Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ - ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.


ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

# ΑΝΑΛΥΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΠΕΙΛΩΝ ΣΤΑ ΔΙΚΤΥΑ AD-HOC ΚΑΙ ΑΙΣΘΗΤΗΡΩΝ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΕΣ M2M ΚΑΙ ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ

*Επιβλέπων Καθηγητής*: Πικραμμένος Ιωάννης

*Φοιτητής.:*

ΓΙΟΥΡΓΚΕΝ ΤΣΑΟΥΣΙ ΑΜ: 2011107

Σπάρτη, Μάιος 2018

## Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

**ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ** **ΥΠΟΓΡΑΦΕΣ**

**1.**

**2.**

**3.**

## Υπεύθυνη Δήλωση

*Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής ΤΕ του Τ.Ε.Ι. Πελοποννήσου.*

Ο συγγραφέας,

ΓΙΟΥΡΓΚΕΝ ΤΣΑΟΥΣΙ

# *Ευχαριστίες*

Έχοντας φτάσει στο τέλος της πτυχιακής μου εργασίας, αισθάνομαι υποχρεωμένος να μιλήσω για κάποιους ανθρώπους, που ο καθένας με τον δικό του τρόπο σηματοδότησε την πορεία των χρόνων μου στις προπτυχιακές σπουδές μου και να τους ευχαριστήσω.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα μου, κύριο Πικραμμένο Ιωάννη, Επιστημονικό Συνεργάτη του Τμήματος Μηχανικών Πληροφορικής ΤΕ του Τ.Ε.Ι. Πελοποννήσου, διότι η συνεργασία μαζί του ήταν ένας καταλύτης για την ολοκλήρωση των προπτυχιακών σπουδών μου. Τα αποτελέσματα της εργασίας αυτής είναι από τη συνεργασία με τον κ. Πικραμμένο. Η συνεργασία μας ξεκίνησε όταν ήμουν προπτυχιακός φοιτητής στο χειμερινό εξάμηνο του 2013 – 2014, στο μάθημα «Σχεδίαση Μελέτη και Υλοποίηση Δικτύων». Από τη συνεργασία αυτή, είχα την πρώτη εμπειρία στις επικοινωνίες. Η πλήρη ηθική στήριξή του και η εμπιστοσύνη του στο πρόσωπό μου, με όπλισαν με κουράγιο, δύναμη και μου έδωσε το θάρρος να αναλάβω την προσπάθεια της συγκεκριμένης εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω τη μητέρα μου Σεμίχα για την αμέριστη υποστήριξή τους όλα αυτά τα χρόνια, των προπτυχιακών σπουδών μου. Αφιερώνω αυτή την εργασία στη μητέρα μου, ως ελάχιστη ευγνωμοσύνη για την κατανόηση και την υπομονή της όλα αυτά τα χρόνια.

*Τσαούσι Γιούργκεν*

*Σπάρτη, Μάιος 2018*

# Περιεχόμενα

# Περίληψη

Ο όρος επικοινωνίας M2M (Machine to Machine) ευαισθητοποιεί οποιαδήποτε λύση ή τεχνολογία που διευκολύνει την ενσύρματη και ασύρματη επικοινωνία μεταξύ δικτυωμένων συσκευών για την ανταλλαγή πληροφοριών. Στα συστήματα παλαιού τύπου, οι ενσύρματες και ασύρματες επικοινωνίες μεταξύ μηχανών χρησιμοποιούν τεχνικές σηματοδότησης για την επικοινωνία μεταξύ πολλών προϊόντων και εφαρμογών όπως τηλεφωνία, τηλεμετρία, βιομηχανικό αυτοματισμό κλπ. Λόγω των πρόσφατων τεχνολογικών καινοτομιών, όχι μόνο οι συνδεδεμένες συσκευές υιοθετούν κινητικότητα λόγω της φύσης τους, αλλά γίνονται επίσης ανταγωνιστικοί όσον αφορά τον τρόπο εκμετάλλευσης των δυνατοτήτων του δικτύου.

Η ad-hoc δικτύωση είναι ένα συστατικό δομικό στοιχείο για τις επικοινωνίες M2M. Σήμερα έχουν ενταθεί οι ευφυείς μεταφορές, τα κυβερνο-φυσικά συστήματα (CPS) και οι τεχνολογίες "Smart <anything>" (π.χ. πόλεις, κτίρια, οχήματα, οικιακές συσκευές, τηλέφωνα) και προσελκύουν την προσοχή των ενθουσιώδων R&D. Η δικτύωση αισθητήρων έχει το μερίδιο του λέοντος μεταξύ σχεδόν όλων των παραπάνω αναδυόμενων τάσεων. Η δικτύωση αισθητήρων χρησιμοποιεί συσκευές που ανταλλάσσουν πληροφορίες με οποιοδήποτε μέσο επικοινωνίας. Σε αυτό το πλαίσιο, είναι σχεδόν μια "προϋπόθεση sine qua non" για τον ορισμό οποιασδήποτε υλοποίησης του M2M χωρίς να συμπεριλαμβάνονται συνδεδεμένοι αισθητήρες σε μια ad hoc προσέγγιση.

Από την άποψη της ασφάλειας, η αυξημένη επιφάνεια επιθέσεων σε δίκτυα ad-hoc και αισθητήρων έχει προωθήσει την ανάπτυξη τεχνολογίας για την πρόληψη συμβάντων επίθεσης και την αντιμετώπιση προβλημάτων συστήματος. Στο πλαίσιο αυτό, τα δίκτυα αποκτούν μεγαλύτερη σημασία σε υποδομές ζωτικής σημασίας (π.χ. βιομηχανικά συστήματα ελέγχου, ύδρευσης και ηλεκτροπαραγωγής, αμυντικές βάσεις) και σε ευαίσθητη εκμετάλλευση δεδομένων (π.χ. υγειονομική περίθαλψη, τραπεζικά συστήματα, κοινωνικά δίκτυα) για τα οποία είναι πιθανό τα ζητήματα απορρήτου και δεοντολογίας σηκώνομαι. Πρόσφατα περιστατικά απέδειξαν ότι οποιαδήποτε συνδεδεμένη συσκευή, όπως οι έξυπνες τηλεοράσεις και οι βιντεοκάμερες, μπορεί να διακυβευτεί για να προωθήσει την παράνομη κίνηση στο δίκτυο, αλλά μπορεί επίσης να θέσει σε κίνδυνο την ασφάλεια σε εθνικό και κυβερνητικό επίπεδο.

Όλα τα παραπάνω συμβάλλουν στην περιγραφή του αναδυόμενου κόσμου του Ίντερνετ των πραγμάτων (IoT), το οποίο μπορεί να αναγνωριστεί ως ο οδηγός για την εξέλιξη των επικοινωνιών M2M. Οι τεχνολογίες επικοινωνιών M2M διευκολύνουν τη μετάδοση δεδομένων και επιτρέπουν την οριζόντια επικοινωνία ενός δικτύου αισθητήρων πολλαπλών κόμβων. Από ποσοτική άποψη, οι συνδέσεις IoT αναμένεται να υπερβούν τα 27 δισεκατομμύρια μέχρι το 2025 σε σύγκριση με 6 δισεκατομμύρια το 2015. Όσον αφορά το μερίδιο αγοράς, η ευκαιρία για έσοδα ανέρχεται σε 6,8 δισεκατομμύρια ευρώ, ενώ το ποσό αυτό θα αυξηθεί σε 2,7 τρισεκατομμύρια ευρώ 2025. Από την άποψη της τεχνολογίας, το 71% όλων των συνδέσεων IoT φιλοξενείται χρησιμοποιώντας τεχνολογία μικρής εμβέλειας (π.χ. WiFi, Zigbee, NFC, Προγραμματιζόμενοι Λογικοί Ελεγκτές εντός PLC).

Η εργασία αυτή παρέχει μια βαθιά εικόνα της τρέχουσας κατάστασης ασφάλειας στην ad-hoc και τη δικτύωση αισθητήρων για τις επικοινωνίες M2M. Σκοπός της είναι να υποστηρίξει τους υπεύθυνους για τη λήψη αποφάσεων, να κατανοήσουν το τοπίο και να λάβουν τεκμηριωμένες αποφάσεις σχετικά με την ασφάλεια στον κυβερνοχώρο με την ενσωμάτωση ενοποιημένων πληροφοριών από την εξέλιξη του τοπίου της απειλής του ευρωπαϊκού δικτύου πληροφοριών και πληροφοριών (NIS).

Η τρέχουσα μελέτη αναλύει αρχικά τις απειλές για αναγνωρισμένα περιουσιακά στοιχεία της ονοματολογίας δικτύων ad hoc και αισθητήρων και επικεντρώνεται στα δίκτυα ασύρματων δικτύων (Mesh Networks - WMN), στα δίκτυα Mobile ad-hoc (MANET) και στα ασύρματα δίκτυα αισθητήρων (WSN). Στη συνέχεια, παρουσιάζουμε τον τρέχοντα τομέα των τριπλών στοιχείων ενεργητικού για τις επικοινωνίες M2M, όπως θεωρείται από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) σε δύο επιπλέον τομείς και κατηγοριοποιούμε τα αντίμετρα που είναι διαθέσιμα στο κοινό στη βιβλιογραφία. Τέλος, πραγματοποιούμε μια ανάλυση κενού που πραγματοποιεί μια σύγκριση μεταξύ των εντοπισμένων απειλών και των αντιμέτρων. Επιπλέον, συζητείται επίσης η έλλειψη των σημερινών αντιμέτρων και των διαφόρων πιεστικών αναγκών για την ανάπτυξη αντιμέτρων νέας γενιάς.

# 1. Εισαγωγή

Η τρέχουσα μελέτη αναλύει τις απειλές και το περιβάλλον απειλής για ad-hoc και δίκτυα αισθητήρων. Εκτελούμε μια ολοκληρωμένη συλλογή των αντίστοιχων απειλών αναλύοντας τις συλλεγμένες πληροφορίες και εκτελούμε τις αντίστοιχες αναλύσεις απειλών και αναφορές τοπίου στον τομέα εφαρμογής.

Τα ad-hoc και αισθητήρα δίκτυα για έξυπνη αντικείμενα που χρησιμοποιούνται για τη συλλογή κρίσιμη, ευαίσθητη, μαζική και άλλους τύπους δεδομένων σε διάφορα σημεία ενδιαφέροντος, όπως μετεωρολογικούς σταθμούς, χώρους υγειονομικής περίθαλψης, της αεροπορίας και τους τομείς του αυτοκινήτου, των αποσκευών και εντοπισμού περιουσιακών στοιχείων, σπίτι και τις εφαρμογές του κλάδου, την ανάλυση και τη διαχείριση της αλυσίδας παραγωγής και της εφοδιαστικής αλυσίδας. Στη συνέχεια, τα δεδομένα μπορούν να αναλυθούν για να προκαλέσουν διάφορες διορθωτικές / προληπτικές ενέργειες. να καταγράφει και να αναλύει τις βλάβες του συστήματος, να ξεκινά τις κατάλληλες διορθωτικές αλλαγές, να εφαρμόζει / να επαναφέρει τις αλλαγές διαμόρφωσης και να παρέχει την αναφορά δεδομένων ποιότητας και την ανάλυση στατιστικής διαδικασίας / ελέγχου. Σήμερα, οι έξυπνες μεταφορές, έξυπνες χρηματοδοτήσεις και δάνεια, έξυπνες επιχειρήσεις κοινής ωφέλειας, έξυπνη προμήθεια και την κατασκευή, έξυπνα περιβάλλοντα, έξυπνη ενέργεια, έξυπνο σπίτι, έξυπνο και υγείας περιλαμβάνει πολλές διασυνδεδεμένες συσκευές και στηρίζονται σε μεγάλο βαθμό σε ad-hoc και δίκτυα αισθητήρων (Σχήμα 1).


**Σχήμα 1**

Αυτά τα διαδεδομένα και πανταχού παρόντα δίκτυα διευκολύνουν την επεξεργασία και συλλογή δεδομένων που παράγονται από αισθητήρες και έξυπνες συσκευές. Προφανώς, οι λειτουργίες, η ευελιξία, η διαθεσιμότητα και η απόδοση αυτών των δικτύων είναι κρίσιμες και, συνεπώς, πρέπει να προστατεύσουμε την ασφαλή ανταλλαγή πληροφοριών και να διασφαλίσουμε την ιδιωτικότητα και την ακεραιότητα των δεδομένων. Εκτός αυτού, η μείωση της επιφάνειας επίθεσης είναι ένα από τα κυρίαρχα ζητήματα που ευδοκιμούν κατά τη λειτουργία των ad-hoc και των δικτύων αισθητήρων. Λόγω της αυξημένης επιφάνειας επιθέσεων σε ad-hoc και δίκτυα αισθητήρων, πρέπει να αποτρέψουμε τα περιστατικά ασφάλειας, να αντιμετωπίσουμε τις αποτυχίες του συστήματος και να μετριάσουμε τους σχετικούς κινδύνους. Ακόμα περισσότερο, η ανάγκη μείωσης της επιφάνειας επίθεσης αποκτά

μεγαλύτερη σημασία σε κρίσιμα περιβάλλοντα (π.χ. συστήματα βιομηχανικού ελέγχου) και όταν εμπλέκονται ευαίσθητα δεδομένα (π.χ. στην υγειονομική περίθαλψη, στα τραπεζικά συστήματα και στα κοινωνικά δίκτυα), ενδέχεται να προκύψουν σοβαρά ζητήματα απορρήτου και ηθικής (π.χ. ευαίσθητα ιατρικά αρχεία και δεδομένα ασθενών). Αναπόφευκτα, τα δίκτυα αυτά αποτελούν ισχυρό σημείο ενδιαφέροντος για πολλές ερευνητικές ομάδες σε όλο τον κόσμο.

## 1.1. Πλαίσιο πολιτικής

Στόχος της παρούσας μελέτης είναι να αναλύσει το περιβάλλον της εξελισσόμενης απειλής τόσο από την πλευρά των ενδιαφερομένων όσο και από την πλευρά των πολιτικών της ΕΕ, προσδιορίζοντας τις εξελισσόμενες απειλές, τους κινδύνους και τις προκλήσεις που σχετίζονται με δίκτυα ad-hoc και αισθητήρων με ειδική προσέγγιση στο αρχιτεκτονικό μοντέλο επικοινωνίας M2M.

Η παρούσα μελέτη προσδιορίζει τα περιουσιακά στοιχεία του δικτύου ad-hoc και του αισθητήρα και απεικονίζει τις απειλές δικτύωσης ad-hoc και αισθητήρων μέσω της αναθεώρησης των τρεχουσών εργασιακών και περιβαλλοντικών πρακτικών, της αξιολόγησης των ιδιωτικών και δημόσιων πρωτοβουλιών και της ανάλυσης των ερευνητικών πληροφοριών σε αυτόν τον τομέα. Η μελέτη παρέχει επίσης την ανάλυση απειλών, τους κινδύνους και τα τρωτά σημεία της Στρατηγικής για την Παγκόσμια Ασφάλεια της ΕΕ ώστε να είναι πιο αποτελεσματική στην αντιμετώπιση των σύγχρονων προκλήσεων της κινητικότητας, των επιθέσεων στον κυβερνοχώρο και της τρομοκρατίας, καθώς και στην αντιμετώπιση κρίσεων και συγκρούσεων.

## 1.2. Κοινό-στόχος

Μελετώντας τις δραστηριότητες και τα παραδοτέα που παρέχονται από τη μελέτη αυτή και από το τοπίο απειλής ENISA, οι ακόλουθες ομάδες στόχοι μπορούν να ταξινομηθούν:

- Η δημόσια κοινότητα να κατανοήσει καλύτερα την έκθεση και τους κινδύνους των περιουσιακών στοιχείων
- Η επιχειρηματική κοινότητα για την απλούστευση του περιεχομένου των πληροφοριών απειλών και τη βελτίωση της χάραξης πολιτικής
- Οι ενδιαφερόμενοι φορείς της βιομηχανίας να αναπτύξουν καλές πρακτικές εργασίας και να αποκαλύψουν τις αναδυόμενες απειλές
- Οι δημόσιοι και ιδιωτικοί οργανισμοί να προσαρμόζουν τους ελέγχους ασφαλείας που λειτουργούν άψογα ώστε να συμπεριλαμβάνονται στα σύνθετα σύγχρονα περιβάλλοντα
- Οι επαγγελματίες ασφαλείας να επεξεργάζονται μοντέλα απειλών και να βελτιώνουν συνεχώς τα εργαλεία προστασίας και ανίχνευσης
- Διαχειριστές κινδύνου σε οποιαδήποτε διαδικασία αξιολόγησης κινδύνου για τον εντοπισμό, την αξιολόγηση και την ιεράρχηση των κινδύνων

Όλοι οι τύποι των παρεχόμενων πληροφοριών στοχεύουν στη στήριξη των υπευθύνων λήψης αποφάσεων σε όλες τις οργανώσεις να κατανοήσουν το τοπίο απειλής και να λάβουν τεκμηριωμένες αποφάσεις σχετικά με την

ασφάλεια στον κυβερνοχώρο, λαμβάνοντας ολοκληρωμένες και ενοποιημένες πληροφορίες σχετικά με την ad-hoc και τη δικτύωση αισθητήρων για τις επικοινωνίες M2M.

## 1.3. Μεθοδολογία

Η τρέχουσα μελέτη εξετάζει διάφορες περιπτώσεις χρήσης για τον προσδιορισμό των αντίστοιχων περιουσιακών στοιχείων και στη συνέχεια συλλέγει, αναλύει και κατηγοριοποιεί τις απειλές δικτύωσης ad-hoc και αισθητήρων. Για την εκτέλεση του έργου, η μεθοδολογία μας διεξήγαγε έρευνα και συγκέντρωσε τις πληροφορίες μέσω διαφόρων πηγών (δηλ. Περιοδικά, έγγραφα συνεδρίου, λευκές βίβλους, συστάσεις βιομηχανίας, ηλεκτρονικά έγγραφα). Διάφορες πηγές ντοκιμαντέρ έχουν εντοπιστεί και μελετηθεί κατά τη διάρκεια της έρευνάς μας.

Εξετάζουμε επίσης αρκετές άλλες πηγές σχετικά με τις υπάρχουσες πολιτικές της ΕΕ και εντοπίζουμε τις εξελισσόμενες απειλές, τους κινδύνους και τις προκλήσεις που σχετίζονται με ad-hoc και δίκτυα αισθητήρων με ιδιαίτερη έμφαση στο αρχιτεκτονικό μοντέλο επικοινωνίας M2M. Όλες αυτές οι απειλές αξιολογούνται, κατηγοριοποιούνται και αναλύονται με διάφορες αναφορές στις πηγές που συλλέγονται. Στη συνέχεια, πραγματοποιούμε μια ανάλυση των υφιστάμενων ορθών πρακτικών και παρουσιάζουμε τον τρόπο μείωσης της έκθεσης στην απειλή, ενώ αναγνωρίζουμε κενά στις υπάρχουσες πρακτικές. Παρουσιάζεται επίσης η παρουσίαση των εξελίξεων στον τομέα της απειλής. Τέλος, μελετάμε πώς μπορούμε να προσαρμόσουμε τις καλύτερες πρακτικές προστασίας της ασφάλειας σε μια πιο ευέλικτη διαχείριση των ελέγχων ασφαλείας.

## 1.4. Δομή της παρούσας μελέτης

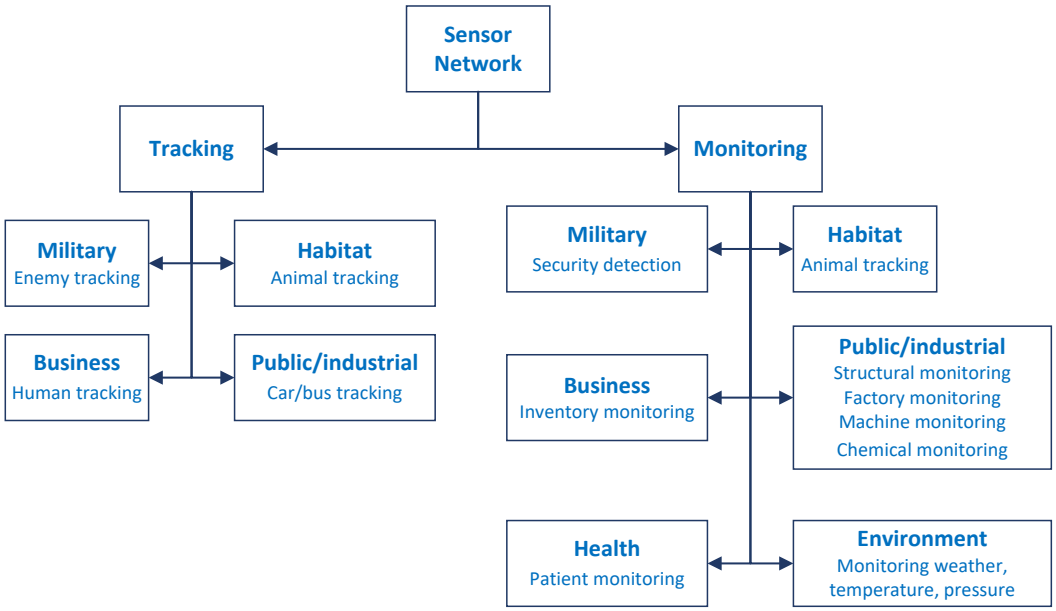
Η δομή της μελέτης έχει ως εξής: στο κεφάλαιο 2 παρέχουμε την ad hoc και τη δικτύωση αισθητήρων για τα βασικά επικοινωνίας του M2M και παρουσιάζουμε την αρχιτεκτονική. Στο κεφάλαιο 3 παρουσιάζουμε την ταξινόμηση περιουσιακών στοιχείων για δίκτυα ad-hoc και αισθητήρων στις επικοινωνίες M2M και παρουσιάζουμε τις περιπτώσεις χρήσης που αναλύονται στην τρέχουσα μελέτη. Στο κεφάλαιο 4 εντοπίζουμε τις απειλές κατά των ad-hoc και των δικτύων αισθητήρων, και στο κεφάλαιο 5 χαρτογραφούμε αυτές τις απειλές στα περιουσιακά στοιχεία. Στο κεφάλαιο 6 εξετάζουμε ποιοι παράγοντες απειλής είναι πιο συναφείς με επιθέσεις ad-hoc και αισθητήρων δικτύων. Στο κεφάλαιο 7 παρουσιάζουμε τις ευπάθειες και τους κινδύνους σε δίκτυα ad-hoc και αισθητήρων. Στο κεφάλαιο 8 παρουσιάζουμε ένα σύνολο συστάσεων και ορθών πρακτικών για ad-hoc και δίκτυα αισθητήρων. Στο Κεφάλαιο 9 παρέχουμε την ανάλυση κενού και τελικά στο κεφάλαιο 10 ολοκληρώνουμε τη μελέτη.

## 2. Αρχιτεκτονική δικτύωσης ad-hoc και αισθητήρα

Ο όρος M2M χρησιμοποιείται για να περιγράψει τεχνολογίες που επιτρέπουν την επικοινωνία μεταξύ συσκευών χωρίς περιορισμένη ή περιορισμένη ανθρώπινη παρέμβαση. Η επικοινωνία M2M απαιτεί ενσύρματη ή ασύρματη σύνδεση μεταξύ των κόμβων. Στην περίπτωση ασύρματων δικτύων ad-hoc, η επικοινωνία M2M είναι ασύρματο. Το M2M επικεντρώνεται κυρίως στην επικοινωνία τύπου μηχανής (MTC), όπου οι συσκευές επικοινωνούν από άκρο σε άκρο. Τα βασικά στοιχεία των μοντέλων M2M είναι ασύρματες συσκευές με ενσωματωμένους αισθητήρες ή ασύρματα δίκτυα επικοινωνιών με χαρακτηριστικά αναγνώρισης ραδιοσυχνοτήτων (RFID).

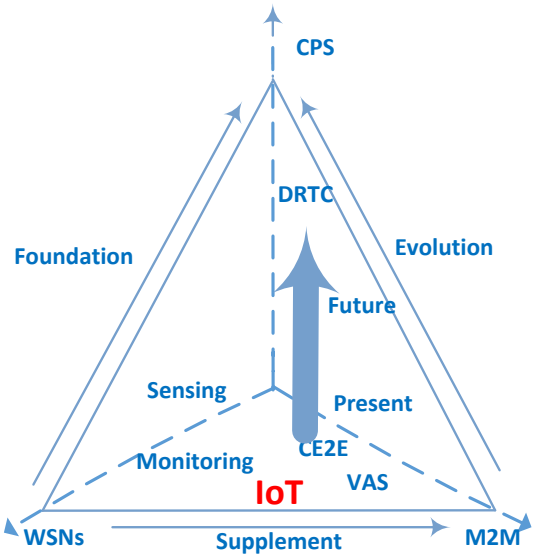
Τα ασύρματα δίκτυα ad-hoc για επικοινωνίες M2M, γνωστά και ως WANET, μπορούν να ταξινομηθούν σε τρεις τύπους, με βάση την εφαρμογή τους:

1. Τα δίκτυα ασύρματων δικτύων (WMN) χρησιμοποιούν μια τοπολογία πλέγματος που αποτελείται από ραδιοφωνικούς κόμβους. Οι κόμβοι είναι ο πελάτης πλέγματος, και οι δρομολογητές ματιών ή οι πύλες πλέγματος. Στο WMN οι πελάτες με πλέγμα, συχνά φορητοί υπολογιστές, κινητά τηλέφωνα κ.λπ., συμπεριφέρονται τόσο ως κεντρικοί υπολογιστές όσο και ως δρομολογητές για το δίκτυο. Με αυτόν τον τρόπο, κάθε πελάτης συμβάλλει στην επέκταση του δικτύου. Οι περισσότερες εφαρμογές WMN βρίσκονται σε σκληρά περιβάλλοντα ή σε καταστάσεις όπως οι πεδίου των στρατιωτικών δυνάμεων, οι δορυφορικές επικοινωνίες μέσα σε έναν αστερισμό, η παρακολούθηση των δημόσιων συγκοινωνιών ή η τηλεμετρία σε πραγματικό χρόνο σε αγώνες αυτοκινήτων. Παρομοίως, αναπτύσσονται επίσης στην ευρυζωνική δικτύωση στο σπίτι, στη δικτύωση των κοινοτήτων και των δήμων.
2. Ένα δίκτυο ad-hoc για κινητά (MANET) είναι ένα δίκτυο που έχει έρθει σε επαφή με το δίκτυο, κυρίως μεταξύ κινητών συσκευών όπως κινητά τηλέφωνα, PDA και tablet. Κάθε κόμβος συμπεριφέρεται σαν δρομολογητής, προωθώντας κάθε κίνηση που δεν σχετίζεται με τη δική του χρήση. Το γεγονός ότι οι κόμβοι κινούνται ανεξάρτητα το ένα από το άλλο καθιστά αυτό το είδος του δικτύου αναξιόπιστο και μιας συνεχώς μεταβαλλόμενης τοπολογίας. Μερικές πιο συγκεκριμένες εφαρμογές του MANET περιλαμβάνουν τη στρατιωτική ad-hoc δικτύωση μεταξύ στρατιωτών στον τομέα, οχημάτων και κεντρικών γραφείων, ad-hoc κινητής επικοινωνίας από πλοίο σε πλοίο, Personal Area Networks (PAN) κ.λπ.
3. Ένα ασύρματο δίκτυο αισθητήρων (WSN) είναι ένα δίκτυο έξυπνων κόμβων αισθητήρων. Ένας έξυπνος κόμβος αισθητήρα είναι μια συσκευή εξοπλισμένη με επεξεργαστή, μνήμη, διεπαφή ασύρματου δικτύου και έναν ή περισσότερους αισθητήρες και ενεργοποιητές. Οι αισθητήρες δίνουν στη συσκευή τη δυνατότητα παρακολούθησης αρκετών φυσικών ή περιβαλλοντικών συνθηκών. Η μνήμη περιορίζεται στην βοήθεια επεξεργασίας, έτσι όλα τα δεδομένα που αποκτούνται από τον κόμβο μεταδίδονται ασύρματα σε ένα σταθμό βάσης για αποθήκευση και περαιτέρω επεξεργασία. Επίσης μέσω του WSN ο σταθμός βάσης ή οποιοσδήποτε άλλος κόμβος μπορεί να στείλει τα δεδομένα πίσω σε έναν κόμβο αισθητήρα. π.χ. μια εντολή για τον ενεργοποιητή. Διάφορες εφαρμογές των WSNs προέκυψαν σε διάφορους τομείς, όπως στην υγειονομική περίθαλψη, το στρατιωτικό, το μεταποιητικό και το βιομηχανικό / δημόσιο σύστημα, το περιβάλλον και τα έξυπνα σπίτια, όπως φαίνεται στο σχήμα 2.




**Σχήμα 2**

Επιπλέον, η ταχεία εξέλιξη των επικοινωνιών M2M δημιουργεί νέες προκλήσεις και ευκαιρίες για τη βιομηχανία πληροφοριών. όπως για τα έξυπνα ρομπότ, τα συστήματα μεταφοράς πληροφορικής (CTS), την τηλεματική και την πρόβλεψη, τα έξυπνα δίκτυα και τα κυβερνο-φυσικά συστήματα (CPS) M2M. Το CPS είναι μια εξέλιξη του M2M στην έξυπνη επεξεργασία πληροφοριών και μια σημαντική μορφή IoT. Οι αντίστοιχες εφαρμογές του CPS θα επωφεληθούν από τα ογκώδη ασύρματα δίκτυα και το IoT με βάση τις πληροφορίες που συλλέγουν από το περιβάλλον. Οι συσχετισμοί μεταξύ των M2M, WSNs, CPS και IoT φαίνονται στο Σχήμα 3.




**CPS: Cyber-Physical Systems**
**DRTC: Distributed real-time control**
**CE2E: Communicating end-to-end**
**VAS: Value added services**

**Σχήμα 3**

Το τρέχον έγγραφο περιλαμβάνει το αρχιτεκτονικό μοντέλο M2M. Το μοντέλο αυτό αποτελείται από διάφορους τομείς, ο καθένας από τους οποίους έχει τα δικά του χαρακτηριστικά, περιουσιακά στοιχεία, απειλές και τρωτά σημεία, υφιστάμενες απειλές στον κυβερνοχώρο, τάσεις, προκλήσεις ασφάλειας, σχετικούς κινδύνους και απαιτούμενα αντίμετρα που σχετίζονται με ad hoc και δίκτυα αισθητήρων. το αρχιτεκτονικό μοντέλο επικοινωνιών M2M.

Το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) θεωρεί ένα δίκτυο M2M ως δομή τριών μερών που περιλαμβάνει:

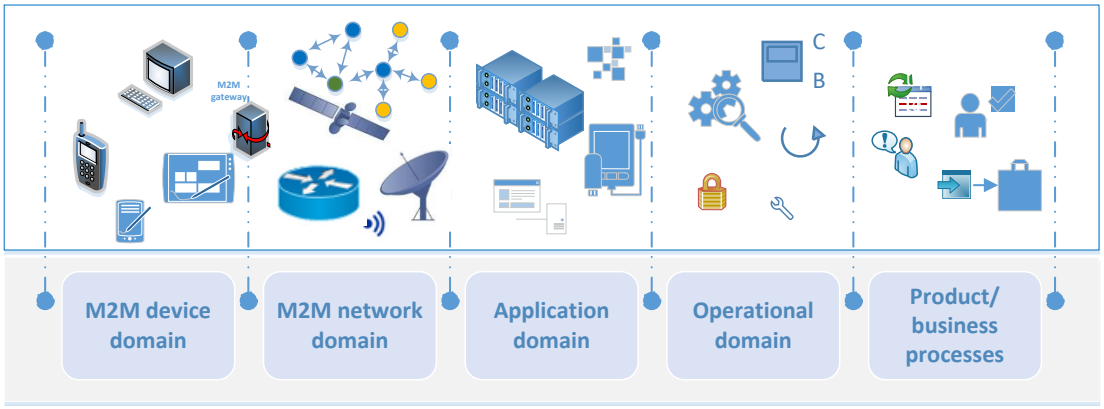
1. Τομέας συσκευής M2M (συνήθως ενσωματωμένο)
2. Τομέας δικτύου M2M (σύνδεση μεταξύ συσκευών, αισθητήρων και πύλης, σύνδεση δικτύου από δίκτυο)
3. Τομέας εφαρμογής (χειρισμός και χρήση δεδομένων από συγκεκριμένες επιχειρηματικές εφαρμογές)

Στην παρούσα μελέτη, εξετάζουμε δύο επιπλέον τομείς για την αντιμετώπιση των επιχειρησιακών προκλήσεων καθώς και των προϊόντων και των διαδικασιών αυτοματοποίησης και ροών εργασίας, συγκεκριμένα του.

1. Επιχειρησιακός τομέας (περιλαμβάνει φυσική ασφάλεια, συστήματα ελέγχου και βοηθητικά προγράμματα)
2. Τομέας προϊόντων / επιχειρήσεων (π.χ. υγειονομική περίθαλψη, μεταφορά)
   Αυτά τα πέντε στοιχεία αποτελούν διάφορους αλληλένδετους τομείς, διευκολύνουν την επεξεργασία δεδομένων από διάφορες υπηρεσίες εφαρμογής και επιτυγχάνουν πλήρη διαλειτουργικότητα του δικτύου και των υπηρεσιών. Η πλήρης εικόνα των πέντε στοιχείων απεικονίζεται στο σχήμα 3.

Στον τομέα της Συσκευής, οι συσκευές M2M συνιστούν αρκετούς κόμβους ad-hoc και αισθητήρα δικτύου για διαβίβαση δεδομένων. Αυτές οι συσκευές είναι εφοδιασμένες με συγκεκριμένες τεχνολογίες ανίχνευσης για παρακολούθηση σε πραγματικό χρόνο, προκειμένου να ληφθούν οι κατάλληλες αποφάσεις μετάδοσης στην πύλη (δηλ. Μετάδοση single-hop ή multi-hop). Η πύλη M2M λειτουργεί ως είσοδος σε άλλο δίκτυο και συλλέγει τα πακέτα από τους κόμβους M2M μέσω του δικτύου M2M. Αυτό το δίκτυο παρέχει μια σύνδεση μεταξύ όλων των ειδών ευφυών συσκευών (ή αισθητήρων) και των πύλων. Στον τομέα του Δικτύου, τα δίκτυα επικοινωνίας επιτυγχάνουν συνδέσεις και μεταδίδουν τα αισθητήρια δεδομένα μεταξύ των πύλων και των εφαρμογών.

Διάφορες υπηρεσίες εφαρμογών χρησιμοποιούνται από τους συγκεκριμένους μηχανισμούς επεξεργασίας επιχειρήσεων στον τομέα της εφαρμογής. Αυτές οι υπηρεσίες είναι υπεύθυνες για την αποθήκευση των δεδομένων και για την παροχή των δεδομένων στις εφαρμογές διαχείρισης M2M.




**Σχήμα 4**

Στο αρχιτεκτονικό μοντέλο επικοινωνιών M2M, οι λειτουργικές διαδικασίες και οι διαδικασίες προϊόντων / επιχειρήσεων μπορούν επίσης να διευρύνουν τις επιχειρηματικές δυνατότητες και να χρησιμοποιούν τις πληροφορίες σε πραγματικό χρόνο που παράγονται από το σύστημα M2M, χρησιμοποιώντας μια σύγκλιση διαφόρων τεχνολογιών.

