IOT SECURITY AND PRIVACY

Στεφάκης Παύλος

Επιβλέπων: Ψάννης Κωνσταντίνος

Τι είναι το IoT

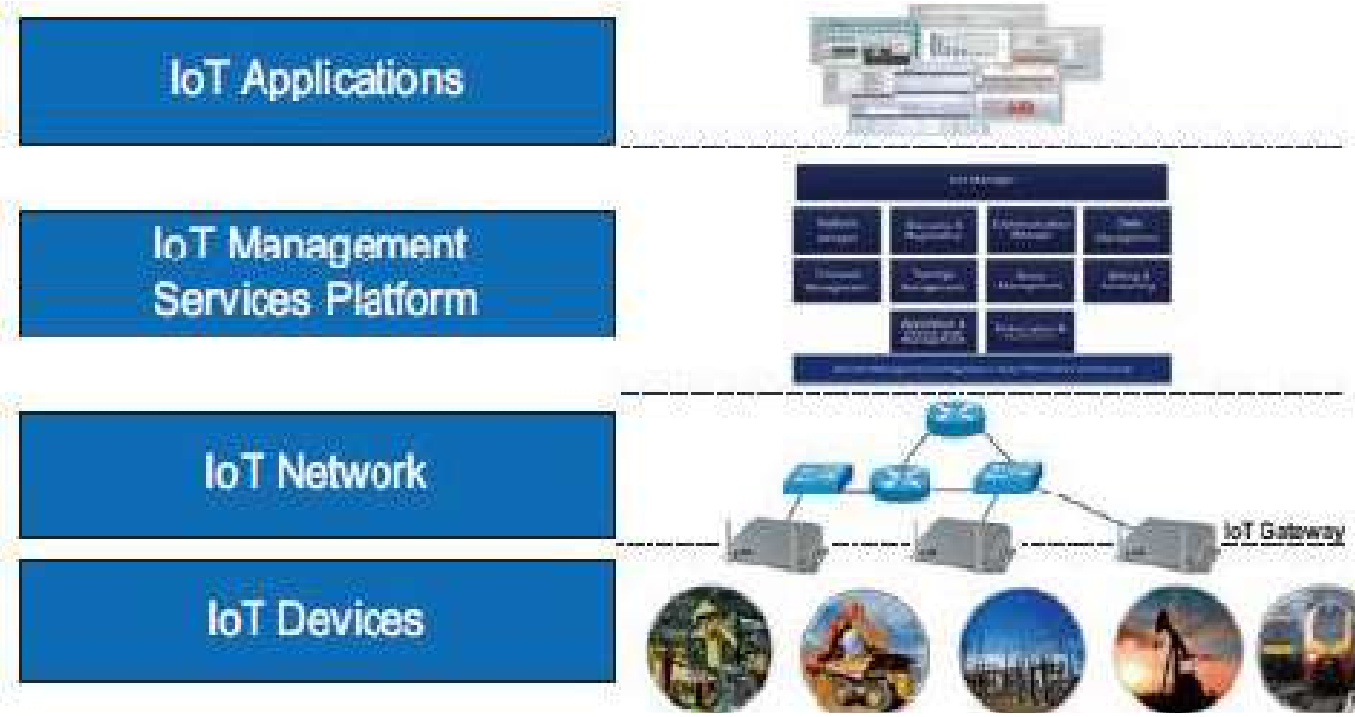
Το “διαδίκτυο των πραγμάτων” (“internet of things” – iot) είναι μια συλλογή από “πράγματα” , τα οποία είναι συνδεδεμένα με τη χρήση του διαδικτύου για τη συλλογή και ανταλλαγή δεδομένων μεταξύ τους.[1]

