University of the Aegean, Samos, **2017-2018**
Information & Communication Systems Engineering – **ICSD**

Ασφάλεια Δικτύων Υπολογιστών και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Review of “Internet of Things: A Survey” (3 December 2016), written by:

Fadele Ayotunde Alabaa, Mazliza Othmana, Ibrahim Abaker Targio Hashema, Faiz Alotaibib

Γιώργος Καμπουράκης
(Διδάσκων)

Νίκος Τρίτσης (icsd11162)
Χρήστος Αυλακιώτης (icsd12015)

Περιεχόμενα

Περίληψη άρθρου

Το άρθρο που μελετήσαμε καταχωρήθηκε στις 3 Δεκεμβρίου του 2016 και εγκρίθηκε 4 Μαρτίου του 2017. Γράφτηκε απ'τους Fadele Ayotunde Alabaa, Mazliza Othmana, Ibrahim Abaker Targio Hashema, Faiz Alotaibib.

Περίληψη άρθρου

Το Internet of things (IoT) έχει γίνει πρόσφατα ένα σημαντικό θέμα έρευνας καθώς ενσωματώνει διάφορους αισθητήρες και αντικείμενα που επικοινωνούν μεταξύ τους χωρίς την ανθρώπινη παρέμβαση.
Με τον όρο αντικείμενα, στο IoT αναφερόμαστε σε φυσικές συσκευές, όπως αισθητήρες που μπορούν να συλλέξουν κάθε είδους πληροφορία είτε για μηχανήματα είτε για την ανθρώπινη κοινωνική ζωή.
Ο βασικός σκοπός του IoT είναι να παρέχει δικτυακή υποδομή με δυσλειτουργικά πρωτόκολλα και λογισμικό επικοινωνίας που θα επιτρέπουν τη σύνδεση και ενσωμάτωση φυσικών / εικονικών αισθητήρων, προσωπικών υπολογιστών, έξυπνων συσκευών, αυτοκινήτων και αντικειμένων όπως ψυγείο, πλυντήριο πιάτων, φούρνο μικροκυμάτων, τρόφιμα και φάρμακα, ανά πάσα στιγμή και σε οποιοδήποτε δίκτυο
Τα θέματα ασφάλειας, όπως η προστασία της ιδιωτικής ζωής, η εξουσιοδότηση, η επαλήθευση, ο έλεγχος πρόσβασης, η διαμόρφωση του συστήματος, η αποθήκευση πληροφοριών και η διαχείριση, είναι οι κύριες προκλήσεις σε ένα περιβάλλον IoT
Το άρθρο που μελετήσαμε επικεντρώνεται στις απειλές και τις αδυναμίες της ασφάλειας στο πλαίσιο του IoT και της τελευταίας τεχνολογίας ασφάλειας IoT.
Στοχεύει να χρησιμεύσει ως χρήσιμο εγχειρίδιο των υφιστάμενων απειλών για την ασφάλεια και των τρωτών σημείων του ετερογενούς περιβάλλοντος του IoT και προτείνει πιθανές λύσεις για τη βελτίωση της αρχιτεκτονικής της ασφάλειας του IoT.

Επισκόπηση του IoT

Το IoT έχει τραβήξει την επιστημονική προσοχή καθώς υπάρχει μεγάλη επέκταση στις εφαρμογές που είναι συνδεδεμένες στο Internet. Το IoT απλά σημαίνει διασύνδεση ετερογενών δικτυακών Facebook και συστήματα με διαφορετικά action επικοινωνίας όπως human-to-human, human-to-thing ή thing-to-thing.
Σε ένα τυπικό μοντέλο IoT συναντούμε συσκευές-κόμβους με αισθητήρες που μεταφέρουν πολύ ελαφριά δεδομένα στον φυσικό κόσμο, μέσω cloud-based πόρων και κάνουν επιλογές απ'τα δεδομένα χρησιμοποιώντας έναν ενεργοποιητή (actuator-device) που διαμορφώνουν και καθορίζουν την επικοινωνία μεταξύ των κόμβων.
Το αποτέλεσμα αυτού είναι τα WSN (Wireless sensor network) που είναι το βασικότερο στοιχείο για την ανάπτυξη των συσκευών του IoT. Τα WSN είναι δίκτυα ad hoc.
Η επικοινωνία κόμβων στα WSN θα πρέπει να ικανοποιεί την εμπιστευτικότητα, την αξιοπιστία, την επαλήθευση και τη μη-ανάκληση (non-revocation).
Τα θέματα ιδιωτικότητα και ασφάλειας στο μοντέλο του IoT διαφέρουν από τα συμβατικά και άλλα ασύρματα δίκτυα όσον αφορά την ανάπτυξη και την τεχνολογία που χρησιμοποιείται.