# 3. Ανίχνευση στοιχείων ad-hoc και αισθητήρων

Οτιδήποτε αξίας μπορεί να θεωρηθεί ως περιουσιακό στοιχείο. Τα περιουσιακά στοιχεία θα μπορούσαν να είναι αφηρημένα περιουσιακά στοιχεία (όπως διαδικασίες ή φήμη), εικονικά περιουσιακά στοιχεία (π.χ. δεδομένα), φυσικά περιουσιακά στοιχεία (καλώδια, εξοπλισμός), ανθρώπινοι πόροι, χρήματα κλπ. Στη μελέτη αυτή εστιάζουμε στην ταξινόμηση ETSI προαναφερθείσα αρχιτεκτονική M2M (Σχήμα 4). Αναλύουμε τα περιουσιακά στοιχεία που σχετίζονται με τον τομέα των συγκεκριμένων περιπτώσεων χρήσης, καθώς υπάρχει ένας πολύ μεγάλος αριθμός διασυνδεδεμένων συσκευών και ένας σημαντικός αριθμός τύπων περιουσιακών στοιχείων στην ad hoc ασύρματη δικτύωση και τη δικτύωση αισθητήρων για τον τομέα επικοινωνιών M2M. Συμπερασματικά, η προσέγγιση που παρουσιάζεται δεν πρέπει να θεωρείται εξαντλητική αλλά μάλλον ανάλυση των περιουσιακών στοιχείων σε διάφορες επιχειρηματικές περιπτώσεις και διαφορετικές προοπτικές.

Στον τομέα της συσκευής, συλλαμβάνουμε αυτές τις συσκευές που είναι ικανές για επεξεργασία δεδομένων, ενώ στον τομέα του Δικτύου, μελετάμε τα στοιχεία ενεργητικού που επιτρέπουν την επικοινωνία μεταξύ των εφαρμογών. Περιλαμβάνουμε επίσης τις επιχειρησιακές πτυχές και τη μοντελοποίηση των επιχειρηματικών διαδικασιών, προκειμένου να συνδυάσουμε κλασικές λειτουργίες και διαδικασίες με επεκτάσεις ad-hoc και δικτύων αισθητήρων και δυνατότητες. Η ανταλλαγή δεδομένων, τα συστήματα ελέγχου, οι εφαρμογές παρακολούθησης και μέτρησης μπορούν να αποτελέσουν μέρος πολλών επιχειρηματικών διαδικασιών που επιτρέπουν την τυποποίηση και τη διαλειτουργικότητα των υλοποιήσεων των λύσεων M2M.

## 3.1. Ταξινόμηση περιουσιακών στοιχείων

Τα στοιχεία ενεργητικού ad-hoc και αισθητήρα δικτύου αναγνωρίζονται και ταξινομούνται με βάση τα δομικά στοιχεία των ακόλουθων τομέων:

1. ***Application domain***
    a. Data
    b. Critical applications
    c. eHealth
    d. Cloud-based applications
2. ***Device domain***
    a. Car/vehicles
    b. Mobile devices
    c. RFID tags
    d. RFID readers
    e. Radars
    f. Transmission nodes
    g. Interconnection point
    h. Support systems
    i. Wearable
    j. Indoor positioning systems
    k. Computer Electronics (CE) devices
3. ***Network domain***
    a. Communication protocols

b. Cooling systems
c. Power supplies
d. Home Automation
e. Mobile user and location registers
f. Radio
g. Public-Key Infrastructure (PKI)
h. Appliance controls
i. Addressing servers
j. Mobile switches
k. Public Switched Telephone Network (PSTN) switches
l. Physical security & control systems
m. Routers & switches
n. Mobile base stations and controllers
o. Servers
p. WBSNs (Wireless Body Sensor Networks)

4. ***Operational domain***
   a. Physical security
   b. Control systems
   c. Utilities

5. ***Product/business processes domain***
   a. Supply and provisioning
   b. Manufacturing
   c. Healthcare
   d. Transportation

## 3.2. Κατηγορίες περιουσιακών στοιχείων

Σύμφωνα με το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI), η αρχιτεκτονική M2M αποτελείται από τρεις τομείς: τον τομέα της συσκευής, τον τομέα δικτύου και τον τομέα εφαρμογών. Όπως παρουσιάζεται στο Κεφάλαιο 2, επεκτείνουμε το μοντέλο που περιλαμβάνει τον τομέα λειτουργίας και τον τομέα προϊόντος / επιχειρηματικών διαδικασιών. Με βάση αυτή την κατηγοριοποίηση, τα πολύτιμα στοιχεία ενεργητικού δικτύου ad-hoc και ασύρματου αισθητήρα παρατίθενται παρακάτω. Ο πλήρης κατάλογος αυτών των στοιχείων ενεργητικού παρουσιάζεται στο σχήμα 5.


Asset details
Assets
Domain
Domain
Assets
Asset details
Ad-hoc & sensor assets
Device
Cars/vehicles
Event Data Recorder
GPS receiver
On-board equip.
Radars and sensors
Omnidirectional antenna
Electronic License Plate
Mobile devices
IoT
Tablets
Mobile phones
PPDs
RFID tags
RFID readers
Tablets
Smartphones
Standalone devices
Radars
Range finders
Motion detectors
Transmission nodes
Interconnection points
Support systems
Wearable
Alerting devices
Accelerometers
Fitness trackers
Indoor positioning systems
CE devices
HDTV
PVR
DVD
Cameras
Operational
Physical security
Surveillance applications
Object/people tracking
Alarms
Control systems
Application control with smart-grid
Building/Campus automation
HVAC
BSS
Utilities
Billing of utilities
Provisioning
Measurement
Application
Data
Financial
Private
Confidential
Critical apps
Billing & mediation
Mobile messaging center
E-health
Portals
Web-services
Private Healthcare Information (PHI) database
Cloud-based apps
Cloud based Clinical information system (CIS)
Network
Communication protocols
Cooling systems
Power supplies
Servers
Mobile user and location registers
Radio
Software
Hardware
PKI
Appliance control with smart-grid
Addressing servers
Mobile switches
PSTN switches
Physical security & control systems
Lighting control system
Household security systems
Physical perimeter
Buildings
Routers & Switches (DSLAM, SBC, etc.)
Mobile base stations and controllers
WBSNs/WBANs
Product/business processes
Home automation
Supply and Provisioning
Distribution monitoring
Vending machines
Freight supply
Manufacturing
Automation
Production chain monitoring
Healthcare
ehealth security
Personal security
Transportation
Road safety
Emission control
Fleet management
Toll payment

**Σχήμα 5**

### 3.2.1. Τομέας εφαρμογής

Ο τομέας εφαρμογής περιλαμβάνει εφαρμογές M2M και πελάτη. Είναι το στρώμα middleware μεταξύ του τελικού χρήστη και των δεδομένων που παρέχονται από το Ddomain συσκευής M2M, αφού υποβάλλονται σε επεξεργασία από διάφορες υπηρεσίες εφαρμογών. Τα περιουσιακά στοιχεία αυτού του τομέα περιγράφονται παρακάτω.

a. Δεδομένα

Σε αυτόν τον τομέα, τα δεδομένα που συλλέγονται από συσκευές αποθηκεύονται, διαχειρίζονται και εκπροσωπούνται μέσω εφαρμογών ή διεπαφών ιστού στον χρήστη. Τα δεδομένα μπορούν να χρησιμοποιηθούν μόνο για πληροφόρηση, στατιστική ανάλυση και δυνατότητες ελέγχου.

b. Κρίσιμες εφαρμογές

Οι κρίσιμες εφαρμογές είναι εφαρμογές ειδικού σκοπού, που συνδυάζουν πληροφορίες και δεδομένα από διάφορες πηγές (π.χ. αισθητήρες, συσκευές, διαδίκτυο και βάσεις δεδομένων).

c. Ηλεκτρονική υγεία

Σε ένα δίκτυο Mobile Healthcare Network (MHN), ο συνδυασμός δεδομένων από φορητό εξοπλισμό, smartphone και εξοπλισμό παρακολούθησης ζωτικών μπορεί να παρέχει στο άτομο ή το γιατρό ολόκληρη την εικόνα μιας περίπτωσης υγείας και το Personal Health Record (PHR). Σημαντικό μέρος ενός MHN είναι οι εφαρμογές ηλεκτρονικής υγείας που αποθηκεύουν, αντιπροσωπεύουν και επεξεργάζονται τα δεδομένα που συλλέγονται για να παράγουν στατιστικά στοιχεία. Στην ανάγκη αποθήκευσης PHR, χρησιμοποιείται μια βάση δεδομένων ιδιωτικής υγειονομικής περίθαλψης (PHI) με ιδιαίτερες ανησυχίες για την προστασία της ιδιωτικής ζωής και των δεδομένων. Οι διασυνδέσεις αντιπροσώπευσης είναι οι πύλες eHealth, οι εφαρμογές μέσω διαδικτύου ή οι κινητές εφαρμογές.

d. Εφαρμογές με βάση το σύννεφο

Η ενσωμάτωση των δικτύων αισθητήρων και του cloud computing υποκινείται από τις δυνατότητες επεξεργασίας και αποθήκευσης του cloud. Αυτή η υπηρεσία ανίχνευσης νέφους αισθητήρα (SSaaS) οδηγεί στην δυνατότητα πολλαπλών εφαρμογών να έχουν ταυτόχρονη πρόσβαση στα δεδομένα αισθητήρα. Επιπλέον, το μοντέλο cloud αισθητήρα βελτιώνει τη χρήση των πόρων του αισθητήρα και τη διαχείριση αισθητήρων και παρέχει το περιβάλλον για την ανάπτυξη διασυνδέσεων λογισμικού μεταξύ αισθητήρων και του κυβερνοχώρου ή του πραγματικού κόσμου.

Επιπλέον, οι εφαρμογές κινητών υπολογιστών δέχονται μια αυξανόμενη προσπάθεια να βοηθήσουν το οικοσύστημα δικτύωσης αισθητήρων. Για τους λόγους αυτούς, οι πρόσφατες τεχνολογικές εξελίξεις στις εφαρμογές για κινητά cloud περιλαμβάνουν τον Smartcard Web Server του Open Mobile Alliance (OMA), ο οποίος συνδυάζεται κυριολεκτικά με μια κινητή συσκευή (π.χ. κάρτα SIM) που συνδέεται άμεσα με τον Μεταφορέα σε κινητά τηλέφωνα. Ένα άλλο παράδειγμα είναι το TokTok, μια τεχνολογία που επιτρέπει την πρόσβαση σε υπηρεσίες που βασίζονται σε σύννεφο, όπως το Gmail και το ημερολόγιο Google με φωνή, χρησιμοποιώντας τη συσκευή κινητού τηλεφώνου.

### 3.2.2. Περιοχή συσκευής

Ο τομέας συσκευής M2M στην αρχιτεκτονική ETSI είναι ο συνδυασμός των συσκευών M2M και του δικτύου περιοχής M2M. Ο τομέας της συσκευής M2M, όπως υποδηλώνει ο όρος, είναι η ομάδα συσκευών που είναι σε θέση να απαντήσουν σε αιτήματα δεδομένων ή να μεταδώσουν αυτά τα δεδομένα αυτόνομα. Η συνδεσιμότητα μεταξύ των συσκευών M2M και των πύλων M2M είναι το δίκτυο περιοχής M2M. Τα παρακάτω υποτμήματα παρουσιάζουν τα πιο συνηθισμένα στοιχεία ενεργητικού στον τομέα της συσκευής.

a. Αυτοκίνητα και οχήματα

Τα οδικά ad hoc δίκτυα (VANET) είναι μια υποκατηγορία των δικτύων ad hoc Mobile (MANETs). Το υλικό εξοπλισμού ενός VANET είναι κυρίως ο ενσωματωμένος στο όχημα εξοπλισμός, ο οποίος παρέχει τα μέσα επικοινωνίας με άλλα οχήματα (επικοινωνία οχήματος προς οχήματα - V2V) ή με την υποδομή δικτύου (οχήματος προς υποδομή - V2I και Infrastructure-to-Vehicle - I2V). Ορισμένα στοιχεία εξοπλισμού VANET παρουσιάζονται παρακάτω:

- Εγγραφή δεδομένων συμβάντων (EDR): καταγράφει τις μεταδόσεις και λαμβάνει μηνύματα και όλα τα συμβάντα που συνέβησαν στο περιβάλλον του οχήματος κατά τη διάρκεια ενός ταξιδιού
- Δέκτης συστήματος GPS (Global Positioning System): ανακοινώνει τη γεωγραφική θέση, την ταχύτητα, την κατεύθυνση της κίνησης και την επιτάχυνση του κόμβου σε συγκεκριμένα χρονικά διαστήματα
- Ραντάρ και αισθητήρες: χρησιμοποιούνται για τον εντοπισμό εμποδίων στο περιβάλλον του οχήματος
- Omnidirectional antenna: χρησιμοποιείται για πρόσβαση σε ασύρματα κανάλια
- Ηλεκτρονική πινακίδα κυκλοφορίας (ELP): παρέχει έναν αριθμό ταυτότητας που χρησιμοποιείται από την αστυνομία ή οποιαδήποτε άλλη αρχή

b. Κινητή συσκευή

Μια ενσωματωμένη διασύνδεση (κεραία GSM, Wi-Fi, Bluetooth, κ.λπ.) και οι εξατομικευμένες φορητές συσκευές (όπως η κάμερα, το γυροσκόπιο, το θερμόμετρο, το GPS κ.λπ.) συνδέονται με το δίκτυο περιοχής χρησιμοποιώντας τους ενσωματωμένους αισθητήρες PPDs).

c. Ετικέτες RFID

Στον τομέα της συσκευής, τα συστήματα RFID περιλαμβάνουν ετικέτες, αναγνώστες και ενδιάμεσο λογισμικό RFID. Οι ετικέτες RFID είναι οι μικρές ετικέτες που επισυνάπτονται σε αντικείμενα, ζώα ή ανθρώπους για να ενσωματώσουν κάποιες πληροφορίες σε αυτά ή να τα καταστήσουν αναγνωρίσιμα μεταξύ άλλων. Ένα κύκλωμα ετικετών RFID αποτελείται από μια μονάδα ελέγχου και μια κεραία.

d. Αναγνώστες RFID

Ένας αναγνώστης RFID είναι μια συσκευή ή δέκτης που συχνά ενσωματώνεται σε άλλες κοινές συσκευές, (δηλαδή smartphones) που μπορούν να πάρουν τις πληροφορίες μιας ετικέτας όταν βρίσκονται εντός εμβέλειας. Το λογισμικό που εξασφαλίζει την επικοινωνία μεταξύ του αναγνώστη και ενός συστήματος αποθήκευσης βάσεων δεδομένων ονομάζεται ενδιάμεσο λογισμικό RFID. Το τελευταίο φιλτράρει, επεξεργάζεται και αποστέλλει τα δεδομένα που συλλέγονται από τον αναγνώστη στη βάση δεδομένων και παρέχει μια διεπαφή για την ενεργοποίηση της πρόσβασης δεδομένων για εξωτερικές εφαρμογές.

e. Ραντάρ

Ένα ραντάρ ώθησης μικρο-τροφοδοσίας (MIR) ισχύει σε πολλά πεδία ως ανιχνευτής κίνησης ή ανιχνευτής εύρους. Τα ραντάρ χρησιμοποιούνται ευρέως στον στρατό για την προστασία των περιουσιακών στοιχείων, στις εφαρμογές διάσωσης, στην αυτοματοποίηση των οχημάτων (βοήθεια στάθμευσης, κρουαζιέρες κ.λπ.), στα συστήματα οικιακής ασφάλειας (κλειδαριές χωρίς κλειδί, αυτόματες πόρτες κλπ.) Και στον τομέα της βιομηχανικής αυτοματισμού ).

f. Κόμβοι μετάδοσης

Σε μια ομαδοποιημένη αρχιτεκτονική, οι κόμβοι των αισθητήρων ομαδοποιούνται σε ομάδες, όπου κάθε σύμπλεγμα έχει εκλέξει έναν κόμβο ως Κεφαλή συμπλέγματος (CH). Αυτός ο κόμβος είναι αυτός που μεταδίδει όλα τα δεδομένα των κόμβων συμπλέγματος στον σταθμό βάσης. Αυτό μετριάζει την κατανάλωση ενέργειας, την κυκλοφοριακή συμφόρηση και τις συγκρούσεις δεδομένων στο δίκτυο.

g. Σημεία διασύνδεσης

Σύμφωνα με την αρχιτεκτονική ETSI M2M, ένα σημείο διασύνδεσης είναι η πύλη μεταξύ των συσκευών και του δικτύου επικοινωνίας, η οποία αναφέρεται επίσης στην αρχιτεκτονική ως πύλη M2M. Το σημείο διασύνδεσης διαχειρίζεται τα πακέτα και παρέχει αποτελεσματικές διαδρομές για τη μετάδοση αυτών των πακέτων στον απομακρυσμένο διακομιστή υποστήριξης μέσω του τομέα Δικτύου.

h. Συστήματα υποστήριξης

Λόγω της πολυπλοκότητας και του μεγάλου όγκου κίνησης σε δίκτυα ad hoc και αισθητήρων, υπάρχει μια αναδυόμενη ανάγκη για τα κατάλληλα, βιώσιμα, συγκλίνοντα, ολοκληρωμένα και λειτουργικά συστήματα υποστήριξης. Τα συστήματα υποστήριξης επιχειρήσεων (BSS) είναι ένας συλλογικός όρος για το σύνολο λύσεων λογισμικού που χρησιμοποιούν οι πάροχοι τηλεπικοινωνιών για την εκτέλεση των επιχειρηματικών τους δραστηριοτήτων. Ο όρος περιλαμβάνει λογισμικό χρέωσης και χρέωσης, διαχείριση πελατών, σχεδιασμό και διαχείριση προϊόντων, πωλήσεις και μάρκετινγκ, καθώς και ενεργοποίηση παραγγελιών και παραγγελιών. Το BSS αποτελεί επίσης λειτουργικό πλεονέκτημα των εν λόγω δικτύων.

i. Απορρίμματα

Μια φορητή συσκευή μπορεί να φορεθεί άνετα ή να μεταφερθεί από ένα άτομο όλη την ημέρα και να παρακολουθεί διάφορα βιομετρικά στοιχεία όπως η θερμοκρασία του σώματος, η αρτηριακή πίεση, τα επίπεδα διαβήτη, η διαπνοή, ο ρυθμός καρδιακού ρυθμού κλπ. Γενικά, η φορητή τεχνολογία έχει κάποια μορφή επικοινωνιακής ικανότητας και επιτρέπει χρήστη να έχει πρόσβαση στις πληροφορίες σε πραγματικό χρόνο. Οι δυνατότητες εισαγωγής δεδομένων διαθέτουν τις φορητές συσκευές, όπως και η τοπική αποθήκευση. Παραδείγματα φορητών συσκευών περιλαμβάνουν ρολόγια, γυαλιά, φακούς επαφής, ηλεκτρονικά κλωστοϋφαντουργικά προϊόντα και έξυπνα υφάσματα, ταινίες κεφαλής, καραμέλες και καπέλα, κοσμήματα όπως δακτυλίους, βραχιόλια και συσκευές ακοής που σχεδιάζονται για να μοιάζουν με σκουλαρίκια.

j. Εσωτερικά συστήματα εντοπισμού θέσης

Τα συστήματα εσωτερικής τοποθέτησης (IPS) παρέχουν τη δυνατότητα εντοπισμού της θέσης ενός αντικειμένου ή ενός ατόμου μέσα σε ένα κτίριο χρησιμοποιώντας ραδιοκύματα, μαγνητικά πεδία, ακουστικά σήματα ή άλλες αισθητηριακές πληροφορίες.

k. Συσκευές CE

Οι συσκευές ηλεκτρονικών καταναλωτών (DVD, κάμερες, τηλεοράσεις, PVR, κονσόλες παιχνιδιών κ.λπ.) χρησιμοποιούν συνήθως σήματα επικοινωνίας Ultra Wideband (UWB) και αποτελούν μέρος του συστήματος οικιακού αυτοματισμού.

### 3.2.3. Τομέας Δικτύου

Όπως αναφέρεται στην περιγραφή του τομέα της συσκευής, η πύλη M2M εξασφαλίζει την αλληλεπίδραση και τη διασύνδεση μεταξύ των συσκευών και του δικτύου επικοινωνίας. Το κύριο μέρος του τομέα του δικτύου M2M είναι η επικοινωνία μεταξύ της πύλης M2M και του τομέα εφαρμογών M2M. Η επικοινωνία εκτελείται είτε μέσω ενσύρματων δικτύων (π.χ. xDSL και PLC) είτε ασύρματων δικτύων (π.χ. 3G κυψελοειδές, Wi-Fi και Παγκόσμια διαλειτουργικότητα για πρόσβαση μικροκυμάτων - WiMAX). Η παρακάτω λίστα περιουσιακών στοιχείων δεν είναι εξαντλητική και περιλαμβάνει ορισμένα από τα πιο κοινά περιουσιακά στοιχεία σε αυτόν τον τομέα.

a. Πρωτόκολλα επικοινωνίας

Το πρωτόκολλο επικοινωνίας αποτελεί βασικό στοιχείο στην ανάπτυξη ad-hoc και δικτύων αισθητήρων και συχνά είναι επιρρεπής σε διάφορες απειλές και επιθέσεις. Το πρωτόκολλο επικοινωνίας μπορεί να έχει διάφορες ευπάθειες ασφαλείας, σφάλματα στον κώδικα, αδυναμία απόκρισης και μη ασφαλείς υπηρεσίες μεταφοράς και υπηρεσιών στρώματος δικτύου.

b. Συστήματα ψύξης

Τα ενεργειακά αποδοτικά και ασφαλή συστήματα ψύξης εξασφαλίζουν τη διαθεσιμότητα και την ορθή λειτουργία των δικτύων ad-hoc και αισθητήρων.

c. Τροφοδοτικά

Γενικά, τα συστήματα τροφοδοσίας ρεύματος σε δρομολογητές, διακόπτες, διακομιστές και υπολογιστές είναι κρίσιμα στοιχεία του δικτύου, τα οποία είναι εξαιρετικά ευάλωτα σε φυσικές επιθέσεις ή αποτυχίες.

d. Καταχωρητές κινητών χρηστών και τοποθεσίας

Οι καταχωρητές κινητών χρηστών και τοποθεσιών χρησιμοποιούνται για τον προσδιορισμό της γεωγραφικής περιοχής και για την ενημέρωση των κόμβων σχετικά με τις τελευταίες πληροφορίες θέσης.

e. Ραδιόφωνο

Δεδομένου ότι τα περισσότερα ad-hoc και δίκτυα αισθητήρων βασίζονται σε ασύρματες επικοινωνίες, το ίδιο το ραδιόφωνο είναι το μέσο, επομένως το ραδιόφωνο είναι ένα στοιχείο στο πεδίο Δικτύου.

f. PKI

Η Υποδομή Δημόσιου Κλειδιού (PKI) είναι ένας τελευταίας τεχνολογίας μηχανισμός εμπιστευτικότητας (κρυπτογράφησης) και ελέγχου ταυτότητας για σχεδόν όλες τις εφαρμογές ad-hoc και την επικοινωνία του δικτύου αισθητήρων.

g. Συσκευές ελέγχου

Λόγω των πρόσφατων εξελίξεων σε ad-hoc και αισθητήρια δίκτυα, οι χρήστες μπορούν τώρα να παρακολουθούν εύκολα τις υπηρεσίες και να ελέγχουν εξ αποστάσεως τις συσκευές.

h. Αντιμετώπιση διακομιστών

Η καταχώρηση και η αντιστοίχιση διευθύνσεων είναι σημαντική σε ad-hoc και δίκτυα αισθητήρων. Επίσης, επηρεάζουν άλλες υπηρεσίες και λειτουργίες, όπως η δρομολόγηση. Πρέπει να χρησιμοποιηθεί μια αποδοτική και ανθεκτική λύση αντιμετώπισης.

i. Κινητοί διακόπτες

Ο πάροχος τηλεπικοινωνιών στις περισσότερες περιπτώσεις είναι ένας πάροχος κυψελοειδούς δικτύου. Το σύστημα του παροχέα αποτελείται από κινητούς χρήστες και καταχωρητές θέσης, κινητούς σταθμούς βάσης, ελεγκτές κ.λπ.

j. Διακόπτες PSTN

Τα δίκτυα υποδομής βασίζονται συνήθως στα συστατικά του πυρήνα του δικτύου και μπορεί να κατασκευαστούν από τους διακόπτες σπονδυλικής στήλης του PSTN.

k. Συστήματα φυσικής ασφάλειας και ελέγχου

Η φυσική ασφάλεια συχνά υποτιμάται και παραβλέπεται στην περίπτωση ad-hoc και δικτύων αισθητήρων. Ένα κατάλληλο σχέδιο με τα απαραίτητα συστήματα ελέγχου είναι ζωτικής σημασίας για να αποφευχθεί η υποβάθμιση των αισθητήρων στο δίκτυο.

l. Δρομολογητές και διακόπτες

Αυτή η ομάδα στοιχείων ενεργητικού είναι ο πυρήνας του τομέα Δικτύου. Οι δρομολογητές, τα DSLAM, οι ελεγκτές συνόρων περιόδου λειτουργίας (SBCs) και οι διακόπτες δικτύου σχηματίζουν το δίκτυο δεδομένων στο οποίο διασυνδέονται ο τομέας Devices Domain και ο τομέας εφαρμογών.

m. Κινητοί σταθμοί βάσης και ελεγκτές

Οι τοπολογίες των σταθμών βάσης και των ελεγκτών επηρεάζουν τη δρομολόγηση σε δίκτυα ad-hoc και αισθητήρων και την απόδοση στην ανταλλαγή αισθητηριακών δεδομένων. Οι περισσότερες εφαρμογές μπορούν

να επωφεληθούν από την τοπολογία των κόμβων αισθητήρων και τη δρομολόγηση δεδομένων στους άλλους κόμβους αισθητήρων, έναν εξωτερικό σταθμό βάσης ή έναν ελεγκτή.

n. Διακομιστές

Το σύστημα διακομιστή που υποστηρίζει τη λειτουργία σύνδεσης δικτύου είναι ένα άλλο στοιχείο στον τομέα Δικτύου. Σημαντικές υπηρεσίες που περιλαμβάνονται σε αυτόν τον τομέα είναι η διεύθυνση και η ονομασία DNS, η αναγνώριση ιδιωτικού κλειδιού για συσκευές ή χρήστες, η παρακολούθηση και η διαχείριση της κίνησης δικτύου κ.λπ.

o. WBSNs / WBAN

Τα ασύρματα δίκτυα αισθητήρων σώματος (WBSN) ή τα δίκτυα σώματος (WBAN) αποτελούν αναδυόμενα ασύρματα δίκτυα φορητών υπολογιστικών συσκευών. Σε γενικές γραμμές, αυτό το είδος δικτύων έχει ενδιαφέρον για εφαρμογές, όπως η υγεία, η απομακρυσμένη μέτρηση πληροφοριών για την υγεία, η παροχή βοήθειας στους ασθενείς και τους ηλικιωμένους, οι αυτοματισμοί στο σπίτι και η παρακολούθηση των αλλαγών του ανθρώπινου σώματος.

### 3.2.4. Επιχειρησιακός τομέας

Οι διαδικασίες αυτοματοποίησης, οι οποίες μέχρι πρόσφατα χειρίστηκαν από τους ανθρώπους, μπορούν να εξασφαλίσουν αποτελεσματικότητα στην ικανοποίηση των απαιτήσεων των πελατών, χρησιμοποιώντας όσο το δυνατόν λιγότερους πόρους. Ορισμένα τυπικά παραδείγματα των περιουσιακών στοιχείων που εμπλέκονται σε αυτόν τον τομέα παρατίθενται παρακάτω.

a. Σωματική ασφάλεια

Η φυσική ασφάλεια παρακολούθησης και διασφάλισης πρόσβασης σε περιοχές / ζώνες, αντικείμενα ή άτομα είναι μια λειτουργία ad-hoc και δικτύων αισθητήρων. Τα τυπικά παραδείγματα περιλαμβάνουν συστήματα συναγερμού, εφαρμογές παρακολούθησης βίντεο και κάμερας κ.λπ.

b. Συστήματα ελέγχου

Τα συστήματα ελέγχου που παρέχουν πρόσβαση σε κτίρια, κατοικίες ή συγκεκριμένες περιοχές αποτελούν περιουσιακά στοιχεία των λειτουργιών ad-hoc και αισθητήρων. Μια περίπτωση είναι η χρήση έξυπνου δικτύου για τη διευκόλυνση της ανάπτυξης συστημάτων ελέγχου συσκευών. Αυτά τα συστήματα αποτελούνται από συσκευές αποθήκευσης ενέργειας, καλώδια μετάδοσης, έξυπνους υποσταθμούς και μετασχηματιστές, προηγμένη υποδομή μέτρησης (AMI) και οικιακά δίκτυα (HAN). Γενικά, τα συστήματα αυτά χρησιμοποιούνται ως συστήματα οικιακού αυτοματισμού (π.χ. συστήματα θέρμανσης, εξαερισμού και κλιματισμού - HVAC), συστήματα αυτοματισμού κτιρίων ή πανεπιστημίων κλπ.

c. Βοηθητικά προγράμματα

Αυτά τα δίκτυα μπορούν να παρέχουν λύσεις αυτοματοποίησης σε περιπτώσεις μέτρησης, παροχής και τιμολόγησης νερού, ηλεκτρισμού, πετρελαίου, θερμότητας κλπ.

Στις επόμενες ενότητες, αναλύουμε τα χαρακτηριστικά και τα χαρακτηριστικά πολλών τύπων περιπτώσεων χρήσης στους προαναφερθέντες τομείς για να προσδιορίσουμε τα αντίστοιχα στοιχεία ενεργητικού. Η χαρτογράφηση μεταξύ αυτών των περιπτώσεων χρήσης και των περιουσιακών στοιχείων συνοψίζεται επίσης στο παράρτημα Α.

### 3.2.5. Πεδίο προϊόντων / επιχειρηματικών διαδικασιών

Τα ad-hoc και τα δίκτυα αισθητήρων μπορούν να παρέχουν λύσεις αυτοματοποίησης για πολλούς τομείς επιχειρηματικής οργάνωσης και λειτουργίας. Μερικά από τα στοιχεία ενεργητικού σε αυτόν τον τομέα παρατίθενται παρακάτω.

a. Προμήθεια και πρόβλεψη

Αυτή είναι μια περιοχή υψηλής αξίας για μια εταιρεία παραγωγής προϊόντων και πρέπει να επιτευχθεί με μεγάλη ταχύτητα και ακρίβεια. Οι αισθητήρες και οι ενεργοποιητές χρησιμοποιούνται για την αυτοματοποίηση διαδικασιών όπως η μεταφορά εμπορευμάτων, η συσκευασία προϊόντων κλπ. Επιπλέον, το λογισμικό στον τομέα της εφαρμογής (π.χ. συστήματα υποστήριξης επιχειρήσεων - BSS) παρέχει παρακολούθηση και διαχείριση ικανοτήτων στους ανθρώπινους πόρους της εταιρείας. Τα μηχανήματα αυτόματης πώλησης είναι επίσης κοινά σε αυτόν τον τομέα.

b. Βιομηχανοποίηση

Σε ένα σύγχρονο περιβάλλον παραγωγής, τα συστήματα κατασκευής χρησιμοποιούν εκτεταμένες λειτουργίες δικτύου ad-hoc και αισθητήρων για τη βελτίωση της ποιότητας των υπηρεσιών, την αποτελεσματική διαχείριση των κατασκευαστικών πόρων και την επίτευξη εργασιών σχεδόν μηδενικού χρόνου.

c. Φροντίδα υγείας

Στην υγειονομική περίθαλψη, διάφορες εφαρμογές ad-hoc και αισθητήρων χρησιμοποιούνται ευρέως για την παρακολούθηση και την αρχειοθέτηση δεδομένων. Αυτές οι εφαρμογές πρέπει να δίνουν μεγάλη προσοχή στην ασφάλεια, λόγω της ευαισθησίας των δεδομένων και των θεμάτων προστασίας της ιδιωτικής ζωής. Οι αισθητήρες συχνά ενσωματώνονται και ενσωματώνονται με συσκευές παρακολούθησης της υγείας που παρέχουν δεδομένα σε πραγματικό χρόνο ή με βάση την παρτίδα.

d. Μεταφορά

Το ζήτημα της διαχείρισης του στόλου είναι σημαντικό για την επιχείρηση και επηρεάζει την αποδοτικότητα της διανομής του προϊόντος, το κόστος του προϊόντος και την οικονομία των επιχειρήσεων γενικά. Με την αυτοματοποίηση και την παρακολούθηση του στόλου, οι εκπομπές, η οδική ασφάλεια και η πληρωμή των διοδίων, καθώς και το επιχειρηματικό κέρδος είναι τελικά καλύτερα ελεγχόμενα.

e. Οικιακός αυτοματισμός

Πρόσφατα, η χρήση ad-hoc και δικτύων αισθητήρων στον οικιακό αυτοματισμό έχει αποκτήσει μεγαλύτερη προσοχή και έχουν εξελιχθεί αρκετές λύσεις, όπως η απομακρυσμένη παρακολούθηση της ηλεκτρικής ενέργειας, η προσαρμογή της παροχής νερού, ο έλεγχος της κατανάλωσης φυσικού αερίου και η διαχείριση συσκευών εξοπλισμένων με αισθητήρες.

## 3.3. Τύποι περιπτώσεων

Με τη συλλογή των πληροφοριών μπορούν να ταξινομηθούν τα δίκτυα ad-hoc και αισθητήρων για τις απειλές επικοινωνίας M2M, συμπεριλαμβανομένων των πληροφοριών για τους κινδύνους, τις ευκαιρίες, τους παράγοντες απειλής, τον αντίκτυπο, τα τρωτά σημεία κλπ. Οι περιπτώσεις χρήσης που έχουν αναλυθεί και μελετηθεί βασίζονται στις πλέον κοινές περιοχές δικτύων αισθητήρων και ενδιαφέροντος. Λόγω της μεγάλης ετερογένειας του τύπου των συσκευών, των δυνατοτήτων τους (δηλαδή της επικοινωνίας, της υπολογιστικής), των τομέων του δικτύου και των εφαρμογών, πρέπει να αξιολογήσουμε τα πιο αντιπροσωπευτικά περιβάλλοντα. Πολλές μικρές και φθηνές φορητές συσκευές μπορούν να χρησιμοποιηθούν για ασύρματες εφαρμογές δικτύου αισθητήρων τόσο για στρατιωτική όσο και για μη στρατιωτική χρήση. Αυτά τα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν για τη μεταφορά των συλλεγόμενων πληροφοριών στον προορισμό ανιχνεύοντας τυχόν διαθέσιμες περιβαλλοντικές μεταβολές. Για παράδειγμα, μια πολιτική εφαρμογή μπορεί να περιλαμβάνει κάποιο είδος παρακολούθησης ενδιαιτημάτων, παρακολούθηση της υγείας και οικιακό αυτοματισμό, ενώ οι στρατιωτικές εφαρμογές θα μπορούσαν να χρησιμοποιηθούν για την παρακολούθηση των εχθρών και τη βελτίωση της αποτελεσματικότητας.

Αναλύουμε πέντε περιπτώσεις χρήσης που παρατίθενται παρακάτω:

1. Επικοινωνία και εφαρμογές υπερευρείας ζώνης (UWB)
2. Εφαρμογές και πρωτόκολλα RFID
3. Mobile cloud computing και κινητή κοινωνική δικτύωση
4. Λογισμικά ad-hoc και δίκτυα αισθητήρων
5. Δίκτυα σώματος και ηλεκτρονική υγεία

Όσον αφορά την τεχνολογία μετάδοσης UWB, σημειώθηκαν πρόσφατα σημαντικές εξελίξεις και καινοτομίες. Το UWB περιλαμβάνει λειτουργίες που θα μπορούσαν να αξιοποιηθούν σε δίκτυα ad-hoc. Όσον αφορά τις εφαρμογές και πρωτόκολλα RFID, ένα τυπικό παράδειγμα και μια κοινή πρακτική που χρησιμοποιείται σε πολλές επιχειρηματικές περιπτώσεις, προϊόντα και ιστότοπους είναι η έξυπνη σήμανση των πραγμάτων. Μπορούν να χρησιμοποιηθούν διάφορες μορφές επικοινωνιών και τεχνολογιών χωρίς επαφή, όπως η επικοινωνία Near-Field (NFC), οι κωδικοί γρήγορης απόκρισης (QR) και το Bluetooth.

