεί να χρησιμοποιηθεί η τακτική της ανάπτυξης προσχημάτων ("pretexting"), δηλαδή η ανάπτυξη ενός φανταστικού σεναρίου, την υιοθέτηση μιας διαφορετικής ταυτότητας ή ρόλου (π.χ. μέλος της ομάδας ασφάλειας του οργανισμού, τεχνικός ηλεκτρονικών υπολογιστών, καθαριστής, διευθυντής θυγατρικού καταστήματος, γενικός διευθυντής του οργανισμού κ.α.) από τον κακόβουλο τρίτο ώστε να πείσει το θύμα να παρέχει πληροφορίες ή να προβεί σε κάποια πράξη/παράλειψη.

4.15.4. Πιθανοί Στόχοι

Κάθε χρήστης του συστήματος με την ευρεία έννοια, δηλαδή συμπεριλαμβανομένων και των διαχειριστών, μπορεί να είναι στόχοι κάποιας εκστρατείας phishing. Η επιλογή των στόχων, ο αριθμός τους και η επένδυση του δράστη στην ποιότητα των μηνυμάτων καθορίζει και την τυπολογία της επίθεσης. Απαντώνται οι εξής κατηγορίες:

1. “απλή” επίθεση phishing: ο δράστης στοχοποιεί μεγάλο αριθμό δυνάμει θυμάτων, τυπικά χρησιμοποιώντας κάποιο γενικό μήνυμα. Στο πλαίσιο αυτής της προσέγγισης ο δράστης υπολογίζει πως ο μεγάλος αριθμός στόχων θα οδηγήσει σε πιθανώς επιτυχημένα περιστατικά της επίθεσης. Επενδύει συνεπώς στην ποσότητα και όχι στην ποιότητα των μηνυμάτων.

2. Επίθεση τύπου “spear phishing”: Σε αυτήν την παραλλαγή ο δράστης στοχοποιεί κάποιον συγκεκριμένο χρήστη η κάποια συγκεκριμένη ομάδα χρηστών. Χαρακτηρίζεται από πιο προσεκτικά κατασκευασμένα μηνύματα, συνήθως με παραποίηση του αποστολέα ώστε να φαίνεται πως προέρχονται από κάποια έμπιστη οντότητα. Εφόσον ο δράστης έχει πρόσβαση σε κάποιον έγκυρο λογαριασμό του οργανισμού, το μήνυμα ενδέχεται να είναι και ψηφιακά υπογεγραμμένο. Οι πιθανότητες επιτυχίας της επίθεσης αυξάνονται ανάλογα με το πόσο συγκεκριμένο, και κατ' επέκταση πειστικό είναι το μήνυμα. Σε αυτό το πλαίσιο η ποιότητα των πληροφοριών που (ιδανικά) συνέλλεξε ο δράστης πριν την εκτέλεση της επίθεση καθορίζει και τις πιθανότητες επιτυχίας.

3. Επίθεση τύπου “whaling”: Σε αυτήν την παραλλαγή ο στόχος είναι τυπικά κάποιο ιδιαίτερα σημαντικό για τον σκοπό του δράστη άτομο με ιδιαίτερη, σχετική για τον σκοπό του δράστη, δύναμη στο πλαίσιο του οργανισμού.

4.15.5. Τρόπος διανομής των μηνυμάτων phishing

Ο συνηθέστερος τρόπος διανομής των μηνυμάτων είναι μέσω ηλεκτρονικού ταχυδρομείου (e-mail). Εναλλακτικά, ο δράστης μπορεί να χρησιμοποιήσει μηνύματα SMS, χωρίς αυτό να επηρεάζει το περιεχόμενο του μηνύματος, αλλά και ομιλία (Voice Phishing/Vishing), είτε ίδια είτε προκατασκευασμένη μέσω σχετικού λογισμικού, με απώτερο σκοπό την προσομοίωση της φωνής κάποιου ατόμου, το οποίο και το δυνάμει θύμα θα αναγνωρίσει (deepfake) [53]. Η

διαφορά στην περίπτωση του vishing είναι πως το θύμα συνήθως επικοινωνεί τις πληροφορίες λεκτικά.

4.15.6. Παραδείγματα από τον χώρο της υγείας

Στο πλαίσιο της ψηφιακής υγείας περιστατικά phishing είναι αρκετά συνηθισμένα, με ιδιαίτερη αύξηση εξαιτίας της πανδημίας COVID-19 και των νέων συνθηκών τηλεργασίας που αυτή επέφερε [54, 55, 56]. Απαντώνται επίσης πολλαπλά περιστατικά, στα οποία δράστες απέκτησαν πρόσβαση σε νοσοκομειακά πληροφοριακά συστήματα μέσω επιθέσεων ηλεκτρονικού ψαρέματος [57, 58, 59].

4.15.7. Τυπικές επιπτώσεις

Επιθέσεις αυτής της οικογένειας μπορούν να οδηγήσουν στην κατάλυση της εμπιστευτικότητας και της ακεραιότητας, ενώ ανοίγουν την πόρτα σε πιο σοβαρές επιθέσεις οι οποίες και μπορούν να αφορούν και τις τρεις πτυχές ασφάλειας, όπως στην περίπτωση κακόβουλου λογισμικού που μεταχειριστήκαμε παραπάνω.

4.16. Σχετικά σχόλια

Αυτό που παρατηρείται εξετάζοντας την κωδικοποίηση των απειλών που απαντώνται στην βιβλιογραφία είναι πως κάθε μια από αυτές μπορεί να αντιστοιχηθεί σε κάποιο ή κάποια CAPEC, πράγμα που με την σειρά του σημαίνει πως οι απειλές δεν είναι μοναδικές στο πλαίσιο της ψηφιακής υγείας, αλλά είναι κοινές με τις απειλές κυβερνοασφάλειας που θα μπορούσαν να αφορούν σε διαφορετικούς χώρους.

Συνέπεια αυτού του συμπεράσματος είναι πως η θεώρηση μας κατά την προσέγγιση των επιπτώσεων των επικινδυνοτήτων στην υγεία των ασθενών και κατ' επέκταση κατά την ανάπτυξη μιας προσέγγισης προτεραιοποίησης των επικινδυνοτήτων αυτών δεν θα πρέπει να περιοριστεί στις 15 απειλές και επιθέσεις που εντοπίστηκαν στο πλαίσιο του παρόντος κεφαλαίου, καθώς αυτές αποτελούν έναν επιβεβαιωμένο μεν, αλλά μικρό αριθμό απειλών και επιθέσεων που αντικειμενικά θα μπορούσαν να διακινδυνεύσουν την ασφάλεια των ασθενών.

Κεφάλαιο 5
Εξάρτηση της υγείας των ασθενών από τις επικινδυνότητες κυβερνοασφάλειας

Στο πλαίσιο κεφαλαίου 5 θα παρουσιαστούν οι επιπτώσεις που θα μπορούσαν να έχουν οι επικινδυνότητες κυβερνοασφάλειας στην ασφάλεια των ασθενών. Αφού αρχικά ορίσουμε το αντικείμενο προστασίας και το εύρος των πιθανών επιπτώσεων στην ασφάλεια των ασθενών (5.1.), θα προσδιορίσουμε τους πιθανούς τύπους απειλών (5.2.) και τα ζητήματα προστασίας που προκύπτουν από αυτούς (5.3.). Έπειτα θα προχωρήσουμε στο πρόβλημα της σύγκλισης της σιγουριάς (safety) ως προστασίας της υγείας των ασθενών και της ασφάλειας (security) των συστημάτων ψηφιακής υγείας που υποστηρίζουν διεργασίες υγείας (5.4.). Τέλος, θα αντιστοιχήσουμε τις επικινδυνότητες κυβερνοασφάλειας στην ασφάλεια των ασθενών (5.5.).

5.1. Αντικείμενο προστασίας των ασθενών

5.1.1. Ορισμοί

Το αγαθό, την εξασφάλιση του οποίου αποσκοπούμε εδώ, είναι πρωτίστως η σιγουριά των ασθενών υπό την έννοια της προστασίας της υγείας τους από σχετικές βλάβες, συμπεριλαμβανομένης και της απώλειας ζωής. Κρίσιμος σε αυτό το σημείο είναι ο προσδιορισμός του όρου “υγεία”. Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας [84], υγεία είναι η κατάσταση της πλήρους σωματικής, ψυχικής και κοινωνικής ευεξίας, και όχι απλώς η απουσία ασθένειας η αναπηρίας.

Σκοπός της σιγουριάς των ασθενών (patient safety) στο πλαίσιο ενός περιβάλλοντος υγείας είναι λοιπόν ο περιορισμός του κινδύνου τραυματισμού ή της πρόκλησης βλάβης στην υγεία

των ασθενών εξαιτίας της ψηφιακής υποδομής και των διεργασιών υγείας στο πλαίσιο της ιατρικής περίθαλψης [61].

Σε δεύτερο επίπεδο, η επιτυχής προστασία της υγείας των ασθενών σε ένα τέτοιο πλαίσιο συνεπάγεται και την επιδότηση της κυβερνοασφάλειας του εκάστοτε συστήματος υγείας στο οποίο οι ασθενείς αυτοί υπάγονται.

5.1.2. Κλίμακα επιπτώσεων στην υγεία των ασθενών

Για να ορίσουμε το εύρος ή την σοβαρότητα των επιπτώσεων επικινδυνοτήτων κυβερνοασφάλειας στην ασφάλεια των ασθενών, ανεξαρτήτως της μεθόδου αντιστοίχισης την οποία θα μεταχειριστούμε παρακάτω, και δεδομένης της δυνατότητας πρόκλησης βλάβης, ο οργανισμός FDA [60] προτείνει στο πλαίσιο συστάσεων σε κατασκευαστές ιατρικών συσκευών μια ποιοτική προσέγγιση προσδιορισμού της βαρύτητας των επιπτώσεων στην υγεία του ασθενή κατά την εκτέλεση σχετικών ελέγχων ασφάλειας, βάσει των επιπέδων σοβαρότητας, όπως αυτή περιγράφεται στο πλαίσιο του ISO 14971 (2019) [85] και επεκτείνεται από το IEC/TR 80001-2-2 (2012) [86]. Η προσέγγιση αυτή περιλαμβάνει μια κλίμακα επιπτώσεων η οποία κυμαίνεται από αμελητέα (ταλαιπωρία ή προσωρινή δυσφορία) έως και καταστροφική (απώλεια ζωής). Σε αυτή τη διατριβή υιοθετούμε μια διασκευή αυτής της προσέγγισης, όπως παρουσιάζεται στην εργασία [60], η οποία παρατίθεται στον πίνακα 5.1.

Επίπεδο επίπτωσης	Περιγραφή επίπτωσης στην υγεία των ασθενών
Αμελητέα	Πρόκληση αναστάτωσης ή προσωρινής δυσφορίας.
Χαμηλή	Πρόκληση προσωρινού τραυματισμού ή βλάβης που δεν απαιτεί επαγγελματική ιατρική παρέμβαση.
Σοβαρή	Πρόκληση τραυματισμού ή βλάβης που απαιτεί επαγγελματική ιατρική παρέμβαση.

Κρίσιμη	Πρόκληση μόνιμης βλάβης ή τραυματισμού που απειλεί την ζωή.
Καταστροφική	Πρόκληση θανάτου του ασθενή.

Πίνακας 5.1: Κλίμακα επιπτώσεων στην υγεία των ασθενών (πηγή: [60])

5.2. Τύποι απειλών

Σε ένα δεύτερο βήμα θα πρέπει να προσδιορίσουμε τους πιθανούς τύπους απειλών για τα προς προστασία αγαθά. Αυτό σημαίνει πως θα πρέπει να προσδιοριστούν οι κατηγορίες δυνάμει δραστών, όπως αυτές απαντώνται στο πλαίσιο της κυβερνοασφάλειας. Ο προσδιορισμός αυτός είναι σημαντικός, καθώς η κάθε κατηγορία συνεπάγεται τυπικά και διαβαθμιζόμενες ικανότητες, κίνητρα και πόρους, συνθήκες που καθορίζουν εν μέρει το εύρος και τις ανάγκες αμυντικών μέτρων στην εκάστοτε περίπτωση. Σχετικές κατηγορίες στο πλαίσιο που εξετάζουμε, με αύξουσες ικανότητες και πόρους, είναι οι εξής (πρβλ. και την ταξινόμηση του Piggin [62]):

1. “απλοί” ή “τυπικοί” κυβερνοεγκληματίες, οι οποίοι και ενεργούν είτε για την πρόκληση, για την προώθηση κάποιας ατζέντας, είτε για οικονομικό όφελος,

2. πιθανές εσωτερικές απειλές, δηλαδή είτε υπαλλήλους είτε προμηθευτές, οι οποίοι και έχουν είτε απεριόριστη είτε λιγότερο περιορισμένη πρόσβαση στο εκάστοτε σύστημα και ενεργούν είτε εκούσια, για παράδειγμα λόγω κάποιας δυσαρέσκειας, είτε ακούσια λόγω λάθους.

   Η αυξημένη επικινδυνότητα στο πλαίσιο εσωτερικών απειλών πηγάζει από την συνθήκη είτε ακούσιας ύπαρξής τους είτε εκούσιας τοποθέτησής τους σε θέση με αναβαθμισμένη πρόσβαση – η κατάσταση αυτή καθιστά την κατηγορία εσωτερικών απειλών ιδιάζουσα καθώς άτομα σε τέτοιες θέσεις μπορούν να αποτελέσουν τα ίδια στόχο ανθρωποκεντρικών επιθέσεων της γενικότερης κατηγορίας κοινωνικής μηχανικής. Μια επιτυχής τέτοιου τύπου ανθρωποκεντρική επίθεση είναι τυπικά πιο οικονομική για τον επιτιθέμενο και αποκόπτει ταυτόχρονα τα ίσως πιο χρονοβόρα ή επίπονα βήματα που

θα έπρεπε να λάβει ως εξωτερική οντότητα για να βρεθεί σε αντίστοιχη θέση προνομιακής πρόσβασης.

3. Προηγμένες Επίμονες Απειλές (Advanced Persistent Threats – APTs), δηλαδή καλά εκπαιδευμένοι, συνήθως κρατικά ελεγχόμενοι επιτιθέμενοι όπως για παράδειγμα ξένες υπηρεσίες πληροφοριών, οι οποίοι και λειτουργούν με ιδιαίτερα στοχευμένο τρόπο, με σκοπό την κατασκοπεία ή το σαμποτάζ, συνήθως για μεγάλο χρονικό διάστημα [63].

5.3. Ζητήματα προστασίας

Σε αυτό το σημείο θα πρέπει να τονιστεί η σημασία της εναρμόνισης των κινήτρων και των στόχων των δυνάμει επιτιθέμενων με τις δυνατότητες τους, ιδιαίτερα στο πλαίσιο της περιορισμένης, εδώ, οπτικής γωνίας μας, η οποία και αφορά στην σιγουριά των ασθενών, με την ασφάλεια πληροφοριών να παίζει έναν σημαντικό μεν, αλλά δευτερεύοντα ή υποστηρικτικό ρόλο – μια σχέση στην οποία θα επιστρέψουμε παρακάτω.

Ενώ λοιπόν η τυπική κυβερνοεπίθεση αφορά πρωτίστως σε δεδομένα [64], κυβερνοεπιθέσεις που αφορούν *στοχευμένα* στην πρόκληση ζημιάς στην υγεία ή και στην απώλεια ζωής αποκτούν μια διαφορετική χροιά μιας και πλέον περνούν στο πεδίο στοχευμένης βίας. Δεδομένων των τυπικών πολιτικών ή στρατηγικών κινήτρων που χαρακτηρίζουν την κορυφή της πυραμίδας απειλών, δηλαδή τις κρατικά κατευθυνόμενες ή τις κρατικές προηγμένες επίμονες απειλές, αύξουσες ικανότητες/πόροι είναι λοιπόν αντιστρόφως ανάλογες με τον προσδοκώμενο αριθμό “φυσικών” θυμάτων και κατά συνέπεια ο κίνδυνος για το *σύνολο* των ασθενών δεν αυξάνεται γραμμικά με την ικανότητα και τους πόρους του επιτιθέμενου.

Διαφορετική θα ήταν η περίπτωση που εξετάζεται η στοχευμένη αποσταθεροποίηση κρατικών συστημάτων υγείας σε περίπτωση κρατικών/κρατικώς κατευθυνόμενων προηγμένων επίμονων απειλών (στην οποία περίπτωση έχουμε περάσει σε κυβερνοπόλεμο (Cyberwar)), με την οποία δεν θα ασχοληθούμε εδώ.

Σε αυτό το σημείο τίθεται βέβαια το εύλογο ερώτημα με ηθικές προεκτάσεις, σχετικά με την ανάγκη μιας τέτοιας διαβάθμισης, ή, με άλλα λόγια, σχετικά με το γιατί να μην αποσκοπείται η προστασία όλων των πιθανών θυμάτων με την ίδια αποτελεσματικότητα, εφόσον πρόκειται για τα σημαντικότατα αγαθά της υγείας και της ζωής.

Μια τέτοια καθολική και ομοιόμορφη προστασία θα ήταν βέβαια ιδανική, δεν είναι όμως βιώσιμη καθώς θα ήταν με την σειρά της σπάταλη για δύο λόγους: αφενός καθίσταται δύσκολα πρακτικά πραγματοποιήσιμη, μιας και η ασφαλέστερη υλοποίηση συνεπάγεται συνήθως και σημαντικά αυξημένο κόστος και αφετέρου αντιτίθεται στην γενικότερη αρχή της ανάγκης καταλληλότητας των εκάστοτε μέτρων προστασίας. Καταλληλότητα σε αυτό το πλαίσιο σημαίνει πως το εκάστοτε μέτρο θα πρέπει να αντιμετωπίζει αποτελεσματικά τον εκάστοτε κίνδυνο έναντι του οποίου υιοθετείται και πως δεν θα πρέπει να είναι δυσανάλογο σε σχέση με αυτόν. Κατ' επέκταση, η ασφάλεια σε περιπτώσεις που οι ανάγκες της ξεπερνούν τα "τυπικώς" αναμενόμενα καθιστά προσωποποιημένη υπηρεσία και εξαρτάται από τις εξατομικευμένες ανάγκες του δυνάμει θύματος. Ένας τυπικός ασθενής, για παράδειγμα, δεν χρειάζεται αποτελεσματική προληπτική προστασία έναντι σε προηγμένες επίμονες απειλές, καθώς παρά τις ικανότητες και τους πόρους που χαρακτηρίζουν αυτήν την πηγή απειλών, η πιθανότητα να στραφεί έναντι τυχαίων πολιτών, είναι τόσο μικρή, που σχετική ενδελεχής προστασία θα ήταν δυσανάλογη των αναγκών ενός "απλού" ασθενή, έναντι, για παράδειγμα, στην περίπτωση κάποιου υψηλόβαθμου κρατικού αξιωματούχου.

5.4. Σύγκλιση σιγουριάς και ασφάλειας

Επιστρέφοντας στις απαιτήσεις ασφάλειας όταν μεταχειριζόμαστε συστήματα που εφάπτονται της ψηφιακής υγείας, το πρόβλημα που γεννάται είναι πως το τρίπτυχο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας αναπτύχθηκε με προτεραιότητα τα εταιρικά πληροφοριακά συστήματα και ιδιαίτερα τα δεδομένα που αποθηκεύουν, επεξεργάζονται και διακινούν.

5.4.1. Περιγραφή του προβλήματος

Παρά το γεγονός πως και στο πεδίο της ψηφιακής υγείας απαντώνται δεδομένα εξέχουσας σημασίας για την ασφάλεια των ασθενών, η προτεραιότητα αλλάζει όταν έχουμε, όπως εδώ, κυβερνο-φυσικά συστήματα τα οποία έχουν την δυνατότητα πρόκλησης βλάβης μέσω της ίδιας της λειτουργικότητας τους – για παράδειγμα στην περίπτωση ιατρικών συσκευών οι οποίες και μπορούν να επενεργήσουν άμεσα στο ανθρώπινο σώμα, αναδεικνύεται πρωτίστως η σημασία της σίγουρης λειτουργίας, με την ασφάλεια των δεδομένων/πληροφοριών να

αποκτά δευτερεύοντα ρόλο. Το τρίπτυχο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας αγνοεί, καθώς δεν σχεδιάστηκε για αυτόν τον σκοπό [62], την ανάγκη αυτής της προτεραιοποίησης ιδιαίτερα στην περίπτωση των κυβερνο-φυσικών συστημάτων.

Μια εναλλακτική προσέγγιση θα ήταν συμπερίληψη της Σιγουριάς (Safety), Αξιοπιστίας (Reliability) και Διαθεσιμότητας (Availability) των διεργασιών, συσκευών και συνδεδεμένων συστημάτων – δηλαδή το τρίπτυχο SRA [62] στην περίπτωση κυβερνο-φυσικών συστημάτων, κάτι που μπορεί να επιτευχθεί με την χρήση του εξαπτύχου ασφάλειας (Parkesian Hexad), μιας εναλλακτικής προσέγγισης του τριπτύχου εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, τροποποιημένου για την χρήση σε περιπτώσεις κυβερνο-φυσικών συστημάτων (Modified Parkesian Hexad for Cyber-Physical Systems [65]). Οι οκτώ πτυχές αυτής της προσέγγισης σύμφωνα με τον Piggin [62], είναι οι εξής:

1. Εμπιστευτικότητα (Confidentiality), δηλαδή η ύπαρξη ελέγχων πρόσβασης και η πρόληψη της κάθε μη εξουσιοδοτημένης πρόσβασης σε συστήματα και πληροφορίες ή και δεδομένα,

2. Ακεραιότητα (Integrity), δηλαδή η διατήρηση της συνέπειας, της συνοχής και της διαμόρφωσης των πληροφοριών και των συστημάτων όπως και η πρόληψη μη εξουσιοδοτημένων αλλαγών σε αυτά,

3. Αυθεντικότητα (Authenticity), δηλαδή η διασφάλιση ότι κάθε είσοδος ή έξοδος από τα συστήματα, η κατάσταση του εκάστοτε συστήματος αλλά και κάθε σχετική διαδικασία, πληροφορίες ή και δεδομένα είναι γνήσια και δεν έχουν αλλοιωθεί ή τροποποιηθεί με οποιονδήποτε τρόπο,

4. Χρησιμότητα (Utility), δηλαδή η διασφάλιση ότι το σύστημα και οι πληροφορίες ή και τα δεδομένα παραμένουν προσβάσιμα και χρήσιμα καθ' όλη τη διάρκεια του κύκλου ζωής του συστήματος και, κατά περίπτωση, μπορούν να μεταφερθούν σε οποιοδήποτε παρεπόμενο (“διάδοχο”) σύστημα,

5. Διαθεσιμότητα (Availability), δηλαδή η διασφάλιση ότι τα συστήματα, οι διαδικασίες και τα δεδομένα είναι σταθερά προσβάσιμα και μπορούν να χρησιμοποιηθούν με τον

κατάλληλο τρόπο και εγκαίρως. Σημαντικό εδώ είναι πως στο πλαίσιο της διαθεσιμότητας συμπεριλαμβάνεται και ένα κατάλληλο και αναλογικό επίπεδο ανθεκτικότητας (Resilience),

6. Κατοχή (ή έλεγχος) (Possession/Control), δηλαδή ο στοχευμένος σχεδιασμός, η υλοποίηση, η λειτουργία και η συντήρηση των συστημάτων και των σχετικών διαδικασιών ώστε να αποτρέπεται ο κάθε μη εξουσιοδοτημένος χειρισμός ή παρέμβαση,

7. Ανθεκτικότητα (Resilience), δηλαδή η ικανότητα των συστημάτων και των πληροφοριών ή των δεδομένων να μετασχηματίζονται, να ανανεώνονται και να ανακάμπτουν εγκαίρως, αντιδρώντας έτσι αποτελεσματικά σε περίπτωση κάποιου δυσμενούς γεγονότος, και τέλος

8. Σιγουριά (Safety), δηλαδή ο σχεδιασμός, η υλοποίηση, η λειτουργία και η συντήρηση των συστημάτων και των σχετικών διαδικασιών, ώστε να αποτρέπεται η πρόκληση κάποιας επιβλαβούς κατάστασης, η οποία θα μπορούσε να οδηγήσει σε τραυματισμό ή απώλεια ζωής ή και σε κάποια ακούσια περιβαλλοντική ζημία.

