Πανεπιστήμιο Πελοποννήσου
Σχολή Μηχανικών
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Αριθμός Πτυχιακής: 1761

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ:

«Μελέτη προβλημάτων ασφαλείας στο Διαδίκτυο των Πραγμάτων»
«A study on security issues in the Internet of Things»

Γερασιμόπουλος Ιωάννης
Α.Μ.: 6641

Επιβλέπων Καθηγητής: Καψάλης Βασίλειος

ΠΑΤΡΑ 2019

Περιεχόμενα

Περίληψη

Η παρούσα πτυχιακή εργασία ασχολείται με το αντικείμενο της ασφάλειας του Διαδικτύου των Πραγμάτων. Γίνεται εγκατάσταση εξυπηρετητή MQTT στην πλατφόρμα Raspberry Pi 4 και δοκιμάζονται διάφορες επιθέσεις με σκοπό να ελεγχθεί ο βαθμός ασφάλειας που προσφέρεται. Στο πρώτο κεφάλαιο παρουσιάζονται ορισμένες βασικές έννοιες και τεχνική ορολογία, σχετικές με τα δίκτυα Η/Υ και το Διαδίκτυο των Πραγμάτων. Στο δεύτερο κεφάλαιο αναλύεται η λειτουργία του Διαδικτύου των Πραγμάτων σε διάφορους τομείς πρακτικών εφαρμογών. Κατόπιν, στο τρίτο κεφάλαιο γίνεται αναφορά των διαφόρων μοντέλων επίθεσης στα διαφορετικά επίπεδα του Διαδικτύου των Πραγμάτων, και παρατίθενται οι δέκα βασικές αδυναμίες ασφαλείας του Διαδικτύου των Πραγμάτων σύμφωνα με τον οργανισμό OWASP (Open Web Application Security Project). Στη συνέχεια, στο τέταρτο και τελευταίο κεφάλαιο, επιχειρούνται επιθέσεις sniffing και Slowloris Denial of Service, ενάντια στον εξυπηρετητή που είναι εγκατεστημένος στην πλατφόρμα Raspberry Pi και παρατίθενται τα ευρήματα. Επίσης γίνεται αναφορά στην έννοια «Dorking» που επιτρέπει την εύρεση τρωτών συσκευών στο Διαδίκτυο των Πραγμάτων. Τέλος, αναφέρονται μερικά παραδείγματα επιθέσεων που χρησιμοποιούν συσκευές του Διαδικτύου των Πραγμάτων.

Εισαγωγή

Ιστορικά, ο όρος τεχνολογία της πληροφορίας αναφέρεται σε όλες τις τεχνολογίες που σχετίζονται με τη συλλογή, την επεξεργασία, την αποθήκευση και την διάδοση πληροφοριών. Ο άνθρωπος, από την προϊστορική εποχή ακόμα, είχε αναπτύξει στοιχειώδεις μεθόδους τις οποίες χρησιμοποιούσε, με σκοπό να επικοινωνεί με τους γύρω του.

- Στην προμηχανική εποχή (3000 π.Χ. έως 1450 μ.Χ.), προσπαθούσαν να χρησιμοποιήσουν γλώσσες ή σκάλιζαν τα τοιχώματα σπηλαίων, δημιουργώντας τις πρώτες εικόνες (πετρόγλυφα). Οι τεχνικές και οι μέθοδοι εξελίχθηκαν ταχύτατα.

- Περίπου το έτος 100 μ.Χ., δημιουργήθηκε στην Ινδία το πρώτο σύστημα αρίθμησης από το 1 έως το 9. Περνώντας στη μηχανική εποχή (1450 – 1840), οι πρώτοι αναλογικοί υπολογιστές παίρνουν μορφή, όπως ο υπολογιστής του Blaise Pascal (Pascaline) και η διαφορική μηχανή του Charles Babbage.

- Η ηλεκτρομηχανική εποχή (1840 - 1940) φέρνει στον κόσμο την πρώιμη τηλεπικοινωνία, τον κώδικα Μόρς (1835), το τηλέφωνο (Alexander Graham Bell – 1876), και το πρώτο ράδιο (Guglielmo Marconi – 1894).

- Ερχόμενοι στην ηλεκτρονική και ψηφιακή εποχή (1940 - σήμερα), βλέπουμε τεχνολογίες που συνεχίζουν να βελτιώνονται με αστραπιαίους ρυθμούς. Από τις διάτρητες κάρτες και τις λυχνίες του ENIAC, τα τρανζίστορ και τα ολοκληρωμένα κυκλώματα ανοίγουν το δρόμο για το μικροτσίπ, κάνοντας τα εξαρτήματα που απαρτίζουν ένα υπολογιστικό σύστημα μικρότερα σε φυσικό μέγεθος και ταυτόχρονα ταχύτερα. Η πλευρά του λογισμικού δεν μένει πίσω, εισάγοντας τις πρώτες γλώσσες προγραμματισμού υψηλού επιπέδου FORTRAN και COBOL. Οι εξελίξεις αυτές οδηγούν στη δημιουργία του προσωπικού υπολογιστή (1977 – Apple II, Commodore PET & TRS – 80 Model I).

Ίσως το μεγαλύτερο επίτευγμα της επιστήμης των υπολογιστών και κατόπιν της τεχνολογίας της πληροφορίας είναι η δημιουργία διαύλων επικοινωνίας μεταξύ υπολογιστών. Το δίκτυο ARPANET του 1960 το οποίο συνέδεε στρατιωτικά και ακαδημαϊκά δίκτυα, αποτέλεσε την αρχή αυτού που αργότερα (το 1991 συγκεκριμένα) θα ονομαζόταν Παγκόσμιος Ιστός (World Wide Web). Το Διαδίκτυο, όπως είναι σήμερα γνωστό, διασυνδέει και εξυπηρετεί περίπου 7 δισεκατομμύρια συσκευές και περίπου 3.2 δισεκατομμύρια χρήστες. Ο αριθμός των χρηστών και συσκευών που θα είναι συνδεδεμένοι στο διαδίκτυο προβλέπεται πως θα συνεχίσει να αυξάνεται σταθερά και στα επόμενα έτη, με την εξέλιξη των εφαρμογών του Internet of Things. Τι είναι όμως το Internet of Things; Ο όρος Internet of Things επινοήθηκε από τον Kevin Ashton το 1999 αν και ήταν υπό συζήτηση τουλάχιστον από το 1991.

Σύμφωνα με το ελληνικό άρθρο της Wikipedia για το λήμμα του Internet of Things: «*Το Διαδίκτυο των Πραγμάτων αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων, καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό , αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό)*».

Πριν όμως αρχίσουμε να κατανοούμε τη σημασία του Internet of Things είναι πρώτα σημαντικό να καταλάβουμε τις διαφορές μεταξύ του Διαδικτύου (Internet) και του Παγκόσμιου Ιστού (World Wide Web). Το Διαδίκτυο είναι το φυσικό επίπεδο που αποτελείται από μεταγωγείς, δρομολογητές και άλλες συσκευές. Η κύρια λειτουργία του είναι να μεταφέρει πληροφορίες από το ένα σημείο στο άλλο γρήγορα, αξιόπιστα και με ασφάλεια. Ο Παγκόσμιος Ιστός από την άλλη πλευρά, είναι ένα επίπεδο εφαρμογών που λειτουργεί πάνω από το Διαδίκτυο. Ο κύριος ρόλος του είναι να παρέχει μία διεπαφή που καθιστά τις πληροφορίες που ρέουν σε όλο το Διαδίκτυο χρησιμοποιήσιμες.

Ουσιαστικά το Internet of Things είναι ένα δίκτυο φυσικών αντικειμένων, συσκευών, οχημάτων, κτιρίων αλλά και άλλων αντικειμένων τα οποία περιέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά, αισθητήρες και διαδικτυακή δυνατότητα σύνδεσης – κάτι που επιτρέπει σε αυτά τα αντικείμενα να συλλέγουν και να ανταλλάσσουν δεδομένα. Το Internet of Things δίνει την δυνατότητα στα αντικείμενα αυτά να ελέγχονται απομακρυσμένα μέσω της υπάρχουσας δικτυακής υποδομής δημιουργώντας ευκαιρίες άμεσης ενσωμάτωσης του φυσικού κόσμου με τα υπολογιστικά συστήματα έχοντας ως αποτέλεσμα τη βελτίωση της αποτελεσματικότητας και της ακρίβειας αλλά και τη μείωση του κόστους. Από τη στιγμή μάλιστα που το Internet of Things εξοπλίζεται με αισθητήρες και ενεργοποιητές, αποτελεί μέρος έξυπνων συστημάτων της καθημερινότητας όπως είναι τα έξυπνα σπίτια, οχήματα και πόλεις. Κάθε αντικείμενο αναγνωρίζεται μοναδικά από το ενσωματωμένο υπολογιστικό σύστημα και μπορεί να λειτουργεί τόσο αυτόνομα όσο και σε συνεργασία με την υπόλοιπη διαδικτυακή υποδομή.

Είναι γνωστό ότι η ραγδαία ανάπτυξη των τεχνολογιών που σχετίζονται με τα υπολογιστικά συστήματα και τα δίκτυα επικοινωνίας αλλάζει την αίσθηση του χρόνου. Ας πάρουμε για παράδειγμα τα έξυπνα κινητά τηλέφωνα (smartphones). Μέσα σε ένα έτος οι κατασκευαστές παράγουν μοντέλα τα οποία βελτιώνονται συνεχώς σε σχέση με εκδόσεις παλαιότερων ετών. Οι συσκευές γίνονται ταχύτερες και πιο αξιόπιστες. Σε τεχνολογικούς όρους, ένα έτος φαντάζει με έναν αιώνα. Το ίδιο συμβαίνει με άλλα προϊόντα λογισμικού ή/και φυσικού υλικού. Ένα προϊόν που αναπτύσσεται στο λιγότερο δυνατό χρόνο δεν σημαίνει πως θα είναι άρτιο σε όλους τους τομείς.

Ένας από αυτούς τους τομείς (και πιθανόν ο σημαντικότερος) στον οποίο συχνά γίνονται σφάλματα και παραλείψεις λόγω της ταχύτητας είναι η ασφάλεια. Ένα προϊόν ή μία τεχνολογική εφαρμογή που εξελίσσονται γρήγορα φέρουν κενά ασφαλείας για τα οποία δεν αφιερώθηκε επαρκής χρόνος να ερευνηθούν και να καλυφθούν.

Αυτός είναι και ο σκοπός της συγκεκριμένης διπλωματικής εργασίας. Το Internet of Things παρότι είναι μία ιδέα που πρωτοσυζητήθηκε το 1982, μόλις τα τελευταία έτη βρέθηκε γόνιμο τεχνολογικό έδαφος ώστε να μπορέσει να εξελιχθεί. Αυτό σημαίνει ότι όντας μία «νέα» τεχνολογία, εξελίσσεται ταχύρρυθμα με σκοπό τη διερεύνηση όλων των δυνατών εφαρμογών και δυνατοτήτων της, χωρίς να προλαβαίνει ο τομέας της ασφάλειας να διατηρήσει αυτή την ταχύτητα. Σε αυτήν τη διπλωματική, θα γίνει επισκόπηση της λειτουργίας του IoT σε διάφορες εφαρμογές. Κατόπιν θα γίνει ανάλυση πιθανών μοντέλων επιθέσεων τόσο σε φυσικό αλλά και σε επίπεδο λογισμικού. Θα ακολουθήσει εκτέλεση επιθέσεων και θα προταθούν πιθανές λύσεις που θα καλύψουν όσο το δυνατόν περισσότερα κενά ασφαλείας. Στο τέλος της διπλωματικής, θα αναφερθούν τα συμπεράσματα και η βιβλιογραφία. Στο κεφάλαιο που ακολουθεί θα εξηγηθούν ορισμένες σημαντικές έννοιες που είναι απαραίτητες για την κατανόηση του περιεχομένου της διπλωματικής.

<u>Κεφάλαιο 1ο: Βασικές έννοιες / Ορολογία.</u>

Σε αυτό το κεφάλαιο αναφέρονται μερικές έννοιες και όροι της τεχνολογίας επικοινωνιών που θα φανούν χρήσιμες για την κατανόηση της λειτουργίας των ανάλογων συσκευών/μηχανισμών.

Ορολογία σχετικά με τα Δίκτυα.

- **Το μοντέλο αναφοράς για τη Διασύνδεση Ανοικτών Συστημάτων (Open Systems Interconnection – OSI)** αναπτύχθηκε από τον Διεθνή Οργανισμό Τυποποίησης (International Organisation for Standardisation – ISO) και προδιαγράφει επτά (7) στρώματα/επίπεδα τα οποία υλοποιούν συγκεκριμένες λειτουργίες, ώστε να είναι εφικτή η διασύνδεση διαφορετικών υπολογιστικών συστημάτων, εφόσον στα αντίστοιχα επίπεδα χρησιμοποιούν συμβατές ή ίδιες τεχνικές και κανόνες (πρωτόκολλα). Το μοντέλο αναφοράς OSI αποτελεί μια πρόταση του ISO προς τους κατασκευαστές φυσικού υλικού και λογισμικού δικτύων, χωρίς να είναι δεσμευτική. Ο βαθμός υλοποίησής του επαφίεται σε αυτούς.

Μοντέλο OSI			
	Μονάδα δεδομένων	**Επίπεδο**	**Λειτουργία**
Λογισμικό	Δεδομένα	7. Εφαρμογών	Παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο
		6. Παρουσίασης	Αναπαράσταση δεδομένων και κρυπτογράφηση
		5. Συνόδου	Έλεγχος του διαλόγου μεταξύ των άκρων της επικοινωνίας
	Τμήμα	4. Μεταφοράς	Αξιόπιστη επικοινωνία από άκρο σε άκρο
Υλικό	Πακέτο	3. Δικτύου	Καθορισμός διαδρομών και λογικών διευθύνσεων των κόμβων στα πλαίσια ενός διαδικτύου
	Πλαίσιο	2. Ζεύξης δεδομένων	Φυσική διευθυνσιοδότηση (MAC & LLC)
	Bit	1. Φυσικό	Δυαδική μετάδοση σήματος μέσω του φυσικού μέσου

Το μοντέλο αναφοράς OSI με τα επιμέρους επίπεδά του. (Πηγή: Wikipedia)

- **TCP/IP** (ορισμός από την Wikipedia): «*Το **TCP/IP** είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Η ονομασία **TCP/IP** προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων της συλλογής: το **Transmission Control Protocol** (Πρωτόκολλο Ελέγχου Μετάδοσης) και το **Internet Protocol** (Πρωτόκολλο Διαδικτύου). Το μοντέλο OSI, το οποίο παραμένει έως σήμερα μόνο θεωρητικό, προτείνει την κατάταξη των πρωτοκόλλων δικτύων σε έναν οργανωμένο σωρό επτά επιπέδων. Συγκρίσεις ανάμεσα στο μοντέλο OSI και το TCP/IP δείχνουν τη σημασία των πρωτοκόλλων που περιέχονται στην συλλογή IP, από την άλλη πλευρά όμως μπορεί να προκληθεί σύγχυση, καθώς το TCP/IP αποτελείται από μόνο τέσσερα επίπεδα*».

- **Η διεύθυνση IP** είναι μία μοναδική αριθμητική διεύθυνση που χρησιμοποιείται από συσκευές σε ένα δίκτυο υπολογιστών που χρησιμοποιούν το Πρωτόκολλο Διαδικτύου για τη μεταξύ τους αναγνώριση και συνεννόηση. Στην κύρια και ευρέως διαδεδομένη έκδοση του Πρωτοκόλλου Διαδικτύου, **IPv4**, οι διευθύνσεις αυτές έχουν μέγεθος 32-bit (τυπική μορφή: 192.168.1.1) που φέρνει το πλήθος τους σε 2^{32} (4.294.967.296) πιθανές μοναδικές διευθύνσεις. Επειδή όμως οι διευθύνσεις του IPv4 πλέον δεν επαρκούν, τα τελευταία χρόνια αναπτύσσεται η έκδοση **IPv6** η οποία εξαπλώνεται σε όλο τον κόσμο με μέγεθος διευθύνσεων 128-bit και πλήθος 2^{128} (ή 3,4 * 10^{38})πιθανές μοναδικές διευθύνσεις.

- Ο **server** ή εξυπηρετητής/διακομιστής στην πιο απλή του μορφή είναι ένας ηλεκτρονικός υπολογιστής που τρέχει κατάλληλο λογισμικό ώστε να εξυπηρετεί τους χρήστες που συνδέονται με αυτόν για κάποιο σκοπό. Ανάλογα με τον σκοπό, ο server τρέχει και τις κατάλληλες υπηρεσίες και έχει και κατάλληλη ονομασία.

- Το ασύρματο σημείο πρόσβασης (**WAP – Wireless Access Point**) ή όπως είναι κοινώς γνωστό, **AP** (**Access Point**) είναι μία συσκευή της οποίας η λειτουργία είναι να συνδέει ασύρματες συσκευές επικοινωνίας μεταξύ τους για τον σχηματισμό ενός ασύρματου δικτύου. Το Access Point, συνήθως συνδέεται σε με ένα ενσύρματο δίκτυο και μπορεί να μεταφέρει δεδομένα ανάμεσα στις ασύρματες και ενσύρματες συσκευές.

- **Ο δρομολογητής** (αγγλ. **router**) είναι μια ηλεκτρονική συσκευή η οποία αναλαμβάνει την αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών, άλλων δρομολογητών και πελατών (clients), κατά μήκος πολλαπλών δικτύων (δρομολόγηση). Η δρομολόγηση, δηλαδή η διαδικασία μεταφοράς δεδομένων από ένα σημείο σε ένα άλλο αποτελεί κεντρική λειτουργία του επιπέδου δικτύου, γίνεται με βάση διάφορα κριτήρια και τελικώς επιλέγεται μία ανάμεσα σε διάφορες πιθανές διαδρομές.

- Ο **μεταγωγέας** (αγγλικά: **switch**) είναι μια ηλεκτρονική συσκευή που χρησιμοποιείται σε δίκτυα υπολογιστών. Αποτελεί ένα συνδυασμό του επαναλήπτη (Hub) και της γέφυρας (bridge). Στην αρχή οι μεταγωγείς χρησιμοποιήθηκαν σε δίκτυα τύπου Ethernet, ενώ σήμερα, κυκλοφορούν μεταγωγείς και για άλλου τύπου πρωτόκολλα όπως για παράδειγμα FDDI, ATM. Προσφέρουν ταχύτητες της τάξης των Gigabits. Μπορούν να πάρουν τη θέση των Hubs χωρίς να γίνει καμιά απολύτως επανασχεδίαση στο δίκτυο ,αλλά προσθέτοντας επιπλέον εύρος ζώνης στους συνδεδεμένους σταθμούς εργασίας. Το κύριο χαρακτηριστικό του μεταγωγέα είναι ότι κάθε θύρα του προσφέρει καθορισμένο εύρος ζώνης, σε αντίθεση με το Hub , όπου όλες οι συσκευές που συνδέονται σε αυτό μοιράζονται το εύρος ζώνης του μέσου.

- **Η διεύθυνση MAC** (Media Access Control) είναι μία μοναδική ταυτότητα που αποδίδεται από τον κατασκευαστή σε ένα κομμάτι του υλικού του δικτύου (όπως μια ασύρματη κάρτα ή μια κάρτα ethernet). Το MAC σημαίνει *Έλεγχος Πρόσβασης Μέσου* και κάθε ταυτοποιητής προορίζεται να είναι μοναδικός για μία συγκεκριμένη συσκευή. Μια διεύθυνση MAC αποτελείται από 48-bit και αναπαρίσταται από έξι διψήφιους δεκαεξαδικούς αριθμούς χωρισμένους με παύλες (-) ή άνω και κάτω τελεία (:). Μια τυπική διεύθυνση MAC έχει τη μορφή: D8:9A:34:26:BF:63

- **Ο όρος Wi-Fi** χρησιμοποιείται για να περιγράψει ασύρματα τοπικά δίκτυα (WLAN – Wireless Local Area Network) που λειτουργούν σύμφωνα με την προδιαγραφή IEEE 802.11. Υπάρχουν διάφορες εκδόσεις του Wi-Fi που καθορίζονται από τα διάφορα πρότυπα του πρωτοκόλλου IEEE 802.11, με τις ποικίλλες τεχνολογίες ραδιοφώνου, να καθορίζουν την εμβέλεια, ζώνες και ταχύτητες που μπορούν να επιτευχθούν. Το Wi-Fi χρησιμοποιεί συνηθέστερα τις ραδιοφωνικές ζώνες των 2.4GHz και 5GHz. Οι ζώνες αυτές μπορούν να υποδιαιρεθούν σε πολλαπλά κανάλια. Το κάθε κανάλι μπορεί να μοιραστεί σε πολλά δίκτυα. Αν και το Wi-Fi είναι σχεδιασμένο να συνεργάζεται άψογα με το Πρωτόκολλο Ethernet, είναι δυνητικά πιο ευάλωτο σε επιθέσεις σε σχέση με τα ενσύρματα δίκτυα, επειδή όποιος βρίσκεται μέσα στην εμβέλεια του ασύρματου δικτύου με ελεγκτή διεπαφής ασύρματου δικτύου μπορεί να επιχειρήσει πρόσβαση.

Ορολογία σχετική με το Internet of Things.

- **Ο όρος Big Data** χρησιμοποιείται για να δηλώσει τον τεράστιο όγκο δεδομένων που θα συλλέγονται από συσκευές του IoT, ο οποίος μπορεί να αναλυθεί για πρότυπα/μοτίβα και τάσεις προτιμήσεων. Τα «μεγάλα» δεδομένα παρέχουν πολύτιμες (και συχνά κερδοφόρες) πληροφορίες που μπορούν να χρησιμοποιηθούν για τον εντοπισμό ευκαιριών πώλησης προϊόντων ή υπηρεσιών και για συμπεριφορές πελατών. Η ανάλυση αυτή είναι σημαντική γιατί μετακινεί τις επιχειρήσεις μακριά από την ενστικτώδη λήψη αποφάσεων και τις ωθεί σε στρατηγικές επιλογές που βασίζονται στα παραπάνω δεδομένα. Οι συσκευές του IoT έχουν τη δυνατότητα να δημιουργούν νέες ροές δεδομένων με σκοπό την επεξεργασία δεδομένων.
- **Με τον όρο Machine to machine (M2M)** ορίζουμε την ανταλλαγή πληροφοριών μεταξύ μιας συσκευής με μια άλλη συσκευή χωρίς ανθρώπινη βοήθεια. Η χρησιμότητα της επικοινωνίας M2M είναι φανερή στη βιομηχανία. Συσκευές που παρακολουθούν τη λειτουργία άλλων συσκευών χωρίς ανθρώπινη παρέμβαση μετασχηματίζουν πολλές βιομηχανίες. Για παράδειγμα, ένα μηχάνημα μπορεί να προειδοποιήσει όταν χρειάζεται ένα νέο εξάρτημα ή πρόκειται να βγει εκτός λειτουργίας, εξαλείφοντας την ανάγκη ανθρώπινης παρακολούθησης η οποία καταναλώνει πολύτιμο χρόνο και πόρους.
- **Η Επικοινωνία Κοντινού Πεδίου (Near Field Communication – NFC)** αποτελεί μία τεχνολογία επικοινωνίας χαμηλής ισχύος, χαμηλών ταχυτήτων και μικρής εμβέλειας. Επιτρέπει αμφίδρομη επικοινωνία μεταξύ δύο συσκευών σε πολύ μικρή απόσταση. Είναι πολύ δημοφιλής μέθοδος επικοινωνίας χωρίς να χρειάζεται φυσική επαφή μεταξύ των συσκευών. Η λειτουργία της βασίζεται στην επαφή ή στην προσέγγιση, σε απόσταση περίπου τεσσάρων με πέντε εκατοστών, της συσκευής που περιέχει το τσιπ NFC, σε κάποια άλλη συσκευή που περιλαμβάνει τον κατάλληλο αισθητήρα.
- Η **Τεχνολογία Ταυτοποίησης Μέσω Ραδιοσυχνοτήτων (Radio Frequency Identification – RFID)** χρησιμοποιείται για την ταυτοποίηση αντικειμένων και προσώπων. Ενσωματώνει ηλεκτρομαγνητική ζεύξη και ραδιοσυχνότητες, και αποτελείται από τρία μέρη: μία κεραία, έναν πομποδέκτη και έναν αναμεταδότη. Ουσιαστικά, όταν η ετικέτα (RFID tag) βρεθεί στην εμβέλεια της κεραίας του αναγνώστη, η μονάδα ελέγχου επικοινωνεί μέσω ραδιοκυμάτων με την κεραία των ετικετών RFID. Οι ετικέτες RFID ενεργοποιούνται με τη σειρά τους και επιστρέφουν τα αναζητούμενα δεδομένα στους αναγνώστες.

- **Ο όρος mote** είναι ένας τρόπος αναφοράς σε ένα «τελικό σημείο» (endpoint) στο IoT. Η ονομασία αυτή χρησιμοποιείται κυρίως στη Βόρειο Αμερική και πρόκειται για έναν απλό αισθητήρα (κόμβο) σε ένα δίκτυο αισθητήρων που είναι σε θέση να συλλέξει δεδομένα, να τα επεξεργαστεί (σε περιορισμένο βαθμό) και να επικοινωνήσει με άλλους αισθητήρες στο δίκτυο. Ένα mote είναι κόμβος αλλά ένας κόμβος δεν είναι πάντα ένα mote.
- **Οι ενεργοποιητές** είναι μηχανισμοί που εκτελούν φυσικές δράσεις βάσει εισόδων από ένα συνδεδεμένο σύστημα, πχ. από κάποιον αισθητήρα.
- **Το Πρωτόκολλο Περιορισμένων Εφαρμογών (Constrained Application Protocol – CoAP)** είναι ένα πρωτόκολλο επιπέδου εφαρμογής (application – layer) που χρησιμοποιείται σε συσκευές περιορισμένων πόρων και επιτρέπει τη σύνδεσή τους στο Διαδίκτυο και τον τηλεχειρισμό.
- **Τα Δίκτυα Προσωπικού Χώρου (Personal Area Network - PAN)** είναι δίκτυα που δημιουργούνται μέσω της διασύνδεσης των συσκευών τεχνολογίας πληροφοριών στο πλαίσιο ενός μόνο χρήστη.
- **Ένα Ασύρματο Δίκτυο Αισθητήρων Χαμηλής Ισχύος (Low – Power Wireless Sensor Network)** είναι μια ομάδα χωρικά κατανεμημένων ανεξάρτητων συσκευών που συλλέγουν δεδομένα μετρώντας φυσικά ή περιβαλλοντικά μεγέθη με ελάχιστη κατανάλωση ενέργειας. Η ελαχιστοποίηση της ενεργειακής κατανάλωσης είναι το κλειδί για την μεγιστοποίηση της διάρκειας ζωής των συσκευών του δικτύου αισθητήρων.
- **Το API (Application Programming Interface)** είναι ένας απλούστερος τρόπος επικοινωνίας μεταξύ υπολογιστή και φυσικού υλικού ή υπολογιστή και κάποιας πλατφόρμας λογισμικού. Ο σχεδιασμός εφαρμογών που εκμεταλλεύονται το API επιτρέπει ταχύτερη ανάπτυξη λογισμικού και ευκολότερη βελτίωση.
- **Τα Chirps** είναι «ελαφριά» πρωτόκολλα, προσαρμόσιμα ανάλογα με το σκοπό/εφαρμογή, που επιτρέπουν στα «πράγματα» του IoT να επικοινωνούν και να εναλλάσσονται. Κατασκευασμένα για επικοινωνία από μηχανή σε μηχανή (Machine to Machine – M2M), είναι αποδοτικά, επεκτάσιμα πλαίσια δεδομένων με δομή ανοικτού πηγαίου κώδικα, ιδιωτικά πεδία δεδομένων και απλά checksums.
- **Το Υπολογιστικό Νέφος (Cloud Computing)** αναφέρεται σε ένα δίκτυο απομακρυσμένων διακομιστών που αποθηκεύουν, διαχειρίζονται και επεξεργάζονται δεδομένα. Το Cloud Computing είναι ζωτικής σημασίας για μεγάλους όγκους δεδομένων. Είναι ιδανικά για όσους χρειάζονται ανάκτηση αρχείων, διάθεση υπολογιστικών πόρων, παρέχουν μεγάλη ασφάλεια και είναι μία φιλική μέθοδος προς το περιβάλλον για την αποθήκευση αρχείων. Τα κεντρικά συστήματα βρίσκονται απομακρυσμένα από τον τελικό χρήστη, τα οποία τον εξυπηρετούν αυτοματοποιώντας διαδικασίες, παρέχοντας ευκολίες και ευελιξία σύνδεσης.
- **Industrial Internet of Things (IIoT).** Είναι η ενσωμάτωση της Μηχανικής Μάθησης (Machine Learning), της τεχνολογίας Big Data, των δεδομένων των αισθητήρων, και της επικοινωνίας μηχανής με μηχανή. Αυτό γίνεται με τη γνώση πως το IoT θα κλιμακώνεται και θα καθοδηγείται από τις επιχειρήσεις. Η ιδέα είναι ότι οι έξυπνες μηχανές θα είναι σε θέση να καταγράφουν και να μοιράζονται δεδομένα με μεγαλύτερη ακρίβεια ώστε να βοηθήσουν τις εταιρείες να εντοπίσουν προβλήματα νωρίτερα και να αυξήσουν την αποδοτικότητα.