Τα κινητά και cloud computing (MCC) αναπτύσσονται γρήγορα, παρέχοντας διάφορες τεχνολογικές, ερευνητικές και επιχειρηματικές ευκαιρίες. Η τεχνολογία MCC αναφέρεται στις κινητές συσκευές, τις διεπαφές υπολογιστών, τους φορείς κινητής τηλεφωνίας και τους παρόχους υπηρεσιών cloud που προσφέρουν αυξημένους υπολογιστικούς πόρους, δυνατότητες και λειτουργίες στους χρήστες κινητών τηλεφώνων. Το MCC περιλαμβάνει κινητές επικοινωνίες, κινητό υλικό, κινητό λογισμικό, τεχνολογίες νέφους και δικτύου για τη χρήση διαφορετικών υπηρεσιών και δρομολόγηση και προώθηση πακέτων σε ετερογενή και κατανεμημένα περιβάλλοντα.

Τα ασύρματα ασύρματα ασύρματα δίκτυα και τα δίκτυα αισθητήρων που ορίζονται από το λογισμικό ενδέχεται να περιλαμβάνουν διάφορους κόμβους που διαδίδονται σε ολόκληρη την περιοχή. Οι νέοι κόμβοι μπορούν να συμμετέχουν / εγκαταλείπουν τα δίκτυα και μπορούν να συμμετέχουν στην επεξεργασία και προώθηση δεδομένων. Με βάση τις δυνατότητες των κόμβων, μπορούν να παρέχουν διαφορετικές υπηρεσίες επικοινωνίας (δηλαδή ασφάλεια, διατήρηση δεδομένων) και ταχύτητες. Τέλος, τα δίκτυα σώματος και οι τεχνολογίες ανταλλαγής πληροφοριών για την ηλεκτρονική υγεία χρησιμοποιούνται όλο και περισσότερο για να παρέχουν ή να έχουν πρόσβαση στα δεδομένα των αντικειμένων (δηλαδή στους ασθενείς, την παρακολούθηση του κέντρου περίθαλψης στο σπίτι και το ηλικιωμένο για χρόνιους και ηλικιωμένους ασθενείς). Τα χαρακτηριστικά αυτών των περιπτώσεων χρήσεων παρουσιάζονται στους παρακάτω πίνακες.

| **1.**Ultra Wideband (UWB) communication and applications | |
|---|---|
| ***1.1 Characteristics*** | Extremely low transmission energy (less than 1mW) |
| | Very high bandwidth within short range (200Mbps within 10m) |
| | Extremely difficult to intercept, because the frequency is constantly shifting |
| | The short duration of the UWB pulses lead to multipath immunity (i.e. the propagation path can be discovered due to the fine time resolution) |
| | Radar, Geo-location / Positioning |
| ***1.2 Applications*** | Wireless Personal Area Networks (WPAN) |
| | Positioning, geo-location, localization, rescue applications |
| | Radar / Sensor: MIR (motion detector, range-finder, etc.) |
| | Military and commercial: Asset protection |
| | Anti-terrorist, search-and-rescue activities, law enforcement and emergency rescue organizations |
| ***1.3 Guidelines, strategies and standardization*** | IEEE 802.15: WPAN |
| | IEEE 802.15.1: Bluetooth, 1Mbps |
| | IEEE 802.15.3: WPAN/high rate, 50Mbps |
| | IEEE 802.15.3a: WPAN/Higher rate, 200Mbps, UWB |
| ***1.4 Advantages*** | Easier to achieve higher data rate, because of the shorter duration of the UWB pulses |
| | Less path loss and better immunity to multipath propagation |
| | Availability of low-cost transceivers |
| | Low transmit power and low interference |
| | Extensive command set of the IEEE 802.15.4 (standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs)). FCC approved wireless protocol, supports communications with multiple devices, very fast communications. |
| ***1.5 Problems/issues to-be considered*** | Distortion of the received waveform from each distinct delayed propagation path, which makes it difficult to explore path diversity inherent in the received signal |
| | Synchronization of very short pulses at the receiver |
| | Performance degradation due to multiple access interference and narrowband jamming |
| | Employing higher order modulation schemes to improve capacity or throughput |
| | Development of link and network layers to take advantage of the UWB transmission benefits at the physical layer |

**Πίνακας 1. Ultra Wideband (UWB) communication and applications**

| **2.**Radio Frequency Identification (RFID) | |
|---|---|
| ***2.1 Characteristics*** | Low frequency (less than 100 MHz) and high frequency (greater than 100 MHz) modes |
| | High-frequency tags can have their data read at distances greater than one meter |
| | New data can also be transmitted to the tags, a process not shown here |
| ***2.2 Applications*** | Low/high frequency systems |
| | Supply chain and automated libraries |
| | Transport payment |
| | Automotive security |
| | Healthcare (e.g. track assets, monitor patients, automate payments) |
| ***2.3 Guidelines, strategies and standardization*** | ISO 11784: Data structure on the tag |
| | ISO 11785: Air interface protocol |
| | ISO 14443: Air interface protocol for RFID tags in payment systems & contactless smart cards |
| | ISO 15693: Air interface protocol for RFID tags in vicinity cards |
| | ISO 18046 & 18047: Testing the conformance of RFID tags and readers |
| ***2.4 Advantages*** | No line of sight (NLOS) |
| | Work in harsh environment (e.g. high temperatures) |
| | Cost effectiveness & high efficiency |
| | Reliable and fast identification of mobile tags in RFID networks |
| | Fast and energy efficient multi-sensor data retrieval approaches |
| ***2.5 Problems/issues to-be considered*** | Large volumes of data & product information maintenance |
| | Configuration and management of readers and devices |
| | Data integration across multiple facilities |
| | Data ownership and partner data integration |
| | Data security and personal privacy (e.g. patient *privacy* and dignity) |

**Πίνακας 2. Radio Frequency Identification (RFID)**

| **3.Mobile Cloud Computing and Mobile Social Networking** | |
|---|---|
| ***3.1 Characteristics*** | On-demand self-service (cloud computing users to manage their own virtual resources) |
| | Broad network and heterogeneous access |
| | Resource pooling; information can be shared with multiple users, who can access the resources anytime |
| | Rapid elasticity; the cloud must be able to scale up and down as load demands for IoT usage |
| | Measured service; subscription based or pay per use services |
| ***3.2 Applications*** | Web-browsing & web-mail |
| | Secure enterprise social networks that connects your business processes, enterprise applications, and content |
| | Augment reality; connect all objects through the Internet for remote sensing and control |
| | HD video streaming (e.g. cloud-based live video broadcasting network) |
| ***3.3 Guidelines, strategies and standardization*** | DTMF OGF GFD.183, DTMF OGF GFD.184 |
| | European cloud strategy, European data infrastructure |

| 3.Mobile Cloud Computing and Mobile Social Networking | |
|---|---|
| | SNIA Cloud Data Management Interface (CDMI) |
| | Federal Information Process Standards Publication (FIPS), standards for security categorization of federal information and information systems for effective management and oversight of information security and consistent reporting on the adequacy and effectiveness of information security policies, procedures, and practices |
| | ISO/IEC 17788:2014,<br>ISO/IEC 17789:2014,<br>ISO/IEC 17826:2012,<br>ISO/IEC DIS 19086-1,<br>ISO/IEC DIS NP 19086-2,<br>ISO/IEC DIS CD 19086-3,<br>ISO/IEC DIS NP 19086-4,<br>ISO/IEC AWI 19941,<br>ISO/IEC WD 19944,<br>ISO/IEC AWI 20889,<br>ETSI Cloud Computing standards and Open Source,<br>IEEE - P2301/P2302/ P2303,<br>Open group - G135/ C141 |
| ***3.4 Advantages*** | Flexibility; access the data from anywhere in the world, using any mobile device |
| | Scalability; ever-changing technology landscape |
| | Real time data availability; get access to real time data, whenever you want and wherever you want |
| | Multiple platforms; various platforms to access the data and applications stored in the cloud |
| | Increased resource availability, enhanced security and reliability, reduced long WAN latency, increased low-cost resources, green computing, streamlined work flow, ease of use and access |
| ***3.5 Problems/issues to-be considered*** | Security |
| | Performance |
| | No offline usability |
| | Connectivity |

**Πίνακας 3. Mobile Cloud Computing and Mobile Social Networking**

| 4.Software-defined ad-hoc and sensor networks | |
|---|---|
| ***4.1 Characteristics*** | Dynamic topologies, fixed nodes |
| | Bandwidth-constrained, variable capacity links |
| | Resources & energy-constrained |
| | Limited physical security, security threats |
| ***4.2 Applications*** | Virtual navigation, Location-aware services |
| | Tele-medicine, tele-geo processing |
| | VAN, PAN, home and enterprise networking, tactical networks, sensor networks |
| | Military applications, crisis-management applications, emergency services |
| | Educational applications, entertainment |
| | IEEE 802.11 Family |

| | |
|---|---|
| *4.3 Guidelines, strategies and standardization* | IEEE 802.15: WPAN<br>IEEE 802.15.1: Bluetooth<br>IEEE 802.15.3: WPAN/high rate, 50Mbps<br>IEEE 802.15.3a: WPAN/Higher rate, 200Mbps, UWB<br>IEEE 802.15.4: WPAN/low-rate, low-power, mW level, 200kbps |
| | IEEE 802.16 |
| | IEEE 802.20 |
| | IEEE 1451 |
| *4.4 Advantages* | Less cost, bigger and faster wireless networks |
| | Rely on same Wi-Fi standards |
| | Convenient where Ethernet connections fail, useful for Non-Line-of-Sight network configurations |
| | Allows local networks to run faster |
| | Adaptable networks, Self-configuring, Self-healing |
| *4.5 Problems/issues to-be considered* | Unstable data links, node cooperation, quality of service, scalability, limited wireless transmission range, packet losses due to transmission errors, Transport layer protocol performance |
| | Limited processing power, energy conservation |
| | Security, broadcast nature of the wireless medium, multicasting |
| | Interoperation with the Internet, client server model shift, pricing scheme |
| | Mobility-induced route changes, mobility-induced packet losses, potentially frequent network partitions |

**Πίνακας 4. Software-defined ad-hoc and sensor networks**

| **5.Body Networks and eHealth Applications** | |
|---|---|
| *5.1 Characteristics* | Completeness |
| | Integrity |
| | Accessibility |
| | Availability |
| *5.2 Applications* | Various telemedicine (remote diagnosis), electronic stethoscopes, Scientific and industrial applications (i.e. in medical imaging), applications of body network and eHealth |
| | Teaching applications are in use with different purposes, medical monitors, medical laboratory equipment |
| | Nuclear medicine with medical devices and wearable sensor-based systems |
| | Therapeutic: physical therapy machines like continuous passive range of motion (CPM) machine, Treatment equipment includes infusion pumps, medical lasers and LASIK surgical machines |
| | Life support equipment is used to maintain a patient's bodily function |
| *5.3 Guidelines, strategies and standardization* | HL7 MLLP, HITRUST CSF |
| | EU Directive 2011/24/EU (article 14), Regulation (EC) No 883/2004 |
| | Guidelines on minimum/non-exhaustive patient summary dataset |
| | National responsible authorities on eHealth (2011/890/EU) |
| | ISO/TR 28380 “Health Informatics – IHE Global Standards Adoption”,<br>ISO 27000,<br>ISO 27799:2008 Health Informatics, |

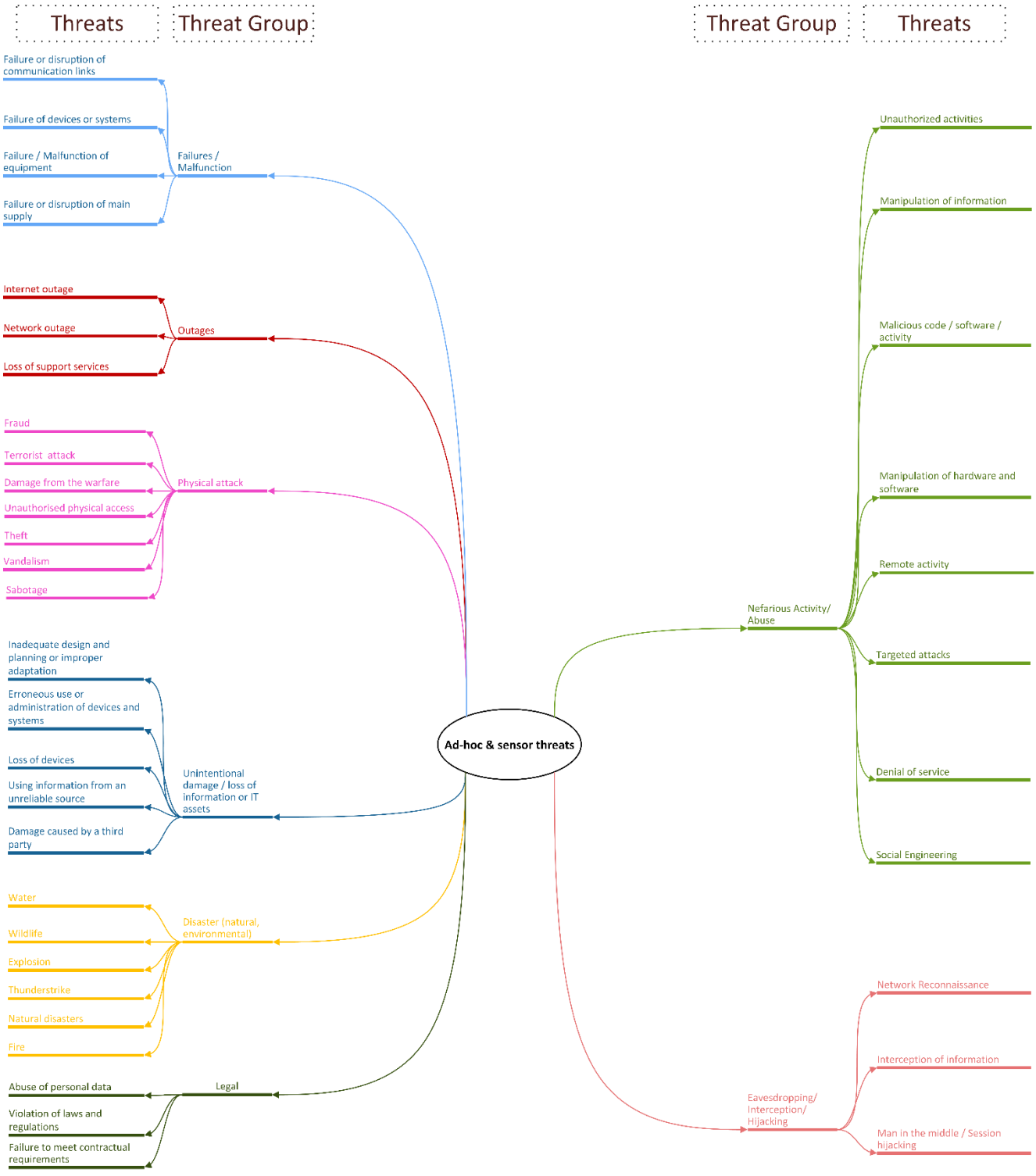
| 5.Body Networks and eHealth Applications | |
|---|---|
| | ISO 80001 |
| ***5.4 Advantages*** | Employers reduce health care costs; Health care organizations use eHealth to reach a large part of the population cost effectively |
| | Providers face eHealth as an opportunity to improve efficiency, reduce administrative costs, facilitate communication, enhance patient care |
| | Improved relationship between patients and insurance companies |
| ***5.5 Problems/issues to-be considered*** | Systems availability |
| | Lack of interoperability, cross-border incidents and incident management |
| | Access control and authentication |
| | Data integrity, network security, data loss, security expertise and awareness |
| | Standardisation, compliance, trust, and sensitiveness of data handled |

**Πίνακας 5. Body Networks and eHealth Applications**

# 4. Ταξινόμηση απειλών

Η ταξινόμηση απειλών είναι μια ταξινόμηση των τύπων απειλών και των ομάδων απειλών σε διάφορα επίπεδα λεπτομέρειας. Ο σκοπός μιας τέτοιας ταξινόμησης είναι να δημιουργηθεί ένα σημείο αναφοράς για τις συναντούμενες απειλές, παρέχοντας παράλληλα τη δυνατότητα ανακατάταξης, διευθέτησης, τροποποίησης και λεπτομερούς ορισμού των απειλών. Επομένως, μια ταξινόμηση απειλών είναι δυναμική και θα πρέπει να χρησιμοποιείται για να διατηρεί μια συνεπή αντίληψη για τις απειλές που βασίζονται στις πληροφορίες που συλλέγονται.

Ο σημερινός χαρτοφυλάκιο απειλών (Σχήμα 6) βασίζεται στην ταξινόμηση απειλών ENISA, η οποία συγκέντρωσε και συνδύασε πολυάριθμες απειλές από διάφορες πηγές σε ένα ενοποιημένο και ενωμένο κατάλογο απειλών. Στην τρέχουσα μελέτη εξετάσαμε επίσης τις απειλές στους τομείς των επιχειρησιακών τομέων και των τομέων προϊόντων / επιχειρηματικών διαδικασιών που επικεντρώθηκε σε φυσικές απειλές, την ασφάλεια των πληροφοριών και τις περιοχές του κυβερνοχώρου.


Threats
Threat Group
Threat Group
Threats
Failure or disruption of communication links
Failure of devices or systems
Failure / Malfunction of equipment
Failure or disruption of main supply
Failures / Malfunction
Internet outage
Network outage
Loss of support services
Outages
Fraud
Terrorist attack
Damage from the warfare
Unauthorised physical access
Theft
Vandalism
Sabotage
Physical attack
Inadequate design and planning or improper adaptation
Erroneous use or administration of devices and systems
Loss of devices
Using information from an unreliable source
Damage caused by a third party
Unintentional damage / loss of information or IT assets
Water
Wildlife
Explosion
Thunderstrike
Natural disasters
Fire
Disaster (natural, environmental)
Abuse of personal data
Violation of laws and regulations
Failure to meet contractual requirements
Legal
Ad-hoc & sensor threats
Nefarious Activity/ Abuse
Unauthorized activities
Manipulation of information
Malicious code / software / activity
Manipulation of hardware and software
Remote activity
Targeted attacks
Denial of service
Social Engineering
Eavesdropping/ Interception/ Hijacking
Network Reconnaissance
Interception of information
Man in the middle / Session hijacking

**Σχήμα 6**

# 5. Χαρτογράφηση απειλών για στοιχεία ενεργητικού

Σύμφωνα με το λεξιλόγιο του ENISA, μια απειλή είναι *«οποιαδήποτε περίσταση ή γεγονός με πιθανότητα να επηρεάσει δυσμενώς ένα περιουσιακό στοιχείο μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης δεδομένων ή / και άρνησης παροχής υπηρεσίας»*.

Με βάση τα προσδιορισμένα περιουσιακά στοιχεία, αναπτύσσεται μια ταξινόμηση σχετικών απειλών που παρεμποδίζουν τα δίκτυα ad-hoc αισθητήρων ή τουλάχιστον σημαντικά τμήματα.

Δεδομένου ότι η μελέτη αυτή επικεντρώνεται στην ασφάλεια των πληροφοριών, η παρουσιαζόμενη ταξινόμηση απειλών καλύπτει κυρίως απειλές για την ασφάλεια στον κυβερνοχώρο. Ωστόσο, για μια άψογη λειτουργία απαιτούνται επίσης φυσικά περιουσιακά στοιχεία και, κατά συνέπεια, λαμβάνονται διάφορες συγκεκριμένες απειλές για μη ΤΠ.

## 5.1. Ομάδα απειλών: Αθέλητη ζημία / απώλεια πληροφοριών ή περιουσιακών στοιχείων της τεχνολογίας της πληροφορίας

Η ακόλουθη ομάδα απειλών αναφέρεται σε εκείνες τις βλάβες ή απώλεια πληροφοριών που προκαλούνται από ανθρώπινα σφάλματα στη διαχείριση συστημάτων ή λανθασμένη διαμόρφωση των συστημάτων. Επιπλέον, αυτές οι ζημιές μπορούν να προκληθούν από μια ακούσια επέμβαση ή από την πραγματική απώλεια των συσκευών ή μέρος αυτών.

### 5.1.1. Απειλή: Ανεπαρκής σχεδιασμός και προγραμματισμός ακατάλληλης προσαρμογής

Το πεδίο του σχεδιασμού και του σχεδιασμού δικτύων αισθητήρων είναι η καλύτερη κάλυψη της περιοχής κατά τρόπο που να επιτρέπει την αδεσπότη πρόσβαση μεταξύ των τελικών χρηστών (π.χ. μια εφαρμογή, μια επιχειρηματική διαδικασία) και τα πρωταρχικά δεδομένα που συλλέγονται από την ελεγχόμενη ή ελεγχόμενη περιοχή. Οποιοδήποτε σφάλμα ή έλλειψη προσοχής στο σχεδιασμό μπορεί να προκαλέσει χαμηλή διαθεσιμότητα ή χρόνο διακοπής λειτουργίας και κατανάλωση πόρων.

Δίκτυα ad-hoc συνεχώς Τσανγκ Ε αρχιτεκτονική, που οφείλεται στον κόμβο κινητικότητα. Η βάση επικοινωνίας τους είναι η μετάδοση μεταξύ γειτονικών κόμβων. Η έλλειψη του κατάλληλου σχεδιασμού θα μπορούσε να οδηγήσει σε δίκτυο αστάθειας και των πόρων πάνω - η κατανάλωση σε κάθε αλλαγή του αριθμού των συμμετεχόντων (κόμβων).

Το γεγονός ότι τα περιουσιακά στοιχεία του δικτύου ad-hoc και του αισθητήρα έχουν περιορισμένες ή μη υπολογιστικές ικανότητες και χαμηλά μέσα είναι ένας παράγοντας της συμπεριφοράς τους. Ένας άλλος παράγοντας είναι ότι το περιβάλλον ή η περιοχή που στοχεύει να παρακολουθείται σε κάθε περίπτωση θα μπορούσε να είναι εχθρική, ανοικτή σε μη επιτηρούμενη ή μη εξουσιοδοτημένη πρόσβαση, συνεχώς μεταβαλλόμενη (λόγω κινητικότητας) και γεωγραφικά ευρεία ένας ανεπαρκής σχεδιασμός θα μπορούσε να οδηγήσει στην ακατάλληλη ή ανεπαρκή κάλυψη της περιοχής, στην κακή επικοινωνία των περιουσιακών στοιχείων ή στην εξάντληση των πόρων των περιουσιακών στοιχείων, προσπαθώντας να υπερνικήσει τα προβλήματα σχεδιασμού.

Τα δεδομένα που συλλέγονται και διαβιβάζονται σε αυτά τα δίκτυα είναι μεγάλης αξίας και ευαισθησίας (π.χ. Ιδιωτικές πληροφορίες για την υγειονομική περίθαλψη - PHI). Ωστόσο, η χαμηλή υπολογιστική ισχύς των στοιχείων

ενεργητικού καθιστά δύσκολη ή αδύνατη την προστασία των δεδομένων και της ίδιας της μετάδοσης δεδομένων. Μια μέθοδος προστασίας δεδομένων μέσω κρυπτογράφησης και αποκρυπτογράφησης, αν και συναισθηματική, είναι ιδιαίτερα απαιτητική στους υπολογιστικούς πόρους. Ένας ανεπαρκής σχεδιασμός του τρόπου αντιμετώπισης αυτού του προβλήματος μπορεί να επιτρέψει την υπονόμευση των πληροφοριών.

Πέραν των παραπάνω, η έλλειψη σχεδιασμού ή η ύπαρξη σφάλματος σχεδίου μπορεί να επιτρέψει την ύπαρξη λογισμικού (Εφαρμογές) που δεν λαμβάνει υπόψη τους περιορισμούς ισχύος και υπολογισμών των συσκευών.

Περιουσιακά στοιχεία στόχαστρο αυτής της ομάδας απειλή είναι εκείνοι από τη ***συσκευή Τομέα*** και των ***δεδομένων*** του ενεργητικού στον ***τομέα*** της ***εφαρμογής.***

### 5.1.2. Απειλή: Χρήση πληροφοριών από μια αναξιόπιστη πηγή

Οποιοδήποτε σύστημα ή συσκευή με υπολογιστική ισχύ και λειτουργικό σύστημα (OS) είναι ευάλωτα σε εκμεταλλεύσεις OS. Αυτή η απειλή οφείλεται κυρίως στις ευάλωτες εκδόσεις του προεγκατεστημένου λογισμικού που χρησιμοποιείται σε εταιρικά περιβάλλοντα. Στις περισσότερες περιπτώσεις, *οι εφαρμογές τρίτων* μπορούν να εγκατασταθούν και να ενεργοποιηθούν στις συσκευές, pos σης πιθανούς κινδύνους για την επιχείρηση. Αυτές οι εφαρμογές ενδέχεται να κρύψουν διάφορα σφάλματα λογισμικού, σφάλματα ασφαλείας, τρωτά σημεία και σφάλματα κωδικοποίησης που μπορούν να χρησιμοποιηθούν σε αντίπαλο υπό ορισμένες συνθήκες. Πρόκειται για μια μη σκόπιμη απειλή, επειδή το λογισμικό και οι κίνδυνοι εφαρμογών θα μπορούσαν να υπάρχουν από το σχεδιασμό.

Όπως αναφέρθηκε στην μελέτη IBM X-Force Threat Intelligence, τα γεγονότα στον κυβερνοχώρο δείχνουν αυξανόμενο ενδιαφέρον για στοιχεία προσωπικής ταυτοποίησης (PII) και δεδομένα υψηλής αξίας (π.χ. αρχεία υγείας) από το 2014. Εκτός αυτού, στην περίπτωση κρίσιμων για τις επιχειρήσεις εφαρμογών (π.χ. τιμολόγηση, ηλεκτρονική υγεία), ευαίσθητα και προσωπικά μπορεί να διασχίσουν ad-hoc και δίκτυα αισθητήρων. Επομένως, αυτά τα δίκτυα είναι επιρρεπή σε επιθέσεις και κακόβουλες δραστηριότητες.

Όλα τα στοιχεία ενεργητικού σε ***όλους τους τομείς*** μπορούν να αποτελέσουν στόχο για αυτήν την απειλή.

### 5.1.3. Απειλή: Εσφαλμένη χρήση ή διαχείριση συσκευών και συστημάτων

Οι διασυνδέσεις προγραμματισμού εφαρμογών (API) είναι στοιχεία λογισμικού, τα οποία χρησιμοποιούνται από προγραμματιστές λογισμικού στην προσπάθειά τους να κατασκευάσουν εφαρμογές ή γραφικές διεπαφές χρήστη. Οι πάροχοι υπηρεσιών Cloud χρησιμοποιούν API για να επιτρέψουν την πρόσβαση σε υπηρεσίες που βασίζονται σε cloud. Τα API μπορούν να χρησιμοποιηθούν ταυτόχρονα από διάφορες συσκευές και εφαρμογές για διάφορους σκοπούς. Ωστόσο, είναι δύσκολο να καθοριστεί ποιος πρέπει ή δεν πρέπει να έχει πρόσβαση. Από ένα API είναι μια δημόσια βιβλιοθήκη, η μη εξουσιοδοτημένη πρόσβαση και φαύλους χρήση του περιεχομένου APIs δεν μπορεί να προληφθεί εύκολα. Πρέπει να σημειωθεί ότι σε αυτή την πρόσβαση, οποιαδήποτε δεδομένα, σύστημα ή υπηρεσία του δικτύου γίνεται ευάλωτα.

Στην περίπτωση του API δικαιώματα, το οποίο περιέχει πληροφορίες ενημέρωσης και πρόσβασης για συστήματα στο δίκτυο, τ αντίπαλος μπορεί να εκτελέσει μια μη εξουσιοδοτημένη χειραγώγηση του API, και να χρησιμοποιούν λανθασμένα τις συσκευές και τα συστήματα.

Όλα τα στοιχεία ενεργητικού σε ***όλους τους τομείς*** μπορούν να αποτελέσουν στόχο για αυτήν την απειλή.

### 5.1.4. Απειλή: Απώλεια συσκευών

Σε δίκτυα ad-hoc και αισθητήρων, η απειλή απώλειας συσκευών μπορεί να επηρεάσει τη σταθερότητα του δικτύου. Στις περισσότερες περιπτώσεις, οι περιοχές που έχουν σχεδιαστεί να καλύψουν τα δίκτυα αισθητήρων είναι γεωγραφικά ευρείες. Καθώς ο κίνδυνος είναι πολύ υψηλός, αυτό οδηγεί στη χρήση ενός μεγάλου αριθμού των συσκευών να επιτύχει επαρκή κάλυψη της περιοχής. Αυτές οι περιοχές (π.χ. υποβρύχια, υπόγεια, χερσαία κ.λπ.) θα μπορούσαν επίσης να παρέχουν ανοικτή πρόσβαση σε οποιονδήποτε. Επιπλέον, οι κόμβοι του δικτύου είναι κυρίως συσκευές μικρού μεγέθους. αυτό το χαρακτηριστικό τους καθιστά ευάλωτους σε επεισόδια ληστειών.

Περαιτέρω σε ad-hoc δίκτυα, η καλυμμένη περιοχή είναι απροσδιόριστη και μπορεί να αλλάξει σε πραγματικό χρόνο. Ο αριθμός των συσκευών αλλάζει συνεχώς. Εκτός από τα παραπάνω, οι κόμβοι είναι συνήθως μικρές συσκευές (π.χ. κινητά τηλέφωνα, PDA, έξυπνες κάρτες, RFID κλπ.), Οι οποίες είναι εύκολο να κλαπούν και περιέχουν ευαίσθητες ή προσωπικές πληροφορίες.

Αυτά τα χαρακτηριστικά καθιστούν τα ad-hoc και αισθητήρα δίκτυα και, πιο συγκεκριμένα, τα περιουσιακά στοιχεία του ***Device Domain*** ευάλωτα σε απειλή απώλειας συσκευών.

### 5.1.5. Απειλή: Ζημιές από τρίτους

Σε ορισμένες περιπτώσεις, ένα *κακόβουλο λογισμικό* είναι ένα εχθρικό κομμάτι του κώδικα προγραμματισμού που στοχεύει ευαίσθητες πληροφορίες μέσα σε ένα σύστημα. Για παράδειγμα, ο όρος "*κακόβουλο λογισμικό κακόβουλης πληροφορίας*" περιγράφει το κακόβουλο λογισμικό που αποκτά πρόσβαση από απόσταση σε ένα σύστημα και επικεντρώνεται στη συλλογή πληροφοριών όταν εγκαθίσταται με κύριο σκοπό τη στοχοθετημένη διαφήμιση.

*Η διαρροή δεδομένων* είναι το παράνομο αποτέλεσμα που παράγεται από μια εφαρμογή τρίτου μέρους που εστιάζεται στη συλλογή προσωπικών πληροφοριών λόγω της ύπαρξης κρίσιμων τρωτών σημείων ή ενσωματωμένων παρασκηνών στον πηγαίο κώδικα των εφαρμογών. Κατά συνέπεια, οι πληροφορίες χρησιμοποιούνται στη συνέχεια χωρίς την άδεια του ιδιοκτήτη για πολλές κακόβουλες δραστηριότητες, όπως η έκθεση στην *μαύρη αγορά*. Τα εν λόγω δεδομένα σχετίζονται με το προφίλ της αγοράς του πελάτη.

Το ενεργητικό που στοχεύει αυτή η απειλή είναι τα ***Δεδομένα Τομέας*** από τον ***τομέα εφαρμογής***.

## 5.2. Ομάδα απειλών: Καταστροφή (φυσική, περιβαλλοντική)

Προφανώς, οι φυσικές και περιβαλλοντικές καταστροφές προκαλούν σοβαρές διαταραχές δικτύου και υπηρεσιών μεγάλης κλίμακας και έχουν κατά μέσο όρο τη μεγαλύτερη επίδραση σε όλες τις αποτυχίες του συστήματος. Η ανάκτηση και η αποκατάσταση των υπηρεσιών διαρκεί το μεγαλύτερο χρονικό διάστημα. το 2014 ο χρόνος ανάκτησης διήρκεσε 81 ώρες, ενώ το 2013 ήταν πάνω από 50 ώρες. Λαμβάνοντας υπόψη την μεγάλη έκθεση στους πολυάριθμους χρήστες και τους κατοίκους, αυτό καταδεικνύει ότι οι καταστροφές όχι μόνο διαρκούν πολύ, αλλά και είναι οι πιο δύσκολες για τη διαχείριση.

Σήμερα παρατηρούμε έναν αυξημένο αριθμό συνδεδεμένων αισθητήρων, που ενσωματώνονται στην υποδομή και τα κτίρια και ενσωματώνονται σε διάφορα συστήματα και υπηρεσίες. Αυτοί οι αισθητήρες μπορούν να παρακολουθούνται και να ελέγχονται με διάφορα μέσα (π.χ. έξυπνα τηλέφωνα, σταθμοί εργασίας μέσω του Διαδικτύου) και αποκαλύπτουν συμπεριφορικά πρότυπα των αντικειμένων που παρακολουθούνται. Συνεπώς, είναι σημαντικό να διασφαλιστεί η ακεραιότητα των δεδομένων και οι λειτουργίες εξυπηρέτησης των WSN έναντι οιασδήποτε φυσικής ή περιβαλλοντικής καταστροφής. Στα ad-hoc ασύρματα δίκτυα και τους αισθητήρες, οι κόμβοι της υποδομής συχνά καθορίζονται και σε πολλές περιπτώσεις οι WSNs χρησιμοποιούνται στις υπηρεσίες παρακολούθησης και ασφάλειας (δηλαδή παρακολουθούν τις ανθρώπινες δραστηριότητες και το περιβάλλον όπως ο έλεγχος του κλίματος, συγκεντρώνουν δεδομένα για ιατρική διάγνωση, δεδομένα κρίσιμης αποστολής και εμπιστευτικές μετρήσεις, παρέχουν τις πληροφορίες θέσης στον αντίστοιχο δέκτη). Παρόλα αυτά, τα WSNs χρησιμοποιούνται επίσης από τα συστήματα διαχείρισης και αντιμετώπισης καταστάσεων έκτακτης ανάγκης και έκτακτης ανάγκης για άμεση εξαγωγή συμπερασμάτων σχετικά με τις διαταραχές δικτύου και υπηρεσιών. Οι αισθητήριες μετρήσεις συλλέγονται σε τακτική βάση από χωρικά διασκορπισμένα δίκτυα που διανέμονται σε μια συγκεκριμένη περιοχή. Έτσι, τα WSNs μπορούν να ενισχύσουν την επιτήρηση και την ευαισθητοποίηση σχετικά με τυχόν αλλαγές στην κατάσταση των απαντήσεων σε καταστροφές και να αποτρέψουν τις τεράστιες καταστροφές από φυσικές ή περιβαλλοντικές καταστροφές.

Παρ 'όλα αυτά, οι ασύρματα δίκτυα αισθητήρων είναι επιρρεπή σε m οποιοδήποτε φυσικό ή περιβαλλοντική καταστροφή s, όπως και κάθε άλλο συστατικό ή δίκτυο. Είναι ευάλωτοι στις αποτυχίες και τις περικοπές ρεύματος, προβλήματα επικοινωνίας και καθυστερήσεις, σφάλματα εμπλοκής και καναλιών, προβλήματα υλικού, φυσικές ζημιές, μη ασφαλής δρομολόγηση και αποτυχίες στη συγκέντρωση δεδομένων.

Η εκτίμηση του αντίκτυπου των φυσικών και περιβαλλοντικών καταστροφών είναι υψίστης σημασίας και θα διευκολύνει τον εντοπισμό των παραγόντων και μεθόδων που μπορούν να συμβάλουν στη μείωση των ζημιών και των διαταραχών των υπηρεσιών μετά από φυσικές καταστροφές.

Τα στοιχεία ενεργητικού που στοχεύουν αυτή η απειλή περιλαμβάνουν τα στοιχεία ενεργητικού από τον ***τομέα*** της ***Συσκευής***, τον ***τομέα*** του ***Δικτύου*** και τα ***συστήματα ελέγχου*** ενεργητικού, τη ***φυσική ασφάλεια***, τις ***μηχανές αυτόματης πώλησης*** και την ***οδική ασφάλεια***.