Τα δίκτυα IoT αναπτύσσονται σε δίκτυα χαμηλής κατανάλωσης (low-power lossy networks) (LLN). Τα δίκτυα LLN είναι δίκτυα που περιορίζονται από την ενέργεια, τη μνήμη και την ισχύ επεξεργασίας. Ως εκ τούτου, απαιτείται πολύ ελαφριά τεχνολογία κρυπτογράφησης, η οποία περιλαμβάνει ελαφρύ κρυπτογραφικό αλγόριθμο, χρησιμοποιείται για τη διασφάλιση των περιβαλλόντων IoT. Αυτές οι πτυχές δεν έχουν ληφθεί υπόψη για συμβατικό και άλλο σύγχρονο ασύρματο δίκτυο?
Για παράδειγμα, η ανάπτυξη του IoT είναι πολύ ιδιαίτερη σε σχέση με αυτή του κανονικού Διαδικτύου. Οι συσκευές IoT είναι εγκατεστημένες σε LLN, ενώ άλλες έχουν εξαιρετικά δυναμικές τοπολογίες που βασίζονται στην εκάστοτε εφαρμογή. Τα LLN είναι πλήρως απαλλαγμένα από δυναμισμό, μνήμη και ισχύ επεξεργασίας.
Για αυτό το λόγο τα LLN αντιμετωπίζουν μεγάλες απώλειες δεδομένων εξαιτίας της πλαστοπροσωπίας κόμβων.
Για παράδειγμα, κατά τη διαδικασία της μετάδοσης δεδομένων, εάν ένας εισβολέας μπορεί να συνδεθεί στο δίκτυο χρησιμοποιώντας οποιαδήποτε ταυτότητα, ο εισβολέας μπορεί να θεωρηθεί ως αυθεντικός κόμβος και να υποβάλει σε επεξεργασία την αποστολή εσφαλμένου μηνύματος ελέγχου (erroneous control messages).
Το IoT επίσης έχει θέματα ασφάλειας σε επιθέσεις man-in-the-middle και counterfeit attacks. Και οι 2 επιθέσεις μπορούν να συλλάβουν και να αποστείλουν ψεύτικες πληροφορίες στους επικοινωνούντες κόμβους στο δίκτυο.
Για το σκοπό αυτό χρησιμοποιούνται μηχανισμοί αυθεντικοποίησης και διασφάλισης της εμπιστευτικότητας των δεδομένων για την αποτροπή μη εξουσιοδοτημένων κόμβων.
Στο επίπεδο εφαρμογών ο διαμοιρασμός δεδομένων είναι το κύριο χαρακτηριστικό, πράγμα που δημιουργεί προβλήματα ασφάλειας στο ιδιωτικό απόρρητο δεδομένων, στον έλεγχο πρόσβασης και την απόκρυψη πληροφοριών (information disclosure).
Τα δίκτυα IoT όμως σε σχέση με τα συμβατικά δίκτυα IoT διαφέρουν όμως και σε επίπεδο επικοινωνία. Για παράδειγμα, το IPv6 χρησιμοποιείται σε ασύρματα δίκτυα προσωπικών περιοχών χαμηλής κατανάλωσης στο physical/virtual στρώμα IoT, ενώ η ασύρματη πιστότητα χρησιμοποιείται στο φυσικό επίπεδο σε συμβατικά δίκτυα.
Τα ζητήματα ασφαλείας και στα δύο δίκτυα ενδέχεται να είναι παρόμοια, αλλά χρησιμοποιούνται διαφορετικές προσεγγίσεις και τεχνικές για το χειρισμό κάθε προβλήματος ασφάλειας δικτύου

Ταξινόμηση του IoT

Το IoT μπορεί να κατηγοριοποιηθεί σε 3 επίπεδα.

Application Layer

Το επίπεδο εφαρμογής είναι το ανώτερο στρώμα και είναι ορατό στον τελικό χρήστη. Ένα πρωτόκολλο επιπέδου εφαρμογής διανέμεται σε συστήματα πολλαπλών άκρων, όπου η εφαρμογή σε ένα τελικό σύστημα χρησιμοποιεί ένα πρωτόκολλο για την ανταλλαγή πακέτων πληροφοριών με μια εφαρμογή σε ένα άλλο τελικό σύστημα. Για αυτό το λόγω τα θέματα ασφαλείας στο επίπεδο εφαρμογής διαφέρουν στη βιομηχανία (παροχής της υπηρεσίας πιθανώς) και στο περιβάλλον (environment).
Παραδείγματα αυτού του επιπέδου περιλαμβάνουν εφαρμογές του τύπου smart environment (Denial of Service attacks), smart grid (θέματα ασφάλειας πελάτη, θέματα φυσικής ασφάλειας, εμπιστοσύνης – endpoints on devices & malicious attacks) , hearth-care system (θέματα με την φυσική ύπαρξη health card) & intelligent transportation (Electronic Fee Collection – EFC).

Perception Layer

Το επίπεδο αντίληψης περιλαμβάνει τη συλλογή πληροφοριών. Αυτό το στρώμα ταξινομείται σε δύο τμήματα, δηλαδή στον κόμβο αντίληψης (αισθητήρες, ελεγκτές και ούτω καθεξής) και το δίκτυο αντίληψης που διασύνδεει το στρώμα δικτύου.

Τα δεδομένα αποκτώνται και ελέγχονται στον κόμβο αντίληψης, ενώ οι οδηγίες ελέγχου για την αποστολή και τον έλεγχο δεδομένων πραγματοποιούνται στο επίπεδο δικτύου αντιλήψεων. Οι τεχνολογίες στρώματος αντίληψης περιλαμβάνουν όλους τους τύπους αισθητήρων, όπως RFID, ZigBee, κόμβους αισθητήρων και πύλες αισθητήρων (nodes/gateways).

RFID: DoS, repudiation, spoofing, eavesdropping, data newness, accessibility, self organization, time management, secure localization, tractability, robustness, survivability, and counterfeiting

Sensor nodes: ευάλωτοι σε διαφορετικές απειλές και επιθέσεις, οι οποίες περιλαμβάνουν ανατροπή κόμβου, αποτυχία κόμβου, διακοπή κόμβου, παθητική συλλογή πληροφοριών, διαφθορά μηνυμάτων ψευδούς κόμβου, εξάντληση, αδικία, Sybil, εμπλοκή, παρεμβολές και συγκρούσεις.

Sensor gateways: λανθασμένη διαμόρφωση, hacking, απώλεια σήματος, DoS, dialing, protocol tunneling, man-in-the-middle attack, interruption interception, and modification fabrication.