Ιστορική αναδρομή

- Η κύρια ιδέα ενός δικτύου έξυπνων συσκευών συζητήθηκε ήδη από το 1982, με ένα τροποποιημένο μηχάνημα αυτόματης πώλησης της coca-cola στο πανεπιστήμιο carnegie mellon [2]
- Η έννοια του "διαδικτύου των πραγμάτων" και ο ίδιος ο όρος, πρωτοεμφανίστηκε σε μια ομιλία του peter T. Lewis, στο 15ο ετήσιο νομοθετικό σαββατοκύριακο του congressional black caucus foundation στην ουάσινγκτον, που δημοσιεύτηκε τον Σεπτέμβριο του 1985.[2]
- Ο όρος «διαδίκτυο των πραγμάτων» και στα αγγλικά (“internet of things” – iot), εμφανίστηκε το 1999 στην προσπάθεια του kevin ashton να παρουσιάσει ένα σύστημα στο οποίο τα αντικείμενα του φυσικού κόσμου θα είχαν τη δυνατότητα να συνδεθούν στο διαδίκτυο, χρησιμοποιώντας αισθητήρες.[2]
- Ορίζοντας το Διαδίκτυο των Πραγμάτων ως "απλά το χρονικό σημείο κατά το οποίο περισσότερα "πράγματα ή αντικείμενα" συνδέονται στο Διαδίκτυο από ό,τι άνθρωποι", η Cisco Systems εκτιμά ότι το IoT "γεννήθηκε" μεταξύ 2008 και 2009, με την αναλογία πραγμάτων/ανθρώπων να αυξάνεται από 0,08 το 2003 σε 1,84 το 2010.[2]

IoT Reference Framework

- IoT Device Level
- IoT Network Level
- IoT Application Services Platform Level
- IoT Application Level



Εικόνα 1. IoT Reference Framework [3]

Πλεονεκτήματα του Framework[3]

- Μειωμένη πολυπλοκότητα
- Τυποποιημένα στοιχεία και διεπαφές
- Μηχανική Ενοτήτων
- Επιτάχυνση της καινοτομίας

ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ

Προκλήσεις ασφάλειας IoT[4]

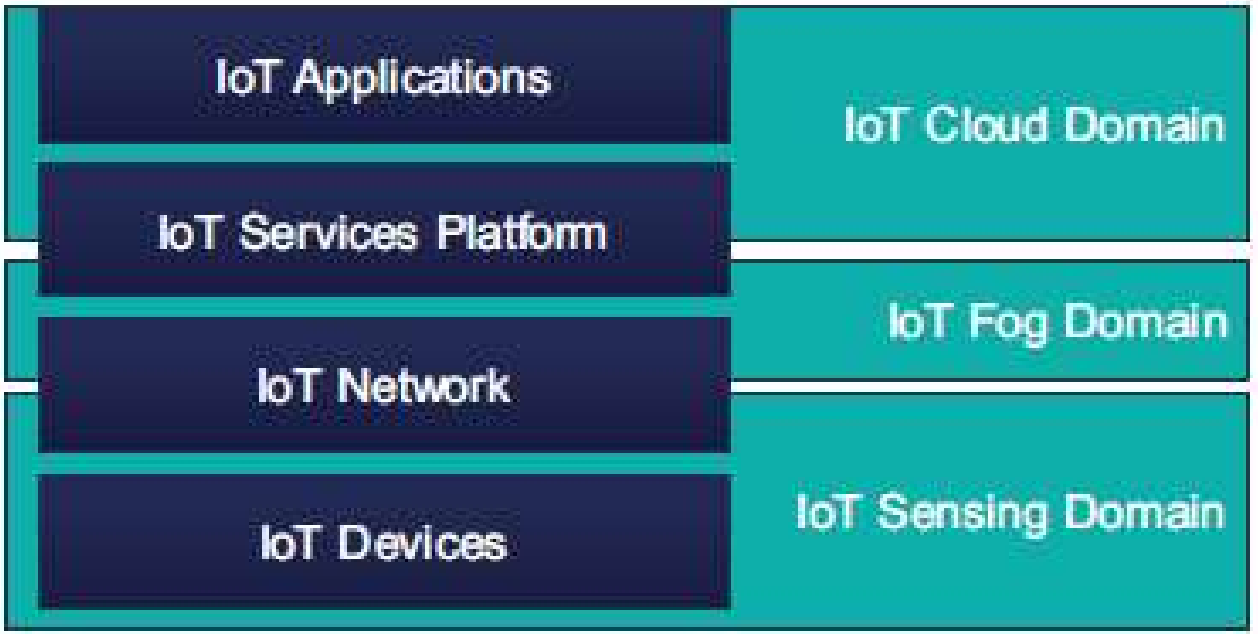
- Πολλαπλές τεχνολογίες
- Πολλαπλές εφαρμογές
- Επεκτασιμότητα
- Διαθεσιμότητα
- Μεγάλα δεδομένα
- Περιορισμοί πόρων
- Απομακρυσμένες τοποθεσίες
- Κινητικότητα
- Υπηρεσία ευαίσθητη στην καθυστέρηση