- **Το Message Queuing Telemetry Transport (MQTT)** είναι ένα ελαφρύ πρωτόκολλο μεταφοράς μηνυμάτων τηλεμετρίας, σχεδιασμένο να «τρέχει» στο υπάρχον πρωτόκολλο **TCP/IP**. Χρησιμοποιείται για επικοινωνία και απομακρυσμένο έλεγχο μικρών συσκευών (αισθητήρες/ενεργοποιητές) με χαμηλές απαιτήσεις στο εύρος ζώνης της σύνδεσης δικτύου.
- **Τα επονομαζόμενα wearables**, είναι συνδεδεμένες συσκευές που μπορούν να εξοπλιστούν με διαφορετικούς τύπους αισθητήρων και φοριούνται στο σώμα ενός ατόμου. Σκοπός τους είναι να παρακολουθούν, να συλλέγουν και να ποσοτικοποιούν δεδομένα σχετικά με τη ζωή και το περιβάλλον ενός ατόμου και να επιτρέπουν τη διάδρασή τους με αυτά τα δεδομένα. Παραδείγματα wearables είναι τα smartwatches και τα fitness bands.
- **Το ZigBee** είναι ένα ανοικτό πρότυπο για ασύρματη επικοινωνία που έχει σχεδιαστεί για τη χρήση ψηφιακών ραδιοσημάτων χαμηλής ισχύος για προσωπικά δίκτυα (Personal Area Networks – PAN). Χρησιμοποιείται για τη δημιουργία δικτύων που απαιτούν χαμηλό ρυθμό μεταφοράς δεδομένων, ενεργειακή απόδοση και ασφαλή δικτύωση.
- **Το Z-Wave** είναι ένα πρωτόκολλο ασύρματης επικοινωνίας για οικιακούς αυτοματισμούς που επικοινωνεί με τεχνολογία ραδιοσυχνοτήτων χαμηλής ισχύος ειδικά σχεδιασμένη για εφαρμογές τηλεχειρισμού.

Κεφάλαιο 2ο: Λειτουργία και Εφαρμογές IoT δικτύων.

Το Διαδίκτυο των Πραγμάτων, όπως αναφέρθηκε, έχει ως βάση τη σύνδεση διάφορων μικρών συσκευών ή οχημάτων με ενσωματωμένους αισθητήρες και εξοπλισμό διασύνδεσης τόσο μεταξύ τους όσο και με τον κατασκευαστή, για να λαμβάνουν και να μεταδίδουν σχετικά δεδομένα με στόχο να προσφέρουν περισσότερες υπηρεσίες.

Με λίγα λόγια, το IoT απεικονίζεται ως μια σειρά από νέα ανεξάρτητα ενσωματωμένα συστήματα διαστάσεων μικροτσίπ, έξυπνων συσκευών, συστήματα πραγματικού χρόνου (real - time systems), συστήματα συγκέντρωσης όλων των πληροφοριών σε μεγάλες βάσεις δεδομένων, που λειτουργούν με δικές τους υποδομές και χρησιμοποιούν το διαδίκτυο για τη διασύνδεσή τους.

Τα τρία κύρια μέρη ενός IoT δικτύου είναι:

i. Τα «πράγματα», όπου συλλέγουν πληροφορίες οπουδήποτε και οποιαδήποτε στιγμή χρησιμοποιώντας τεχνολογία RFID, αισθητήρες και κώδικα.

ii. Τα δίκτυα επικοινωνιών που συνδέουν τα «πράγματα».

iii. Τα υπολογιστικά συστήματα και οι εφαρμογές που επεξεργάζονται όσα δεδομένα ρέουν από και προς τα «πράγματα» όπως το cloud computing.

Από λειτουργικής πλευράς, είναι χρήσιμο να σκεφτούμε πως οι συσκευές του IoT συνδέονται και επικοινωνούν σε σχέση με τα τεχνικά μοντέλα επικοινωνίας. Τον Μάρτιο του 2015, το Συμβούλιο Αρχιτεκτονικής του Διαδικτύου, (Internet Architecture Board – IAB) κυκλοφόρησε ένα κατευθυντήριο αρχιτεκτονικό έγγραφο για τη δικτύωση των έξυπνων αντικειμένων, που περιγράφει ένα πλαίσιο τεσσάρων κοινών μοντέλων επικοινωνίας που χρησιμοποιείται από συσκευές IoT. Παρακάτω παρουσιάζονται τα βασικά χαρακτηριστικά του κάθε μοντέλου.

i. Το μοντέλο επικοινωνίας Device-to-Device αντιπροσωπεύει δύο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους, και όχι μέσω ενδιάμεσου server εφαρμογών. Αυτές οι συσκευές επικοινωνούν μέσω πολλών τύπων δικτύων, συμπεριλαμβανομένων των δικτύων IP ή το Internet. Συχνά, ωστόσο, αυτές οι συσκευές χρησιμοποιούν πρωτόκολλα όπως Bluetooth, Z-Wave ή ZigBee για την καθιέρωση Device-to-Device επικοινωνίας.

ii. Σε ένα μοντέλο επικοινωνίας Device-to-Cloud, η IoT συσκευή συνδέεται απευθείας σε μια διαδικτυακή υπηρεσία cloud όπως ένας πάροχος υπηρεσιών εφαρμογής, ώστε να ανταλλάσσει δεδομένα και να διαχειρίζεται την κίνηση μηνυμάτων. Αυτή η προσέγγιση συχνά εκμεταλλεύεται υπάρχοντες μηχανισμούς επικοινωνίας όπως η παραδοσιακή ενσύρματη Ethernet ή Wi-Fi συνδέσεις για να εγκαταστήσει μια σύνδεση μεταξύ της συσκευής και του δικτύου IP, το οποίο τελικά συνδέεται με την υπηρεσία cloud.

iii. Στο μοντέλο Device-to-Gateway, ή αλλιώς, Device-to-Application-Layer-Gateway (ALG), η συσκευή IoT συνδέεται μέσω μιας υπηρεσίας ALG ως αγωγός για να επιτευχθεί μια σύνδεση με την υπηρεσία cloud. Με πιο απλά λόγια, αυτό σημαίνει ότι το μοντέλο Device-to-Gateway διαθέτει λογισμικό εφαρμογής, το οποίο δρα ως διαμεσολαβητής μεταξύ της συσκευής και της υπηρεσίας cloud και παρέχει ασφάλεια και άλλες λειτουργίες όπως δεδομένα ή μετάφραση πρωτοκόλλων.

iv. Το μοντέλο Back-End Data-Sharing αναφέρεται σε μια αρχιτεκτονική επικοινωνίας η οποία επιτρέπει στους χρήστες να εξάγουν και να αναλύουν τα δεδομένα του έξυπνου αντικειμένου από μια υπηρεσία cloud, σε συνδυασμό με δεδομένα από άλλες πηγές. Αυτή η προσέγγιση είναι μια επέκταση του μοντέλου επικοινωνίας Device-to-Cloud, η οποία επιτρέπει στις συσκευές IoT να ανεβάζουν τα δεδομένα μόνο για έναν πάροχο υπηρεσιών εφαρμογής. Η Back-End Data-Sharing αρχιτεκτονική επιτρέπει στα δεδομένα που συλλέγονται από μια συσκευή IoT να συγκεντρώνονται και να αναλύονται.

Για να κατανοήσουμε τους κινδύνους ασφαλείας που ελλοχεύουν στο IoT πρέπει πρώτα να καταλάβουμε το πως είναι στημένο ένα δίκτυο συσκευών (αισθητήρες, brokers, ενεργοποιητές) σε διάφορες εφαρμογές. Δεν πρέπει να ξεχνάμε ότι στο IoT οποιαδήποτε ηλεκτρονική συσκευή θα είναι ικανή να συνδέεται στο δίκτυο, προσφέροντας έτσι αναρίθμητες πιθανότητες εφαρμογών σε πολλά πεδία. Είναι αδύνατο να προβλέψει κανείς όλες τις πιθανές εφαρμογές του IoT έχοντας κατά νου την εξέλιξη της τεχνολογίας και τις διαφορετικές ανάγκες των δυνητικών χρηστών. Παρακάτω, θα δούμε μερικές κατηγορίες εφαρμογών του IoT. Ενώ υπάρχουν κυριολεκτικά εκατοντάδες εφαρμογές που αναγνωρίζονται από διάφορες βιομηχανίες, είναι εφικτό να ταξινομηθούν με έναν απλό, λογικό τρόπο.

- **Πρώτη κατηγορία εφαρμογών**

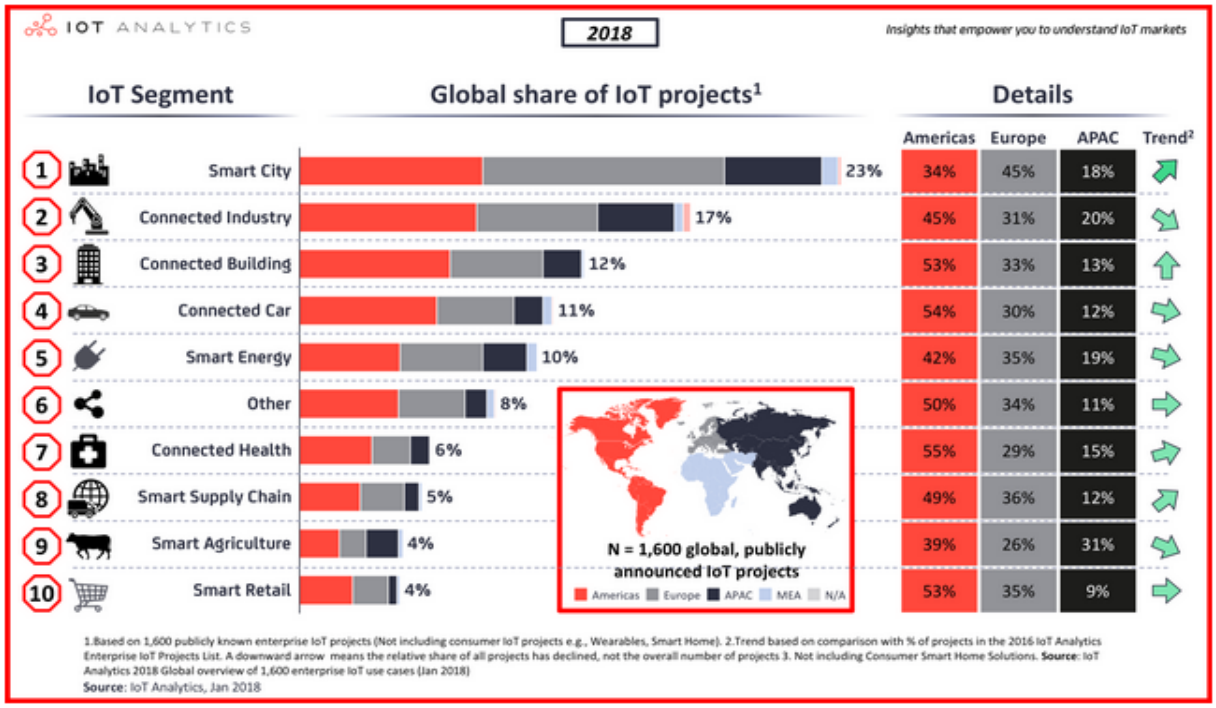
  Η πρώτη κατηγορία εφαρμογών περικλείει την ιδέα εκατομμυρίων ετερογενών έξυπνων και διασυνδεδεμένων συσκευών με μοναδικά αναγνωριστικά (ID) τα οποία αλληλεπιδρούν με άλλα μηχανήματα/αντικείμενα, υποδομές και το φυσικό περιβάλλον. Στην κατηγορία αυτή, το IoT παίζει σε μεγάλο βαθμό, τον ρόλο της διοίκησης, του ελέγχου και της διαδρομής. Όπως συμβαίνει με όλες τις πτυχές του IoT, η ασφάλεια και η προστασία είναι υψίστης σημασίας. Οι εφαρμογές αυτές δεν αποσκοπούν στην εξόρυξη δεδομένων από τις συμπεριφορές των ανθρώπων, αλλά κυρίως στην επέκταση του αυτοματισμού και της μηχανής προς μηχανή, μηχανής προς υποδομή, μηχανής προς φύση και γενικότερα επικοινωνιών που μπορούν να συνεισφέρουν και να βοηθήσουν στην απλοποίηση της ζωής των ανθρώπων.

- **Δεύτερη κατηγορία εφαρμογών**

  Η δεύτερη κατηγορία σχετίζεται με την επεξεργασία των δεδομένων που συλλέγονται από τους τελικούς κόμβους (έξυπνες συσκευές με αισθητήρες και δυνατότητα σύνδεσης) και την εύρεση των δεδομένων για τις τάσεις και τις συμπεριφορές που μπορούν να παράγουν χρήσιμες πληροφορίες σχετικές με το marketing προκειμένου να δημιουργηθεί επιπλέον εμπόριο. Οι εταιρείες πιστωτικών καρτών αλλά και οι κάρτες μελών των καταστημάτων, ήδη παρακολουθούν και χρησιμοποιούν την συμπεριφορά των ανθρώπων προκειμένου να καταλήξουν σε προσφορές που μπορούν να οδηγήσουν σε αυξημένες πωλήσεις. Τώρα, το ερώτημα είναι πόσο μακριά θα μπορούσαν να περιλαμβάνουν την παρακολούθηση των καταστημάτων που έχουμε επισκεφθεί, τους διαδρόμους που περιηγηθήκαμε και τον χρόνο που ξοδέψαμε κατά την διάρκεια των αγορών μας, ακόμα και το είδος των αντικειμένων που προμηθευτήκαμε. Τέτοια σενάρια είναι εύκολα εφικτά με τη χρήση ενός κινητού τηλεφώνου με GPS, RFID και έξυπνες/ασύρματες ετικέτες στα καταστήματα. Το αποτέλεσμα θα μπορούσε να είναι τόσο απλό όσο η παροχή προσφορών μέσω e-mail ή οι υπηρεσίες push στα σημεία πώλησης. Έτσι, μπορούμε να δούμε πως σε αυτή την κατηγορία το IoT μπορεί να επιτρέψει τη συλλογή δεδομένων σε κάθε πτυχή της καθημερινής ζωής του ανθρώπου με ευχάριστες ή δυσάρεστες συνέπειες. Αυτή η δεύτερη κατηγορία, κυρίως οι συζητήσεις γύρω από την ιδιωτική ζωή, την ασφάλεια

και την κοινωνική ευθύνη που πάει μαζί με την αυτοεπίγνωση, συνέδεσε τον κόσμο.

Όταν περάσαμε το κατώφλι του να συνδέουμε τελικά περισσότερα αντικείμενα απ' ότι ανθρώπους στο Διαδίκτυο, άνοιξε ένα τεράστιο παράθυρο που μας έδωσε την ευκαιρία να δημιουργήσουμε εφαρμογές σε τομείς όπως ο αυτοματισμός και η επικοινωνία μηχανής προς μηχανή. Στην πραγματικότητα, οι δυνατότητες είναι σχεδόν ατελείωτες. Τομείς των εφαρμογών περιλαμβάνουν: την πολεοδομία, τη διαχείριση αποβλήτων, το περιβάλλον, την κοινωνική αλληλεπίδραση, την αντιμετώπιση των καταστάσεων έκτακτης ανάγκης, τις έξυπνες αγορές, τις συσκευές οικιακού αυτοματισμού, τους έξυπνους μετρητές και πολλά άλλα. Τα ακόλουθα παραδείγματα τονίζουν μερικούς από τους τρόπους που το IoT αλλάζει τη ζωή των ανθρώπων προς το καλύτερο.



Παγκόσμια μερίδια έργων IoT τον Ιανουάριο του 2018. (Πηγή: iot-analytics.com). Τα ποσοστά της παραπάνω φωτογραφίας βασίζονται σε 1600 δημοσίως γνωστά επιχειρηματικά σχέδια (δεν περιλαμβάνονται προγράμματα για τον καταναλωτή, πχ. έξυπνο σπίτι, wearables).

- **Έξυπνες Πόλεις**. Οι ευφυείς πόλεις υπόσχονται μέγιστη ασφάλεια και αποτελεσματικότητα για το σύνολο των κατοίκων τους. Αισθητήρες τοποθετημένοι στα αυτοκίνητα, τα φώτα των οδικών αξόνων, ακόμα και στους κάδους απορριμμάτων συλλέγουν δεδομένα με στόχο τη μείωση του ενεργειακού κόστους και την παροχή καλύτερων υπηρεσιών. Αφορά κυρίως τη βελτίωση των πόλεων στην επίλυση προβλημάτων. Μερικές από τις δυνατότητες μιας έξυπνης πόλης φαίνονται παρακάτω.
  - **Μελέτη κατάστασης**.

    Παρακολούθηση των δονήσεων και των υλικών συνθηκών σε κτίρια, γέφυρες και ιστορικά μνημεία.
  - **Χάρτες αστικού θορύβου**.

    Παρακολούθηση των επιπέδων θορύβου σε περιοχές που υπάρχουν κέντρα ψυχαγωγίας και σε κεντρικές αστικές ζώνες σε πραγματικό χρόνο.

- **Ανίχνευση Έξυπνων Συσκευών**.

  Εντοπισμός συσκευών Android και iOS και γενικά οποιασδήποτε συσκευής λειτουργεί με διεπαφές Wi-Fi ή Bluetooth.

- **Έξυπνη Φωταγώγηση**.

  Πρόκειται για μια λύση στην απομακρυσμένη διαχείριση δημόσιας φωταγώγησης που θα ελέγχεται από συνδυασμό δεδομένων που θα προκύπτουν από αισθητήρες φωτός, βροχής και κίνησης, μέσω των οποίων θα ρυθμίζεται το άναμμα και το σβήσιμό τους. Πιθανές επιπρόσθετες δυνατότητες είναι η διαφοροποίηση λειτουργίας του συστήματος σε κατοικημένες περιοχές και σε μη κατοικημένες περιοχές, καθώς επίσης και η προσαρμοσμένη συμπεριφορά του συστήματος σε περιπτώσεις έκτακτης ανάγκης.

- **Διαχείριση Απορριμμάτων**.

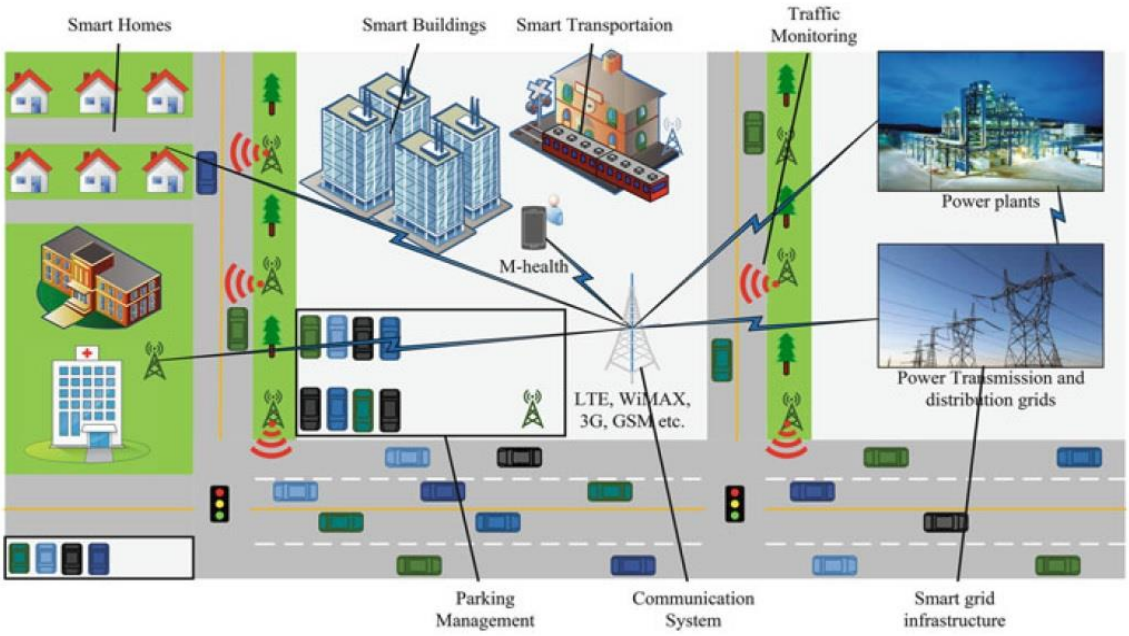
  Ανίχνευση των επιπέδων των σκουπιδιών για τη βελτιστοποίηση των δρομολογίων συλλογής απορριμμάτων.

- **Έξυπνοι Δρόμοι**.

  Ευφυείς αυτοκινητόδρομοι με προειδοποιητικά μηνύματα και εκτροπές ανάλογα με τις κλιματικές συνθήκες και απροσδόκητα γεγονότα όπως ατυχήματα ή κυκλοφοριακή συμφόρηση.

- **Έξυπνη Συγκοινωνία**.

  Σχετικά με τα μέσα μαζικής μεταφοράς, τα οχήματα θα είναι εξοπλισμένα με αισθητήρες που θα ανιχνεύουν την τοποθεσία τους σε πραγματικό χρόνο και θα ενημερώνουν τους επιβάτες για την πρόοδο της διαδρομής ή για τυχόν καθυστερήσεις. Επιπρόσθετα, οι έξυπνες στάσεις θα παρέχουν ακριβή πληροφόρηση, με ακρίβεια δευτερολέπτου, σε ότι αφορά τα δρομολόγια.



Παράδειγμα μιας έξυπνης πόλης. (Πηγή: "Internet of Things for Smart Cities. Technologies, Big Data and Security" Συγγραφείς: Waleed Ejaz & Alagan Anpalagan. Εκδόσεις Springer, 2019).

- **Έξυπνο Σπίτι**. Το έξυπνο σπίτι είναι το σύνολο των αυτοματισμών, με τους οποίους ομαδοποιούνται, οργανώνονται και αυτοματοποιούνται οι λειτουργίες μιας κατοικίας, ανάλογα με τις καθημερινές ανάγκες και συνήθειες που έχει ο εκάστοτε ιδιοκτήτης. Η δυνατότητα παρακολούθησης και διαχείρισης όλων των χώρων και εγκαταστάσεων μιας κατοικίας γίνεται με οποιοδήποτε τρόπο επικοινωνίας όπως μέσω σταθερού τηλεφώνου, κινητού τηλεφώνου ή/και διαδικτύου. Τα μελλοντικά έξυπνα σπίτια θα έχουν «συνείδηση» για το τι συμβαίνει μέσα σε ένα κτίριο, κυρίως επηρεαζόμενα από τρεις πτυχές: τη χρήση των πόρων, την ασφάλεια και την άνεση. Στόχος είναι να επιτευχθούν καλύτερα επίπεδα άνεσης όπως επίσης και μείωση των συνολικών δαπανών. Επιπλέον, τα έξυπνα σπίτια θα είναι σε θέση να αντιμετωπίσουν επαρκώς τα θέματα ασφαλείας μέσω πολύπλοκων συστημάτων ασφαλείας για την ανίχνευση πυρκαγιάς, κλοπής ή παράνομης εισόδου. Οι φορείς που εμπλέκονται σε αυτό το σενάριο αποτελούν μία πολύ ετερογενή ομάδα. Διάφοροι φορείς θα συνεργάζονται στο σπίτι του κάθε χρήστη, όπως εταιρείες του Διαδικτύου, κατασκευαστές συσκευών, φορείς εκμετάλλευσης τηλεπικοινωνιών, πάροχοι υπηρεσιών οπτικοακουστικών μέσων, εταιρείες προστασίας, εταιρείες κοινής ωφέλειας ηλεκτρικής ενέργειας κ.α. Ορισμένες από τις λειτουργίες ενός σπιτιού που μπορούν να ελεγχθούν / αυτοματοποιηθούν είναι:

  - **Χρήση ενέργειας και νερού**.

    Η κατανάλωση ενέργειας και νερού παρακολουθείται από έξυπνους μετρητές, ώστε να ληφθούν οι κατάλληλες συμβουλές για τη μείωση υπερβολικής κατανάλωσης των πόρων και του κόστους με σκοπό την καλύτερη διαχείριση ενέργειας.

  - **Απομακρυσμένος έλεγχος συσκευών**.

    Ενεργοποίηση και απενεργοποίηση συσκευών εξ' αποστάσεως για την αποφυγή ατυχημάτων και εξοικονόμηση ενέργειας. Με τη χρήση της έξυπνης πρίζας

προσαρμόζεται και ρυθμίζεται απλά και εύκολα η λειτουργία των συσκευών. Ουσιαστικά, με το πάτημα ενός κουμπιού π.χ. από το κινητό μας τηλέφωνο, μέσω Wi-Fi μπορούμε να συνδέσουμε οτιδήποτε: από καφετιέρα, μέχρι τηλεόραση και λαμπτήρες, και έτσι να ελέγχουμε με ακρίβεια την ενεργοποίηση και την απενεργοποίησή τους.

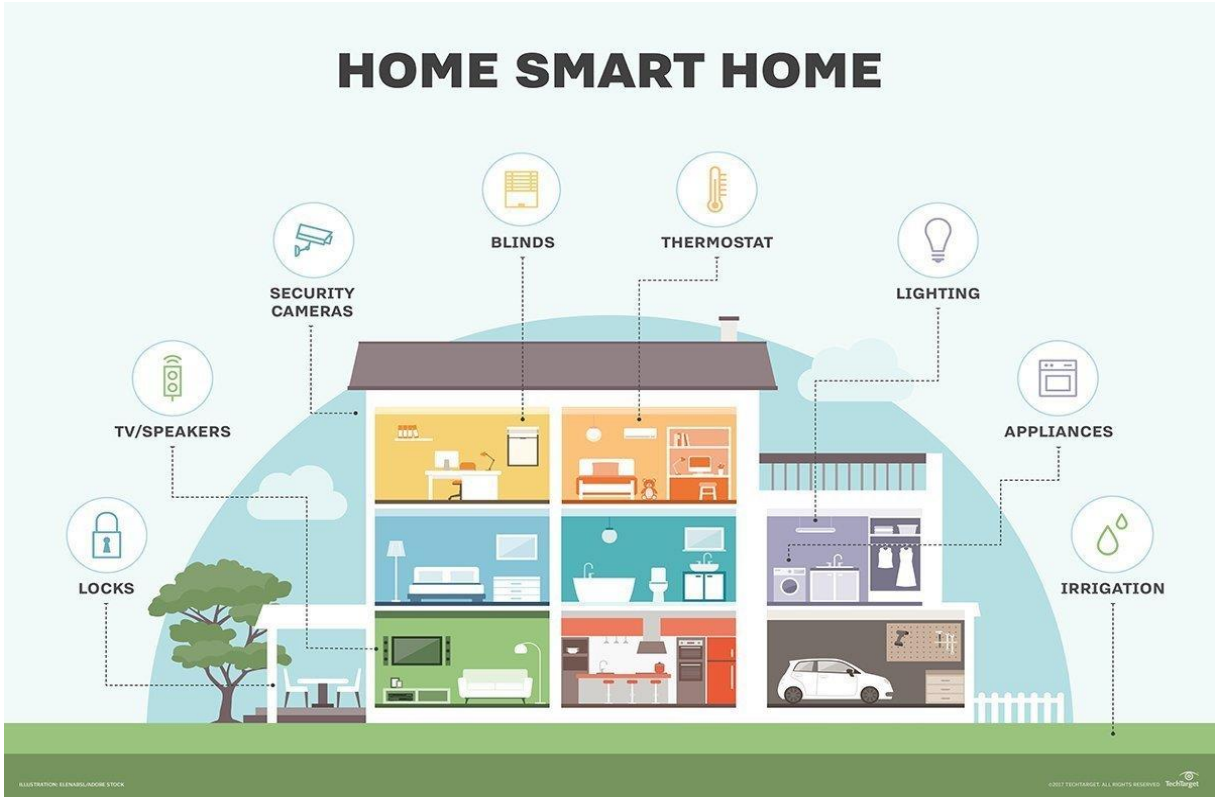
- **Συστήματα ανίχνευσης εισβολής**.

  Παρακολούθηση παραθύρων και θυρών, ώστε να γίνονται αντιληπτές οι παραβιάσεις και να αποτρέπονται οι εισβολείς.

- **Περιμετρικός έλεγχος πρόσβασης**.

  Έλεγχος πρόσβασης σε ζώνες περιορισμένης πρόσβασης και εντοπισμός ατόμων σε μη εγκεκριμένες περιοχές.

- **Έλεγχος φωτισμού**.
- **Κεντρικό σύστημα συναγερμού**.
- **Κεντρικό σύστημα θέρμανσης**.
- **Κεντρικό σύστημα διανομής εικόνας και ήχου**.
- **Απομακρυσμένη παρακολούθηση κλειδαριών**.
- **Σύστημα ποτίσματος**.
- **Έλεγχος ζεστού νερού**.
- **Έλεγχος τροφίμων – έξυπνα ψυγεία**.



Παράδειγμα έξυπνου σπιτιού (Πηγή: internetofthingsagenda.techtarget.com).

- **Έξυπνη βιομηχανία**. Σε μία παγκόσμια αλυσίδα εφοδιασμού, οι εταιρείες θα είναι σε θέση να παρακολουθούν όλα τα προϊόντα τους μέσω ετικετών RFID. Ως εκ τούτου, οι εταιρείες θα μειώσουν τα λειτουργικά τους έξοδα και θα βελτιώσουν την παραγωγικότητά τους. Επίσης, η συντήρηση των μηχανημάτων θα διευκολυνθεί από τους συνδεδεμένους αισθητήρες, επιτρέποντας την παρακολούθηση σε πραγματικό χρόνο, της καλής λειτουργίας και της απόδοσης του εξοπλισμού του εργοστασίου. Σε γενικές γραμμές το IoT θα παρέχει αυτόματες διαδικασίες που συνεπάγονται τη δραστική μείωση του αριθμού των εργαζομένων που χρειάζονται. Οι εργαζόμενοι θα αντικατασταθούν από αναγνώστες barcode, αισθητήρες και ενεργοποιητές, και τελικά από πολύπλοκα ρομπότ τόσο αποτελεσματικά όσο ένα ανθρώπινο ον. Χωρίς καμία αμφιβολία, οι τεχνολογίες αυτές θα φέρουν ευκαιρίες για τους εργαζόμενους σε νέες υπαλληλικές θέσεις και ένας μεγάλος αριθμός τεχνικών θα είναι απαραίτητος για τον προγραμματισμό και την επισκευή αυτών των μηχανημάτων. Αυτό είναι συνώνυμο με την ανάγκη δημιουργίας νέων θέσεων εργασίας κυρίως στον τομέα της συντήρησης αλλά αποτελεί επίσης μία νέα πρόκληση προκειμένου να προχωρήσουμε και να εξελίξουμε τέτοια είδη εργασίας για την αποφυγή της ανεργίας. Κάποιες από τις δυνατότητες ενός έξυπνου εργοστασίου αναφέρονται παρακάτω.

  - **Ποιότητα εσωτερικού αέρα**

    Παρακολούθηση τοξικών επιπέδων φυσικού αερίου και οξυγόνου μέσα στους χώρους εργασίας για την εξασφάλιση της ασφάλειας των εργαζομένων και των εμπορευμάτων.

  - **Παρακολούθηση θερμοκρασίας**

    Έλεγχος της θερμοκρασίας στο εσωτερικό των βιομηχανιών και σε ψυγεία που περιέχουν ευαίσθητα εμπορεύματα.