Network Layer

Το στρώμα δικτύου παρέχει ασφάλεια μετάδοσης δικτύου και πληροφοριών και παρέχει ένα περιβάλλον διαβίβασης στο perception layer, δηλαδή συνειδητοποίηση της μετάδοσης δεδομένων και αποθήκευσης. Το επίπεδο δικτύου περιλαμβάνει τις κινητές συσκευές, το cloud computing και το Internet.
Στη συνεχεία γίνεται μια επισκόπηση των απειλών και αδυναμιών που εμφανίζονται διάφορες υπάρχουσες αρχιτεκτονικές που έχουν προταθεί ή και εφαρμόζονται σήμερα. Παρουσιάζει σύντομα τη κάθε αρχιτεκτονική και υστέρα αναφέρει τις αδυναμίες και τις ευπάθειες της. Αυτές περιλαμβάνουν αδυναμίες στην εμπιστευτικότητα και ιδιωτικότητα λέγω χρήσης «ελαφριάς» κρυπτογραφίας για τη κρυπτογράφηση των κρισίμων δεδομένων ή και λέγω αδυναμιών στην αυθεντικοποίηση, ευπάθεια σε επιθέσεις DDoS λέγω αργής επεξεργασίας και προαγωγής των πακέτων και απαιτήσεις αυξημένης υπολογιστικής ισχύς λέγω χρήσης «βαριών» κρυπτογραφικών μεθόδων. Άλλα και άλλα αρνητικά χαρακτηριστικά αυτών των αρχιτεκτονικών όπως μη υποστήριξη VoIP κα. Τονίζει ότι καμιά από αυτές δεν έχει τα παρακάτω χαρακτηριστικά:

- Μια λύση ιδιωτικού απορρήτου για τον ορισμό των θέσεων κόμβων και το χειρισμό νέων προκλήσεων δρομολόγησης που δημιουργούνται κατά την κρυπτογράφηση κεφαλίδας για τους κόμβους IoT που κοιμούνται (δηλαδή, μια ασφαλή αρχιτεκτονική IoT που βοηθά στην αντιμετώπιση μεταφράσεων, καθορίζοντας την ιδιωτικότητα τους τοποθεσίας και χαρακτηρίζοντας την κινητικότητα
- Απλή συμμετρική λύση κρυπτογραφίας σε τρίτους τους περιορισμένους κόμβους για εκφόρτωση
- Διαχείριση χειρότερων επιδόσεων στην επεξεργασία πακέτων ως αποτέλεσμα του διαχωρισμού των επιπέδων ελέγχου και δεδομένων στον SDN (δηλαδή, ο μόνος

τρόπος για να βελτιωθεί Η απόδοση SDN είναι να εξασφαλιστεί η ενσωμάτωση των επιπέδων ελέγχου και δεδομένων, έτσι ώστε η τεχνολογία SDN να μπορεί να χρησιμοποιεί εφαρμογές τους κρυπτογράφηση, ανάλυση και ταξινόμηση τους κυκλοφορίας)

- Αφήνοντας τους κόμβους να περιορίζουν δυναμικά το κοινόχρηστο κλειδί με οποιαδήποτε ασύρματη λειτουργία με την οποία δεν έχουν δημιουργηθεί προηγούμενες κοινές γνώσεις (τα τρίτα μέρη είναι αφιερωμένα στην υποστήριξη των περιορισμένων κόμβων σε αυτό διαδικασία για την επίτευξη αυτού του στόχου)
- Διασφάλιση τους κώδικα E2E όπου καμία οντότητα δεν έχει τη γνώση του ανταλλασσόμενου μυστικού εκτός από τους περιορισμένους κόμβους και τα ασύρματα πράγματα
- Επίσης επισημαίνει ότι βάσει της ανάλυσης των υπαρχουσών αρχιτεκτονικών, προκύπτει η ανάγκη για δημιουργία μιας νέας απλής και ειδική ταξινόμησης στη ασφάλεια για την απλή και συγκεκριμένη κατηγοριοποίηση των κλάσεων των απειλών και αδυναμιών σε κάθε τομέα εφαρμογής IoT. Κάτι που θα διευκολύνει όπως αναφέρει θα βοηθήσει στη συνεχεία να καθοριστούν οι λειτουργίες και οι επιδόσεις κάθε τομέα σε διαφορετικές απειλές και ευπάθειες και να μελετηθεί πώς τα αντίμετρα ασφαλείας μπορούν να βελτιώσουν τις υπηρεσίες ασφαλείας σε κάθε τομέα εφαρμογής IoT.

Ασφάλεια στα επιμέρους επίπεδα του IoT

Ασφάλεια στο επίπεδο της Εφαρμογής

Στη συνεχεία αναλύει την ασφάλεια που πρέπει να περιέχει το επίπεδο της εφαρμογής των συσκευών του IoT. Οι πιο συνηθισμένες τεχνικές ασφαλείας που θεωρούνται με τις περιπτώσεις χρήσης σε αυτόν τον τομέα εφαρμογής είναι (I) η πιστοποίηση ταυτότητας, (ii) η εξουσιοδότηση, (iii) η εξάντληση των πόρων και (iv) η εγκατάσταση εμπιστοσύνης.

i. Πιστοποίηση

Στον τομέα εφαρμογής IoT, ο έλεγχος ταυτότητας επιτρέπει την ενσωμάτωση διαφόρων συσκευών IoT και την ανάπτυξή τους σε διάφορα έξυπνα περιβάλλοντα, όπως οι έξυπνες πόλεις.

ii. Εξουσιοδότηση

Η εξουσιοδότηση περιλαμβάνει τον καθορισμό δικαιωμάτων πρόσβασης σε πόρους, όπως οι συσκευές υγειονομικής περίθαλψης, που σχετίζονται με την ασφάλεια των πληροφοριών και έλεγχος πρόσβασης.

iii. Προφύλαξη Εξάντλησης Πόρων

Η υψηλή ζήτηση για όλους τους πόρους, όπως πηγές ενέργειας, μπορεί να σε μεγάλο βαθμό να επηρεάσει την απόδοση διαφορετικών εφαρμογών, γεγονός που μπορεί με τη σειρά του να οδηγήσει σε διαρροές πόρων και υπερφόρτωση του IoT.

iv. Εδραίωση Εμπιστευτικότητας

Ένας πειστικός μηχανισμός πρέπει να είναι διαθέσιμος για την εδραίωση της εμπιστοσύνης μεταξύ των φυσικών αντικειμένων και γεγονότων του IoT όπως διασυνδεδεμένα WSNs, RFID – βασισμένα συστήματα και κινητά τηλεφωνά.