Η ενδιαφέρουσα αυτή πρόταση αναδεικνύει όμως (συνειδητά σύμφωνα με τον Piggin [62]), ειδικά αν παρατηρήσουμε την τελευταία της πτυχή, αυτήν της σιγουριάς, ένα σημαντικό πρόβλημα που προκύπτει όταν προσεγγίζουμε τον τομέα της ψηφιακής υγείας υπό το πρίσμα της ασφάλειας, το οποίο και έγκειται στην σύγκλιση δυο εννοιολογικά συγγενικών αλλά πρακτικά διαφορετικών εννοιών – την σιγουριά (safety) και την ασφάλεια (security). Το πρόβλημα εναρμόνισης σιγουριάς και ασφάλειας δεν είναι ξένο στο πλαίσιο της βιβλιογραφίας, με τους Lisova et al. [66] να παρουσιάζουν συγκεντρωτικά 33 προσεγγίσεις.

Θα πρέπει λοιπόν αρχικά να αποσαφηνίσουμε τους δυο αυτούς όρους. Για να το πετύχουμε αυτό θα πρέπει να επιστρέψουμε στις αιτίες των απειλών για την ασφάλεια της ζωής και της υγείας των ασθενών, οι οποίες και μπορούν να χωριστούν σε δύο κατηγορίες:

1. επικινδυνότητες κυβερνοασφάλειας (cybersecurity risks) και

2. κίνδυνοι (hazards).

Οι επικινδυνότητες κυβερνοασφάλειας αφορούν σε κακόβουλες επιθέσεις σε κάποιο σύστημα από κάποιον ευφυή αντίπαλο και αντιμετωπίζονται μέσω μέτρων ασφάλειας. Οι κίνδυνοι αφορούν σε μη κακόβουλα σφάλματα και αντιμετωπίζονται μέσω μέτρων σιγουριάς [67].

Στο πλαίσιο αξιολόγησης του επιπέδου ασφάλειας ενός συστήματος, το αποτέλεσμα είναι τυπικά ποιοτικό και δυναμικά μεταβαλλόμενο, καθώς αλλάζουν οι πιθανοί δράστες/αντίπαλοι, και συνεπώς τόσο τα κίνητρα όσο και οι ικανότητές τους. Ταυτόχρονα δεν αποκλείεται να αποκαλυφθούν νέες, εκμεταλλεύσιμες ευπάθειες στο σύστημα που εξετάζεται, κάτι που με την σειρά του επηρεάζει το αποτέλεσμα μιας σχετικής αξιολόγησης όπως διαπιστώνουν και οι Lisova et al. [66] αλλά και οι Johnson et al [68] – αυτός είναι άλλωστε και ο λόγος που σχετικές αξιολογήσεις της ασφάλειας ενός συστήματος θα έπρεπε ιδανικά να επαναλαμβάνονται τακτικά.

Στο πλαίσιο αξιολόγησης του επιπέδου σιγουριάς ενός συστήματος πάλι, το αποτέλεσμα είναι τυπικά πιθανολογικό, ποσοτικό και σπανίως μεταβαλλόμενο, καθώς δεν συστήνονται/προκύπτουν νέες ευπάθειες στο/ή από το σύστημα [67].

Παρά το γεγονός πως τόσο οι επικινδυνότητες όσο και οι κίνδυνοι μπορούν να οδηγήσουν τόσο σε βλάβη της υγείας των ασθενών όσο και σε πιθανή απώλεια ζωής, η διαχείρισή τους αφορά σε διαφορετικές ειδικότητες – η διαχείριση της σιγουριάς αφορά στην εφαρμοσμένη ιατρική μηχανική, ενώ η διαχείριση της ασφάλειας αφορά στην ασφάλεια πληροφοριών.

Η πιο σημαντική διαφορά μεταξύ των δύο έγκειται όμως στο γεγονός πως στην περίπτωση των κινδύνων ο "αντίπαλος" είναι ουσιαστικά *ο ίδιος ο σχεδιασμός* – αφορά δηλαδή σε υλικά, λογισμικό, περιβάλλον λειτουργίας και στον σκοπό του προϊόντος. Αντιθέτως, στην περίπτωση των επικινδυνοτήτων κυβερνοασφάλειας ο αντίπαλος είναι ευφυής οντότητα, η οποία και μπορεί να στοχοποιήσει και κατ' επέκταση να εκμεταλλευτεί, μεταξύ άλλων, *και* την εκάστοτε προσέγγιση αντιμετώπισης πιθανολογικά σπάνιων περιστατικών κατά τον σχεδιασμό υπό το πρίσμα της σιγουριάς, επιφέροντας κατά αυτόν τον τρόπο το εκάστοτε αντίξοο αποτέλεσμα, όπως φαίνεται από τα παρακάτω παραδείγματα [62]:

Αν κάποια συγκεκριμένη συμπεριφορά χρήστη προκαλεί την ενεργοποίηση ασφαλούς λειτουργίας (safe mode) ενός συστήματος, ο κακόβουλος τρίτος μπορεί να μιμηθεί την συμπεριφορά αυτή, προκαλώντας έτσι την ενεργοποίηση της ασφαλούς λειτουργίας, η οποία με την

σειρά της μπορεί να οδηγεί σε τεχνικά περιορισμένη αποδοτικότητα και κατ' επέκταση διαθεσιμότητα του συστήματος – ως μια μορφή Denial of Service (DoS) – και να επιφέρει έτσι το εκάστοτε αντίξοο αποτέλεσμα. Ενδιαφέρον σε αυτήν την περίπτωση είναι πως το αντίξοο αποτέλεσμα προκαλείται εξαιτίας κάποιας "τυπικής", στο σενάριό μας βέβαια μη εξουσιοδοτημένης, συμπεριφοράς και όχι ως *άμεσο* αποτέλεσμα κάποιας στοχευμένα "κακόβουλης" ενέργειας η οποία και επέφερε κάποια παράτυπη συμπεριφορά του συστήματος – με άλλα λόγια, το σύστημα αντιδρά ακριβώς όπως *εκούσια σχεδιάστηκε* να αντιδρά, προκαλώντας όμως ζημιά.

Αντίστοιχα αποτελέσματα προέκυψαν και στο πλαίσιο της έρευνας στο πεδίο της ρομποτικής χειρουργικής [69], όπου κατόπιν εκτέλεσης επίθεσης τύπου Man-in-The Middle (MiTM) αποκτήθηκε επιτυχώς ο έλεγχος ενός ρομποτικού βραχίονα. Εν συνεχεία προκλήθηκε μια επείγουσα διακοπή λειτουργίας εξαιτίας γρήγορης (μη ασφαλούς) κίνησης ή κίνησης πέρα από τις ζώνες ασφαλείας. Και πάλι βλέπουμε πως ο βραχίονας ήταν προγραμματισμένος να σταματά την λειτουργία του σε περιστατικά γρήγορης κίνησης ή κίνησης πέρα από τις προκαθορισμένες ζώνες ασφαλείας *βάσει του σχεδιασμού του*, κάτι που εκμεταλλεύτηκαν οι ερευνητές στην προσομοίωση της επίθεσης.

Ένα ακόμη παράδειγμα είναι αυτό των εμφυτεύσιμων καρδιακών ηλεκτρονικών συσκευών (Cardiac Implantable Electronic Devices – CIEDs), όπως οι βηματοδότες και οι εμφυτεύσιμοι καρδιομετατροπείς-απινιδωτές (Implantable cardioverter-defibrillators – ICDs). Πρόκειται για κυβερνο-φυσικά συστήματα, τα οποία και εμφυτεύονται χειρουργικά στο σώμα του ασθενή. Ο βηματοδότης λειτουργεί στέλνοντας ηλεκτρικούς παλμούς με σκοπό την διατήρηση των κανονικών ρυθμών της καρδιάς, ενώ ο καρδιομετατροπέας-απινιδωτής παρακολουθεί τους καρδιακούς ρυθμούς και χορηγεί ηλεκτρικό σοκ όταν εντοπίζει κάποιο πρόβλημα με αυτούς. Το οικοσύστημα των εμφυτεύσιμων καρδιακών ηλεκτρονικών συσκευών αποτελείται από την εμφυτεύσιμη συσκευή, έναν εξωτερικό "προγραμματιστή", μια συσκευή που χρησιμοποιείται για την εξαγωγή δεδομένων ή την τροποποίηση των ρυθμίσεων της εμφυτεύσιμης συσκευής, μια οικιακή συσκευή παρακολούθησης, η οποία και μεταδίδει δεδομένα μέσω ασύρματου δικτύου τυπικά στον διακομιστή νέφους (cloud server), τον ίδιο τον διακομιστή νέφους και τέλος το σχετικό υλικό και λογισμικό στο γραφείο του γιατρού το οποίο καθιστά δυνατή την πρόσβαση στα δεδομένα του ασθενή [70]. Ήδη το 2008, μια ομάδα ερευνητών παρουσίασε πιθανές επιθέσεις εναντίον ενός εμπορικού καρδιομετατροπέα-απινιδωτή [71], στο πλαίσιο

των οποίων επιτεύχθηκε και η πρόκληση μιας επ'αόριστον επικοινωνία της συσκευής με μια μη αυθεντικοποιημένη εξωτερική συσκευή, γεγονός που οδήγησε στην εξάντληση της μπαταρίας της συσκευής – στόχου και συνεπώς σε μια κατάσταση αντίστοιχη με Denial of Service (DoS). Το συμπέρασμα της μελέτης είναι πως δεν υπάρχουν μηχανισμοί που να διασφαλίζουν πως μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση στους προγραμματιστές – κάτι που αναδεικνύει και πάλι την ένταση μεταξύ σιγουριάς και ασφάλειας, καθώς η αδυναμία διάκρισης μεταξύ των εξουσιοδοτημένων αιτημάτων θεραπείας και των μη εξουσιοδοτημένων αιτημάτων είναι ουσιαστικά ένα χαρακτηριστικό σιγουριάς [67], έτσι ώστε οι συσκευές να ανταποκρίνονται άμεσα σε οδηγίες επαναπρογραμματισμού από γιατρούς, για παράδειγμα σε κάποιο περιστατικό έκτακτης ανάγκης. Βλέπουμε λοιπόν και πάλι πως η εκμετάλλευση χαρακτηριστικών σιγουριάς, τα οποία και επιτρέπουν στον καρδιομετατροπέα-απινιδωτή να επιτελεί την λειτουργία για την οποία σχεδιάστηκε, μπορεί να οδηγήσει σε σοβαρό κίνδυνο για την φυσική ασφάλεια του ασθενή.

Αυτό που παρατηρούμε λοιπόν στο πλαίσιο της σχέσης επικινδυνοτήτων κυβερνοασφάλειας και κινδύνων ως προς την φυσική ασφάλεια των ασθενών, είναι πως η σχέση είναι κάθετη και όχι παράλληλη, καθώς αφενός ο σχεδιασμός του εκάστοτε συστήματος αποτελεί τον καμβά ή την επιφάνεια επίθεσης και αφετέρου τα μέτρα προστασίας έναντι κινδύνων μπορούν να αποτελέσουν *τα ίδια* επικινδυνότητα κυβερνοασφάλειας. Αυτή η διαπίστωση εντατικοποιεί όμως το πρόβλημα, καθώς προκύπτουν δύο επιπλέον ερωτήματα.

Το πρώτο είναι το κατά πόσο ισχύει και το αντίστροφο, αν δηλαδή μπορούν τα μέτρα προστασίας στο πλαίσιο της κυβερνοασφάλειας να αποτελέσουν τα ίδια κίνδυνο για την φυσική ασφάλεια των ασθενών. Η απάντηση στο ερώτημα αυτό εξαρτάται άμεσα από τον τρόπο και την ποιότητα της υλοποίησης μέτρων προστασίας στο πεδίο της κυβερνοασφάλειας: στην περίπτωση που τα μέτρα προστασίας υλοποιούνται ως μέρος του σχεδιασμού το προϊόντος, δηλαδή όταν πρόκειται για περιπτώσεις της λεγόμενης ενσωματωμένης ασφάλειας (baked-in security)/ προσέγγιση άμυνας μέσω προτεραιοποίησης της ασφάλειας (security-first defense), κατά την οποία η ασφάλεια συνυπολογίζεται με την σιγουριά, τότε τα μέτρα δεν παρουσιάζουν κάποιον κίνδυνο για την υγεία ή την ζωή των ασθενών. Στην περίπτωση πάλι που η ασφάλεια δεν αποτελεί μέρος του σχεδιασμού του προϊόντος, η μόνη λύση είναι η ετερόχρονη λήψη μέτρων προστασίας – η λεγόμενη "βιδωτή" ασφάλεια (bolted-on security). Εφόσον μια τέτοιου

τύπου προσέγγιση είναι τεχνικά εφικτή, το κατά πόσο η λήψη σχετικών μέτρων μπορεί να αποτελέσει κίνδυνο για την φυσική ασφάλεια των ασθενών εξαρτάται από την υλοποίησή της.

Για παράδειγμα, ένα περιστατικό προβληματικής υλοποίησης έλαβε χώρα στο πλαίσιο μιας επέμβασης καρδιακού καθετηριασμού, όπου και ο διαγνωστικός υπολογιστής που χρησιμοποιείται για την παρακολούθηση, τη μέτρηση και την καταγραφή των φυσιολογικών δεδομένων του ασθενούς κατέρρευσε, κάτι που οδήγησε σε περίπου πεντάλεπτη καθυστέρηση της εγχείρησης, συνθήκη η οποία θα μπορούσε να είχε οδηγήσει και σε βλάβη της υγείας του ασθενούς. Το περιστατικό, σύμφωνα με την σχετική αναφορά του οργανισμού FDA [72] προκλήθηκε από ένα σφάλμα διαμόρφωσης της αντι – ιικής σάρωσης (Antivirus scan) – αιτία ήταν το γεγονός πως ο πελάτης δεν ακολούθησε τις οδηγίες του κατασκευαστή σχετικά με την εγκατάσταση και διαμόρφωση του σχετικού λογισμικού.

Το δεύτερο ερώτημα που προκύπτει είναι το γιατί μας ενδιαφέρει ένας τέτοιος διαχωρισμός – αν τόσο οι επικινδυνότητες όσο και οι κίνδυνοι μπορούν να οδηγήσουν σε βλάβη της υγείας ή και σε απώλεια ζωής, τι καθιστά τον διαχωρισμό τους απαραίτητο; Πέρα από το γεγονός πως οι επικινδυνότητες και οι κίνδυνοι αφορούν σε διαφορετικές ειδικότητες όπως είδαμε παραπάνω, ένας τέτοιος διαχωρισμός είναι απαραίτητος καθώς τα μέτρα προστασίας στην εκάστοτε περίπτωση είναι διαφορετικά. Απαραίτητη είναι η υλοποίηση και των δύο με τέτοιο τρόπο, ώστε να μην συστήνονται νέοι κίνδυνοι από μέτρα ασφάλειας ή επικινδυνότητες από μέτρα προστασίας.

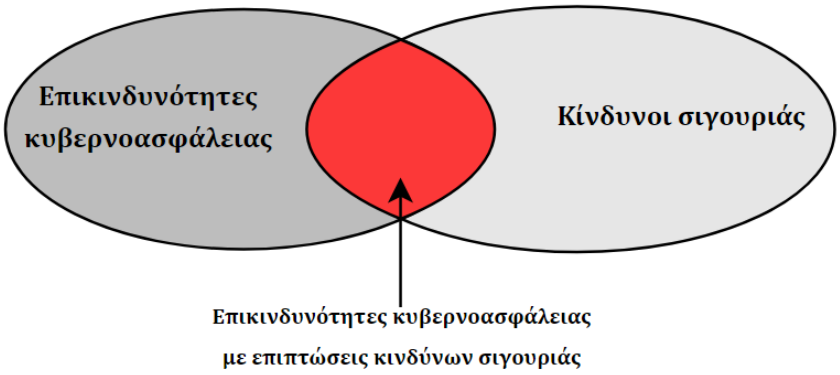
5.4.2. Σύνδεση σιγουριάς και ασφάλειας

Παρατηρείται λοιπόν η ανάγκη διαλειτουργικότητας των μέτρων προστασίας στο πλαίσιο της κυβερνοασφάλειας και των μέτρων σιγουριάς – μια παρατήρηση η οποία όμως είναι δύσκολα υλοποιήσιμη, ιδιαιτέρως αν αναλογιστούμε το περιβάλλον στο οποίο καλούμαστε να πραγματοποιήσουμε μια τέτοια εναρμόνιση. Στην περίπτωση των κυβερνο-φυσικών συστημάτων για παράδειγμα έχουμε τυπικά να κάνουμε με ενσωματωμένα υπολογιστικά συστήματα (embedded systems), τα οποία και διαθέτουν περιορισμένους πόρους. Συνεπώς η αύξηση των απαιτήσεων ασφάλειας σε ένα τέτοιο πλαίσιο μπορεί να οδηγήσει σε αρνητικές επιπτώσεις σε επίπεδο διαθεσιμότητας και χρηστικότητας, και κατ΄επέκταση, σιγουριάς [67], όπως φάνηκε άλλωστε και στην περίπτωση του παραδείγματος εμφυτεύσιμων καρδιακών

ηλεκτρονικών συσκευών που είδαμε παραπάνω – κάτι που αναδεικνύει την ανάγκη υλοποίησης/συνυπολογισμού μέτρων κυβερνοασφάλειας ήδη κατά τον σχεδιασμό του εκάστοτε προϊόντος.

Μια τέτοιου τύπου σύνδεση σιγουριάς και ασφάλειας προτείνεται και από την τεχνική προδιαγραφή IEC TS 63069 (2019) [87], η οποία και προτείνει ένα πλαίσιο για λειτουργική σιγουριά και ασφάλεια σε συστήματα βιομηχανικού αυτοματισμού και ελέγχου (Industrial Automation and Control Systems – IACS). Αποσαφηνίζει την ανάγκη εγκαθίδρυσης ενός περιβάλλοντος ασφάλειας (Security Environment), το οποίο και ορίζει ως το σύνολο των μέτρων προστασίας, τα οποία και απαιτούνται για την εξασφάλιση ενός αποτελεσματικά προστατευμένου περιβάλλοντος λειτουργίας των χαρακτηριστικών σιγουριάς, χωρίς όμως να περιορίζεται μόνο σε αυτές. Παρατηρούμε λοιπόν πως τα μέτρα προστασίας στο πλαίσιο της κυβερνοασφάλειας νοούνται (και) ως ομπρέλα προστασίας των μέτρων σιγουριάς. Η προδιαγραφή προτείνει επιπλέον την διενέργεια μιας (περιορισμένης) διαδικασίας Αναγνώρισης Κινδύνων (Hazard Identification – HazID). Πρόκειται για μια συστηματική διαδικασία εντοπισμού κινδύνων, η οποία και τυπικά εκτελείται από μηχανικούς ειδικούς σε ζητήματα σιγουριάς, κάτι που καθιστά έναν συνδυασμό παράλληλης (parallel) και συνδυαστικής (unified) προσέγγισης ζητημάτων σιγουριάς και ασφάλειας (πρβλ. και την σύγκριση των δύο προσεγγίσεων από τους Lisova et al. [66]) και έτσι μια αποδεκτή, η τουλάχιστον επαρκή, μέση λύση του προβλήματος της σύγκλισης σιγουριάς και ασφάλειας, με ειδικούς σε ζητήματα σιγουριάς να εμπλέκονται και στο κομμάτι της διαδικασίας που εκτελείται στο πλαίσιο της κυβερνοασφάλειας.

Συμπερασματικά, στο πλαίσιο της δικής μας προσέγγισης μας απασχολεί αποκλειστικά το σημείο τομής ανάμεσα σε επικινδυνότητες κυβερνοασφάλειας και κινδύνους σιγουριάς, όπως αυτό αποτυπώνεται στην εικόνα 5.1..



Εικόνα 5.1.: Η σχέση μεταξύ επικινδυνοτήτων κυβερνοασφάλειας και κινδύνων σιγουριάς (Πηγή: [62])

5.5. Επιπτώσεις επικινδυνοτήτων κυβερνοασφάλειας στην σιγουριά των ασθενών

Για να προχωρήσουμε σε μια αντιστοίχιση των επικινδυνοτήτων κυβερνοασφάλειας με τις επιπτώσεις τους στην σιγουριά των ασθενών, θα πρέπει αρχικά εντοπίσουμε τον συνδετικό κρίκο ανάμεσα στα δύο.

5.5.1. Μοντέλο διεργασίας – δομής – αποτελέσματος του Donabedian

Σε αυτό μας εξυπηρετεί αρχικά μια αναδρομή στον κατευθυντήριο άξονα στο πλαίσιο της έρευνας για την ασφάλεια των ασθενών, απαγκιστρωμένη από ζητήματα κυβερνοασφάλειας. Στο πλαίσιο αυτού του προσδιορισμού μας βοηθά το μοντέλο διεργασίας – δομής – αποτελέσματος που περιγράφεται από τον Donabedian [74]. Ο στόχος της έρευνας για την ασφάλεια των ασθενών πρέπει να είναι η βελτίωση του *αποτελέσματος*, δηλαδή η ελαχιστοποίηση της βλάβης των ασθενών λόγω λαθών στη διεργασία ή τη δομή της φροντίδας (εφόσον πρόκειται για διεργασία που εκτελείται από νοσοκόμο/α) ή της θεραπείας (εφόσον πρόκειται για διεργασία που εκτελείται από κάποιον/α γιατρό). Η βελτίωση της ασφάλειας θα προέλθει από αλλαγές (βελτιώσεις) σε αυτούς τους τομείς [61].