Απαιτήσεις ασφάλειας IoT[5]

- Εμπιστευτικότητα
- Ακεραιότητα
- Αυθεντικοποίηση
- Διαθεσιμότητα
- Εξουσιοδότηση
- Φρεσκάδα
- Μη άρνηση
- Forward & Backward Secrecy

3 Domain Architecture

- IoT Cloud Domain
- IoT Fog Domain
- IoT Sensing Domain



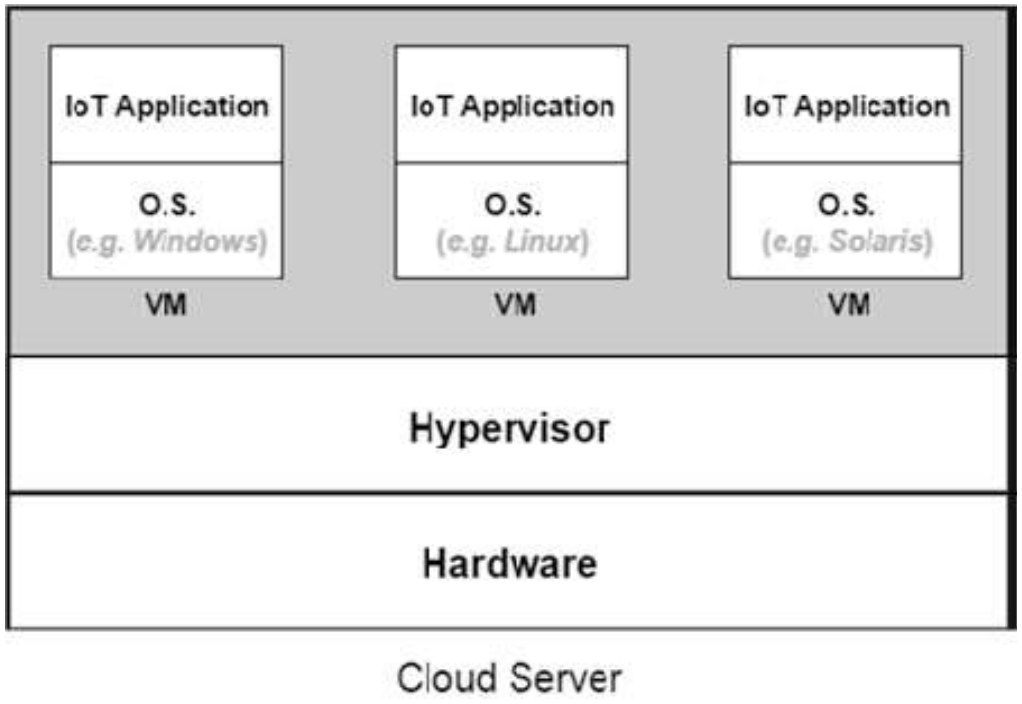
Εικόνα 2. 3 Domain Architecture [6]

Επιθέσεις και Αντίμετρα

Επιθέσεις & Αντίμετρα στον Τομέα νέφους

- Επιθέσεις κρυφού καναλιού (Hidden-Channel Attacks)
- Επιθέσεις μετανάστευσης VM
- Επίθεση κλοπής υπηρεσιών
- Επίθεση διαφυγής VM
- Επιθέσεις εκ των έσω