  - **Παρουσία όζοντος**

    Παρακολούθηση των επιπέδων του όζοντος κατά τη διάρκεια της διαδικασίας ξήρανσης του κρέατος σε εργοστάσια τροφίμων.

  - **Παρακολούθηση εσωτερικού χώρου**

    Αξιολόγηση εσωτερικού χώρου με χρήση ενεργού ZigBee και παθητικών ετικετών (RFID/NFC).

Παράδειγμα έξυπνης βιομηχανικής μονάδας (Πηγή: industryweek.com)

- **Έξυπνο περιβάλλον**. Η έννοια του έξυπνου περιβάλλοντος προωθεί την ιδέα ενός φυσικού κόσμου που είναι πλούσιος και ορατά συνυφασμένος με αισθητήρες, ενεργοποιητές, οθόνες και υπολογιστικά στοιχεία, που είναι ενταγμένα αρμονικά στα καθημερινά αντικείμενα της ζωής μας και συνδέονται μέσω ενός συνεχούς δικτύου. Έχουν περιγραφεί ως το υποπροϊόν των υπολογιστικών συστημάτων καθιστώντας την ανθρώπινη αλληλεπίδραση με το σύστημα μία ευχάριστη εμπειρία. Σε ένα έξυπνο περιβάλλον μπορούμε να συλλέξουμε και να αξιοποιήσουμε τις ακόλουθες πληροφορίες και έτσι να προστατευτούν οι πολίτες αλλά και η πολιτεία από καταστάσεις έκτακτης ανάγκης και φυσικών καταστροφών.
  - **Πυρανίχνευση δασικών περιοχών**

    Παρακολούθηση των αερίων καύσης και των συνθηκών που ευνοούν μία ενδεχόμενη πυρκαγιά προκειμένου να οριστούν οι επικίνδυνες ζώνες.
  - **Ατμοσφαιρική ρύπανση**

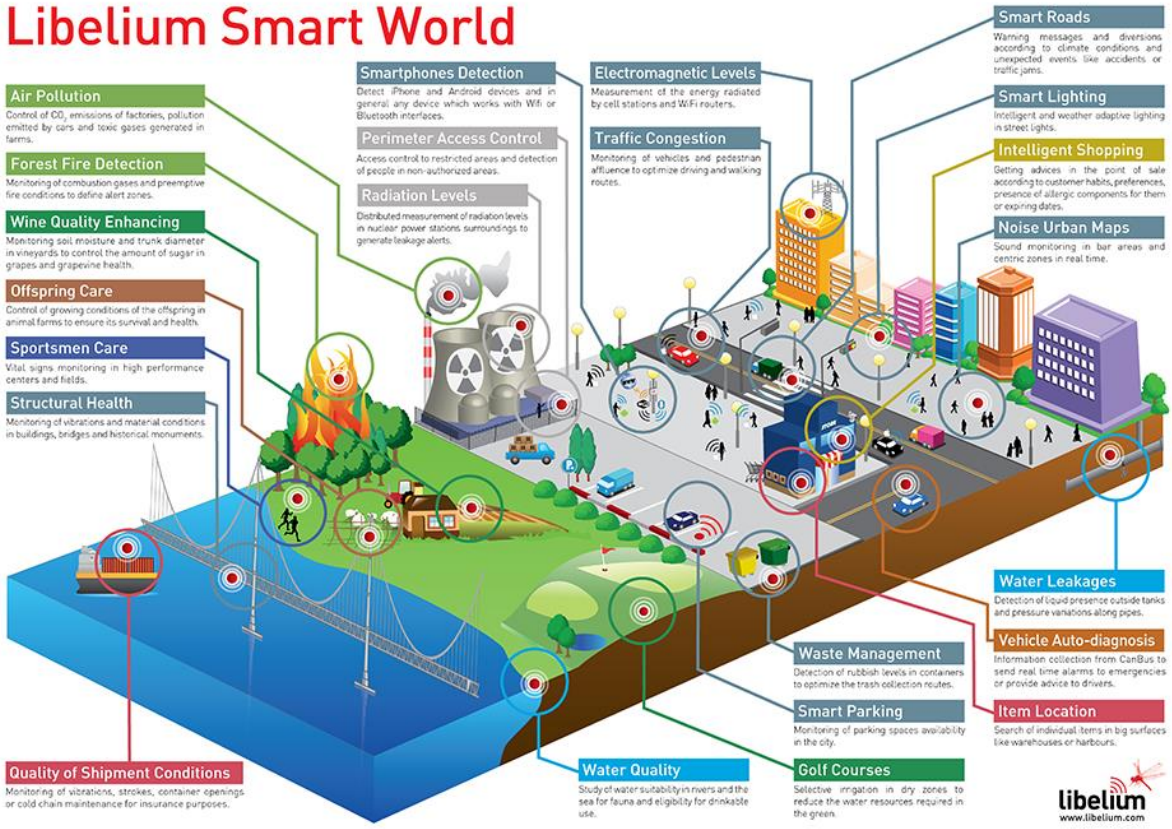
    Έλεγχος των εκπομπών διοξειδίου του άνθρακα (CO_2) των εργοστασίων και των αυτοκινήτων καθώς και των τοξικών αερίων που παράγονται σε αγροκτήματα.
  - **Παρακολούθηση επιπέδων χιονιού**

    Μέτρηση της στάθμης του χιονιού και ενημέρωση σε πραγματικό χρόνο για την ποιότητα του χιονιού σε πίστες του σκι και τον κίνδυνο χιονοστιβάδων.
  - **Πρόληψη κατολισθήσεων και χιονοστιβάδων**

    Παρακολούθηση της υγρασίας του εδάφους, των δονήσεων και της πυκνότητας της γης για την ανίχνευση επικίνδυνων φαινομένων.
  - **Πρώιμη ανίχνευση σεισμών**

    Κατανεμημένος έλεγχος σε συγκεκριμένες περιοχές δονήσεων.

- **Μετεωρολογικό έλεγχο**
- **Ανίχνευση ακτινοβολίας**
- **Έλεγχος κυμάτων και ακτών**
- **Παρακολούθηση του επιπέδου των ποταμών**
- **Έλεγχος ρύπανσης των υδάτων**



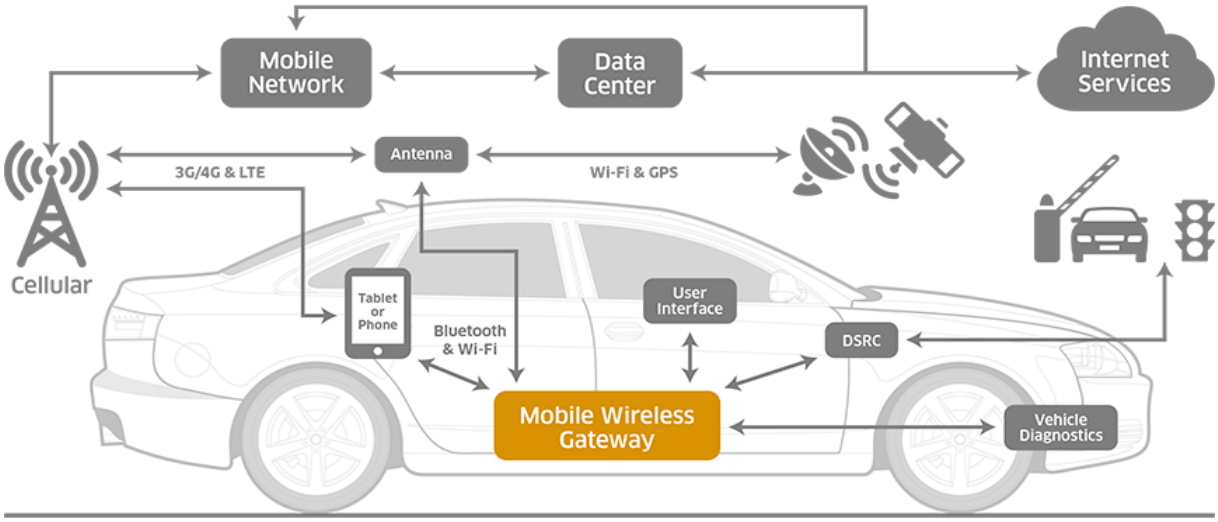
Παράδειγμα τμήματος έξυπνου περιβάλλοντος (Πηγή: libelium.com)

- **Έξυπνη κινητικότητα και μεταφορά**. Η σύνδεση των οχημάτων με το Διαδίκτυο δημιουργεί μια πληθώρα νέων δυνατοτήτων και εφαρμογών κάνοντας τη μεταφορά ευκολότερη και ασφαλέστερη. Στο πλαίσιο αυτό, η έννοια του Διαδικτύου Οχημάτων (Internet of Vehicles – IoV) συνδέεται με την έννοια του Διαδικτύου Ενέργειας (Internet of Energy – IoE), οι οποίες αντιπροσωπεύουν τις μελλοντικές τάσεις για έξυπνες εφαρμογές μεταφοράς και κινητικότητας. Ταυτόχρονα, η δημιουργία νέων κινητών οικοσυστημάτων που βασίζονται στην εμπιστοσύνη, την ασφάλεια και την ευκολία, είναι εφαρμογές που θα διασφαλίσουν την ασφάλεια, την κινητικότητα και την ευκολία στις συναλλαγές και υπηρεσίες που απευθύνονται στους καταναλωτές. Εκπροσωπώντας την ανθρώπινη συμπεριφορά στο σχεδιασμό, την ανάπτυξη και τη λειτουργία των κυβερνο-φυσικών συστημάτων σε αυτόνομα οχήματα είναι μια πρόκληση. Ενσωματώνοντας τα ανθρώπινα ζητήματα είναι ζωτικής σημασίας για την ασφάλεια, την αξιοπιστία και την προβλεψιμότητα. Επί του παρόντος, υπάρχει περιορισμένη κατανόηση του πως θα επηρεαστεί ο τρόπος συμπεριφοράς του οδηγού από αυτά τα συστήματα. Επιπλέον, είναι δύσκολο να προβλεφθούν τα αποτελέσματα

που θα προκύψουν από οδηγούς που βρίσκονται σε μεικτό περιβάλλον κυκλοφορίας (δηλαδή, οδηγούμενων οχημάτων και αυτόνομων οχημάτων). Δεδομένου ότι τα κυβερνο-φυσικά συστήματα έχουν γίνει πιο περίπλοκα και οι αλληλεπιδράσεις μεταξύ των εξαρτημάτων αυξάνεται, η ασφάλεια θα συνεχίσει να είναι υψίστης σημασίας. Όλα αυτά τα στοιχεία είναι πολύ σημαντικά για τα IoT οικοσυστήματα που έχουν αναπτυχθεί με βάση αυτές τις τεχνολογίες ευρείας εφαρμογής. Ακολουθούν κάποια σενάρια εφαρμογής του IoT στο πλαίσιο της αυτοκινητοβιομηχανίας και της τηλεματικής.

- **Το IoT ως αναπόσπαστο μέρος του ελέγχου και της διαχείρισης του οχήματος**. Ήδη σήμερα ορισμένες τεχνικές λειτουργίες των συστημάτων πλοήγησης των οχημάτων παρακολουθούνται σε απευθείας σύνδεση με το κέντρο εξυπηρέτησης ή το γκαράζ επιτρέποντας να καταστεί δυνατή η προληπτική συντήρηση, η απομακρυσμένη διάγνωση, η στιγμιαία υποστήριξη και έγκαιρη διαθεσιμότητα ανταλλακτικών. Για το σκοπό αυτό, τα δεδομένα από τους αισθητήρες που βρίσκονται στο όχημα, συλλέγονται από μια έξυπνη μονάδα και στέλνονται μέσω του Διαδικτύου στο κέντρο εξυπηρέτησης.
- **Το IoT επιτρέπει τη διαχείριση και τον έλεγχο της κυκλοφορίας**. Τα αυτοκίνητα θα πρέπει να είναι σε θέση να οργανωθούν προκειμένου να αποφευχθεί η κυκλοφοριακή συμφόρηση και να βελτιστοποιήσουν την χρήση ενέργειας. Αυτό μπορεί να γίνει σε συντονισμό και σε συνεργασία με την υποδομή του ελέγχου της κυκλοφορίας και του συστήματος διαχείρισης μιας έξυπνης πόλης. Επιπλέον οδική τιμολόγηση και φόρος στάθμευσης είναι σημαντικά στοιχεία ενός τέτοιου συστήματος. Περαιτέρω αμοιβαία επικοινωνία μεταξύ των οχημάτων και των υποδομών επιτρέπουν την ανάπτυξη νέων μεθόδων για την αύξηση της οδικής ασφάλειας, συμβάλλοντας έτσι στη μείωση του αριθμού των τροχαίων ατυχημάτων.
- **Το IoT δημιουργεί νέα σενάρια μεταφορών (πολυτροπικές μεταφορές)**. Σε αυτά τα σενάρια, π.χ. οι αυτοκινητοβιομηχανίες θα θεωρούν τους εαυτούς τους ως πάροχους κινητικότητας και όχι οι κατασκευαστές οχημάτων. Θα πρέπει να προσφέρεται στον χρήστη μια βέλτιστη λύση για τη μεταφορά του από το σημείο Α στο σημείο Β, με βάση όλα τα διαθέσιμα και κατάλληλα μέσα μεταφοράς. Έτσι, με βάση την στιγμιαία κατάσταση της κυκλοφορίας η ιδανική λύση μπορεί να είναι ένας συνδυασμός οχημάτων, κοινή χρήση οχημάτων, σιδηρόδρομοι και άλλα μέσα μεταφοράς. Προκειμένου να καταστεί δυνατή η απρόσκοπτη χρήση και η έγκαιρη διαθεσιμότητα των εν λόγω στοιχείων (συμπεριλαμβανομένων και των χώρων στάθμευσης), η διαθεσιμότητα θα πρέπει να επαληθευτεί και να διασφαλίζεται μέσα από on-line κρατήσεις, σε αλληλεπίδραση με τα προαναφερθέντα συστήματα διαχείρισης της κυκλοφορίας μιας έξυπνης πόλης.
- **Αυτόνομη οδήγηση και διασύνδεση με τις υποδομές**. Τα αυτόνομα οχήματα είναι σήμερα σε πρωτότυπη φάση. Εξειδικευμένα τσιπ βοηθούν τα οχήματα να κατανοήσουν το περιβάλλον γύρω τους, ανιχνεύοντας πεζούς, φανάρια, συγκρούσεις και οδικές λωρίδες. Τα οχήματα αυτά θα μπορούν να βοηθήσουν έναν οδηγό σε ασυνήθιστες συνθήκες, αντί να αναλάβουν τον πλήρη έλεγχο.

Αυτά τα σενάρια δεν είναι ανεξάρτητα το ένα από το άλλο και δείχνουν το πλήρες δυναμικό τους όταν συνδυάζονται και χρησιμοποιούνται σε διαφορετικές εφαρμογές. Τα έξυπνα συστήματα συλλέγουν πληροφορίες από τον χρήστη (π.χ. θέση, προορισμό, χρονοδιάγραμμα, κατάσταση του οχήματος, χρήση ενέργειας, κλιματικές συνθήκες, οδικές συνθήκες και προφίλ οδήγησης) και αλληλεπιδρούν με εξωτερικά συστήματα (π.χ. συστήματα ελέγχου της κυκλοφορίας, διαχείριση στάθμευσης, κοινή χρήση οχημάτων, υποδομές φόρτισης ηλεκτροκίνητων οχημάτων). Αυτό απαιτεί ισχυρούς αισθητήρες (και ενεργοποιητές) οι οποίοι θα είναι σε θέση να παραδώσουν αξιόπιστες πληροφορίες για τα συστήματα που αναφέρονται παραπάνω. Τέτοια αξιόπιστη επικοινωνία πρέπει να βασίζεται σε πρωτόκολλα επικοινωνίας M2M τα οποία θεωρούν σημαντικά την ασφάλεια και το χρονοδιάγραμμα. Η αναμενόμενη (τεράστια) ποσότητα των δεδομένων θα απαιτεί εξειδικευμένες τεχνικές εξόρυξης. Όταν ασχολούμαστε όμως, με πληροφορίες που σχετίζονται με τις θέσεις των οδηγών, τους προορισμούς, τις συνήθειες των χρηστών και τα χρονοδιαγράμματα, η ανησυχία για την προστασία της ιδιωτικής ζωής αποκτά υψηλότερη προτεραιότητα. Η ανησυχία αυτή μπορεί ακόμη και να σταθεί εμπόδιο στην ανάπτυξη τέτοιων τεχνολογιών. Κατά συνέπεια, ασφαλή μονοπάτια επικοινωνίας, αλλά και διαδικασίες που εγγυώνται την ανωνυμία και την απο-προσωποίηση των δεδομένων, αποκτούν μεγάλο ενδιαφέρον.



Έξυπνο αυτοκίνητο (Πηγή: rfpage.com)

- **Λιανική πώληση**. Το IoT αντιλαμβάνεται τόσο τις ανάγκες των πελατών όσο και τις ανάγκες των επιχειρήσεων: συγκρίνει την τιμή ενός προϊόντος σε σχέση με άλλα προϊόντα της ίδιας ποιότητας με χαμηλότερη τιμή και δίνει πληροφορίες όχι μόνο στους πελάτες αλλά και στα καταστήματα και επιχειρήσεις. Έχοντας αυτές τις πληροφορίες σε πραγματικό χρόνο βοηθά τις επιχειρήσεις να βελτιώσουν τις αγορές τους και να ικανοποιήσουν τις ανάγκες των πελατών. Προφανώς, μεγάλες αλυσίδες λιανικής πώλησης θα εκμεταλλευτούν τη δεσπόζουσα θέση τους για να ενδυναμώσουν και να επιβάλλουν τη μελλοντική IoT αγορά λιανικής πώλησης. Ειδικότερα οι εταιρείες με θέσεις ελέγχου θα είναι ικανές να ωθήσουν την υιοθέτηση της τεχνολογίας IoT λόγω των τεράστιων μεριδίων των αγορών τους. Αναφέρονται διάφοροι τομείς της λιανικής αγοράς που επηρεάζονται από την εισαγωγή IoT-συμβατής τεχνολογίας.

- **Έλεγχος προμηθειών**

  Παρακολούθηση των συνθηκών αποθήκευσης και παρακολούθηση προϊόντων.

- **Πληρωμή NFC**

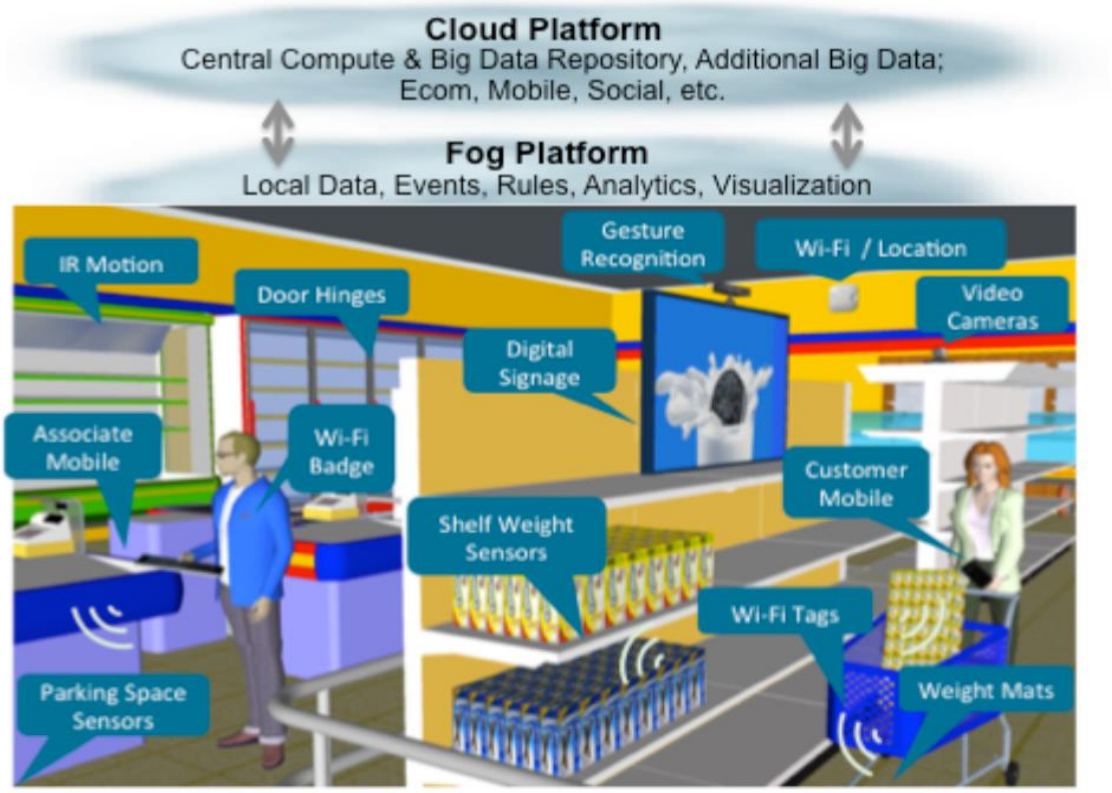
  Επεξεργασία των πληρωμών με βάση την περιοχή ή την διάρκεια της δραστηριότητας για τα μέσα μαζικής μεταφοράς, τα γυμναστήρια, τα θεματικά πάρκα κ.α.

- **Εφαρμογές έξυπνης αγοράς**

  Παροχή συμβουλών στο σημείο πώλησης σύμφωνα με τις συνήθειες των πελατών, τις προτιμήσεις και ενημέρωση για αλλεργικά συστατικά ή ημερομηνίες λήξεως.

- **Έξυπνη διαχείριση προϊόντων**

  Έλεγχος των προϊόντων στα ράφια και στις αποθήκες για την αυτοματοποίηση των διαδικασιών ανεφοδιασμού του αποθέματος.



Παράδειγμα έξυπνου καταστήματος (Πηγή: ibtimes.com)

- **Ιατρική παρακολούθηση εξ' αποστάσεως**. Ο έλεγχος και η πρόληψη είναι δύο από τους βασικούς στόχους της διατήρησης της υγείας. Ήδη σήμερα, οι άνθρωποι έχουν την δυνατότητα να παρακολουθούνται και να ελέγχονται από τους ειδικούς ακόμα και στην περίπτωση που βρίσκονται σε διαφορετικό μέρος. Το IoT δείχνει επίσης, μεγάλη ευελιξία στην παρακολούθηση του ιστορικού της υγείας των ασθενών.

Επιχειρηματικές εφαρμογές θα μπορούσαν να προσφέρουν την δυνατότητα ιατρικών υπηρεσιών όχι μόνο στους ασθενείς αλλά και στους ειδικούς, οι οποίοι χρειάζονται πληροφορίες για να προχωρήσουν στην ιατρική αξιολόγησή τους. Στον τομέα αυτό, το IoT καθιστά την ανθρώπινη αλληλεπίδραση πολύ πιο αποτελεσματική αφού επιτρέπει όχι μόνο τον εντοπισμό αλλά και την παρακολούθηση των ασθενών. Η παροχή πληροφοριών σχετικά με την κατάσταση του ασθενή καθιστά την όλη διαδικασία αποτελεσματικότερη, και επίσης αφήνει τους ανθρώπους πολύ πιο ικανοποιημένους. Οι πιο σημαντικοί παράγοντες σε αυτό το σενάριο θα είναι τα ιδιωτικά νοσοκομεία και τα ιδρύματα. Αξίζει να σημειωθεί οτι οι φορείς εκμετάλλευσης επικοινωνιών είναι αρκετά ενεργοί στην ηλεκτρονική υγεία. Το IoT μπορεί να προσφέρει βοήθεια στην παροχή υπηρεσιών υγείας με μερικούς από τους παρακάτω τρόπους.

- **Ιατρικά ψυγεία**

  Έλεγχος των συνθηκών μέσα σε καταψύκτες αποθήκευσης εμβολίων, φαρμάκων και οργανικών στοιχείων.

- **Φροντίδα αθλητών**

  Σημεία ελέγχου σε κέντρα υψηλής απόδοσης.

- **Επιτήρηση κατάστασης ασθενών**

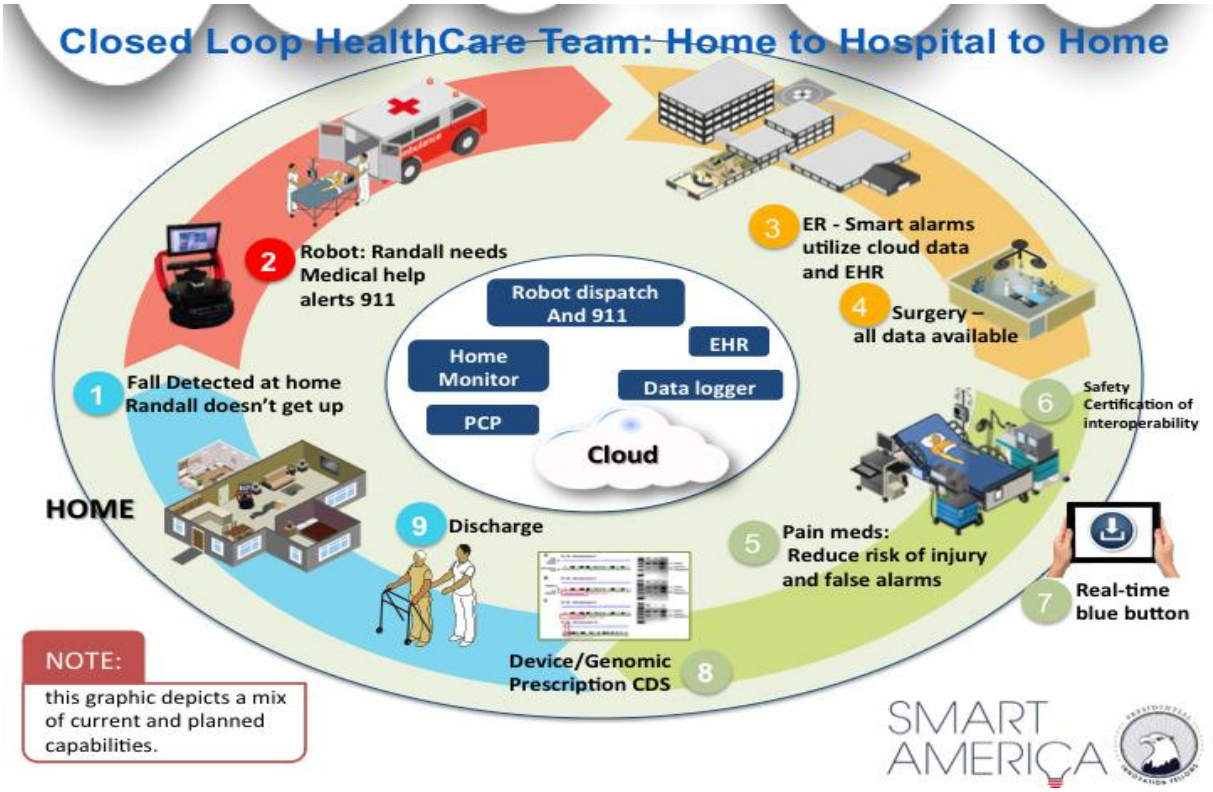
  Παρακολούθηση της πορείας των ασθενών μέσα σε νοσοκομεία, γηροκομεία και άλλους φορείς υγείας.

- **Υπεριώδης ακτινοβολία**

  Μέτρηση της υπεριώδους ακτινοβολίας (Ultraviolet Radiation – UV Radiation) του ηλίου, προκειμένου να προειδοποιείται ο κόσμος για την υπερβολική έκθεση στον ήλιο σε συγκεκριμένες ώρες.

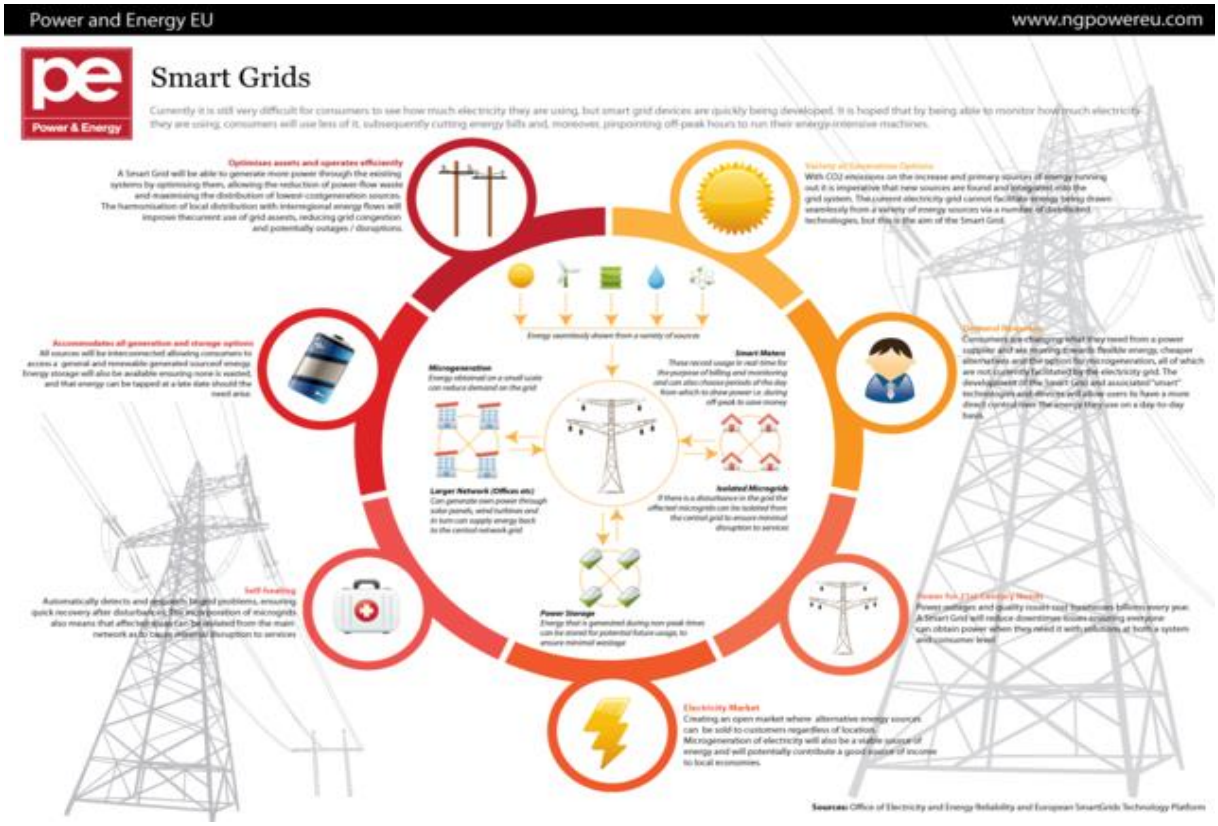
- **Βελτίωση της ποιότητας ζωής για τους ηλικιωμένους**

  Το IoT μπορεί να βελτιώσει σημαντικά την ποιότητα ζωής για τους ηλικιωμένους. Για παράδειγμα, μία ατομική, φορητή συσκευή, ικανή να ανιχνεύσει τις ζωτικές λειτουργίες ενός ατόμου, μπορεί να ειδοποιήσει έναν επαγγελματία υγείας σε περίπτωση σημείωσης κάποιας ανωμαλίας στις ζωτικές ενδείξεις, απώλεια αισθήσεων ή εάν κάποιος πέσει και αδυνατεί να σηκωθεί.