Γίνεται επίσης αναφορά στα υπάρχοντα σχεδία για την υλοποίηση εφαρμογών που ικανοποιούν τη χρήση τέτοιων τεχνικών και χαρακτηρίζονται όσο αναφορά τα αρνητικά τους στοιχειά, της αδυναμίες και τις ευπάθειες που αυτά έχουν.

Ασφάλεια στο επίπεδο Αρχιτεκτονικής

Γενικά δεν υπάρχει κάποια universal αρχιτεκτονική IoT. Έχουν γίνει αρκετά ήδη έρευνας για την αρχιτεκτονική του IoT σε διαφορετικά σενάρια και domain εφαρμογών όσο αφορά το αυθεντικοποίηση και την αδειοδότηση (authentication & authorization).

Smart environment	SDN
	Η αρχιτεκτονική SDN βοηθά στην εξάλειψη της ακαμψίας στα παραδοσιακά δίκτυα. Τα SDN επιτρέπουν στους διαχειριστές να έχουν μια συνολική προοπτική του συστήματος και την ικανότητα να ελέγχουν το δίκτυο σύμφωνα με τις απαιτήσεις κάθε οργανισμού. Τα SDN απλοποιούν τη χρήση και τη λειτουργία του δικτύου, μειώνοντας το συνολικό κόστος των δικτύων οργάνωσης παρέχοντας προγραμματιζόμενες υπηρεσίες δικτύου. Ωστόσο, υπάρχουν πολλές αδυναμίες ασφαλείας σε SDN. Έλλειψη καλών μηχανισμών αυθεντικοποίησης Ένας επιτιθέμενος μπορεί να ανακατασκευάσει την κίνηση του δικτύου και να πάρει πρόσβαση σε εμπιστευτικά αρχεία.
Healthcare	SEA
	DTLS handshake protocol (public key authentication & ECC primitives) ECDH – ECDSA (Diffie Hellman – Signature Algorithm) DoS attacks, θέματα privacy
Smart City	Smart City / Black SDN
Smart transportation	Service-Oriented
	Αρχιτεκτονική επικεντρωμένη στην διαχείριση της πληροφορίας & την ασφάλεια Γενίκευση τις αοριστίας των υπηρεσιών μεταξύ των IoT συσκευών, εγγυώντας confidentiality, integrity & την προστασία καναλιών επικοινωνίας
Smart grid	OSCAR: Object Security
	E2E security (802.15.4 LLN & M2M communication χρησιμοποιώντας MAC layers με real testbed και τον προσομοιωτή Cooja) CoAP nodes που είναι απαραίτητο το authorization για την απαίτηση πόρων + multicasting (authorization for E2E) Βασικό μειονέκτημα το latency του ECSDSA authorization Μη εξουσιοδοτημένοι χρήστες μπορούν να πάρουν πρόσβαση στον έλεγχο όλου του συστήματος.
Business organizations	Conceptual Organizations Framework

Αυθεντικοποίηση στην αρχιτεκτονική του IoT

Η εξουσιοδότηση στην αρχιτεκτονική του Διαδικτύου επιτυγχάνεται με την ανταλλαγή αναγνωρισμένων δεδομένων μεταξύ των συνδεδεμένων αντικειμένων. Αυτή η διαδικασία είναι ευάλωτη στην υποκλοπή, η οποία μπορεί να οδηγήσει σε μια επίθεση MitM που διακινδυνεύει ολόκληρο το πλαίσιο της Διασύνδεσης IoT.

Ασφάλεια στο επίπεδο της Επικοινωνίας

Η επικοινωνία του IoT περιλαμβάνει ανταλλαγή πληροφοριών / ανταλλαγή πληροφοριών μεταξύ των συσκευών του ή μεταξύ διαφορετικών του στρωμάτων. Με τις τεράστιες δυνατότητες του IoT σε πολλούς τομείς, ολόκληρη η υποδομή επικοινωνίας του IoT είναι ασυμβίβαστη με την προοπτική ασφάλειας και ευάλωτη στην απώλεια της ιδιωτικής ζωής από την οπτική γωνία των τελικών χρηστών.
Περιγράφει τις πιθανές επιθέσεις στο κανάλι ως εξής:

i. MitM επιθέσεις

Κατά τις επιθέσεις Man in the Middle, ένας εισβολέας μεταδίδει σιωπηλά και πιθανόν τροποποιεί την επικοινωνία μεταξύ δύο συσκευών. Για παράδειγμα, ένας εισβολέας μπορεί να θέλει να πλαστογραφήσει τις πληροφορίες θερμοκρασίας από μια συσκευή παρακολούθησης εντός του IoT για να αναγκάσει τη συσκευή να υπερθερμανθεί, η οποία μπορεί να σταματήσει τη λειτουργία της συσκευής. Τα ελαφριά κρυπτογραφικά πρωτόκολλα θεωρούνται ότι παρέχουν ασφάλεια επικοινωνιών για τις συσκευές IoT μέσω ενός δικτύου υπολογιστών ως μέρος του DTLS. Ωστόσο, οι επιθέσεις MitM εκμεταλλεύονται τα ελαττώματα στα πρωτόκολλα ελέγχου ταυτότητας που χρησιμοποιούνται από τα επικοινωνούντα μέρη.

ii. Eavesdropping

Η υποκλοπή δεδομένων παρατηρείται στο στρώμα δικτύου στο Διαδίκτυο και παίρνει τη μορφή του data sniffing. Το Eavesdropping επίσης δημιουργεί μοναδικές προκλήσεις για την αρχιτεκτονική του IoT, ιδιαίτερα όταν ένας εισβολέας στοχεύει τα κανάλια επικοινωνίας για να εξαγάγει δεδομένα από τη ροη των πληροφοριών.