Cloud Server



Εικόνα 3. Cloud Server [7]

Επιθέσεις & Αντίμετρα κρυφού καναλιού

1. Χαρτογράφηση του VM-στόχου
2. Κακόβουλη τοποθέτηση VM
3. Διαρροή δεδομένων μεταξύ των VM

- Σκληρή απομόνωση
- Εκκαθάριση κρυφής μνήμης
- Περιορισμός του ρυθμού εναλλαγής της κρυφής μνήμης
- Χρόνος πρόσβασης σε δεδομένα με θόρυβο

Επιθέσεις μετανάστευσης VM

1. Επιθέσεις στο επίπεδο ελέγχου
    1. Πλημμυρισμός Μετανάστευσης
    2. Ψευδής διαφήμιση πόρων
2. Επιθέσεις στο επίπεδο δεδομένων
    1. Sniffing
    2. Man in the Middle

- Αυθεντικοποίηση
- Κρυπτογράφηση
- Χρονοσφραγίδες
- Ελεγχος ταυτότητας

Επίθεση κλοπής υπηρεσιών

Με αυτή την επίθεση ένα κακόβουλο VM συμπεριφέρεται με τρόπο που κάνει τον hypervisor να του αναθέτει περισσότερους πόρους από το μερίδιο που υποτίθεται ότι να λάβει. Αυτή η επιπλέον κατανομή πόρων για το κακόβουλο VM έρχεται σε εις βάρος των άλλων VM που μοιράζονται τον ίδιο διακομιστή με το κακόβουλο VM, όπου αυτά τα VM-θύματα λαμβάνουν μικρότερο μερίδιο πόρων από αυτό που θα έπρεπε να λαμβάνουν στην πραγματικότητα, γεγονός που με τη σειρά του υποβαθμίζει την απόδοσή τους.[7]

- Ακριβέστερη καταγραφή της ώρας έναρξης και λήξης
- Τυχαιοποίηση των χρόνων δειγματοληψίας

Επίθεση διαφυγής VM

Οι εικονικές μηχανές είναι σχεδιασμένες με τρόπο που απομονώνουν κάθε VM από τις άλλες VM που εκτελούνται στον ίδιο διακομιστή, γεγονός που αποτρέπει τις VM από το να έχουν πρόσβαση σε δεδομένα που ανήκουν σε άλλα VM που βρίσκονται στον ίδιο διακομιστή. Ωστόσο, στην πραγματικότητα μπορούν να αξιοποιηθούν σφάλματα λογισμικού για να σπάσει αυτή η απομόνωση. Εάν ένα VM ξεφύγει από το επίπεδο hypervisor και φτάσει στο υλικό του διακομιστή, τότε το κακόβουλο VM μπορεί να αποκτήσει πρόσβαση root σε ολόκληρο τον διακομιστή όπου βρίσκεται. Αυτό δίνει στο VM πλήρη έλεγχο σε όλα τα VM που φιλοξενούνται στον παραβιασμένο διακομιστή.[7]

- CloudVisor

Επιθέσεις εκ των έσω

Σε όλες τις επιθέσεις που συζητήθηκαν προηγουμένως, αντιμετωπίζαμε τους διαχειριστές του κέντρου δεδομένων νέφους ως έμπιστες οντότητες και εστιάζαμε μόνο στις επιθέσεις που προέρχονται από άλλα κακόβουλα VM που φιλοξενούνται στο κέντρο δεδομένων νέφους. Ωστόσο, ορισμένες ευαίσθητες εφαρμογές μπορεί να έχουν σοβαρές ανησυχίες σχετικά με τη φιλοξενία των συλλεγόμενων πληροφοριών τους στο νέφος δεδομένων καθώς οι διαχειριστές του κέντρου δεδομένων υπολογιστικού νέφους σε αυτή την περίπτωση θα έχουν τη δυνατότητα πρόσβασης και τροποποίησης των συλλεγόμενων δεδομένων.[7]