«Έξυπνη» παροχή βοήθειας στο σπίτι και στο νοσοκομείο (Πηγή: smartamerica.org).

- **Έξυπνη ενέργεια**. Το πεδίο αυτό έχει πολλές συσχετίσεις με άλλα σενάρια, όπως το έξυπνο σπίτι και την έξυπνη πόλη. Το βασικό ζήτημα σε αυτά τα σενάρια είναι ο εντοπισμός τρόπων για την μεγαλύτερη δυνατή εξοικονόμηση ενέργειας. Ουσιαστικά αναφερόμαστε σε αυτό που είναι γνωστό ως ένα έξυπνο πλέγμα (Smart Grid). Περιλαμβάνει τους έξυπνους μετρητές και την έξυπνη διαχείριση σκουπιδιών. Τα έξυπνα συστήματα μέτρησης συλλέγουν και μεταφέρουν δεδομένα μεταξύ του μετρητή και των προμηθευτών ενέργειας, των διαχειριστών δικτύων και τρίτων. Αυτό το ευφυές δίκτυο είναι ένα δισδιάστατο δίκτυο παροχής ηλεκτρικής ενέργειας που συνδυάζει πληροφορίες από χρήστες του δικτύου με στόχο την αποτελεσματική και οικονομικότερη παραγωγή, διανομή και κατανάλωση ηλεκτρικής ενέργειας.



Δυνατότητες ενός έξυπνου δικτύου (Smart Grid) (Πηγή: Wikipedia)

- **Έξυπνη μέτρηση**.

  Τα οφέλη των εφαρμογών έξυπνης μέτρησης είναι η βελτιωμένη ακρίβεια, η αξιοπιστία, η ευκολία βαθμονόμησης, η ασφάλεια και η καλύτερη διαχείριση της ενεργειακής κατανάλωσης. Ορισμένες από αυτές τις εφαρμογές αναφέρονται παρακάτω.

- **Έξυπνη παρακολούθηση**

  Παρακολούθηση και διαχείριση της κατανάλωσης ηλεκτρικής ενέργειας και νερού.

- **Παρακολούθηση επιπέδου στάθμης**

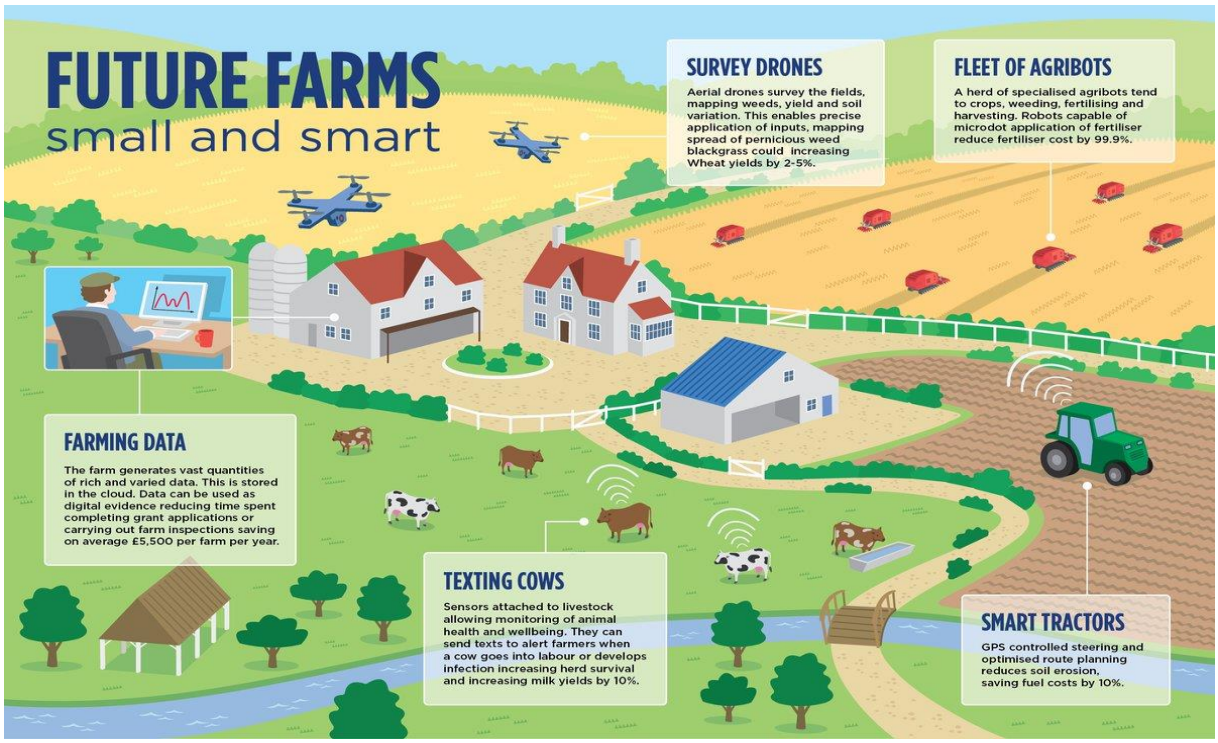
  Επιτήρηση της στάθμης του νερού, πετρελαίου και φυσικού αερίου σε δεξαμενές αποθήκευσης και βυτία.

- **Φωτοβολταϊκές εγκαταστάσεις**

  Παρακολούθηση και βελτιστοποίηση της απόδοσης, στον τομέα της ηλιακής ενέργειας.

- **Ροή νερού**

  Μέτρηση της πίεσης του νερού σε συστήματα μεταφοράς υδάτων.



Παράδειγμα έξυπνης φάρμας (Πηγή: nesta.org.uk).

- **Έξυπνη κτηνοτροφία**. Οι κανονισμοί για την δυνατότητα ανίχνευσης των αγροτικών ζώων και τις κινήσεις τους, απαιτούν τη χρήση τεχνολογιών IoT, ώστε να καταστεί δυνατός ο εντοπισμός των ζώων σε πραγματικό χρόνο, π.χ. κατά τη διάρκεια κρούσματος μεταδοτικής ασθένειας. Επιπλέον, σε πολλές περιπτώσεις οι χώρες δίνουν επιδοτήσεις ανάλογα με τον αριθμό των ζώων σε ένα κοπάδι, σε φάρμες με βοοειδή, αμνοερίφια και άλλα ζώα. Καθώς ο προσδιορισμός του αριθμού είναι δύσκολος, υπάρχει πάντα η πιθανότητα απάτης. Έξυπνα συστήματα αναγνώρισης μπορούν να βοηθήσουν στην ελαχιστοποίηση αυτής της απάτης. Ως εκ τούτου, με την εφαρμογή των συστημάτων αναγνώρισης, οι ασθένειες των ζώων μπορούν να ελεγχθούν, να ερευνηθούν και να προλαμβάνονται. Η επίσημη αναγνώριση των ζώων σε εθνικό, ενδοκοινοτικό και διεθνές εμπόριο έχει ήδη καθιερωθεί, ενώ την ίδια στιγμή, η ταυτοποίηση των ζώων που έχουν εμβολιαστεί ή ελέγχονται από επίσημο οργανισμό ελέγχου ασθενειών είναι επίσης δυνατή. Τα δείγματα αίματος και ιστού μπορούν να προσδιοριστούν με ακρίβεια, και η κατάσταση της υγείας των ζώων, όλων των χωρών και περιφερειών μπορεί επίσης να πιστοποιηθεί με τη χρήση του IoT.
- **Έξυπνη γεωργία**. Υπάρχει ένα ευρύ φάσμα της γεωργίας που βασίζεται σε διάφορες πρακτικές και εφαρμογές που έχουν τη δυνατότητα να αυξήσουν την παραγωγή τροφίμων και τη ικανότητα προσαρμογής του συστήματος παραγωγής τροφίμων, καθώς και τη μείωση των εκπομπών, όπως επίσης και να ενισχύσουν την αποθήκευση του άνθρακα στα γεωργικά εδάφη και τη βιομάζα. Με την χρήση του IoT, οι γεωργοί θα είναι σε θέση να παραδίδουν τις καλλιέργειες απευθείας στους καταναλωτές όχι μόνο σε μια μικρή περιοχή όπως οι ανοικτές αγορές ή τα καταστήματα, αλλά και στην ευρύτερη περιοχή. Αυτό θα αλλάξει το σύνολο της αλυσίδας εφοδιασμού, η οποία απαρτίζεται κυρίως από μεγάλες εταιρείες, σε μια πιο άμεση, μικρότερη αλυσίδα μεταξύ παραγωγών και καταναλωτών.

Κεφάλαιο 3ο: Ασφάλεια και Μοντέλα Επίθεσης.

Ένα περιβάλλον Internet of Things θα πρέπει να δομηθεί με τρόπο που θα διασφαλίζει την ασφάλεια και παράλληλα την ευκολία στη χρήση. Προέχει, οι πιθανοί χρήστες να πειστούν για τις εν λόγω ιδιότητες, προκειμένου να είναι σε θέση να απολαύσουν τα δυνητικά οφέλη του IoT, αποφεύγοντας επισφαλείς λύσεις. Στα πλαίσια του IoT, κάθε έξυπνο αντικείμενο έχει τη δυνατότητα να συνδέεται στο Διαδίκτυο και να επικοινωνεί με άλλα έξυπνα αντικείμενα, γεγονός που γεννά νέου είδους ζητήματα ασφάλειας και ιδιωτικότητας. Υπό αυτές τις συνθήκες, όσο πιο αυτόνομο γίνεται ένα αντικείμενο και ικανό να αναλαμβάνει πρωτοβουλίες, όλο και περισσότερα ζητήματα που αφορούν την ασφάλεια αναδύονται. Στα πλαίσια της ασφάλειας των υπολογιστικών συστημάτων και κατ' επέκταση του IoT, οι βασικές αρχές που θα πρέπει να διασφαλιστούν είναι οι εξής:

- **Εμπιστευτικότητα**

  Οι υπηρεσίες του IoT είναι πιθανό να εμπεριέχουν «ευαίσθητα» δεδομένα και πληροφορίες, για το λόγο αυτό, όλα τα διασυνδεδεμένα IoT αντικείμενα πρέπει να είναι διασφαλισμένα σχετικά με τους χρήστες που τα διαχειρίζονται. Η εμπιστευτικότητα μπορεί να επιτευχθεί μέσω συμμετρικής ή ασύμμετρης κρυπτογράφησης (κρυπτογράφησης δημόσιου κλειδιού). Παρόλα αυτά όμως, το είδος κρυπτογράφησης που θα επιλεχθεί έχει άμεση εξάρτηση με τις υπολογιστικές δυνατότητες του κάθε αντικειμένου. Λόγου χάρη, στο περιβάλλον ενός έξυπνου σπιτιού, που υπάρχουν πληροφορίες για τις δραστηριότητες των ενοίκων, οι ίδιοι δεν θα επιθυμούσαν οι τυχόν επισκέπτες να έχουν πρόσβαση σε τέτοια δεδομένα με την απλή παρατήρηση έξυπνων συσκευών.

- **Ιδιωτικότητα**

  Το IoT βρίσκει εφαρμογή σε πολλούς διαφορετικούς τομείς της καθημερινότητας που σχετίζονται με τα προσωπικά δεδομένα των χρηστών. Πιο συγκεκριμένα, τέτοιοι τομείς είναι η απομακρυσμένη παροχή ιατρικής φροντίδας, η διαχείριση της κυκλοφορίας, αλλά και η κατηγοριοποίηση των καταναλωτών σύμφωνα με τις αγοραστικές τους προτιμήσεις. Τεχνικές που χρησιμοποιούνται στις ροές πληροφοριών (Information Flow Control), αν και απαιτούν σημαντική υπολογιστική ισχύ, δίνουν τη δυνατότητα στα μεταδιδόμενα δεδομένα να χαρακτηρίζονται με στοιχεία, που προσδιορίζουν το λόγο της μεταφοράς και της ύπαρξης τους, προστατεύοντας έτσι την ιδιωτικότητα του χρήστη. Παράλληλα, προς την ίδια κατεύθυνση μπορούν να χρησιμοποιηθούν πρωτόκολλα ελέγχου πρόσβασης, που στηρίζονται σε τεχνικές που προφυλάσσουν την ανωνυμία (context-aware k-anonymity). Επιπρόσθετα, μπορεί να χρησιμοποιηθεί και μία τεχνική που υποβοηθά την επίτευξη ανωνυμίας. Αυτή καλείται CASTLE (Continuously Anonymizing Streaming data via adaptive cLustEring) και δίνει έμφαση στη «φρεσκάδα» και τον περιορισμό των καθυστερήσεων των δεδομένων. Έπειτα, ένα ενισχυμένο σύστημα DNS, προασπίζει την ιδιωτικότητα, μη αναθέτοντας ένα όνομα τομέα (Domain Name) σε ένα IoT κόμβο και προαπαιτώντας την ταυτοποίηση του χρήστη πριν του παρέχει πρόσβαση.

- **Ακεραιότητα**

  Στα πλαίσια του IoT, ανταλλάσσονται σημαντικά δεδομένα και με φορείς όπως κυβερνητικές αρχές, πάροχοι υπηρεσιών διαδικτύου (Internet Service Provider - ISP) και ελεγκτικοί μηχανισμοί, οι οποίοι απαιτούν τα δεδομένα, κατά την αποθήκευση και τη μετάδοσή τους, να μην αλλοιώνονται ούτε από δόλο αλλά ούτε από σφάλμα. Η ακεραιότητα των δεδομένων είναι πρωταρχικής σημασίας κατά το σχεδιασμό

αξιόπιστων IoT συστημάτων. Αυτό επιτυγχάνεται με κώδικες αυθεντικοποίησης μηνύματος (Message Authentication Code - MAC) που χρησιμοποιούν συναρτήσεις κατακερματισμού (Hash Functions). Η επιλογή των τεχνικών αυτών πάλι καθορίζεται από τις δυνατότητες των εκάστοτε συσκευών. Χαρακτηριστικό παράδειγμα που η ακεραιότητα των δεδομένων είναι εξ' ορισμού αναγκαία αποτελεί το έξυπνο σπίτι το οποίο είναι συνδεδεμένο με ένα έξυπνο πλέγμα ηλεκτροδότησης. Σ' αυτήν την περίπτωση, η ηλεκτρονική και αυτόματη έκδοση των λογαριασμών δεν συνάδει με πιθανή αλλοίωση στα δεδομένα της κατανάλωσης ηλεκτρικού ρεύματος.

- **Διαθεσιμότητα**

  Σε ένα σύγχρονο IoT περιβάλλον είναι δεδομένο ότι θα υπάρχουν κόμβοι που λειτουργούν ως εξυπηρετητές / διακομιστές. Στα πλαίσια ενός έξυπνου σπιτιού λόγου χάρη, θα υπάρχουν συσκευές - κόμβοι που θα αναμεταδίδουν δικτυακά, δεδομένα όπως τρέχουσα κατανάλωση ρεύματος, εικόνα από οικιακές κάμερες αλλά και την κατάσταση του συναγερμού. Είναι πολύ βασικό αυτές οι πληροφορίες να είναι ανά πάσα στιγμή διαθέσιμες στους άμεσα ενδιαφερόμενους. Κανένα όμως πρωτόκολλο ασφάλειας δεν διαβεβαιώνει από μόνο του την διαθεσιμότητα των δεδομένων και των υπηρεσιών στους ενδιαφερομένους. Χρειάζεται ένας συνδυασμός τεχνικών και πολλαπλές μετρήσεις πραγματικών δεδομένων για να βεβαιωθεί το ποσοστό διαθεσιμότητας. Συνήθως τέτοια χαρακτηριστικά αποτελούν αντικείμενο συμφωνιών σε επίπεδο υπηρεσιών (Service Level Agreements - SLAs) μεταξύ των παρόχων και των πελατών. Στο προαναφερθέν έξυπνο σπίτι, ένας πιθανός εισβολέας, που γνωρίζει την ύπαρξη μιας τέτοιας συσκευής καταγραφής, μπορεί, μέσω επαναλαμβανόμενων και συνεχών αιτημάτων, να εξαπολύσει επίθεση άρνησης υπηρεσιών (Denial Of Service - DoS), εκμεταλλευόμενος τους χαμηλούς ενεργειακούς της πόρους.

- **Αυθεντικότητα**

  Η αυθεντικότητα σχετίζεται με την επαλήθευση της ταυτότητας κάποιου. Στα πλαίσια του IoT, η αυθεντικότητα απαιτείται να υπάρχει και από τις δύο πλευρές. Με άλλα λόγια και ο αποδέκτης των δεδομένων πρέπει να είναι σίγουρος για την ταυτότητα του αποστολέα και την αυθεντικότητα της πηγής των πληροφοριών του, αλλά και η συσκευή – πάροχος των δεδομένων οφείλει να ταυτοποιεί τον αποδέκτη αυτών. Η αυθεντικότητα προϋποθέτει ισχυρούς μηχανισμούς στην πλευρά των IoT συσκευών, και πρωτόκολλα όπως το Datagram Transport Layer Security (DTLS), που εφαρμόζεται μεταξύ επιπέδου μεταφοράς και εφαρμογών στο μοντέλο OSI. Το εν λόγω πρωτόκολλο περιλαμβάνει πλήθος γνωστών αλγορίθμων (π.χ. βασισμένων σε ψηφιακά πιστοποιητικά) αυθεντικοποίησης και μπορεί να λειτουργήσει στο IPv4 και το IPv6. Επιπρόσθετα, άλλοι μηχανισμοί που υπόσχονται την ταυτοποίηση των IoT αντικειμένων είναι τα πρότυπα κωδικοποίησης EPC και ucode. Λέγοντας EPC εννοούμε τον ηλεκτρονικό κωδικό προϊόντων (Electronic Product Code), που είναι ένα παγκόσμιο πρότυπο ταυτοποίησης των προϊόντων μέσω ετικετών ανάγνωσης. Έχει τη μορφή Uniform Resource Identifier (URI). Το ucode επίσης, είναι ένας μηχανισμός ταυτοποίησης αντικειμένων ή τοποθεσιών, που χρησιμοποιεί 128-bit. Αποτελεί ουσιαστικό στοιχείο στην υλοποίηση του IoT. Η έλλειψη όμως υπολογιστικών πόρων των IoT συσκευών, αποτελεί μια τροχοπέδη προς την υιοθέτηση των εν λόγω προτύπων.

- **Έλεγχος Πρόσβασης**

  Οι μηχανισμοί ελέγχου πρόσβασης αναλαμβάνουν να υλοποιήσουν μοντέλα για τη διασφάλιση της εξουσιοδοτημένης πρόσβασης σε δεδομένα και πόρους, λαμβάνοντας αποφάσεις, βάσει ενός μοντέλου ελέγχου πρόσβασης. Καθώς το IoT είναι πλέον διάχυτο, η ιδιωτική και περιορισμένη πρόσβαση σε δεδομένα καθίσταται επιτακτική. Το βασικό στοιχείο που χρησιμοποιείται για τον έλεγχο πρόσβασης είναι οι λίστες ελέγχου πρόσβασης (Access-Control List - ACL) που καθορίζουν τα δικαιώματα των χρηστών. Παράλληλα υπάρχει και ο έλεγχος πρόσβασης που στηρίζεται στους ρόλους των χρηστών (Role-Based Access Control - RBAC). Εκεί οι άδειες χρήσης αποκτούνται με την ανάθεση ρόλων. Αυτοί οι ρόλοι δύναται να διαφοροποιούνται ανάλογα με το εκάστοτε περιεχόμενο κάθε εφαρμογής. Ακόμη έχουν δυναμικό χαρακτήρα και δύνανται να τροποποιηθούν σε ένα πραγματικό IoT σενάριο. Για παράδειγμα, ένας γιατρός μπορεί απομακρυσμένα να διαχειριστεί μηχανήματα διαφορετικού νοσοκομείου απ' το οποίο υπάγεται, μόνο εάν «κερδίσει» την εμπιστοσύνη των εκεί IoT οντοτήτων. Το μειονέκτημα των καταλόγων ελέγχου, είναι ότι στα ευρέως κατανεμημένα IoT συστήματα, με πολλαπλούς διαδραστικούς χρήστες, υστερούσαν στην απονομή των ελάχιστων δυνατών δικαιωμάτων ανά χρήστη. Αυτό διορθώθηκε με την ανάπτυξη του CapBAC (Capability Based Access Control), στο έργο IoT@Work του FP7, όπου ο χρήστης ο ίδιος παρουσιάζει τα δικαιώματα του, και δεν του τα απονέμει ο διακομιστής.

- **Αξιοπιστία**

  Πολλές εφαρμογές και υπηρεσίες εκ φύσεως είναι ευάλωτες, όπως οι υπηρεσίες ιατρικής περίθαλψης. Όταν αυτές στηρίζουν τη λειτουργεία τους σε IoT συσκευές θα πρέπει σίγουρα να διασφαλίζεται η αξιοπιστία που παρέχουν. Η αξιοπιστία αφορά επίσης και το πόσο «φρέσκα» είναι τα δεδομένα που μεταδίδονται. Πιθανώς λανθασμένα δεδομένα, είτε από δόλο είτε από σφάλμα, είναι ικανά να οδηγήσουν σε ανεπιθύμητες καταστάσεις. Για την εξασφάλιση της αξιοπιστίας συνήθως δομείται ένας μηχανισμός «διαπραγμάτευσης εμπιστοσύνης» (Trust Negotiation). Αυτός στηρίζεται στην ανταλλαγή διαπιστευτηρίων, μέσω P2P (Peer to Peer), πριν τη μετάδοση πληροφοριών. Ακολουθεί ένας πίνακας όπου διακρίνεται η ευαισθησία που έχουν τα διάφορα κομβικά σημεία ενός IoT περιβάλλοντος στις αρχές της ακεραιότητας, της αυθεντικότητας, της εμπιστευτικότητας και της διαθεσιμότητας.

Property / Topic	Integrity	Authenticity	Confidentiality	Privacy	Availability	Regulation
Communication	+++	+++	+++	++	+++	+
Sensors	+++	++	+	+++	+	+++
Actuators	+	+	+		+	++
Storage	+++	++	+++	+++	+	+++
Devices	+++	+	+	++	++	++
Processing	++	+	+	+++	+	+++
Localization/Tracking	+	+	+++	+++	+++	+++
Identification	++	+	+++	+++	+++	+++

Table 1: Sensitivity of topics in the Internet of Things to different security and privacy properties, and the need for laws and regulations (+ low sensitivity, ++ middle sensitivity, +++ high sensitivity)

Ευαισθησία των IoT οντοτήτων στις αρχές ασφαλείας. (Πηγή: Security and Privacy Challenges in the Internet of Things. Συγγραφέας: Christoph P. Mayer, ECEASST - 2009).

Τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Network - WSN) και τα συστήματα RFID διαδραματίζουν καθοριστικό ρόλο στο IoT περιβάλλον. Αυτές οι τεχνολογίες χαρακτηρίζονται από εξαιρετικά περιορισμένους υπολογιστικούς και ενεργειακούς πόρους. Αυτοί οι περιορισμοί πρέπει να ληφθούν σοβαρά υπόψη κατά το σχεδιασμό των προτάσεων διευθέτησης των ζητημάτων ασφαλείας. Ακόμη, το γεγονός ότι τα ασύρματα συνδεδεμένα αντικείμενα βρίσκονται και αλληλεπιδρούν με το φυσικό κόσμο δημιουργεί διόδους και επιλογές στα θέματα προστασίας και στο φυσικό στρώμα του μοντέλου OSI. Καθώς το Διαδίκτυο αποτελεί τη βάση πάνω στην οποία δομείται το IoT, είναι επόμενο, ότι τα κενά ασφαλείας του πρώτου θα ακολουθήσουν και το δεύτερο.

Ανάλυση Προβλημάτων Ασφαλείας.

Προκειμένου να καταλάβουμε το μέγεθος του προβλήματος, θα πρέπει να αποκτήσουμε μια πλήρη εικόνα του πώς σε ένα IoT σύστημα ενθυλακώνονται και χρησιμοποιούνται τα εκάστοτε πρωτόκολλα και οι τεχνολογίες που τα υλοποιούν. Ιδανικός οδηγός για αυτό είναι το μοντέλο OSI μιας και μπορούμε να τοποθετήσουμε κάθε τεχνολογία στο επίπεδο που της αναλογεί και να τη μελετήσουμε γενικότερα αλλά και ως προς την ασφάλεια ειδικότερα. Για παράδειγμα, οι τεχνολογίες που βασίζονται στο πρότυπο IEEE 802.15.4 καλύπτουν το Φυσικό Επίπεδο και το Επίπεδο Ζεύξης Δεδομένων, το ίδιο και το IEEE 802.15.1. Ουσιαστικά, με τον κατάλληλο εξοπλισμό μπορεί κανείς να υποκλέψει τα δεδομένα καθώς αυτά διακινούνται εντός ή εκτός της συσκευής IoT. Αν υποθέσουμε ότι κάποιος έχει στα χέρια του κάποια IoT συσκευή, π.χ. αισθητήρες συνδεδεμένους με Arduino, προκειμένου να εκτελέσει μια επίθεση με σκοπό την αλλοίωση των δεδομένων των αισθητήρων που η κάθε συσκευή φέρει, αρκεί να συνδέσει έναν παλμογράφο ανάμεσα στον αισθητήρα και στην πλακέτα του Arduino και να δει τα σήματα που ανταλλάσσονται. Κατόπιν μπορεί να αναπαράγει τέτοια σήματα κατά το δοκούν προσποιούμενος τον αισθητήρα. Δεδομένου ότι στις συσκευές Arduino η σειριακή θύρα είναι διαθέσιμη, μπορεί κάποιος να επαναπρογραμματίσει τα Arduino όπως επιθυμεί έτσι ώστε να αποστέλλονται λανθασμένα δεδομένα από αυτό. Μια τέτοια επίθεση θα μπορούσε να αποφευχθεί με την αφαίρεση της εκτεθειμένης σειριακής θύρας και τον εγκλεισμό σε προστατευμένο κουτί της IoT συσκευής.

Όσον αφορά το δεύτερο επίπεδο της Ζεύξης Δεδομένων (**Data Link Layer**) μια πολύ κοινή επίθεση είναι το MAC Spoofing όπου ο επιτιθέμενος όχι μόνο έχει αποκτήσει φυσική πρόσβαση στο δίκτυο στόχο αλλά αλλάζει/κρύβει και τη φυσική διεύθυνση του συστήματός του ώστε να μην γίνει εύκολα αντιληπτός. Αν όμως η στοίβα πρωτοκόλλων που χρησιμοποιείται δεν αξιοποιεί τις διευθύνσεις MAC, τότε αξιοποιώντας μια εφαρμογή ανάλυσης πρωτοκόλλων (Protocol Analyzer) μπορούμε να καταγράψουμε τα πλαίσια (frames) που ανταλλάσσονται. Αφενός μπορούμε να αποκτήσουμε πρόσβαση στο περιεχόμενο τους αν αυτό δεν κρυπτογραφείται χωρίς να είμαστε εμείς ο παραλήπτης. Αφετέρου μπορούμε να παρέμβουμε αποστέλλοντας με τη σειρά μας παρόμοια πλαίσια.

Επιθέσεις σε ανώτερα επίπεδα όπως αυτό του Δικτύου (**Network Layer**), ειδικά όταν χρησιμοποιείται το ευρύτατα χρησιμοποιούμενο IP, μπορούμε να βρούμε αρκετές και συνήθεις:

- **IP Spoofing** (πλαστογράφηση διεύθυνσης IP), είναι η τεχνική με την οποία στέλνονται IP πακέτα που έχουν ψεύτικη διεύθυνση αποστολέα. Το IP spoofing χρησιμοποιείται κατά κόρον από τους επιτιθέμενους καθώς τους δίνει την δυνατότητα να κρύβουν την πραγματική τους ταυτότητα σε διάφορες επιθέσεις που υλοποιούν. Άμεση εφαρμογή έχει σε επιθέσεις οι οποίες εκμεταλλεύονται την αδυναμία που παρουσιάζουν ορισμένες υπηρεσίες, οι οποίες χρησιμοποιούν μεθόδους ταυτοποίησης βασισμένες μόνο στην IP διεύθυνση του αποστολέα. Σε αυτό το μοντέλο μια υπηρεσία δημιουργεί ένα μήνυμα και το στέλνει στην αντίστοιχη υπηρεσία σε ένα απομακρυσμένο σύστημα. Η υπηρεσία στο απομακρυσμένο σύστημα κάνει δεκτή την αίτηση εξετάζοντας απλά την IP διεύθυνση που βρίσκεται μέσα στο μήνυμα. Συνήθως τέτοιου είδους ταυτοποίηση γίνεται όταν ο απομακρυσμένος host θεωρείται έμπιστος. Δυστυχώς όμως οι IP διευθύνσεις δεν σχεδιάστηκαν για να προσφέρουν ταυτοποίηση και κάποιος κακόβουλος χρήστης μπορεί να δημιουργήσει μια ψεύτικη αίτηση.