Στο πλαίσιο του μοντέλου που προτείνεται από τον Donabedian [74], απαιτείται έρευνα για τον προσδιορισμό της σχετικής ασφάλειας των διεργασιών και των δομών του συστήματος. Το πρόβλημα και σημείο κριτικής [73] με το μοντέλο έγκειται στο γεγονός πως όλα τα δυσμενή αποτελέσματα, συμπεριλαμβανομένου και του θανάτου, δεν οφείλονται απαραίτητα σε

προβλήματα είτε στη διαδικασία είτε στη δομή της περίθαλψης, αλλά (και) στην κατάσταση του ασθενούς πριν εισέλθει στο σύστημα υγειονομικής περίθαλψης [61], συνθήκη που θα πρέπει να ληφθεί υπόψη κατά την απόπειρα βελτίωσης του αποτελέσματος [73]. Συνεπώς, όταν αναφερόμαστε σε βλάβες της υγείας στο πλαίσιο της υγειονομικής περίθαλψης εννοούμε τις βλάβες ή τους τραυματισμούς που σχετίζονται με την εκάστοτε διεργασία υγείας και όχι με μια υποκείμενη ή φυσιολογική, περιβαλλοντική κατάσταση του ασθενούς ή προϋπάρχουσα ασθένεια [61]. Μια δεύτερη τροποποίηση του μοντέλου από τους Battles και Lilford [61] είναι η *συμπερίληψη* της εκάστοτε διεργασίας στην δομή του συστήματος υγειονομικής περίθαλψης, αντί για μια παράλληλη συνύπαρξη, δεδομένης της δυσκολίας διαφοροποίησης ανάμεσα στα δύο και του γεγονότος πως τροποποίηση της δομής, αντί για τροποποίηση της υπεύθυνης για το εκάστοτε αντίξοο αποτέλεσμα διεργασίας μπορεί να επηρεάσει αντίξοα την υγεία ασθενών τους οποίους δεν αφορά η ουσιαστικά προβληματική διεργασία [73].

5.5.2. Τυποποίηση αποτυχιών στο πλαίσιο διεργασιών και δομών υγειονομικής περίθαλψης

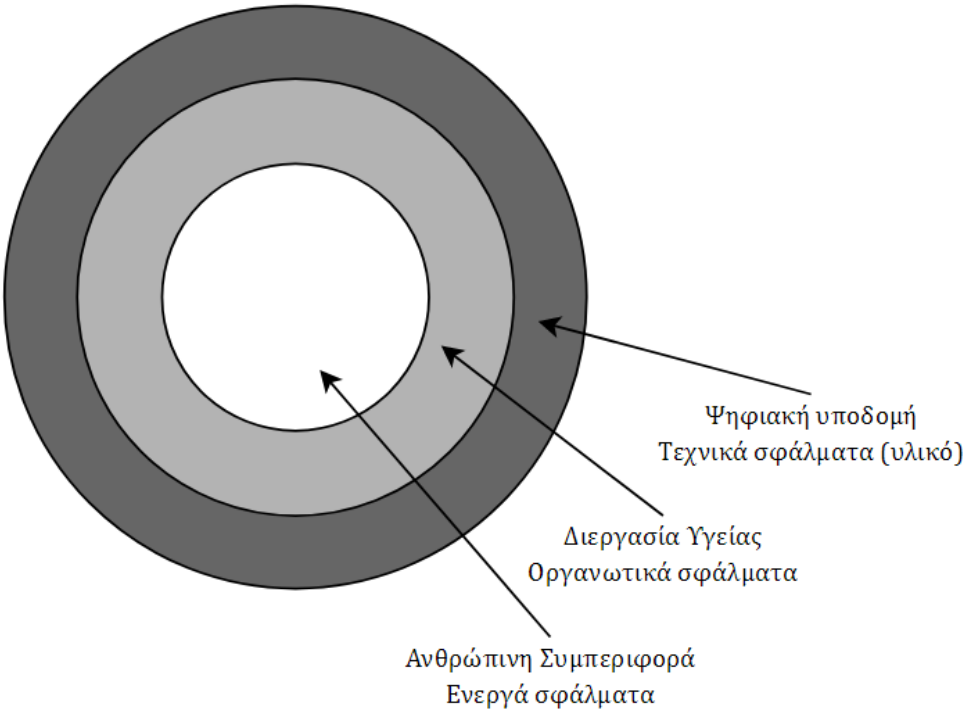
Σύμφωνα με τον Reason [75, 76] απαντώνται δύο κατηγορίες αποτυχιών/σφαλμάτων, ανάλογα με το ποιος τις ξεκίνησε και τον χρόνο που χρειάζεται για να επέλθει το εκάστοτε δυσμενές αποτέλεσμα:

1. Ενεργές αποτυχίες, δηλαδή αυτές που διαπράττονται από άτομα που έρχονται σε άμεση επαφή με τον ασθενή στο πλαίσιο παροχής φροντίδας, οι οποίες απαντώνται και ως ανθρώπινο σφάλμα. Ως σφάλμα μπορεί να θεωρηθεί κάθε πράξη η παράλειψη, η οποία οδηγεί σε αποκλίσεις από προθέσεις ή προσδοκίες.

2. Λανθάνουσες αποτυχίες, δηλαδή αποτυχίες που προκύπτουν ως συνέπειες τεχνικών και οργανωτικών ενεργειών και αποφάσεων, οι οποίες όμως επέρχονται καθυστερημένα.

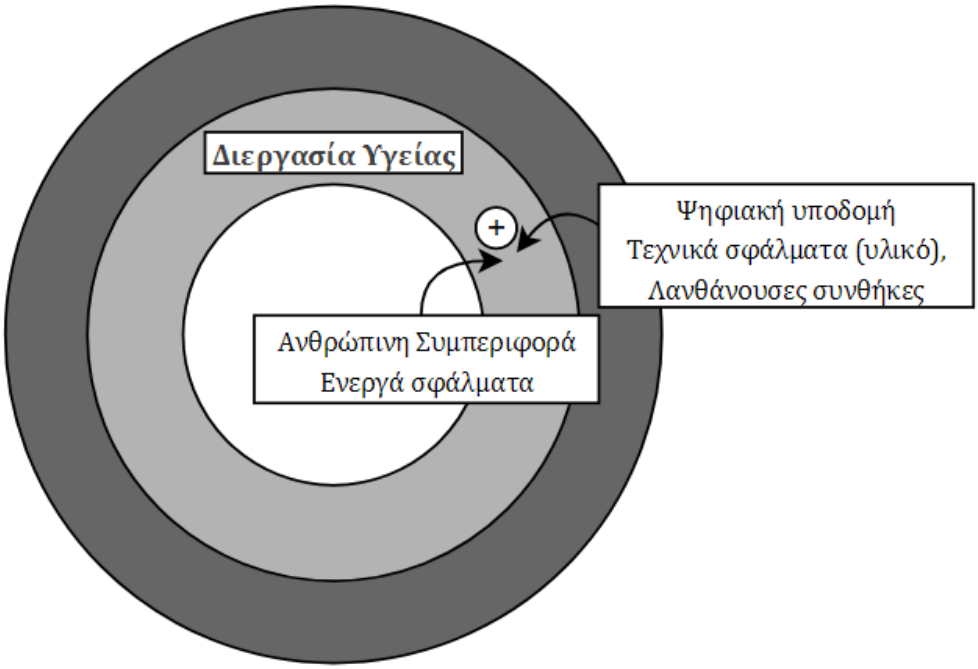
Στο πλαίσιο των ανθρώπινων σφαλμάτων, ο Rasmussen [77] εξέτασε τους παράγοντες που επηρεάζουν την ανθρώπινη συμπεριφορά που οδηγεί σε σχετικές αποτυχίες ή σφάλματα, εντοπίζοντας τρεις κατηγορίες σφαλμάτων: σφάλματα που βασίζονται στην (ενδεχομένως ελλιπή) ικανότητα, σφάλματα που βασίζονται σε κανόνες (ή την παράβλεψη τους) και σφάλματα που βασίζονται σε (ενδεχομένως ελλιπείς ή λάθος) γνώσεις.

Ο Van der Schaaf [78] οργάνωσε με την σειρά του τις ενεργές αποτυχίες και λανθάνουσες καταστάσεις σε ανθρώπινες, οργανωτικές και τεχνικές αποτυχίες. Συνδυάζοντας αυτό το μοντέλο ταξινόμησης με το μοντέλο του Donabedian [74] που είδαμε παραπάνω, προκύπτει η διασκευή από τους Battles και Lilford [61] που απεικονίζεται στο σχήμα της εικόνας 5.2.



Εικόνα 5.2.: Το τροποποιημένο μοντέλο του Donabedian (Πηγή: [61])

Τα ενεργά (ή ανθρώπινα) σφάλματα πηγάζουν από τον πυρήνα, δηλαδή την ανθρώπινη συμπεριφορά, και διακινδυνεύουν εκ των έσω την διεργασία υγείας, ενώ οι λανθάνουσες συνθήκες αντιπροσωπεύουν κινδύνους που είναι ενσωματωμένοι στο σημείο τομής της διεργασίας υγείας και της εξωτερικής στρώσης της ψηφιακής υποδομής (οργανωτική ή τεχνική) της υγειονομικής περίθαλψης [78], όπως φαίνεται στην εικόνα 5.3. Όπως επισημαίνει ο Reason [75, 76] σε αυτό το πλαίσιο, το εκάστοτε αντίξοο αποτέλεσμα προκαλείται από την συνύπαρξη ενεργών σφαλμάτων και λανθανουσών συνθηκών.



Εικόνα 5.3.: Προϋποθέσεις πρόκλησης βλάβης κατά Reason (Πηγή: [75, 76])

5.5.3. Θεώρηση του προβλήματος υπό το πρίσμα της κυβερνοασφάλειας

Αν θεωρήσουμε τώρα το πρόβλημα υπό το πρίσμα της κυβερνοασφάλειας, ζημιά στην υγεία του ασθενή μπορεί να προκληθεί με δύο τρόπους, άμεσα και έμμεσα.

1. Όταν η επίθεση επιφέρει *η ίδια* το αντίξοο αποτέλεσμα, η ζημιά είναι *άμεση*.

2. Όταν η επίθεση επηρεάζει την απόφαση κάποιου τρίτου, η οποία με την σειρά της επιφέρει την βλάβη στην υγεία του ασθενή, η ζημιά είναι *έμμεση*. Ενδιαφέρον σε αυτό το σημείο είναι όμως πως στην περίπτωση της έμμεσης ζημιάς, αυτή επιφέρεται άμεσα από τον επαγγελματία υγείας, είτε με την μορφή ιατρικής απόφασης είτε ως προ-προγραμματισμένη αντίδραση εφόσον πρόκειται για ιατρική συσκευή – παρά το γεγονός πως η σχετική απόφαση ουσιαστικά ετεροκαθορίζεται από τον κακόβουλο τρίτο, για παράδειγμα σε περίπτωση που η σχετική απόφαση βασίζεται σε παραποιημένα δεδομένα κάποιου ανθρωποκεντρικού αισθητήρα.

Αν προχωρήσουμε στην εξέταση των εξής παραδειγμάτων έμμεσης και άμεσης ζημιάς:

1. αλλοίωση των δεδομένων ανθρωποκεντρικού αισθητήρα στα οποία βασίζεται συγκεκριμένη αντίδραση ιατρικής συσκευής, όπως στην περίπτωση αντλίας έγχυσης (έμμεση ζημιά),

2. αλλοίωση των δεδομένων ανθρωποκεντρικού αισθητήρα στα οποία βασίζεται δοσολογία φαρμάκου από τον επαγγελματία υγείας (έμμεση ζημιά),

3. αλλοίωση των δεδομένων ανθρωποκεντρικού αισθητήρα στα οποία βασίζεται απόφαση για επεμβατική παρέμβαση (έμμεση ζημιά),

4. αλλοίωση της γενικότερης κατηγορίας ιατρικών δεδομένων σε περίπτωση που βασίζεται σε αυτά σχετική θεραπεία ή επέμβαση (έμμεση ζημιά),

5. πρόκληση συγκεκριμένης, επιβλαβούς αντίδρασης ιατρικής συσκευής στο σώμα του ασθενή (άμεση ζημιά),

6. απενεργοποίηση λειτουργιών ιατρικής συσκευής που είναι απαραίτητες για την διατήρηση μιας συγκεκριμένης κατάστασης υγείας (άμεση ζημιά),

Καταλαβαίνουμε πως ζημιά, ανεξαρτήτως αν πρόκειται για άμεση ή έμμεση, προκαλείται όταν:

1. κατόπιν επιτυχούς επίθεσης καταλύεται μια (ή περισσότερες) σχετική πτυχή του τριπτύχου εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, η οποία συνδέεται με την διαδικασία λήψης ιατρικών αποφάσεων για τον ασθενή, κάτι που μπορεί να συμβαίνει αυτοματοποιημένα ή από τον υπεύθυνο επαγγελματία υγείας, ή

2. διαθεσιμότητα, της οποίας η ύπαρξη αποτρέπει άμεσα το αντίξοο αποτέλεσμα, καταλύεται κατόπιν επιτυχούς επίθεσης.

5.5.4. Συνδυαστική προσέγγιση

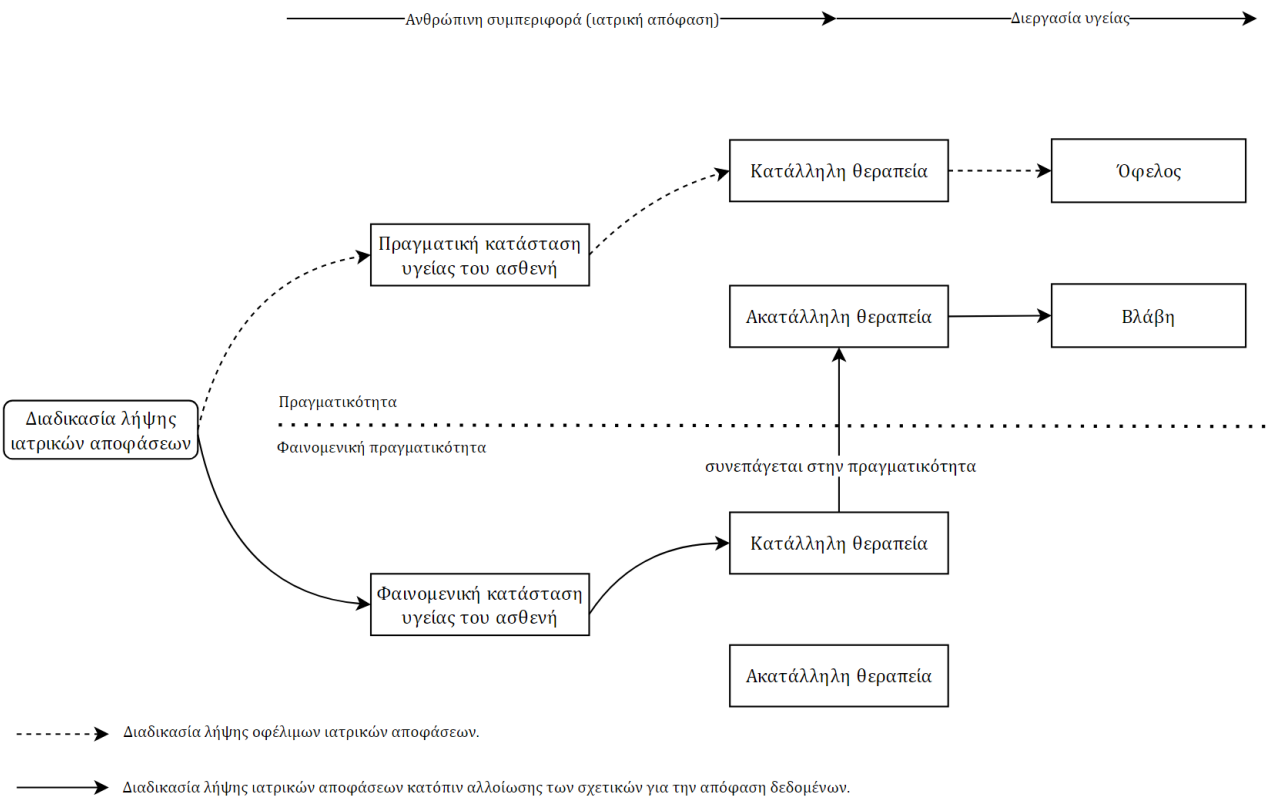
Αν επιστρέψουμε στο τροποποιημένο από τον Van der Schaaf [78] μοντέλο διεργασίας – δομής – αποτελέσματος του Donabedian [74], παρατηρούμε πως τόσο τα ενεργά σφάλματα όσο και τα τεχνικά σφάλματα ή οι λανθάνουσες συνθήκες μπορούν να οδηγήσουν σε βλάβη του ασθενή όταν επενεργούν στην σχετική διεργασία υγείας.

Υπό το πρίσμα της κυβερνοασφάλειας, μια επίθεση οδηγεί σε βλάβη όταν προκαλεί την κατάλυση της σχετική πτυχής του τριπτύχου εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, η οποία είτε συνδέεται με την διαδικασία λήψης ιατρικών αποφάσεων για τον ασθενή είτε προϋποτίθεται για την διατήρηση του status quo της υγείας του ασθενή, τυπικά στην περίπτωση της διαθεσιμότητας.

Αν εφαρμόσουμε αυτήν την διαπίστωση στο τροποποιημένο από τον Van der Schaaf [78] μοντέλο διεργασίας – δομής – αποτελέσματος του Donabedian [74], παρατηρούμε μια ταύτιση των σημείων τομής των παραγόντων που οδηγούν σε βλάβη, όπως προκύπτει στις ακόλουθες περιπτώσεις:

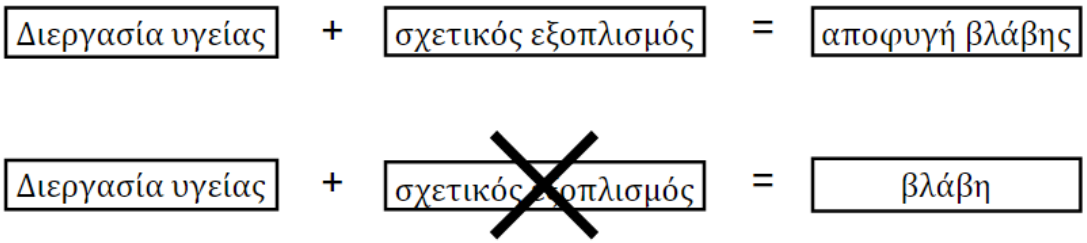
- Περίπτωση 1: τα ενεργά σφάλματα, τα οποία και αφορούν στην ανθρώπινη συμπεριφορά, η οποία καθιστά τον πυρήνα του τροποποιημένου μοντέλου του Donabedian [78], μπορούν να αντιστοιχηθούν με την, κατόπιν επιτυχούς επίθεσης, ετεροκαθοριζόμενη και συνεπώς παρουσιάζουσα σφάλμα βασιζόμενο σε αλλοιωμένα δεδομένα διαδικασία λήψης ιατρικών αποφάσεων για τον ασθενή.

  Σε αυτήν την περίπτωση επηρεάζεται το γνωστικό στοιχείο της ανθρώπινης συμπεριφοράς που καθορίζει την διεργασία υγείας και η βλάβη που προκύπτει είναι το αποτέλεσμα *ελλιπούς* (και όχι εσφαλμένης) γνώσης κατά τον Rasmussen [77]: η ιατρική απόφαση σχετικά με την αρμόζουσα θεραπεία ανταποκρίνεται στην φαινομενική κατάσταση υγείας του ασθενή χωρίς να παρουσιάζει κάποιο γνωστικό σφάλμα – θα ήταν δηλαδή όντως η lege artis θεραπεία για την συγκεκριμένη περίπτωση. Καθώς όμως οι παράγοντες που καθορίζουν τις απαιτήσεις υγείας στην εκάστοτε περίπτωση έχουν αλλοιωθεί κατόπιν επιτυχούς κυβερνοεπίθεσης, η ιατρική απόφαση σχετικά με την αρμόζουσα θεραπεία δεν ανταποκρίνεται πια στην πραγματική κατάσταση υγείας του ασθενή και συνεπώς καθιστά (ενεργό) ιατρικό σφάλμα, όπως φαίνεται στην εικόνα 5.4..



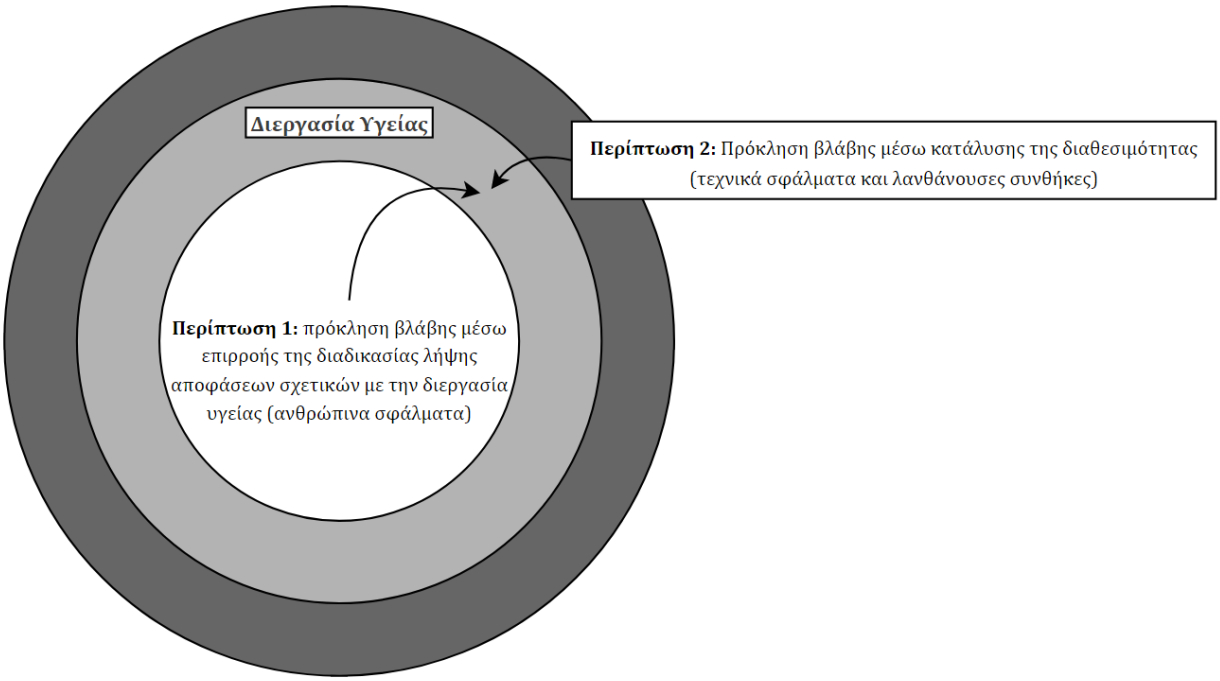
Εικόνα 5.4.: Διαδικασία λήψης ιατρικών αποφάσεων που οδηγούν σε βλάβη στην περίπτωση 1.