## 5.3. Ομάδα απειλών: Νομική

Αυτή η ομάδα περιλαμβάνει απειλές λόγω των νομικών συνεπειών όπως η παραβίαση νόμων ή κανονισμών, η παραβίαση της νομοθεσίας, η μη τήρηση των συμβατικών απαιτήσεων, η μη εξουσιοδοτημένη χρήση πόρων πνευματικής ιδιοκτησίας, η κατάχρηση προσωπικών δεδομένων και η αναγκαιότητα να υπακούει σε αποφάσεις δικαστικών και δικαστικών αποφάσεων.

### 5.3.1. Απειλή: Κατάχρηση προσωπικών δεδομένων

Η ενσωμάτωση ασύρματων δικτύων αισθητήρων σώματος (WBSN), εξατομικευμένων φορητών συσκευών (PPD) και ασύρματων δικτύων σώματος (WBAN) στον τομέα της υγείας για τη βελτιστοποίηση της ποιότητας των ιατρικών υπηρεσιών και της θεραπείας των ασθενών να εισαγάγει πολλά ζητήματα απορρήτου και δεοντολογίας. Αυτά τα ζητήματα συνδέονται άκρως με την επιφάνεια προσβολής των αισθητήρων eHealth και pHealth. Οι αισθητήρες ad

hoc και ασύρματου δικτύου ενδέχεται να αντιμετωπίσουν δύσκολες και ανώμαλες φυσιολογικές συνθήκες στην απομακρυσμένη παρακολούθηση, οι οποίες απαιτούν την συνεχή παρακολούθηση για την παροχή εντατικής φροντίδας. Οι λειτουργίες και η συγκέντρωση δεδομένων από τους ιατρικούς αισθητήρες, όπως στην περίπτωση του συστήματος καρδιοδιατάξεων, πρέπει να διαχειρίζονται οι γιατροί και ο βρεφονηπιακός σταθμός. Κατά την παραλαβή των δεδομένων, οι αισθητήρες αποστέλλουν τα δεδομένα στον διακομιστή back-end για επεξεργασία χρησιμοποιώντας ένα ασύρματο δίκτυο μικρής εμβέλειας. Ωστόσο, κατά τη διάρκεια αυτής της διαδικασίας, τα WBAN απειλούνται κυρίως από εξαντλητικές επιθέσεις, οι οποίες είναι: *(α)* οι επιθέσεις σύγκρουσης, *(β)* η άρνηση των επιθέσεων ύπνου και *(γ)* οι εγωιστικές επιθέσεις.

Στο πεδίο των δικτύων κινητής Υγείας (MHNs), όπου επικοινωνούν wearable συσκευές αισθητήρων που βασίζονται στην έννοια της συσκευής προς συσκευή (D2D), η προστασία της AEA παίζει σημαντικό ρόλο. Ως εκ τούτου, εάν η PII (π.χ. ημερήσια στοιχεία για την υγεία του ασθενούς) υποβάλλονται σε επεξεργασία στο Cloud, θα πρέπει να προστατεύονται από την πρόσβαση από μια ασφαλιστική εταιρεία ή η έκθεση με ένα κινητό εισβολέας που μπορεί να διαδώσει τα αρχεία της υγείας μέσω ενός online κοινωνικό δίκτυο. Με αυτό τον τρόπο, η ποιότητα της ιδιωτικής ζωής (QoP) έχει μεγάλη σημασία.

Οι ευαίσθητες τραπεζικές πληροφορίες μπορούν να ανακτηθούν με κακόβουλο τρόπο στην περίπτωση καρτών επικοινωνίας κοντά στο πεδίο (NFC). Ο επιτιθέμενος μπορεί να χρησιμοποιήσει ραδιοκύματα NFC και στη συνέχεια να έχει πρόσβαση σε δεδομένα που είναι αποθηκευμένα στην κάρτα του θύματος.

Επιπλέον, η απάτη κοινωνικής μηχανικής μπορεί επίσης να είναι ένας τρόπος κατάχρησης των προσωπικών δεδομένων σε ad-hoc ή κινητά δίκτυα.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τη ***Τομέα*** ομάδες περιουσιακών στοιχείων ***Εφαρμογές*** και ***συσκευών τομέα*** και τα περιουσιακά στοιχεία ***Φυσική Ασφάλεια, Προμήθεια και Provisioning*** και ***Υγείας.***

### 5.3.2. Απειλή: Παραβίαση κανόνων και κανονισμών

Η τεράστια διασπορά αναπτυγμένων εφαρμογών στο οικοσύστημα ad-hoc και αισθητήρα δικτύωσης υπογραμμίζει την ανάγκη συμμόρφωσης με τους κανόνες και τους κανονισμούς που βασίζονται σε αυτές τις εφαρμογές καθώς και στην ευημερία της κοινωνίας. Οι ενδιαφερόμενοι που είναι επιρρεπείς στην παραβίαση των κανόνων είναι: *α)* οι φορείς εκμετάλλευσης (δηλαδή οι οποίοι συνδέονται άμεσα με τη φυσική υποδομή) και *β)* οι πάροχοι ψηφιακών υπηρεσιών (που έχουν διασυνοριακό χαρακτήρα).

Τα στοιχεία ενεργητικού που στοχεύουν αυτές οι απειλές περιλαμβάνουν τις ομάδες περιουσιακών στοιχείων ***Εφαρμογή τομέα, Συσκευή τομέα, Δίκτυο τομέα, Επιχειρησιακό Τομέα*** και ***προϊόντων / επιχειρηματικές διαδικασίες τομέα.***

## 5.4. Ομάδα απειλών: Διακοπές

Λόγω της φύσης των ad-hoc ασύρματων δικτύων και δικτύων αισθητήρων, υπάρχουν συγκεκριμένοι περιορισμοί. Εκτός από την περιορισμένη χωρητικότητα αποθήκευσης και υπολογιστικής δαπάνες, η κατανάλωση ενέργειας είναι μεταξύ των κρίσιμων παραγόντων επιτυχίας και σημαντικό εμπόδιο s για ad-hoc και αισθητήρα δίκτυα.

### 5.4.1. Απειλή: Διακοπή Διαδικτύου

Δεν πρέπει να υποτιμούμε τη μεγάλη σημασία των αποδείξεων για τις αναφορές και τα περιστατικά *διακοπής* του *διαδικτύου*, καθώς στις σημερινές επιχειρήσεις που εξαρτώνται σε μεγάλο βαθμό από το διαδίκτυο εξαρτώνται εκτενώς από τις υπηρεσίες Διαδικτύου και, κατά συνέπεια, οποιαδήποτε διακοπή του Διαδικτύου ενδέχεται να πλήξει σοβαρά τις επιχειρηματικές δραστηριότητες. Παρόλο που οι περισσότερες επιχειρήσεις έχουν ορίσει τις διαδικασίες και τα αντίμετρα για την αντιμετώπιση των διακοπών του Διαδικτύου, εξακολουθούν να υπάρχουν πολλές πολύπλοκες εξαρτήσεις, προβλήματα δυναμικότητας, καθυστερήσεις επιδόσεων και κίνδυνοι συνέχισης της λειτουργίας στην περίπτωση αποτυχιών στο Διαδίκτυο. Η διακοπή του Διαδικτύου μπορεί να προκληθεί από πολλούς παράγοντες είτε τυχαία είτε εκ προθέσεως. ανθρώπινα λάθη, προβληματικά και λανθασμένα έργα συντήρησης, κακή διαμόρφωση του BGP και μαζικές διαρροές διαδρομής, αποτυχημένο διεθνές καλώδιο που επηρεάζει εσωτερικές λειτουργίες κινητής τηλεφωνίας και δεδομένων και κίνδυνοι στον κυβερνοχώρο και κυβερνοεπαγγελματικά προβλήματα. Δεν είναι μόνο οι διακοπές παροχής υπηρεσιών βλάψει το εμπορικό σήμα του παρόχου υπηρεσιών, αλλά επίσης να δημιουργήσει πολλές επιχειρηματικές επιπτώσεις και απογοήτευση για τους χρήστες.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τις ομάδες περιουσιακών στοιχείων ***Αίτηση τομέα, Συσκευή τομέα, Δίκτυο τομέα, Επιχειρησιακό Τομέα*** και ***προϊόντων / επιχειρηματικές διαδικασίες τομέα.***

### 5.4.2. Απειλή: Διακοπή δικτύου

Ένας εισβολέας μπορεί να προσπαθήσει να εξαντλήσει την υποδομή δικτύου και τους πόρους υπηρεσίας υποβάλλοντας παράνομες αιτήσεις, μέχρι να επιτευχθεί το μέγιστο όριο. Αυτό έχει ως αποτέλεσμα την διακοπή λειτουργίας και τις διακοπές λειτουργίας, δεδομένου ότι κανένα άλλο νόμιμο αίτημα δεν μπορεί να λάβει περαιτέρω πόρους. Με την έγχυση μη έγκυρων αιτημάτων, οι πόροι εξαντλούνται και αυτό προκαλεί επιθέσεις άρνησης παροχής υπηρεσιών.

Ένα κοινό παράδειγμα διακοπής δικτύου είναι η *διακοπή των καλωδιακών δικτύων*. Εάν τα καλώδια τροφοδοσίας ή δικτύου είναι απροστάτευτα, μπορεί να καταστραφούν τυχαία ή σκόπιμα. Συχνά, τα καλώδια αποσύρονται από το προσωπικό καθώς σκοντάφτουν πάνω τους, το μη εξουσιοδοτημένο προσωπικό (δηλαδή υπηρεσίες καθαρισμού) αποσυνδέει το καλώδιο και συνδέει το χαλαρό άκρο σε μια κενή «τρύπα» που φαίνεται να ταιριάζει ή η σύνδεση καλωδίου τερματίζεται απότομα ( δηλαδή μια άγκυρα πλοίου φέρεται τυχαία καλώδια διαδικτύου). Η μη διαθεσιμότητα και η *απώλεια υπηρεσιών υποστήριξης που είναι* απαραίτητες για την ορθή λειτουργία του συστήματος πληροφοριών και των επιχειρηματικών διαδικασιών προκαλούν συχνά διαταραχές και διακοπές.

Διαλείποντα προβλήματα και *διακοπές σε ασύρματα δίκτυα* περιβάλλον ενδέχεται επίσης να οφείλονται σε τεχνικές εκμεταλλεύσεις και ευπάθειες (π.χ. οικογένειες IEEE 802.11 και IEEE 802.15). Σε περίπτωση *διακοπών των δικτύων κινητής τηλεφωνίας*, εκτός από τα προβλήματα επικοινωνίας με τα δίκτυα (π.χ. 3G, GSM, LTE, δορυφορικές συνδέσεις), μπορεί να προκύψουν διάφορα λειτουργικά και επιχειρηματικά ζητήματα που έχουν ως αποτέλεσμα διακοπές λειτουργίας και διακοπές. Η αφερεγγυότητα, οι χρηματοπιστωτικές αστάθειες, τα θέματα του υπεργολάβου, οι συνέπειες της ανάθεσης σε εξωτερικούς συνεργάτες, οι δυσκολίες στις συμβατικές ρυθμίσεις είναι λίγοι τυπικοί λόγοι για τους οποίους οι πάροχοι υπηρεσιών ενδέχεται να μην ανταποκριθούν στην προσδοκώμενη ποιότητα των υπηρεσιών και να οδηγήσουν σε δυσλειτουργίες. Επιπλέον, οι επιχειρηματικές

διαδικασίες ενδέχεται να αποτύχουν λόγω κακής ευθυγράμμισης και ακατάλληλης επικοινωνίας με τον πάροχο υπηρεσιών ή ακόμη και λόγω ανεπαρκώς τεκμηριωμένων διαδικασιών.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τις ομάδες περιουσιακών στοιχείων ***Αίτηση τομέα, Συσκευή τομέα, Δίκτυο τομέα, επιχειρησιακό πεδίο,*** και το ***προϊόν / επιχειρηματικές διαδικασίες τομέα.***

### 5.4.3. Απειλή: Απώλεια υπηρεσιών υποστήριξης

Ένα άλλο χαρακτηριστικό παράδειγμα διακοπής είναι η ανυπαρξία των απαραίτητων υπηρεσιών υποστήριξης, οι οποίες. απαιτούνται για τη σωστή λειτουργία των δικτύων και των συστημάτων.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τις ομάδες περιουσιακών στοιχείων ***Αίτηση τομέα, Συσκευή τομέα, Δίκτυο τομέα, επιχειρησιακό πεδίο,*** και το ***προϊόν / επιχειρηματικές διαδικασίες τομέα.***

## 5.5. Ομάδα απειλών: Επηρεασμένη δραστηριότητα / κατάχρηση

Το γεγονός ότι η βάση ad-hoc και των δικτύων αισθητήρων είναι μια ομάδα συσκευών με χαμηλή ή καθόλου αποθήκευση δεδομένων και αυτονομία χαμηλής ισχύος καθιστά αυτά τα δίκτυα ευάλωτα σε επιθέσεις κατά της φρικτής δραστηριότητας. Αυτή η ομάδα επιθέσεων περιλαμβάνει αθέμιτα δημιουργούμενες απειλές με στόχο την υποδομή.

### 5.5.1. Απειλή: Άρνηση παροχής υπηρεσιών

Σε αυτό το πλαίσιο, τα δίκτυα ad-hoc και αισθητήρων υποφέρουν από επιθέσεις παραδοσιακής άρνησης παροχής υπηρεσιών (DoS), όπως αυτές παρατηρούνται σε άλλα δίκτυα δεδομένων και επικοινωνιών. Τα δίκτυα αισθητήρων ικανοποιούνται σε περιβάλλοντα κρίσιμης ανάπτυξης, όπως τα συστήματα υγειονομικής περίθαλψης. Έτσι, οι επιθέσεις DoS και κατανεμημένων DoS (DDoS) έχουν μεγάλη σημασία να μετριαστούν με την έγκαιρη ανίχνευσή τους. Σε περιβάλλον υποβοηθούμενης διαβίωσης (AAL), ειδικά σε περιβάλλοντα ηλεκτρονικής υγείας, ο πολλαπλός χαρακτήρας των ασύρματων δικτύων ματιών (WMN) είναι ευάλωτος έναντι ανεπιθύμητης επαναδρομολόγησης. Επομένως, μια τέτοια κατάσταση επίθεσης DoS (π.χ. hello flooding) μπορεί να υπονομευθεί με τη χρήση ανθεκτικών πρωτοκόλλων δρομολόγησης. Παρόλο που υπάρχουν πολλά διαφορετικά χαρακτηριστικά μεταξύ των WSNs και των MANETs και αρκετές συγκεκριμένες επιθέσεις που απευθύνονται σε κάθε τύπο αυτών των δικτύων, είναι και οι δύο επιρρεπείς σε επιθέσεις κακόβουλου κόμβου και δρομολόγησης. Για παράδειγμα, σε μια *επίθεση κατά των πλημμυρών*, ο επιτιθέμενος προσπαθεί να στραγγίξει τους πόρους του θύματος αποστέλλοντας από μακριά πολυάριθμες αιτήσεις εγκατάστασης σύνδεσης. Σε ένα σύστημα βασισμένο σε νέφος, το οποίο θα μπορούσε να αποτελέσει βασικό στοιχείο μιας λύσης IoT, αυτό το είδος επίθεσης επηρεάζει σοβαρά τον Autonomic Manager, ο οποίος είναι ο φορέας ελέγχου και αυτόματης ρύθμισης των απαραίτητων αλλαγών στον κύκλο ζωής του συστήματος.

Ωστόσο, υπάρχουν πολλές αμφισημίες για το πώς μπορούμε θεωρητικά να ορίσουμε μια επίθεση DoS σε ad-hoc και δίκτυα αισθητήρων. Παρ 'όλα αυτά, οι αναδυόμενες ερευνητικό έργο έχει επιμ illustrat τυπικές μεθόδους που καθορίζουν προφανώς μια τέτοια κατάσταση επίθεσης.

Οι επιθέσεις DoS προκαλούνται κυρίως από: *(α)* την παραγωγή κυμαινόταν επιδράσεις σε διάφορα επίπεδα OSI επί του στόχου (δηλ *Slowloris), (β)* τεχνικές ενίσχυσης / ανάκλαση (δηλ DNS και ενίσχυση NTP, αλλαγή ανάκλασης) και *(γ)* μηχανισμούς πλημμύρες (π.χ. ping του θανάτου), *δ)* επιθέσεις εκμετάλλευσης πρωτοκόλλου (π.χ. επιθέσεις TCP SYN) και *ε)* εσφαλμένες επιθέσεις πακέτων (π.χ. επίθεση γης και κατακερματισμένες επιθέσεις πακέτων). Για παράδειγμα, η *επίθεση λόγω πείνας σε πόρους* μπορεί να επιτευχθεί με την αποστολή πολλών πακέτων που απαιτούν έλεγχο ταυτότητας με αποτέλεσμα την έναρξη δαπανηρής κρυπτογραφικής επεξεργασίας πόρων. Όταν οι κακοί κόμβοι είναι συνδεδεμένοι στο εσωτερικό δίκτυο, μπορούν να ξεκινήσουν διαφορετικούς τύπους επιθέσεων, όπως *δηλητηρίαση δρομολόγησης* ή *πτώση πακέτων*. Με βάση τα χαρακτηριστικά των επιθέσεων, μπορούν να διακριθούν ως *προσανατολισμένες στο στόχο επιθέσεις*, *επιθέσεις με προσανατολισμό των εκτελεστών και επιθέσεις προσανατολισμένες στο στρώμα*. Όσον αφορά τις επιθέσεις με προσανατολισμό των εκτελεστών, οι εσωτερικοί επιτιθέμενοι μπορούν να εκτελέσουν *επιθέσεις μαύρης τρύπας* και *γκρίζας τρύπας*. Κατά τη διάρκεια μιας επίθεσης με μαύρη τρύπα, όλη η κυκλοφορία δικτύου ανακατευθύνεται, με αποτέλεσμα την απώλεια πακέτων δεδομένων. Στην περίπτωση επίθεσης γκρίζας οπής, υπάρχει *επιλεκτική προώθηση* των πακέτων δεδομένων. Αυτοί οι τύποι επιθέσεων συμβαίνουν συνήθως σε δίκτυα ματιών.

Τα δίκτυα αισθητήρων είναι επιρρεπή σε *μηχανισμούς παρεμβολής*, πράγμα που σημαίνει ότι ένας αντίπαλος μπορεί να εισάγει ανεπιθύμητα σήματα στο κανάλι επικοινωνίας. Αυτά τα σήματα μπορεί να εμπλέκει τελείως το κανάλι έτσι ώστε αυθεντική επικοινωνία δεν μπορεί να λάβει χώρα ή τα πακέτα στη μετάδοση να είναι κατεστραμμένο. Σε ένα επεισόδιο DoS που χρησιμοποιεί τεχνικές παρεμβολής, υπάρχουν ενεργειακά ζητήματα σχετικά με τον ομόλογο του επιτιθέμενου που μπορεί να εξαντληθεί, όταν ο ενεργειακός του προϋπολογισμός είναι περιορισμένος και μπορεί επίσης να οδηγήσει σε έναν κόμβο αποτυχία. Σε αυτό το πνεύμα, το state-of-the-art εν εξελίξει έργων έχουν στόχο πώς ο εισβολέας μπορεί να εξοικονομήσει ενέργεια, χρησιμοποιώντας μια εκτίμηση για το αν θα μπλοκάρει το κανάλι να υποβαθμίσει την ικανότητα της ανίχνευσης εισβολής.

Καθώς η μετατόπιση τεχνολογίας αναδεικνύει νέες εξελίξεις στη δικτύωση ad-hoc, οι κινητές συσκευές και οι αισθητήρες μπορούν να κυριαρχήσουν στην αγορά τηλεπικοινωνιών στο μη-μακρινό μέλλον. Προχωρώντας προς τη σύγκλιση δικτύων κινητών και cloud, προκύπτουν πολλά ζητήματα ασφάλειας, ενώ οι παράγοντες που βασίζονται σε κινητά δεν διαθέτουν κοινή γλώσσα / οντολογία και επομένως είναι επιρρεπείς σε επιθέσεις DoS, κατατάσσοντας τη φύση τους.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τις ομάδες περιουσιακών στοιχείων ***Αίτηση τομέα, Συσκευή τομέα, Δίκτυο τομέα*** και το ***προϊόν / επιχειρηματικές διαδικασίες τομέα.***

### 5.5.2. Απειλή: κακόβουλο κώδικα / λογισμικό / δραστηριότητα

Τα δίκτυα ad-hoc και αισθητήρων πρέπει να παρακολουθούνται για περιβαλλοντικές παραμέτρους, δομική ακεραιότητα του δομημένου περιβάλλοντος και χρήση αστικών χώρων, υπηρεσιών και υπηρεσιών κοινής ωφέλειας. Ωστόσο, οι αισθητήρες μπορούν να διακυβευτούν μέσω *κακόβουλου κώδικα* ή με την εκμετάλλευση της φυσικής διεπαφής τους. Ένας επιτιθέμενος μπορεί να επιδιώξει να προκαλέσει μια ακατάλληλη απόκριση του

συστήματος (π.χ. ενεργοποίηση υπερφόρτωσης σε δίκτυο ηλεκτρικού ρεύματος και μερική διακοπή λειτουργίας) ή κάλυψη μιας επιθυμητής απόκρισης του συστήματος (π.χ. σίγαση συναγερμού εισβολής).

Λόγω των πιθανών τρωτών σημείων των ενεργοποιητών και των αισθητήρων, είναι σημαντικό να μελετηθεί και να αναλυθεί η διάδοση κακόβουλου κώδικα (π.χ. κακόβουλου λογισμικού) στα δίκτυα. Για σκοπούς ανάλυσης πολλαπλασιασμού, πρόσφατες έρευνες έχουν εισαγάγει μαθηματικά μοντέλα σε τρόπο ανά συσκευή (δηλ. Αυτόνομο). Επιπλέον, το μοντέρνο κακόβουλο λογισμικό χαρακτηρίζεται από περίπλοκες τεχνικές παρατήρησης και πρόσφατες ερευνητικές προσεγγίσεις οδήγησαν σε νέες τεχνικές ανίχνευσης και ταξινόμησης.

Η έννοια του *υλικού Trojan* (HWT) εμφανίζεται στα ασύρματα δίκτυα αισθητήρων. Ένα HWT είναι μια εσκεμμένη τροποποίηση του υλικού κατά τη διάρκεια της διαδικασίας κατασκευής και μπορεί να σχεδιαστεί για να παρακολουθεί ήσυχα, για να στέλνει ενεργά ευαίσθητες πληροφορίες ή για να καταστήσει την μολυσμένη συσκευή υποδοχής άχρηστη. Μέσα στο οικοσύστημα IoT, οι κόμβοι των αισθητήρων μπορούν να αναπτυχθούν σε ένα κατανεμημένο δίκτυο για να αναγνωρίσουν αμοιβαία την αξιοπιστία του γειτονικού τους αισθητήρα. Σύμφωνα με αυτό το σχήμα, μπορούμε να εντοπίσουμε διαρροές πληροφοριών που προκαλούνται από ένα HWT.

Τα δίκτυα ad-hoc μπορούν να χρησιμοποιούν κινητές συσκευές για συγκεκριμένο σκοπό, όπως για παιχνίδια, όπως στο στ amous παιχνίδι s της Blizzard World of Warcraft (WOW) και Linden Research για το Second Life (SL). Σε αυτή την περίπτωση, τα μαζικά multiplayer online παιχνίδια (MMOG) μπορούν να εκτεθούν σε κακόβουλες δραστηριότητες.

Τα περιουσιακά στοιχεία που στοχεύουν αυτές οι απειλές περιλαμβάνουν τις κατηγορίες ενεργητικού ***Domain Domain***, ***Domain Device***, ***domain Domain*** και ***Product / Business Processes Domain***.

### 5.5.3. Απειλή: Χειρισμός υλικού και λογισμικού

Σε αντίθεση με τους ξένους (δηλαδή άτομα εκτός της περιμέτρου πρόσβασης στο δίκτυο) που δεν είναι σε θέση να επικοινωνούν απευθείας με το δίκτυο, οι εμπλεκόμενοι έχουν αυξήσει την πρόσβαση στους πόρους και τις προνομιακές γνώσεις του εσωτερικού δικτύου. Αυτή η επίθεση των έσω είναι μια αυξανόμενη ανησυχία για τις περισσότερες εφαρμογές, όπως ο είναι η επίθεση είναι πιο δύσκολο να προληφθεί, λόγω των άγνωστων σχέδια επίθεσης και την ποικιλία των εσωτερικών επιθέσεων. Εάν λαμβάνεται μια ειδοποίηση για ένα μη έγκυρο μοτίβο, απαιτείται επιπλέον ανάλυση για να επαληθεύσετε εάν υπάρχει κακόβουλη προσπάθεια ή όχι.

Ορισμένες κακόβουλες δραστηριότητες είναι επίσης πιθανό να παραμείνουν ανυπολόγιστες, καθώς μπορούν να παρακάμψουν τις μεθόδους ελέγχου ταυτότητας και εξουσιοδότησης, επειδή είναι ήδη συνδεδεμένες στο εσωτερικό δίκτυο. *Rogue σημεία πρόσβασης,* ασύρματα σημεία πρόσβασης που έχουν εγκατασταθεί χωρίς προηγούμενη συναίνεση ή τη γνώση, μπορεί να εκθέσει την εσωτερική πληροφόρηση προς τον έξω κόσμο και θα μπορούσε να προσφέρει παράνομη πρόσβαση σε μη εξουσιοδοτημένους χρήστες.

Τα στοιχεία ενεργητικού που στοχεύουν αυτές οι απειλές περιλαμβάνουν το ***Domain Domain Application Domain***, ***Device Domain***, ***Domain Network***, ***Operational Domain*** και ***Product / Business Process Domain***.

### 5.5.4. Απειλή: Χειρισμός πληροφοριών

Οι WSNs χρησιμοποιούν συνήθως ένα πρότυπο επικοινωνίας πολλών προς ένα, που σημαίνει ότι διάφοροι αισθητήρες συλλέγουν και στέλνουν δεδομένα στο μοναδικό κέντρο ελέγχου (δηλαδή στον κόμβο νεροχύτη ή στον σταθμό βάσης). Αυτός είναι ο λόγος για τον οποίο τα WSNs είναι ευάλωτα σε *επιδρομές*. Ο επιτιθέμενος ισχυρίζεται ότι έχει τη συντομότερη διαδρομή προς τον σταθμό βάσης και, ως εκ τούτου, μπορεί να αλλάξει εξ 'αποστάσεως τα δεδομένα διέλευσης και με αυτόν τον τρόπο να απειλήσει τη λειτουργία του δικτύου.

Μεταξύ των διαφόρων προτύπων που προτείνονται για επικοινωνίες M2M και IoT από διάφορους ερευνητές, το μεσαίος λογισμικό με μεσαίο λογισμικό Semantic middleware και Service Oriented Architecture (SOA) βασίζεται στην ανταλλαγή μεταδεδομένων γλώσσας Extensible Mark-up Language (XML) για διαλειτουργικότητα, ενώ το SOA και το Representational State Transfer (REST) είναι πιο δημοφιλή σε περιβάλλοντα επιχειρήσεων. Τα κύρια εκμεταλλεύματα που σχετίζονται με τα παραπάνω είναι: *(α) η* επανάληψη μιας συσκευής, *(β) η* επίθεση των μαύρων οπών ή των οπών νεροχύτη (που είναι επίσης συμβάντα DoS) στο πρωτόκολλο δρομολόγησης για δίκτυα χαμηλής κατανάλωσης και απώλειας (RPL *)* επιθέσεις replay, όταν έγκυρα δεδομένα αναμεταδίδεται ή καθυστερήσει κατά ένα αντίπαλο για να κερδίσει παράνομη και μη εξουσιοδοτημένη πρόσβαση, *(δ)* συμβιβασμός του απορρήτου, όταν μπορεί να χειριστεί τα αναμετάδοση δεδομένων, *(ε)* ενεργό εισαγωγή της κίνησης του δικτύου (δηλαδή την πλαστογράφηση, πλαστοπροσωπία) για την αποστολή κακόβουλη επισκεψιμότητα σε άλλους κόμβους, *(στ)* παθητική παρακολουθεί την κίνηση του δικτύου (π.χ. εισπνοή, υποκλοπή) σε Zigbee και IEEE 802.15.4 δίκτυα λόγω της αδύναμης εφαρμογής τους από τα κλειδιά κρυπτογράφησης κόμβους (δηλαδή μεταδίδονται σε απλό κείμενο). Παραδείγματα σημαντικά θέματα σχετικά με τη διαδικασία δρομολόγησης είναι η *υπερχείλιση πίνακα δρομολόγησης* (δηλαδή μεταδίδουν ψευδείς πληροφορίες με τους γείτονες, πλημμυρίζουν τα τραπέζια τους και ως εκ τούτου αρνούνται οι πραγματικές διαδρομές) και η *δηλητηρίαση πίνακα δρομολόγησης* (δηλαδή διαφημίζουν μια ψεύτικη διαδρομή με το μικρότερο hop και το αργότερο αριθμός ακολουθίας) στο πρωτόκολλο Ad-hoc Διανύσματος Απόστασης Απαιτήσεων (AODV).

Τα περιουσιακά στοιχεία που απευθύνονται από αυτές τις απειλές των περιουσιακών στοιχείων ***του τομέα*** ομάδες ***συσκευής, Δίκτυο τομέα*** και η ***εφαρμογή s d omain***.

### 5.5.5. Απειλή: Απομακρυσμένη δραστηριότητα

Ένα παράδειγμα για την απομακρυσμένη δραστηριότητα περιλαμβάνει τη χρήση του *Botnet* ως ένα δίκτυο μολυσμένων μηχανών, το οποίο ελέγχεται από ένα απομακρυσμένο μηχάνημα και στοχεύει να ξεκινήσει επιθέσεις εναντίον περισσότερων θυμάτων. Από την άποψη της κινητής υπολογιστικής και με την αξιοποίηση των πλεονεκτημάτων των επικοινωνιών M2M στην κάλυψη της διάδοσης κακόβουλου κώδικα, το MobiBots μπορεί να μολύνει και να συντονίσει αυτές τις συσκευές σε μεγάλη κλίμακα. Για παράδειγμα, ένα MobiBot μπορεί να μολύνει ένα δίκτυο 96 κόμβων σε λίγα μόνο λεπτά και να μπορεί να κλιμακώσει έως και 10.000 δίκτυα κόμβων.

Για παράδειγμα, όταν πρόκειται για ενσωματωμένα συστήματα στην οικιακή δικτύωση, όπου οι αισθητήρες αποτελούν βασικό στοιχείο για τη μελέτη, υπάρχουν ειδικές ανάγκες. δηλαδή σύνδεση στο Internet για ενημερώσεις υλικολογισμικού. Σήμερα, οι *ενημερώσεις απομακρυσμένου υλικολογισμικού* δεν συμμορφώνονται με τον μύθο της απόλυτης ασφάλειας, καθώς είναι υπεύθυνοι για τη διανομή κακόβουλου περιεχομένου μέσω του Διαδικτύου. Ένα άλλο παράδειγμα κακόβουλου υλικολογισμικού είναι ο έλεγχος των οχημάτων και του επιταχυντή τους. Επιπλέον, ένα άλλο rootkit υλικολογισμικού είναι υπεύθυνο για τον κακό χειρισμό πακέτων δικτύου ελέγχοντας την CPU της κάρτας διασύνδεσης δικτύου (NIC).

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τις ομάδες περιουσιακών στοιχείων ***της συσκευής τομέα, Δίκτυο τομέα, Επιχειρησιακό Τομέα*** και ***προϊόντων / επιχειρηματικές διαδικασίες τομέα.***

### 5.5.6. Απειλή: Στοχευμένες επιθέσεις

*Η κινητή συμμετοχική ανίχνευση* εκμεταλλεύεται τις δυνατότητες ανίχνευσης που διατίθενται στα κινητά τηλέφωνα για μια εις βάθος ανάλυση των συμμετεχόντων ατόμων και του περιβάλλοντος τους. Σε αυτή την ιδέα ad-hoc δικτύωσης, κατά τη λήψη των εργασιών από το διακομιστή εφαρμογών ή την αναφορά μετρήσεων αισθητήρων στο διακομιστή, μπορούν να αποκαλυφθούν οι πληροφορίες απορρήτου του συμμετέχοντα (π.χ. ταυτότητα και τοποθεσία) ακόμη και αν χρησιμοποιείται ψευδώνυμο. Για παράδειγμα, μια αντίστροφη αναζήτηση αναζήτησης διευθύνσεων μπορεί να αποκαλύψει το όνομά τους, καθώς οι συμμετέχοντες μετακινούνται συνήθως μεταξύ της κατοικίας τους και του χώρου εργασίας τους. Επιπλέον, η θέση των σημερινών συμμετεχόντων μπορεί επίσης να προσδιοριστεί με βάση τις συλλεγμένες μετρήσεις αισθητήρων. Για παράδειγμα, οι εικόνες, τα δείγματα ήχου και τα δεδομένα ρύπανσης ενδέχεται να περιλαμβάνουν μοναδικά χαρακτηριστικά, αποκαλύπτοντας τον τόπο των συμμετεχόντων.

Στοχευμένες επιθέσεις υπάρχουν επίσης στο φυσικό στρώμα οποιασδήποτε επικοινωνίας αισθητήρα. Η *Παραποίηση Δεδομένων Αισθητήρων Φάσματος (SSDF)* ή αλλιώς η βυζαντινή επίθεση διεξάγεται για την επίτευξη δύο στόχων: *(α)* βανδαλισμού και *(β)* εκμετάλλευσης. Ο πρώτος στόχος αναφέρεται στην παρεμβολή στα πρωτεύοντα συστήματα μέσω των κακόβουλων χρηστών που αναφέρουν την κενή θέση του καναλιού, γεγονός που δείχνει ότι το κανάλι είναι απασχολημένο. Έτσι, τα δεδομένα ανίχνευσης προκαλούν τον ειδικό κόμβο (δηλαδή το κέντρο σύντηξης - FC) για να επιτρέψουν σε άλλους αισθητήρες να έχουν ψευδή πρόσβαση στο κανάλι. Ο δεύτερος στόχος αναφέρεται στον αποκλεισμό αδρανών καναλιών. Εδώ, οι επιτιθέμενοι στέλνουν καναλιού απασχολημένες πληροφορίες όταν τα δεδομένα αίσθησης καταλήγουν στο συμπέρασμα ότι το κανάλι είναι αδρανές.

Ομοίως, ο μηχανισμός αντεπιστροφής χειρίζεται τον χρόνο απόσπασης για την περίπτωση του μέσου ελέγχου πρόσβασης (MAC) και ειδικά του IEEE 802.11. Η αποτυχημένη συμπεριφορά ή αλλιώς η *επίθεση* είναι απρόβλεπτη σε τέτοια δίκτυα και οδηγεί σε έναν κόμβο ο οποίος σκοπεύει να αποκτήσει το κανάλι με μεγαλύτερη πιθανότητα μειώνοντας τον χρόνο του (δηλαδή του χρόνου αναμονής).

Τα στοιχεία ενεργητικού που στοχεύουν αυτές οι απειλές περιλαμβάνουν τις ομάδες στοιχείων ***Domain Device*** και ***Domain Network***.

### 5.5.7. Απειλή: Κοινωνική Μηχανική

Στο πεδίο των επικοινωνιών M2M, ως ο πυρήνας του οικοσυστήματος IoT, που περιλαμβάνει και τον άνθρωπο, η κοινωνική μηχανική εξακολουθεί να αποτελεί σοβαρή απειλή για την ασφάλεια των ατόμων και των οργανώσεων και συχνά εκτοξεύεται μέσω τηλεφώνου ( *τηλεφωνική απάτη* ) ή ηλεκτρονικού ταχυδρομείου ( *phishing* ). Πρόσφατες μελέτες υποστηρίζουν ότι υπάρχει συσχέτιση μεταξύ της πρόθεσης των ατόμων να αντισταθούν στην κοινωνική μηχανική και τις ενέργειες ασφαλείας τους (δηλ. Αυτοαναφερόμενες ή παρατηρημένες) σε πολλαπλά πολιτισμικά περιβάλλοντα.