- Ομομορφική κρυπτογράφηση

Επιθέσεις και Αντίμετρα στον Τομέα Νέφους

Attack	Vulnerability reason	Security violation	Countermeasures
Hidden-channel attack	Shared hardware components (e.g., cache) among the server's VMs	Confidentiality	Hard isolation Cache flushing Noisy data access time Limiting cache switching rate
VM migration attacks	VM migration software bugs VM migration is performed without authentication Memory pages copied in clear	Confidentiality Integrity Availability	Server authentication Encrypting migrated memory pages
Theft-of-service attack	Periodic sampling of VMs' used resources	Availability Non-repudiation	Fine-grain sampling using high precision clocks Random sampling
VM escape attack	Hypervisor software bugs	Confidentiality Availability Integrity	Add an isolation domain between the hypervisor and hardware
Insider attacks	Lack of trust in cloud administrators	Confidentiality Integrity	Homomorphic encryption Secret storage through data chopping and permutation based on a secret key

Εικόνα 4. Επιθέσεις και Αντίμετρα στον Τομέα Νέφους[8]

Επιθέσεις και αντίμετρα στον τομέα της ομίχλης

1. Ζητήματα αυθεντικοποίησης και εμπιστοσύνης
2. Υψηλότεροι κίνδυνοι ασφάλειας της μετανάστευσης
3. Υψηλότερη ευπάθεια σε επιθέσεις DoS
4. Πρόσθετες απειλές για την ασφάλεια λόγω της χρήσης εμπορευματοκιβωτίων
5. Θέματα απορρήτου

- Συστήματα Φήμης
- Αυθεντικοποίηση – Κρυπτογράφηση
- Obfuscator

Επιθέσεις και αντίμετρα στον τομέα της ανίχνευσης

1. Επίθεση παρεμβολής
2. Επίθεση επιλεκτικής προώθησης
3. Επίθεση σε καταβόθρα

Επίθεση Παρεμβολής

- **Παρεμπόδιση του δέκτη** : Αυτή η επίθεση στοχεύει τον δέκτη, ένας κακόβουλος χρήστης εκπέμπει ένα σήμα το οποίο παρεμβαίνει στα νόμιμα σήματα που λαμβάνονται στον πλευρά του δέκτη.[9]
- **Παρεμπόδιση του αποστολέα** : Σε αντίθεση με την προηγούμενη επίθεση, αυτός ο τύπος στοχεύει τα αντικείμενα. Ο παρεμβολέας σε αυτή την επίθεση στέλνει ένα σήμα παρεμβολής που εμποδίζει τα γειτονικά αντικείμενα να μεταδώσουν τα πακέτα τους[9]

Επίθεση παρεμβολής – Στρατηγικές παρεμβολής

- Συνεχής εμπλοκή
- Παραπλανητική παρεμβολή
- Αντιδραστικές παρεμβολές
- Τυχαία παρεμβολή

Επίθεση παρεμβολής – Αντίμετρα

- Μεταπήδηση συχνότητας
- Φάσμα διασποράς
- Κατευθυντικές κεραίες
- Ανίχνευση παρεμβολών

Επίθεση επιλεκτικής προώθησης

Η επίθεση αυτή λαμβάνει χώρα στην περίπτωση που το αντικείμενο δεν μπορεί να στείλει τα παραγόμενα πακέτα του απευθείας στη συσκευή ομίχλης αλλά πρέπει να βασιστεί σε άλλα αντικείμενα που βρίσκονται κατά μήκος της διαδρομής προς τη συσκευή ομίχλης για να παραδώσουν αυτά τα πακέτα. Το κακόβουλο αντικείμενο σε αυτή την επίθεση δεν προωθεί ένα μέρος των πακέτων που λαμβάνει από τα γειτονικά αντικείμενα.[9]