- Περίπτωση 2: τα τεχνικά σφάλματα και οι λανθάνουσες συνθήκες, οι οποίες στην ουσία τους αφορούν σφάλματα σε επίπεδο εξοπλισμού που χρησιμοποιείται στο πλαίσιο κάποιας διεργασίας υγείας (τυπικά εμφυτεύσιμες ιατρικές συσκευές), μπορούν να αντιστοιχηθούν στην περίπτωση που καταλύεται η διαθεσιμότητα, όταν αυτή προϋποτίθεται για την διατήρηση της υγείας του ασθενούς. Η ζημιά σε αυτήν την περίπτωση προκαλείται λοιπόν εξαιτίας της αφαίρεσης του απαραίτητου για την εκάστοτε διεργασία υγείας εξοπλισμού, όπως φαίνεται στην εικόνα 5.5..



Εικόνα 5.5.: Πρόκληση βλάβης μέσω κατάλυσης της διαθεσιμότητας στην περίπτωση 2.

Και στις δύο περιπτώσεις παρατηρείται λοιπόν πως μια επιτυχής επίθεση κυβερνοασφάλειας μπορεί να οδηγήσει σε βλάβη του ασθενή όταν επενεργεί στην σχετική διεργασία υγείας, είτε εκ των έσω, δηλαδή κατόπιν επιρροής της διαδικασίας λήψης ιατρικών αποφάσεων σχετικά με αυτήν, είτε σε επίπεδο (ψηφιακών) υποδομών, με την αφαίρεση του απαραίτητου για την αποτελεσματική υλοποίηση της εξοπλισμού μέσω κατάλυσης της διαθεσιμότητάς του (εικόνα 5.6.).



Εικόνα 5.6.: Προϋποθέσεις πρόκλησης βλάβης στην υγεία του ασθενή υπό το πρίσμα της κυβερνοασφάλειας

Κεφάλαιο 6
Υπολογισμός και προτεραιοποίηση επικινδυνοτήτων

Στο πλαίσιο του κεφαλαίου 6 θα μεταχειριστούμε την μέθοδο υπολογισμού και προτεραιοποίησης των επικινδυνοτήτων στο πλαίσιο της ψηφιακής υγείας ως προς τις επιπτώσεις τους στην υγεία των ασθενών. Αφού περιγραφεί η μεθοδολογία ARES [79], στην οποία στηριχτήκαμε για την ανάπτυξη της προτεινόμενης προσέγγισης και την οποία τροποποιήσαμε για να ανταποκρίνεται στις απαιτήσεις που προκύπτουν στο πλαίσιο της ψηφιακής υγείας (6.1.), θα παρουσιαστεί η προτεινόμενη προσέγγιση προτεραιοποίησης επικινδυνοτήτων (6.2.).

6.1. Η μεθοδολογία ARES

Η μεθοδολογία ARES (Automated Risk Estimation in Smart Sensor Environments) [79] έχει αναπτυχθεί με σκοπό την αυτοματοποιημένη εκτίμηση επικινδυνότητας σε υπολογιστικά συστήματα και μέρη αυτών μέσω της αξιοποίησης του Πλαισίου Επιχειρησιακών Διεργασιών (Business Process Context – BPC) και των Κοινών Προτύπων Ασφάλειας (Common Security Standards – CSSs).

Βασίζεται στην επέκταση του σχετικού *πλαισίου* της εκάστοτε επιχειρησιακής διεργασίας (Business Process Context – BPC), όπως αυτό ορίζεται από το σύστημα οργάνωσης και ταξινόμησης επιχειρησιακών διεργασιών (Business Process Cataloging and Classification System – BPCCS), έτσι ώστε η *πτυχή πλαισίου* "Πώς" να συμπεριλαμβάνει την διάσταση "Συστήματα, λογισμικό και πακέτα" (Systems, Software and Packages – SSP), τα οποία και εκφράζονται μέσω του συστήματος ονοματοδοσίας CPE.

Για τον προσδιορισμό των παραγόντων κινδύνου του μοντέλου, δηλαδή της πιθανότητας και της επίπτωσης, η προσέγγιση που ακολουθεί το ARES επικεντρώνεται στην εκάστοτε ευπάθεια και στηρίζεται στην δημιουργία μιας αλυσίδας ιχνηλάτησης των ευπαθειών (CVEs) του εκάστοτε υπολογιστικού συστήματος ή συστατικών αυτού (τα οποία και εκφράζονται μέσω του συστήματος ονοματοδοσίας CPE), των ασθενειών (CWEs) που σχετίζονται με τις ευπάθειες αυτές και τέλος τους τύπους (μοτίβα) επιθέσεων (CAPECs) που εκμεταλλεύονται τις ασθένειες που εντοπίστηκαν.

Υιοθετεί μια ποιοτική προσέγγιση υπολογισμού του επιπέδου επικινδυνότητας για κάθε μια από τις πτυχές εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας για το εκάστοτε συστατικό στοιχείο του υπολογιστικού συστήματος (το οποίο και εκφράζεται μέσω του συστήματος ονοματοδοσίας CPE). Το γινόμενο της πιθανότητας (likelihood) εμφάνισης μιας απειλής (η οποία και προκύπτει από το εκάστοτε CAPEC) και της δυνητικής επίπτωσης (impact) που μπορεί να έχει η απειλή αυτή σε κάθε πτυχή του τριπτύχου ασφάλειας οδηγεί σε ένα ποιοτικό εύρος τιμών κινδύνου πέντε επιπέδων: Κανένας, Χαμηλός, Μέτριος, Υψηλός και Πολύ Υψηλός, όπως παρουσιάζεται στον πίνακα 6.1.:

Επίπτωση / Πιθανότητα	Καμία	Πολύ Χαμηλή	Χαμηλή	Μέτρια	Υψηλή	Πολύ υψηλή
Χαμηλή	Κανένας	Χαμηλός	Χαμηλός	Μέτριος	Μέτριος	Υψηλός
Μέτρια	Κανένας	Χαμηλός	Μέτριος	Μέτριος	Υψηλός	Υψηλός
Υψηλή	Κανένας	Χαμηλός	Μέτριος	Υψηλός	Υψηλός	Πολύ υψηλός

Πίνακας 6.1.: Μοντέλο επικινδυνότητας του ARES (Πηγή: [79])

Για τον παράγοντα πιθανότητας, το ARES χρησιμοποιεί την πιθανότητα του CAPEC το οποίο και καθιστά το χειρότερο πιθανό σενάριο, ενώ για τον παράγοντα επίπτωσης συγκρίνεται η τιμή επιπτώσεων του CAPEC το οποίο και καθιστά το χειρότερο πιθανό σενάριο με την τιμή επιπτώσεων όπως αυτές αποτυπώνονται στο πλαίσιο του εκάστοτε βαθμού CVSS του CVE το οποίο και μπορεί να εκμεταλλευτεί το εκάστοτε σχετικό CAPEC. Ο παράγοντας επίπτωσης σε αυτό το πλαίσιο είναι πάντα η χαμηλότερη τιμή.

Σε περίπτωση που το CAPEC δεν παρέχει τιμή επίπτωσης, το ARES χρησιμοποιεί την τιμή επίπτωσης του γονικού του CAPEC. Αν, αντιστρόφως, η βαθμονόμηση CVSS δεν παρέχει τιμή επίπτωσης, χρησιμοποιείται η τιμή επίπτωσης του CAPEC, με τους Dimitriades et al. [79] να προτείνουν την εξάρτηση του συντελεστή επίπτωσης από την σχετική βαθμονόμηση CVSS.

Αφού εκτιμηθούν οι παράγοντες επιπτώσεων και πιθανότητας, το επίπεδο επικινδυνότητας για κάθε πτυχή ασφάλειας μπορεί να προσδιοριστεί με βάση το γινόμενό τους, βάσει του πίνακα 6.1..

Το ARES προτείνει την επισύναψη της συνολικής τιμής επικινδυνότητας για κάθε πτυχή ασφάλειας σε ένα ανώτερο όριο κινδύνου με βάση το CAPEC που δεδομένης της πιθανότητας και της επίπτωσης του καθιστά το χειρότερο σενάριο (αντί να βασίζεται για παράδειγμα στο άθροισμα όλων των κινδύνων), προσέγγιση που ανταποκρίνεται σε αντίστοιχο σκεπτικό του NIST [88].

Σε ένα περαιτέρω βήμα το ARES επικυρώνει επίσης ότι το CAPEC που καθιστά το χειρότερο σενάριο μπορεί πραγματικά να αποτελέσει απειλή για το συγκεκριμένο CPE χρησιμοποιώντας μια αντιστοίχιση CAPECs-σε-CPE, αξιοποιώντας μια τεχνική biclustering[2] - αν το εξεταζόμενο CAPEC δεν δύναται να αντιστοιχεί στο συγκεκριμένο CPE, επιλέγεται το CAPEC που καθιστά την επόμενη μεγαλύτερη επικινδυνότητα κ.ο.κ..

6.2. Τροποποίηση της μεθοδολογίας ARES για χρήση στο πλαίσιο της ψηφιακής υγείας

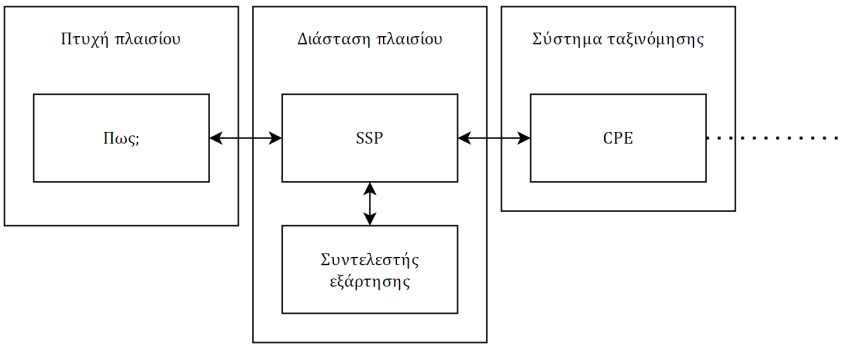
Κατά την αντιστοίχηση επικινδυνοτήτων κυβερνοασφάλειας στην υγεία των ασθενών (5.5.4.) προσδιορίσαμε πως καθοριστική για την πρόκληση βλάβης είναι η επενέργεια στην σχετική διεργασία υγείας μέσω κατάλυσης της πτυχής ασφάλειας στην οποία βασίζεται η σχετική διεργασία. Εντοπίσαμε επίσης, πως η κατάλυση της εκάστοτε πτυχής ασφάλειας εξαρτάται άμεσα από τον εξοπλισμό, είτε πρόκειται για κάποιον αισθητήρα, στα δεδομένα του οποίου μπορεί να βασίζεται κάποια ιατρική απόφαση, είτε για ιατρική συσκευή, της οποίας η αδιάκοπη λειτουργία είναι καθοριστική για την αποτροπή της βλάβης.

6.2.1. Προσθήκη συντελεστή εξάρτησης διεργασίας υγείας από τον εξοπλισμό

Μεταφέροντας αυτό το σκεπτικό στο πλαίσιο της προσέγγισης του ARES, δεδομένης της ύπαρξης σχετικής διεργασίας υγείας βάσει κάποιου μοντέλου και συμβολισμού επιχειρησιακών διεργασιών (Business Process Model and Notation – BPMN), προτείνουμε την προσθήκη

2 Πρβλ. Εδώ την περιγραφή των συγγραφέων, Dimitriades et al. [79].

της υποκατηγορίας “συντελεστής εξάρτησης” στο επίπεδο πλαισίου επιχειρησιακής διεργασίας (BPC), ο οποίος και περιγράφει τον βαθμό που η εκάστοτε διεργασία υγείας εξαρτάται από τον εξοπλισμό (δηλαδή τα SSPs τα οποία και σχετίζονται με το εκάστοτε CPE), ως προς κάθε μία από τις τρεις πτυχές ασφάλειας (εικόνα 6.1.).

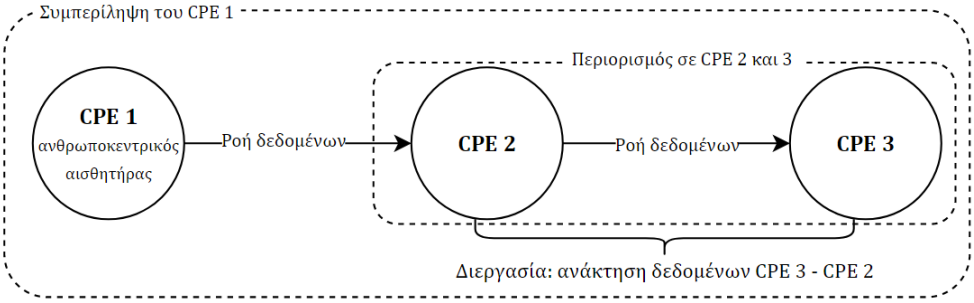


Εικόνα 6.1.: Προτεινόμενη επέκταση της διάστασης του πλαισίου επιχειρησιακής διεργασίας (BPC)

Το πρώτο ερώτημα που τίθεται σε αυτό το πλαίσιο είναι το κατά πόσο θα πρέπει ο συντελεστής εξάρτησης να αφορά στις απαιτήσεις ασφάλειας της εκάστοτε διεργασίας υγείας ή στις επιμέρους απαιτήσεις ασφάλειας του κάθε CPE ως προς την σχετική διεργασία υγείας. Η απάντηση στο ερώτημα αυτό εξαρτάται από τις επιμέρους απαντήσεις σε διάφορα περαιτέρω ερωτήματα.

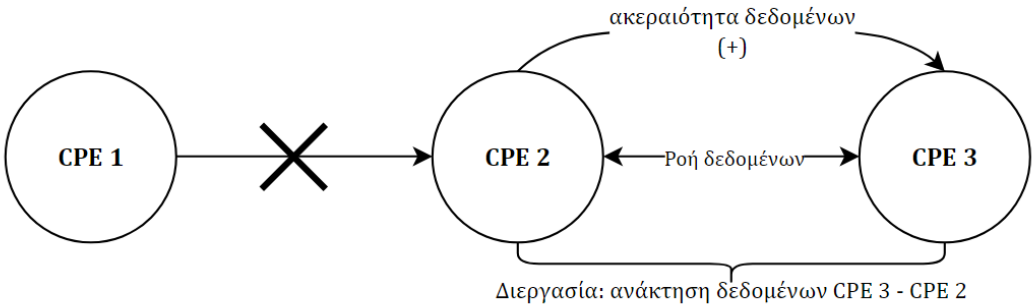
Αρχικά, θα πρέπει να προσδιορίσουμε το εύρος των CPEs που ανήκουν στην εκάστοτε διεργασία υγείας. Για παράδειγμα, αν θεωρήσουμε την περίπτωση κάποιου ανθρωποκεντρικού αισθητήρα (CPE 1) ο οποίος αποστέλλει τα δεδομένα που συλλέγει σε κάποια οικιακή συσκευή παρακολούθησης (CPE 2), η οποία επικοινωνεί με κάποιον διακομιστή νέφους (CPE 3) όπου και τα δεδομένα αποθηκεύονται έτσι ώστε ο υπεύθυνος επαγγελματίας υγείας να έχει πρόσβαση σε αυτά, η διεργασία η οποία και αφορά στην *ανάκτηση δεδομένων* στη σχέση μεταξύ του διακομιστή νέφους (CPE 3) και της οικιακής συσκευής παρακολούθησης (CPE 2) θα μπορούσε να αφορά αποκλειστικά τα CPE διακομιστής νέφους (CPE 3) και οικιακή συσκευή παρακολούθησης (CPE 2) ή να συμπεριλαμβάνει και τον ανθρωποκεντρικό αισθητήρα (CPE 1).

Το ερώτημα αφορά ουσιαστικά στο επίπεδο αφαιρετικότητας κατά την μεταχείριση της εκάστοτε διεργασίας. Σύμφωνα με μια πιο αφαιρετική θεώρηση, η διεργασία του παραδείγματος αφορά αποκλειστικά τα CPE 2 και 3 καθώς αφορά αποκλειστικά στην *ανάκτηση* δεδομένων (CPEs 2, 3), και όχι στην *συλλογή* τους (CPE 1) ή την ανάκτηση τους από το CPE 2 (CPEs 2, 1). Αν πάλι συμπεριλάβουμε την συλλογή (ή την ύπαρξη) των δεδομένων ως απαραίτητη προϋπόθεση για την ανάκτηση τους, τότε αναγκαστικά πρέπει να συμπεριλάβουμε και το CPE 1, το οποίο και δεν εμπλέκεται άμεσα στην συγκεκριμένη διεργασία, όπως φαίνεται στην εικόνα 6.2..



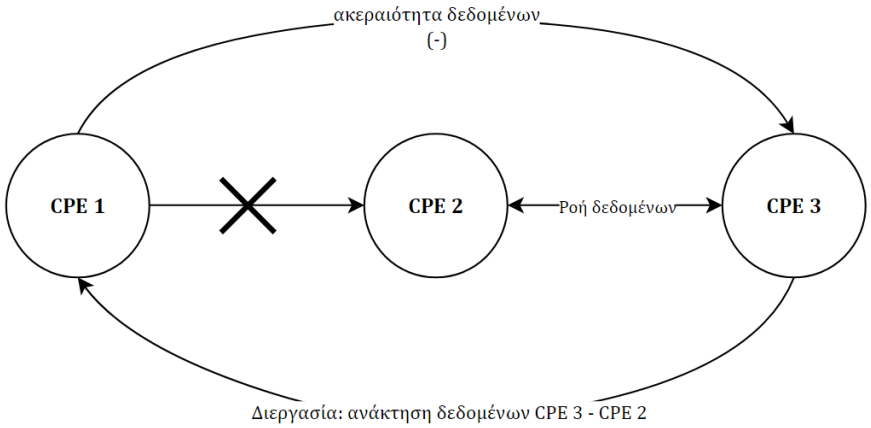
Εικόνα 6.2.: Καθολική/αφαιρετική θεώρηση των CPEs που εμπλέκονται στην διεργασία του παραδείγματος

Η διάκριση είναι σημαντική, καθώς σε περίπτωση κατάλυσης της ακεραιότητας των δεδομένων που συλλέγονται από το CPE 1 του παραδείγματος κατά την μεταφορά τους στο CPE 2, αν η θεώρηση μας κατά την αξιολόγηση του επιπέδου ασφάλειας της διεργασίας ανάκτησης δεδομένων αφορά αφαιρετικά αποκλειστικά τα CPE 2 και 3, η ακεραιότητα των δεδομένων *συνεχίζει να διατηρείται* στο πλαίσιο της εξεταζόμενης διεργασίας ανεξαρτήτως της επιτυχούς κατάλυσης της ακεραιότητας στην σχέση CPE 1 και CPE 2, καθώς τα δεδομένα που ανακτώνται στην σχέση μεταξύ CPE 3 και CPE 2 είναι όντως ακέραια – παρά το γεγονός πως δεν αντικατοπτρίζουν τα πραγματικά δεδομένα που συλλέχθηκαν από το CPE 1, όπως φαίνεται στην εικόνα 6.3..



Εικόνα 6.3.: Επίπτωση επιτυχημένης επίθεση στην περίπτωση αφαιρετική θεώρησης στο πλαίσιο του παραδείγματος

Αν πάλι συμπεριλάβουμε στην θεώρησή μας το CPE 1, τότε στο παράδειγμά μας πλήττεται η ακεραιότητα των δεδομένων και στο πλαίσιο της εξεταζόμενης διεργασίας, καθώς η επίπτωση της επιτυχούς επίθεσης στην σχέση CPE 1 και CPE 2 διαδίδεται στην σχέση CPE 2 και CPE 3, όπως φαίνεται στην εικόνα 6.4..



Εικόνα 6.4.: Επίπτωση επιτυχημένης επίθεση στην περίπτωση καθολικής θεώρησης στο πλαίσιο του παραδείγματος

Παρά το γεγονός πως μόνο η πιο καθολική θεώρηση οδηγεί στο θεμιτό αποτέλεσμα στο πλαίσιο του παρόντος παραδείγματος, την διαπίστωση δηλαδή πως η ακεραιότητα των δεδομένων που (συν-)καθορίζουν κάποια ενδεχόμενη ιατρική απόφαση έχει πληγεί, μια αντιστοίχως καθολική αξιολόγηση του επιπέδου ασφάλειας αλλοιώνεται από αυτήν την καθολικότητα καθώς δεν διατηρείται με συνέπεια το επίπεδο αφαιρετικότητας που αποσκοπείται εδώ – από την στιγμή που μέσω του ARES εξετάζουμε το επίπεδο ασφάλειας του κάθε εμπλεκόμενου στην εκάστοτε διεργασία CPE ξεχωριστά πριν καταλήξουμε στην σύνθεση του τελικού επιπέδου ασφάλειας που προκύπτει, προσεγγίζουμε την αξιολόγηση επαγωγικά, έχοντας

ταυτόχρονα επίγνωση της συνθήκης πως τα CPEs που συμπεριλαμβάνονται στην εκάστοτε διεργασία είναι μέρος ενός συνόλου. Στο πλαίσιο μιας τέτοιας επαγωγικής προσέγγισης η επέκταση σε CPEs που δεν συμπεριλαμβάνονται άμεσα στην εκάστοτε διεργασία είναι αντιπαραγωγική. Το κόστος αυτής της ακρίβειας κατά τον προσδιορισμό του επιπέδου ασφάλειας στο πλαίσιο της εκάστοτε διεργασίας είναι βέβαια μια αυξημένη πολυπλοκότητα. Στο πλαίσιο λοιπόν του παραδείγματος, η επίπτωση της επιτυχούς επίθεσης αφορά στην διεργασία "ανάκτηση δεδομένων στην σχέση CPE 2 και CPE 1" και όχι στην εξεταζόμενη διεργασία "ανάκτηση δεδομένων στην σχέση CPE 3 και CPE 2" ή στην διεργασία "συλλογή δεδομένων μέσω του CPE 1".

Αν υιοθετήσουμε αυτήν την αφαιρετική θεώρηση σχετικά με την εκάστοτε διεργασία, η συσχέτιση του συντελεστή εξάρτησης απαιτήσεων ασφάλειας με αυτή οδηγεί στην συνθήκη πως το κάθε CPE κληρονομεί ουσιαστικά τις απαιτήσεις ασφάλειας της γονικής διεργασίας. Το πρόβλημα που δημιουργείται όμως είναι πως και πάλι απαντάται μια επιστροφή από το ειδικό στο γενικό – το κάθε *συγκεκριμένο* CPE κληρονομεί *γενικευμένες* απαιτήσεις ασφάλειας, ανεξαρτήτως του περιβάλλοντος και των χαρακτηριστικών του, συνθήκη που δεν εναρμονίζεται με το επίπεδο αφαιρετικότητας που αποσκοπούμε μέσω της προσέγγισης ARES.