Η αυξανόμενη τάση προς την BYOD (φέρει τη δική σας συσκευή) έχει επιδεινώσει το πρόβλημα. Μια δικτυακή δικτύωση d-hoc και ευάλωτες εφαρμογές κινητής τηλεφωνίας μπορούν να χρησιμοποιηθούν για την πραγματοποίηση επιθέσεων για πλαστογράφηση ταυτότητας χρηστών ή για αεροπειρατεία λογαριασμών χρηστών και πολλά άλλα. Ως εκ τούτου, η *επίθεση δόλωσης* αναφέρεται σε επιτιθέμενους που εγκαταλείπουν μέσα μνήμης που έχουν μολυνθεί από κακόβουλο λογισμικό σε μια τοποθεσία όπου είναι πιθανό να βρεθούν από μελλοντικά θύματα. Ένα άλλο παράδειγμα είναι το *ηλεκτρονικό ψάρεμα* ( *phishing)* μέσω της προσπάθειας απόκτησης ευαίσθητων πληροφοριών με την περιποίηση ως αξιόπιστη οντότητα. Επιπλέον, η *επίθεση* στο *νερό θα* πρέπει να υπονομεύει έναν ιστότοπο που πιθανόν να ενδιαφέρει το επιλεγμένο θύμα.

Τα στοιχεία ενεργητικού που στοχεύουν αυτές οι απειλές περιλαμβάνουν τις ομάδες στοιχείων ***Domain Application, Device Domain*** και ***Domain Network.***

### 5.5.8. Απειλή: Μη εξουσιοδοτημένες δραστηριότητες

Η κλοπή της ταυτότητας μέσα σε ένα ad-hoc δίκτυο και ένα δίκτυο αισθητήρων μπορεί να επιτευχθεί με την απελευθέρωση μιας *επίθεσης Sybil.* Εδώ, οι αντίπαλοι μπορούν να δημιουργήσουν πολλές κακόβουλες ταυτότητες είτε δημιουργώντας ένα νέο προσδιορισμό είτε κλέβοντας μια ταυτότητα από έναν νόμιμο κόμβο.

Τα στοιχεία ενεργητικού που στοχεύουν αυτές οι απειλές περιλαμβάνουν τον ***τομέα της*** ομάδας στοιχείων ***Device Domain.***

## 5.6. Ομάδα απειλών: Παρακολούθηση, υποκλοπή και αεροπειρατεία

Η ομάδα αυτή περιλαμβάνει τις απειλές που βασίζονται στην τροποποίηση / χειραγώγηση του συνδέσμου επικοινωνίας μεταξύ των δύο μερών. Αυτές οι επιθέσεις δεν απαιτούν την εγκατάσταση πρόσθετων εργαλείων ή λογισμικού στην υποδομή των θυμάτων. Η μη ασφαλή πρόσβαση στο δίκτυο είναι μια γνωστή απειλή, όταν συνδέεται με μη ασφαλή δίκτυα (δηλ. Δημόσιες εστίες) που εκτίθενται σε πολλές επιθέσεις λόγω της ανοικτότητας και των δημόσιων χαρακτηριστικών τους. Συνήθως, δεν υπάρχουν μέτρα ασφαλείας και κανόνες πολιτικής, οι οποίοι επίσης διευκολύνουν την υποκλοπή ή τις κακόβουλες δραστηριότητες.

### 5.6.1. Απειλή: Αναγνώριση Δικτύου

Τα WSNs είναι εξαιρετικά κατανεμημένα δίκτυα ad-hoc. Λόγω ειδικών περιορισμών της ακτίνας επικοινωνίας των κόμβων τους, δρομολογούν την κυκλοφορία τους μέσω ενός σταθμού βάσης (BS). ή αλλιώς σε βάση hop-by-hop. Η *επιλεκτική προς τα εμπρός επίθεση* είναι ένα παράδειγμα στο οποίο ο εισβολέας τοποθετεί έναν κακόβουλο κόμβο αισθητήρα σε μια διαδρομή μεταξύ μιας πηγής δεδομένων και ενός σταθμού βάσης. Ως εκ τούτου, ο εισβολέας μπορεί να εντοπίσει και να επεξεργαστεί την κυκλοφορία του δικτύου στο παράνομο πλεονέκτημά του.

Λόγω του ασταθούς ασύρματου καναλιού που είναι κοινό σε τέτοια δίκτυα, ο ρυθμός απώλειας πακέτων είναι μεγάλος και ποικίλλει από καιρό σε καιρό. Ως εκ τούτου, είναι δύσκολο να γίνει διάκριση ανάμεσα σε μια κακόβουλη πτώση και την απώλεια φυσιολογικών πακέτων. Πρόσφατες μελέτες προτείνουν εναλλακτικά δεδομένα διαβίβασης συμπεριφορών των αισθητηρίων κόμβων ανά απόκλιση του παρακολουθούμενου έναντι της εκτιμώμενης φυσιολογικής απώλειας. Στο πλαίσιο αυτό, η προσαρμοστική διαχείριση της άμυνας του δικτύου για

την αντιμετώπιση επιθέσεων μπορεί να εφαρμοστεί σε συγκεκριμένους τομείς εφαρμογής, όπως: *α)* υποδομή πετρελαίου και φυσικού αερίου, *β)* πυρηνικοί σταθμοί ηλεκτροπαραγωγής, *γ)* έξυπνες πόλεις και *δ)* περιβάλλον ηλεκτρονικής υγείας.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τις ομάδες περιουσιακών στοιχείων ***Αίτηση τομέα, Συσκευή τομέα, Δίκτυο τομέα, Επιχειρησιακό Τομέα*** και ***προϊόντων / επιχειρηματικές διαδικασίες τομέα.***

### 5.6.2. Απειλή: Υποκλοπή πληροφοριών

Η ανίχνευση φάσματος αποτελεί τον πυρήνα των λειτουργικών τεχνικών που παρατηρούνται σε ένα ασύρματο δίκτυο. Μπορεί να υπάρξει παρακολούθηση πληροφοριών. Η πιο γνωστή αυτή ενέργεια ονομάζεται *προσομοίωση πρωτεύοντος χρήστη (PUE).* Σε ένα τέτοιο περιστατικό, οι επιτιθέμενοι μπορούν να τροποποιήσουν τη συχνότητα ραδιοφωνικής μετάδοσης για να μιμηθούν το πρωτεύον σήμα (δηλαδή το σήμα από τον κύριο χρήστη - PU). Επομένως, οι δευτερεύοντες χρήστες (SU) προσδιορίζουν εσφαλμένα τους επιτιθέμενους ως PU. Οι επιτιθέμενοι του PUE μπορούν να ταξινομηθούν ως *(α)* εγωιστές και κακόβουλοι (δηλαδή κλέβοντας το εύρος ζώνης) και *(β)* στατικές και κινητές (δηλαδή ανά θέση).

Στο περιβάλλον του φορητού υπολογιστή, υπάρχουν διάφορες τεχνικές ανίχνευσης κακόβουλου λογισμικού, όπως οι δυναμικοί μηχανισμοί που βασίζονται στην εκτέλεση προγραμμάτων για το λειτουργικό σύστημα Android. Παρόλα αυτά, κακόβουλοι εισβολείς μπορούν εύκολα να επικρατήσουν σε αυτούς, αναπτύσσοντας μπλοκ κώδικα dump και κλήσεις API. Ο τελευταίος φιλοξενείται σε μια *προχωρημένη απειλή (APT),* η οποία έχει ως αποτέλεσμα την παθητική και κακόβουλη καταγραφή πληροφοριών από το δίκτυο.

Σε μια εταιρεία ή εταιρεία, η παρακολούθηση πληροφοριών είναι ένα από τα εργαλεία για την εταιρική κατασκοπεία ή την κυβερνο-κατασκοπεία. Το προσωπικό υψηλής ειδίκευσης που απασχολείται στις εταιρείες σήμερα τείνει να χρησιμοποιεί αυτές τις δεξιότητες για το δικό τους κέρδος με την παρακολούθηση και την πώληση εμπιστευτικών πληροφοριών ή με τη λειτουργία εξωτερικών παραγόντων και προσπαθεί να παρακολουθήσει τις πληροφορίες των αντιμαχόμενων εταιρειών. Στην πρώτη περίπτωση στην οποία παρακολουθούνται εντός της επιχείρησης, η ύπαρξη ad-hoc πρόσβασης στο Intranet της εταιρείας ή η μετάδοση δεδομένων μέσω του αέρα, καθίσταται ευκολότερη η επιτυχία της κυβερνο-κατασκοπείας.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τη ομάδων περιουσιακών στοιχείων ***της συσκευής τομέα, Δίκτυο τομέα,*** και ***το προϊόν / επιχειρηματικών διαδικασιών τομέα.***

### 5.6.3. Απειλή: Ο άνθρωπος στη μέση / η απόπειρα αεροπειρατείας

Σε ορισμένες περιπτώσεις, ένας κακόβουλος κόμβος μπορεί να εισέλθει στο δίκτυο και να προσποιηθεί ότι είναι άλλος κόμβος. Μόλις ο κόμβος συνδεθεί στο δίκτυο, τότε μπορεί να εμφανιστεί παραχάραξη και υποκλοπή δεδομένων. Σε άλλες περιπτώσεις, αυτός ο τύπος επίθεσης είναι γνωστός ως *άνθρωπος-στη-μέση* (MiMA), καθώς οι κόμβοι μπορούν να παρακολουθήσουν την επικοινωνία και να λάβουν τις πληροφορίες και να αναμεταδώσουν λανθασμένες πληροφορίες μεταξύ δύο μερών που επικοινωνούν άμεσα. Η απειλή αυτή μπορεί να οδηγήσει σε αστάθεια του συστήματος ή σε ανώμαλη συμπεριφορά λόγω ψεύτικο πληροφορίες, ακόμη και σύγκρουσης s των πακέτων λόγω της αύξησης των αιτήσεων μεταφοράς ή υποκλαπούν συνδέσεις.

Με βάση πρόσφατες έρευνες, αν και τα ad-hoc και τα αισθητήρια δίκτυα καθώς και τα συστήματα RFID αναπτύσσουν κρυπτογραφικά πρωτόκολλα οριοθέτησης αποστάσεων (DB), εξακολουθούν να αποκτούν σημαντικούς μηχανισμούς υψηλής ασφάλειας για την υπεράσπιση από παράνομες ενέργειες. Τα πρωτόκολλα DB είναι ευάλωτα στην *απάτη της μαφίας* ( *ή αλλιώς στο* πρόβλημα των μεγάλων διευθυντών) και στις επιθέσεις *τρομοκρατικής απάτης*. Στην απάτη της μαφίας, ένας επιτιθέμενος εκτελεί μια επίθεση μεταξύ ενός επαληθευτή (δηλαδή εκείνου που επαληθεύει την τοποθεσία του χρήστη) και ενός χρήστη και ενημερώνει λανθασμένα τον τελευταίο για την τοποθεσία του κόμβου χρήστη. Μια περίπτωση αυτής της επίθεσης είναι μια μηχανή ATM που βρίσκεται σε φυσική θέση. Σε ένα τρομοκρατική απάτη, ένας ανέντιμος χρήστης συνεργάζεται με έναν "τρομοκράτη" επιτιθέμενο κατά τρόπο που ο τελευταίος μπορεί εσφαλμένα να ενημερώσει τον κόμβο επαληθευτή για την τοποθεσία του κόμβου του χρήστη.

Ένα άλλο παράδειγμα είναι οι εφαρμογές που φιλοξενούνται από τα ad hoc δίκτυα οχημάτων (VANET) τα οποία περιγράφονται ως μέρος του οικοσυστήματος για τα ευφυή συστήματα μεταφορών (ITS). Αυτά τα δίκτυα περιλαμβάνουν μια ποικιλία αναδυόμενων εφαρμογών, όπως διαχείριση και έλεγχος της κυκλοφορίας, υπηρεσίες πλησίον πληροφοριών και υπολογισμοί δρομολόγησης πληροφοριών σε πραγματικό χρόνο. Τέτοιες εφαρμογές, οι οποίες ανήκουν στην οικογένεια εφαρμογών της οικογένειας ειδικών εφαρμογών μικρής εμβέλειας (DSRC), μπορούν να διευκολύνουν τις ειδοποιήσεις συνειδητοποίησης σύγκρουσης και τις καταστάσεις έκτακτης ανάγκης, καθώς και εμπορικές εφαρμογές που επιτρέπουν πρόσβαση στο διαδίκτυο, πλοήγηση χάρτη και εξοικονόμηση καυσίμου. Αναλυτικότερα, όσον αφορά τις επικοινωνίες μεταξύ οχημάτων προς οχήματα (V2V) και οχημάτων προς υποδομή (V2I) με χρήση μονάδων της οδού (RSU), σημαντικά ζητήματα ιδιωτικής ζωής θα μπορούσαν να προκύψουν υπό τις επιθέσεις "άνθρωπος-στη-μέση". Οι επιθέσεις αυτές είναι εφικτές λόγω της μη κρυπτογραφημένης επικοινωνίας μεταξύ των RSU και των οχημάτων.

Τα περιουσιακά στοιχεία που απευθύνονται από τις απειλές αυτές περιλαμβάνουν τη ομάδων περιουσιακών στοιχείων ***Τομέα της συσκευής*** και ***Δικτύων τομέα,*** και το ενεργητικό ***της ηλεκτρονικής υγείας*** και ***γ δυνατά με βάση το app lication s.***

## 5.7. Ομάδα απειλών: Βλάβες / Βλάβη

### 5.7.1. Απειλή: Αποτυχία συσκευών ή συστημάτων

Σε ό, τι αφορά σε άλλα μηχανήματα υπολογιστών, οι κόμβοι αισθητήρων υποφέρουν από σφάλματα λογισμικού που ενδέχεται να καταλήξουν είτε σε προσωρινή κατάσταση εκτός υπηρεσίας είτε σε πλήρη αποτυχία αυτών των συσκευών. *Η επιδιόρθωση σφαλμάτων εκτός σύνδεσης* και *η αυτοθεραπεία* είναι δύο τεχνικές που μπορούν να χρησιμοποιηθούν για την ανίχνευση και αντιμετώπιση των συνθηκών πριν από την ανάπτυξη ή κατά τη διάρκεια του χρόνου εκτέλεσης.

Εκτός από τα παραπάνω, η αποτυχία των συστημάτων μπορεί να είναι δραματικά επιβλαβής όχι μόνο για τις συσκευές που χρησιμοποιούν, αλλά και για τις πιθανές επιπτώσεις στον ανθρώπινο πληθυσμό που φιλοξενούν. Για παράδειγμα, ο σκουλήκι υπολογιστών που ονομάζεται *Stuxnet, ο οποίος* εργάστηκε για να επιτεθεί στην πυρηνική εγκατάσταση του Natanz που βρίσκεται στο Ιράν, εκμεταλλεύτηκε τα PLC στην υποδομή συστημάτων βιομηχανικού ελέγχου. Αυτό το περιστατικό υπογράμμισε ότι τα σφάλματα και τα τρωτά σημεία του μηχανισμού κατασκευής καθώς και ο ανθρώπινος παράγοντας μπορούν να οδηγήσουν σε θανατηφόρα ατυχήματα.

Τα στοιχεία ενεργητικού που στοχεύουν αυτές οι απειλές περιλαμβάνουν τις ομάδες στοιχείων ***Device Domain*** και ***Domain του Δικτύου,*** αλλά και τα συστήματα ***παραγωγής*** και ***ελέγχου*** περιουσιακών στοιχείων.

### 5.7.2. Απειλή: Αποτυχία ή διακοπή συνδέσεων επικοινωνίας

*Οι επιθέσεις με παρεμβολές* αποτελούν σημαντικό πρόβλημα για τα ad-hoc και τα δίκτυα αισθητήρων και αφορούν όλο και περισσότερο τις κρατικές αρχές για την αντιμετώπιση των καταστροφών. Η συσκευή εμπλοκής επιδιώκει να επιλέξει μια θέση επιλέγοντας το ίδιο κανάλι που χρησιμοποιούν οι κόμβοι, έτσι ώστε τα δεδομένα να μπλοκάρουν ή να διαταράσσονται από την επιτυχή μετάδοση. Η διακοπή των επικοινωνιακών ζεύξεων απειλείται επίσης με ένα εναλλακτικό τρόπο από *(α)* συνεχή jammer (δηλαδή που μεταδίδει συνεχώς τυχαία), *(b)* παραπλανητικό jammer (δηλαδή συνεχώς, αλλά όχι τυχαία), *(c)* τυχαίο jammer ισχύς), *(δ)* αντιδραστικός παρεμποδιστής (δηλαδή ακούστε το κανάλι και την εφεδρική ισχύ). Εμπλοκές επιθέσεις είναι πολύ σοβαρές, όπως το σήμα παρεμβολής s είναι *(α)* ανθεκτικές στις συγκρούσεις, *(β)* μπορούν να ταξιδεύουν για μεγαλύτερες αποστάσεις και *(γ)* πιθανόν να μεταδοθούν σε σύντομες διάρκειες (π.χ. ως πλαίσιο ACK).

Τα στοιχεία ενεργητικού που στοχεύουν αυτές οι απειλές περιλαμβάνουν τις ομάδες στοιχείων ***Domain Device (Device Domain*** ) και τον ***τομέα δικτύου (Network Domain*** ) και το ***ραδιόφωνο*** του παγίου (asset).

## 5.8. Ad-hoc και αισθητήρες δικτύων έκθεση σε απειλές

Σε αυτή την ενότητα συνοψίζεται και ταξινομείται η απειλή έκθεσης των περιουσιακών στοιχείων ad-hoc και αισθητήρων δικτύου.

| THREAT GROUP | THREAT | ASSET GROUP | ASSET/DETAIL |
|---|---|---|---|
| **Unintentional damage / loss of information or IT assets** | | Device domain<br>Network domain<br>Application Domain<br>Operational<br>Business Processes | |
| | Inadequate design and planning or improper adaptation | Device domain | Data |
| | Using information from unreliable source | Ditto | |
| | Erroneous use or administration of devices and systems | Ditto | |
| | Loss of devices | Device domain | |
| | Damage caused by a third party | | Data |
| **Disaster (natural, environmental)** | | Device domain<br>Network domain | **Control Systems**<br>**Physical Security**<br>**Vending Machines**<br>**Road Safety** |
| | Water | Ditto | Ditto |
| | Wildlife | Ditto | Ditto |
| | Explosion | Ditto | Ditto |
| | Thunder strike | Ditto | Ditto |
| | Natural disasters | Ditto | Ditto |
| | Fire | Ditto | Ditto |
| **Legal** | | Application Domain<br>Business Processes | |
| | Abuse of personal data | | Healthcare<br>Physical Security<br>Supply & provisioning |
| | Violation of laws and regulations | Device domain<br>Network domain<br>Application Domain<br>Operational<br>Business Processes | |
| | Failure to meet contractual requirements | Ditto | |
| **Outages** | | Device domain<br>Network domain | |

| THREAT GROUP | THREAT | ASSET GROUP | ASSET/DETAIL |
|---|---|---|---|
| | | Application Domain<br>Operational<br>Business Processes | |
| | Internet outage | Ditto | |
| | Network outage | Ditto | |
| | Loss of support services | Ditto | |
| Nefarious activity / abuse | | Device domain<br>Network domain<br>Application Domain<br>Operational<br>Business Processes | |
| | Denial of service | Device domain<br>Network domain<br>Application Domain<br>Business Processes | |
| | Malicious code, software or activity | Device domain<br>Network domain<br>Application Domain<br>Business Processes | |
| | Manipulation of hardware and software | Ditto | |
| | Manipulation of information | Device domain<br>Network domain<br>Application Domain | |
| | Remote activity | Device domain<br>Network domain<br>Operational<br>Business processes | |
| | Targeted attacks | Device domain<br>Network domain | |
| | Social Engineering | Device domain<br>Application Domain<br>Network domain | |
| | Unauthorized activities | Device domain | |

| THREAT GROUP | THREAT | ASSET GROUP | ASSET/DETAIL |
|---|---|---|---|
| | | Device domain<br>Network domain<br>Application Domain<br>Operations<br>Business Processes | |
| **Eavesdropping, Interception, Hijacking** | Network Reconnaissance | Ditto | |
| | Interception of information | Device domain<br>Network domain<br>Business processes | Manufacturing<br>Control systems |
| | Man-in-the-middle / Session hijacking | Device domain<br>Network domain | E-health<br>Cloud-based apps |
| **Failures / Malfunction** | | Device domain<br>Network domain | |
| | Failure of devices or systems | Ditto | Control<br>Manufacturing |
| | Failure or disruption of communication links | Ditto | Radio |
| | Failure or malfunction of equipment | Ditto | Power Supplies<br>Cooling systems |
| | Failure or disruption of main supply | Ditto | |
| **Physical attack** | | Device domain<br>Network domain | |
| | Terrorist attack | Ditto | |
| | Damage from the warfare | Ditto | |
| | Unauthorized physical access | Ditto | |
| | Theft | Ditto | Mobile devices<br>RFID tags & readers<br>Cars & vehicles<br>Interconnection points<br>Transmission nodes |
| | Vandalism | Ditto | |
| | Sabotage | Ditto | |

# 6. Threat Agents

Σε αυτό το κεφάλαιο, παρουσιάζουμε μια λίστα κατηγοριών παραγόντων απειλής. Οι απειλητικοί παράγοντες ή οι πηγές απειλών είναι τα άτομα ή οι ομάδες ανθρώπων που χρησιμοποιούν τις απειλές και τα τρωτά σημεία ενός συστήματος για τους σκοπούς τους. Για κάθε κατηγορία απειλών, επικεντρωνόμαστε στα χαρακτηριστικά εκπομπής, θέσης, ποσότητας, κινήτρου, ορθολογισμού, κινητικότητας και δεξιοτήτων. Οι προτεινόμενες κατηγορίες είναι οι ακόλουθες:

Οι εταιρίες υιοθετούν συχνά επιθετική τακτική με το κίνητρο να αποκτήσουν πλεονέκτημα έναντι των ανταγωνιστών. Συνήθως δέχονται επιθέσεις ως εξωτερικοί. Επίσης, οι εταιρείες είναι ορθολογικοί επιτιθέμενοι δεδομένου ότι θεωρούν την αναλογία κέρδους αποτελέσματος και κόστους της επίθεσης. Το επίπεδο εξειδίκευσης των μεθόδων επίθεσης τους είναι σχετικό με το μέγεθος και τον τομέα της εταιρείας.

Το κίνητρο των εγκληματιών του κυβερνοχώρου είναι οικονομικό κέρδος ή σε πολλές περιπτώσεις η ίδια η πειρατεία, ως δοκιμασία δεξιοτήτων ή εμπόδιο. Είναι πολύ εξειδικευμένοι και αυτός ο παράγοντας μπορεί να οδηγήσει σε παράλογες επιθέσεις, όπου ο κίνδυνος είναι μεγαλύτερος από το αναμενόμενο αποτέλεσμα της επίθεσης. Μπορούν να εργάζονται σε τοπικές, εθνικές ή διεθνείς ομάδες.

Η ομάδα τρομοκρατών του κυβερνοχώρου εμπλέκει τρομοκράτες που εκμεταλλεύονται τις επιπτώσεις των επιθέσεων στον κυβερνοχώρο σε κρίσιμες υποδομές όπως το σύστημα παραγωγής ενέργειας, οι τηλεπικοινωνίες, οι κυβερνητικοί χώροι κλπ. Το επίπεδό τους είναι χαμηλότερο από τους εγκληματίες στον κυβερνοχώρο και διαπράττουν πιο ορθολογικές επιθέσεις. Το κίνητρό τους είναι συνήθως πολιτική ή θρησκεία. Θεωρούνται ως εξωτερικοί πράκτορες και μπορούν επίσης να εργάζονται σε ομάδες.

Οι Script kiddies χρησιμοποιούν υπάρχοντα σενάρια ηλεκτρονικών υπολογιστών ή κώδικα για να hack. Δεν διαθέτουν την εμπειρογνωμοσύνη για να δημιουργήσουν τα δικά τους εργαλεία. Το κίνητρό τους είναι η συγκίνηση του κινδύνου. Οι επιθέσεις που διαπράττονται από αυτούς είναι ως επί το πλείστον αφελείς, καθώς δεν έχουν το υπόβαθρο για την εκτίμηση του λόγου αποτελέσματος / κινδύνου ή είναι αδιάφορες γι 'αυτούς.

Οι online κοινωνικοί χάκερ (hacktivists) είναι ακτιβιστές που χρησιμοποιούν το hacking ως εργαλείο. Αυτή η ομάδα είναι σαν τρομοκράτες στον κυβερνοχώρο. Το κίνητρό τους είναι επίσης πολιτικά ή κοινωνικά θέματα. το επίπεδο δεξιοτήτων τους μπορεί να ποικίλει και μπορεί να λειτουργούν σε ομάδες. Στοχεύουν στην κρίσιμη δημόσια υποδομή.

Οι εργαζόμενοι είναι εμπιστευόμενοι που ενδέχεται να ευθύνονται για ακούσια ζημιά που οφείλεται σε σφάλματα ή άδικες επιθέσεις σε συνεργασία με τους αλλοδαπούς σκοπίμως ή για να κάνουν προσωπικό κέρδος. Παρέχουν εμπιστευτικές πληροφορίες και καθιστούν το στοχευμένο σύστημα εξαιρετικά ευάλωτο.

Τα κράτη μέλη του κυβερνοεγκληματικού εγκλήματος και του εγκλήματος στον κυβερνοχώρο έχουν αναπτύξει εξαιρετικά εξελιγμένα όπλα στον κυβερνοχώρο, συστήματα με πόρους και εμπειρογνώμονες υψηλού επιπέδου. Αυτά τα χαρακτηριστικά τους καθιστούν σημαντικούς παράγοντες απειλής.

Οι φυσικές καταστροφές δεν ελέγχονται από μια ομάδα αντιπάλων. ωστόσο, θα πρέπει να θεωρούνται ως παράγοντας απειλής για ad-hoc και δίκτυα αισθητήρων. Κυρίως τα δίκτυα αισθητήρων είναι ευάλωτα σε φυσικές

καταστροφές, δεδομένου ότι οι κόμβοι του δικτύου θα μπορούσαν να βρίσκονται σε ευρεία περιοχή ακατέργαστων ή ανοικτών σε περιβάλλοντα πρόσβασης (δηλαδή υποβρύχια, υπόγεια, πετούν, εξαπλωμένα σε ευρεία χερσαία περιοχή κ.λπ.).

Στον παρακάτω πίνακα, προτείνουμε μια διασύνδεση μεταξύ απειλών και παραγόντων σε δίκτυα ad-hoc και αισθητήρων.

| | CORPORATIONS | CYBER CRIMINALS | CYBER TERRORISTS | SCRIPT KIDDIES | HACKTIVISTS | EMPLOYEES | NATION STATES | NATURAL DISASTERS |
|---|---|---|---|---|---|---|---|---|
| Disaster | | | | | | | • | • |
| Outages | | | | | | • | • | • |
| Legal | • | | | | | • | | |
| Failures, Malfunction | | • | | | • | • | • | |
| Unintentional damage | | | | • | • | • | | |
| Nefarious Activity | • | • | • | • | • | • | • | |
| Physical attacks | | | | | | | • | • |
| Eavesdropping, Interception, Hijacking | • | • | • | • | • | • | • | |

# 7. Ευπάθειες και κίνδυνοι σε δίκτυα ad-hoc και αισθητήρων

Μια εγκατάσταση ad-hoc και δίκτυα αισθητήρων είναι παρά η αύξηση δεν οφείλεται μόνο στην αύξηση του όγκου των συσκευών IoT, αλλά και λόγω των ad-hoc και αισθητήρα δικτύων βιομηχανικών και ερευνητικό ενδιαφέρον έχουν προσελκύσει έκδοση από τη δεκαετία του '80. *«Smart <κάτι>»* (π.χ. πόλεις, κτίρια, οχήματα, οικιακές συσκευές, κινητά τηλέφωνα κλπ) είναι μια μεγάλη τάση και, ως εκ τούτου, αυτά τα τρωτά σημεία του δικτύου έχουν γίνει ένα σημαντικό ζήτημα μεταξύ των ερευνητών και των επαγγελματιών. Έτσι, οι διαθέσιμες στο κοινό πληροφορίες σχετικά με τη δικτύωση ad-hoc και αισθητήρων για θέματα ασφάλειας επικοινωνιών M2M προέρχονται ευρέως από την έρευνα, την τυποποίηση και τις βιομηχανικές δραστηριότητες.

Από τώρα και στο εξής, οι αισθητήρες και η ευκαιριακή σημασία τους στο μοντέλο επικοινωνίας M2M κατέχουν ένα τεράστιο μερίδιο για τον ορισμό του τι και πώς είναι κάτι ευάλωτο. Τα δίκτυα αυτά χαρακτηρίζονται από ευέλικτη αρχιτεκτονική, χωρική φύση, τα μέσα επικοινωνίας, και το συγκρότημα τητα των συσκευών. Για να εξαγάγετε αυτές τις πληροφορίες, θα επικεντρωθεί σε οργανισμούς τυποποίησης ization όπως το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC) και της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU), σε κυβερνητικές αρχές, όπως Defense Advanced Research Projects Οργανισμού (DARPA) και Του Εθνικού Κέντρου Ασφαλείας του Κατάρ αλλά και σε δημοσιευμένα ερευνητικά έργα. Περισσότερες λεπτομέρειες παρουσιάζονται στο επόμενο κεφάλαιο.

Σε αυτό το κεφάλαιο παρέχεται μια σύντομη περιγραφή των τρωτών σημείων και των κινδύνων για δίκτυα ad-hoc και αισθητήρων. Μια προσεκτική αξιολόγηση των σχετικών καλών πρακτικών παρουσιάζεται στο επόμενο κεφάλαιο.

## 7.1. Ad-hoc και ευπάθειες δικτύων αισθητήρων

Τα ad-hoc δίκτυα και τα δίκτυα αισθητήρων μοιάζουν με οποιοδήποτε άλλο σύστημα πληροφορικής και υποφέρουν από τις αναδυόμενες απειλές και ασαφή ευπάθειες σε κάθε έναν από τους πέντε τομείς, που σχετίζονται με την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα, την ιδιωτικότητα και την αυθεντικότητα. Πιο συγκεκριμένα, τα κύρια τρωτά σημεία σε αυτά τα δίκτυα αφορούν την ασφάλεια της συσκευής, η προστασία των δεδομένων, η ακεραιότητα της επικοινωνίας και η διαθεσιμότητα (και για τα δύο πρωτόκολλα και το υλικό που συμμετέχουν), η διαθεσιμότητα των επιχειρηματικών διαδικασιών, την ιδιωτική ζωή και η σταθερότητα λειτουργίας. Η ασφάλεια της συσκευής αντιμετωπίζεται κυρίως με τη χρήση μεθόδων ελέγχου ταυτότητας και τα κατάλληλα εργαλεία παρακολούθησης. Οι μέθοδοι ελέγχου ταυτότητας σε συνεργασία με τη ταξινόμηση στοιχείων στοχεύουν στο να προστατεύσουν τα δεδομένα. Με τις κατάλληλες τεχνικές διαχείρισης και εξειδικευμένου πρωτοκόλλου, η επικοινωνία δικτύου μπορεί να εξασφαλιστεί. Οι διαδικασίες διαχείρισης κινδύνων οδηγούν επίσης στη διαθεσιμότητα των επιχειρηματικών διαδικασιών και στη σταθερότητα της λειτουργίας τους.

Η εξάντληση πόρων των συσκευών είναι μια ευπάθεια των ad-hoc και των δικτύων αισθητήρων, λόγω της φύσης αυτών των συσκευών (δηλαδή μικρών συσκευών με χαμηλή ανεξαρτησία ισχύος). Αυτό μπορεί να εξαλειφθεί με ταξινόμηση δεδομένων, κατάλληλες δραστηριότητες διαχείρισης και προσομοίωσης / οπτικοποίησης / δοκιμών.

Η χρήση της ασύρματης επικοινωνίας σε ad-hoc και δίκτυα αισθητήρων δημιουργεί δυνητικά ορισμένες αδυναμίες που ανήκουν στη φύση του καναλιού επικοινωνίας (π.χ. ανοιχτό αέρα, νερό). Εκτός, τα τρωτά σημεία παρεμπόδισης και παρεμβολής ισχύουν στην περίπτωση χρήσης επικοινωνίας RFID, Bluetooth, NFC και Zigbee. Ένα άλλο χαρακτηριστικό παράδειγμα είναι η παραβίαση ελέγχου πρόσβασης που εκμεταλλεύεται ευπάθειες, όπως μη κρυπτογραφημένες μεταδόσεις που προκαλούνται από συγκεκριμένα πρωτόκολλα που χρησιμοποιούνται για ασύρματη επικοινωνία μεταξύ ενός αναγνώστη ελέγχου πρόσβασης (π.χ. αναγνώστη RFID) και της συσκευής ελεγκτή.

## 7.2. Τα δίκτυα ad-hoc και αισθητήρων κινδυνεύουν

Πολλοί κίνδυνοι επηρεάζουν τα περιουσιακά στοιχεία και τις λειτουργίες των δικτύων ad-hoc και αισθητήρων. Σε ολόκληρη τη βιβλιογραφία, επισημαίνεται ότι τα δίκτυα αυτά συχνά μπορούν να αξιοποιηθούν για δραστικές δραστηριότητες και να παρακολουθήσουν επιθέσεις που οδηγούν σε υψηλό κίνδυνο απώλειας δεδομένων. Δεδομένου ότι τα δίκτυα αυτά έχουν ποικίλους τύπους φυσικής τοποθέτησης (υποβρύχια, υπόγεια κ.λπ.), ο κίνδυνος απώλειας συσκευών σε περίπτωση φυσικών ή περιβαλλοντικών καταστροφών (σεισμός, πλημμύρα, ανεμοστρόβιλος) είναι επίσης σημαντικός.

Η ποικιλία της φυσικής τοποθέτησης των ad-hoc και των δικτύων αισθητήρων, οι περιορισμοί πόρων των συσκευών και η τοπολογία των δικτύων μπορεί να οδηγήσουν στη διαρροή προσωπικών ή ευαίσθητων δεδομένων. Ειδικότερα, οι συμπεριφορές κινδύνου διαρροής απορρήτου σε ad-hoc και δίκτυα αισθητήρων θα μπορούσαν να απειλήσουν ακόμη και ανθρώπινες ζωές.

Η υπερνίκηση και η διαχείριση κακών δραστηριοτήτων μπορεί να επιτευχθεί με αυστηρότερους τρόπους διαχείρισης κινδύνου και επιχειρησιακούς ελέγχους και με τη διαθεσιμότητα εξειδικευμένων εργαλείων και τεχνικών για την επίλυση αυτών των κινδύνων. Εξάλλου, μπορούν να υιοθετηθούν διάφορες άλλες τεχνικές διαχείρισης κινδύνου (π.χ. βαθμολογία κινδύνου, μήτρες κινδύνου), ώστε να εξασφαλιστεί η συνοχή κατά την ιεράρχηση των κινδύνων, να παρουσιαστούν τα σύνθετα δεδομένα κινδύνου και να διευκολυνθούν οι αναθεωρήσεις για την κατανομή των επαρκών πόρων και των μεθόδων μετριασμού.

Πρέπει να σημειωθεί ότι η εκτίμηση των κινδύνων είναι μια συνεχής διαδικασία και η συνεχής παρακολούθηση του δικτύου είναι απαραίτητη. Ως εκ τούτου, η συνεχής αξιολόγηση και αξιολόγηση των κινδύνων από τα ενδιαφερόμενα μέρη θα είναι ασφαλώς προστιθέμενη αξία σε οποιοδήποτε σημείο της διαδικασίας αυτής.