Έτσι, οι επιθέσεις MitM και υποκλοπής στο IoT εμφανίζονται μεταξύ των δυναμικών κόμβων αισθητήρων που δεν απαιτούν έναν dedicated κεντρικό εξυπηρετητή, σε αντίθεση με το συμβατικό δίκτυο όπου ένας αποκλειστικός διακομιστής χρησιμοποιείται για τον έλεγχο της κυκλοφορίας παρακολούθησης.

Ασφάλεια στα Δεδομένα

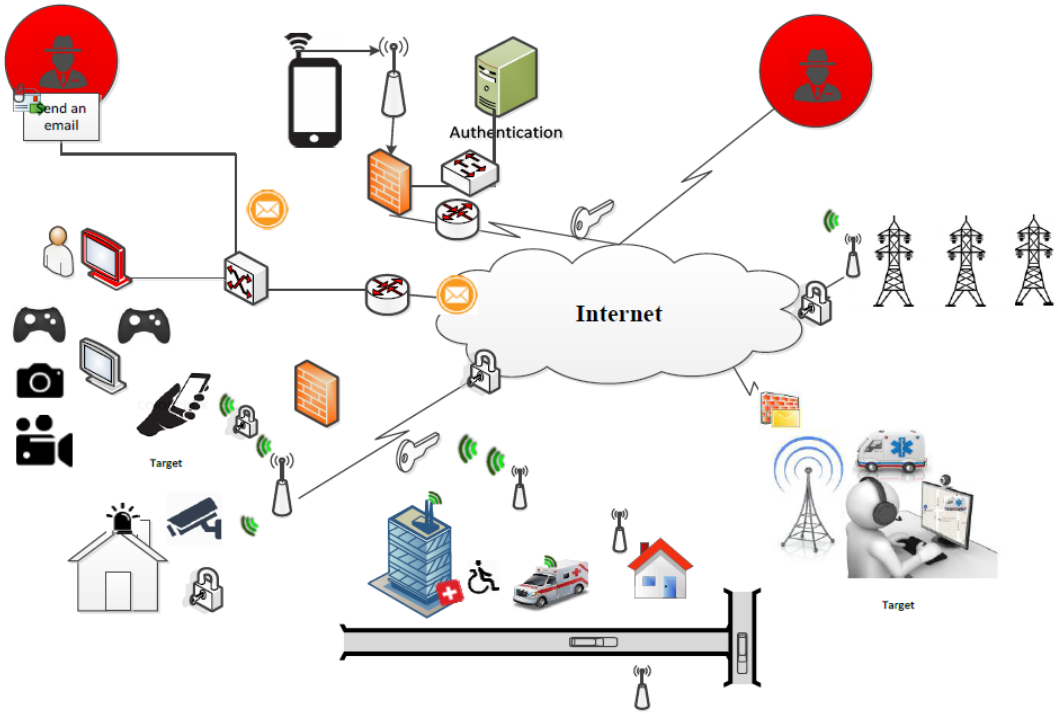
Το απόρρητο και η εμπιστοσύνη των χρηστών πρέπει να προστατεύονται για την πλήρη ανάπτυξη και αποδοχή του IoT. Η εμπιστοσύνη συνεπάγεται τη διατήρηση της ιδιωτικής ζωής των χρηστών, η οποία περιλαμβάνει προσωπικά δεδομένα χρηστών, από την πολιτική και την προοπτική των χρηστών με ευέλικτο τρόπο. Η μετάδοση και ο υπολογισμός της εμπιστοσύνης μεταξύ διαφορετικών κόμβων σε ένα ετερογενές IoT είναι ένα δύσκολο ζήτημα, διότι διαφορετικοί κόμβοι δικτύου έχουν διαφορετικά κριτήρια αξιοπιστίας. Οι υπηρεσίες ασφαλείας που παρέχονται από το IEEE 802.15.4 είναι αυθεντικότητα δεδομένων, εμπιστευτικότητα δεδομένων και προστασία από replay attacks. Οι κύριες απειλές για αυτό το πρωτόκολλο είναι τα κρυπτογραφημένα πλαίσια ACK, οι μετρητές πλαισίων χωρίς χρονικό διάστημα και το επίπεδο ασφάλειας NULL. Όταν το πλαίσιο ACK δεν είναι κρυπτογραφημένο, ένας εισβολέας μπορεί να παρεμποδίσει ένα πλαίσιο MAC και να κατασκευάσει ένα πλαίσιο ACK με έναν αριθμό ακολουθίας, με αποτέλεσμα την απώλεια πλαισίου χωρίς αναμετάδοση.

Τέλος συνοψίζει σε ένα πίνακα τις απειλές που υφίστανται σε κάθε επίπεδο του IoT.

Επίπεδο	Απειλές
Φυσικό	Micro-probing, παραβίαση σκληρών εξαρτημάτων, jamming
Σύνδεσμοι	Συγκρούσεις, αδικίες, εξάντληση, επανάληψη, επιθέσεις meta-data
Δίκτυο	Παραμέληση, απληστία, προσέλκυση, κακή διεύθυνση, ανάλυση κυκλοφορίας, μαύρες τρύπες, επιθέσεις μεταδιδομένων

Σενάριο Ασφάλειας IoT

Στη συνεχεία του άρθρου παρουσιάζεται ένα σενάριο για να δειχτεί πόσο σημαντική είναι η ανάγκη να αναπτυχθεί ένας ασφαλής τύπος αρχιτεκτονικής IoT που να ικανοποιεί τα πρότυπα ασφάλειας των νέων υπηρεσιών δικτύου όπου πολλαπλές συσκευές και αισθητήρες επικοινωνούν μεταξύ τους με ασφάλεια περιβάλλον.