- **PING Flood (ICMP Flood)**. Τα ICMP (Internet Control Message Protocol) πακέτα μεταφέρουν ειδικά μηνύματα ελέγχου που χρησιμοποιούνται από το δίκτυο για θέματα συνδεσιμότητας. Όταν εκτελείται η εντολή ping, στέλνονται ICMP πακέτα στον παραλήπτη με κωδικό «ECHO_REQUEST» και ο παραλήπτης απαντά με μήνυμα «ECHO_REPLY». Όταν εκτελείται η επίθεση, ο εξυπηρετητής – θύμα «πλημμυρίζεται» με «ECHO_REQUEST» πακέτα, απασχολώντας τον από την ωφέλιμη εργασία του, αφού θα απαντά με «ECHO_REPLY» στις αιτήσεις που λαμβάνει. Η συγκεκριμένη μορφή επίθεσης αποσκοπεί στο να εξαντληθεί το εύρος ζώνης (Bandwidth) του θύματος. Στην πράξη, αυτό μπορεί να επιτευχθεί εφόσον ο επιτιθέμενος έχει μεγαλύτερο εύρος ζώνης από το θύμα (σε περίπτωση για παράδειγμα που ο επιτιθέμενος διαθέτει σύνδεση DSL ενώ ο αμυνόμενος απλή dial – up σύνδεση, που είναι πιο αργή).
- **Ping Of Death**. Παραλλαγή της ανωτέρω μορφής επίθεσης αποτελεί η επίθεση «Ping του θανάτου». Από την Wikipedia: *«Η επίθεση Ping Of Death συντελείται όταν ένας ηλεκτρονικός υπολογιστής στέλνει κακοσχηματισμένα πακέτα ping σε έναν άλλο υπολογιστή με σκοπό να τον θέσει εκτός λειτουργίας. Ένα πακέτο ping έχει κανονικά μέγεθος 64 bytes (ή 84 bytes εάν προστεθεί και η κεφαλίδα που προσθέτει το πρωτόκολλο IP). Πολλοί τύποι ηλεκτρονικών υπολογιστών δεν μπορούν να χειριστούν πακέτα ping που έχουν μέγεθος μεγαλύτερο από 65535 bytes, δηλαδή το μέγιστο επιτρεπτό από το πρωτόκολλο IP. Κατά συνέπεια, η επίθεση Ping Of Death περιλαμβάνει την συνεχή αποστολή μεγάλων πακέτων ping σε κάποιον υπολογιστή μέχρι ο τελευταίος να τεθεί εκτός λειτουργίας. Σύμφωνα με τα πρωτόκολλα του διαδικτύου, η αποστολή ενός πακέτου ping μεγαλύτερου των 65535 bytes είναι παράνομη και δεν προβλέπεται, δεδομένου ότι στην κεφαλίδα IP προβλέπονται μονάχα 16 bits για την καταχώρηση του μεγέθους του πακέτου (2^{16}-1 = 65535). Παρ' όλα αυτά ένας υπολογιστής μπορεί να σπάσει το πακέτο ping σε δύο τμήματα και να το στείλει ως δύο ξεχωριστά πακέτα IP. Όταν ο υπολογιστής-στόχος παραλάβει τα δύο πακέτα, θα τα συνθέσει και θα δημιουργήσει ένα μεγάλο πακέτο ping, το οποίο στην συνέχεια ενδέχεται να δημιουργήσει σφάλματα του τύπου buffer overflow, τα οποία συνήθως οδηγούν σε δυσλειτουργία ολόκληρου του υπολογιστή (computer crash)»*.
- **Teardrop**. Οι επιθέσεις Teardrop εκμεταλλεύονται την επανασυναρμολόγηση των κατακερματισμένων πακέτων IP. Ένα από τα πεδία της επικεφαλίδας IP είναι το fragmentation offset το οποίο δείχνει την αρχική και τελική θέση των δεδομένων που περιέχονται σε ένα κατακερματισμένο πακέτο, σε σχέση με τα δεδομένα του αρχικού μη κατακερματισμένου πακέτου. Όταν το άθροισμα της κεφαλίδας IP και του μεγέθους του κατακερματισμένου πακέτου διαφέρουν από το offset του επόμενου κατακερματισμένου πακέτου, τότε τα πακέτα συμπίπτουν και ο εξυπηρετητής προσπαθεί να συγκεντρώσει εκ νέου το πακέτο που μπορεί να χαλάσει, ιδιαιτέρως κιόλας όταν τρέχει σε παλιό λειτουργικό σύστημα που μπορεί να έχει αυτή την ευπάθεια.
- **Packet Sniffing**. Με το sniffing ο επιτιθέμενος είναι ικανός να βλέπει όλα τα πακέτα που ανήκουν στην δικτυακή κίνηση (traffic), που δημιουργείται από την επικοινωνία του θύματος με τα υπόλοιπα δικτυωμένα συστήματα και το Διαδίκτυο. Το sniffing συνήθως υλοποιείται από ειδικά προγράμματα τα οποία ονομάζονται sniffers και εκτελούνται σε κάποιο σημείο του δικτύου από το οποίο περνάει το traffic που αφορά το σύστημα - στόχο. Για παράδειγμα, σε ένα τοπικό LAN, που διάφορα συστήματα συνδέονται με ένα Hub, αν σε κάποιο από αυτά έχει εγκατασταθεί και λειτουργεί ένα sniffer, τότε αυτό μπορεί να βλέπει όλο το traffic του LAN και τις πληροφορίες που ανταλλάσσονται μεταξύ των συστημάτων του.

Μέσω του sniffing ο επιτιθέμενος μπορεί να συλλέξει κάποια σημαντική πληροφορία η οποία μεταφέρεται μέσα στα πακέτα που ανταλλάσσει το σύστημα - θύμα, όπως διάφορα Usernames και Passwords.

Αν περάσουμε στο επίπεδο Μεταφοράς (**Transport Layer**) τότε εκεί θα συναντήσουμε επιθέσεις σε πρωτόκολλα όπως το TCP και το UDP:

- **TCP SYN flood**. Από την Wikipedia: *«Η επίθεση SYN flood είναι ένα είδος επίθεσης άρνησης πρόσβασης (Denial of Service - DoS) κατά την οποία ο επιτιθέμενος αποστέλλει πολλαπλές αιτήσεις SYN προς το θύμα. Η επίθεση SYN flood είναι αρκετά συνηθισμένη και η πλειοψηφία των σημερινών δικτύων υπολογιστών είναι σε θέση να την αντιμετωπίσει με επιτυχία. Κύρια προϋπόθεση για να επιτύχει η επίθεση είναι ο διακομιστής να δεσμεύει πόρους του συστήματος αμέσως μόλις δεχθεί το πρώτο ACK πακέτο και όχι μετά το πέρας της τριμερούς χειραψίας. Η επίθεση έχει ως εξής: Ο επιτιθέμενος αποστέλλει στον διακομιστή - θύμα πολλαπλά πακέτα TCP SYN. Ο διακομιστής θεωρεί ότι τα πακέτα αυτά προέρχονται από κανονικό χρήστη, οπότε απαντά με πακέτα SYN-ACK σύμφωνα με την διαδικασία χειραψίας του πρωτοκόλλου TCP. Ο επιτιθέμενος όμως δεν αποστέλλει πακέτα ACK για να ολοκληρωθεί η χειραψία, αλλά αφήνει τον διακομιστή να περιμένει. Επειδή για κάθε ημιτελή σύνδεση TCP ο διακομιστής ξοδεύει υπολογιστικούς πόρους, μετά από κάποιο συγκεκριμένο αριθμό τέτοιων συνδέσεων ο διακομιστής φτάνει στα όριά του και δεν μπορεί να εξυπηρετήσει τους νόμιμους χρήστες. Αυτή η κατάσταση ονομάζεται άρνηση υπηρεσιών (DOS - Denial of Service)»*.
- **TCP reset attack**. Η επίθεση επαναφοράς TCP, γνωστή και ως «πλαστογράφηση TCP reset», «πλαστογραφημένα πακέτα επαναφοράς TCP» ή «επιθέσεις επαναφοράς TCP», είναι ένας τρόπος παραβίασης και να τερματισμού της σύνδεσης στο Διαδίκτυο στέλνοντας ένα πλαστό πακέτο επαναφοράς TCP. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί από ένα τείχος προστασίας (firewall) ή από κάποιον κακόβουλο χρήστη προκειμένου να διακόψει συνδέσεις στο Διαδίκτυο. Το Μεγάλο “Τείχος” της Κίνας είναι γνωστό για την χρήση πακέτων επαναφοράς TCP για την παρέμβαση και διακοπή συνδέων και αποτελεί μια σημαντική μέθοδο διεξαγωγής λογοκρισίας στο Διαδίκτυο.
- **UDP flood attack**. Από την Wikipedia: *«Η επίθεση UDP flood είναι μία υποπερίπτωση των επιθέσεων άρνησης υπηρεσιών (Denial of Service - DoS) στην οποία χρησιμοποιούνται πακέτα UDP. Η αντίστοιχη μορφή επίθεσης υπάρχει και για πακέτα TCP και μάλιστα είναι πολύ πιο συνηθισμένη. Μία επίθεση UDP flood περιλαμβάνει την αποστολή ενός πολύ μεγάλου αριθμού UDP πακέτων σε τυχαίες πόρτες ενός υπολογιστή. Ο υπολογιστής που δέχεται την επίθεση θα πρέπει αρχικά να διαπιστώσει εάν κάποια από τις υπηρεσίες του ακούει στην συγκεκριμένη πόρτα και εάν δεν ακούει να απαντήσει με ένα πακέτο “ICMP Destination Unreachable”. Άρα λοιπόν, η εισροή μεγάλου αριθμού UDP πακέτων στον υπολογιστή που υφίσταται την επίθεση τον αναγκάζει να απαντήσει με εξίσου μεγάλο αριθμό πακέτων ICMP, γεγονός που τελικά εμποδίζει άλλους απλούς χρήστες από το να χρησιμοποιήσουν τις υπηρεσίες του υπό επίθεση υπολογιστή. Ο επιτιθέμενος μπορεί στο πεδίο Source Address των πακέτων UDP να μην χρησιμοποιήσει την δικιά του διεύθυνση IP, αλλά κάποια άλλη τυχαία διεύθυνση. Με τον τρόπο αυτό παραμένει ανώνυμος και ο υπολογιστής που δέχεται την επίθεση δεν μπορεί να τον εντοπίσει. Επιπροσθέτως τα πακέτα ICMP που στέλνει ο υπολογιστής που υφίσταται την επίθεση δεν τον επηρεάζουν καθόλου»*.

Στο επίπεδο Συνόδου (**Session Layer**) έχουμε Session hijacking επιθέσεις σε υφιστάμενες συνδέσεις Επιπέδου Μεταφοράς όπως επιθέσεις:

- **Man-In-The-Middle**. Από την Wikipedia: *«Η επίθεση Man-In-The-Middle είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή/και να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες. Οι επιθέσεις Man-In-The-Middle εφαρμόζονται ιδιαίτερα στο πρωτόκολλο Diffie-Hellman, όταν η συμφωνία ανταλλαγής κλειδιών γίνεται χωρίς επικύρωση (authentication)»*.
- **Blind hijacking**. Η τυφλή «πειρατεία» περιγράφει έναν τύπο απόπειρας απόκτησης ελέγχου συνόδου, στον οποίο ο επιτιθέμενος δεν μπορεί να καταγράψει την κυκλοφορία επιστροφής από τον host. Αυτό σημαίνει ότι ο επιτιθέμενος εισάγει κακόβουλα ή χειριστικά πακέτα στα «τυφλά» χωρίς να έχει καμία επιβεβαίωση για την επίτευξη του επιθυμητού αποτελέσματος μέσω sniffing. Ο επιτιθέμενος πρέπει να επιχειρήσει να προβλέψει τους αριθμούς ακολουθίας των πακέτων TCP που διασχίζουν το δίκτυο μεταξύ του θύματος και όσων βρίσκονται στο άλλο άκρο της καθιερωμένης σύνδεσης. Ο λόγος αυτής της πρόβλεψης πηγαίνει πίσω στην τριμερή χειραψία TCP η οποία εκτελεί τον συγχρονισμό αριθμών ακολουθίας μεταξύ των μερών της σύνδεσης κατά τη διαδικασία δημιουργίας αυτής.

Στο επίπεδο Παρουσίασης (**Presentation Layer**) έχουμε επιθέσεις στον τρόπο που τα δεδομένα παραδίδονται στις τελικές εφαρμογές χρήστη. Σε αυτό το επίπεδο συνήθως γίνεται η κρυπτογράφηση/αποκρυπτογράφηση δεδομένων σε διάφορα πρωτόκολλα όπως το SSL και το TLS. Οπότε επιθέσεις σε τέτοια πρωτόκολλα είναι Session Layer επιθέσεις:

- **BEAST**. Το ακρωνύμιο BEAST σημαίνει **B**rowser **E**xploit **A**gainst **S**SL/**T**LS (Ευπάθεια Προγράμματος Περιήγησης εναντίον SSL/TLS). Αυτό το τρωτό σημείο αποτελεί επίθεση κατά της εμπιστευτικότητας μιας HTTP Secure (HTTPS) σύνδεσης, που εκτελείται σε αμελητέο χρονικό διάστημα. Παρέχει δηλαδή έναν τρόπο εξαγωγής μη κρυπτογραφημένου κειμένου από μια κρυπτογραφημένη συνεδρία. Για να εκτελεστεί η επίθεση πρέπει να πληρούνται τρεις προϋποθέσεις:
  i. Να υπάρχει JavaScript ή ένεση applet στην ίδια προέλευση της ιστοσελίδας.
  ii. Πρέπει να είναι δυνατή η καταγραφή πακέτων της σύνδεσης (sniffing).
  iii. Πρέπει να χρησιμοποιείται μια ευάλωτη έκδοση του SSL που κάνει χρήση block cipher.
- **Compression attacks**. Σε μια επίθεση κατά της συνάρτησης «συμπίεσης», η χρήση προσαρμοστικής «συμπίεσης» δεδομένων σε ένα μείγμα επιλεγμένου γνωστού και αγνώστου κειμένου, μπορεί να οδηγήσει σε αλλαγές στο μήκος και το περιεχόμενο του κειμένου προς κρυπτογράφηση, οι οποίες είναι δυνατόν να ανιχνευθούν ακόμα και αν το περιεχόμενο του κειμένου είναι κρυπτογραφημένο. Αυτό μπορεί να χρησιμοποιηθεί σε επιθέσεις πρωτοκόλλου για να ανιχνεύσει πότε το εγχυμένο γνωστό κείμενο ομοιάζει έστω και ελάχιστα με το άγνωστο περιεχόμενο του μυστικού μηνύματος, μειώνοντας σημαντικά την πολυπλοκότητα της αναζήτησης για το μυστικό κείμενο.

Τέλος, στο επίπεδο Εφαρμογής (**Application Layer**) οι επιθέσεις αφορούν την εκάστοτε εφαρμογή τελικού χρήστη όπως:

- **FTP bounce επίθεση**. Η επίθεση αυτή εκμεταλλεύεται το πρωτόκολλο FTP, στην οποία ο επιτιθέμενος χρησιμοποιεί την εντολή PORT για να ζητήσει πρόσβαση σε θύρες δια μέσου της μηχανής – θύματος. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί για την διακριτική ανίχνευση θυρών και την απόκτηση πρόσβασης σε συγκεκριμένες θύρες που θα ήταν διαφορετικά αδύνατη, όπως π.χ. με τον σαρωτή nmap.
- **SSH brute force**. Όπως είναι γνωστό, σε μια επίθεση «ωμής δύναμης» (Brute Force Attack) ο επιτιθέμενος δοκιμάζει αλλεπάλληλα, πολλούς συνδυασμούς usernames και passwords με σκοπό την πρόσβαση σε κάποιο λογαριασμό ή (σε αυτήν την περίπτωση) έναν εξυπηρετητή. Το μεγαλύτερο πρόβλημα με μια τέτοια επίθεση είναι οτι τα συστήματα είναι σχεδιασμένα να σταματούν τους εισβολείς μετά από έναν προκαθορισμένο αριθμό προσπαθειών εισόδου. Και σε αντίθεση με έναν κανονικό ιστότοπο, με το SSH, μια επίθεση «ωμής δύναμης» δεν είναι δυνατή offline. Αυτός είναι και ο λόγος όπου σε μια επίθεση «ωμής δύναμης» SSH, ο μηχανισμός αντιστρέφεται. Αντι να δοκιμάζει χιλιάδες usernames και passwords, ο επιτιθέμενος δοκιμάζουν έναν συνδυασμό username και password σε χιλιάδες εξυπηρετητές. Οι άνθρωποι πολύ συχνά χρησιμοποιούν «αδύναμους» κωδικούς, πράγμα που καθιστά εφικτή την επίθεση, και επειδή ο κάθε εξυπηρετητής καταγράφει μόνο μία αποτυχημένη απόπειρα εισόδου, ο επιτιθέμενος δεν χρειάζεται να ανησυχεί για οποιονδήποτε μηχανισμό αποκλεισμού.
- **SQL Injection**. Μια SQL επίθεση συμβαίνει όταν ο επιτιθέμενος πληκτρολογεί SQL κώδικα ερωτήματος σε μια φόρμα στο διαδίκτυο και η web εφαρμογή που επεξεργάζεται αυτόν τον κώδικα δεν τον ελέγχει σωστά και τον επικυρώνει (δηλαδή τον εκτελεί), επιτρέποντας με αυτόν τον τρόπο τον εισβολέα να δώσει εντολές στη βάση δεδομένων για να διαρρεύσει αυτή τα δεδομένα της. Διαφορετικές εντολές παίρνουν διαφορετικά αποτελέσματα και συχνά ένας εισβολέας θα προσπαθήσει πολλές παραλλαγές για να δει τι θα του δώσει ως απάντηση μια βάση δεδομένων σε αυτές. Ένας εισβολέας, για παράδειγμα, μπορεί να στείλει ένα είδος εντολών SQL για να εμφανίσει όλα τα περιεχόμενα μιας βάσης δεδομένων στον περιηγητή του ή μπορεί να χρησιμοποιήσει άλλες εντολές για να εμφανίσει μέρη της βάσης δεδομένων ή για να αποκτήσει την δυνατότητα να προσθέσει, να τροποποιήσει ή να διαγράψει τα περιεχόμενα της βάσης δεδομένων.
- **Cross Site Request Forgery**. Το CSRF είναι ένας τύπος κακόβουλης εκμετάλλευσης ενός ιστότοπου, στον οποίο μεταδίδονται εντολές από έναν χρήστη που εμπιστεύεται η εφαρμογή ιστού. Υπάρχουν πολλοί τρόποι με τους οποίους ένας κακόβουλος ιστότοπος μπορεί να μεταδώσει τέτοιες εντολές. Ειδικά επεξεργασμένες ετικέτες εικόνας (HTML image tags), κρυφές φόρμες και JavaScript XMLHttpRequests, για παράδειγμα, μπορούν να λειτουργήσουν χωρίς την αλληλεπίδραση ή τη γνώση του χρήστη. Σε αντίθεση με την επίθεση XSS (που θα δούμε παρακάτω), η οποία εκμεταλλεύεται την εμπιστοσύνη που έχει ένας χρήστης για έναν συγκεκριμένο ιστότοπο, η CSRF εκμεταλλεύεται την εμπιστοσύνη που έχει ένας ιστότοπος στο πρόγραμμα περιήγησης ενός χρήστη.

- **XSS (Cross-Site Scripting)**. Από την Wikipedia: *«Με τον όρο Cross-Site Scripting ή XSS (δεν είναι CSS γιατί αλλιώς θα υπήρχε πρόβλημα ονομασίας) αναφερόμαστε στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή Javascript σε κάποιο ιστοχώρο. Κάποιος κακόβουλος χρήστης, θα μπορούσε να εισάγει κώδικα σε έναν ιστοχώρο, μέσω ενός κειμένου εισόδου για παράδειγμα, ο οποίος αφού δεν θα φιλτραριζόταν από τον ιστοχώρο σωστά, θα μπορούσε να προκαλέσει προβλήματα στον διαχειριστή ή επισκέπτη του ιστοχώρου. Ο κακόβουλος χρήστης θα μπορούσε να επιτύχει:*

    - *Κλοπή κωδικών/λογαριασμών κλπ προσωπικών δεδομένων*
    - *Αλλαγή ρυθμίσεων του ιστοχώρου*
    - *Κλοπή των cookies*
    - *Ψεύτικη διαφήμιση (μέσω, π.χ., ενός συνδέσμου)*

    Η ευπάθεια αναφέρεται στην αδυναμία του συστήματος που υποστηρίζει ο ιστοχώρος να φιλτράρει και να απορρίψει τυχόν επιβλαβείς εισόδους».

- **Slowloris DoS**. Η Slowloris είναι μια επίθεση άρνησης υπηρεσιών που επιτρέπει σε ένα μόνο μηχάνημα να «ρίξει» τον διακομιστή ενός άλλου μηχανήματος με ελάχιστο εύρος ζώνης και παρενέργειες στις μη σχετικές υπηρεσίες και θύρες. Η Slowloris προσπαθεί να δημιουργήσει πολλές συνδέσεις στον διακομιστή – θύμα και να τις κρατήσει ενεργές όσο το δυνατόν περισσότερο. Αυτό το πετυχαίνει ανοίγοντας συνδέσεις με τον διακομιστή προορισμού και στέλνοντας ένα μερικό αίτημα. Ανά μικρές περιόδους θα στέλνει κεφαλίδες HTTP, που προστίθενται στο αίτημα αλλά ποτέ δεν το ολοκληρώνουν. Οι διακομιστές – θύματα θα διατηρήσουν τις συνδέσεις αυτές «ζωντανές», φθάνοντας σταδιακά στο μέγιστο αριθμό ταυτόχρονων συνδέσεων που μπορούν να υποστηρίξουν, ώσπου τελικά θα αρνηθούν περαιτέρω συνδέσεις από χρήστες.

Ακόμη, θα αναλυθούν οι δέκα βασικές αδυναμίες ασφαλείας του IoT όπως αυτές έχουν καταγραφεί από τον οργανισμό OWASP (Open Web Application Security Project).

- **Insecure Web Interface (Μη Ασφαλής Διεπαφή Ιστοτόπου).**

  Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι μπορούν να κάνουν τα εξής για να πραγματοποιήσουν με *εύκολο* τρόπο μία επίθεση: να χρησιμοποιήσουν τα «αδύναμα» προεπιλεγμένα διαπιστευτήρια (credentials) τα οποία δεν έχουν αλλαχθεί, να πάρουν στην κατοχή τους κωδικούς πρόσβασης οι οποίοι διακινούνται με απλό κείμενο, να απαριθμήσουν τους λογαριασμούς (account enumeration) που έχουν πρόσβαση στην διεπαφή ιστοτόπου (web interface). Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση δύναται να είναι εσωτερικοί ή εξωτερικοί χρήστες οι οποίοι έχουν πρόσβαση στην διεπαφή ιστοτόπου. Η Μη Ασφαλής Διεπαφή Ιστοτόπου (Insecure Web Interface) είναι μια αδυναμία ασφάλειας η οποία είναι *κοινώς διαδεδομένη* και, *εύκολα ανιχνεύσιμη*. Μία τέτοιου είδους αδυναμία λαμβάνει χώρα, όταν ζητήματα όπως, η απαρίθμηση των λογαριασμών, η έλλειψη της επιλογής αποσύνδεσης του χρήστη (account lockout) ή οι «αδύναμοι» κωδικοί πρόσβασης του διαχειριστή (admin), παρουσιάζονται σε μία διεπαφή ιστοτόπου. Οι μη ασφαλείς διεπαφές ιστοτόπου είναι διαδεδομένες καθώς η πρόθεση είναι τα συγκεκριμένα interfaces να είναι εκτεθειμένα μόνο σε εσωτερικά δίκτυα, ωστόσο οι απειλές από τους εσωτερικούς χρήστες μπορούν να είναι εξίσου σημαντικές όσο είναι και οι απειλές οι οποίες μπορούν να προέρχονται από εξωτερικούς χρήστες. Ζητήματα που αφορούν μια τέτοιου είδους απειλή, μπορεί εύκολα να ανακαλυφθούν εάν εξετασθεί το interface χειροκίνητα με την βοήθεια αυτόματων εργαλείων ελέγχου (testing tools), τα οποία εντοπίζουν και άλλες απειλές όπως είναι το Cross-Site Scripting. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η απώλεια ή αλλοίωση των δεδομένων, έλλειψη λογοδοσίας (lack of accountability), άρνηση πρόσβασης σε εξουσιοδοτημένους χρήστες ή ακόμα και απόκτηση του πλήρους ελέγχου των συσκευών από τον επιτιθέμενο. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν εάν σε μια τέτοια επίθεση θα μπορούσαν να δεχτούν οποιαδήποτε απώλεια των συσκευών τους και κατά συνέπεια μ' αυτό τον τρόπο να θιγούν οι πελάτες τους και η ίδια η επωνυμία της εταιρίας. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν η διεπαφή ιστότοπού μας είναι ασφαλής ή όχι είναι οι εξής:

  i. Εάν το προεπιλεγμένο όνομα χρήστη και κωδικός πρόσβασης μπορεί να αλλάξει κατά την διάρκεια της αρχικής εγκατάστασης ενός προγράμματος.

  ii. Εάν ένας συγκεκριμένος λογαριασμός χρήστη, κλειδώνεται μετά από 3 ή 5 αποτυχημένες προσπάθειες εισόδου.

  iii. Εάν λογαριασμοί χρηστών οι οποίοι είναι σε ισχύ, μπορούν να αναγνωριστούν χρησιμοποιώντας μηχανισμούς ανάκτησης κωδικών ή νέες σελίδες χρηστών.

  iv. Να επανεξεταστεί το interface για θέματα όμως το Cross-Site Scripting, το Cross Site Request Forgery και το SQL injection.

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι μια διεπαφή ιστότοπου θα είναι ασφαλής απαιτείται:

i. Να αλλαχθούν οι προεπιλεγμένοι κωδικοί πρόσβασης και τα ονόματα χρηστών κατά την διάρκεια της αρχικής εγκατάστασης ενός προγράμματος.

ii. Να εξασφαλιστεί σύνθετη δημιουργία κωδικού πρόσβασης.

iii. Να εξασφαλιστεί ότι η διεπαφή ιστοτόπου δεν είναι επιρρεπής σε XSS, SQLi ή CSRF.

iv. Να εξασφαλιστεί ότι οι κωδικοί πρόσβασης δεν είναι εκτεθειμένοι στο εσωτερικό ή εξωτερικό δίκτυο.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι ικανός να διαπιστώσει εύκολα εάν ένας λογαριασμός χρήστη είναι έγκυρος ή όχι, ή μπορεί να εξακριβώσει εάν η ιστοσελίδα είναι επιρρεπής σε Cross-Site Scripting (XSS):

Σενάριο 1ο: ο ιστότοπος παρουσιάζει την λειτουργικότητα «This user account does not exist» κατά την οποία εάν εισαχθεί ένας μη έγκυρος λογαριασμός χρήστη, ενημερώνει τον επιτιθέμενο ότι ο συγκεκριμένος λογαριασμός δεν υπάρχει. Μόλις εντοπιστεί ένας έγκυρος λογαριασμός χρήστη, ο επιτιθέμενος ξεκινά την διαδικασία για να μαντέψει τον κωδικό πρόσβασης μέχρι να τον βρει. Αυτό του επιτρέπεται να το πραγματοποιήσει, από την στιγμή που δεν υπάρχει έλεγχος κλειδώματος λογαριασμού:

Account john_doe@email.com does not exist.

Σενάριο 2ο: ο ιστότοπος είναι τρωτός σε Cross-Site Scripting:

http://abc.com/index.php?user=<script>alert(XSS!)</script> ...
Ο εξυπηρετητής μέσω του προγράμματος περιήγησης θα εμφανίσει pop-up το οποίο θα αναγράφει «XSS!».

- **Insufficient Authentication/Authorisation (Ανεπαρκής Ταυτοποίηση/Εξουσιοδότηση).**
  Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τα εξής για να πραγματοποιήσουν με *σχετικά εύκολο* τρόπο μία επίθεση: τους «αδύναμους» κωδικούς πρόσβασης, τους μη ασφαλείς μηχανισμούς ανάκτησης κωδικών πρόσβασης, τα ανεπαρκώς προστατευμένα διαπιστευτήρια (credentials) ή την έλλειψη λεπτομερούς ελέγχου πρόσβασης που αφορά μια συγκεκριμένη διεπαφή. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση δύναται να είναι εσωτερικοί ή εξωτερικοί χρήστες, οι οποίοι έχουν πρόσβαση στην διεπαφή χρήστη, διεπαφή κινητής συσκευής (mobile interface) ή στην διεπαφή cloud (cloud interface). Η Ανεπαρκής Ταυτοποίηση/Εξουσιοδότηση (Insufficient Authentication/Authorisation), είναι μια αδυναμία ασφάλειας η οποία είναι *κοινώς διαδεδομένη* και *εύκολα ανιχνεύσιμη*. Όταν χρησιμοποιούνται κωδικοί πρόσβασης οι οποίοι είναι αδύναμοι ή δεν προστατεύονται με τον σωστό τρόπο, οποιαδήποτε προσπάθεια Ταυτοποίησης ή Εξουσιοδότησης δεν θα έχει αποτέλεσμα.

Πολλά ζητήματα που αφορούν την ταυτοποίηση και εξουσιοδότηση μπορούν να εξιχνιαστούν εάν γίνει έλεγχος της διεπαφής χειροκίνητα ή με αυτόματους ελέγχους. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η απώλεια ή αλλοίωση των δεδομένων, έλλειψη λογοδοσίας, άρνηση πρόσβασης σε εξουσιοδοτημένους χρήστες ή ακόμα και απόκτηση του πλήρους ελέγχου από τον επιτιθέμενο, των συσκευών ή των λογαριασμών των χρηστών. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν εάν σε μια τέτοια επίθεση θα μπορούσαν να δεχτούν οποιαδήποτε απώλεια των συσκευών τους ή των λογαριασμών των χρηστών τους. Όλα τα δεδομένα είναι πιθανό να κλαπούν, να τροποποιηθούν ή και να διαγραφούν. Κάτι τέτοιο θα έχει σαν συνέπεια να θιγούν και οι πελάτες τους. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν μία διεπαφή ιστότοπου έχει επαρκή Ταυτοποίηση ή όχι είναι οι εξής:

i. Αν προσπαθήσετε να χρησιμοποιήσετε έναν απλό κωδικό πρόσβασης όπως είναι το «1234» και σας επιτραπεί, είναι ένας απλός και γρήγορος τρόπος για να διαπιστώσετε εάν η πολιτική που ακολουθείται στους κωδικούς πρόσβασης σε όλα τα interfaces είναι επαρκής.

ii. Επανεξέταση της κυκλοφορίας των διαπιστευτηρίων στο δίκτυο ώστε να διαπιστωθεί εάν μεταδίδονται σε μορφή απλού κειμένου.

iii. Επανεξέταση των απαιτήσεων όσο αφορά τον έλεγχο των κωδικών πρόσβασης, όπως για παράδειγμα η πολυπλοκότητα του κωδικού πρόσβασης, ο έλεγχος της ιστορικότητάς του, η λήξη του και ο εξαναγκασμός για ορισμό καινούργιου, από τους νέους χρήστες.

iv. Επανεξέταση εάν απαιτείται ταυτοποίηση σε δύο διαφορετικά στοιχεία (2FA - Two Factor Authentication) για ευαίσθητες λειτουργίες.

Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν η διεπαφή ενός ιστότοπου έχει επαρκή έλεγχο εξουσιοδότησης ή όχι είναι οι εξής:

i. Επανεξέταση των διαφόρων interfaces που διαθέτουμε για να διαπιστωθεί εάν γίνεται διαχωρισμός των ρόλων. Για παράδειγμα, όλες οι λειτουργίες είναι διαθέσιμες στον διαχειριστή (administrator), αλλά οι χρήστες έχουν πρόσβαση μόνο σε έναν περιορισμένο αριθμό λειτουργιών.
ii. Επανεξέταση του ελέγχου πρόσβασης και έλεγχος για αύξηση δικαιωμάτων (Privilege Escalation).

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι θα γίνει η καλύτερη δυνατή προσπάθεια για επαρκή Ταυτοποίηση ή Εξουσιοδότηση απαιτείται να εξασφαλιστεί:

i. Ότι απαιτούνται μόνο ισχυροί κωδικοί πρόσβασης.

ii. Γίνεται λεπτομερής έλεγχος πρόσβασης όπου αυτό απαιτείται.

iii. Διασφαλίζεται η σωστή προστασία των διαπιστευτηρίων.

iv. Πραγματοποιείται ταυτοποίηση σε δύο στοιχεία όπου είναι δυνατόν.

v. Η ύπαρξη μηχανισμών ανάκτησης ενός κωδικού πρόσβασης είναι ασφαλής.

vi. Ότι θα απαιτηθεί ταυτοποίηση εκ νέου σε ευαίσθητες λειτουργίες.

vii. Ότι θα υπάρχουν επιλογές για διαμόρφωση ελέγχου των κωδικών πρόσβασης.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι ικανός εύκολα να μαντέψει τον κωδικό πρόσβασης ή να αποκτήσει πρόσβαση στα διαπιστευτήρια καθώς αυτά διασχίζουν το δίκτυο καθώς και να τα αποκωδικοποιήσει αφού είναι προστατευμένα μόνο βάση της κωδικοποίησης Base64:

Σενάριο 1ο: η διεπαφή χρήστη απαιτεί μόνο απλούς κωδικούς πρόσβασης:

Username = Bob; Password = 1234

Σενάριο 2ο: το όνομα χρήστη και ο κωδικός πρόσβασης δεν είναι επαρκώς προστατευμένα όταν μεταδίδονται μέσω του δικτύου:

Authorisation: Basic YWRtaW46MTIzNA==

- **Insecure Network Services (Μη Ασφαλείς Υπηρεσίες Δικτύου).**
Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τα εξής για να πραγματοποιήσουν με *σχετικά εύκολο* τρόπο μία επίθεση: τις ευάλωτες υπηρεσίες δικτύου για να επιτεθούν σε μια συσκευή, επιθέσεις χρησιμοποιώντας διαδοχικές συνδέσεις (bounce attacks) των συσκευών. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση δύναται να είναι εσωτερικοί ή εξωτερικοί χρήστες, οι οποίοι έχουν πρόσβαση σε μια συσκευή μέσω μίας σύνδεσης δικτύου. Οι Μη Ασφαλείς Υπηρεσίες Δικτύου (Insecure Network Services) είναι μια αδυναμία ασφάλειας η οποία *δεν είναι κοινώς διαδεδομένη* και *σχετικά εύκολα ανιχνεύσιμη*. Μία συσκευή μπορεί να είναι επιρρεπής σε επιθέσεις υπερχείλισης μνήμης (Buffer Overflow) ή σε επιθέσεις που δημιουργούν άρνηση υπηρεσιών (DoS), με αποτέλεσμα να μην είναι προσβάσιμη από τον χρήστη. μη ασφαλείς υπηρεσίες δικτύου συχνά ανιχνεύονται από αυτοματοποιημένα εργαλεία όπως είναι τα port scanners και τα fuzzers. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *μέτριες*, αφού είναι πιθανή η απώλεια ή αλλοίωση των δεδομένων, η άρνηση παροχής υπηρεσιών και η διευκόλυνση των επιθέσεων σε άλλες συσκευές. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρησή τους, σε περίπτωση που οι συσκευές τους δεν θα είναι προσβάσιμες λόγω επίθεσης τύπου άρνησης παροχής υπηρεσιών ή εάν οι συσκευές χρησιμοποιούνται για να διευκολύνουν επιθέσεις απέναντι σε άλλες συσκευές και δίκτυα. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν οι υπηρεσίες δικτύου είναι ασφαλείς ή όχι είναι οι εξής:

i. Να εξεταστεί η συσκευή μας για ανοιχτές θύρες (open ports), χρησιμοποιώντας έναν σαρωτή για θύρες (port scanner).

ii. Αν βρεθούν ανοιχτές θύρες, μπορεί η κάθε μια απ' αυτές να δοκιμαστεί χρησιμοποιώντας ένα αυτόματο εργαλείο το οποίο ψάχνει για ευπάθειες οι οποίες μπορεί να: είναι τύπου DoS, αφορούν UDP (User Datagram Protocol) υπηρεσίες, αφορούν υπερχείλιση μνήμης και επιθέσεις τύπου fuzzing (fuzzing attacks).

iii. Επανεξέταση των δικτυακών θυρών (network ports) για να διαπιστωθεί εάν όντως χρειάζεται να είναι εκτεθειμένες στο διαδίκτυο χρησιμοποιώντας UPnP (Universal Plug and Play).

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι θα γίνει η καλύτερη δυνατή προσπάθεια για να εξασφαλιστούν ασφαλείς υπηρεσίες δικτύου απαιτείται:

i. Μόνο οι απαραίτητες θύρες να είναι εκτεθειμένες και διαθέσιμες.

ii. Να εξασφαλιστούν υπηρεσίες οι οποίες δεν είναι ευπαθείς σε υπερχείλιση μνήμης και επιθέσεις τύπου fuzzing.

iii. Να υπάρχουν υπηρεσίες οι οποίες δεν είναι ευπαθείς σε επιθέσεις DoS, και δεν μπορούν να επηρεάσουν τις ίδιες ή άλλες συσκευές ή ακόμα και τους χρήστες του τοπικού δικτύου ή άλλου δικτύου.

iv. Οι δικτυακές θύρες ή οι υπηρεσίες δεν είναι εκτεθειμένες στο διαδίκτυο για παράδειγμα μέσω UPnP.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι ικανός να απενεργοποιήσει μια συσκευή πλήρως μέσω της εντολής HTTP GET ή να αποκτήσει πρόσβαση σε μία συσκευή μέσω του διαδικτύου δια μέσου της θύρας 80 ή 443:

Σενάριο 1ο: Επίθεση Fuzzing η οποία προκαλεί διακοπή λειτουργίας των υπηρεσιών δικτύου και των συσκευών:

GET %s%s%s%s%s%s%s%s%s%s%s%s%s%s HTTP/1.0

Σενάριο 2ο: Θύρες οι οποίες είναι ανοιχτές στο διαδίκτυο, ενδεχομένως χωρίς να το γνωρίζει ο χρήστης, μέσω UPnP :

Οι θύρες 80 και 443 συνδέονται με το Διαδίκτυο μέσω οικιακού δρομολογητή.

- **Lack of Transport Encryption (Έλλειψη Κρυπτογράφησης κατά την Μεταφορά των Δεδομένων).**

Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι προκειμένου να πραγματοποιήσουν με *σχετικά εύκολο* τρόπο μία επίθεση μπορούν να χρησιμοποιήσουν την έλλειψη την κρυπτογράφησης κατά την μεταφορά των δεδομένων, για να δουν τα δεδομένα που διακινούνται μέσω του δικτύου. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση δύναται να είναι εσωτερικοί ή εξωτερικοί χρήστες, οι οποίοι έχουν πρόσβαση στο δίκτυο μέσω μιας συνδεδεμένης συσκευής. Η Έλλειψη Κρυπτογράφησης κατά την Μεταφορά των Δεδομένων (Lack of Transport Encryption), είναι μια αδυναμία ασφάλειας η οποία είναι *κοινώς διαδεδομένη* και *εύκολα ανιχνεύσιμη*. Μία τέτοιου είδους αδυναμία αφήνει εκτεθειμένα στον επιτιθέμενο τα δεδομένα τα οποία «ταξιδεύουν», μέσω του τοπικού δικτύου ή του Διαδικτύου.

Η Έλλειψη Κρυπτογράφησης κατά την Μεταφορά των Δεδομένων είναι ιδιαίτερα διαδεδομένη στα τοπικά δίκτυα παρόλο που μπορούμε εύκολα να υποθέσουμε ότι ένα τοπικό δίκτυο δεν μπορεί να είναι ευρέως ορατό, όμως στην περίπτωση του ασύρματου τοπικού δικτύου, η ελλιπής διαμόρφωσή του, μπορεί να το κάνει ορατό στον οποιοδήποτε είναι στο εύρος του. Πολλά ζητήματα που αφορούν την κρυπτογράφηση κατά την μεταφορά των δεδομένων είναι εύκολο να έρθουν στην επιφάνεια αρκεί να παρακολουθήσει κάποιος την κίνηση στο δίκτυο και να ψάξει για δεδομένα που είναι αναγνώσιμα. Επίσης, υπάρχουν αυτοματοποιημένα εργαλεία τα οποία αναζητούν για την σωστή υλοποίηση των γνωστών transport encryption (common transport encryption) όπως είναι το πρωτόκολλο SSL και το TLS. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η απώλεια των δεδομένων. Ανάλογα τα δεδομένα τα οποία έχουν εκτεθεί, υπάρχει η πιθανότητα να οδηγηθούμε σε πλήρη έκθεση των συσκευών ή των λογαριασμών των χρηστών. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρηση τους, σε περίπτωση που τα δεδομένα τους εκτεθούν ενώ «ταξιδεύουν» σε διάφορα δίκτυα. Θα πρέπει λοιπόν να αναρωτηθούν εάν θιγούν οι πελάτες τους, σε περίπτωση που τα δεδομένα τους κλαπούν ή τροποποιηθούν. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν υπάρχει έλλειψη κρυπτογράφησης κατά την μεταφορά των δεδομένων ή όχι είναι οι εξής:

i. Να διερευνηθεί η κίνηση των συσκευών στο δίκτυο, οι εφαρμογές για κινητές συσκευές τους και οποιαδήποτε cloud σύνδεση, ώστε να διασφαλιστεί ότι καμία πληροφορία δεν διακινείται σε μορφή απλού κειμένου.

ii. Να διερευνηθεί εάν τα πρωτόκολλα SSL ή TSL είναι ενημερωμένα και σωστά υλοποιημένα.

iii. Να διερευνηθεί εάν η χρήση των συγκεκριμένων πρωτοκόλλων κρυπτογράφησης συστήνεται και είναι αποδεκτή.

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι θα γίνει η καλύτερη δυνατή προσπάθεια για να διασφαλιστεί η κρυπτογράφηση κατά την μεταφορά των δεδομένων απαιτείται:

i. Τα δεδομένα κατά την μετακίνησή τους στο δίκτυο, να έχουν κρυπτογραφηθεί χρησιμοποιώντας πρωτόκολλα όπως το SSL και το TLS.

ii. Σε περίπτωση που δεν χρησιμοποιούνται τα πρωτόκολλα SSL ή TLS, να χρησιμοποιείται κάποια άλλη τεχνική κρυπτογράφησης, για να προστατευτούν τα δεδομένα κατά την κίνησή τους στο δίκτυο.

iii. Να χρησιμοποιούνται μόνο κοινώς αποδεκτοί μηχανισμοί κρυπτογράφησης και να αποφεύγονται τα ιδιόκτητα πρωτόκολλα κρυπτογράφησης.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι σε θέση να δει καθαρά τα ευαίσθητα δεδομένα, αφού διακινούνται χωρίς κρυπτογράφηση κατά την μεταφορά τους:

Σενάριο 1ο: η διεπαφή cloud χρησιμοποιεί μόνο HTTP:

http://www.somecloudsite.com

Σενάριο 2ο: το όνομα χρήστη και ο κωδικός του χρήστη, μεταδίδονται σε μορφή απλού κειμένου, μέσω του δικτύου:

http://www.somecloud.com/login.php?userid=3&password=1234

- **Privacy Concerns (Προστασία Προσωπικών Δεδομένων).**
  Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα εξής για να έχουν πρόσβαση με *σχετικά εύκολο* τρόπο σε προσωπικά δεδομένα που δεν είναι σωστά προστατευμένα ή έχουν συλλεχθεί χωρίς πραγματικά να χρειάζονται: τον ανεπαρκή έλεγχο ταυτοποίησης, την έλλειψη κρυπτογράφησης κατά την μεταφορά των δεδομένων και τις μη ασφαλείς υπηρεσίες δικτύου. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση, δύναται να είναι εσωτερικοί ή εξωτερικοί χρήστες, οι οποίοι έχουν πρόσβαση, σε μια συσκευή μεμονωμένα ή στο δίκτυο στο οποίο αυτή είναι συνδεδεμένη, σε μια εφαρμογή για κινητή συσκευή (mobile application), σε μια cloud σύνδεση (cloud connection). Όσον αφορά την Προστασία Προσωπικών Δεδομένων (Privacy Concerns), είναι κάτι το οποίο είναι *κοινώς διαδεδομένο* και *εύκολα ανιχνεύσιμο*. Κάτι τέτοιο προκύπτει από την συλλογή προσωπικών δεδομένων και επιπλέον από την έλλειψη της σωστής τους προστασίας. Είναι εύκολο να ανιχνευτεί απλά επανεξετάζοντας τα δεδομένα τα οποία συλλέγονται κατά την διάρκεια της ενεργοποίησης μίας συσκευής από τον χρήστη. Επίσης, υπάρχουν αυτοματοποιημένα εργαλεία, τα οποία έχουν την ικανότητα να αναζητούν συγκεκριμένα πρότυπα των δεδομένων που μπορούν να υποδηλώσουν ενδεχόμενη συλλογή προσωπικών δεδομένων ή άλλων ευαίσθητων δεδομένων. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η δημοσίευση ή απώλεια των προσωπικών δεδομένων των χρηστών. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρησή τους, σε περίπτωση που τα προσωπικά δεδομένα των χρηστών τους, τα οποία δεν είναι καν απαραίτητο να έχουν στην κατοχή τους ή δεν έχουν προστατευθεί σωστά, κλαπούν. Θα πρέπει λοιπόν να αναρωτηθούν, εάν θιγούν οι πελάτες τους σε μία αντίστοιχη περίπτωση. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν υπάρχει λόγος ανησυχίας για έκθεση των προσωπικών δεδομένων ή όχι είναι οι εξής:

  i. Προσδιορισμός όλων των τύπων δεδομένων τα οποία συλλέγονται από την συσκευή, την εφαρμογή για κινητή συσκευή και οποιοδήποτε cloud διεπαφή.

  ii. Μια συσκευή και τα επιμέρους στοιχεία της, πρέπει να συλλέγει μόνο τα δεδομένα που πραγματικά της χρειάζονται.

  iii. Αν οι προσωπικές αναγνωρίσιμες πληροφορίες μπορούν να εκτεθούν κατά την διάρκεια της αποθήκευσής τους ή της διακίνησής τους μέσω του δικτύου, όταν δεν είναι σωστά κρυπτογραφημένες.

  iv. Αν είναι σαφές ποιος έχει πρόσβαση στις προσωπικές πληροφορίες οι οποίες έχουν συλλεχθεί.

  v. Να καθοριστεί εάν τα δεδομένα που έχουν συλλεχθεί δύναται να γίνουν αποχαρακτηρισμένα ή ανώνυμα.

vi. Να καθοριστεί εάν τα δεδομένα τα οποία συλλέγονται είναι αυτά που πραγματικά είναι απαραίτητα για την συγκεκριμένη λειτουργία της συσκευής και αν ο τελικός χρήστης έχει την επιλογή γι' αυτή την συλλογή δεδομένων.

vii. Να προσδιοριστεί εάν έχει οριστεί πολιτική διατήρησης των δεδομένων.

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι θα γίνει η καλύτερη δυνατή προσπάθεια για να διατηρηθούν τα προσωπικά δεδομένα, άθικτα από τον επιτιθέμενο απαιτείται:

i. Να συλλέγονται μόνο τα απαραίτητα δεδομένα τα οποία είναι χρήσιμα για την λειτουργικότητα μιας συσκευής.

ii. Τα δεδομένα τα οποία συλλέγονται να είναι όσο το δυνατό λιγότερο ευαίσθητα.

iii. Τα δεδομένα που συλλέγονται να είναι αποχαρακτηρισμένα ή ανώνυμα.

iv. Τα δεδομένα που συλλέγονται να είναι σωστά προστατευμένα με κρυπτογράφηση.

v. Η κάθε συσκευή και όλα τα επιμέρους στοιχεία της, να προστατεύουν σωστά τις προσωπικές πληροφορίες.

vi. Μόνο εξουσιοδοτημένα άτομα να είναι σε θέση να έχουν πρόσβαση σε προσωπικές πληροφορίες που έχουν συλλεχθεί.

vii. Να τηρούνται τα όρια διατήρησης των δεδομένων που έχουν συλλεχθεί.

viii. Οι τελικοί χρήστες να έχουν την επιλογή να διαθέσουν τα δεδομένα τους, όταν αυτά είναι επιπρόσθετα από τα απαιτούμενα του προϊόντος.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι σε θέση να οδηγηθεί σε κλοπή της ταυτότητας ή του λογαριασμού ενός χρήστη:

Σενάριο 1^{ο}: Συλλογή προσωπικών δεδομένων:

Ημερομηνία γεννήσεως, διεύθυνση οικίας, αριθμός τηλεφώνου, κ.α.

Σενάριο 2^{ο}: Συλλογή οικονομικών πληροφοριών ή ακόμα κ πληροφοριών υγείας:

Δεδομένα πιστωτικών/χρεωστικών καρτών και τραπεζικών λογαριασμών, ιατρικό ιστορικό, κ.α.

- **Insecure Cloud Interface (Μη Ασφαλής Cloud Διεπαφή).**
  Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα εξής για να αποκτήσουν πρόσβαση *σχετικά εύκολα* σε δεδομένα πρόσβασης ή στις πολιτικές διακυβέρνησης των δεδομένων μέσω των cloud ιστοσελίδων (cloud websites): τον ανεπαρκή έλεγχο ταυτοποίησης, την έλλειψη κρυπτογράφησης κατά την μεταφορά των δεδομένων και την μη απαρίθμηση των λογαριασμών. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση δύναται να είναι όσοι έχουν πρόσβαση στο Διαδίκτυο. Η Μη Ασφαλής Cloud Διεπαφή (Insecure Cloud Interface), είναι μια αδυναμία ασφαλείας η οποία είναι *κοινώς διαδεδομένη* και *εύκολα ανιχνεύσιμη*. Κάτι τέτοιο συμβαίνει όταν κάποιος μπορεί εύκολα να μαντέψει τα διαπιστευτήρια που χρησιμοποιούνται ή να απαριθμήσει λογαριασμούς. Ένα τέτοιο πρόβλημα ασφαλείας μπορεί εύκολα να ανιχνευτεί εάν διαπιστωθεί η χρήση ή μη του πρωτοκόλλου SSL κατά την σύνδεση με την cloud διεπαφή. Μπορεί επίσης να χρησιμοποιηθεί μηχανισμός ανάκτησης κωδικού πρόσβασης για να βρεθούν έγκυροι λογαριασμοί για να διαπιστωθεί εάν κάτι τέτοιο είναι ικανό να οδηγήσει σε απαρίθμηση λογαριασμών. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η έκθεση των δεδομένων των χρηστών και η απόκτηση του πλήρους ελέγχου της συσκευής. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρησή τους, σε περίπτωση που τα προσωπικά δεδομένα των χρηστών τους κλαπούν ή ανακτήσουν τον έλεγχο των συσκευών τους οι επιτιθέμενοι. Θα πρέπει λοιπόν να αναρωτηθούν εάν θιγούν οι πελάτες τους ή το όνομα της εταιρίας τους σε μία ανάλογη περίπτωση. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν οι cloud διεπαφές είναι ασφαλείς ή όχι είναι οι εξής:

  i. Να διαπιστωθεί εάν το προεπιλεγμένο όνομα χρήστη και κωδικός πρόσβασης μπορούν να αλλαχθούν κατά την διάρκεια της αρχικής εγκατάστασης ενός προϊόντος.

  ii. Να διαπιστωθεί εάν ένας συγκεκριμένος λογαριασμός χρήστη κλειδώνεται μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.
  iii. Να διαπιστωθεί εάν οι έγκυροι λογαριασμοί χρηστών μπορούν να εντοπιστούν χρησιμοποιώντας μηχανισμούς ανάκτησης κωδικών πρόσβασης ή σελίδες νέων χρηστών.
  iv. Να επανεξεταστεί η διεπαφή για ζητήματα ασφαλείας, όπως Cross-Site Scripting, Cross-Site Request Forgery και SQL Injection.
  v. Να επανεξεταστούν όλες οι cloud διεπαφές για ευπάθειες (API Interfaces & Cloud-Based Web Interfaces).

  Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι οι cloud διεπαφές θα είναι ασφαλείς απαιτείται:

  i. Οι προεπιλεγμένοι κωδικοί πρόσβασης και ιδανικά τα ονόματα των χρηστών, να αλλάζουν κατά την αρχική εγκατάσταση.

  ii. Να διασφαλιστεί ότι οι λογαριασμοί των χρηστών δεν θα μπορούν να απαριθμηθούν χρησιμοποιώντας μεθόδους όπως είναι οι μηχανισμοί επαναφοράς κωδικών πρόσβασης.

iii. Να κλειδώνεται ο λογαριασμός ενός χρήστη, μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.

iv. Να διασφαλιστεί ότι οι cloud διεπαφές δεν είναι ευπαθείς σε επιθέσεις τύπου Cross-Site Scripting, SQL Injection ή Cross-Site Request Forgery.

v. Να διασφαλιστεί ότι τα διαπιστευτήρια δεν είναι εκτεθειμένα στο διαδίκτυο.

vi. Να εφαρμόζεται ταυτοποίηση σε δύο διαφορετικά στοιχεία (2FA - Two Factor Authentication) εάν είναι δυνατό.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι σε θέση να διαπιστώσει πότε ένας λογαριασμός χρήστη είναι έγκυρος ή να καταγράψει τα διαπιστευτήρια κατά την διακίνηση τους στο διαδίκτυο, δεδομένου ότι τα συγκεκριμένα προστατεύονται μόνο με κωδικοποίηση Base64:

Σενάριο 1ο: ο μηχανισμός ανάκτησης του κωδικού πρόσβασης καταδεικνύει εάν ένας λογαριασμός είναι έγκυρος:

Password Reset: "This account does not exist."

Σενάριο 2ο: το όνομα χρήστη και ο κωδικός πρόσβασης, είναι ανεπαρκώς προστατευμένα κατά την διακίνηση τους στο διαδίκτυο:

Authorisation: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3

- **Insecure Mobile Interface (Μη Ασφαλής Διεπαφή Κινητής Συσκευής).**

Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα εξής για να αποκτήσουν πρόσβαση *σχετικά εύκολα* σε δεδομένα πρόσβασης ή στις πολιτικές διακυβέρνησης των δεδομένων μέσω των διεπαφών για κινητές συσκευές: τον ανεπαρκή έλεγχο ταυτοποίησης, την έλλειψη κρυπτογράφησης κατά την μεταφορά των δεδομένων, την μη απαρίθμηση των λογαριασμών. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση δύναται να είναι όσοι έχουν πρόσβαση σε εφαρμογές για κινητές συσκευές. Η Μη Ασφαλής Διεπαφή Κινητής Συσκευής (Insecure Mobile Interface), είναι μια αδυναμία ασφαλείας η οποία είναι *κοινώς διαδεδομένη* και *εύκολα ανιχνεύσιμη*. Κάτι τέτοιο συμβαίνει όταν κάποιος μπορεί εύκολα να μαντέψει τα διαπιστευτήρια που χρησιμοποιούνται ή να απαριθμήσει τους λογαριασμούς. Ένα τέτοιο πρόβλημα ασφαλείας μπορεί εύκολα να ανιχνευτεί εάν διαπιστωθεί η χρήση ή μη του πρωτοκόλλου SSL κατά την σύνδεση με την ασύρματη σύνδεση δικτύου. Μπορεί επίσης να χρησιμοποιηθεί μηχανισμός ανάκτησης κωδικού πρόσβασης για να βρεθούν έγκυροι λογαριασμοί και, εάν διαπιστωθεί κάτι τέτοιο, είναι ικανό να οδηγήσει σε απαρίθμηση λογαριασμών. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η έκθεση των δεδομένων των χρηστών και η απόκτηση του πλήρους ελέγχου της συσκευής. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρησή τους, σε περίπτωση που τα προσωπικά δεδομένα των χρηστών τους κλαπούν ή ανακτήσουν τον έλεγχο των συσκευών τους οι επιτιθέμενοι. Θα πρέπει λοιπόν να αναρωτηθούν εάν θιγούν οι πελάτες τους ή το όνομα της εταιρίας τους σε μία ανάλογη περίπτωση.

Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν οι διεπαφές για μία κινητή συσκευή είναι ασφαλείς ή όχι είναι οι εξής:

i. Να διαπιστωθεί εάν το προεπιλεγμένο όνομα χρήστη και κωδικός πρόσβασης μπορούν να αλλαχθούν κατά την διάρκεια της αρχικής εγκατάστασης ενός προϊόντος.

ii. Να διαπιστωθεί εάν ένας συγκεκριμένος λογαριασμός χρήστη κλειδώνεται μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.

iii. Να διαπιστωθεί εάν οι έγκυροι λογαριασμοί χρήστη μπορούν να εντοπιστούν χρησιμοποιώντας μηχανισμούς ανάκτησης κωδικών πρόσβασης ή σελίδες νέων χρηστών.

iv. Να επανεξεταστεί εάν τα διαπιστευτήρια του χρήστη είναι εκτεθειμένα κατά την ασύρματη σύνδεση του με το δίκτυο.

v. Να επανεξεταστεί εάν είναι διαθέσιμη η ταυτοποίηση σε δύο διαφορετικά στοιχεία (2FA - Two Factor Authentication).

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι οι διεπαφές για κινητές συσκευές θα είναι ασφαλείς απαιτείται:

i. Οι προεπιλεγμένοι κωδικοί πρόσβασης και ιδανικά τα ονόματα των χρηστών, να αλλάζουν κατά την αρχική εγκατάσταση μιας εφαρμογής.

ii. Να διασφαλιστεί ότι οι λογαριασμοί των χρηστών δεν θα μπορούν να απαριθμηθούν χρησιμοποιώντας μεθόδους όπως είναι οι μηχανισμοί επαναφοράς κωδικών πρόσβασης.

iii. Να κλειδώνεται ο λογαριασμός ενός χρήστη, μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.

iv. Να διασφαλιστεί ότι τα διαπιστευτήρια του χρήστη δεν είναι εκτεθειμένα κατά την ασύρματη σύνδεση του στο δίκτυο.

v. Να εφαρμόζεται ταυτοποίηση σε δύο διαφορετικά στοιχεία (2FA - Two Factor Authentication) εάν είναι δυνατό.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι σε θέση να διαπιστώσει πότε ένας λογαριασμός χρήστη είναι έγκυρος ή να καταγράψει τα διαπιστευτήρια κατά την διακίνηση τους στο διαδίκτυο, δεδομένου ότι τα συγκεκριμένα προστατεύονται μόνο με κωδικοποίηση Base64:

Σενάριο 1ο: ο μηχανισμός ανάκτησης του κωδικού πρόσβασης καταδεικνύει εάν ένας λογαριασμός είναι έγκυρος:

Password Reset: "This account does not exist."

Σενάριο 2ο: το όνομα χρήστη και ο κωδικός πρόσβασης, είναι ανεπαρκώς προστατευμένα κατά την διακίνηση τους στο διαδίκτυο:

Authorisation: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3

- **Insufficient Security Configurability (Ανεπαρκής Ικανότητα Παραμετροποίησης Ασφάλειας)**

Στην συγκεκριμένη περίπτωση αδυναμίας, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα εξής για να αποκτήσουν πρόσβαση *σχετικά εύκολα* σε δεδομένα πρόσβασης ή στις πολιτικές διακυβέρνησης των δεδομένων της συσκευής καθώς και να εκθέσουν σε κίνδυνο την ίδια την συσκευή: την έλλειψη κλιμακωτών δικαιωμάτων (granular permissions) στην πρόσβαση των δεδομένων ή των controls της συσκευής, την έλλειψη κρυπτογράφησης, δεν υπάρχει δυνατότητα επιλογής κωδικού πρόσβασης (password options). Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση είτε εκούσια ή ακούσια, δύναται να είναι όσοι έχουν πρόσβαση σε μία συσκευή. Η Ανεπαρκής Ικανότητα Παραμετροποίησης Ασφάλειας (Insufficient Security Configurability), είναι μια αδυναμία ασφαλείας η οποία είναι *κοινώς διαδεδομένη* και *εύκολα ανιχνεύσιμη*. Κάτι τέτοιο μπορεί να συμβεί όταν οι χρήστες των συσκευών έχουν περιορισμένη ή καθόλου ικανότητα να μεταβάλλουν τους ελέγχους ασφαλείας. Επίσης, η συγκεκριμένα ευπάθεια μπορεί να εμφανιστεί όταν η διεπαφή ιστότοπου δεν έχει επιλογές για την δημιουργία κλιμακωτών δικαιωμάτων ή για παράδειγμα, όταν αναγκάζει τον χρήστη να χρησιμοποιήσει κάποιο δυνατό κωδικό πρόσβασης. Αυτές οι ελλείψεις μπορούν να εντοπιστούν με έναν χειροκίνητο έλεγχο της διεπαφή ιστότοπου και των διαθέσιμων επιλογών του. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *μέτριες*, αφού είναι πιθανή η εκούσια ή ακούσια απώλεια δεδομένων καθώς και η έκθεση της συσκευής. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρηση τους, σε περίπτωση που: τα δεδομένα των χρηστών τους κλαπούν ή τροποποιηθούν και ανακτήσουν τον έλεγχο των συσκευών τους οι επιτιθέμενοι. Θα πρέπει λοιπόν να αναρωτηθούν εάν θιγούν οι πελάτες τους σε μία ανάλογη περίπτωση. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν η παραμετροποίηση των παραμέτρων ασφάλειας είναι ανεπαρκής ή όχι είναι οι ακόλουθοι σχετικά με το αν:

i. Η διεπαφή του διαχειριστή της συσκευής αναγκάζει τον χρήστη να δημιουργήσει ισχυρό κωδικό πρόσβασης.

ii. Η διεπαφή του διαχειριστή έχει την ικανότητα να διαχωρίζει τους χρήστες που είναι διαχειριστές (admin users) από τους απλούς.

iii. Η διεπαφή του διαχειριστή έχει επιλογές κρυπτογράφησης.

iv. Η διεπαφή του διαχειριστή διαθέτει επιλογές για ασφαλή καταγραφή των διαφόρων συμβάντων ασφαλείας.

v. Η διεπαφή του διαχειριστή διαθέτει επιλογές για να ενεργοποιηθούν ειδοποιήσεις και κοινοποιήσεις προς τον τελικό χρήστη, που να αφορά συμβάντα ασφαλείας.