# 8. Καλές πρακτικές

Για αντιμετωπιστεί το ζήτημα των ορθών πρακτικών στον τομέα της ad-hoc και αισθητήρα δικτύωσης για επικοινωνίες M2M, θα προβεί σε ποιοτική ανάλυση σχετικά με τις τρέχουσες προσεγγίσεις και ρουτίνες. Για να το επιτύχουμε αυτό, χρησιμοποιούμε και κατηγοριοποιούμε το δημόσιο διαθέσιμο στη βιβλιογραφία που προέρχεται είτε από τη *βιομηχανία*, τους *δημόσιους οργανισμούς* είτε από τον τομέα της *έρευνας και της ανάπτυξης* (Ε & Α).

Αναγνωρίζουμε ότι σήμερα υπάρχουν αρκετές πηγές ορθών πρακτικών που παρέχουν ένα εκτεταμένο σύνολο μέτρων ασφαλείας και ελέγχων. Πιο αναλυτικά, οι πηγές μας είναι: το *Κέντρο για την Προστασία των Εθνικών Υποδομών (CPNI),* η *Διεθνής Ένωση Τηλεπικοινωνιών (ITU)*, η *Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC),* η *Ομοσπονδιακή Επιτροπή Εμπορίου,* η *Ένωση GSM (GSMA),* η *Διασφάλιση Smart Cities*, το *Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST)*, *το Εθνικό Κέντρο Κατάταξης Πληροφοριών του Κατάρ (Q-CERT)*, τα *Sandia National Laboratories* και πολλά *άλλα (π.χ. ENISA, IETF, DARPA, ερευνητικά κείμενα,* κλπ.). Σε ποσοτικούς όρους, τα περισσότερα *άλλα* έγγραφα που αναλύθηκαν καλύπτουν ένα μέτριο μέρος των μέτρων / ελέγχων ασφαλείας στον τομέα μας. Ωστόσο, όλες οι παραπάνω πηγές θεωρούνται ότι έχουν την ίδια σημασία και παρουσιάζονται στον Πίνακα 3.

Έχουμε εντοπίσει ένα σημαντικό αριθμό μέτρων ασφαλείας / ελέγχων που έχουμε κατηγοριοποιήσει ως εξής:

- Αυθεντικοποίηση
- Προστασία δεδομένων
- Παρακολούθηση
- Δραστηριότητες προσομοίωσης, απεικόνισης και δοκιμών
- Ταξινόμηση δεδομένων
- Διαχείριση και υποστήριξη
- Διαχείριση κινδύνου
- Ειδικευμένος εργαλεία και τεχνικές

Τα εντοπισμένα μέτρα ασφαλείας / έλεγχοι χαρτογραφούνται ενάντια στις απειλές, οριστικοποιώντας το γρίφο των σχέσεων μεταξύ έκθεσης απειλής και προτεινόμενων μέτρων ασφαλείας, ελέγχων και πολιτικής. Αυτές οι πληροφορίες μπορούν επίσης να βρεθούν στον Πίνακα 3 ο οποίος ολοκληρώνει το τρέχον κεφάλαιο.

## 8.1. Αυθεντικοποίηση

1. Εφαρμόστε μεθόδους η κύρωση για την πρόσβαση σε ένα σύστημα / υπηρεσίας από μια συσκευή / άτομο (π.χ. επιβολή της χρήσης ισχυρό κωδικό πρόσβασης, one-time - λογαριασμών πρόσβασης, πιστοποιητικά με κοινό ανάκληση και επανέκδοση, έλεγχος ταυτότητας με βιομετρικά στοιχεία, μάρκες ασφάλεια, πρωτόκολλα πρόκληση-χειραψίες, μηχανισμοί επαλήθευσης πρόκλησης-απάντησης, εξαγνισμένο password hashing, παγκόσμιο κοινόχρηστο κλειδί)
2. Αναπτύξτε πρωτόκολλα που προσδιορίζουν τη βιωσιμότητα των γειτόνων (αξιόπιστο δίκτυο) και επιλύστε βέλτιστα τα προβλήματα
3. Χρησιμοποιήστε τον έλεγχο ταυτότητας των δεδομένων αισθητήρων για χαμηλό κόστος ασφαλείας
4. Πιστοποιήστε τα πακέτα (π.χ. πακέτα hello), έτσι ώστε να μην μπορούν να πλαστογραφηθούν
5. Εφαρμόστε ένα αξιόπιστο μοντέλο για να σχηματίσετε γείτονες για κόμβους και εξαλείψτε έναν συμβιβασμένο κόμβο από τη διαφήμιση της θέσης του
6. Ασφαλείς και στιβαρό μοντέλο επικοινωνίας M2M (δηλ ETSI TS 102 921 επικοινωνίες M2M)

7. Εφαρμόστε τον εγκεκριμένο έλεγχο ταυτότητας που χρησιμοποιείται σε ισχυρά συστήματα ελέγχου ταυτότητας
8. Σχεδιάστε και εφαρμόστε ασφάλεια από το σχεδιασμό
9. Σχεδιάζει και εφαρμόζει μέτρα ασφάλειας σε διάφορα επίπεδα. σχεδιάζουν άμυνας σε βάθος (π.χ. λειτουργία υποβάθμιση ή την αποτυχία, περιττές διαδρομές, ιεραρχική δρομολόγηση, την παράδοση ασφάλεια επιπέδου δικτύου, τα μέτρα δρομολόγησης πολλαπλών-hop)
10. Χρησιμοποιήστε τυποποιημένο έλεγχο ταυτότητας δικτύου και οντότητας (δηλ. ISO / IEC 13157-4: 2016)
11. Συμμορφωθείτε με τις αρχές του δικτύου αισθητήρων (π.χ. ISO / IEC 29182-3: 2014)
12. Χρήση υπηρεσιών ελέγχου ταυτότητας δικτύου (π.χ. 3GPP TS 33.220)
13. Αποσυνδέστε τις διαδικασίες πιστοποίησης ταυτότητας και εξουσιοδότησης με τη διαδικασία ελέγχου ταυτότητας δικτύου
14. Χρησιμοποιώ Κωδικός ελέγχου ταυτότητας μηνύματος με κλειδί (HMAC) για την επικοινωνία μεταξύ ετικετών και αναγνωστών
15. Το απομακρυσμένο τερματικό πρέπει να διαθέτει λειτουργίες ασφαλείας, όπως έλεγχο ταυτότητας οντοτήτων, διαχείριση κλειδιών, κρυπτογράφηση με το διακομιστή εφαρμογών σε επίπεδο εφαρμογής ή επίπεδο δικτύου
16. Η πύλη θα πρέπει να διαθέτει λειτουργίες ασφαλείας, όπως έλεγχο ταυτότητας οντότητας και MAC ή ακεραιότητα, με το διακομιστή εφαρμογής
17. Εφαρμόστε τη σχέση σκουριάς με τη χρήση φορέων ασφαλείας που βασίζονται σε κινητά τηλέφωνα που χρησιμοποιούν μηχανισμούς ενός σημείου σύνδεσης ή τεχνικές διαχείρισης βασισμένες στη διαχείριση (π.χ. πληροφορίες βασισμένες σε συμβάντα, ανωμαλία, μεταχειρισμένα) για να διακρίνουν κακόβουλες παρεμβολές από συμβάντα ή σφάλματα
18. Χρησιμοποιήστε προϊόντα κατά της εξαπάτησης (π.χ. Punkbuster) για να αποτρέψετε μη εξουσιοδοτημένες τροποποιήσεις σε πελάτες εικονικού κόσμου και μηχανισμούς ελέγχου ταυτότητας δύο παραγόντων (π.χ. πιστοποίηση World of Warcraft)
19. Επέκταση του τεχνικού προτύπου Europay MasterCard και VISA ( EMV) για έξυπνες κάρτες πληρωμής για την αποτελεσματική αντιμετώπιση και αποτελεσματική διαχείριση των αδυναμιών του EMV με τη χρήση σημείου πώλησης (POS) αίτημα επαλήθευσης και αίτησης και επιβεβαιώσεις σύνδεσης
20. Εντοπίστε τον δυσλειτουργικό κόμβο χρησιμοποιώντας τεχνικές αυτόματης παλινδρόμησης και αξιολόγησης αξιοπιστίας
21. Επαληθεύστε τους κόμβους και επαληθεύστε τις λεπτομέρειες του προγραμματισμού για να αποτρέψετε την ανατροπή του κόμβου υλικού
22. Βεβαιωθείτε ότι οι επικοινωνούντες κόμβοι είναι επικυρωμένοι πριν από την κρυπτογράφηση δεδομένων που εφαρμόζεται στην ανταλλαγή δρομολόγησης για να υπερασπιστεί τις επιθέσεις σκόπιμης έκθεσης
23. Εξασφαλίστε την εμπιστευτικότητα των πληροφοριών δρομολόγησης κόμβων ζητώντας πληροφορίες δρομολόγησης, οι οποίες πρέπει να είναι επικυρωμένες και πρέπει να είναι εξουσιοδοτημένες για την πρόσβαση αυτή για να υπερασπιστούν τις επιθέσεις πρόσβασης συσκευών απομακρυσμένης συσκευής

## 8.2. Προστασία δεδομένων

1. Ανάπτυξη λύσεων ασφάλειας για τη διαχείριση ομάδων, την προστασία δεδομένων (π.χ. κρυπτογραφία δεδομένων) για δεδομένα σε κατάσταση ηρεμίας ή διαμετακόμισης και ασφαλείς μηχανισμούς οριζόντιας παράδοσης
2. Ανάπτυξη κρυπτογραφικών εφαρμογών μικροεπεξεργαστών για την κάλυψη της ασφάλειας και της ιδιωτικής ζωής σε περιορισμένα περιβάλλοντα (π.χ. ανάγκη για χαμηλό κόστος ασφαλείας, ανοχή σε απώλειες δίκτυα, κρίσιμη χρονική στιγμή και υψηλά ποσοστά δεδομένων)
3. Ελέγξτε τα χαρακτηριστικά απορρήτου για να διαχειριστείτε τις πληροφορίες που παρέχονται σε τρίτους

4. Εντοπίστε τις επιθέσεις επανάληψης διατηρώντας έναν αυξανόμενο μετρητή για κάθε σύνδεσμο και συμπεριλαμβάνοντας την επόμενη τιμή του μετρητή με κάθε πακέτο και απορρίπτοντας πακέτα που περιέχουν παλαιότερες τιμές
5. Χρησιμοποιήστε τεχνικές κρυπτογράφησης για να αποτρέψετε επιθέσεις επιλεκτικής προώθησης
6. Ασφαλής διάθεση ετικετών RFID
7. Επιβολή μορφής αναγνωριστικού μη αποκάλυψης σε ετικέτες RFID
8. Κρυπτογράφηση ευαίσθητων δεδομένων χρήστη
9. Χρησιμοποιήστε ψηφιακές υπογραφές
10. Ανάπτυξη διαδικασίας επιβεβαίωσης χρήστη πριν από την εγκατάσταση και εκτέλεση των εφαρμογών
11. Συνάθροιση Secur e δεδομένων με βάση το πρωτόκολλο DTLS όπου κάθε κόμβος συνάθροιση επιλέξτε είναι το επόμενο ασφαλές και αξιόπιστο hop
12. Χρησιμοποιήστε τις βιβλιοθήκες κρυπτογράφησης
13. Ανάπτυξη συστημάτων διαφύλαξης απορρήτου, ελέγχου πρόσβασης σε δεδομένα υγείας και επεξεργασίας δεδομένων για την προστασία της ιδιωτικής ζωής
14. Αποτρέψτε το μήνυμα να καταστραφεί χρησιμοποιώντας κρυπτογράφηση ελλειπτικής καμπύλης (ECC) μέσω υποδομής δημόσιου κλειδιού (PKI). εφαρμόζεται σε εφαρμογές ειδικής επικοινωνίας μικρής εμβέλειας (DSRC)
15. Συμπληρώστε την κρυπτογράφηση και τον έλεγχο ταυτότητας του layer Link χρησιμοποιώντας ένα μυστικό κλειδί παγκοσμίως για να αποτρέψετε τις επιθέσεις δρομολόγησης
16. Εφαρμογή κρυπτογραφίας πλήκτρων (Ad-hoc δίκτυα) & κρυπτογράφησης συμμετρικού κλειδιού (δίκτυα αισθητήρων)
17. Χρησιμοποιήστε ένα κρυπτοσύστημα είτε βασισμένο σε πλέγματα όπως το NTRUEncrypt είτε ένα πολυμεταβλητό, όπως το TTS
18. Ορχηστεύστε ένα ασφαλές σχήμα συσσωρευτή δεδομένων που βασίζεται σε κρυπτογραφικά πρωτόγοντα για να αναθέσετε την απόκρυψη δεδομένων στο σύστημα *ομομορφικής κρυπτογράφησης* (HE)

## 8.3. Παρακολούθηση

1. Προγραμματισμός ελέγχων, ειδοποιήσεων και αρχείων καταγραφής που εκτελούνται συχνά σε κάθε σύστημα και συσκευή (συγκεκριμένα παραδείγματα: Σύστημα παρακολούθησης ECG χαμηλής ισχύος που μπορεί να φοριέται για απομακρυσμένη παρακολούθηση πολλαπλών ασθενών)
2. Περιορίστε ή παρακολουθήστε οποιαδήποτε μη εξουσιοδοτημένη φυσική πρόσβαση για συγκεκριμένες περιοχές (περιοχή Wi-Fi, ένα πολύ εξοπλισμένο δωμάτιο, όπως ένα κέντρο υπολογιστών, μια περιοχή ετικετών RFID). Αυτός ο έλεγχος μπορεί να επιτευχθεί από ένα σύστημα επιτήρησης ή από έναν Οργανισμό Υπηρεσιών Ασφαλείας
3. Χρησιμοποιήστε την παρακολούθηση απομακρυσμένης εισβολής (RIM), τα συστήματα ανίχνευσης εισβολής (IDS) και άλλα εργαλεία ανίχνευσης επίθεσης. Ελέγξτε βαθιά τα πακέτα για φιλτράρισμα IDS / IPS από κακόβουλη κίνηση
4. Αναπτύξτε την έρευνα μαθηματικών και στατιστικών αναλύσεων για να συλλέξετε και να χειριστείτε μεγάλα σύνολα δεδομένων για να διαμορφώσετε την κανονική συμπεριφορά δικτύου
5. Χρησιμοποιήστε ενσωματωμένα συστήματα παρακολούθησης για ασφάλεια, ανάλυση δεδομένων και συσχετισμό σε WSNs. Αυτό οδηγεί σε ασφαλέστερα συμπεράσματα και μείωση του κόστους των πόρων ανά ταυτότητα
6. Χρησιμοποιήστε ένα σύστημα ενεργειακής παρακολούθησης βάρους, το οποίο αποφεύγει την περιττή μετάδοση πακέτων ή βρόχο και εξοικονομεί δύναμη των κόμβων, αποτρέπει τα WSNs από επιθέσεις βαμπίρ
7. Μετατρέψτε τους αισθητήρες σε αυτοματοποιημένο έλεγχο ως μέρος της πλήρως ολοκληρωμένης και συνδεδεμένων συστημάτων

8. Ανάπτυξη ειδικών κόμβων (gNodes) που παρακολουθούν ομάδες συμπλεγμάτων ή κόμβους ελέγχου (cNodes) που παρακολουθούν τη ροή της κυκλοφορίας σε ομάδες
9. Χρησιμοποιήστε ένα χαμηλό γενικό και μη ενοχλητικό πλαίσιο ελέγχου το οποίο παρακολουθεί (σε πραγματικό χρόνο) τα πρότυπα χρήσης πόρων των εφαρμογών eHealth και ενεργοποιεί τις ειδοποιήσεις προς τους χρήστες αν ανιχνεύονται μη φυσιολογικά πρότυπα
10. Ελέγξτε προσεκτικά την κίνηση των δεδομένων στα σύνορα του δικτύου, για να ελαχιστοποιήσετε την έκθεση στους επιτιθέμενους
11. Διατηρήστε ένα σταθερό ποσό κίνησης σε διαφορετικούς προορισμούς μέσω της δημιουργίας αυθαίρετων κυκλοφοριακών ροών για να υπερασπιστείτε τις επιθέσεις της κυκλοφοριακής ανάλυσης

## 8.4. Δραστηριότητες προσομοίωσης, απεικόνισης και δοκιμών

1. Δημιουργήστε τα κατάλληλα επιχειρηματικά μοντέλα, τις μεθόδους σχεδιασμού και το κοινό σύνολο προτύπων
2. Συνεργαστείτε με προμηθευτές και πωλητές και ελέγξτε τις απαιτήσεις και τις εκτιμήσεις ασφαλείας. Όποτε είναι δυνατόν και αναγκαίο, αλλάξτε τη διαμόρφωση των προεπιλεγμένων συστημάτων για να αποφύγετε την ύπαρξη παραθυρόφυλλων, με την έγκριση και τη συνεργασία των προμηθευτών
3. Προτιμήστε το υλικό, το λογισμικό και τις εφαρμογές που αγοράζονται από την ασφάλεια που αφορούν τους πωλητές. Κρατήστε τους προμηθευτές υπό συνεχή αξιολόγηση
4. Διεξάγετε έρευνες φυσικής ασφάλειας και αξιολογείτε τις ευπάθειες του δικτύου και των υπηρεσιών
5. Ανάπτυξη και εφαρμογή διαδικασιών και αρχών συγκριτικής αξιολόγησης για OS, μικροκώδικα και διορθώσεις
6. Ανάπτυξη μεθόδων διασφάλισης λογισμικού, μεθόδων ιδιωτικού απορρήτου και ασφάλειας, μεθοδολογιών συγκριτικής αξιολόγησης και συνόλων δεδομένων αναφοράς για τη μέτρηση της αξιοπιστίας, της ευπάθειας και της ανθεκτικότητας κατά τη διάρκεια των δραστηριοτήτων ανάπτυξης, δοκιμών και ανάπτυξης, προκειμένου να εξασφαλιστεί μια διαδικασία διασφάλισης ποιότητας και πιστοποίησης
7. Ανάπτυξη τυποποιημένης μεθοδολογίας αξιολόγησης και μέτρησης της μεταφοράς δεδομένων
8. Ενσωματώστε τις δυνατότητες μέτρησης για παρεμβολές σήματος και ισχύ
9. Ανάπτυξη, υποστήριξη και εμπορία προτύπων μέτρησης για την απόδοση και τον κύκλο ζωής των εξαρτημάτων
10. Βεβαιωθείτε ότι τα πρότυπα επικοινωνίας περιλαμβάνουν προδιαγραφές συμμόρφωσης και παρέχουν αυτοματοποιημένα εργαλεία και δοκιμές ελέγχου που μπορούν να δημιουργηθούν δυναμικά και γρήγορα
11. Εξασφαλίστε τη σύγκλιση αρχιτεκτονικής ασφαλείας που επηρεάζει τη βιωσιμότητα της επιχείρησης
12. Εφαρμογή επικύρωσης εισόδου στη στρώση παρουσίασης και εφαρμογής
13. Εξασφαλίστε και συντηρήστε τις διεπαφές και τα σημεία ενοποίησης με άλλες υπηρεσίες ή εξαρτήματα
14. Εκμεταλλευτείτε τις δραστηριότητες εξομοίωσης για να ανιχνεύσετε το αποτέλεσμα των αλλαγών διαμόρφωσης και να καθορίσετε τη βέλτιστη ρύθμιση. Οπτικοποίηση μπορεί επίσης να προ v ent την εξάπλωση των πιθανών επιθέσεων
15. Χρησιμοποιήστε την κοινωνική μηχανική για να αποκαλύψετε τις συμπεριφορές σε ασύρματα και αισθητήρια περιβάλλοντα
16. Τυποποιήστε το πλαίσιο δοκιμών ασύρματου δικτύου και αισθητήρων (π.χ. ISO / IEC DIS 19637)
17. Δημιουργήστε νέες μεθόδους (π.χ. Fuzzing) για να ανιχνεύσετε πιθανά ελαττώματα
18. Χρησιμοποιήστε ελεύθερα προσβάσιμες βιβλιοθήκες για δραστηριότητες δοκιμών και αξιολόγησης
19. Ανάπτυξη (α) Κακή ανίχνευση, η οποία συγκρίνει καλά γνωστά πρότυπα επίθεσης, (β) Ανίχνευση ανωμαλιών που χαρακτηρίζει κανονική συμπεριφορά και (γ) Ανίχνευση με βάση τις προδιαγραφές, η οποία μετρά αποκλίσεις από τις συνήθεις συμπεριφορές
20. Συγκρίνετε τα δεδομένα ιστορικού δρομολόγησης / τοπολογίας για να υπερασπιστείτε τα ενάντια στις υπερβάσεις και τις αλλοδαπές επιθέσεις

## 8.5. Ταξινόμηση δεδομένων

1. Δημιουργήστε ρόλους για να εκχωρήσετε δικαιώματα σε άτομα ή συσκευές. Περιορισμός πρόσβασης στο δίκτυο με διαχωρισμό δικτύου (VLAN, υποδικτυακό δίκτυο IP, ACL)
2. Να επιβάλλει την περαιτέρω χρήση των αδειών που χορηγούνται από το ρόλο ενός ατόμου ή μιας συσκευής και να παραμένει εντός των ορίων και του σκοπού αυτού του ρόλου
3. Ορίστε τις πολιτικές ταξινόμησης ασφαλείας για δεδομένα και σύνολα τύπων δεδομένων
4. Αξιολογεί τη χρήση τεχνολογιών XML με πρότυπα ανταλλαγής δεδομένων για την υποστήριξη της ολοκλήρωσης και της διαλειτουργικότητας του συστήματος
5. Ενσωματώστε λογικά όρια συλλογής δεδομένων και μεθοδολογίες ανασκόπησης ασφαλείας
6. Να καταστήσει τις οργανώσεις υπεύθυνες για τις πρακτικές απορρήτου τους
7. Ανάπτυξη και διατήρηση εκτενών διαδικασιών διαχείρισης δεδομένων

## 8.6. Διαχείριση και Υποστήριξη

1. Χρησιμοποιήστε ένα συγκεντρωτικό πλαίσιο διαχείρισης για audit λειτουργίες και για την παρακολούθηση τους ανθρώπους, τις διαδικασίες και τα συστήματα
2. Αίτημα άμεσης και άμεσης υποστήριξης από προμηθευτές υλικού ή λογισμικού σε περίπτωση εμφάνισης προβλήματος ή επίθεσης
3. Διατηρήστε ένα επιτυχώς δοκιμασμένο "Σχέδιο Β" σε περίπτωση αποτυχίας ή επίθεσης. Η εναλλακτική λύση θα ήταν κατά προτίμηση εντελώς ανεξάρτητη από την ενεργό λύση / εφαρμογή (σχέδιο αποκατάστασης καταστροφών, σχέδιο συνέχειας των επιχειρήσεων)
4. Δημιουργήστε και διατηρήστε έναν εικονικό χάρτη πραγματικού χρόνου της υποδομής και των διαύλων επικοινωνίας μεταξύ των κόμβων
5. Προγραμματίστε αντίγραφα ασφαλείας ρουτίνας
6. Απενεργοποιήστε ή αλλάξτε τον κωδικό πρόσβασης για κάθε λογαριασμό προεπιλογής / επισκέπτη
7. Εφαρμόστε και δοκιμάστε τις αυτοματοποιημένες ενημερώσεις για firmware / OS / λογισμικό και εφαρμογές διαμορφωμένες για να εξαλείψουν τις αδυναμίες
8. Καθορισμός μοντέλων διαχείρισης για τη διαχείριση (δηλ. ISO / IEC 30100-1: 2016, ISO / IEC DIS 30140-1)
9. Ανάπτυξη και εφαρμογή τυπικών τεχνολογιών διαχείρισης των ενημερώσεων κώδικα, κατάλληλα μέτρα και διαδικασίες και τυποποιημένες τεχνικές ασφαλείας (π.χ. θέματα σχετικά με το χρονοδιάγραμμα, την ιεράρχηση προτεραιοτήτων, τις δοκιμές κατά το σχεδιασμό και την εκτέλεση των διαδικασιών διαχείρισης των διορθώσεων)
10. Σχεδιάστε και εφαρμόστε τα κατάλληλα εργαλεία για τη διαχείριση των χαρακτηριστικών από τους καταναλωτές και εξουσιοδοτήστε τα να είναι αρμόδια για τον εντοπισμό τρωτών σημείων ασφαλείας, πιθανών απειλών ή για τη λήψη αποφάσεων σχετικά με τα δεδομένα τους
11. Διατηρήστε ένα μοντέλο ανάκτησης και ανάκτησης υπηρεσιών
12. Διατυπώστε τα αποδεκτά κριτήρια συμμόρφωσης και τα πρότυπα αξιοπιστίας, ανθεκτικότητας, ασφάλειας και ιδιωτικότητας
13. Εφαρμογή και χρήση ενός συστήματος αποκατάστασης καταστροφών
14. Διατήρηση ασφαλών τρόπων εκκίνησης, διακοπής και αποτυχίας για τα συστατικά έξυπνου δικτύου: τα συστήματα πρέπει να μπορούν να λειτουργούν σε λειτουργική ή μη λειτουργική κατάσταση σύμφωνα με ορισμένες πολιτικές
15. Ανάκτηση επαρκών πληροφοριών πελατών σχετικά με ζητήματα ασφάλειας ή ανησυχίες
16. Περπατήστε τον τρόπο με τον οποίο οι καταναλωτές θα χρησιμοποιούν το δίκτυο ή την υπηρεσία σε μια καθημερινή ρύθμιση για να εντοπίσουν πιθανούς κινδύνους και πιθανά σημεία μαλακής ασφάλειας
17. Διατηρήστε και ενημερώστε ένα απόθεμα με τις πληροφορίες εξουσιοδοτημένου και μη εξουσιοδοτημένου λογισμικού / λειτουργικών συστημάτων / εφαρμογών / συσκευών μέσα στο δίκτυο

18. Διατηρήστε και προστατεύσετε τους κωδικούς πρόσβασης ετικέτες RFID (πρόσβαση, ασφάλεια και σκοτώνουν τους κωδικούς πρόσβασης)? και εγώ διασύνδεση τον πομποδέκτη RFID με έναν διακομιστή back-end ο οποίος διαχειρίζεται αυτούς τους κωδικούς πρόσβασης
19. Εφαρμόστε την ασφάλεια των συστημάτων αναγνώρισης RFID και των συστημάτων RFID μεσαίας τάξης
20. Επιλέξτε μια κατάλληλη τοποθέτηση ετικετών RFID και αναγνωστών. Επίσης, προστατεύστε τους αναγνώστες RFID με ηλεκτρομαγνητικές θωρακισμένες σήραγγες
21. Όλα τα συστήματα και συσκευές θα πρέπει να έχουν προστατεύσει ή να σταματήσουν οποιαδήποτε περιττή υπηρεσία, διαδικασία ή θύρα / πρίζα (σκλήρυνση OS, κανόνες τείχους προστασίας)
22. Αποτρέψτε τις συσκευές δικτύου να χρησιμοποιούν προγράμματα autorun για πρόσβαση σε αφαιρούμενα μέσα
23. Βεβαιωθείτε ότι όλα τα ασύρματα σημεία πρόσβασης είναι διαχειρίσιμα χρησιμοποιώντας εργαλεία διαχείρισης της επιχείρησης
24. Συγκρίνετε τις παραμέτρους των συσκευών δικτύου με τα πρότυπα για κάθε τύπο συσκευής
25. Προσδιορίστε προσεκτικά και διαχωρίστε τα κρίσιμα δεδομένα από πληροφορίες που είναι άμεσα διαθέσιμες στους χρήστες του εσωτερικού δικτύου
26. Ελέγξτε την πρόσβαση των διαδικασιών και των χρηστών σε πόρους και / ή υπηρεσίες
27. Harde n τα στοιχεία δικτύου (δηλαδή κλειστό πρωτόκολλο SNMP για Σημείο Πρόσβασης (AP) ή επιτρέπουν SNMPv3)
28. Απασχόληση και ελεγχόμενη διαχείριση (δηλ. Απενεργοποίηση διεπαφής HTTP σε σημείο πρόσβασης (AP) ή ενεργοποίηση HTTPS)
29. συνθέσεων του ηλεκτρονικού ο αριθμός καναλιού και η έξοδος ισχύος του σημείου πρόσβασης (AP)
30. Εφαρμόστε τις βέλτιστες πρακτικές σχετικά με τη διαμόρφωση (π.χ. αποφύγετε το προεπιλεγμένο όνομα SSID στα AP)
31. Χρησιμοποιήστε δυνατό μηχανισμό ασφαλείας (δηλ. Αποφύγετε τη χρήση προ-κοινόχρηστων κλειδιών (PSK))
32. Χρησιμοποιήστε ελέγχους ασφαλείας (π.χ. χρήση των λιστών ελέγχου πρόσβασης MAC (MAC ACL) στα AP)
33. Εφαρμόστε τις βέλτιστες πρακτικές ρύθμισης διαμόρφωσης (δηλ. Χρησιμοποιήστε το πρωτόκολλο Dynamic Host Control Protocol (DHCP) για την εκχώρηση IP)
34. Συμμορφωθείτε με τη στρατηγική διαμόρφωσης (δηλαδή μέγιστο χρονικό διάστημα φάρου (ανακοινώσεις θέσης) στα AP)
35. Αποτρέψτε τη μη εξουσιοδοτημένη διαχείριση u (π.χ. αποτρέψτε την μη εξουσιοδοτημένη επαναφορά των σημείων πρόσβασης (AP))
36. Ελέγξτε μια πρόσβαση στις πληροφορίες RFID
37. Ζητήστε χειροκίνητα και επιτρέψτε τη σύνδεση των συσκευών STA (συσκευή με ασύρματη διασύνδεση) με ένα σημείο πρόσβασης (AP)

## 8.7. Διαχείριση κινδύνου

1. Χρησιμοποιήστε μοντέλο απειλών και αξιολόγηση κινδύνου
2. Δημιουργία, συντήρηση και ενημέρωση μιας βάσης γνώσεων απειλών
3. Ορίστε ως αδιάκριτη ομάδα ατόμων που είναι υπεύθυνα για την πρόληψη των επιθέσεων και την ανάκτηση από αυτά
4. Ευθυγράμμιση της στρατηγικής ασφάλειας με τη στρατηγική της συνολικής πληροφορικής της επιχείρησης με βάση το καθορισμένο προφίλ κινδύνου
5. Εφαρμογή δοκιμής ελέγχου και ευπάθειας σάρωσης εξαρτημάτων τρίτων που ενσωματώνονται ή χρησιμοποιούνται από το δίκτυο
6. Μειώστε τους κινδύνους με τις τεχνολογίες διαχείρισης των ενημερώσεων κώδικα (π.χ. τροποποιήσεις των ενημερωμένων εκδόσεων κώδικα, κατάχρηση διαπιστευτηρίων, ευπάθειες) και αποφυγή καταστάσεων υπερφόρτωσης πόρων, πείνας πόρων, συμφόρησης δικτύου κλπ.