- Αύξηση ικανότητας μετάδοσης
- Πλεονασμός Διαδρομής

Επίθεση σε καταβόθρα

Ενα κακόβουλο αντικείμενο ισχυρίζεται ότι έχει τη συντομότερη διαδρομή προς την συσκευή ομίχλης και προσελκύει όλα τα γειτονικά αντικείμενα που δεν έχουν τη δυνατότητα μετάδοσης να φτάσουν στη συσκευή ομίχλης, να προωθήσουν τα πακέτα τους σε αυτό το κακόβουλο αντικείμενο και να βασίζονται σε αυτό το αντικείμενο για να παραδώσουν τα πακέτα τους. Τώρα όλα τα πακέτα που προέρχονται από τους γειτονικούς κόμβους περνούν από αυτόν τον κακόβουλο κόμβο. Αυτό το δίνει στον κακόβουλο κόμβο τη δυνατότητα να εξετάζει το περιεχόμενο όλων των προωθούμενων πακέτων, εάν τα δεδομένα αποστέλλονται χωρίς κρυπτογράφηση. [9]

Τεχνικές ανίχνευσης και απομόνωσης των κακόβουλων αντικειμένων προτάθηκαν και βασίζονται στην ιδέα της συλλογής πληροφοριών από διάφορα αντικείμενα, όπου κάθε αντικείμενο αναφέρει τα γειτονικά αντικείμενα μαζί με την απόσταση μεταξύ τους. Ένα σύστημα ανίχνευση εισβολής χρησιμοποιείται στη συνέχεια για να βασιστεί σε αυτές τις πληροφορίες για τον εντοπισμό των αντικειμένων που ενδεχομένως να παρέχουν παραπλανητικές πληροφορίες.[9]

πιθέσεις και αντίμετρα στον τομέα της ανίχνευσης

Attack	Target OSI layer	Vulnerability reason	Security violation	Countermeasures
Jamming attack	Physical Data link	Shared wireless channel	Availability	Frequency hopping Spread spectrum Directional antennas Jamming detection techniques
Selective-forwarding attack	Network	Limited transmission capability	Availability	Increase transmission range Path redundancy Choose certain intermediate objects as checkpoints to acknowledge received packets
Sinkhole attack	Network	Limited transmission capability	Confidentiality Availability	Analyze the collected routing information from multiple objects

Εικόνα 5. Επιθέσεις και Αντίμετρα στον τομέα ανίχνευσης [9]

Μελλοντικές Επεκτάσεις

- **Ελαφριά κρυπτογραφία** : ο στόχος είναι να βρεθούν αποδοτικές τεχνικές κρυπτογράφησης που να μπορούν να αντικαταστήσουν τις παραδοσιακές υπολογιστικά δαπανηρές, επιτυγχάνοντας παράλληλα ένα αποδεκτό επίπεδο ασφάλειας.[10][11]
- **Ασφάλεια τομέα ομίχλης** : Πρέπει να δοθεί προσοχή σε αυτόν τον τομέα. Η εστίαση θα πρέπει να γίνει στον εντοπισμό μοντέλων απειλής που σχετίζονται με τον τομέα της ομίχλης και στην εξεύρεση αποτελεσματικών λύσεων. [10][11]
- **Συνεργατική άμυνα** : μια συνεργατική λύση όπου οι διάφοροι τομείς (νέφος, ομίχλη και ανίχνευση) αλληλοεπιδρούν μεταξύ τους για να σταματήσουν ή να μετριάσουν μια συγκεκριμένη επίθεση. [10][11]

Βιβλιογραφία

- [1] IoT Wikipedia
  https://en.wikipedia.org/wiki/Internet_of_things
- [2] IoT Wiki
  https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CF%84%CF%89%CE%BD_%CF%80%CF%81%CE%B1%CE%B3%CE%BC%CE%AC%CF%84%CF%89%CE%BD
- [3] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 7-8
- [4] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 212-214
- [5] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 214
- [6] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 215-216
- [7] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 216-224
- [8] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 224-227
- [9] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 227-234
- [10] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 235
- [11] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 2014, pp. 1-8, doi: 10.1109/PRISMS.2014.6970594.