Στο σενάριο που παρουσιάζεται ένα εικονικό σύστημα υγειονομικής περίθαλψης θεωρείται ότι απεικονίζει την επικοινωνία μεταξύ διαφορετικών χρηστών. Ας υποθέσουμε α ο χρήστης με μια συσκευή υγειονομικής περίθαλψης είναι στο σπίτι και πρέπει να επικοινωνήσει με ένα νοσοκομείο για να ζητήσει βοήθεια. Η κινητή συσκευή και οι πληροφορίες των χρηστών και των νοσοκομείων που χρησιμοποιούν διαφορετικά δίκτυα και οι συσκευές παραμένουν εκτεθειμένοι σε χακέα και τύπους επιθέσεων σε όλα τα επίπεδα του IoT. Εκτός από την διαθέσιμη ασφάλεια στα τρέχοντα δίκτυα, η ασφάλεια χαρακτηριστικών πρέπει να επικεντρώνεται στις απαιτήσεις για τις συσκευές περιορισμένης χρήσης κατά τη διάρκεια της επικοινωνίας. Ωστόσο, τα τρέχοντα δίκτυα δεν μπορούν να ικανοποιούν επαρκώς τις απαιτήσεις ασφαλείας των ευαίσθητων εφαρμογών δεδομένων. Η ασφάλεια δικτύων και συσκευών είναι δύο σημαντικές απαιτήσεις που πρέπει επίσης να ληφθούν υπόψη κατά τον σχεδιασμό της αρχιτεκτονικής ασφάλειας για περιορισμένους εξοπλισμούς

Σύγχρονες απειλές και ευπάθειες του IoT

Σε ένα σύγχρονο περιβάλλον IoT αναμένεται να χρησιμοποιούνται πιθανώς δισεκατομμύρια συνδεδεμένων αντικειμένων IoT, πράγμα που μπορεί να γίνει επίκεντρο επιθέσεων καθώς η παγκόσμια διαθεσιμότητα και η συνδεσιμότητα είναι 2 εξαιρετικά βασικοί κόμβοι στο IoT.
Το IoT γενικότερα έχει θέματα ασφάλειας και ιδιωτικότητα που πρέπει να αντιμετωπισθούν προκειμένου να μπορεί να χρησιμοποιηθεί διαφορετικά σε μεγαλύτερη κλίμακα.
Οι απειλές στο IoT κατά βάση χωρίζονται σε 3 κατηγορίες:

Hardware threats:

RFID threats (tags) - tracking, DoS, repudiation, spoofing, eavesdropping, and counterfeiting
ZigBee - packet manipulation, hacking, key exchange, KillerBee, and Scapy
Bluetooth - eavesdropping, DoS, Bluesnarfing, Bluejacking, car whisperer, and Bluebugging
Sensor nodes - DoS, exhaustion, unfairness, Sybil, jamming, tampering, and collisions.

Network threats:

Wired - data manipulation, extortion hack, equipment hijacking, Signaling System No. 7, and malicious attacks
Wireless - misconfiguration, hacking, signal loss, DoS, war dialing, protocol tunneling, and MitM

Smart Application threats:

Smart City - smart city DoS, information manipulation, fake seismic detection, and fake flood detection
Smart Grids - customer security, physical security, trust between traditional power devices, device endpoints, and malicious attacks
HealthCare - theft and loss, insider misuse, unintentional actions, hacking, internal attacks, and cyber attacks
Intelligent transporation - traffic control, parking, and public transportation

Bluetooth		safe and convenient								
Sensors node	Sensors and Actuators	Flexibility, Higher latency in communication	DoS, Exhaustion, Unfairness, Sybil	Flooding, Routing Protocols	Jamming, Tampering, Collisions	±	±	+	+	+
Network Infrastructure										
Wired	Cable, Network adapters, and Router	Enhanced security, Greater Reliability and Ease of use	Manipulation of data, Extortion hack	Signaling system No.7 (SS7), Hijacking of equipment	Weak Link, Malicious attacks	+	±	+	+	+
Wireless	Radio Communication, transmitters, and receivers	Enhanced guest access, Easier network expansion, Increased mobility and collaboration	Rogue access points, Misconfiguration	Hacking, Signal lost	DoS, War dialing, protocol tunneling; man-in-the-middle	±	±	±	+	+
Smart Application										
Smart City	e-governance, Street Lighting, Water and Waste Management	Better city planning, Faster delivery of service, Economic development	Smart City DoS, Manipulation of information	Fake seismic detection, fake flood detection	Mobile apps, Sensors	±	±	±	±	-
Smart grid	Smart meters, Smart Energy	Reliability, cost savings, and energy independence	Customer security, Physical security	trust between traditional power devices	End points on devices, malicious attacks	±	±	±	±	±
Healthcare	Smart health cards	improves patients security and privacy details	Theft and loss, Insider misuse, Unintentional actions	Hacking	Internal attack, cyber attack	±	±	±	-	-
Smart Transportation	Traffic control, Parking, Public Transportation	Ease-of-use	Smart City DoS	Security plagued	Cyber-attacks	-	-	±	±	±

Group	Features	Benefits	Threats	Vulnerability	Attacks	Confidentiality	Integrity	Authentication	Availability	Non-repudiation
Hardware										
RFID	Unique identity, Auto identification, and Unique identity	Rapid exchange of information between tags and readers through wireless connection	Tracking, DoS, Repudiation, Spoofing	Alteration, Corruption and Deletion	Eavesdropping, Counterfeiting,	-	-	-	+	-
ZigBee	Radio, Microcontroller, Simple protocol and Small size	Reliable, Low power consumption Low Cost	Packet manipulation	Hacking	Key exchange, KillerBee, and Scapy	±	+	±	+	±
	Frequency hopping spectrum	Allows two devices to connect wirelessly very	Eavesdropping, DoS	Bluesnarfing Bluejacking	Car Whisperer, Bluebugging,	-	-	±	±	±

Μελλοντικές προκλήσεις στον τομέα της ασφάλειας του IoT.