7. Φροντίστε να ενημερώνεστε μέσω των φόρουμ ασφαλείας και των λιστών αλληλογραφίας (π.χ. bugtraq) για τις τελευταίες απειλές από αξιόπιστες πηγές ασφαλείας
8. Ενδυναμώστε τη τυποποιημένη αξιολόγηση της απόδοσης για τη μείωση των κινδύνων και να βελτιώσει την ελαστικότητα της υπηρεσίας
9. Αναλύστε λεπτομερώς τους κινδύνους της λύσης και τη διατήρηση της συλλογής δεδομένων
10. Καταγράψτε την αρχιτεκτονική και τη διαμόρφωση των ασύρματων και αισθητήρων ad-hoc. εντοπίστε και ελέγξτε κρίσιμα στοιχεία και υπηρεσίες που απαιτούν πρόσθετα επίπεδα προστασίας
11. Δημιουργήστε μαύρες λίστες (γνωστές κακόβουλες λίστες IP) και λευκές λίστες (έγκυρη λίστα IP) και, κατά συνέπεια, απορρίψτε ή επιτρέψτε την πρόσβαση
12. Εκτελέστε την ασφάλεια χρησιμοποιώντας ένα οικονομικό μοντέλο
13. Εφαρμογή ενός ειδικού τομεακού κανονισμού (π.χ. ειδικός για τον πολίτη ή πολυκεντρικό κανονισμό)
14. Ανάπτυξη μοντέλων για τη συλλογή πληροφοριών και τη διαμόρφωση επίθεσης κοινωνικής μηχανικής
15. Προωθήστε και ενθαρρύνετε την κουλτούρα που έχει επίγνωση της ασφάλειας μέσα στον οργανισμό

## 8.8. Εξειδικευμένα εργαλεία και τεχνικές

1. Χρησιμοποιήστε τείχος προστασίας, λογισμικό προστασίας από σκουλήκια και λογισμικό προστασίας από ιούς σε όλες τις συσκευές, αν είναι δυνατόν. Επιπλέον, το τείχος προστασίας προστατεύει οποιαδήποτε εφαρμογή Ιστού, διεπαφή ή API
2. Χρήση συστημάτων ασύρματης ανίχνευσης εισβολής (WIDS); επίσης, η χρήση ελέγχου χαμηλού επιπέδου πακέτων στην κάλυψη WIDS είναι όπως προτείνεται από το πρότυπο ISO / IEC / IEEE P21451-1-4
3. Αφήστε τη θέση των κόμβων που είναι διατεταγμένα σε πλέγμα (λιγότερη ανάγκη για διαφήμιση των πληροφοριών θέσης)
4. Χρησιμοποιήστε τη δρομολόγηση πολλαπλών διαδρομών κατά επιλεκτικών προσβολών προώθησης. Επιλέγοντας πιθανότατα το επόμενο λυκίσκο, μειώνετε τους κινδύνους και εμποδίζετε τον συμβιβασμένο κόμβο να αποκτήσει τον έλεγχο
5. Απορρίψτε τις ληφθείσες κλήσεις / SMS / MMS / e-mail από άγνωστους παραλήπτες
6. Υπογραφή κώδικα για την επαλήθευση των ταυτοτήτων στους χρήστες του κώδικα (και να αποφασίσετε αν θα εγκαταστήσετε ή όχι το λογισμικό)
7. Σχεδιάστε και διατηρήστε πρωτόκολλα δρομολόγησης βασισμένα σε επίπεδο, ιεραρχικά, βάσει τοποθεσίας και ιεραρχικά δρομολόγια για να υπερασπιστείτε τις επιθέσεις από σκουληκότρυπες και καταβόθρες
8. (S-MAC, T-MAC, B-MAC ή G-MAC) και να αποτρέψει την είσοδο του κόμβου WSN στην κατάσταση αναστολής.
9. Ανάπτυξη στρατηγικής ασφάλειας στον κυβερνοχώρο γύρω από το πρότυπο ασφαλείας IEC 62351
10. Εφαρμογή φιλτραρίσματος δεδομένων εξόδου για περιορισμένους χαρακτήρες
11. Εφαρμόστε ελέγχους ασφαλείας και προληπτικά αντίμετρα (π.χ. περιορισμό του ρυθμού) που μειώνουν τον κίνδυνο DoS ή αυτοματοποιημένων επιθέσεων
12. Χρησιμοποιήστε το ελαφρύ ασφαλές μηχανισμό για να υπερασπιστείτε τις επιθέσεις DOS με βάση το Path. Μια νέα αλυσίδα κατακερματισμού χρειάζεται και επαληθεύεται κάθε φορά. Σε περίπτωση που ο αριθμός δεν επαληθευτεί, τότε το πακέτο έχει πέσει
13. Χρησιμοποιήστε πρωτόκολλα ελέγχου πρόσβασης της επόμενης γενιάς και ορισμούς API (NGAC-FA, NGAC-GOADS, INCITS 499, SP 800-178 κ.λπ.)
14. Χρησιμοποιήστε Leach Packet, το οποίο επιτρέπει σύνδεση μεταξύ δύο μη γειτονικών κακόβουλων κόμβων, για την ανίχνευση επιθέσεων από σκουληκότρυπα, όπου χρειάζεται
15. Αποτρέψτε τις επιθέσεις Sybil περιορίζοντας τον αριθμό των γειτόνων που μπορεί να έχει ένας κόμβος και στέλνοντας ένα μήνυμα σφάλματος

16. Χρησιμοποιήστε το παζλ Spread Spectrum και Cryptographic για να προστατεύσετε το δίκτυο από εξωτερικές επιθέσεις Jamming. Για την αποφυγή προσβολών εμπλοκής στο εσωτερικό μοντέλο, μπορεί να χρησιμοποιηθεί το πακέτο που κρύβεται πριν από την ταξινόμηση του πακέτου
17. Χρησιμοποιήστε ένα δίκτυο επικάλυψης στο οποίο ο σταθμός βάσης πρέπει να αλλάζει συχνά. Κατά συνέπεια, η αλλαγή ή η αντικατάσταση των σταθμών βάσης καθιστά πιο δύσκολη τη συμβιβασμό αυτών των κόμβων. Εναλλακτικά, η χρήση σταθμών βάσης Long-Term Evolution (LTE) και Long-Term Evolution-Advanced (LTE-A)
18. Χρησιμοποιήστε αλγορίθμους κουτσομπολιού για να μειώσετε τις συγκρούσεις και το κόστος μηνυμάτων
19. Χρησιμοποιήστε τις κατάλληλες μεθόδους (π.χ. σαρωτής ευπάθειας, σαρωτή ασφάλειας, ανιχνευτή ανοιχτής θύρας)
20. Εφαρμόστε την επαλήθευση διεύθυνσης b, όπου διατίθενται αρκετές συνδέσεις L2 στις ρυθμίσεις ελεγκτή / ακτίνων και συνεχώς επικυρώνει τη συνδεσιμότητα. Ανάπτυξη του αναμενόμενου αριθμού μετάδοσης (ETX) με το πρωτόκολλο MESH-LINK (HELLO Flood Attacks και ACK Spoofing Attacks)
21. Χρησιμοποιήστε τη μέθοδο over-coding στην επικοινωνία RFID
22. Ανάπτυξη κόμβων αισθητήρων που διαθέτουν προστατευτικό μηχανισμό προστασίας από ραδιοσυχνότητες
23. Χρησιμοποιήστε ετικέτες με ένα διακόπτη "πατήστε για ενεργοποίηση"
24. Εφαρμόστε την ψηφοφορία σε μικρά χρονικά διαστήματα
25. Χρησιμοποιήστε γεωγραφικές πληροφορίες για τον έλεγχο ροής ή απομονώστε κόμβους που λαμβάνουν κίνηση πάνω από ένα συγκεκριμένο όριο ή επιτρέψτε να λαμβάνετε και να διαβιβάζετε μόνο αξιόπιστα δεδομένα ή να λαμβάνετε δυναμικά το επόμενο hop από ένα σύνολο υποψηφίων (Geographic Routing Protocol)
26. Χρησιμοποιήστε επικυρωμένες αναγνωρίσεις από άκρο σε άκρο και συγχρονισμό συγχρονισμένου χρόνου κατά της επίθεσης Sybil και μαζική πλημμύρα απαντήσεων
27. Επιβολή διαχείρισης k ey και bootstrapping (δηλαδή συμβολικά με βάση προ-διαμόρφωση των πλήκτρων κατά τη διάρκεια της κατασκευής των κόμβων, φυσική προστασία των μηνυμάτων, στη ζώνη κατά τη διάρκεια ενός set-up φάση αδύναμη ασφάλειας, out-of-band επικοινωνίας)
28. Εφαρμόστε τη δρομολόγηση με πληροφορίες ανάδρασης που περιλαμβάνουν τις πληροφορίες καθυστέρησης, εμπιστοσύνης, θέσης, πλεονάζουσας χωρητικότητας στα πλαίσια αναγνώρισης του στρώματος ελέγχου πρόσβασης πολυμέσων (MAC)
29. Χρησιμοποιήστε το ξυπνητήρι και βεβαιωθείτε ότι έχετε ξεκινήσει την εκκίνηση για να αποτρέψετε μια ειδική κατηγορία επιθέσεων άρνησης εξυπηρέτησης, τις αποκαλούμενες επιθέσεις στέρησης ύπνου
30. Διαδικασία και σύγκριση πληροφοριών δρομολόγησης σύνδεσης-ρευμάτων που λαμβάνονται από διαφορετικούς χρήστες ή υποστήριξη έμμεσων ανταλλαγών επικοινωνιών μεταξύ μη γειτονικών φορέων δρομολόγησης για την παροχή δευτερεύοντος καναλιού για την πραγματοποίηση επικύρωσης πληροφοριών διαδρομής διανύσματος αποστάσεων (επίθεση πλαστογράφησης δεδομένων αίσθησης φάσματος)
31. Παροχή μηχανισμών για μηνύματα unicast. να επιβάλλουν μηχανισμούς που προστατεύουν μηνύματα μεταξύ ενός σημείου εξυπηρέτησης και ενός μόνο κινητού κόμβου ή διανέμοντας κλειδιά ομάδας σχετικά με μηνύματα πολλαπλής διανομής (δηλ. τις τροπολογίες 2 και 4 του IEEE 802.21)
32. Χρησιμοποιήστε έναν μηχανισμό παρακολούθησης μηνυμάτων (MoM)
33. Προσέγγιση μιας επαναλαμβανόμενης θεωρίας παιχνιδιών και μιας θεωρίας Bayesian Game για την υπεράσπιση των επιθέσεων DoS
34. Εφαρμογή διεύθυνσης με βάση την ισχύ του σήματος και ανάπτυξη ενός Ant-Based Framework για την υπεράσπιση των επιθέσεων DoS
35. Ενσωματώστε τις απαιτήσεις ασφαλείας μέσα στην αρχιτεκτονική των λειτουργικών συστημάτων εφαρμόζοντας πλαίσια διαχείρισης της ασφάλειας

36. Ανάπτυξη κατανεμημένων αλγορίθμων για την ανίχνευση επιθέσεων θραύσης που δεν χρησιμοποιούν κρυπτογράφηση (δηλαδή καθόλου χρόνο επιβάρυνσης) ή επιπλέον κινητούς κόμβους και χρήση των πληροφοριών συνεργασίας των γειτονικών κόμβων
37. Κάλυψη ή απόκρυψη κόμβων αισθητήρων
38. Χρησιμοποιήστε τον τυχαίο πολυκάναλο ή τη γραμματοσειρά επιλεγμένο Multicast για να αποτρέψετε τις επιθέσεις αναπαραγωγής κόμβων
39. Επιλέξτε πρωτόκολλα δρομολόγησης, όπως το Ariadne, το *Secure Effective ad-hoc Distance vector (SEAD)* και το *Authenticated Routing για δίκτυο ad-hoc (ARAN)*

| THREAT GROUP | THREAT | GOOD PRACTICES | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | CPNI | ITU | IEC | FTC | GSMA | SECURING SMART CITIES | NIST | Q-CERT | SANDIA | OTHER |
| **Unintentional damage / loss of information or IT assets** | Inadequate design and planning / improper adaptation | [8.3].1, [8.4].1, [8.5].1, [8.6].1-5, [8.6].14, [8.7].1-3, [8.7].15 | | | | | [8.3].1, [8.4].1, [8.4].3, [8.6].1-3, [8.6].14, [8.7].1 | [8.7].15 | [8.3].1, [8.5].1, [8.6].1, [8.6].3-5, [8.7].2-3, [8.7].15 | | |
| | Using information from unreliable source | [8.3].1, [8.4].3, [8.6].2, [8.6].6-7, [8.6].14, [8.6].21-22, [8.7].2, [8.7].11, [8.7].15, [8.8].1 | | | | | [8.3].1, [8.4].3, [8.6].2, [8.6].6-7, [8.6].14, [8.6].21 | [8.3].1, [8.6].6-7, [8.6].21, [8.7].15, [8.8].1 | [8.3].1, [8.4].3, [8.6].6-7, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5 | | |
| | Loss of devices | [8.3].1-2, [8.6].2-4, [8.6].14 | | | | | [8.3].1-2, [8.6].2-3 | [8.3].1-2, [8.6].20 | [8.3].1-2, [8.6].4 | | |
| | Loss of information in the cloud | [8.1].1, [8.3].1, [8.4].3, [8.5].1, [8.6].5-6, [8.7].2, [8.7].15 | | | | | [8.1].1, [8.3].1, [8.4].3, [8.6].6 | [8.1].1, [8.3].1, [8.6].6, [8.7].15 | [8.1].1, [8.3].1, [8.4].3, [8.5].1, [8.6].5, [8.7].2, [8.7].15 | | |
| | Damage caused by third party | [8.1].1, [8.2].1, [8.3].1, | | | | | [8.1].1, [8.2].1, [8.3].1, | [8.1].1, [8.2].1, [8.3].1, | [8.1].1, [8.2].1, [8.3].1 | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | [8.4].3, [8.5].5, [8.6].5-7, [8.6].14, [8.6].21, [8.7].2, [8.7].11, [8.7].15, [8.8].1 | | | | | [8.4].3, [8.6].6-7, [8.6].14, [8.6].21 | [8.5].5, [8.6].6-7, [8.6].21, [8.7].15, [8.8].1 | [8.4].3, [8.5].5, [8.6].5-7, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5 | | |
| **Disaster (natural, environmental)** | Water | [8.3].1, [8.6].2-5, [8.7].2 | | | [8.4].13 | [8.3].1, [8.6].11, [8.7].1 | [8.3].1, [8.6].2-3, [8.7].1 | [8.3].1 | [8.3].1, [8.6].3-5, [8.7].2 | | [8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15 |
| | Wildlife | [8.3].1, [8.6].2-5, [8.7].2 | | | [8.4].13 | [8.3].1, [8.6].11, [8.7].1 | [8.3].1, [8.6].2-3, [8.7].1 | [8.3].1 | [8.3].1, [8.6].3-5, [8.7].2 | | [8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15 |
| | Explosion | [8.3].1, [8.6].2-5, [8.7].2 | | | [8.4].13 | [8.3].1, [8.6].11, [8.7].1 | [8.3].1, [8.6].2-3, [8.7].1 | [8.3].1 | [8.3].1, [8.6].3-5, [8.7].2 | | [8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | [8.7].15 |
| | Thunder strike | [8.3].1, [8.6].2-5, [8.7].2 | | | [8.4].13 | [8.3].1, [8.6].11, [8.7].1 | [8.3].1, [8.6].2-3, [8.7].1 | [8.3].1 | [8.3].1, [8.6].3-5, [8.7].2 | | [8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15 |
| | Natural disasters | [8.3].1, [8.6].2-5, [8.7].2 | | | [8.4].13 | [8.3].1, [8.6].11 | [8.3].1, [8.6].2-3 | [8.3].1 | [8.3].1, [8.6].3-5, [8.7].2 | | [8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15 |
| | Fire | [8.3].1, [8.6].2-5, [8.7].2 | | | | [8.3].1, [8.6].11 | [8.3].1, [8.6].2-3 | [8.3].1 | [8.3].1, [8.6].3-5, [8.7].2 | | [8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15 |
| **Legal** | Unauthorized use of intellectual property rights (IPR) protected resources | | [8.6].1, [8.6].26 | | | | | | | | [8.8].35 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Abuse of personal data | | [8.2].9-10, [8.6].26 | | | | | | | | [8.1].19, [8.2].13 |
| | Violation of rules and regulations | | | | | | | | | | [8.7].13 |
| | Internet outage | [8.2].1, [8.3].1-3, [8.4].1, [8.4].3, [8.5].1, [8.5].5-6, [8.6].3, [8.6].6, [8.7].15, [8.6].22, [8.7].11, [8.8].1-2 | | | [8.1].1, [8.2].1, [8.4].13, [8.5].5-7, [8.6].16, [8.7].5, [8.7].7, [8.7].15, [8.8].11 | [8.1].1, [8.1].12-13, [8.2].1, [8.2].3-4, [8.4].3, [8.5].3, [8.6].8, [8.6].15, [8.8].10-11 | [8.1].1, [8.2].1, [8.3].1-2, [8.4].1, [8.4].3, [8.6].3, [8.6].6, [8.6].21 | [8.1].1, [8.1].14, [8.2].1-2, [8.2].6-7, [8.2].16, [8.3].1-3, [8.4].5-7, [8.5].4-6, [8.6].32-33, [8.6].35, [8.7].6, [8.7].15, [8.8].1, [8.8].13, [8.8].19 | [8.1].1, [8.2].1, [8.3].1-3, [8.4].3, [8.5].1-2, [8.5].5, [8.6].3, [8.6].6, [8.7].15, [8.8].1 | [8.3].3, [8.3].5, [8.4].16 | [8.1].1, [8.2].1-5, [8.3].1, [8.3].3, [8.4].2-4, [8.4].13, [8.5].7, [8.6].3, [8.6].15, [8.7].6, [8.7].15, [8.8].8, [8.8].12, [8.8].17-18, [8.8].20 |
| | Network outage | [8.3].1-2, [8.4].1, [8.4].3, [8.5].2, [8.6].1-2, [8.6].6, [8.6].14 | | [8.1].6 | [8.1].8-9, [8.2].1, [8.4].13, [8.6].10, [8.7].5, [8.7].7 | [8.1].6-7, [8.1].10, [8.1].12-13, [8.2].4, [8.6].8 | [8.3].1-2, [8.4].3, [8.6].1-2, [8.6].6 | [8.1].7, [8.1].14, [8.2].1, [8.3].1-2, [8.4].5-7, [8.6].27-34, [8.6].37 | [8.3].1-2, [8.4].3, [8.5].2, [8.6].6 | [8.3].4 | [8.1].2, [8.1].4-7, [8.2].4-5, [8.3].1, [8.3].5-7, [8.4].2-4, [8.4].13, [8.6].27, [8.7].10, [8.8].3-4, [8.8].14-15 |
| | Loss of support services | [8.3].1, [8.4].1, | | | [8.1].1, [8.4].13, | [8.1].1, | [8.1].1, [8.3].1-2, | [8.1].1, [8.1].14, | [8.1].1, [8.3].1-2, | [8.3].4, [8.4].14 | [8.1].1, [8.2].3-5, |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | [8.4].3, [8.6].1, [8.6].14 | | | [8.7].5, [8.7].7 | [8.1].12-13, [8.2].3, [8.6].8, [8.6].11 | [8.4].3, [8.6].1 | [8.2].6-7, [8.3].1-2, [8.4].4-7, [8.7].6, [8.7].8, [8.2].16, [8.8].5 | [8.4].3, [8.6].1 | | [8.3].1-2, [8.3].5-7, [8.4].2-4, [8.4].13, [8.7].6, [8.7].10, [8.8].15, [8.8].17, [8.8].25-26 |
| **Nefarious activity / abuse** | Unauthorized activities | | [8.1].15 | [8.2].11 | | | | [8.1].1 | | | |
| | Manipulation of information | | [8.1].16 | | | | | [8.1].1 | | | [8.2].14, [8.2].17-18 [8.8].39 |
| | Malicious code / software / activity | | [8.6].17, [8.6].21-22 | | | | | | | | [8.1].17-18 |
| | Manipulation of hardware and software | | [8.6].7, [8.6].23-24 | [8.8].7, [8.8].27-28 | | | | [8.8].31 | | | [8.1].22-23, [8.2].15, [8.2].20, [8.3].11, [8.4].20, [8.8].4, [8.8].38 |
| | Misuse of audit tools | | [8.3].10, [8.6].1, [8.6].25 | | | | | | | | [8.3].9 |
| | Remote activity | | [8.6].17, [8.6].21-22 | | | | | | | | [8.8].4, [8.8].36 |
| | Targeted attacks | | [8.6].17, [8.6].21 | [8.2].12 | | | | | | | [8.8].30 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Denial of service | | | [8.8].29 | | | | | | | [8.2].17, [8.3].8, [8.7].12, [8.8].20, [8.8].32-34 |
| | Social Engineering | | [8.2].8, [8.3].10, [8.8].1 | | | | | | | | [8.7].14 |
| **Eavesdropping, Interception, Hijacking** | Network Reconnaissance | [8.3].1, [8.3].3, [8.5].1, [8.6].6, [8.6].14, [8.6].21, [8.7].2, [8.7].15, [8.8].1-2 | | | | | [8.3].1, [8.6].6, [8.6].14, [8.6].21 | [8.1].14, [8.3].1, [8.3].3, [8.6].6, [8.6].21, [8.6].31, [8.8].1, [8.8].24 | [8.3].1, [8.3].3, [8.5].1, [8.7].2, [8.7].15, [8.8].1, [8.8].5 | | [8.2].4, [8.8].4, [8.8].25 |
| | Interception of information | [8.2].1, [8.3].1, [8.3].3, [8.5].1, [8.6].1, [8.6].5-6, [8.6].14, [8.6].21, [8.7].2, [8.7].15, [8.8].1-2 | | | | | [8.2].1, [8.3].1, [8.6].1, [8.6].6, [8.6].14, [8.6].21 | [8.1].14, [8.2].1, [8.2].6, [8.2].8, [8.3].1, [8.3].3, [8.5].5, [8.6].6, [8.6].18-21, [8.6].27-32, [8.6].34-37, [8.8].1, [8.8].21, [8.8].23 | [8.2].1, [8.3].3 [8.4].3, [8.5].1, [8.6].1, [8.6].5-7, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5 | | [8.2].4, [8.2].16, [8.8].20 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Intercepting compromising emissions | [8.3].1-3, [8.5].1, [8.6].1, [8.6].5-7, [8.6].14, [8.6].21, [8.7].2, [8.7].15, [8.8].1-2 | | | | | [8.2].1, [8.3].1-2, [8.6].1, [8.6].6-7, [8.6].14, [8.6].21 | [8.1].14, [8.2].1, [8.2].8, [8.3].1-3, [8.6].6-7, [8.6].19-21, [8.6].27-32, [8.6].34-37, [8.8].1, [8.8].21-24 | [8.2].1, [8.3].1-3, [8.4].3, [8.5].1, [8.6].1, [8.6].5-7, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5 | | [8.2].4, [8.2].16, [8.8].3, [8.8].20 |
| | Man-in-the-middle / Session hijacking | [8.2].1, [8.3].1, [8.3].3, [8.5].1, [8.6].6, [8.6].14, [8.6].21, [8.7].15, [8.7].2, [8.8].1-2 | | [8.2].11 | | | [8.2].1, [8.3].1, [8.6].6, [8.6].14, [8.6].21, | [8.1].14, [8.2].1, [8.2].6, [8.2].8, [8.3].1, [8.3].3, [8.6].6, [8.6].21, [8.6].27, [8.6].31, [8.6].35, [8.8].1, [8.8].21, [8.8].24 | [8.2].1, [8.3].1, [8.3].3, [8.4].3, [8.5].1, [8.6].6, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5 | | [8.2].4, [8.2].16, [8.8].4 |
| **Failures / Malfunction** | Failure or disruption of communication links | [8.3].1, [8.6].3 | | [8.4].1, [8.4].9 | [8.6].10, [8.7].7 | | [8.3].1, [8.6].3 | [8.3].1, [8.4].6-9, [8.6].18-25, [8.6].36, [8.8].21-24 | [8.3].1, [8.6].3-4 | | [8.3].1, [8.4].1, [8.4].6, [8.6].3, [8.6].13, [8.8].16 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Failure of devices or systems | [8.3].1, [8.6].3, [8.6].14, [8.6].22 | | [8.4].1, [8.4].9, [8.4].12 | [8.4].17, [8.6].10 | [8.4].16, [8.6].8 | [8.3].1, [8.6].3, [8.6].7, [8.6].14 | [8.3].1, [8.4].6, [8.4].9, [8.4].18, [8.6].12, [8.7].6 | [8.3].1, [8.6].3-7 | | [8.3].1, [8.4].1, [8.4].6, [8.4].9, [8.6].3, [8.6].13-14, [8.7].6, [8.8].6-7 |
| | Malfunction of equipment | [8.3].1, [8.6].3, [8.6].14 | | [8.4].9 | [8.4].17, [8.6].6, [8.6].10 | [8.4].16 | [8.3].1, [8.6].3, [8.6].14 | [8.3].1, [8.4].5-6, [8.4].9, [8.4].10, [8.4].18, [8.6].12 | [8.3].1, [8.6].3-5 | | [8.3].1 [8.4].6, [8.4].9, [8.6].3, [8.6].13-14 |
| | Failure or disruption of main supply | [8.3].1, [8.6].3, [8.6].14 | | [8.4].9 | | | [8.3].1, [8.6].3, [8.6].14 | [8.3].1, [8.4].6, [8.4].9, [8.6].12 | [8.3].1, [8.6].3-4 | | [8.3].1, [8.4].6, [8.4].9, [8.6].3, [8.6].13-14 |
| **Physical attack** | Terrorist attack | | | | | | | | | | |
| | Damage from the warfare | | | | | | | | | | |
| | Unauthorized physical access | | | | | | | | | | [8.4].19, [8.8].37 |
| | Theft | | | | | | | | | | |
| | Vandalism | | | | | | | | | | [8.1].21 |
| | Sabotage | | | | | | | | | | [8.8].22 |

# 9. Ανάλυση κενού

Τα ad hoc και τα δίκτυα αισθητήρων αποτελούνται κυρίως από κατανεμημένους κόμβους επεξεργασίας κρίσιμης, ευαίσθητης, μάζας και πολλών άλλων τύπων δεδομένων. Επιπλέον, αυτοί οι κόμβοι σχηματίζουν συχνά δυναμικές τοπολογίες και ενσωματώνουν μεταβαλλόμενα χαρακτηριστικά, όπως υψηλή κινητικότητα και κυμαινόμενο εύρος ζώνης. Αυτά τα χαρακτηριστικά μαζί με τη μετάδοση δεδομένων ροής σε πραγματικό χρόνο, τον χαμηλό ενεργειακό εφοδιασμό, τη χαμηλή ισχύ επεξεργασίας, τα πρωτόκολλα δρομολόγησης και τα συστήματα επαλήθευσης ταυτότητας θα μπορούσαν να δημιουργήσουν αρκετές ανησυχίες για την ασφάλεια.

Μπορεί επίσης να προκύψουν διάφορες ανησυχίες σχετικά με την ασφάλεια όσον αφορά τα ενσωματωμένα εξαρτήματα που χρησιμοποιούνται στους αισθητήρες. Συνήθως, τα PLC μπορούν να διαβάζουν σήματα από διαφορετικούς αισθητήρες, και η ενσωμάτωση των αισθητήρων με τα PLC στα συστήματα ελέγχου εποπτείας και εξαγοράς δεδομένων (SCADA) - που αποσκοπούν στη βελτιστοποίηση του επιπέδου παραγωγής - πρέπει να εξεταστούν διεξοδικά λαμβάνοντας υπόψη τυχόν απειλές και κινδύνους για την ασφάλεια. Για παράδειγμα, η ηλεκτροδότηση και η υδροδότηση των πόλεων θα μπορούσαν να διακινδυνεύσουν, εάν δεν εξετάσουμε σε διαρκή βάση όλα τα κατάλληλα και αποτελεσματικά αντίμετρα ασφαλείας. Στο ίδιο πλαίσιο, η ένταξη των ad-hoc και αισθητήρα δίκτυα σε οικιακές συσκευές επιτρέπει την απομακρυσμένη διαχείριση των σπιτιών και προσφοράς s αυξημένη ευελιξία · Ωστόσο, υπάρχουν διάφορες ανησυχίες για την ασφάλεια των έξυπνων αντικειμένων και τις συνδεδεμένες συσκευές (π.χ. συστήματα οικιακού αυτοματισμού, έξυπνες τηλεοράσεις και ψυγεία) που απειλούν τη διασύνδεση στο διαδίκτυο των σπιτιών, λόγω της ευπάθειας ασφαλείας και τα ζητήματα προστασίας των προσωπικών δεδομένων. Σε περιβάλλοντα υγειονομικής περίθαλψης (π.χ. νοσοκομεία), η σύντηξη αισθητήρων σε κλινικές λειτουργίες που στοχεύουν στην παρακολούθηση των φυσιολογικών ζωτικών σημείων των ασθενών οδηγεί σε κρίσιμες τεχνικές και νομικές παραμέτρους, όπως είναι οι επιχειρηματικοί και τεχνικοί περιορισμοί στην εφαρμογή και οι ρυθμιστικές αναθεωρήσεις. Για παράδειγμα, ένας ασθενής έχει το δικαίωμα να γνωρίζει τα ονόματα όλων των εργαζομένων ο οποίος μπορεί να έχει πρόσβαση στα ιατρικά αρχεία, αλλά από την άλλη στις περιπτώσεις "break-the-glass" και κρίσιμων για τη ζωή πράξεων, ο μέσος χρόνος διαβούλευσης θα πρέπει να είναι σημαντικά μικρότερος.

Στόχος της τρέχουσας ανάλυσης των κενών είναι να προσδιοριστεί η πορεία προς τη βελτιστοποίηση των αντιμέτρων και να καθοριστούν συγκεκριμένοι στόχοι στόχοι που έχουν τεθεί από τη βιομηχανία, την ακαδημαϊκή κοινότητα και το ερευνητικό έργο των εμπειρογνωμόνων στον τομέα της ασφάλειας (π.χ. Black Hat Conferences) και πόρους για τη βελτίωση της ασφάλειας και την παροχή καλύτερης προστασίας. Η ανάλυση του κενού πραγματοποιείται και στις πέντε περιοχές της λειτουργικής αρχιτεκτονικής του M2M ( βλ Εικόνα 4 Αρχιτεκτονική M2M ): 1) Μια εφαρμογή D omain, 2) Τομέας Συσκευής, 3) Τομέας Δικτύου, 4) Operational Domain, και 5) P roduct / επιχειρηματικές διαδικασίες Domain.

## 9.1. Κενά στο πεδίο της συσκευής

Στην περίπτωση της RFID, οι ετικέτες RFID εκτίθενται σε ορισμένες απειλές, όπως οι επιθέσεις "άνθρωπος στη μέση" (βλ. 5.6.3) και εργαλεία όπως το Thastic RFID Thief. Η ενορχήστρωση της μεθόδου κωδικοποίησης κάλυψης, ο διακόπτης τύπου ενεργοποίησης και οι πρακτικές μορφοποίησης μη αναγνωρίσιμων μορφών ( βλ. 8.2, 8.8)

μετριάζουν αυτές τις απειλές. Έτσι, η προσοχή των εισβολέων εκτρέπεται προς τους αναγνώστες RFID για τη διεξαγωγή πολλών επιθέσεων με τη χρήση συνδυασμών ευπάθειας (βλ. 5.6.3).

Μια άλλη κοινή πρακτική που οδηγεί σε αναδυόμενες προκλήσεις ασφάλειας στο πλαίσιο της RFID είναι ο έλεγχος πρόσβασης στις πληροφορίες RFID (βλέπε 8.6). Πολλοί αναγνώστες RFID χρησιμοποιούν το πρωτόκολλο Wiegand για επικοινωνία με τις συσκευές που βρίσκονται σε προηγούμενη ροή. Ωστόσο, το Gecko και το BLEkey εκμεταλλεύονται τις ευπάθειες του πρωτοκόλλου Wiegand και κατάφεραν να εκτελέσουν παθητικές επιθέσεις με παραβίαση των μεταδιδόμενων πληροφοριών ελέγχου πρόσβασης. Το πιο πρόσφατο σύστημα διείσδυσης s διευκολύνει την υποκλοπή των δεδομένων RFID κατά τη μεταφορά, και θα μπορούσε να ελέγχεται εξ αποστάσεως μέσω Bluetooth Low Energy (BLE). Αυτά τα συστήματα πρέπει να τοποθετούνται στους αναγνώστες RFID για να μπορούν να εκτελούν τις κακόβουλες δραστηριότητές τους. Για το σκοπό αυτό, όχι μόνο η παρακολούθηση των σημείων πρόσβασης πρέπει να είναι συνεχής, αλλά και αυστηρή πρόσβαση στο σύστημα παρακολούθησης. Αυτή η ανάγκη έχει μεγάλη αξία, διότι η επιτυχία αυτών των επιθέσεων εξαρτάται από το αν ο εισβολέας μπορεί να παραβιάσει το σύστημα παρακολούθησης ως ένα ενδιάμεσο στάδιο στην εκμετάλλευση των συσκευών ανάγνωσης RFID.

## 9.2. Κενά στο δίκτυο

Είναι προφανές ότι μια λύση ανίχνευσης εισβολής δεν μπορεί να εφαρμοστεί για κάθε κόμβο ενός ad-hoc και δικτύου αισθητήρων λόγω των περιορισμών ενέργειας. Επιπλέον, η ανάγκη για την παρακολούθηση των δεδομένων σε πραγματικό χρόνο πριν από το αποτέλεσμα της μετάδοσης του s σε καθυστερήσεις. Στην περίπτωση των δικτύων ad-hoc και αισθητήρων, παρόλο που τα συστήματα ασύρματης ανίχνευσης εισβολών (WIDS) (βλ. 8.8) επιτρέπουν ορισμένες ενεργές δραστηριότητες που μπορούν να οδηγήσουν στον εντοπισμό κακόβουλων συμβάντων, όπως η παρακολούθηση δεδομένων σε πραγματικό χρόνο, η ανίχνευση ανωμαλίες σε τμήματα του δικτύου των ανταλλασσόμενων πακέτων μεταξύ των αισθητήρων και την υποβολή εκθέσεων, οι WIDS συγκρατούνται από συγκεκριμένες προκλήσεις. Λόγω της δυναμικής τοπολογίας τέτοιων δικτύων, ο καθορισμός της καλύτερης θέσης για τους αισθητήρες WIDS, καθώς και ο αντίστοιχος διακομιστής συσχέτισης, είναι ένα πολύπλοκο και δύσκολο έργο. Κατά συνέπεια, για κάθε νέο αισθητήρα που δημιουργεί μια σύνδεση με ένα δίκτυο ad-hoc, οι WIDS για αισθητήρες κάλυψη θα πρέπει να αξιολογηθούν. Στην περίπτωση που ο νέος αισθητήρας είναι εκτός κάλυψης WIDS, τότε ένας νέος αισθητήρας WIDS θα πρέπει να ενσωματωθούν. Αυτή η διαδικασία αποκαλύπτει ένα κενό, καθώς οι αισθητήρες συνδέονται και αποσυνδέονται δυναμικά σε δίκτυα ad-hoc. Έτσι, σε περίπτωση που αφήνει ένα νέο αισθητήρα εκτός της περιοχής κάλυψης ενός WIDS «s, τα τρωτά σημεία του αισθητήρα απειλούν το δίκτυο ad-hoc.

Υπάρχει μια μεγάλη ανησυχία σχετικά με την αποτελεσματικότητα της πρακτικής που ονομάζεται αλλαγή ή αντικατάσταση των σταθμών βάσης που δυσκολεύουν περισσότερο να θέσουν σε κίνδυνο τους κινητούς κόμβους (βλ. 8.8), γεγονός που αυξάνει το επίπεδο ασφάλειας και την πολυπλοκότητα σε ad-hoc και δίκτυα αισθητήρων. Με την υιοθέτηση αυτής της διαδικασίας αυξάνονται επίσης τα λειτουργικά έξοδα των δικτύων λόγω του μεγέθους της τοπολογίας και του αριθμού των αισθητήρων. Ωστόσο, αμφισβητείται η μακροπρόθεσμη βιωσιμότητα της διαδικασίας. Τα έξοδα αποθαρρύνουν οποιονδήποτε πάροχο υπηρεσιών ad-hoc δικτύων να εφαρμόσουν την εξεταζόμενη πρακτική λόγω του οικονομικά αποδοτικού χαρακτήρα αυτών των δικτύων. Η ποικιλομορφία των μηχανισμών ασφαλείας για κάθε ένα από τους τομείς της αρχιτεκτονικής M2M απαιτεί ανθρώπινη αλληλεπίδραση,

προκειμένου να μετριαστούν οι κίνδυνοι και να εξασφαλίσει επαρκή προστασία από απειλές. Εκτός αυτού, πρέπει να αντιμετωπίσουμε αποτελεσματικά τις προκλήσεις της διαχείρισης της έκδοσης (π.χ. αναβαθμίσεις υλικολογισμικού, ενημερωμένες εκδόσεις, διορθώσεις, ενημερώσεις λειτουργικών συστημάτων) και να επιτύχουμε ένα υψηλό επίπεδο ασφάλειας. Για παράδειγμα, τ αυτοματοποιημένες ενημερώσεις firmware αυξήσει τους κινδύνους ασφαλείας αυξάνοντας τις δυνατότητες τρωτών σημείων στα μονάδας ελέγχου του κινητήρα (ECU) οχήματα και σε κατανεμημένα δίκτυα Αισθητήρες. Για το σκοπό αυτό, η αυτοματοποιημένη ή απομακρυσμένη ενημέρωση υλικολογισμικού ( βλέπε 5.5.5) αμβλύνεται από τη διαδικασία δοκιμής αυτής της πρακτικής. Ωστόσο, το απαιτούμενο χρονικό διάστημα για την εκτέλεση της διαδικασίας ελέγχου των νέων ενημερώσεις και patches, αφήνει τους αισθητήρες επιρρεπή σε τρωτά σημεία που θα μπορούσαν να μετριαστούν από τα εξεταζόμενα ενημερώσεις αμέσως μόλις εγκριθούν και να αναπτυχθεί. Σε αυτό το χρονικό διάστημα, η εκμετάλλευση οποιουδήποτε τρωτού σημείου είναι εξαιρετικά επικίνδυνη, λόγω του ότι εξαρτάται από τις δυνατότητες του εισβολέα και την εκλέπτυνση της μεθόδου εκμετάλλευσης.

## 9.3. Κενά στο πεδίο εφαρμογής

Σε περίπτωση που οι ανεπάρκειες λογισμικού των εφαρμογών M2M δεν είναι γνωστές ευπάθειες (π.χ. Exploit Database) και, κατά συνέπεια, δεν διαχειρίζονται και επιλύονται από ενημερώσεις κώδικα ασφαλείας και επείγουσες επιδιορθώσεις, τότε οι εφαρμογές M2M θα μπορούσαν να ενδιαφέρουν τους δράστες που εκμεταλλεύονται τη δύναμη των μηδενικών εκμεταλλεύσεων για να αποκτήσουν πρόσβαση. Παραδείγματος χάριν, οι επιθέσεις που προκύπτουν από την απειλή κακών δραστηριοτήτων (βλ. 5.5) συνδέονται άκρως με εκμεταλλεύσεις μηδενικών ημερών και οδηγούν σε κακόβουλο κώδικα ένεσης, εκμετάλλευση εσφαλμένων ρυθμίσεων ασφαλείας καθώς και σπασμένη πιστοποίηση ταυτότητας. Έτσι, η ανάπτυξη των εφαρμογών θα πρέπει να ακολουθεί τις βέλτιστες πρακτικές και τις πλέον σύγχρονες λύσεις, οι οποίες θα μπορούσαν να δώσουν προτεραιότητα στην πρακτική εφαρμογή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, αξιοποιώντας μηχανισμούς ασφαλείας όπως η κρυπτογραφία και ο διαχωρισμός μεταξύ λειτουργικών δεδομένων και δεδομένων χρηστών. Επιπλέον, η εξάπλωση, η ενημέρωση και η επίλυση συμβάντων έκτακτης ανάγκης για την ασφάλεια θα πρέπει να καθοδηγούνται από ομάδες κοινοποίησης έκτακτης ανάγκης (CERT) που διαδίδονται παγκοσμίως. Σε αυτή τη φλέβα, η ασφάλεια στο στρώμα εφαρμογής μπορεί να ενισχυθεί.