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι η παραμετροποίηση των παραμέτρων ασφαλείας είναι επαρκής πρέπει να εξασφαλιστεί ότι θα υπάρχει η δυνατότητα για:

i. Τον διαχωρισμό των απλών χρηστών με τους χρήστες που είναι διαχειριστές.

ii. Κρυπτογράφηση των δεδομένων είτε αυτά διακινούνται στο δίκτυο ή όχι.

iii. Ύπαρξη πολιτικών ασφαλείας που αναγκάζουν τον χρήστη να δημιουργεί ισχυρό κωδικό πρόσβασης.

iv. Καταγραφή των διαφόρων συμβάντων ασφαλείας.

v. Ενημέρωση των τελικών χρηστών για τα συμβάντα ασφαλείας.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι σε θέση να εκμεταλλευτεί την έλλειψη ισχυρών κωδικών πρόσβασης για να αποκτήσουν πρόσβαση σε λογαριασμούς χρηστών, καθώς και την έλλειψη κρυπτογράφησης των δεδομένων που δεν διακινούνται στο δίκτυο, αλλά είναι αποθηκευμένα στην συσκευή (data at rest):

Σενάριο 1ο: Απουσία πολιτικής ασφαλείας όπου αναγκάζει τον χρήστη να δημιουργεί ισχυρούς κωδικούς πρόσβασης:

Οι χρήστες και οι διαχειριστές δεν υποχρεώνονται να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης.

Σενάριο 2ο: Απουσία δυνατότητας να κρυπτογραφηθούν τα δεδομένα τα οποία είναι αποθηκευμένα στην συσκευή και δεν διακινούνται:

Είναι πιθανό τα ευαίσθητα δεδομένα ή οι κωδικοί πρόσβασης που είναι αποθηκευμένοι στη συσκευή, να μην είναι κρυπτογραφημένοι.

- **Insecure Software/Firmware (Μη Ασφαλές Λογισμικό/Λογισμικό Υλικού).**

Στην συγκεκριμένη περίπτωση αδυναμίας, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί *δύσκολα* τα εξής: να υποκλέψει ένα αρχείο ενημέρωσης το οποίο δεν είναι κρυπτογραφημένο μέσω μιας μη ασφαλούς σύνδεσης και να εκτελέσει τις δικές του κακόβουλες ενημερώσεις με την μέθοδο του DNS hijacking. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση, δύναται να είναι όσοι έχουν πρόσβαση σε μία συσκευή ή στο δίκτυο στο οποίο βρίσκεται η συσκευή, μέσω του τοπικού δικτύου ή του Διαδικτύου. Το Μη Ασφαλές Λογισμικό/Λογισμικό Υλικού (Insecure Software/Firmware), είναι μια αδυναμία ασφαλείας η οποία είναι *κοινώς διαδεδομένη* και *εύκολα ανιχνεύσιμη*. Κάτι τέτοιο μπορεί να συμβεί όταν τα αρχεία ενημέρωσης και η σύνδεση δικτύου η οποία χρησιμοποιείται για την διακίνηση τους δεν είναι προστατευμένη. Το λογισμικό/λογισμικό υλικού μπορεί να χαρακτηρισθεί σαν μη ασφαλές, όταν περιέχει ενσωματωμένα ευαίσθητα δεδομένα όπως είναι τα διαπιστευτήρια. Τέτοιου είδους θέματα είναι σχετικά εύκολα να ανιχνευτούν ελέγχοντας απλά την κίνηση του δικτύου κατά την διάρκεια των ενημερώσεων, για την ύπαρξη κρυπτογράφησης. Ένας άλλος τρόπος είναι η χρήση ενός δεκαεξαδικού προγράμματος επεξεργασίας για να διαπιστωθεί εάν το αρχείο ενημέρωσης περιέχει κατάλληλες πληροφορίες.

Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η έκθεση των δεδομένων των χρηστών και η έκθεση του ελέγχου της συσκευής. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρηση τους, σε περίπτωση που: τα δεδομένα των χρηστών τους κλαπούν ή τροποποιηθούν, ανακτήσουν τον έλεγχο των συσκευών τους οι επιτιθέμενοι και έχουν σκοπό να επιτεθούν σε άλλες συσκευές. Θα πρέπει λοιπόν να αναρωτηθούν εάν θιγούν οι πελάτες τους ή άλλοι χρήστες σε μία ανάλογη περίπτωση. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν το λογισμικό/λογισμικό υλικού είναι ασφαλές ή όχι, αφότου έχει εξασφαλιστεί ότι η συσκευή θα είναι σε θέση να εκτελέσει τις ενημερώσεις κανονικά, είναι οι εξής:

i. Μπορεί ένας άνθρωπος χρησιμοποιώντας δεκαεξαδικό πρόγραμμα επεξεργασίας να αναγνώσει ευαίσθητες πληροφορίες από ένα αρχείο ενημέρωσης;
ii. Μπορεί να διαπιστωθεί μέσω αποδεκτών αλγορίθμων, ότι ένα παραγωγικό αρχείο ενημέρωσης έχει κρυπτογραφηθεί ορθά;
iii. Έχει υπογραφεί ορθά το παραγωγικό αρχείο ενημέρωσης;
iv. Οι μέθοδοι επικοινωνίας που χρησιμοποιούνται για την μετάδοση της ενημέρωσης είναι αυτές που πραγματικά πρέπει;
v. Είναι ενημερωμένες και σωστά ρυθμισμένες, οι μέθοδοι μεταφοράς κρυπτογράφησης, στον εξυπηρετητή cloud (cloud server) ενημέρωσης ο οποίος δεν είναι ευπαθής;
vi. Είναι επικυρωμένα τα υπογεγραμμένα αρχεία ενημέρωσης της συσκευής;

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι το λογισμικό και το firmware θα είναι ασφαλές, πρέπει να εξασφαλιστεί ότι θα υπάρχει η δυνατότητα:

i. Η συσκευή να ενημερώνεται.
ii. Το αρχείο ενημέρωσης να είναι κρυπτογραφημένο χρησιμοποιώντας αποδεκτές μεθόδους κρυπτογράφησης.
iii. Το αρχείο ενημέρωσης να μεταδίδεται μέσω κρυπτογραφημένης σύνδεσης.
iv. Το αρχείο ενημέρωσης να μην εκθέτει ευαίσθητα δεδομένα.
v. Να επιβεβαιωθεί ότι η ενημέρωση είναι υπογεγραμμένη και επικυρωμένη πριν φορτωθεί και εφαρμοστεί.
vi. Ο εξυπηρετητής που εκτελεί τις ενημερώσεις (update server) να είναι ασφαλής.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι σε θέση είτε να συλλάβει το αρχείο ενημέρωσης και ενδεχομένως να αναγνώσει και τα περιεχόμενα του:

Σενάριο 1^{ο}: Το αρχείο ενημέρωσης μεταδίδεται μέσω HTTP:

http://www.abc.com/update.bin

Σενάριο 2ο: Το αρχείο ενημέρωσης δεν είναι κρυπτογραφημένο και τα δεδομένα είναι αναγνώσιμα από τον άνθρωπο:

admin.htm advanced.htm alarms.htm

- **Poor Physical Security (Ελλιπής Φυσική Ασφάλεια).**

Στην συγκεκριμένη περίπτωση αδυναμίας, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί την πρόσβασή του σε μια θύρα USB, σε μια SD κάρτα ή σε οποιοδήποτε άλλο μέσο αποθήκευσης για να αποκτήσει πρόσβαση στο λειτουργικό σύστημα και στα δεδομένα που είναι αποθηκευμένα στην συσκευή *σχετικά εύκολα*. Αυτοί που θα μπορούσαν να πραγματοποιήσουν μία τέτοιου είδους επίθεση, δύναται να είναι όσοι έχουν φυσική πρόσβαση σε μία συσκευή. Η Ελλιπής Φυσική Ασφάλεια (Poor Physical Security), είναι μια αδυναμία ασφαλείας η οποία είναι *κοινώς διαδεδομένη* και *σχετικά εύκολα ανιχνεύσιμη*. Κάτι τέτοιο μπορεί να συμβεί όταν ένας επιτιθέμενος μπορεί εύκολα να αποκτήσει πρόσβαση στο μέσο αποθήκευσης της συσκευής και κατ' επέκταση στα δεδομένα που είναι αποθηκευμένα σ' αυτή, αποσυναρμολογώντας την συσκευή. Επίσης, οι USB θύρες ή άλλες εξωτερικές θύρες είναι σε θέση να χρησιμοποιηθούν για πρόσβαση στην συσκευή, χρησιμοποιώντας χαρακτηριστικά τα οποία προορίζονται για παραμετροποίηση ή συντήρηση. Οι τεχνικές επιπτώσεις που δύναται να προκληθούν από μία τέτοιου είδους έλλειψη προστασίας, είναι *σοβαρές*, αφού είναι πιθανή η έκθεση της συσκευής και των δεδομένων που είναι αποθηκευμένα σ' αυτή. Από την πλευρά των επιχειρήσεων, πρέπει να εξετάσουν την επιρροή που θα έχουν στην επιχείρησή τους, σε περίπτωση που οι επιτιθέμενοι καταφέρουν να: κλέψουν ή τροποποιήσουν τα δεδομένα των χρηστών και ανακτήσουν τον έλεγχο των συσκευών τους. Θα πρέπει, λοιπόν, να αναρωτηθούν εάν οι πελάτες τους ή η επωνυμίας τους θιγούν σε μία ανάλογη περίπτωση. Οι έλεγχοι που οφείλεται να γίνονται για να διαπιστωθεί εάν υπάρχει ελλιπής φυσική ασφάλεια ή όχι, είναι οι εξής:

i. Είναι εφικτό να αποσυναρμολογήσει κάποιος την συσκευή και να αποκτήσει πρόσβαση ή ακόμα και να αφαιρέσει τα μέσα αποθήκευσης της;

ii. Είναι εφικτό κάποιος με την χρήση της USB θύρας να αποκτήσει πρόσβαση στα δεδομένα της συσκευής, χωρίς να την αποσυναρμολογήσει;

iii. Είναι απαραίτητες όλες οι εξωτερικές θύρες;

iv. Μπορούν να απενεργοποιηθούν οι εξωτερικές θύρες, όπως οι USB, μέσω της διεπαφής του διαχειριστή;

v. Έχει ελεγχθεί η διεπαφή του διαχειριστή ώστε να διαπιστωθεί ότι οι αρμοδιότητες του είναι περιορισμένες μόνο τοπικά;

Έτσι, σύμφωνα με τα προηγούμενα για να εξασφαλιστεί ότι δεν θα είναι ελλιπής η φυσική ασφάλεια, πρέπει να εξασφαλιστεί ότι θα υπάρχει η δυνατότητα:

i. Να μην μπορούν να αφαιρεθούν εύκολα τα μέσα αποθήκευσης ή να απαιτούνται ειδικά εργαλεία του κατάλληλου προσωπικού για τον σκοπό αυτό.

ii. Τα δεδομένα που είναι αποθηκευμένα και δεν διακινούνται, να είναι κρυπτογραφημένα.

iii. Οι USB ή άλλες εξωτερικές θύρες, να μην μπορούν να χρησιμοποιηθούν για κακόβουλη πρόσβαση στη συσκευή.

iv. Να μην μπορεί να αποσυναρμολογηθεί εύκολα η συσκευή.

v. Να υπάρχουν μόνο οι απαραίτητες εξωτερικές θύρες, όπως οι USB, για την λειτουργία του προϊόντος.

vi. Το προϊόν να έχει την δυνατότητα να περιορίσει τις δυνατότητες του διαχειριστή.

Παραδείγματα σεναρίων επιθέσεων στα οποία ο επιτιθέμενος είναι σε θέση να αποκτήσει πρόσβαση στο λογισμικό της συσκευής και να τροποποιήσει ή απλά να αντιγράψει συγκεκριμένα δεδομένα:

Σενάριο 1ο: Η συσκευή μπορεί να αποσυναρμολογηθεί εύκολα και το μέσο αποθήκευσης της είναι μια μη κρυπτογραφημένη κάρτα SD:

Η κάρτα αποθήκευσης SD μπορεί να αφαιρεθεί και να εισαχθεί σε έναν αναγνώστη καρτών μνήμης, ώστε τα δεδομένα της να τροποποιηθούν ή/και να αντιγραφούν.

Σενάριο 2ο: Η ύπαρξη των USB θυρών στην συσκευή:

Θα μπορούσαν να γραφούν ειδικά προγράμματα που εκμεταλλεύονται δυνατότητες όπως η ενημέρωση μέσω θύρας USB, ώστε να τροποποιηθεί το αρχικό λογισμικό της συσκευής.

Κεφάλαιο 4ο: Εκτέλεση Επιθέσεων και Αντιμετώπιση.

Στο κεφάλαιο αυτό θα γίνει πειραματική μελέτη του βαθμού τρωτότητας ενός στοιχειώδους περιβάλλοντος IoT που θα συναντούσαμε σε ένα έξυπνο σπίτι/έξυπνη βιομηχανία, απέναντι σε κοινές επιθέσεις. Στο τέλος του κεφαλαίου θα γίνει αναφορά και στην έννοια "Dorking". Το πρωτόκολλο επικοινωνίας που θα χρησιμοποιηθεί είναι η σουίτα MQTT. Οι επιθέσεις που θα πραγματοποιηθούν είναι δύο:

Επίθεση No. 1: Sniffing Attack (Network Traffic Analysis).

- Η πρώτη επίθεση είναι μία επίθεση sniffing στην οποία θα επιχειρηθεί η υποκλοπή και ανάλυση των πακέτων δεδομένων που μεταφέρονται από και προς έναν εξυπηρετητή MQTT (Broker/Server) σε έναν ή περισσότερους συνδρομητές/«πελάτες» (MQTT Subscribers). Η επίθεση θα γίνει σε δύο σκέλη. Στο πρώτο, ο δίαυλος επικοινωνίας δεν θα είναι κρυπτογραφημένος. Κατόπιν, θα ενεργοποιήσουμε τη δυνατότητα κρυπτογράφησης και θα αναλύσουμε ξανά τα πακέτα. Αξίζει να σημειωθεί πως το πρωτόκολλο MQTT επιτρέπει στις συσκευές του δικτύου να «αλλάξουν» ρόλους, όταν αυτό είναι δυνατόν. Δηλαδή, μία συσκευή όπως είναι π.χ. ένα μοντέρνο κινητό τηλέφωνο μπορεί να είναι ταυτόχρονα και Publisher (Αποστολέας/Εκδότης) αλλά και Subscriber (Συνδρομητής) στο δίκτυο, όπως επίσης ο Broker/Server (Εξυπηρετητής) να είναι συγχρόνως και Publisher (Αποστολέας/Εκδότης). Το υλικό και λογισμικό που χρησιμοποιήθηκαν για το πείραμα είναι τα ακόλουθα:

  - Raspberry Pi Model 4 B (2GB RAM) με εγκατεστημένο λειτουργικό σύστημα Raspbian και τις κατάλληλες βιβλιοθήκες για τη χρήση του πρωτοκόλλου MQTT.
  - Σταθερός Ηλεκτρονικός Υπολογιστής με Windows 10.
  - TP-Link Archer D2 Modem/Router.
  - Το λογισμικό MQTT Explorer του Thomas Nordquist.
  - Ο αναλυτής δικτυακής κίνησης Wireshark.
  - Η διανομή Kali του λειτουργικού συστήματος Linux, εγκατεστημένη ως εικονική μηχανή (Virtual Machine) στο σύστημα VirtualBox της Oracle.

Το πρώτο βήμα στη διαδικασία είναι η συνοπτική επεξήγηση του πρωτοκόλλου MQTT. Το MQTT (Message Queuing Telemetry Transport) είναι ένα ελαφρύ και ελεύθερο πρωτόκολλο μεταφοράς μηνυμάτων βασισμένο σε αρχιτεκτονική έκδοσης/συνδρομής (Publish/Subscribe) μεταξύ πελάτη και εξυπηρετητή (Client/Server). Με σκοπό την διατήρηση του μικρού υπολογιστικού και δικτυακού κόστους το MQTT υλοποιεί τις εξής βασικές ιδέες:

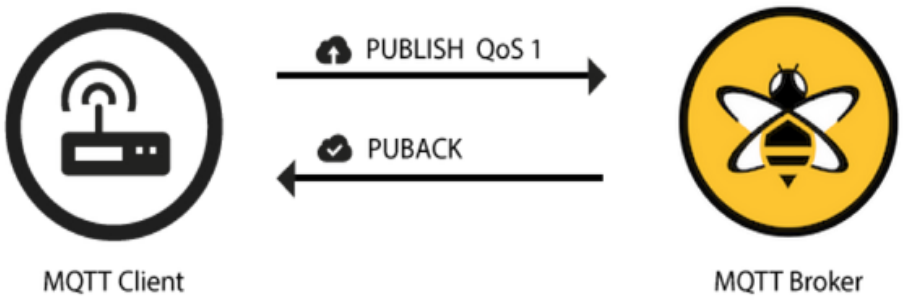
- **Publish/Subscribe**: Το μοντέλο αυτό επιτρέπει στους πελάτες (clients) να λαμβάνουν τα μηνύματα που τους αφορούν και μόνο αυτά, ενώ παράλληλα στέλνουν μηνύματα σε θέματα (topics) που γίνονται διαθέσιμα μόνο στους πελάτες που έχουν κάνει «εγγραφή/συνδρομή» (subscribe) στα θέματα αυτά. Εδώ είναι σημαντικό να αναφέρουμε ότι το μοντέλο αυτό προσφέρει την δυνατότητα επικοινωνίας μεταξύ πελατών χωρίς να γνωρίζει ο ένας την ύπαρξη του άλλου, που είναι βασική απαίτηση ενός επεκτάσιμου (scalable) περιβάλλοντος.
- **Θέματα και συνδρομές (topics/subscriptions)**: Τα θέματα είναι ουσιαστικά ο τρόπος διευθυνσιοδότησης των μηνυμάτων αγνοώντας την ύπαρξη των πελατών. Αποτελούν θεματικές ενότητες στις οποίες κάνουν «εγγραφή/συνδρομή» (subscribe) οι ενδιαφερόμενοι πελάτες και έτσι έχουν πρόσβαση στα μηνύματα που αφορούν αυτές τις θεματικές ενότητες.

- **<u>Επίπεδα ποιότητας υπηρεσιών (Quality of Service – QoS)</u>**: Το MQTT παρέχει 3 επίπεδα QoS για την παράδοση μηνυμάτων. Κάθε επίπεδο προσφέρει μεγαλύτερη αξιοπιστία παράδοσης με μεγαλύτερο κόστος αντίστοιχα:

  - **QoS 0 (Αποστολή το πολύ μία φορά)**. Στο επίπεδο αυτό δεν ελέγχεται η ορθή αποστολή του μηνύματος. Το μήνυμα αποστέλλεται χωρίς να αναμένεται απάντηση ή νέα αποστολή σε περίπτωση σφάλματος. Προφανώς, σε αυτή την περίπτωση έχουμε και την ταχύτερη αποστολή. Χρησιμοποιείται όταν το δίκτυο είναι αξιόπιστο και η πιθανότητα απρόβλεπτης αποσύνδεσης κάποιου/ων πελάτη/ων είναι μικρή.

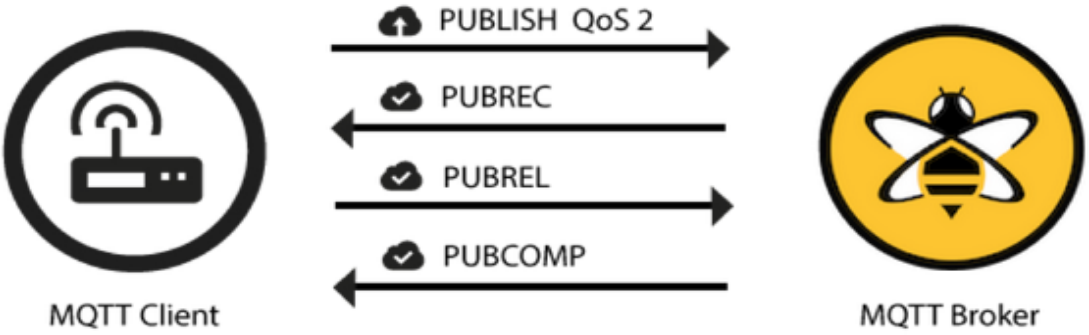
Μετάδοση πακέτου με QoS 0 (Πηγή: hivemq.com)

  - **QoS 1 (Αποστολή τουλάχιστον μία φορά)**. Σε αυτό το επίπεδο ο αποστολέας αναμένει αναγνώριση της αποστολής από τον εξυπηρετητή (Broker) με PUBACK (Publish Acknowledge). Σε περίπτωση που δεν ληφθεί το PUBACK μέσα σε έναν προκαθορισμένο χρόνο, το μήνυμα αποστέλλεται ξανά με τη σημαία (flag) DUP που καταδεικνύει πως είναι αντίγραφο (Duplicate). Όταν ο εξυπηρετητής λάβει το αντίγραφο, το επαναπροωθεί στους σωστούς αποδέκτες και στέλνει στον αποστολέα PUBACK. Όταν υπάρχει πρόβλημα στην αποστολή του PUBACK αλλά όχι του PUBLISH, οι αποδέκτες λαμβάνουν πολλά αντίγραφα του ίδιου μηνύματος. Τέλος, από την πλευρά των πελατών, εφαρμόζονται μέθοδοι αποθήκευσης μηνυμάτων (MQTT Persistence) σε περίπτωση διακοπής της μετάδοσής τους, πριν ληφθεί η αναγνώριση της αποστολής, ώστε να είναι δυνατή η συνέχεια της διαδικασίας αποστολής με την επαναλειτουργία τους.



Μετάδοση πακέτου με QoS 1 (Πηγή: hivemq.com).

- **QoS 2 (Αποστολή μόνο μία φορά)**. Το υψηλότερο επίπεδο του QoS, σε σχέση με το QoS 1, εξασφαλίζει επιπλέον οτι οι αποδέκτες δεν λαμβάνουν αντίγραφα του ίδιου μηνύματος. Για να το επιτύχει αυτό, ο αποστολέας και ο εξυπηρετητής, αποθηκεύουν το μήνυμα μέχρι να ολοκληρωθεί η διαδικασία αποστολής. Αφού ο πελάτης στείλει PUBLISH και αποθηκεύσει το μήνυμα, ο εξυπηρετητής απαντά στον αποστολέα με PUBREC και αποθηκεύει και αυτός το μήνυμα. Ο αποστολέας επιβεβαιώνει την αποστολή με PUBREL, που μόλις ληφθεί από τον εξυπηρετητή αρχίζει τη διαδικασία αποστολής του μηνύματος στους αποδέκτες και απαντά στον αποστολέα με PUBCOMP το οποίο ολοκληρώνει τη διαδικασία και επιτρέπει στον αποστολέα να διαγράψει το αποθηκευμένο μήνυμα. Σε περίπτωση σφάλματος η παραπάνω διαδικασία επαναλαμβάνεται με τη σημαία DUP. Είναι προφανές, πως η διαδικασία αυτή, είναι η πιο αργή από τις τρεις για αυτό χρησιμοποιείται μόνο όταν πρέπει να εξασφαλιστεί πως οι αποδέκτες δεν λαμβάνουν αντίγραφα του ίδιου μηνύματος.



Μετάδοση πακέτου με QoS 2 (Πηγή: hivemq.com).

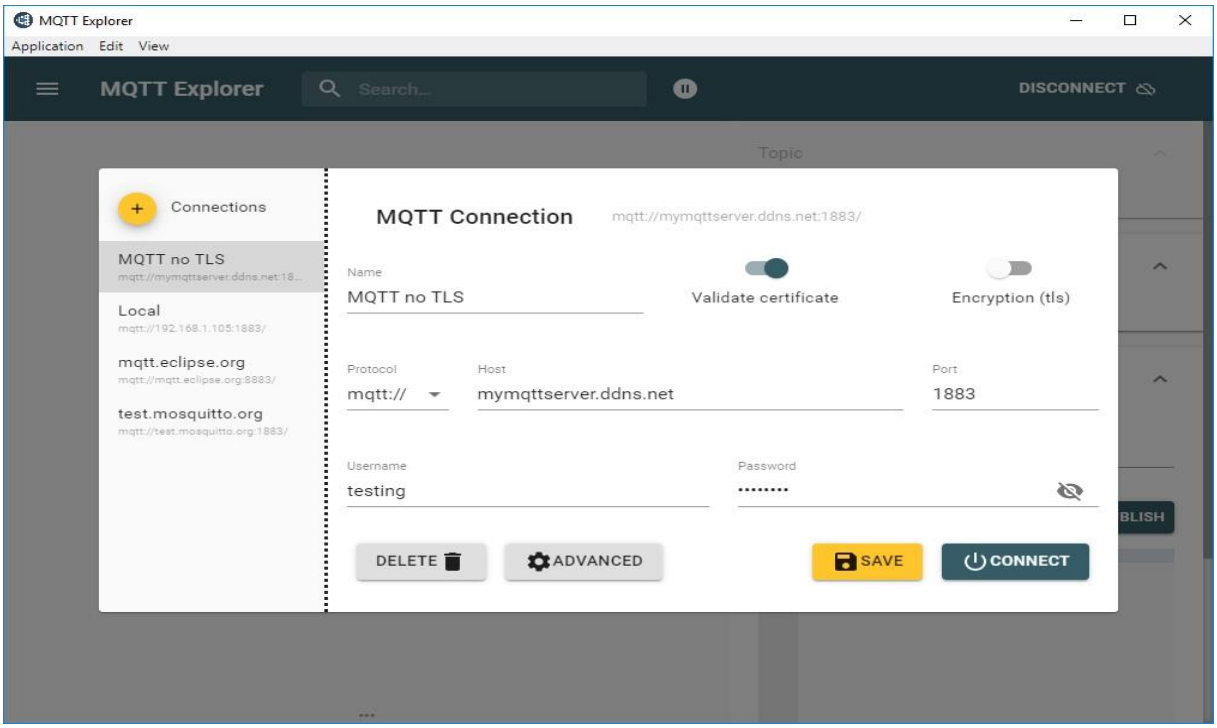
- **<u>Διατήρηση μηνυμάτων και συνδέσεων (retained messages and connections)</u>**: Υπάρχει η δυνατότητα να ληφθούν μηνύματα σε ένα θέμα (topic) ακόμη και αν ο πελάτης έκανε «εγγραφή/συνδρομή» μετά την αποστολή αυτών. Επίσης, είναι δυνατή η διατήρηση των «εγγραφών/συνδρομών» (subscriptions) ενός πελάτη ακόμη και σε περίπτωση ξαφνικής αποσύνδεσης, ώστε να συνεχίσει απρόσκοπτα μετά την επανασύνδεσή του. Σε περιπτώσεις ξαφνικών αποσυνδέσεων έχουμε και την δυνατότητα «διαθήκης» (Last Will), η οποία εκτελεί κάποια συγκεκριμένη εργασία με την αποσύνδεση.

Η εκτέλεση του πρώτου σκέλους του πειράματος είναι αρκετά απλή. Ένας MQTT Broker μπορεί να «στηθεί» σε συστήματα με βάση το Linux ή με μερικές προσθήκες και τροποποιήσεις σε περιβάλλον Windows. Για τους σκοπούς της παρούσας εργασίας, χρησιμοποιήθηκαν εκτός από εκείνον του Raspberry Pi, δημόσιοι brokers από την σελίδα: **https://github.com/mqtt/mqtt.github.io/wiki/public_brokers**, η επιλογή των οποίων έγινε με γνώμονα τις δυνατότητες σύνδεσης και της έκδοσης του πρωτοκόλλου MQTT. Στον ρόλο των πελατών/αποστολέων (subscribers/publishers) χρησιμοποιήθηκαν:

- Η/Υ με Windows 10 και εγκατεστημένο το MQTT Explorer (μαζί με το λογισμικό που αναφέρθηκε στην αρχή του κεφαλαίου),
- ένα Raspberry Pi 4 και,
- ένα «έξυπνο» κινητό τηλέφωνο με Android έκδοσης 9 και εγκατεστημένες εφαρμογές συμβατές με το πρωτόκολλο MQTT.