Μια λύση του προβλήματος αυτού προκύπτει από την θεώρηση του συστήματος βαθμονόμησης ευπαθειών CVSS, το οποίο ανταποκρίνεται στο επίπεδο αφαιρετικότητας που μας αφορά, καθώς ασχολείται με *συγκεκριμένες* ευπάθειες στο πλαίσιο *συγκεκριμένου* ψηφιακού περιβάλλοντος. Στο πλαίσιο του συστήματος αυτού απαντάται μια διασκευή του προτεινόμενου συντελεστή εξάρτησης, μεταμφιεσμένου ως απαιτήσεις ασφάλειας (security requirements) για την κάθε πτυχή ασφάλειας ως τμήμα των *περιβαλλοντικών παραγόντων* της κάθε ευπάθειας, οι οποίες με την σειρά τους επηρεάζουν την αρχική κρίση σχετικά με την επίπτωση της ευπάθειας στην κάθε (γενική) πτυχή ασφάλειας, την εκμεταλλευσιμότητά της (exploitability) αλλά και το εύρος των επιπτώσεων (scope) της. Οι περιβαλλοντικοί παράγοντες της κάθε ευπάθειας εξαρτώνται από τα μέτρα προστασίας που έχουν υιοθετηθεί στο εκάστοτε *συγκεκριμένο* περιβάλλον. Αν, για παράδειγμα, μια ευπάθεια της οποίας η επίπτωση οδηγεί σε κατάλυση της διαθεσιμότητας αφορά στην υπηρεσία ssh και η σχετική θύρα στο συγκεκριμένο CPE είναι κλειστή, τότε οι απαιτήσεις ασφάλειας σχετικά με την διαθεσιμότητα για το συγκεκριμένο CPE είναι χαμηλές/μηδαμινές.

Μεταφέροντας αυτό το σκεπτικό στον προτεινόμενο συντελεστή εξάρτησης, θα πρέπει να ξεκινήσουμε από έναν ορισμό των απαιτήσεων ασφάλειας για την σχετική διεργασία υγείας, οι οποίες σε ένα δεύτερο βήμα θα πρέπει να τροποποιηθούν ώστε να ανταποκρίνονται στο συγκεκριμένο περιβάλλον του εκάστοτε CPE.

Για τον προσδιορισμό του συντελεστή εξάρτησης μπορεί να χρησιμοποιηθεί ως βάση η προσέγγιση του οργανισμού FDA που είδαμε παραπάνω (πίνακας 5.1), η οποία σχεδιάστηκε για τον καθορισμό του εύρους της βαρύτητας των πιθανών επιπτώσεων στην υγεία των ασθενών στο πλαίσιο της διαδικασίας εκτίμησης κινδύνων που ο οργανισμός προτείνει σε κατασκευαστές ιατρικών συσκευών.

Ο προσδιορισμός του συντελεστή εξάρτησης γίνεται μέσω της αντιστοίχησης των πιθανών επιπτώσεων στην υγεία σε περίπτωση κατάλυσης των απαιτήσεων της κάθε πτυχής ασφάλειας του σχετικού εξοπλισμού, σε μορφή ποιοτικής προσέγγισης με τα επίπεδα Χαμηλός, Μέτριος, Υψηλός, Πολύ Υψηλός, όπως παρουσιάζεται στον πίνακα 6.2.

Σε αυτό το σημείο παρεισφρέει ένας παράγοντας υποκειμενικότητας στην διαδικασία, ο οποίος και επενεργεί άμεσα και με μεγάλη βαρύτητα στο τελικό αποτέλεσμα υπολογισμού της σχετικής επικινδυνότητας. Η συνθήκη αυτή είναι όμως αναπόφευκτη δεδομένου του εύρους απαιτήσεων ασφάλειας στην περίπτωση της εκάστοτε διεργασία υγείας.

Επίπεδο επίπτωσης	Περιγραφή επίπτωσης στην υγεία των ασθενών σε περίπτωση κατάλυσης των απαιτήσεων της κάθε πτυχής ασφάλειας του σχετικού εξοπλισμού στο πλαίσιο της εξεταζόμενης διεργασίας υγείας	Συντελεστής Εξάρτησης
Χαμηλή	Πρόκληση προσωρινού τραυματισμού ή βλάβης που δεν απαιτεί επαγγελματική ιατρική παρέμβαση.	1
Σοβαρή	Πρόκληση τραυματισμού ή βλάβης που απαιτεί επαγγελματική ιατρική παρέμβαση.	2
Κρίσιμη	Πρόκληση μόνιμης βλάβης ή τραυματισμού που απειλεί την ζωή.	3

Καταστροφική	Πρόκληση θανάτου του ασθενή.	4

Πίνακας 6.2.: Προτεινόμενος τρόπος προσδιορισμού του συντελεστή εξάρτησης διεργασίας υγείας από την κάθε πτυχή ασφάλειας στο πλαίσιο των σχετικών CPE

Αφού υπολογιστεί το επίπεδο επικινδυνότητας μέσω του ARES για το κάθε CAPEC, θα πρέπει να επιστρέψουμε στον συντελεστή που ορίστηκε για να μετρήσουμε την επίπτωση της επιμέρους επικινδυνότητας για την εκάστοτε πτυχή ασφάλειας, η οποία και είναι το γινόμενο του επιπέδου επικινδυνότητας του εκάστοτε CAPEC και του συντελεστή εξάρτησης, δηλαδή:

$$\textit{Επιμέρους επικινδυνότητα CAPEC}_{(\text{CIA})} = (\text{Πιθανότητα}_{\text{CAPEC}} * \text{Επίπτωση}_{(\text{CIA, Πηγή CAPEC/CVSS})}) * \text{συντελεστής εξάρτησης}_{(\text{CIA})}$$

Η αντιστοίχιση σε αυτό το πλαίσιο μπορεί να γίνει παραδειγματικά βάσει του παρακάτω πίνακα επικινδυνότητας (πίνακας 6.3.). Εδώ, και πάλι, η αντιστοίχηση των επιπέδων επικινδυνότητας γίνεται υποκειμενικά. Ο εκάστοτε χρήστης της μεθόδου μπορεί συνεπώς να την τροποποιήσει ώστε να ανταποκρίνεται στις εξατομικευμένες απαιτήσεις ασφάλειας που μπορεί να έχει.

Συντελεστής εξάρτησης / *Επίπεδο επικινδυνότητας CAPEC*	Χαμηλός	Μέτριος	Υψηλός	Πολύ υψηλός
Πολύ υψηλή	Μέτρια	Υψηλή	Πολύ υψηλή	Πολύ υψηλή
Υψηλή	Χαμηλή	Μέτρια	Υψηλή	Πολύ υψηλή
Μέτρια	Χαμηλή	Μέτρια	Μέτρια	Υψηλή
Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή	Μέτρια

Πίνακας 6.3.: Προτεινόμενος πίνακας επικινδυνότητας του εκάστοτε CAPEC βάσει του συντελεστή εξάρτησης της κάθε πτυχής ασφάλειας

Αφού προσδιοριστεί το επιμέρους επίπεδο επικινδυνότητας του CAPEC ως προς την κάθε πτυχή ασφάλειας, επιστρέφουμε στην προσέγγιση ARES, σύμφωνα με την οποία επιλέγεται η υψηλότερη τιμή ως το τελικό επίπεδο επικινδυνότητας του εξεταζόμενου CAPEC.

Για τον τελικό προσδιορισμό του επιπέδου επικινδυνότητας του CPE επιλέγεται το CAPEC με την υψηλότερη τιμή επικινδυνότητας, η οποία καθορίζει το ανώτατο όριο κινδύνου το οποίο και χρησιμοποιείται ως η τιμή κινδύνου για το συγκεκριμένο CPE. Αφού προσδιοριστεί κατά

αυτόν τον τρόπο η τιμή κινδύνου όλων των εξεταζόμενων CPEs, καθορίζεται το τελικό επίπεδο επικινδυνότητας βάσει της ανώτερης τιμής κινδύνου μεταξύ τους.

Την χρησιμότητα του συντελεστή εξάρτησης αναδεικνύει το εξής παράδειγμα: έστω ότι έχουμε μια ευπάθεια (CVE), της οποίας η επίπτωση στην διαθεσιμότητα είναι χαμηλή ενώ στην εμπιστευτικότητα είναι μέτρια. Σύμφωνα με το εξεταζόμενο CAPEC, η πιθανότητα ορίζεται ως μέτρια.

Εκτελώντας την προσέγγιση ARES σε αυτό το παράδειγμα, το επίπεδο επικινδυνότητας διαμορφώνεται ως εξής:

Επιμέρους επικινδυνότητα CAPEC$_{\text{Εμπιστευτικότητα}}$ = CAPEC$_{\text{Επίπτωση στην εμπιστευτικότητα}}$ * CAPEC$_{\text{Πιθανότητα}}$ = Μέτρια * Μέτρια = Μέτρια

Επιμέρους επικινδυνότητα CAPEC$_{\text{Διαθεσιμότητα}}$ = CAPEC$_{\text{Επίπτωση στην διαθεσιμότητα}}$ * CAPEC$_{\text{Πιθανότητα}}$ = Χαμηλή * Μέτρια = Μέτρια

Επιμέρους επικινδυνότητα $_{\text{CAPEC}}$ = Μέτρια

Αν τώρα συστήσουμε στο παράδειγμα έναν πολύ υψηλό συντελεστή για την διαθεσιμότητα και έναν χαμηλό συντελεστή για την εμπιστευτικότητα, συνδυασμός που θα μπορούσε για παράδειγμα να ανταποκρίνεται στις απαιτήσεις ασφάλειας κάποιου βηματοδότη, οι τιμές διαμορφώνονται ως εξής:

Επιμέρους επικινδυνότητα CAPEC$_{\text{Εμπιστευτικότητα}}$ = Επικινδυνότητα$_{\text{Εμπιστευτικότητα}}$ * Συντελεστής εξάρτησης$_{\text{Εμπιστευτικότητα}}$ = Μέτρια * Χαμηλή = Χαμηλή

Επιμέρους επικινδυνότητα CAPEC$_{\text{Διαθεσιμότητα}}$ = Επικινδυνότητα$_{\text{Διαθεσιμότητα}}$ * Συντελεστής εξάρτησης$_{\text{Διαθεσιμότητα}}$ = Μέτρια * Πολύ υψηλή = Υψηλή

Επιμέρους επικινδυνότητα $_{\text{CAPEC}}$ = Υψηλή

Ο συντελεστής εξάρτησης εκφράζει συνεπώς επιτυχώς τους παράγοντες που μπορούν να οδηγήσουν σε ζημιά στην υγεία των ασθενών, μεταβάλλοντας, πολλές φορές, το επίπεδο επικινδυνότητας έτσι ώστε να αντικατοπτρίζει τις απαιτήσεις ασφάλειας σε ένα υγειονομικό πλαίσιο.

6.2.2. Επιλογή του συντελεστή επίπτωσης

Μια δεύτερη προτεινόμενη τροποποίηση της προσέγγισης ARES είναι η εξάρτηση του συντελεστή επίπτωσης από το εκάστοτε CAPEC και όχι βάσει της σχετικής τιμής του διανύσματος CVSS του εκάστοτε CVE.

Ο λόγος για αυτό, είναι πως η τιμή στο πλαίσιο των CAPEC είναι στενά συνυφασμένος με την εκάστοτε αδυναμία (CWE) [81], σε αντίθεση με την σχετική τιμή στο πλαίσιο του διανύσματος CVSS, όπου και αφορά στο εκάστοτε (συγκεκριμένο) CVE. Καθώς μέσω της προσέγγισης ARES έχουμε πρόσβαση στα CWE που θα μπορούσαν να αφορούν στο εκάστοτε CPE, έχουμε πρόσβαση στις *συνθήκες* που μπορούν να οδηγήσουν σε περαιτέρω ευπάθειες (CVEs). Το εύρος των πιθανών επιπτώσεων των ευπαθειών και η ασθένεια στην οποία βασίζονται διαφέρουν, συνθήκη που με την σειρά της επηρεάζει άμεσα έναν παράγοντα ο οποίος συνυπολογίζεται κατά την εκτίμηση του σχετικού κινδύνου.

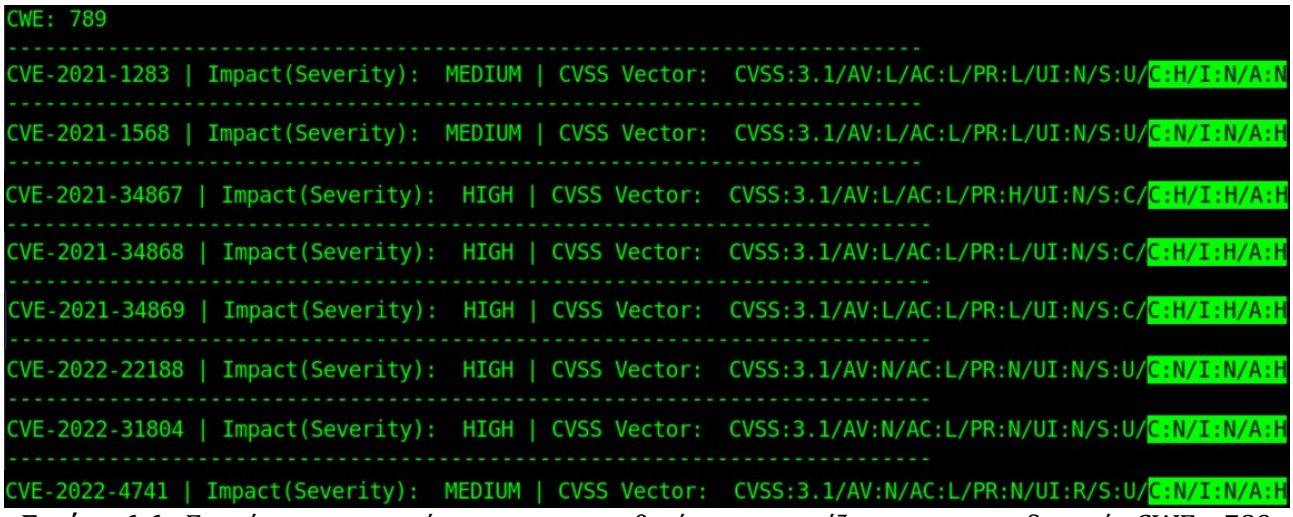
Αν εξετάσουμε για παράδειγμα την αδυναμία CWE – 789, παρατηρούμε πως σχετίζεται με 8 διαφορετικές ευπάθειες, των οποίων ο βαθμός επίπτωσης κυμαίνεται από μέτριος έως και ψηλός (εικόνα 6.5.):

```
CWE: 789
--------------------------------------------------------------------------
CVE-2021-1283 | Impact(Severity):  MEDIUM | CVSS Vector:  CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
--------------------------------------------------------------------------
CVE-2021-1568 | Impact(Severity):  MEDIUM | CVSS Vector:  CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
--------------------------------------------------------------------------
CVE-2021-34867 | Impact(Severity):  HIGH | CVSS Vector:  CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
--------------------------------------------------------------------------
CVE-2021-34868 | Impact(Severity):  HIGH | CVSS Vector:  CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
--------------------------------------------------------------------------
CVE-2021-34869 | Impact(Severity):  HIGH | CVSS Vector:  CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
--------------------------------------------------------------------------
CVE-2022-22188 | Impact(Severity):  HIGH | CVSS Vector:  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
--------------------------------------------------------------------------
CVE-2022-31804 | Impact(Severity):  HIGH | CVSS Vector:  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
--------------------------------------------------------------------------
CVE-2022-4741 | Impact(Severity):  MEDIUM | CVSS Vector:  CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
```

Εικόνα 6.5.: Κατάλογος ευπαθειών και των επιπτώσεών τους που σχετίζονται με την αδυναμία CWE – 789.

Αν εξετάσουμε τις επιπτώσεις του διανύσματος CVSS της κάθε ευπάθειας, στο τέλος του οποίου αποτυπώνεται ο βαθμός επίπτωσης της ευπάθειας στην εμπιστευτικότητα (C: επίπτωση), ακεραιότητα (I: επίπτωση) και διαθεσιμότητα (A: επίπτωση), όπως επισημαίνεται στην εικόνα 6.6., παρατηρούμε πως μπορούν να έχουν *πολύ* διαφορετικές επιπτώσεις σε κάθε μια από τις πτυχές ασφάλειας, με τιμές οι οποίες κυμαίνονται από καμία (none – N) έως και

υψηλή (high – H), ή συνδυαστικά από κατανομές εύρους καμία – καμία – υψηλή έως και υψηλή/υψηλή/υψηλή.



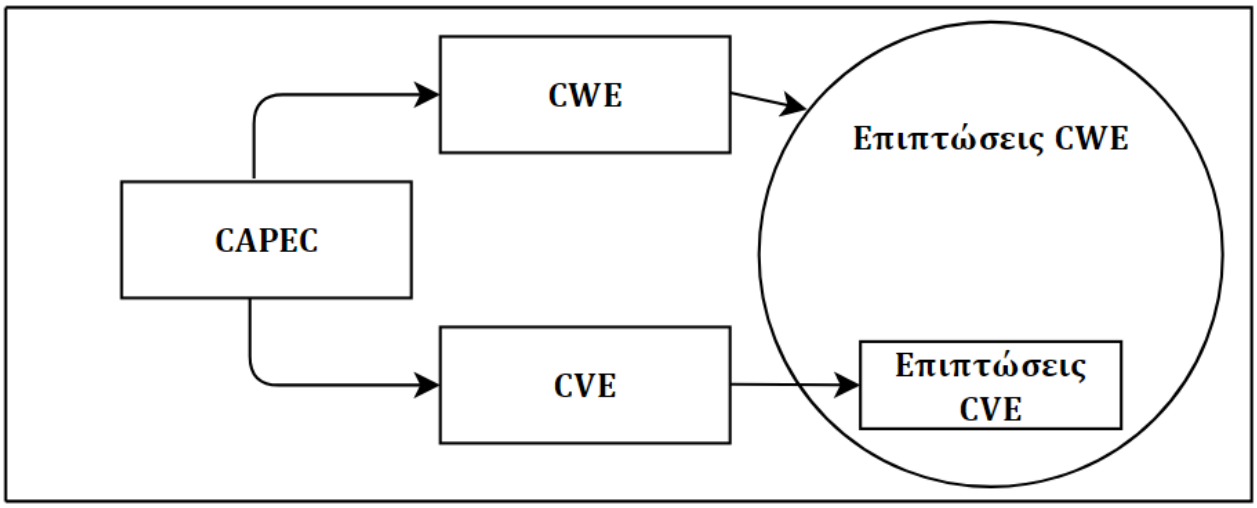
Εικόνα 6.6.: Επισήμανση επιπτώσεων των ευπαθειών που σχετίζονται με την αδυναμία CWE – 789 στην κάθε πτυχή ασφάλειας βάσει του διανύσματος CVSS τους.

Αν λοιπόν η εκτίμηση της επικινδυνότητας βασιστεί στις σχετικές τιμές συντελεστή επίπτωσης του εκάστοτε διανύσματος CVSS, η εκτίμηση είναι μεν ακριβής, καθώς περιορίζεται σε υπάρχουσες ευπάθειες, αλλά ταυτόχρονα περιορίζει το πρίσμα της εκτίμησης, καθώς την κατευθύνει στο *σύμπτωμα* κάποιας αδυναμίας και συνεπώς όχι στην γενεσιουργό κατάσταση της εκάστοτε ευπάθειας.

Το πρόβλημα του εύρους των επιπτώσεων εντείνεται αν συνυπολογίσουμε το γεγονός πως η κάθε ευπάθεια υπό την έννοια κάποιου CVE αφορά σε ευπάθεια που αφενός *αποκαλύφθηκε* και αφετέρου *δημοσιεύτηκε*, πριν καταχωρηθεί ως CVE. Αυτό με την σειρά του σημαίνει πως η εξάρτηση της τιμής βαρύτητας της εκάστοτε επίπτωσης κάποιου CVE αφορά αποκλειστικά σε *δημοσίως προσβάσιμες* πληροφορίες του *παρελθόντος* και συνεπάγεται ταυτόχρονα τον περιορισμό του εύρους βαρύτητας των επιπτώσεων σε πολύ συγκεκριμένα σενάρια επίθεσης – αυτά που εκμεταλλεύονται την ύπαρξη της συγκεκριμένης ευπάθειας.

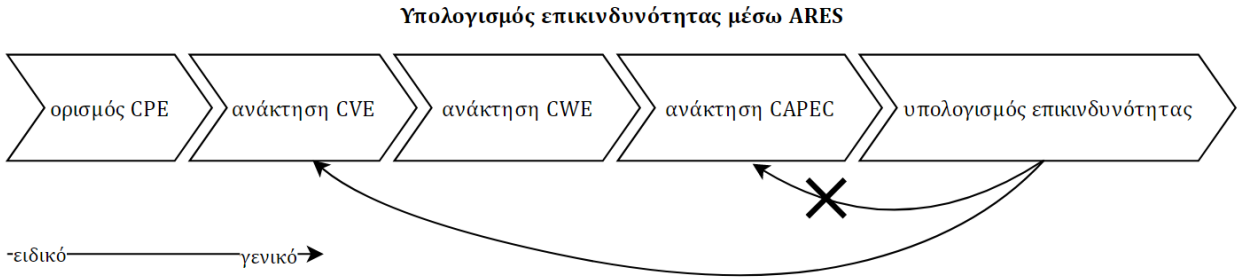
Ένας τέτοιου τύπου περιορισμός μπορεί να αποφευχθεί από την στιγμή που μέσω της προσέγγισης ARES έχουμε πρόσβαση στις αδυναμίες που καθιστούν δυνατή την ύπαρξη της εκάστοτε ευπάθειας και που μπορούν, κατόπιν επιτυχούς εκμετάλλευσης με τρόπο που περι-

γράφεται μέσω του εκάστοτε σχετικού CAPEC, να οδηγήσουν σε μεγαλύτερο εύρος επιπτώσεων, το οποίο *περιλαμβάνει* τις επιπτώσεις της εκάστοτε συγκεκριμένης ευπάθειας, όπως φαίνεται στην εικόνα 6.7.:



Εικόνα 6.7.: Εύρος επιπτώσεων CWE/CVE

Επιπλέον, σε αυτό το σημείο, η χρήση των τιμών του συντελεστή επίπτωσης του εκάστοτε διανύσματος CVSS αντί για την σχετική τιμή του εκάστοτε CAPEC δεν εναρμονίζεται με την διαδικασία υπολογισμού επικινδυνότητας του ARES καθώς συνεπάγεται εισαγωγή παραγωγικών συλλογισμών στο πλαίσιο μιας επαγωγικής προσέγγισης, ή, με άλλα λόγια, εκτελείται επιστροφή σε ειδικά δεδομένα σε στάδιο της διαδικασίας που αφορά σε πιο γενικευμένα συμπεράσματα όπως φαίνεται στην εικόνα 6.8..



Εικόνα 6.8.: Επιστροφή σε τιμές επίπτωσης CVSS αντί για την σχετική τιμή CAPEC

Αυτή η διάσπαση της επαγωγικής προσέγγισης του ARES έχει και πρακτικές προεκτάσεις στον υπολογισμό του αποτελέσματος καθώς συνδυάζονται γενικές τιμές πιθανότητας επιτυχημένης

επίθεσης (CAPEC) με ειδικές τιμές επίπτωσης του εκάστοτε CVE (CVSS), οδηγώντας έτσι σε έναν υπολογισμό επικινδυνότητας που συνδυάζει τυπικά και ειδικά χαρακτηριστικά.