Προκλήσεις στην Ασφάλεια

Ασφαλή smart grids

Δεν έχει γίνει σε βάθος έρευνα για το σημείο κλειδί στην ασφάλεια των smart grids και των energy-aware smart homes πράγμα που καθιστά τους end-users ευάλωτους σε απειλές όπως πλαστογράφηση πλαστοπροσωπία / ταυτότητα, παραβίαση δεδομένων και μη εξουσιοδοτημένη πρόσβαση ελέγχου όταν χρησιμοποιούνται έξυπνοι μετρητές / έξυπνες συσκευές.
Ένα άρθρο που μελετήθηκε στο άρθρο που μελετάμε αφορά την χρήση embedded IoT εφαρμογές κινητού υπολογισμού με τεχνικές cloud όπως mobile sensor data processing engine, αλλιώς γνωστό ως mobile fog.

Lightweight authentication

No-pairing Attribute-Based Encryption (ABE) – κακό scalability και δεν μπορεί να κάνει revoke attributes και κατά συνέπεια δεν μπορεί να υπάρχουν multi-authority εφαρμογές
Pervesive verification mechanism for WSN (DTLS scheme), PAuthKey protocol – πολλαπλά security threats και προβλήματα όπως το access control και το multicasting. Απαιτείται να γίνει περαιτέρω μελέτη για ένα certificate scheme για access control και multicasting μεγάλης κλίμακας καθώς επίσης πρέπει να ενταχθούν σε αυτό αρκετά πρωτόκολλα ασφάλειας που μπορούν να διαχειριστούν θέματα απειλών σε κατανεμημένες δικτυακές εφαρμογές IoT.
Secure channel establishment (έλεγχος confidentiality level) μέσω ενός sensor, πράγμα που κάνει διαθέσιμη την πληροφορία μόνο ενός σεναρίου (π.χ. sensitivity) και κατά συνέπεια πρέπει να αναπτυχθούν πολυδιάστατοι αισθητήρες.

Heterogenity

Calvin (framework που συνδυάζει το IoT και το cloud) – αποφυγή ενός direct device-to-cloud client/server approach. Ακόμα είναι στις αρχικές φάσεις του development λόγω της υβριδικής του φύσης.
Certificate-Less Cryptography (CLC) based on Identity-Based Cryptography (IBC). Το βασικό χαρακτηριστικό της είναι η ετερογένοια. Πιο συγκεκριμένα οι οντότητες που αποστέλλουν μηνύματα ανήκουν σε 2 διαφορετικά κρυπτογραφικά περιβάλλοντα (π.χ. ένας sender χρησιμοποιώντας CLC μπορεί να μεταδώσει ένα πακέτο με IBC μέσω cyphertext authenticity που επιτρέπει την μείωση του υπολογιστικού κόστους στο gateway. Το CLC δεν απαιτεί certificates, παρόλα αυτά, χρησιμοποιεί ένα trusted third party που ονομάζεται Key Generating Center που είναι υπεύθυνο για την δημιουργία ενός ημιμερούς κλειδιού που χρησιμοποιεί την ταυτότητα του χρήστη και ένα master key.

QoS

Επιλύσεις που υπάρχουν στον τομέα του QoS είναι τα:
Adaptive edge (fog) (βασισμένο πάνω σε Regressive Admission Control -REAC – βοηθάει) – optimize and control traffic flaws and network resources
Fuzzy Weighted Queueing (FWQ) – control with feedback for system stability, short settling times & fast responise time.

Γενικότερα ο τομέας του QoS αντιμετωπίζει προβλήματα interoperability και άλυτα metric issues όπως η συνδεσιμότητα, η αξιοπιστία και το delay.

Black SDN

Μια έκδοση του SDN που κρυπτογραφεί το header και το payload του network layer. Αυτή η μέθοδος αντιμετωπίζει ενεργά κάποιες επιθέσεις και βελτιώνει τον προβλεπόμενο χρόνο ζωής και την δικτυακή επίδοση στα δίκτυα IoT. Ένα black network είναι ένα application delivery network που παρέχει μια υπηρεσία για να διασφαλίζει όλα τα δεδομένα (πράγμα που μειώνει την αποδοτικότητα του δικτύου όμως και κάνει τη δρομολόγηση πιο περίπλοκη). Αυτό που χρειάζονται τα black networks είναι sleep synchronization protocols προκειμένου να σιγουρεύεται το packet delivery σε όλους τους κόμβους και να διασφαλίζεται το black link layer frame μέσω πολλαπλών μεθόδων.

AWFQ

Queue status & priority assignment προκειμένου για ελεγχθεί ο διαμοιρασμός του bandwidth και να διασφαλισθεί ότι κάποιο QoS defined policy για resource-constrained devices.