Λόγω της κλιμάκωσης της ζήτησης σε πηγές back-end, οι εφαρμογές M2M βασίζονται όλο και περισσότερο στο πρότυπο του cloud computing (CC) και στα αντίστοιχα μοντέλα ανάπτυξης και εξυπηρέτησης. Τα μοντέλα υπηρεσιών CC ανήκουν σε διαφορετικά επίπεδα αφαίρεσης στην αρχιτεκτονική και αλληλοεξαρτώνονται για την παροχή των τελικών υπηρεσιών. Επιπλέον, υπάρχουν διάφορες συνέπειες για την ασφάλεια μεταξύ των μοντέλων υπηρεσιών υπολογιστικού νέφους. Για παράδειγμα, οι συγκεκριμένες ευπάθειες της πλατφόρμας ως υπηρεσία (PaaS) θα μπορούσαν να θέσουν σε κίνδυνο την ασφαλή ανάπτυξη του λογισμικού-ως-υπηρεσίας (SaaS). Κατά συνέπεια, οι εξαρτήσεις ασφαλείας μεταξύ αυτών των μοντέλων θα μπορούσαν να οδηγήσουν σε απειλές όπως στο εσφαλμένη χρήση ή χορήγηση συσκευών και συστημάτων (βλέπε 5.1.3). Με στόχο την εξασφάλιση του στρώματος εφαρμογής σύμφωνα με τις πρακτικές περιβάλλοντος παλαιού τύπου, όπως με τη συντήρηση και την ενημέρωση των αποθεμάτων με τις πληροφορίες εξουσιοδοτημένου και μη εξουσιοδοτημένου λογισμικού / OS / εφαρμογών / συσκευών μέσα στο δίκτυο (βλ. 8.6), πολλές αδυναμίες Οι εξαρτήσεις μοντέλων CC δεν αντιμετωπίζονται. Για παράδειγμα, η Εικονικά Περιβάλλοντος Ξεχασμένες Επιχειρήσεων χειρισμοί (VENOM) 209 ευπάθεια μόχλευση από επιτιθέμενους με στόχο την virtuali s συστήματα ation των Παρόχων Υπηρεσιών Cloud

(CSP) που χρησιμοποιούν το-as-a-Service Υποδομών μοντέλο (IaaS). Στην περίπτωση αυτή, οι αρνητικές επιπτώσεις μιας επιτυχημένης επιπτώσεων επίθεση το λογισμικό-as-a-Service επιχειρήσεις.

## 9.4. Κενά στο Επιχειρησιακό Τομέα

Κατά το σχεδιασμό, τα πρωτόκολλα δρομολόγησης σε ad-hoc δίκτυα και αυτόνομα συστήματα κινητών κόμβων (MANETs) ταξινομούνται σε τρεις κατηγορίες. δηλαδή η ενεργητική, η αντιδραστική / κατά ζήτηση και οι υβριδικές. Τα πρωτόκολλα διευκολύνουν επίσης την ανταλλαγή πληροφοριών δρομολόγησης, η οποία επιτρέπει στους κόμβους ad-hoc και αισθητήρα να μάθουν και να προσαρμόζονται στις αλλαγές των κόμβων ή τοπολογίας. Ωστόσο, κανένας από αυτούς δεν μπορεί να διαφυλάξει επαρκώς τη λειτουργία τέτοιων δικτύων ενάντια σε όλο το φάσμα των επιθέσεων, όπως κατά των επιθέσεων DoS ( βλέπε 5.5.1), εξαιτίας συμβιβασμών και περιορισμών που κληρονομούνται από τα χαρακτηριστικά τους. Οι περιορισμοί αυτοί δεν αντιμετωπίζονται επαρκώς με την εφαρμογή των πρακτικών που ονομάζεται σχεδιασμό και τη διατήρηση επίπεδη βάση, ιεραρχική, με βάση, με βάση τη θέση και την ιεραρχική πρωτόκολλα δρομολόγησης (βλέπε 8.8), οι οποίοι διασφαλίζουν μόνο εν μέρει τη λειτουργία των MANET προσφέρουν ». Έτσι, τα πρωτόκολλα δρομολόγησης είναι επιρρεπή σε ένα ευρύτερο φάσμα κακόβουλων επιθέσεων, όπως μπλοκαρίσματος (βλέπε 5.5.1) και υποκλοπής (βλέπε 5.6).

## 9.5. Κενά στον τομέα του προϊόντος / επιχειρηματικές διεργασίες

Η κατανεμημένη φύση και οι κοινόχρηστοι πόροι της αρχιτεκτονικής M2M εκθέσει τις επιχειρηματικές διαδικασίες για την απειλή s κατάχρηση των προσωπικών δεδομένων, καθώς και για φαύλους δραστηριότητες. Αυτή η έκθεση θα μπορούσε ενδεχομένως να οδηγήσει σε δόλιες δραστηριότητες, οι οποίες κατά κύριο λόγο παραβιάζουν την ακεραιότητα των περιουσιακών στοιχείων και οδηγούν σε χαμηλό επίπεδο εμπιστοσύνης και ιδιωτικότητας. Η ύπαρξη επιχειρησιακών αμυντικών μηχανισμών στοχεύει στην εξασφάλιση της τεχνικής στρώσης των επιχειρήσεων (δηλ εμπιστοσύνης χρησιμοποιώντας παράγοντες ασφάλειας που βασίζονται σε κινητά τηλέφωνα και χρησιμοποιούν μηχανισμούς ενιαίας σύνδεσης ή τεχνικές διαχείρισης εμπιστοσύνης ( βλ. 8.1) ). Η εφαρμογή αυτών των μηχανισμών χωρίς οποιαδήποτε υποστήριξη από το λειτουργικό στρώμα των επιχειρήσεων στις οποίες εμφανίζεται η τεκμηρίωση των πολιτικών οδηγεί σε ασυνέπειες όπως μια στατική προσέγγιση κατά των απειλών κατά της απάτης.

Το μοντέλο διάρθρωσης των επιχειρηματικών διαδικασιών για δίκτυα ad-hoc και αισθητήρων που ενσωματώνονται στις επιχειρήσεις θα πρέπει να βασίζεται σε ένα ρυθμιστικό πλαίσιο που καθορίζει τη νομιμότητα και το επίπεδο προστασίας της ιδιωτικής ζωής. Το ρυθμιστικό πλαίσιο για την ασφάλεια και τις επιχειρήσεις θα πρέπει να καθορίζει και να παρέχει τους παράγοντες επιτυχίας (π.χ. εμπιστευτικότητα, ακεραιότητα και επίπεδο προστασίας της ιδιωτικής ζωής) για τα αισθητήρια δεδομένα και την επικοινωνία. Στη συνέχεια, η απειλή παραβίασης των κανόνων και των κανονισμών ( βλέπε 5.3.2) μπορεί να εξαλειφθεί και να εξαλειφθεί. Ωστόσο, πάρτε το ρυθμιστικό πλαίσιο s υπόψη μόνο το είδος των συλλέγονται και υφίστανται επεξεργασία δεδομένων χωρίς εστίαση με τον τύπο του υποκείμενου περιβάλλοντος. Κατά συνέπεια, οι κανονισμοί ρυθμίζουν μόνο τις απειλές κατά του τύπου των συλλεγέντων και των επεξεργασμένων δεδομένων. Έτσι, το ρυθμιστικό πλαίσιο s δεν αποτελούν πάντα ορισμένες μεθόδους και τεχνικές προστασίας απειλή για την εξάλειψη των απειλών σε ad-hoc και αισθητήρα δίκτυα. Ως αποτέλεσμα, ακόμη και αν τα ad-hoc δίκτυα λειτουργούν σύμφωνα με το κανονιστικό

πλαίσιο, το οποίο επίσης σύμφωνα με το νόμο, αυτό δεν επαρκεί για την επίτευξη υψηλού επιπέδου ασφάλειας. Έτσι, η επιχείρηση μπορεί να καθορίσει τους στόχους που θα εξαλείψουν τις απειλές όπως οι διακοπές και οι επιθέσεις DDoS.

Τυπικά, το ρυθμιστικό πλαίσιο s καθορίζουν τις υποχρεώσεις και τις ευθύνες σχετικά με την ασφάλεια δραστηριοτήτων, οι οποίες θα πρέπει να εκτελούνται από τους φορείς παροχής υπηρεσιών. Για παράδειγμα, την ενσωμάτωση τεχνικών και οργανωτικών μέτρων για την προστασία των προσωπικών δεδομένων από τυχαία ή παράνομη καταστροφή ή τυχαία απώλεια μπορεί να χρησιμοποιηθεί. Τ ο κανονιστικού πλαισίου s δεν καθορίζουν ρητώς τις υποχρεωτικές ενέργειες που επιβαρύνουν τους τελικούς χρήστες concering την ασφάλεια δραστηριοτήτων τους. Ως αποτέλεσμα, οι τελικοί χρήστες απειλούνται, δεδομένου ότι δεν έχουν ενημερωθεί σχετικά με την προοπτική ασφάλειας των εφαρμογών M2M. Στις περισσότερες περιπτώσεις, οι εφαρμογές που συλλέγουν PII είναι οι εφαρμογές e-Health και ενεργοποιούνται από την ενορχήστρωση των δικτύων Mobile Healthcare Networks (MHNs) ( βλ. 5.3.1).

Κάθε επίπεδο επικοινωνίας ενός ad-hoc και δικτύου αισθητήρων απειλείται από την έλλειψη σφαλμάτων σχεδιασμού ή σχεδίασης (βλέπε 5.1.1) κατά τη διάρκεια της φάσης έναρξης τους. ο εφαρμογή της πρακτικής του σχεδιασμού και της ασφάλειας την εφαρμογή του σχεδιασμού (βλέπε 8.1) παρέχουν s επαρκείς μηχανισμούς ασφάλειας σε κάθε επίπεδο. Ωστόσο, η εφαρμογή της ασφάλειας από το σχεδιασμό δεν κατορθώνει να προστατεύσει τις επιχειρηματικές διαδικασίες λόγω της σύνδεσής τους με την επιφάνεια επίθεσης εξωτερικών στοιχείων που είναι ενσωματωμένα σε ad-hoc και δίκτυα αισθητήρων. Για παράδειγμα, τα συστήματα SCADA αποτελούνται από διάφορα εξωτερικά εξαρτήματα (π.χ. PLC) που διευκολύνουν την επιχειρησιακή διαχείριση των ad-hoc και των δικτύων αισθητήρων. Τα PLC συνήθως ενορχηστρώνονται για να επιτύχουν τους στόχους της επιχείρησης σχετικά με το επίπεδο απόδοσης και QoS. Όσον αφορά τα PLC που κατασκευάζονται από συγκεκριμένους πωλητές, τα υπάρχοντα τρωτά σημεία επιτρέπουν την αυθαίρετη αποκάλυψη αρχείων και τον τηλεχειρισμό. Οι ευπάθειες των PLC εισάγουν κινδύνους ασφαλείας που δεν θα μπορούσαν να μετριαστούν στο πλαίσιο της ασφάλειας από το σχεδιασμό. Εκτός αυτού, οι επιχειρήσεις που διαθέτουν συστήματα SCADA, όπως οι μονάδες παραγωγής ηλεκτρικής ενέργειας και διανομής νερού, δεν μπορούν να αλλάξουν ή να τροποποιήσουν τα PLC, προκειμένου να εξαλείψουν τις ευπάθειές τους, διότι υπόκεινται να έχω ntellectual ΙΔΙΟΤΗΤΕΣ Δικαιωμάτων (ΔΔΙ), όπως τα πνευματικά δικαιώματα και τα δικαιώματα βιομηχανικής ιδιοκτησίας σχεδιασμό των πωλητών. Ένα άλλο παράδειγμα αυτού του περιορισμού είναι το γεγονός ότι ορισμένοι αισθητήρες λειτουργούν με ένα προεγκατεστημένο λειτουργικό σύστημα το οποίο μπορεί να έχει διάφορες αδυναμίες χωρίς τη δυνατότητα εγκατάστασης μιας ενημερωμένης έκδοσης OS ή patches ασφαλείας. Ως αποτέλεσμα, τα τρωτά σημεία αυτών των αισθητήρων δεν μπορούν να επιλυθούν με την εξεταζόμενη πρακτική που ονομάζεται ασφάλεια από το σχεδιασμό και είναι ευαίσθητα σε εκμεταλλεύσεις OS (βλ. 5.1.2). Για το σκοπό αυτό, ο περιορισμός αυτός προκύπτει τόσο για τους αισθητήρες όσο και για τα εξωτερικά εξαρτήματα όπως οι απομακρυσμένες μονάδες τερματικών (RTU) και οι προγραμματιζόμενοι ελεγκτές αυτοματισμού (PAC) που αγοράζονται από τους πωλητές. Αντίστοιχα, η ασφάλεια από το σχεδιασμό δεν μετριάζει πλήρως την απειλή της έλλειψης σχεδιασμού ή σφαλμάτων σχεδιασμού, στο πλαίσιο των επιχειρηματικών διαδικασιών.

## 9.6. Συστάσεις

Τα παραπάνω κενά οδηγούν φυσικά σε μια σειρά συστάσεων που μπορούν να βελτιώσουν τη συνολική απόδοση ασφαλείας και μπορούν να ταξινομηθούν είτε ως οργανωτικές είτε ως τεχνικές συστάσεις.

### 9.6.1. Οργανωτικές συστάσεις

***Λειτουργικές συστάσεις***

Στο πλαίσιο των χαρακτηριστικών ασφαλείας, η ανάπτυξη δικτύου ad-hoc και αισθητήρων θα μπορούσε να ενισχυθεί με πρακτικές που τεκμηριώνονται σε σχέση με τα πρότυπα.

Υπάρχει αυξανόμενη ανησυχία για τα προνόμια των φυσικών προσώπων που έχουν πρόσβαση σε αισθητηριακά σύνολα δεδομένων για την εκτέλεση μιας ποικιλίας λειτουργιών διαχείρισης (π.χ. φορείς παροχής υπηρεσιών M2M). Αυτή η ανησυχία αναφέρεται στις περισσότερες από τις προκλήσεις που αφορούν τη διαχείριση δεδομένων επιτήρησης σε περιοχές που παρακολουθούνται από συστήματα ασφαλείας κλειστού κυκλώματος και στα στοιχεία εσωτερικής τοποθέτησης κυρίως στις αλυσίδες εφοδιασμού και τις ροές δεδομένων, οι οποίες διευκολύνουν τον τηλεχειρισμό οικιακών συσκευών M2M. Για το σκοπό αυτό, είναι πολύ σημαντικό να προσδιοριστεί από ποιον έχουν πρόσβαση τα δεδομένα και τις συνθήκες που χρειάζονται για την πρόσβαση στα δεδομένα. Θα πρέπει να οριστούν οι κατάλληλοι ρόλοι για τη σύνδεση των τελικών χρηστών (π.χ. υπαλλήλων και πελατών του παρόχου υπηρεσιών M2M, πελάτες) με συγκεκριμένα τμήματα των δεδομένων που συλλέγονται και να τους εξουσιοδοτούνται με συγκεκριμένα προνόμια όσον αφορά τις υπολογιστικές λειτουργίες. Η διαδικασία αυτή θα πρέπει να συνδυαστεί με την αυστηρή παρακολούθηση του δικτύου ad-hoc και των αισθητήρων ώστε να διασφαλιστεί και να καταστεί δυνατή η ασφαλή συλλογή ευαίσθητων δεδομένων. Επιπλέον, η ανάπτυξη εφαρμογών M2M και ανάπτυξης σε CC περιβάλλον s θα πρέπει να γίνεται με την προσαρμογή και τη διεύρυνση των κατευθυντήριων γραμμών της ασφάλειας των εφαρμογών των οργανισμών τυποποίησης και καλύπτουν τις ανάγκες και τις απαιτήσεις της αρχιτεκτονικής M2M.

***Συστάσεις πολιτικής***

Λόγω των ζητημάτων προστασίας της ιδιωτικής ζωής που πρέπει να εξεταστούν στην ad-hoc δικτύου αισθητήρων και s με το που ανταλλάσσονται προσωπικά, εμπιστευτικά, ευαίσθητα δεδομένα, πρέπει να θεσπιστούν ειδικές πολιτικές για την έγκριση των διαδικασιών και την κοινή χρήση συμφωνίες σχετικά με τις αισθητηριακές δεδομένων. Για λόγους διαφάνειας, πολιτικές πρέπει να ληφθούν υπόψη, τα οποία αφορούν τον ορισμό των υποχρεώσεων και τις πράξεις διαχείρισης περιγραφή. Επιπλέον, η πολιτική προστασίας της ιδιωτικής ζωής θα πρέπει να διατυπώνει τους λόγους και τις μεθόδους που χρησιμοποιούνται για τη συλλογή καθώς και για την επεξεργασία αισθητικών δεδομένων και τους μηχανισμούς που μετριάζουν τις απειλές κατά λειτουργικών και λειτουργικών διαδικασιών. Επιπλέον, η συμμόρφωση με την ιδιωτική ζωή θα πρέπει να διασφαλίζεται στο πλαίσιο μιας αξιόπιστης και συνεπούς εφαρμογής του M2M. Πρέπει να ακολουθείται τυποποιημένη τεκμηρίωση σχετικά με τη συμμόρφωση με την ιδιωτική ζωή. τυπικά παραδείγματα είναι η ανάλυση κατώτατου ορίου απορρήτου (PTA) ή η αξιολόγηση επιπτώσεων στην ιδιωτική ζωή (PIA). Εκτός από το ευαίσθητο επίπεδο δεδομένων, η πολιτική απορρήτου σχετίζεται επίσης με πρόσθετα έγγραφα. Για παράδειγμα, στον τομέα της υγειονομικής περίθαλψης,

τα ενημερωμένα έγγραφα συγκατάθεσης συνδέονται με τους στόχους προστασίας της ιδιωτικής ζωής που καθορίζονται από τα ολοκληρωμένα ad-hoc δίκτυα που αναπτύσσονται στο περιβάλλον των νοσοκομείων. Οι ασθενείς είναι εξουσιοδοτημένοι να ελέγχουν και να εγκρίνουν τη συγκέντρωση καθώς και την επεξεργασία των ευαίσθητων πληροφοριών τους από τους BSN. Με άλλα λόγια, οι ασθενείς συμφωνούν να ελέγχουν την αποκάλυψη του PII τους σε έναν αξιόπιστο και προκαθορισμένο τρίτο, όπως σε συγκεκριμένο νοσηλευτικό προσωπικό και γιατρούς.

Το επίπεδο ασφάλειας των εφαρμογών M2M επηρεάζεται έντονα από τα τρωτά σημεία των διακομιστών back-end. Για το σκοπό αυτό, οι διακομιστές αυτοί θα πρέπει να ενημερώνονται χρησιμοποιώντας ενημερωμένες εκδόσεις ασφαλείας και θα πρέπει επίσης να υπόκεινται σε διαχείριση ευπάθειας. Τα στοιχεία αυτής της διαχείρισης θα πρέπει να είναι μια τεχνική αξιολόγηση καθώς και η αναπροσαρμογή της η οποία καθορίζει αποδεκτές μεθόδους για την εκτέλεση της ίδιας της αξιολόγησης.

Η ασφάλεια από το σχεδιασμό θα πρέπει να εφαρμοστεί για κάθε στρώμα του ad-hoc δικτύου, πράγμα που σημαίνει ότι, η υψηλότερη στρώση αφαίρεσης, η ανάπτυξη της πολιτικής διαχείρισης κωδικού πρόσβασης έχει μεγάλη σημασία για την άμβλυνση διάφορες απειλές. Ωστόσο, πριν από την προσαρμογή αυτού του τύπου πολιτικής, θα πρέπει να αντιμετωπιστούν πολλές προκλήσεις, όπως η μετάβαση των κωδικών πρόσβασης και τα χρονικά διαστήματα κατά τα οποία θα πραγματοποιηθεί η αλλαγή των κωδικών πρόσβασης. Επιπλέον, η επιχειρησιακή εφαρμογή αυτής της πολιτικής θα πρέπει να διασφαλιστεί στο πλαίσιο της συμμόρφωσής της με τη διεξαγωγή κατάλληλων ελέγχων και αξιολογήσεων. Επιπλέον, οι τεχνικές πρακτικές που χρησιμοποιούνται για τη διασφάλιση της αλληλεπίδρασης RFID μεταξύ ετικετών και αναγνωστών πρέπει να συμμορφώνονται με τα πρότυπα και τους πλέον σύγχρονους μηχανισμούς ασφαλείας.

### *Κανονιστικές συστάσεις*

Η συλλογή και η επεξεργασία των ΠΑΠ πρέπει να γίνεται ακολουθώντας τους περιορισμούς που τίθενται από τις Ευρωπαϊκές οδηγίες, όπως η οδηγία 95/46 / ΕΚ, η οδηγία για τη διασυνοριακή υγειονομική περίθαλψη 2011/24 / ΕΕ και η απόφαση 2011/890 / ΕΕ σχετικά με τη θέσπιση κανόνων για τη δημιουργία, τη διαχείριση και τη λειτουργία του Δικτύου εθνικών αρμόδιων αρχών για την ηλεκτρονική υγεία. Ωστόσο, η υποκείμενη υποδομή εφαρμογών και λειτουργιών M2M πρέπει να συμμορφώνεται με τα κανονιστικά πλαίσια ασφάλειας και λειτουργιών σχετικά με την προστασία των προσωπικών δεδομένων. Για παράδειγμα, σε δύο χρόνια, οι αιτήσεις αυτές θα πρέπει να λειτουργούν σύμφωνα με τις κατευθυντήριες γραμμές του Κανονισμού 2016/679 για την Γενική Προστασία Δεδομένων, η οποία ακολουθεί μια προσέγγιση βασισμένη στον κίνδυνο και επιτρέπει την προστασία της ιδιωτικής ζωής από το σχεδιασμό. Τέλος, οι πάροχοι υπηρεσιών ad-hoc δικτύων θα πρέπει να ενημερώνουν τους τελικούς χρήστες σχετικά με τις ευθύνες τους (π.χ. ισχυρά διαπιστευτήρια, χρήση ψηφιακών υπογραφών) σχετικά με την απόκρυψη του PII κατά τη λειτουργία των δικτύων και ιδιαίτερα σε περιπτώσεις ενορχηστρώσεων MHN.

### *Προτάσεις διαδικασιών για επιχειρήσεις / προϊόντα*

Η κατασκευή ορισμένων προϊόντων (π.χ. δέκτες GPS, ιατρικοί αισθητήρες) θα πρέπει να βασίζεται σε απειλές για την ελαχιστοποίηση των πιθανών τρωτών σημείων, πράγμα που θα μπορούσε να συμβεί επιτρέπουν επιθέσεις

κατά τη φάση εγκατάστασης και ανάπτυξης. Τ ο μεταποιητικές επιχειρήσεις των δεκτών GPS θα πρέπει επίσης να γνωρίζουν τη συνεχώς αυξανόμενη επιφάνεια επίθεσης των προϊόντων τους. Η λειτουργία GPS βασίζεται στη συναλλαγή σημάτων μεταξύ του δέκτη GPS και τεσσάρων ή περισσότερων δορυφόρων. Αυτή η συναλλαγή σημάτων λαμβάνει χώρα έτσι ώστε ο δέκτης GPS να μπορεί να καθορίσει τις τρέχουσες τρεις συντεταγμένες του και να συγχρονίσει το ρολόι του με τα ατομικά ρολόγια του αστερισμού. Η κυρίαρχη μέθοδος, κατά την οποία λειτουργεί το GPS, μπορεί να εκμεταλλευτεί εξαιτίας τρωτών σημείων που επιτρέπουν επιθέσεις πλαστογράφησης. Οι αμυντικές τεχνικές που μπορούν να χρησιμοποιηθούν για να κατασκευαστεί ένας ανιχνευτής παραβίασης GPS μπορούν να εφαρμοστούν μόνο κατά τη διάρκεια της κατασκευής τους λόγω της έλλειψης γνώσεων και πόρων των ατόμων. Επιπλέον, θα πρέπει να εφαρμοστεί κρυπτογράφηση από άκρο σε άκρο κατά την επικοινωνία των δεκτών GPS και των δορυφόρων. Επομένως, το θέμα αυτό συνιστάται να αντιμετωπιστεί από τις εταιρείες κατά τη διάρκεια των διαδικασιών σχεδιασμού και μοντελοποίησης.

Στο πλαίσιο της αντιμετώπισης δόλιων δραστηριοτήτων εντός της αρχιτεκτονικής M2M, θα πρέπει να οργανωθούν προληπτικές λειτουργικές διαδικασίες, πρωτόκολλα και πολιτικές με στόχο την πρόληψη της απάτης και τη διαβεβαίωση στους τελικούς χρήστες. Συγκεκριμένα, ένας κώδικας δεοντολογίας και μια πολιτική καταπολέμησης της απάτης συνιστούν τις ελάχιστες διασφαλίσεις που πρέπει να καθοριστούν και να ενσωματωθούν στην αρχιτεκτονική M2M μέσω της πολιτικής αδειοδότησης στα δεδομένα που συλλέγονται. Αυτά τα προληπτικά μέτρα διασφάλισης σε επιχειρήσεις λειτουργικό στρώμα πρέπει να ενισχύσουμε ed από μηχανισμούς ανίχνευσης της απάτης.

### 9.6.2. Τεχνικές συστάσεις

***Συστάσεις έγκρισης / εξουσιοδότησης***

Κατ 'αρχήν, θα πρέπει να στοχεύουν στην ΑΥΞΗΣΗΣ ε την ασφάλεια κατά τη διαδικασία πιστοποίησης με την ανάπτυξη μεθόδων ισχυρή ή πολυ-παράγοντα πιστοποίησης (ΣΠΙ), όπου ver ισχύει. Ωστόσο, όσον αφορά τον έλεγχο ταυτότητας συσκευών για δίκτυα ad-hoc και αισθητήρων, οποιαδήποτε συσκευή θα μπορούσε επίσης να βασίζεται σε πιστοποίηση βάσει πιστοποιητικού και σε μεθόδους που σκληρύνουν τη διαδικασία εκμετάλλευσης χρησιμοποιώντας μια ασφαλής καταχώρηση δικτύου. Ακόμη περισσότερο, μία ελαστική τύπο του μηχανισμού ελέγχου πρόσβασης, συνιστάται να ενσωματωθεί στο ad-hoc και δίκτυο αισθητήρων s όπως το χαρακτηριστικό που βασίζεται πρόσβαση ελέγχους. Ως εκ τούτου, αυτές οι ενισχυμένες ασφαλείς συσκευές θα μπορούσαν να τοποθετηθούν σε μη ασφαλείς θέσεις και εγκαταστάσεις χωρίς παρακολούθηση. Επιπλέον, στο πλαίσιο της επικοινωνίας RFID μεταξύ των ετικετών και των αναγνωστών, συνιστάται να πραγματοποιείται η διαδικασία επαλήθευσης ταυτότητας σε συσκευές ανάντη για τη σύνδεση μοναδικών κωδικών πρόσβασης σε άτομα.

***Προληπτική σύσταση για την άμυνα***

Τα τελευταία χρόνια, υπάρχει μια αυξανόμενη ανησυχία για τις DDoS και επιθέσεις πλημμυρών καθώς και για την επιδείνωση των επιθετικών τεχνικών τους. τα botnets χρησιμοποιούνται σε επιθέσεις DDoS σε δίκτυα ad-hoc και αισθητήρων. λόγω της κρυφής φύσης των bots, τα botnets μπορεί να γίνουν ένας απρόβλεπτος αντίπαλος. Από μια άλλη σκοπιά, οι ad-hoc και αισθητήρα δίκτυα στοχευμένες με το πεδίο εφαρμογής που πρόκειται να τεθεί σε κίνδυνο και οι συσκευές που εγγράφονται στο botnets, που εκτελούν επιθέσεις DDoS. Αυτή η μέθοδος

ακολουθήθηκε κατά τη διάρκεια του αμερικανικού περιστατικού που αφορούσε μια κρίσιμη υποδομή διαδικτύου, η οποία είχε στοχεύσει το botnet IoT με βάση το Mirai. Έτσι, παρά την ενορχήστρωση του WIDS στο πλαίσιο των ad-hoc δικτύων, συνιστάται η χρήση του IDS σε κάθε συμφόρηση της αρχιτεκτονικής M2M όπως η πύλη M2M. Μετά την προσαρμογή αυτού του μέτρου, οποιαδήποτε εισερχόμενη κυκλοφορία ανεπιθύμητης αλληλογραφίας από τις συσκευές M2M που στοχεύουν οντότητες εκτός του ad-hoc και του δικτύου αισθητήρων θα μπορούσε να εντοπιστεί και να αποφευχθεί. Για το σκοπό αυτό, η κίνηση του δικτύου της κάθε συσκευής που συνδέεται στο διαδίκτυο παρακολουθείται και προληπτική ανίχνευση ενορχηστρωμένη. Εκτός αυτού, συνιστάται να εξασφαλίζεται η συνεχής ενημέρωση του συνόλου κανόνων αισθητήρων IDS σε αυστηρά χρονικά διαστήματα και με την παρακολούθηση αξιόπιστων πηγών υπογραφών. Ακόμη περισσότερο, λόγω των χαρακτηριστικών του Μανέ τα πρωτόκολλα δρομολόγησης, συνιστάται ιδιαίτερα η αξιολόγηση της ασφάλειας του δικτύου να επικεντρώνεται πρωτίστως στα πρωτόκολλα δρομολόγησης ευπάθειες.

### *Αντιδραστική Αμυντική Σύσταση*

Η αναγνώριση των εκμεταλλεύσεων μηδενικής ημέρας είναι αδύνατο να εφαρμοστεί από την WIDS. Η λειτουργία των αμυντικών μηχανισμών που διενεργούν βαθιά έλεγχο πακέτων (DPI) βασίζεται σε υπογραφές γνωστών επιθέσεων. Έτσι, συνιστάται να δημιουργήσει μια άμυνα ζώνης αποτελούνται σης του Honeynet, παράλληλα με τις ad-hoc και αισθητήρα δίκτυα. Αυτό το δίκτυο αποτελείται από τα honeypots που εξομοιώνουν τη λειτουργία των αισθητήρων. Το honeynet αποτελεί ένα είδος σκοτεινού δικτύου το οποίο είναι σε θέση να εντοπίσει νέες μεθόδους επιθέσεων και εκμεταλλεύσεις μηδενικών ημερών. Το Mobile Edge Cloud Computing συνιστάται να ενορχηστρωθεί για να αναπτύξει το honeynet. Η λειτουργία των κυψελοειδών δικτύων επιτρέπει την παρακολούθηση κακόβουλων δραστηριοτήτων για να τους αναλύσει και να συλλέξει ιατροδικαστικές πληροφορίες σχετικά με τις επιθέσεις και τη συμπεριφορά των εισβολέων. Θα πρέπει να χρησιμοποιηθεί ένα δίκτυο εικονικών οντοτήτων που εξομοιώνουν τη λειτουργία αισθητήρων και, σε περίπτωση απειλητικού συμβάντος, η κακόβουλη κίνηση θα μπορούσε να εκφορτωθεί στο Mobile Edge Cloud (MEC) για να καταγραφεί και να παρακολουθηθεί αυτή η κίνηση. Λόγω του γεγονότος ότι η διαδικασία εκφόρτωσης αυξάνει το γενικό κόστος της κατανάλωσης ενέργειας, θα πρέπει να χρησιμοποιηθούν εικονικές μηχανές που λειτουργούν εντός του MEC, προκειμένου να αποφευχθούν περιορισμοί επιδόσεων αντίθετοι με την περίπτωση χρήσης αισθητήρων.

# 10. Συμπεράσματα

Η ανάπτυξη της δικτύωσης ad-hoc και αισθητήρων για το τοπίο απειλής επικοινωνιών M2M ήταν εντυπωσιακή σε ένα πράγμα: επεκτείνεται εκθετικά στα δικά της όρια αντίκτυπου, ενώ η βιομηχανία, οι αρχές και οι εμπειρογνώμονες αναλύουν τη μεγάλη εικόνα μέχρι σήμερα.

Το τοπίο επεξεργασίας έχει εξελιχθεί με βάση το ενεργητικό ποσοτικό σύνολο το οποίο επηρεάζεται ή ενδέχεται να συμβάλλει ακούσια σε αυτή την επέκταση του τοπίου. Συμπληρώνοντας το τρέχον ερευνητικό έγγραφο, τα συμπεράσματά μας χωρίστηκαν σε τρεις κατηγορίες: τα συμπεράσματα πολιτικής, επιχειρήσεων και έρευνας.

***Συμπεράσματα πολιτικής***

- Καθιέρωση συγκεκριμένων πολιτικών για την έγκριση διαδικασιών
- Ορίστε συμφωνίες κοινής χρήσης όσον αφορά τα αισθητήρια δεδομένα
- Εξασφαλίστε τη συμμόρφωση με την προστασία της ιδιωτικής ζωής στο πλαίσιο αξιόπιστων και συνεπών εφαρμογών του M2M
- Εφαρμογή ασφάλειας από το σχεδιασμό

***Επιχειρηματικά συμπεράσματα***

- Ελαχιστοποίηση πιθανών τρωτών σημείων ακόμα και κατά τη φάση έναρξης και ανάπτυξης
- Βεβαιωθείτε ότι η παραγωγή ορισμένων προϊόντων είναι απειλητική
- Καθιέρωση ενός κώδικα συμπεριφοράς μέσω της πολιτικής αδειοδότησης στα δεδομένα που συλλέγονται
- Ενσωματώστε μια πολιτική ελέγχου κινδύνων απάτης στην αρχιτεκτονική M2M

***Συμπεράσματα της έρευνας***

- Ενσωματώστε έναν ελαστικό τύπο μηχανισμού ελέγχου πρόσβασης, όπως οι έλεγχοι πρόσβασης που βασίζονται σε χαρακτηριστικά
- Χρησιμοποιήστε ένα IDS σε κάθε συμφόρηση της αρχιτεκτονικής M2M όπως η πύλη M2M
- Δημιουργήστε μια αμυντική ζώνη η οποία αποτελείται από ένα honeynet με την ενορχήστρωση του Mobile Edge Cloud Computing (MEC) για την παρακολούθηση των κακόβουλων δραστηριοτήτων

# Βιβλιογραφία

## ENISA papers


[1] *Big Data Threat Landscape and Good Practice Guide*. [online] Available at https://www.enisa.europa.eu/publications/bigdata-threat-landscape, 2016

[2] *ENISA Threat Landscape 2015*. [online] Available at: https://www.enisa.europa.eu/publications/etl2015, 2016

[3] *Guideline on Threats and Assets. Technical guidance on threats and assets in Article 13a*. [online] Available at: https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets, 2015

[4] *Security and Resilience in eHealth Infrastructures and Services*. [online] Available at: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services, 2015

[5] *Threat Landscape and Good Practice Guide for Software Defined Networks/5G*. [online] Available at: https://www.enisa.europa.eu/publications/sdn-threat-landscape, 2015

[6] *Cyber security for Smart Cities - An architecture model for public transport*. [online] Available at: https://www.enisa.europa.eu/publications/smart-cities-architecture-model, 2015

[7] *Security and Resilience in eHealth - Security Challenges and Risks*. [online] Available at: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services, 2015

[8] *Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations*. [online] Available at: https://www.enisa.europa.eu/publications/cloud-in-finance, 2015

[9] *ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats*. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014, 2015

[10] *Threat Landscape and Good Practice Guide for Internet Infrastructure*. [online] Available at: https://www.enisa.europa.eu/publications/iitl, 2015

[11] *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*. [online] Available at: https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence, 2014

[12] *ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats*. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats, 2013

[13] *ENISA Threat Landscape, Mid-year 2013*. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-mid-year-2013, 2013

[14] *ENISA Threat Landscape - Responding to the Evolving Threat Environment*. [online] Available at: https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape, 2013


## Νομοθεσία


[15] *Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0611&rid=1, 2013

[16] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection -*

*Achievements and next steps: towards global cyber-security*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0163&from=EN, 2011

[17]*Proposal for a Regulation of the European Parliament and of the Council establishing a European Securities and Markets Authority*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009PC0503&rid=1, 2009

[18]*Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services*. [online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF, 2009

[19]*Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&rid=5, 2008

[20]*Green Paper on a European Programme for Critical Infrastructure Protection*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:52005DC0576, 2005

[21]*Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32004R0883R(01), 2004

[22]*Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=en, 2002

*[23]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=1, 1995