Αν, για παράδειγμα, κατά την εξέταση κάποιου $CAPEC_x$ το οποίο και φέρει *τυπικά* πολύ υψηλή πιθανότητα επιτυχίας και έχει *τυπικά* επιπτώσεις μέτριας βαρύτητας συνυπολογίσουμε μέσω του ARES την τιμή πιθανότητας του $CAPEC_x$ με τις επιπτώσεις *συγκεκριμένης* ευπάθειας η οποία και φέρει πολύ χαμηλή πιθανότητα επιτυχούς εκμετάλλευσης (κάτι που αγνοείται αν χρησιμοποιήσουμε μόνο την τιμή βαρύτητας των επιπτώσεων της) αλλά έχει επιπτώσεις πολύ υψηλής βαρύτητας, καταλήγουμε σε ένα αποτέλεσμα που στην πραγματικότητα αφορά σε ένα πλασματικό $CAPEC_y$ το οποίο και περιγράφει μοτίβο επίθεσης το οποίο ταυτίζεται με το $CAPEC_x$ ως προς τα επιμέρους χαρακτηριστικά του, φέρει όμως πολύ υψηλή πιθανότητα επιτυχίας σχετικής επίθεσης και επιπτώσεις πολύ υψηλής βαρύτητας, συνθήκη που δεν αντι-κατοπτρίζει την πραγματικότητα, καθώς το $CAPEC_y$ δεν υπάρχει.

Λαμβάνοντας υπόψη τα παραπάνω, το πλαίσιο στο οποίο κινούμαστε αλλά και την αξία του αντικειμένου προστασίας, θεωρούμε πως θα ήταν ορθότερο να βασιστούμε σε ένα μεγαλύτερο εύρος επιπτώσεων, οι οποίες και προκύπτουν από την εξάρτηση από την εκάστοτε αδυναμία, και κατ' επέκταση από το εκάστοτε CAPEC.

Κεφάλαιο 7
Παρουσίαση λογισμικού

Στο πλαίσιο του κεφαλαίου 7 παρουσιάζεται το λογισμικό που αναπτύχθηκε για την υλοποίηση της προσέγγισης που παρουσιάστηκε στο κεφάλαιο 6. Αφού αρχικά παρουσιαστούν τα χαρακτηριστικά του λογισμικού (7.1.) και η διαδικασία υπολογισμών και εξαγωγής αποτελεσμάτων βάσει εφαρμογής στην περίπτωση ενός πρότυπου συστήματος (7.2.), θα σχολιαστεί ως προς τις αδυναμίες και τους περιορισμούς του (7.3.).

7.1. Χαρακτηριστικά λογισμικού

Για την ανάπτυξη του λογισμικού επιλέχθηκε η γλώσσα προγραμματισμού Python (έκδοση 3.9.2.) καθώς δεν απαιτεί την διενέργεια compiling, είναι αντικειμενοστραφής και υπάρχουν για αυτήν αρκετά πακέτα υποστήριξης (βιβλιοθήκες). Το πρόγραμμα αναπτύχθηκε σε περιβάλλον Linux.

7.2. Διαδικασία υπολογισμών και εξαγωγής αποτελεσμάτων

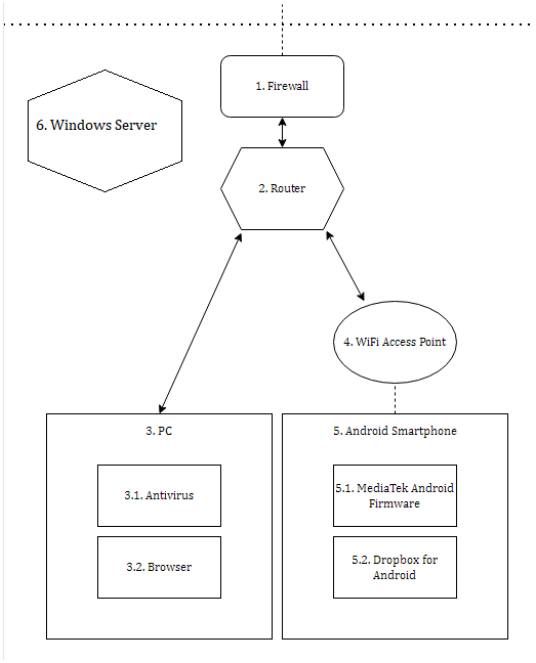
Η εκτέλεση του αλγορίθμου εκτίμησης του επιπέδου επικινδυνότητας προϋποθέτει την ύπαρξη δύο αρχείων τα οποία και περιέχουν απαραίτητα δεδομένα για την διαδικασία biclustering (capec2cpe.xml), στην οποία θα επιστρέψουμε παρακάτω, και για την διαδικασία ταξινόμησης που την ακολουθεί (CAPECs.csv και CPEs.csv).

7.2.1. Περιγραφή του πρότυπου συστήματος

Το πρότυπο σύστημα (εικόνα 7.1.) το οποίο θα χρησιμοποιθεί ως παράδειγμα αποτελείται από τα εξής στοιχεία (CPEs):

1. cpe:2.3:h:asus:dsl-n17u:-:*:*:*:*:*:*:*
2. cpe:2.3:a:a10networks:acos_web_application_firewall:4.1.1:p3:*:*:*:*:*:*
3. cpe:2.3:h:dlink:dir-816l:b1:*:*:*:*:*:*:*
4. cpe:2.3:a:microsoft:internet_information_server:7.5:*:*:*:*:*:*:*
5. cpe:2.3:a:malwarebytes:malwarebytes:3.3.1.2183:*:*:*:premium:*:*:*
6. cpe:2.3:a:avast:secure_browser:77.1.1831.91:*:*:*:*:*:*:*
7. cpe:2.3:o:mediatek:mt8163_firmware:-:*:*:*:*:android:*:*
8. cpe:2.3:a:dropbox:dropbox:98.2.2:*:*:*:*:android:*:*

Σκοπός του παραδείγματος είναι η ανάδειξη της λειτουργίας του συντελεστή εξάρτησης της κάθε πτυχής ασφάλειας στο πλαίσιο ενός ολοκληρωμένου συστήματος. Τα συστατικά του στοιχεία επιλέχθηκαν αποκλειστικά βάσει του κριτηρίου μιας γενικότερης συνοχής.



Εικόνα 7.1.: Εικονική αναπαράσταση του πρότυπου συστήματος

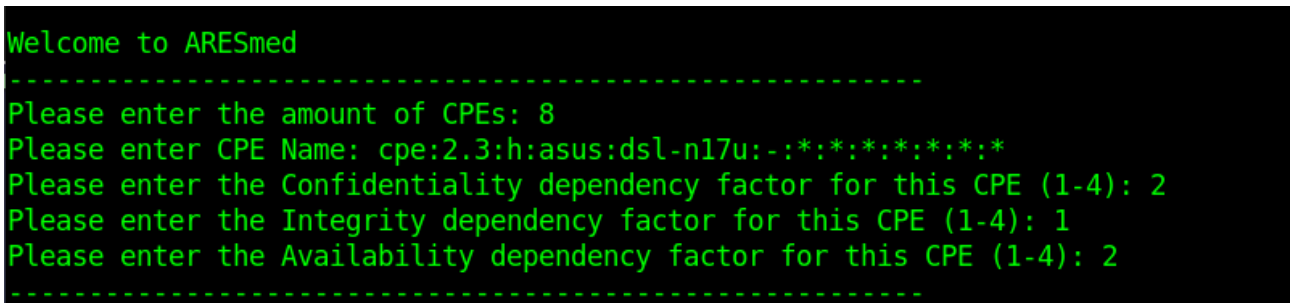
7.2.2. Εισαγωγή δεδομένων από τον χρήστη

Αφού εκτελεστεί ο κώδικας του αρχείου aresmed.py, το λογισμικό ζητά την εισαγωγή δεδομένων από τον χρήστη (εικόνα 7.2), για την οποία χρησιμοποιείται η γραμμή εντολών (command-line interface – CLI), σχετικά με:

1. τον αριθμό των CPEs που θα εξεταστούν, ο οποίος και καθορίζει τον αριθμό επαναλήψεων προτροπής του χρήστη για την εισαγωγή δεδομένων των που ακολουθούν,

2. το όνομα του εκάστοτε CPE χρησιμοποιώντας το σχετικό σχήμα ονοματοδοσίας,

3. τον συντελεστή εξάρτησης της διεργασίας υγείας από το κάθε CPE ως προς την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα.



Εικόνα 7.2.: Εισαγωγή δεδομένων από τον χρήστη για την περίπτωση του πρώτου CPE

7.2.3. Ανάκτηση ευπαθειών, βαθμονόμησης CVSS και ασθενειών του κάθε CPE

Με την ολοκλήρωση εισαγωγής των δεδομένων από τον χρήστη πραγματοποιείται διασύνδεση με τις βάσεις δεδομένων του NIST, αξιοποιώντας την βιβλιοθήκη nvdlib η οποία και διευκολύνει την διαδικασία. Βάσει των ερωτημάτων (queries) που εκτελούνται επιστρέφονται, για κάθε CPE που έχει εισαχθεί από τον χρήστη, τα εξής, όπως φαίνεται παραδειγματικά για το πρώτο CPE του πρότυπου συστήματος στην εικόνα 7.3.:

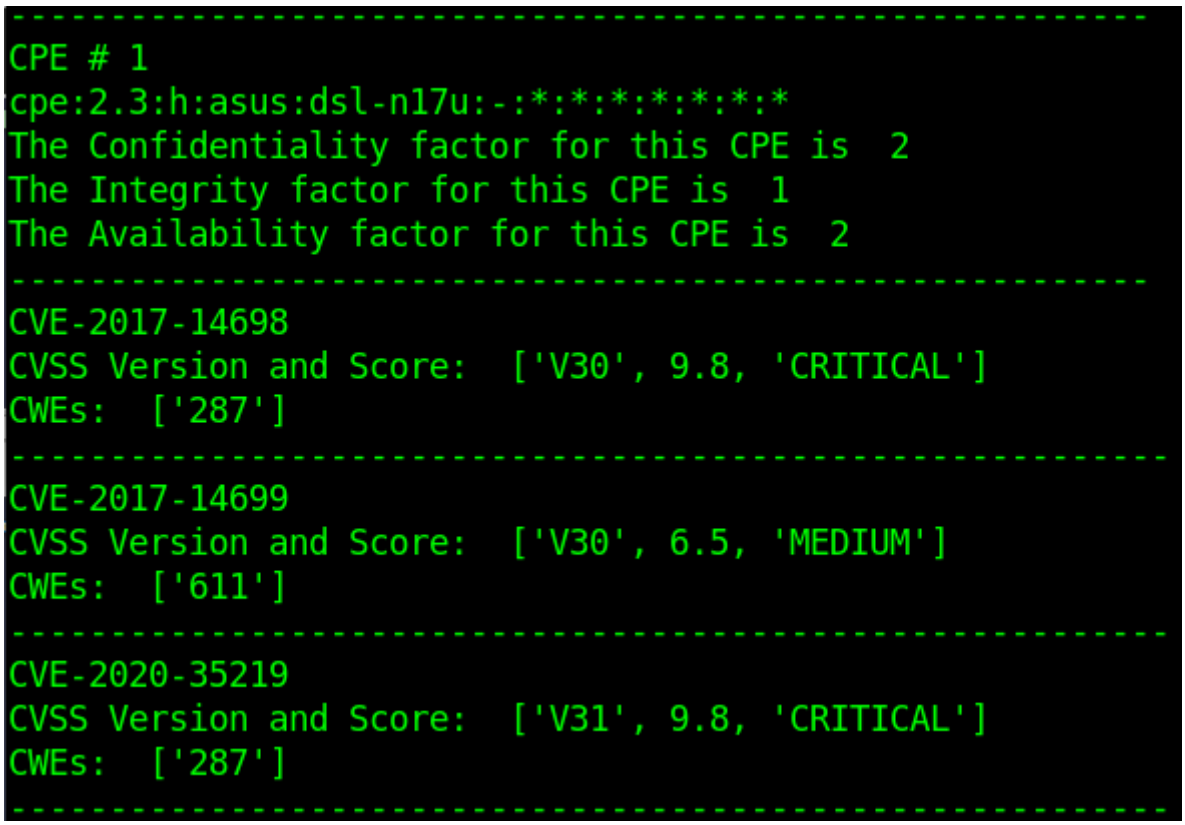
1. το όνομα του CPE,

2. οι συντελεστές εξάρτησης εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας που επιλέχθηκαν για αυτό,

3. οι ευπάθειες (CVEs), οι οποίες και σχετίζονται με το συγκεκριμένο CPE,

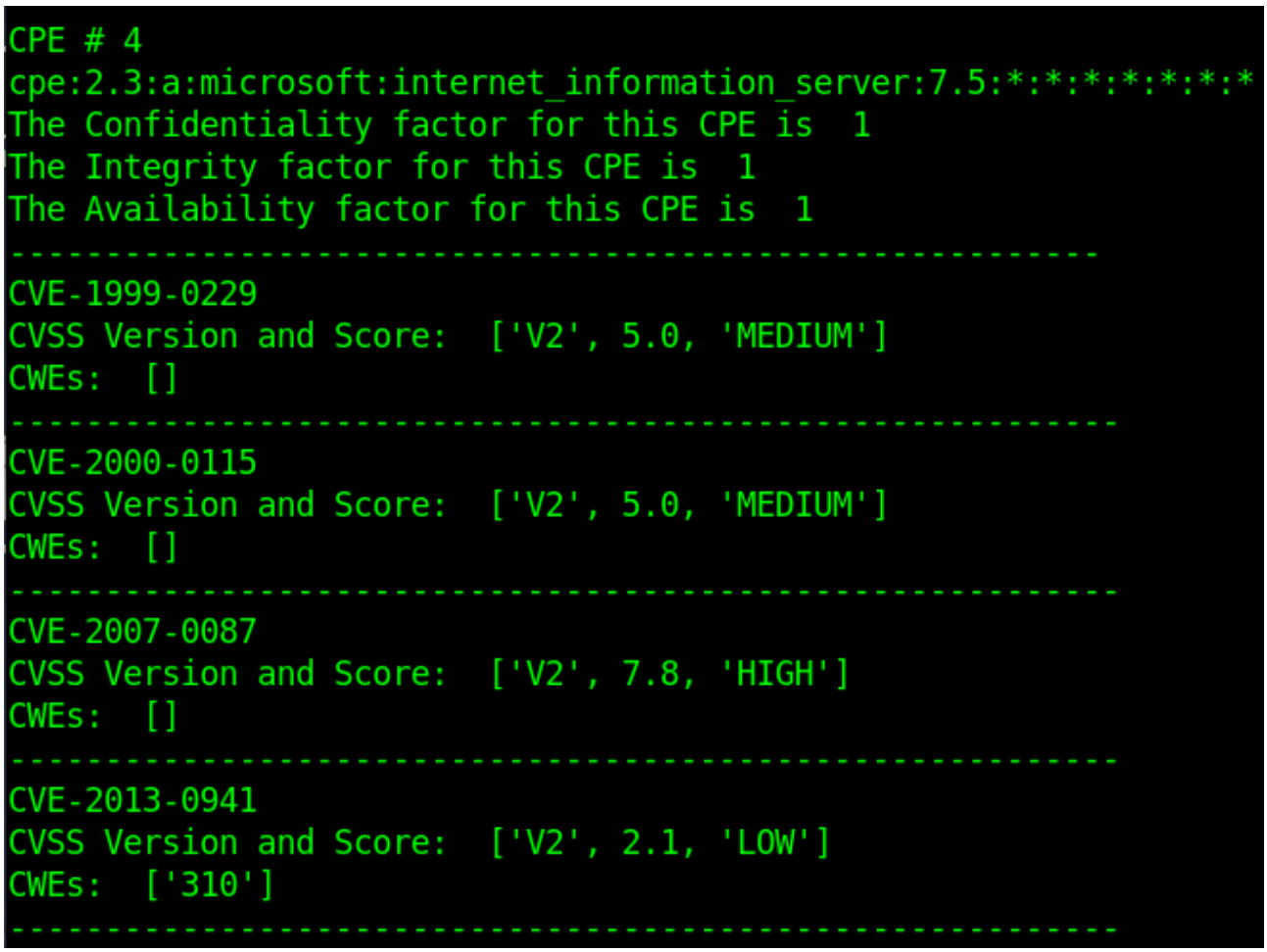
4. η έκδοση της σχετικής βαθμονόμησης CVSS όπως επίσης ο βαθμός επίπτωσης και ο ποιοτικός χαρακτηρισμός του,

5. οι αδυναμίες (CWEs) που σχετίζονται με κάθε CVE.



Εικόνα 7.3.: Ανάκτηση CVEs, της σχετικής βαθμονόμησης CVSS και σχετικών CWEs στην περίπτωση του πρώτου CPE

Καθώς στο πλαίσιο εντοπισμού των σχετικών αδυναμιών (CWEs) υπάρχει περίπτωση είτε να μην υπάρχει καταχωρημένη αδυναμία για εκάστοτε ευπάθεια (CVE), είτε επειδή δεν υπάρχουν επαρκείς σχετικές πληροφορίες για την σχετική ταξινόμησή ή επειδή οι λεπτομέρειες είναι άγνωστες ή απροσδιόριστες, οπότε και η σχετική καταχώρηση είναι "NVD-CWE-noinfo", είτε η εκάστοτε αδυναμία να μην συμπεριλαμβάνεται στο υποσύνολο των αδυναμιών που χρησιμοποιείται από τον οργανισμό NIST, κάτι που με την σειρά του οδηγεί στην καταχώρηση "NVD-CWE-Other". Σε αυτές τις περιπτώσεις το σχετικό πεδίο επιστρέφεται κενό (εικόνα 7.4.) και ο υπολογισμός της επικινδυνότητας της ευπάθειας στηρίζεται στην τιμή βαρύτητας της βαθμονόμησης CVSS κατόπιν μετατροπής για να ανταποκρίνεται στο σύστημα βαθμονόμησης του λογισμικού, ενημερώνοντας τον χρήστη πως τιμές CVSS έχουν συμπεριληφθεί στο τελικό αποτέλεσμα υπολογισμού του επιπέδου επικινδυνότητας του εκάστοτε CPE (εικόνα 7.5.), για τον υπολογισμό του οποίου συνυπολογίζεται σε ένα τελευταίο στάδιο και η ανώτατη των τιμών CVSS για την εκάστοτε ευπάθεια που δεν μπορεί να συνδεθεί με κάποια CWE και κατ'επέκταση με κάποιο(α) CAPEC.

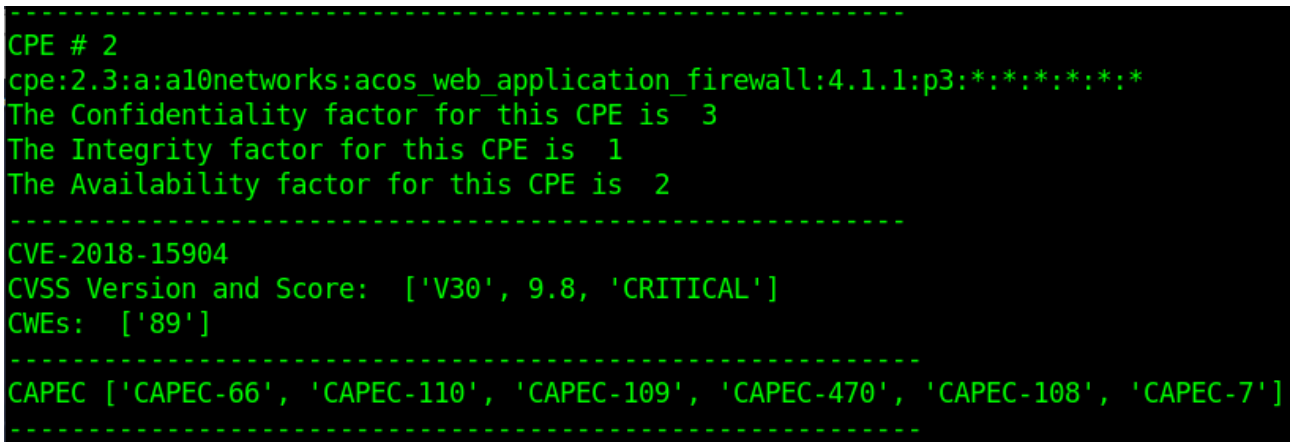


Εικόνα 7.4.: Αδυναμία ανάκτησης τιμών CWE στην περίπτωση του τέταρτου CPE

Εικόνα 7.5.: Ενημέρωση του χρήστη πως στον υπολογισμό του τελικού αποτελέσματος συνυπολογίστηκαν τιμές CVSS (CPE 4)

7.2.4. Ανάκτηση σχετικών CAPEC

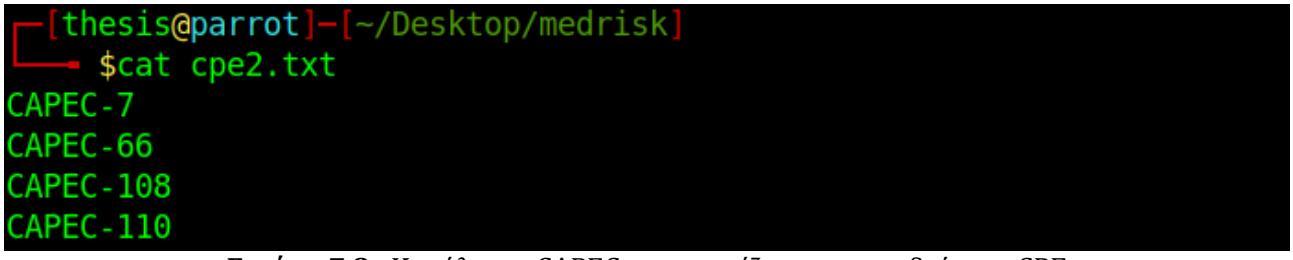
Επόμενο βήμα είναι η πραγματοποίηση διασύνδεσης με τις βάσεις δεδομένων του κέντρου αντιμετώπισης περιστατικών κυβερνοασφάλειας του Λουξεμβούργου (The Computer Incident Response Center Luxembourg (CIRCL)), μέσω της οποίας ανακτώνται όλα τα CAPEC τα οποία αντιστοιχούν στις αδυναμίες (CWE) που εντοπίστηκαν. Το αποτέλεσμα αυτής της διαδικασίας φαίνεται στην εικόνα 7.6.:



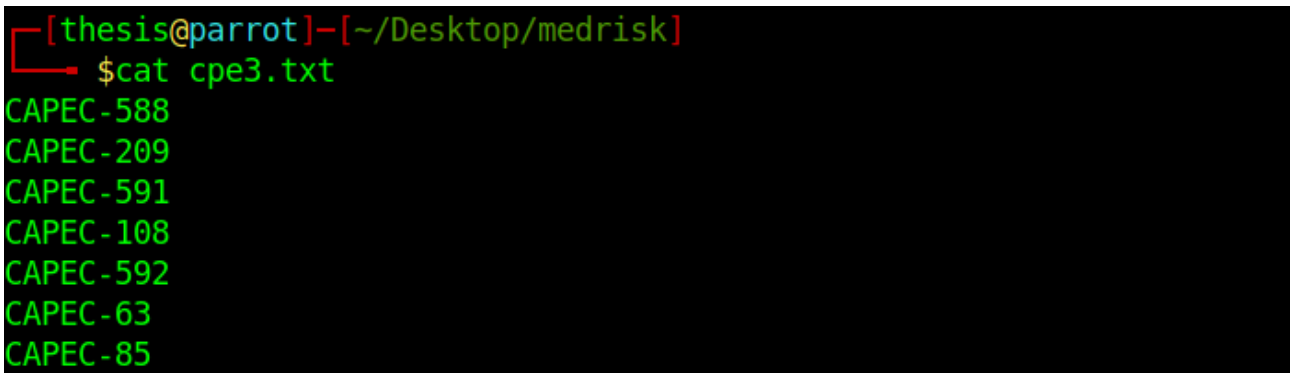
Εικόνα 7.6.: Ανάκτηση CAPEC στην περίπτωση του δεύτερου CPE

Για κάθε CPE δημιουργείται ένας κατάλογος των CAPEC που προέκυψαν, σε μορφή αρχείου .txt (εικόνες 7.7. – 7.14.):

Εικόνα 7.7.: Κατάλογος CAPEC που σχετίζονται με το πρώτο CPE



Εικόνα 7.8.: Κατάλογος CAPEC που σχετίζονται με το δεύτερο CPE



Εικόνα 7.9.: Κατάλογος CAPEC που σχετίζονται με το τρίτο CPE

Εικόνα 7.10.: Κατάλογος CAPEC που σχετίζονται με το τέταρτο CPE

```
┌─[thesis@parrot]─[~/Desktop/medrisk]
└──╼ $cat cpe5.txt
CAPEC-42
CAPEC-267
CAPEC-78
CAPEC-109
CAPEC-53
CAPEC-79
CAPEC-47
CAPEC-135
CAPEC-120
CAPEC-9
CAPEC-66
CAPEC-13
CAPEC-71
CAPEC-7
CAPEC-52
CAPEC-88
CAPEC-10
CAPEC-72
CAPEC-45
CAPEC-67
CAPEC-64
CAPEC-80
CAPEC-3
CAPEC-250
CAPEC-43
CAPEC-153
CAPEC-261
CAPEC-73
CAPEC-473
CAPEC-110
CAPEC-24
CAPEC-23
CAPEC-46
CAPEC-8
CAPEC-28
```

Εικόνα 7.11.: Κατάλογος CAPEC που σχετίζονται με το πέμπτο CPE

```
┌─[thesis@parrot]─[~/Desktop/medrisk]
└──╼ $cat cpe6.txt
CAPEC-588
CAPEC-209
CAPEC-591
CAPEC-592
CAPEC-63
CAPEC-85
```

Εικόνα 7.12.: Κατάλογος CAPEC που σχετίζονται με το έκτο CPE

```
┌─[thesis@parrot]─[~/Desktop/medrisk]
└──╼ $cat cpe7.txt
CAPEC-88
CAPEC-43
CAPEC-15
CAPEC-108
```

Εικόνα 7.13.: Κατάλογος CAPEC που σχετίζονται με το έβδομο CPE

```
┌─[thesis@parrot]─[~/Desktop/medrisk]
└──╼ $cat cpe8.txt
CAPEC-194
CAPEC-650
CAPEC-57
CAPEC-114
CAPEC-94
CAPEC-22
CAPEC-151
CAPEC-633
CAPEC-593
CAPEC-115
```

Εικόνα 7.14.: Κατάλογος CAPEC που σχετίζονται με το όγδοο CPE

7.2.5. Διαδικασίες biclustering και ταξινόμησης

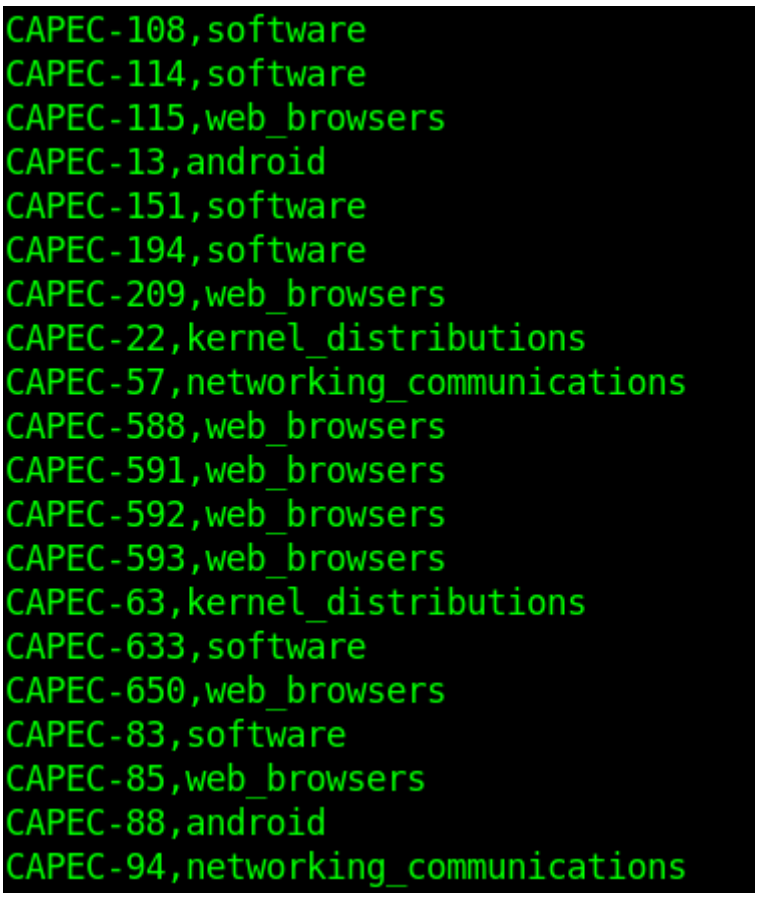
Επόμενο βήμα είναι η διαδικασία biclustering, μέσω της οποίας επιτυγχάνεται αποσυμφόρηση της λίστας των CAPEC τα οποία και συνυπολογίζονται στο πλαίσιο προσδιορισμού του συνολικού επιπέδου επικινδυνότητας μέσω απόρριψης των CAPEC που δεν μπορούν αντικειμενικά να αφορούν το εκάστοτε CPE.

Μέσω χρήσης του αλγορίθμου UMDA (Univariate Marginal Distribution Algorithm) ο οποίος προτείνεται από την προσέγγιση ARES [79] δημιουργούνται ομάδες οι οποίες αποτελούνται από CPE και CAPEC με την μέγιστη δυνατή λογική συσχέτιση. Η εφαρμογή της χαρτογράφησης γίνεται μέσω του προκατασκευασμένου αρχείου capec2cpe.xml, το οποίο και χρησιμοποιείται για την εκτέλεση αυτής της διαδικασίας. Σε περίπτωση που το εκάστοτε εξεταζόμενο CAPEC δεν εμφανίζεται στην ίδια λίστα με το CPE στο οποίο αντιστοιχήθηκε, απορρίπτεται από την διαδικασία προσδιορισμού του συνολικού επιπέδου επικινδυνότητας.

Την διαδικασία biclustering ακολουθεί η διαδικασία ταξινόμησης, στο πλαίσιο της οποίας τα CPE και τα CAPEC ταξινομούνται με ανάλογο τρόπο και εντάσσονται σε όμοιες κατηγορίες, στο παράδειγμά μας με την μορφή των αρχείων CPEs.csv (εικόνα 7.15.) και CAPECs.csv (εικόνα 7.16.). Μέσω του λογισμικού εντοπίζεται η κατηγορία του εκάστοτε CPE και του εκάστοτε CAPEC. Αν τα αποτελέσματα ταυτίζονται, το εκάστοτε CAPEC διατηρείται – αλλιώς απορρίπτεται. Τα αποτελέσματα της διαδικασίας biclustering και ταξινόμησης φαίνονται στις εικόνες καταχωρούνται σε αρχεία τύπου .csv για το κάθε CPE, στα οποία προστίθεται το αποτέλεσμα του υπολογισμού του επιμέρους επιπέδου επικινδυνότητας και θα παρουσιαστούν παρακάτω.

	A	B	C
1	ASUS DSL-N17U	networking_communications	cpe:2.3:h:asus:dsl-n17u:-:*:*:*:*:*:*:*
2	A10 Networks Advanced Core Operating System (ACOS) Web Application Firewall (WAF) 4.1.1 Patch 3	networking_communications	cpe:2.3:a:a10networks:acos_web_application_firewall:4.1.1:p3:*:*:*:*:*:*
3	D-Link DIR-816L B1	networking_communications	cpe:2.3:h:dlink:dir-816l:b1:*:*:*:*:*:*:*
4	Microsoft Internet Information Services (IIS) 7.5	kernel_distributions	cpe:2.3:a:microsoft:internet_information_server:7.5:*:*:*:*:*:*:*
5	Malwarebytes 3.3.1.2183 Premium Edition	support_utilities	cpe:2.3:a:malwarebytes:malwarebytes:3.3.1.2183:*:*:premium:*:*:*
6	Avast Secure Browser 77.1.1831.91	web_browsers	cpe:2.3:a:avast:secure_browser:77.1.1831.91:*:*:*:*:*:*:*
7	Mediatek MT8163 Firmware for Android	android	cpe:2.3:o:mediatek:mt8163_firmware:-:*:*:*:*:android:*:*
8	Dropbox 98.2.2 for Android	android	cpe:2.3:a:dropbox:dropbox:98.2.2:*:*:*:*:android:*:*
9	HP S1000-E VPN Firewall Appliance JD272A	networking_communications	cpe:2.3:h:hp:s1000-e_vpn_firewall_appliance:jd272a:*:*:*:*:*:*:*
10	Huawei Access Router V200R002C01SPC200	networking_communications	cpe:2.3:h:huawei:access_router:v200r002c01spc200:*:*:*:*:*:*:*
11	Acexy Wireless-N WiFi Repeater 1.0	networking_communications	cpe:2.3:h:acexy:wireless-n_wifi_repeater:1.0:*:*:*:*:*:*:*
12	Microsoft Windows 10 1803 on x64	kernel_distributions	cpe:2.3:o:microsoft:windows_10:1803:*:*:*:*:*:x64:*
13	Microsoft Windows Defender	support_utilities	cpe:2.3:a:microsoft:windows_defender:-:*:*:*:*:*:*:*
14	Microsoft Edge	web_browsers	cpe:2.3:a:microsoft:edge:-:*:*:*:*:*:*:*
15	Google Android 8.0	android	cpe:2.3:o:google:android:8.0:*:*:*:*:*:*:*
16	Samsung Members 3.9.10.11	android	cpe:2.3:a:samsung:members:3.9.10.11:*:*:*:*:*:*:*

Εικόνα 7.15.: Περιεχόμενο του αρχείου CPEs.csv



Εικόνα 7.16.: Τμήμα του περιεχομένου του αρχείου CAPECs.csv

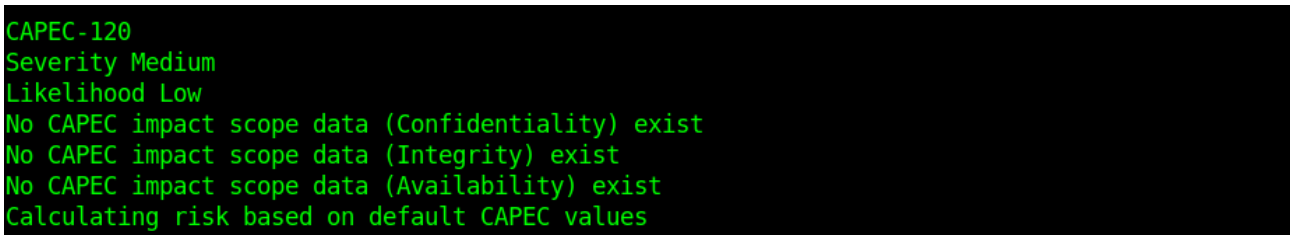
7.2.6. Υπολογισμός επιμέρους επιπέδου επικινδυνότητας για το κάθε CAPEC

Επόμενο βήμα είναι ο υπολογισμός του επιμέρους επιπέδου επικινδυνότητας για το κάθε CAPEC. Μέσω του λογισμικού ανακτώνται από την βάση δεδομένων του εγχειρήματος CAPEC δύο αρχεία (τύπου .xml και .csv) τα οποία και περιέχουν έναν κατάλογο όλων των CAPEC συμπεριλαμβανομένων των καίριων χαρακτηριστικών για την εκτίμηση του επιπέδου επικινδυνότητας, δηλαδή της τυπική πιθανότητα επιτυχούς επίθεσης, την τυπική σοβαρότητα των επιπτώσεων και τέλος πληροφορίες σχετικά με το εύρος των επιπτώσεων, πληροφορίες δηλαδή σχετικά με τις πτυχές ασφάλειας στις οποίες αφορούν οι επιπτώσεις επιτυχούς επίθεσης.

Για το κάθε CAPEC, προβάλλεται η τιμή πιθανότητας επιτυχούς επίθεσης, η τυπική σοβαρότητα των επιπτώσεων και το αν οι επιπτώσεις αφορούν στην εκάστοτε πτυχή ασφάλειας όπως φαίνεται στην εικόνα 7.17., για ένα CAPEC του τρίτου CPE:

Εικόνα 7.17.: Παράγοντες υπολογισμού επικινδυνότητας βάσει του CAPEC – 85 (CPE 3)

Σε αυτό το σημείο το λογισμικό εξετάζει τα δεδομένα που εισήγαγε ο χρήστης σχετικά με τον βαθμό εξάρτησης της κάθε πτυχής ασφάλειας με το συγκεκριμένο CPE. Καθώς η τιμή σοβαρότητας των επιπτώσεων στο πλαίσιο του εκάστοτε CAPEC είναι μια και δεν χωρίζεται σε ξεχωριστό ορισμό της σοβαρότητας των επιπτώσεων για την κάθε πτυχή ασφάλειας, το λογισμικό αρχικά απορρίπτει τους συντελεστές εξάρτησης για τις πτυχές ασφάλειας που δεν απαντώνται στο πλαίσιο του εύρους των επιπτώσεων του εξεταζόμενου CAPEC και έπειτα επιλέγει τον υψηλότερο εναπομείναντα συντελεστή, τον οποίον και χρησιμοποιεί για τον υπολογισμό του επιπέδου επικινδυνότητας του εξεταζόμενου CAPEC. Σε περίπτωση που η καταχώρηση του CAPEC στο πλαίσιο του εύρους των επιπτώσεων απουσιάζει (μιας και οι πληροφορίες του εκάστοτε CAPEC διαρκώς εξελίσσονται/συμπληρώνονται από τον οργανισμό MITRE), το λογισμικό δεν χρησιμοποιεί κάποιον συντελεστή εξάρτησης, βασίζει τον υπολογισμό της τιμής κινδύνου του CAPEC στο γινόμενο πιθανότητας επιτυχούς επίθεσης*σοβαρότητα επιπτώσεων και ενημερώνει τον χρήστη, όπως φαίνεται στην εικόνα 7.18.:



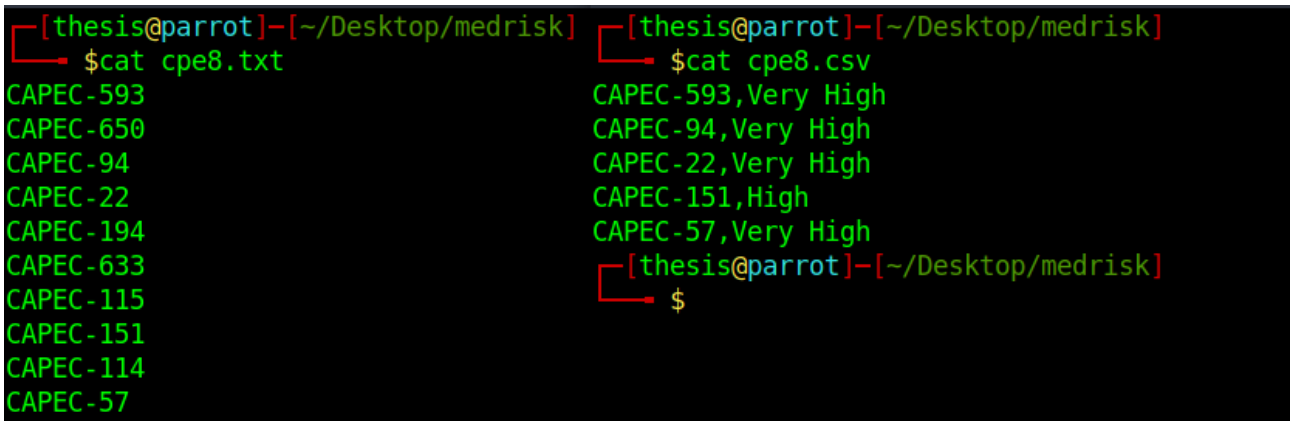
Εικόνα 7.18.: Παράδειγμα απουσίας στοιχείων σχετικών με το εύρος επιπτώσεων στην περίπτωση του CAPEC – 120 (CPE 5)

Για τον υπολογισμό της κάθε τιμής κινδύνου το λογισμικό υιοθετεί την προσέγγιση του ARES για τον υπολογισμό του επιπέδου επικινδυνότητας του εκάστοτε CAPEC, η οποία και συμπληρώνεται με ένα περαιτέρω βήμα συνυπολογισμού του συντελεστή εξάρτησης όπως παρουσιάστηκε στον πίνακα 6.3.. Ο υπολογισμός του επιμέρους επιπέδου επικινδυνότητας για το κάθε CAPEC προβάλλεται στον χρήστη, όπως φαίνεται στην εικόνα 7.19. στην περίπτωση του CAPEC – 85 (CPE 4):

Εικόνα 7.19: Παράδειγμα υπολογισμού επιμέρους επιπέδου επικινδυνότητας του CAPEC – 85 (CPE 4)

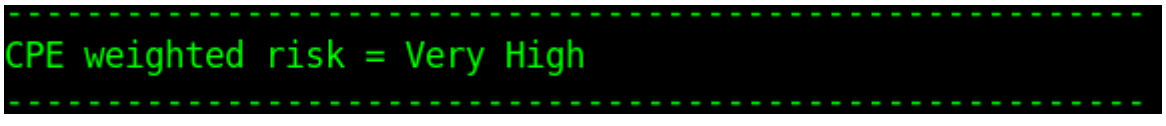
7.2.7. Υπολογισμός του συνολικού επιπέδου επικινδυνότητας για την ασφάλεια (σιγουριά) των ασθενών

Αφού οι υπολογισμοί ολοκληρωθούν, συμπληρώνονται τα αρχεία που δημιουργήθηκαν στο πλαίσιο της διαδικασίας biclustering και ταξινόμησης με το αποτέλεσμα κάθε CAPEC που εν τέλει διατηρήθηκε, όπως φαίνεται στην εικόνα 7.20. για το CPE 8: τα 10 αρχικά CAPEC που εντοπίστηκαν (αριστερά) περιορίστηκαν κατόπιν της διαδικασίας biclustering και ταξινόμησης σε 5 (δεξιά), πριν υπολογιστεί και προστεθεί το ζυγισμένο επίπεδο επικινδυνότητας για το κάθε ένα.



Εικόνα 7.20.: Αποτέλεσμα διαδικασίας biclustering και ταξινόμησης στην περίπτωση του CPE 8

Το συνολικό επίπεδο επικινδυνότητας για το εκάστοτε CPE είναι η υψηλότερη επιμέρους τιμή επικινδυνότητας των CAPEC που σχετίζονται με αυτό όπως φαίνεται παραδειγματικά για το CPE 8 στην εικόνα 7.21., ενώ το συνολικό επίπεδο επικινδυνότητας του συστήματος για την ασφάλεια των ασθενών είναι η υψηλότερη επιμέρους τιμή κινδύνου των CPEs που περιλαμβάνει.



Εικόνα 7.21.: Συνολικό επίπεδο επικινδυνότητας του CPE 8

Στο παράδειγμά μας, βάσει των CPEs που εξετάστηκαν και των επιλογών του χρήστη ως προς τον βαθμό εξάρτησης της (εδώ πλασματικής) διεργασίας υγείας από την κάθε πτυχή ασφάλειας των εμπλεκόμενων CPEs, το συνολικό επίπεδο επικινδυνότητας του πρότυπου συστήματος υπολογίζεται ως πολύ υψηλό (εικόνα 7.22.) για την σιγουριά των ασθενών.

Εικόνα 7.22.: Συνολικό επίπεδο επικινδυνότητας του πρότυπου συστήματος για την σιγουριά των ασθενών

7.3. Σχολιασμός της υλοποίησης

Το προτεινόμενο λογισμικό συστήνει επιτυχώς τον συντελεστή εξάρτησης της κάθε πτυχής ασφάλειας στον υπολογισμό του επιμέρους κινδύνου του κάθε CAPEC και κατά συνέπεια του τελικού επιπέδου επικινδυνότητας.

7.3.1. Αδυναμία λόγω εισροής υποκειμενικών παραγόντων στο αποτέλεσμα

Σε αυτό το σημείο έγκειται όμως και η πρώτη αδυναμία της υλοποίησης, καθώς δεδομένου του βάρους της επιλογής του χρήστη σχετικά με τους τρεις συντελεστές επηρεάζεται σε πολύ μεγάλο βαθμό το αποτέλεσμα, το οποίο φέρει πλέον υποκειμενική χροιά.

7.3.2. Αδυναμία σχετική με το πεδίο επιπτώσεων του εκάστοτε CAPEC

Η δεύτερη αδυναμία έγκειται σε έναν περιορισμό ο οποίος σχετίζεται με την ακρίβεια του πεδίου των επιπτώσεων του εκάστοτε CAPEC. Το εγχείρημα CAPEC, στην παρούσα υλοποίηση, δεν φέρει ξεχωριστές τιμές για την κάθε πτυχή ασφάλειας αλλά μια γενική τιμή. Παρά το γεγονός πως επιμέρους τιμές, πιθανώς βασιζόμενες στο εύρος των επιπτώσεων των σχετικών αδυναμιών, προτείνονται από τον οργανισμό MITRE [81], η πρόταση αυτή δεν έχει υλοποιηθεί, κάτι που οδηγεί σε γενικευμένα αποτελέσματα, μιας και δεν είναι σαφές αν το ανώτατο όριο κινδύνου που αντικατοπτρίζεται από την σχετική τιμή που φέρει το κάθε CAPEC αφορά στις πτυχές που ενδιαφέρουν τον εκάστοτε χρήστη.