Trust Management

Η ιδιωτικότητα των κόμβων και των χρηστών του Διαδικτύου είναι εξαιρετικά σημαντική και πρέπει να εξεταστεί σοβαρά κατά την ανάπτυξη του Συσκευές IoT. Η Trust Management (TM) περιλαμβάνει τη διαφύλαξη της ιδιωτικής ζωής των χρηστών, όπως προσωπικά δεδομένα χρήστη, από την πολιτική και το προοπτική των χρηστών του Διαδικτύου με ευέλικτο τρόπο. Έτσι, η ενσωμάτωση της TM στις συσκευές RFID του IoT είναι απαραίτητη. Επιπλέον, TM όχι μόνο συμβαίνει μεταξύ των συσκευών ανάγνωσης και των ετικετών RFID κατά την επικοινωνία, αλλά και μεταξύ των συσκευών ανάγνωσης και της βάσης σταθμούς. Η τεχνολογία ψηφιακών υπογραφών χρησιμοποιείται στην περιοχή TM. είναι σημαντικό στην περιοχή εμπιστοσύνης επειδή χρησιμοποιείται για (δηλ. και στις συσκευές IoT και στα δεδομένα) και κατά τη διάρκεια της επικοινωνίας δεδομένων μεταξύ διαφορετικών εφαρμογών IoT
Όμως τονίζει πως λίγοι τύποι έρευνας έχουν εκτελεστεί για το TM στον τομέα IoT.

Υστέρα παρουσιάζει στοιχεία από διάφορες πρόσφατες μελέτες που έχουν διεξαχθεί σχετικά με το TM για το IoT και έχουν προταθεί διαφορετικά μοντέλα εμπιστοσύνης. Αυτά τα μοντέλα εμπιστοσύνης μπορούν να συμπεριληφθούν στην θέσπιση και ανάπτυξη του TM για το IoT. Το όποιο παραμένει ακόμα ανοιχτό θέμα.

Υποδομή

Σε αυτό το τμήμα επισημαίνονται διάφορες προκλήσεις που υπάρχουν και σχετίζονται με την υλοποίηση ασφαλών υποδομών IoT για τις παρακάτω περιπτώσεις.

SDN

Η κρυπτογράφηση του header δημιουργεί πρόκληση στη δρομολόγηση για τους κόμβους του IoT, που συχνά “κοιμούνται”. Ως εκ τούτου, πρέπει να αναπτυχτούν και να σχεδιαστούν sleep synchronization πρωτόκολλα που είναι κατάλληλα για τα black networks για την εξασφάλιση της παράδοσης του πακέτου σε όλους τους κόμβους και ένα ασφαλές τύπο αρχιτεκτονικής IoT που μπορεί να βοηθήσει στην αντιμετώπιση των address translations και να καθορίσει την ιδιωτικότητα της τοποθεσίας
Πρέπει να αναπτυχθεί ένα πλαίσιο για το software-defined framework μοντέλο SDIoT για τη διερεύνηση διαφόρων τύπων τοπολογιών IoT που να μπορεί να αντιμετωπίσει ζητήματα ασφάλειας και διαλειτουργικότητας στο SDN.

Smart e-health

Απαιτούνται ασφαλείς δικτυακές υποδομές για επικοινωνία μικρής εμβέλειας, για να περιοριστούν οι κίνδυνοι στην αρχιτεκτονική. Πρέπει να αναπτυχθεί ένας τύπος αρχιτεκτονικής που μπορεί να καλύψει μια ολόκληρη πόλη χωρίς να παραμελήσει οποιαδήποτε περιοχή και να εκτελέσει πειράματα σχετικά με την ιδέα που συζητήθηκε.

Ενδιάμεσο Λογισμικό

Χρειάζεται να αναπτυχθεί ένα σύστημα αντιμέτρων ασφαλείας στην αρχιτεκτονική για ενδιάμεσα λογισμικά του IoT για προστασία από επιθέσεις. Μια ενιαία αρχιτεκτονική ασφάλειας IoT δεν έχει ακόμη διαμορφωθεί. Επομένως, είναι απαραίτητη η κρυπτογράφηση του σήματος RFID μέσω κατάλληλου αλγορίθμου για την ασφάλεια των δεδομένων. Επιπλέον, πρέπει να δημιουργηθεί ένας ακριβής ενοποιημένος μηχανισμός ελέγχου ταυτότητας, ο έλεγχος ταυτότητας E2E, ο μηχανισμός συμφωνίας κλειδιών, η υποδομή δημόσιου κλειδιού (PKI), το ασύρματο PKI, η δρομολόγηση ασφαλείας και η ανίχνευση εισβολής για διαφορετικούς τύπους αρχιτεκτονικών δικτύων

Αξιολόγηση Άρθρου

Το άρθρο γενικά καλύπτει το στόχο του ο οποίος είναι να αναδείξει τα κενά στο θέμα της ασφάλειας που υπάρχουν στο IoT και να τονίσει την σημαντικότητα της ανάπτυξης τεχνολογικών λύσεων για την διατήρηση της ασφάλειας. Γενικά συνοψίζει τα πιο πρόσφατα και σημαντικά άρθρα μελέτες και υλοποιήσεις που έχουν γίνει τα τελευταία χρόνια πάνω σε αρχιτεκτονικές, μοντέλα, μεθόδους για διαφέρεις τομείς του ΙoT και έπειτα τονίζει τις αδυναμίες τους και τι χρειάζεται να γίνει για να εδραιωθεί τόσο η ασφάλεια στην ιδιωτικότητα, εμπιστοσύνη μεταξύ των οντοτήτων του IoT όσο και αξιοποιήστε τους. Το ύφος και η γλωσσά είναι γενικά απλή και επιστημονική ωστόσο περιέχει και χωρία που έχουν πιο ειδικές άνοιες και απαιτούν την μελέτη άλλων άρθρων διότι εισάγονται νέες άνοιες. Κάνει παραπομπές σε πολλές βιβλιογραφικές αναφορές και καλύπτει ευρύ φάσμα των στοιχείων και περιπτώσεων του IoT. Ωστόσο συχνά μοιάζει να επαναλαμβάνεται το παραθέτοντας στοιχειά από άρθρα