Σημαντικό εδώ είναι επίσης πως καθώς ο εκάστοτε βαθμός βαρύτητας CVSS ο οποίος και αναγκαστικά συνυπολογίζεται στον υπολογισμό του επιμέρους (CPE) ή τελικού αποτελέσματος σε περίπτωση που δεν απαντηθεί κάποια CWE για την εκάστοτε ευπάθεια που φέρει το εξεταζόμενο CPE, διαθέτει, σε αντίθεση με το εκάστοτε CAPEC, στο πλαίσιο του σχετικού διανύσματος, τιμές επίπτωσης για την *κάθε* πτυχή ασφάλειας. Για λόγους συνέπειας της προσέγγισής μας οι επιμέρους αυτές τιμές δεν συνυπολογίζονται βάσει του συντελεστή εξάρτησης.

7.3.3. Αδυναμία αντιστοίχισης συγκεκριμένων οικογενειών CAPEC με CWEs

Ο τρίτος περιορισμός έγκειται στην αδυναμία αντιστοίχισης συγκεκριμένων οικογενειών CAPEC με σχετικές CWEs. Ο περιορισμός αυτός αφορά στις εξής περιπτώσεις:

1. Η αλυσίδα εφοδιασμού (supply chain), οι επικοινωνίες (communications) και οι επιθέσεις κοινωνικής μηχανικής (social engineering) δεν καλύπτονται από το εγχείρημα CWE με τον τρόπο που παρουσιάζονται από το εγχείρημα CAPEC. Ως εκ τούτου, δεν μπορεί να γίνει αντιστοίχιση μεταξύ των δύο σωμάτων. Αποτέλεσμα του περιορισμού αυτού είναι πως τα CAPEC – 440, 511, 516, 517 – 521, 530 – 532, 534, 535, 537, 670 – 674, 677 και 678 (σχετικά με την αλυσίδα εφοδιασμού), τα CAPEC- 559, 582 - 585, 601 και 603 – 605 (σχετικά με τις επικοινωνίες) και τα CAPEC - 407, 410, 412 - 418, 420 - 429 και 433 – 435 (σχετικά με επιθέσεις κοινωνικής μηχανικής) δεν συμπεριλαμβάνονται στην διαδικασία υπολογισμού της επικινδυνότητας.

2. Ο όρος “φυσική ασφάλεια” (physical security) χρησιμοποιείται τόσο στο πλαίσιο των CAPEC όσο και σε αυτό των CWE, με διαφορετικό όμως ορισμό σε κάθε σώμα. Στο πλαίσιο των CAPEC χρησιμοποιείται για να περιγράψει τη φυσική πρόσβαση σε κτίρια ή/και σε συγκεκριμένους χώρους. Αντίθετα, στο πλαίσιο των CWE χρησιμοποιείται τυπικά για να περιγράψει τη φυσική πρόσβαση σε στοιχεία υλικού. Αποτέλεσμα του περιορισμού αυτού είναι πως τα CAPEC – 390 - 395, 397 - 400, 507, 547 και 626 δεν συμπεριλαμβάνονται στην διαδικασία υπολογισμού της επικινδυνότητας.

3. Τέλος απαντάται η ιδιάζουσα περίπτωση όπου κάποιο *CAPEC δημιουργεί CWE* και όχι το τυπικά αντίστροφο, στις περιπτώσεις επίθεσης τροποποίησης κατά την κατασκευή ή/και την διανομή, οι οποίες και ανήκουν στην ευρύτερη οικογένεια CAPEC σχετικών με την αλυσίδα εφοδιασμού. Η σπάνια αυτή περίπτωση αφορά στα CAPEC - 438, 443 -

447, 539, 677 και 678, τα οποία επίσης δεν συμπεριλαμβάνονται στην διαδικασία υπολογισμού της επικινδυνότητας.

Κεφάλαιο 8
Επίλογος

Στόχος της παρούσας μεταπτυχιακής διατριβής ήταν ο εντοπισμός των επικινδυνοτήτων κυβερνοασφάλειας που χαρακτηρίζουν τα συστήματα ψηφιακής υγείας, η συσχέτισή τους με ζητήματα προστασίας της υγείας και της ζωής των ασθενών που θα μπορούσαν να προκληθούν από αυτές και τέλος η προτεραιοποίηση τους ως προς τις επιπτώσεις τους στην σιγουριά των ασθενών.

Αφού καθορίστηκε το πλαίσιο στο οποίο κινούμαστε παρουσιάστηκαν οι απειλές που το χαρακτηρίζουν. Βάσει αυτής της κωδικοποίησης συμπεράναμε πως η θεώρηση μας κατά την προσέγγιση των επιπτώσεων των επικινδυνοτήτων στην ασφάλεια των ασθενών και κατ' επέκταση κατά την ανάπτυξη μιας μεθόδου προτεραιοποίησης τους θα πρέπει να επεκταθεί στο σύνολο των απειλών και επιθέσεων που αντικειμενικά θα μπορούσαν να την διακινδυνεύσουν.

Για να αναπτυχθεί μια τέτοιου είδους αντιστοίχιση, διερευνήσαμε τον συνδετικό κρίκο ανάμεσα στις επικινδυνότητες και το εκάστοτε αντίξοο αποτέλεσμα, καταλήγοντας στο συμπέρασμα πως μια επιτυχής επίθεση κυβερνοασφάλειας μπορεί να οδηγήσει σε βλάβη της υγείας ή της ζωής του ασθενή όταν επενεργεί στα ψηφιακά συστήματα από τα οποία εξαρτάται η σχετική διεργασία υγείας την οποία υποστηρίζουν.

Οπλισμένοι με αυτήν την διαπίστωση, τροποποιήσαμε την προσέγγιση αυτοματοποιημένου υπολογισμού επικινδυνότητας ARES, αξιοποιώντας την δυνατότητα που προσφέρει ως προς την δημιουργία μιας αλυσίδας ιχνηλάτησης των ευπαθειών του εκάστοτε υπολογιστικού συστήματος η μέρος αυτού, των ασθενειών που σχετίζονται με τις ευπάθειες αυτές και τέλος τους τύπους επιθέσεων που εκμεταλλεύονται τις ασθένειες που εντοπίστηκαν. Προχωρήσαμε στην πρόταση σύστασης ενός συντελεστή εξάρτησης της εκάστοτε διεργασίας υγείας από την κάθε πτυχή ασφάλειας των ψηφιακών υποδομών που την υποστηρίζουν.

Τέλος, υλοποιήθηκε η προσέγγιση μας ως εφαρμογή, η οποία και παρουσιάστηκε στο πλαίσιο ενός πρότυπου συστήματος, αναδεικνύοντας την λειτουργία του προτεινόμενου συντελεστή εξάρτησης.

Βιβλιογραφία

[1] Razaque, A., Amsaad, F., Khan, M.J., Hariri, S., Chen, S., Siting, C. and Ji, X., 2019. Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access*, 7, pp.168774-168797.

[2] Newaz, A.I., Sikder, A.K., Rahman, M.A. and Uluagac, A.S., 2021. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, 2(3), pp.1-44.

[3] Rushanan, M., Rubin, A.D., Kune, D.F. and Swanson, C.M., 2014, May. Sok: Security and privacy in implantable medical devices and body area networks. In 2014 *IEEE symposium on security and privacy* (pp. 524-539). IEEE.

[4] Yaqoob, T., Abbas, H. and Atiquzzaman, M., 2019. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Communications Surveys & Tutorials*, 21(4), pp.3723-3768.

[5] Almohri, H., Cheng, L., Yao, D. and Alemzadeh, H., 2017, July. On threat modeling and mitigation of medical cyber-physical systems. In *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)* (pp. 114-119). IEEE.

[6] Algarni, A., 2019. A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access*, 7, pp.101879-101894.

[7] Djenna, A. and Saïdouni, D.E., 2018, October. Cyber attacks classification in IoT-based-healthcare infrastructure. In *2018 2nd Cyber Security in Networking Conference (CSNet)* (pp. 1-4). IEEE.

[8] Oh, S.R., Seo, Y.D., Lee, E. and Kim, Y.G., 2021. A comprehensive survey on security and privacy for electronic health data. *International Journal of Environmental Research and Public Health, 18*(18), p.9668.

[9] Batista, E., Moncusi, M.A., López-Aguilar, P., Martínez-Ballesté, A. and Solanas, A., 2021. Sensors for context-aware smart healthcare: a security perspective. *Sensors, 21*(20), p.6886.

[10] AlTawy, R. and Youssef, A.M., 2016. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *Ieee Access, 4*, pp.959-979.

[11] Gloukhovtsev, M., 2018. IoT security: challenges, solutions & future prospects. *Proceedings of the Proven Professional Knowledge Sharing Article*, pp.1-44.

[12] ENISA, Cyber Security and Resilience for Smart Hospitals—ENISA. European Union Agency For Network And Information Security.

[13] Hajar, M.S., Al-Kadri, M.O. and Kalutarage, H.K., 2021. A survey on wireless body area networks: Architecture, security challenges and research opportunities. *Computers & Security, 104*, p.102211.

[14] Ambrose, J.A., Ragel, R.G., Jayasinghe, D., Li, T. and Parameswaran, S., 2015, March. Side channel attacks in embedded systems: A tale of hostilities and deterrence. In *Sixteenth International Symposium on Quality Electronic Design* (pp. 452-459). IEEE.

[15] Aloseel, A., He, H., Shaw, C. and Khan, M.A., 2020. Analytical review of cybersecurity for embedded systems. *IEEE Access*, 9, pp.961-982.

[16] Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D. and Douligeris, C., 2020. Security in IoMT communications: A survey. *Sensors, 20*(17), p.4828.

[17] Ponemon Institute, Cyber Insecurity in Healthcare: Cost & Impact on Patient Care, προσβάσιμο μέσω του συνδέσμου: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[18] "4 emerging threats to healthcare providers", προσβάσιμο μέσω του συνδέσμου: https://www.symantec.com/blogs/expert-perspectives/4-emerging-threats-healthcareproviders/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[19] “Orangeworm cyberattack group puts healthcare industry in the crosshairs”, προσβάσιμο μέσω του συνδέσμου: http://www.aami.org/newsviews/newsdetail.aspx?ItemNumber=6205/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[20] O'Kane, P., Sezer, S. and Carlin, D., 2018. Evolution of ransomware. *Iet Networks, 7*(5), pp.321-327.

[21] Bhunia, S., Majerus, S. and Sawan, M. eds., 2015. *Implantable biomedical microsystems: design principles and applications.* Elsevier.

[22] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J. and Lymberopoulos, D., 2022. A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies, 33*(6), p.e4049.

[23] Rathore, H., Mohamed, A., Al-Ali, A., Du, X. and Guizani, M., 2017, June. A review of security challenges, attacks and resolutions for wireless medical devices. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1495-1501). IEEE.

[24] Casey, W., Kellner, A., Memarmoshrefi, P., Morales, J.A. and Mishra, B., 2018. Deception, identity, and security: the game theory of sybil attacks. *Communications of the ACM, 62*(1), pp.85-93.

[25] Dang, L.M., Piran, M.J., Han, D., Min, K. and Moon, H., 2019. A survey on internet of things and cloud computing for healthcare. *Electronics, 8*(7), p.768.

[26] Partala, J., Keräneny, N., Särestöniemi, M., Hämäläinen, M., Iinatti, J., Jämsä, T., Reponen, J. and Seppänen, T., 2013, October. Security threats against the transmission chain of a medical health monitoring system. In *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)* (pp. 243-248). IEEE.

[27] Hlavacek, D. and Chang, J.M., 2014. A layered approach to cognitive radio network security: A survey. *Computer Networks, 75*, pp.414-436.

[28] Tripathi, M., Gaur, M.S. and Laxmi, V., 2013. Comparing the impact of black hole and gray hole attack on LEACH in WSN. *Procedia computer science, 19*, pp.1101-1107.

[29] Baronti, P., Pillai, P., Chook, V.W., Chessa, S., Gotta, A. and Hu, Y.F., 2007. Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. *Computer communications, 30*(7), pp.1655-1695.

[30] McCarty, B., 2021. *Cyberjutsu: cybersecurity for the modern ninja.* No Starch Press.

[31] Hickey, M. and Arcuri, J., 2020. *Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming.* John Wiley & Sons.

[32] Graham, D. G., 2021. *Ethical Hacking: A Hands-on Introduction to Breaking In.* NoStartch Press.

[33] Kanta, A., 2023. *Context-Based Password Cracking for Digital Investigation* (Doctoral dissertation, University College Dublin).

[34] Teng, J., Gu, W. and Xuan, D., 2012. Defending against physical attacks in wireless sensor networks. *Handbook on Securing Cyber-physical Critical Infrastructure*, pp.251-279.

[35] Hei, X., Du, X., Lin, S., Lee, I. and Sokolsky, O., 2014. Patient infusion pattern based access control schemes for wireless insulin pump system. *IEEE Transactions on Parallel and Distributed Systems, 26*(11), pp.3108-3121.

[36] Paoletti, N., Jiang, Z., Islam, M.A., Abbas, H., Mangharam, R., Lin, S., Gruber, Z. and Smolka, S.A., 2019, April. Synthesizing stealthy reprogramming attacks on cardiac devices. In *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems* (pp. 13-22).

[37] "Medical devices at risk of dos attacks - 5 insights", προσβάσιμο μέσω του συνδέσμου: https://www.beckersasc.com/asc-quality-infection-control/medical-devices-atrisk-of-denial-of-service-attacks-5-insights.html/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[38] Ransford, B., Kramer, D.B., Foo Kune, D., Auto de Medeiros, J., Yan, C., Xu, W., Crawford, T. and Fu, K., 2017. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. *Pacing and Clinical Electrophysiology, 40*(8), pp.913-917.

[39] Raymond, D.R., Marchany, R.C., Brownfield, M.I. and Midkiff, S.F., 2008. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE transactions on vehicular technology, 58*(1), pp.367-380.

[40] Hei, X. and Du, X., 2013. *Security for wireless implantable medical devices* (pp. 19-35). New York, NY, USA, Springer.

[41] Spreitzer, R., Moonsamy, V., Korak, T. and Mangard, S., 2017. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Communications Surveys & Tutorials, 20*(1), pp.465-488.

[42] Zhang, M., Raghunathan, A. and Jha, N.K., 2013, May. Towards trustworthy medical devices and body area networks. In *Proceedings of the 50th Annual Design Automation Conference* (pp. 1-6).

[43] Park, Y., Son, Y., Shin, H., Kim, D. and Kim, Y., 2016, August. This ain't your dose: Sensor spoofing attack on medical infusion pump. In 10th *USENIX Workshop on Offensive Technologies.* USENIX.

[44] Hanna, S., Rolles, R., Molina-Markham, A., Poosankam, P., Blocki, J., Fu, K. and Song, D., 2011, August. Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices. In *HealthSec.*

[45] Rios, B. and Butts, J., 2017. Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies. *WhiteScope, sl.*

[46] Zubair, M., Unal, D., Al-Ali, A. and Shikfa, A., 2019, July. Exploiting bluetooth vulnerabilities in e-health IoT devices. In *Proceedings of the 3rd international conference on future networks and distributed systems* (pp. 1-7).

[47] Mitnick, K.D. and Simon, W.L., 2003. *The art of deception: Controlling the human element of security.* John Wiley & Sons.

[48] "Social Engineering – or: How we get tricked", προσβάσιμο μέσω του συνδέσμου: https://blog.rwth-aachen.de/itc/en/2020/11/06/social-engineering/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[49] "Social Engineering - From the Trojan Horse to Firewalls", προσβάσιμο μέσω του συνδέσμου: https://www.mitnicksecurity.com/in-the-news/social-engineering-from-the-trojan-horse-to-firewalls (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[50] "Rare BadUSB attack detected in the wild against US hospitality provider", προσβάσιμο μέσω του συνδέσμου: https://www.zdnet.com/article/rare-badusb-attack-detected-in-the-wild-against-us-hospitality-provider/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[51] Hadnagy, C., 2010. *Social engineering: The art of human hacking.* John Wiley & Sons.

[52] Chiew, K.L., Yong, K.S.C. and Tan, C.L., 2018. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications, 106*, pp.1-20.

[53] "Voice fraud scams company out of $243,000", προσβάσιμο μέσω του συνδέσμου: https://blog.avast.com/deepfake-voice-fraud-causes-243k-scam (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[54] Anti-Phishing Working Group. Phishing Activity Trends Report—3rd Quarter 2020; Technical Report; Anti-Phishing Working Group: Washington, DC, USA, 2020. Προσβάσιμο μέσω του συνδέσμου: https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[55] The US Department of Justice. "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams—Hundreds of Domains Disrupted Through Public and Private Sector Cooperative Efforts.", Προσβάσιμο μέσω του συνδέσμου: https: //www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-COVID-19-related-scams (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[56] Symanovich, S. Coronavirus Phishing Emails: How to Protect against COVID-19 Scams. Προσβάσιμο μέσω του συνδέσμου:Προσβάσιμο μέσω του συνδέσμου: https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[57] Priestman, W., Anstis, T., Sebire, I.G., Sridharan, S. and Sebire, N.J., 2019. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics, 26*(1).

[58] Wright, A., Aaron, S. and Bates, D.W., 2016. The big phish: cyberattacks against US healthcare systems. *Journal of General Internal Medicine, 31*, pp.1115-1118.

[59] Jalali, M.S., Bruckes, M., Westmattelmann, D. and Schewe, G., 2020. Why employees (still) click on phishing links: investigation in hospitals. *Journal of medical Internet research, 22*(1), p.e16775.

[60] U.S. Food and Drug Administration, "Postmarket Management of Cybersecurity in Medical Devices (2016)", προσβάσιμο μέσω του συνδέσμου: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[61] Battles, J.B. and Lilford, R.J., 2003. Organizing patient safety research to identify risks and hazards. *BMJ Quality & Safety, 12*(suppl 2), pp.ii2-ii7.

[62] Piggin, R., 2017. Cybersecurity of medical devices-addressing patient safety and the security of patient health information. *London: BSI*, pp.3-22.

[63] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Advanced Persistent Threat", προσβάσιμο μέσω του συνδέσμου: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[64] Cybersecurity and Infrastructure Security Agency (CISA), “APT Groups Target Healthcare and Essential Services”, προσβάσιμο μέσω του συνδέσμου: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-126a (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[65] Piggin, R.S.H. and Boyes, H.A., 2015. Safety and security-a story of interdependence.

[66] Lisova, E., Šljivo, I. and Čaušević, A., 2018. Safety and security co-analyses: A systematic literature review. *IEEE Systems Journal, 13*(3), pp.2189-2200.

[67] Skierka, I.M., 2018, March. The governance of safety and security risks in connected healthcare. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1-12). IET.

[68] Johnson, P., Gorton, D., Lagerström, R. and Ekstedt, M., 2016. Time between vulnerability disclosures: A measure of software product vulnerability. *Computers & Security, 62*, pp.278-295.

[69] Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T. and Chizeck, H.J., 2015. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv preprint arXiv:1504.04339*.

[70] Das, S., Siroky, G.P., Lee, S., Mehta, D. and Suri, R., 2021. Cybersecurity: the need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm, 18*(3), pp.473-481.

[71] Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T. and Maisel, W.H., 2008, May. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)* (pp. 129-142). IEEE.

[72] U.S. Food and Drug Administration, “MAUDE Adverse Event Report: MERGE HEALTHCARE MERGE HEMO PROGRAMMABLE DIAGNOSTIC COMPUTER”, προσβάσιμο μέσω του συνδέσμου: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi__id=5487204 (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[73] Coyle, Y.M. and Battles, J.M., 1999. Using antecedents of medical care to develop valid quality of care measures. *International Journal for Quality in Health Care, 11*(1), pp.5-12.

[74] Donabedian, A., 1980. Explorations in quality assessment and monitoring: the definition of quality and approaches to its assessment.

[75] Reason, J., 1990. *Human error.* Cambridge university press.

[76] Reason J. *The organizational accident.* New York: Ashgate, 1997.

[77] Rasmussen, J., 1976. Outlines of a hybrid model of the process plant operator. *Monitoring behavior and supervisory control*, pp.371-383.

[78] Van der Schaaf TW. *Near miss reporting in the chemical process industry*, PhD Thesis. Eindhoven, NL: Eindhoven University of Technology, 1992.

[79] Dimitriadis, A., Flores, J.L., Kulvatunyou, B., Ivezic, N. and Mavridis, I., 2020. Ares: Automated risk estimation in smart sensor environments. *Sensors, 20*(16), p.4617.

[80] Fenrich, K., 2008. Securing your control system: the" CIA triad" is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering, 112*(2), 44-49.

[81] MITRE Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description, 15 January 2008. Προσβάσιμο μέσω του συνδέσμου: https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1. 3.pdf (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[82] Nipuni Nanayakkara, Malka Halgamuge, and Ali Syed. 2019. Security and privacy of internet of medical things (IoMT) based healthcare applications: A review. In *Proc. 262nd IIER Int. Conf. Institute for Technology and Research*, 1–18.

[83] Younghyun Kim et al. 2015. Implantable Biomedical Microsystems: Design Principles and Applications. William Andrew Publishing, Oxford, Κεφάλαιο: *Reliability and security of implantable and wearable medical devices*, 167–199.

[84] World Health Organization – Constitution. Προσβάσιμο μέσω του συνδέσμου: https://www.who.int/about/governance/constitution (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[85] International Organization for Standardization [ISO], 2019. ISO 14971: Medical devices — Application of risk management to medical devices.

[86] International Organization for Standardization [ISO], 2012. IEC/TR 80001-2-2:2012: Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the communication of medical device security needs, risks and controls.

[87] International Electrotechnical Commission [IEC], 2019. IEC TS 63069: Industrial-process measurement, control and automation - Framework for functional safety and security.

[88] Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. NIST SP 800-30r1.

[89] National Institute of Standards and Technology – COMPUTER SECURITY RESOURCE CENTER: Glossary. Προσβάσιμο μέσω του συνδέσμου: https://csrc.nist.gov/glossary (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[90] FIRST Common Vulnerability Scoring System Version 3.1, Forum of Incident Response and Security Teams. Προσβάσιμο μέσω του συνδέσμου: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[91] MITRE CPE—Common Platform Enumeration. Προσβάσιμο μέσω του συνδέσμου: https://cpe.mitre.org/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[92] MITRE CAPEC—Common Attack Pattern Enumeration and Classification (CAPEC). Προσβάσιμο μέσω του συνδέσμου: https://capec.mitre.org/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[93] MITRE CWE—Common Weakness Enumeration. Προσβάσιμο μέσω του συνδέσμου: https://cwe.mitre.org/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[94] MITRE CVE List (Home). Προσβάσιμο μέσω του συνδέσμου: https://cve.mitre.org/cve/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[95] MITRE ATT&CK (Home). Προσβάσιμο μέσω του συνδέσμου: https://attack.mitre.org/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[96] Κανονισμός (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, 2017: 2017/745, Προσβάσιμο μέσω του συνδέσμου: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32017R0745&from=HU (Τελευταία ανάκτηση: 8 Μαΐου 2023).

[97] National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021. SP 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171.

[98] Ινστιτούτο Νεοελληνικών Σπουδών (Ίδρυμα Μανόλη Τριανταφυλλίδη), Θεσσαλονίκη, 1998. Λεξικό της κοινής νεοελληνικής (διαδικτυακή έκδοση). Προσβάσιμο μέσω του συνδέσμου: https://www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/ (Τελευταία ανάκτηση: 8 Μαΐου 2023).