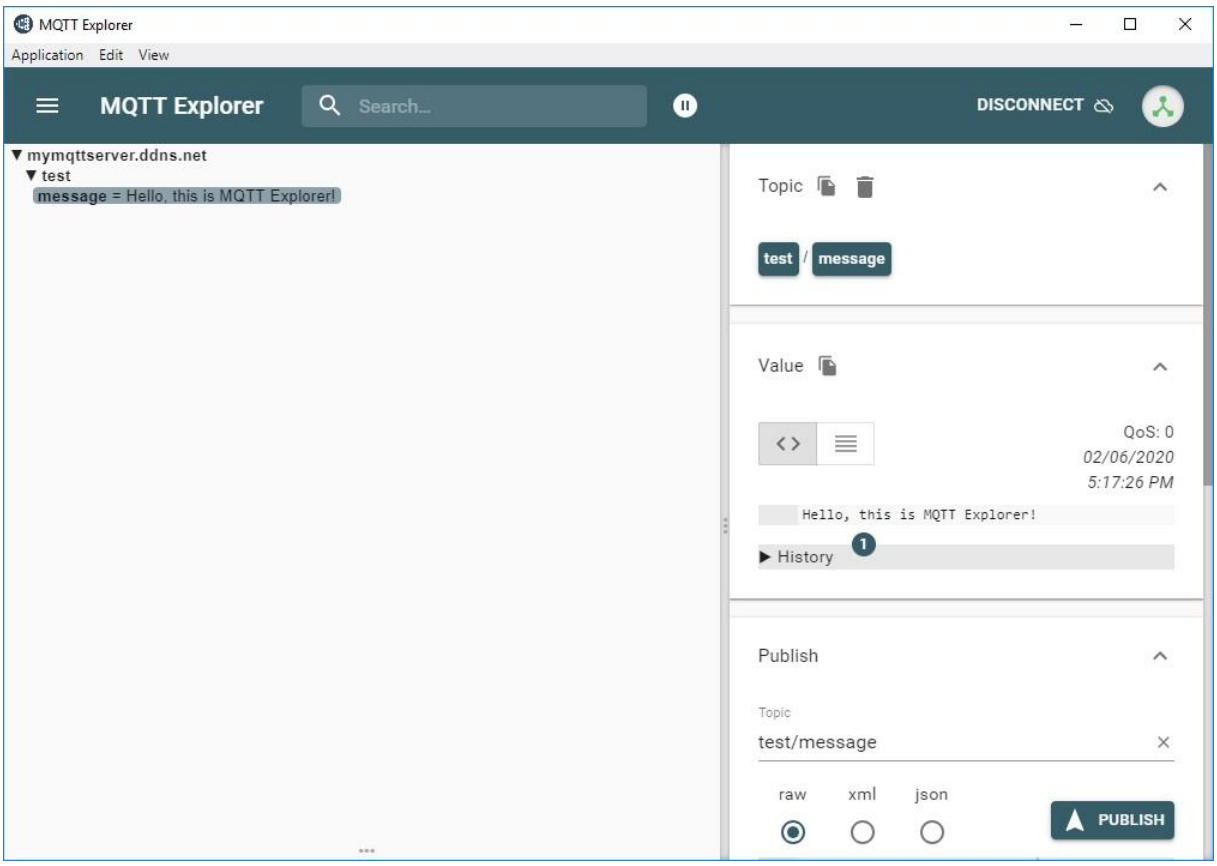
Μία απλή ανταλλαγή μηνυμάτων μεταξύ του publisher (MQTT Explorer) και του subscriber (κινητό τηλέφωνο Android) μέσω του broker (Raspberry Pi 4), ακολουθεί παρακάτω:

i. Ο εκδότης (publisher) θα στείλει το μήνυμα «Hello, this is MQTT Explorer!», στο θέμα (topic) «test/message».
ii. Όσες συσκευές είναι συνδεδεμένες στον broker και είναι εγγεγραμμένες στο συγκεκριμένο θέμα, θα λάβουν το μήνυμα. Στην συγκεκριμένη περίπτωση, ο παραλήπτης είναι το κινητό τηλέφωνο Android.
iii. Αφού λάβει το μήνυμα, το κινητό απαντά με «Hello, this is an android device!».

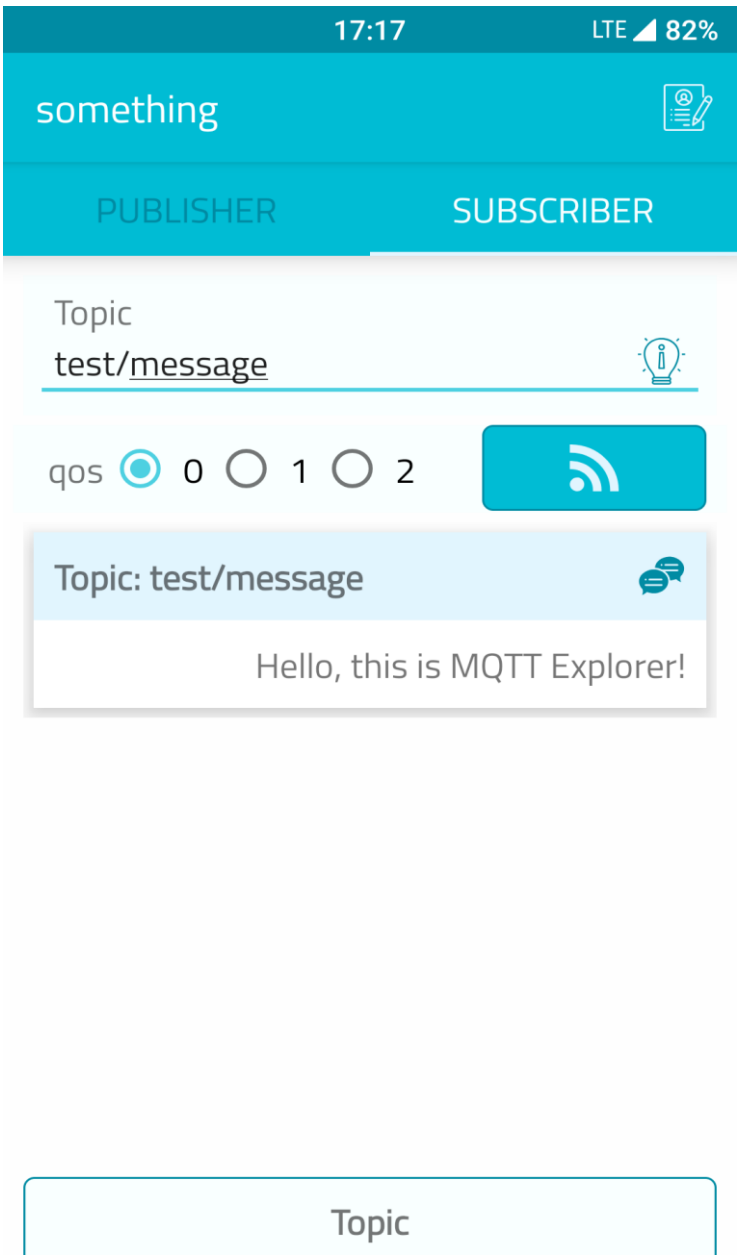


Η αρχική οθόνη του προγράμματος MQTT Explorer.

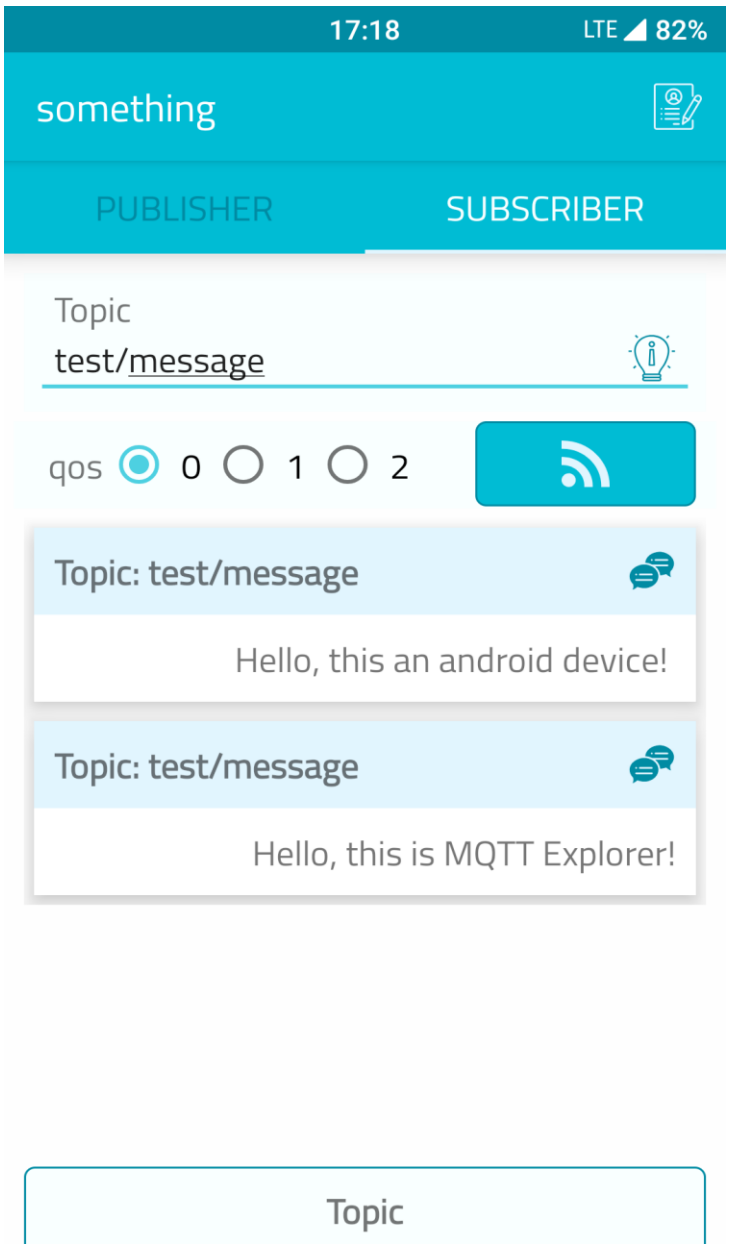
Ο σκοπός της δοκιμής, είναι η ανάγνωση της παραπάνω συζήτησης εάν κάποιος επιτιθέμενος κάνει ανάλυση της δικτυακής κίνησης στην πλευρά του αποστολέα/εξυπηρετητή. Επίσης, όλες οι συσκευές θα είναι εγγεγραμμένες (subscribed) στο θέμα «test/message» ώστε να επαληθευτεί η επιτυχής μετάδοση των μηνυμάτων. Στο συγκεκριμένο πείραμα, ο πρώτος αποστολέας/συνδρομητής (H/Y με Windows 10 και MQTT Explorer) και ο εξυπηρετητής (Raspberry Pi 4) είναι συνδεδεμένοι στο ίδιο τοπικό δίκτυο. Ο δεύτερος αποστολέας/συνδρομητής (κινητό τηλέφωνο Android) συνδέεται με το Διαδίκτυο μέσω δεδομένων (4G LTE).



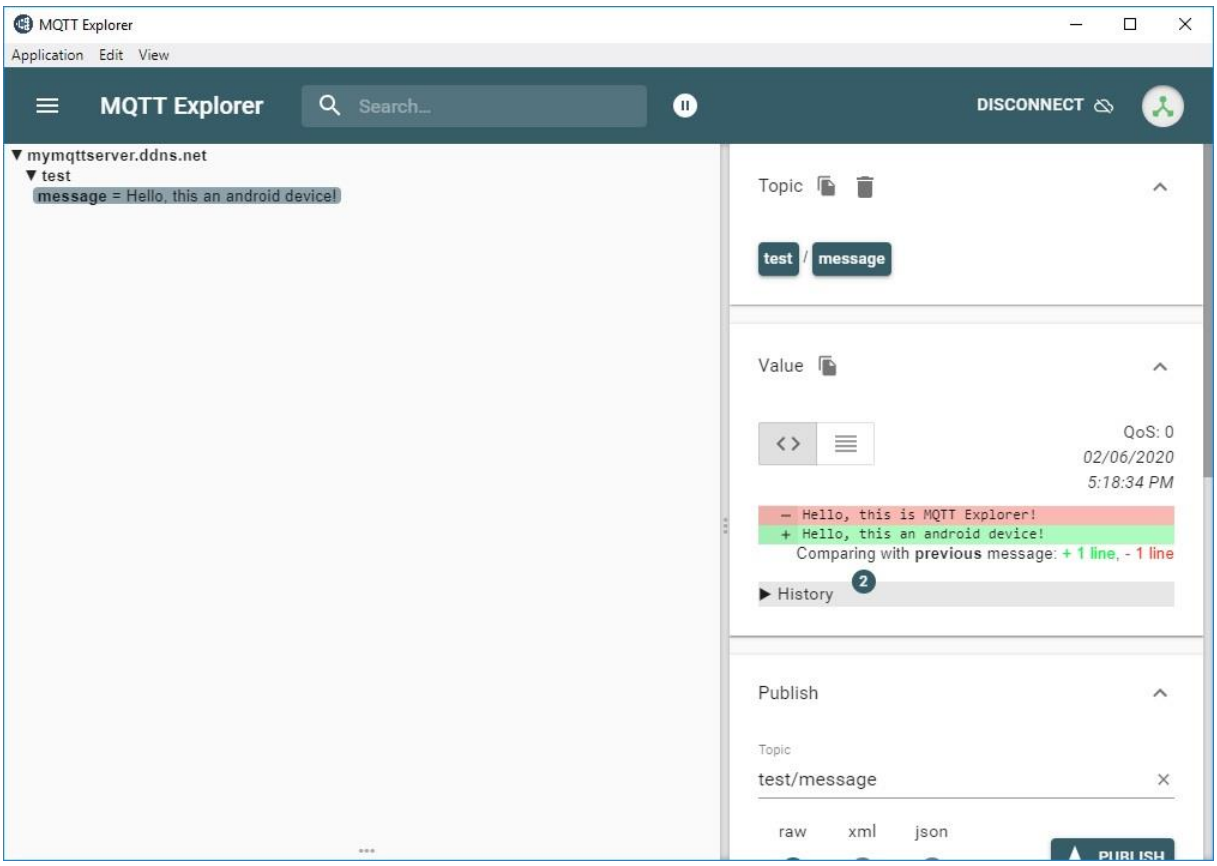
Σύνδεση με τον Broker και αποστολή του πρώτου μηνύματος.



Το κινητό λαμβάνει το μήνυμα.



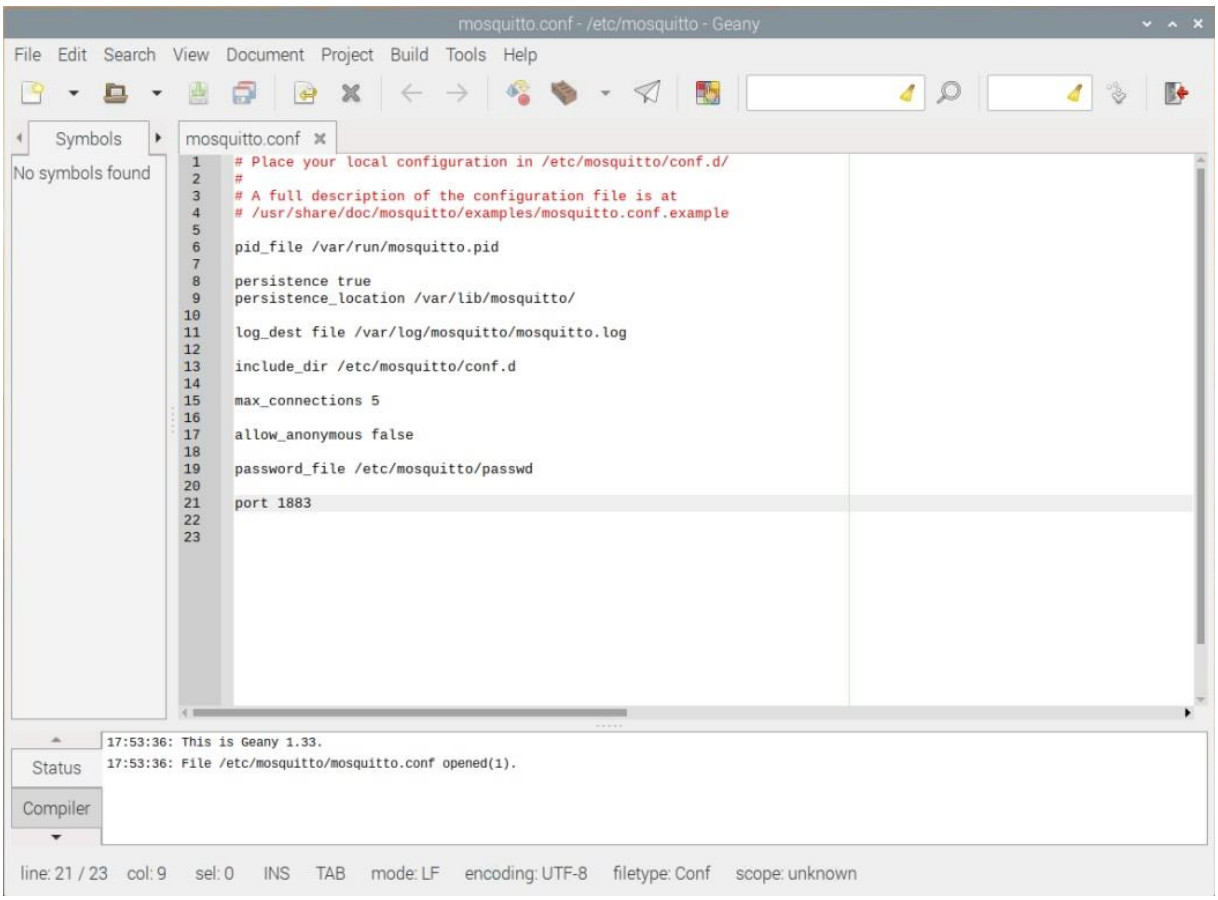
Κατόπιν, το κινητό απαντά (από την καρτέλα Publisher, της εφαρμογής).



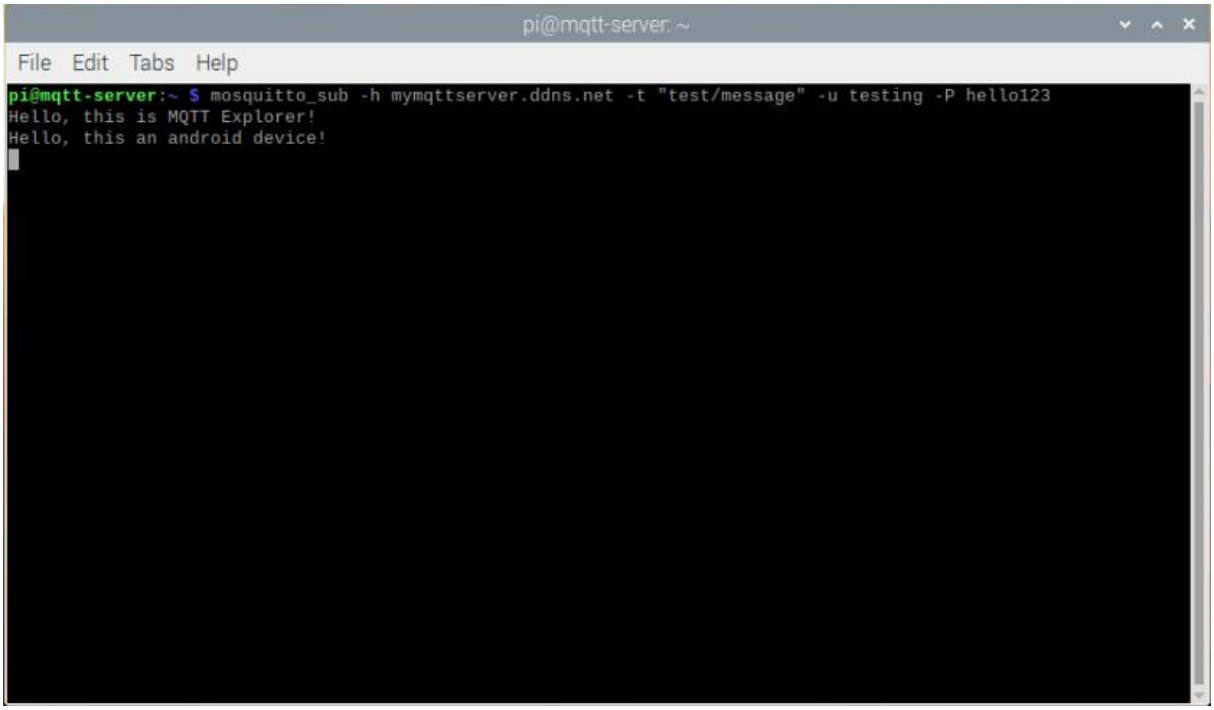
Το μήνυμα του κινητού λαμβάνεται από τον πελάτη (MQTT Explorer).

Ο broker στο Raspberry Pi είναι ρυθμισμένος με τρόπο τέτοιο ώστε να απαιτεί από τους συνδρομητές του επαλήθευση της ταυτότητάς τους προκειμένου να μπορούν να συνδεθούν σε αυτόν. Μέσω του αρχείου ρυθμίσεων (configuration) mosquitto.conf, ο διαχειριστής του εξυπηρετητή μπορεί να εφαρμόσει πληθώρα ρυθμίσεων. Η επεξεργασία και μετακίνηση του αρχείου απαιτεί δικαιώματα διαχειριστή (Superuser/Root). Οι εντολές που χρησιμοποιήθηκαν για την απαίτηση ταυτοποίησης με όνομα χρήστη και κωδικό (username/password) φαίνονται στην φωτογραφία που ακολουθεί και ονομαστικά είναι:

- «allow_anonymous false». Ο εξυπηρετητής δεν δέχεται συνδέσεις από ανώνυμους χρήστες/συσκευές.
- «password_file /etc/mosquitto/passwd». Μέσω της εφαρμογής «mosquitto_passwd» δημιουργήσαμε αρχείο passwd.txt το οποίο περιέχει τα ονόματα χρηστών και τους κωδικούς πρόσβασης, στους οποίους επιτρέπεται η σύνδεση στον εξυπηρετητή. Η εφαρμογή κρυπτογραφεί τον κωδικό πρόσβασης αλλά αφήνει το όνομα χρήστη σε μορφή απλού κειμένου. Η επεξεργασία και μετακίνηση του αρχείου απαιτεί δικαιώματα διαχειριστή (Superuser/Root). Η παραπάνω εντολή, «δείχνει» στον εξυπηρετητή την τοποθεσία του αρχείου με τους συνδυασμούς ονομάτων χρηστών/κωδικών πρόσβασης.

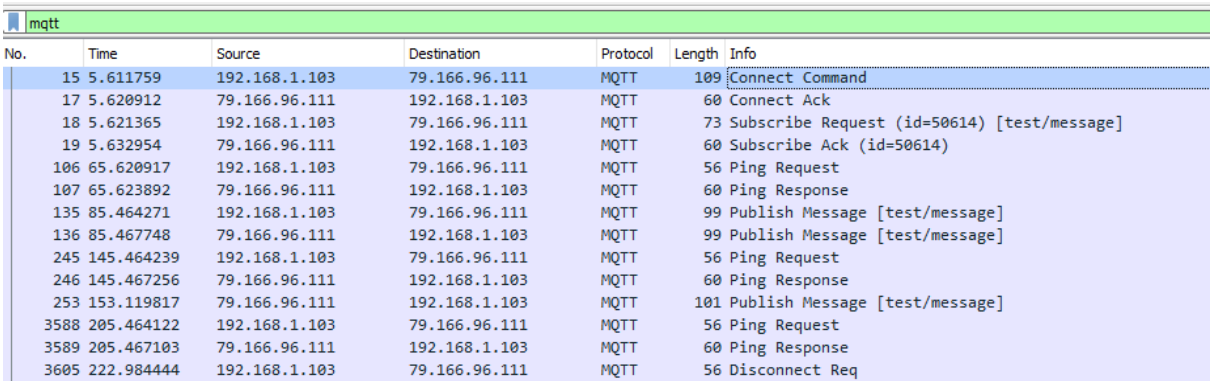


Το αρχείο ρυθμίσεων mosquitto.conf ανοιγμένο στον επεξεργαστή κειμένου Geany. Σημειώνεται πως η ανάγνωση του αρχείου γίνεται από τον οποιονδήποτε, αλλά η επεξεργασία απαιτεί δικαιώματα διαχειριστή.



Τα μηνύματα που ανταλλάχθηκαν μέσω του εξυπηρετητή (Raspberry Pi 4).

Με τη χρήση του αναλυτή δικτυακής κίνησης Wireshark κάναμε ανάγνωση των πακέτων που λαμβάνονται και αποστέλλονται στον αντάπτορα δικτύου της επιλογής μας. Με την εφαρμογή του φίλτρου «mqtt» εμφανίζονται μόνο τα πακέτα του πρωτοκόλλου MQTT.

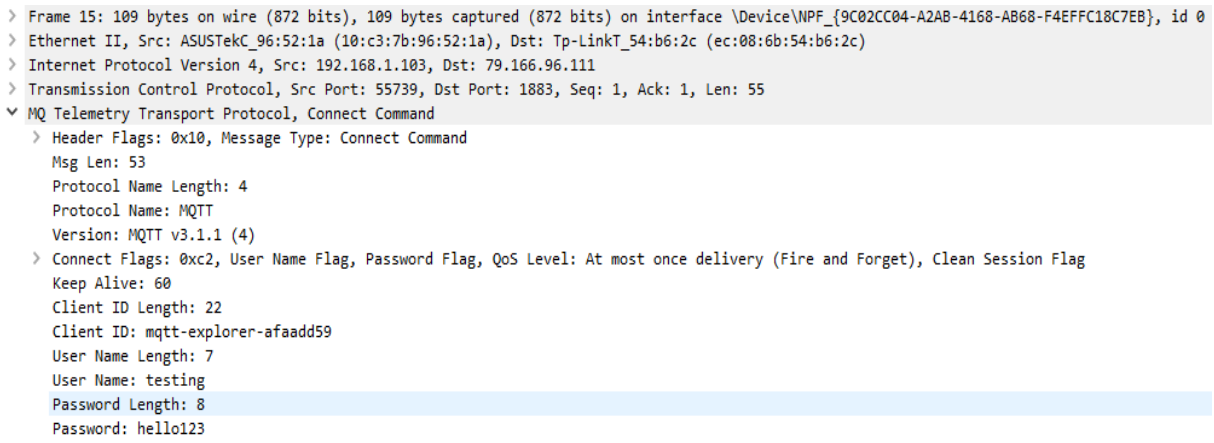


mqtt

No.	Time	Source	Destination	Protocol	Length	Info
15	5.611759	192.168.1.103	79.166.96.111	MQTT	109	Connect Command
17	5.620912	79.166.96.111	192.168.1.103	MQTT	60	Connect Ack
18	5.621365	192.168.1.103	79.166.96.111	MQTT	73	Subscribe Request (id=50614) [test/message]
19	5.632954	79.166.96.111	192.168.1.103	MQTT	60	Subscribe Ack (id=50614)
106	65.620917	192.168.1.103	79.166.96.111	MQTT	56	Ping Request
107	65.623892	79.166.96.111	192.168.1.103	MQTT	60	Ping Response
135	85.464271	192.168.1.103	79.166.96.111	MQTT	99	Publish Message [test/message]
136	85.467748	79.166.96.111	192.168.1.103	MQTT	99	Publish Message [test/message]
245	145.464239	192.168.1.103	79.166.96.111	MQTT	56	Ping Request
246	145.467256	79.166.96.111	192.168.1.103	MQTT	60	Ping Response
253	153.119817	79.166.96.111	192.168.1.103	MQTT	101	Publish Message [test/message]
3588	205.464122	192.168.1.103	79.166.96.111	MQTT	56	Ping Request
3589	205.467103	79.166.96.111	192.168.1.103	MQTT	60	Ping Response
3605	222.984444	192.168.1.103	79.166.96.111	MQTT	56	Disconnect Req

Τα πακέτα MQTT που μεταδόθηκαν.

Επιλέγοντας το πρώτο πακέτο της παραπάνω εικόνας βλέπουμε τα εξής:



```
> Frame 15: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF_{9C02CC04-A2AB-4168-AB68-F4EFFC18C7EB}, id 0
> Ethernet II, Src: ASUSTekC_96:52:1a (10:c3:7b:96:52:1a), Dst: Tp-LinkT_54:b6:2c (ec:08:6b:54:b6:2c)
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 79.166.96.111
> Transmission Control Protocol, Src Port: 55739, Dst Port: 1883, Seq: 1, Ack: 1, Len: 55
v MQ Telemetry Transport Protocol, Connect Command
  > Header Flags: 0x10, Message Type: Connect Command
    Msg Len: 53
    Protocol Name Length: 4
    Protocol Name: MQTT
    Version: MQTT v3.1.1 (4)
  > Connect Flags: 0xc2, User Name Flag, Password Flag, QoS Level: At most once delivery (Fire and Forget), Clean Session Flag
    Keep Alive: 60
    Client ID Length: 22
    Client ID: mqtt-explorer-afaadd59
    User Name Length: 7
    User Name: testing
    Password Length: 8
    Password: hello123
```

Οι λεπτομέρειες του πρώτου πακέτου της σύνδεσης.

Το πρώτο πακέτο που αποστέλλεται είναι από τον MQTT Explorer προς τον εξυπηρετητή (broker) που είναι εγκατεστημένος στο Raspberry Pi. Πρόκειται για μία εντολή εκκίνησης σύνδεσης η οποία περιέχει τα εξής στοιχεία:

- Την έκδοση του πρωτοκόλλου MQTT
- Την σημαία QoS η οποία στην συγκεκριμένη δοκιμή έχει την τιμή μηδέν (0).
- Την σημαία Clean Session που δείχνει ότι πρόκειται για μία νέα σύνδεση.
- Την τιμή του Keep Alive.
- Την ταυτότητα του πελάτη, Client ID καθώς και το μήκος της σε χαρακτήρες.
- Τις σημαίες «User Name» και «Password».

Όπως είναι προφανές, εάν η σύνδεση δεν είναι κρυπτογραφημένη, όλα τα στοιχεία μπορούν να αναγνωστούν λεπτομερώς από τον επιτιθέμενο. Εδώ, αναγράφεται το όνομα χρήστη (Username) «testing» με μήκος επτά (7) χαρακτήρων και ο κωδικός πρόσβασης «Password» με μήκος οκτώ (8) χαρακτήρων.

```
> Frame 135: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{9C02CC04-A2AB-4168-AB68-F4EFFC18C7EB}, id 0
> Ethernet II, Src: ASUSTekC_96:52:1a (10:c3:7b:96:52:1a), Dst: Tp-LinkT_54:b6:2c (ec:08:6b:54:b6:2c)
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 79.166.96.111
> Transmission Control Protocol, Src Port: 55739, Dst Port: 1883, Seq: 77, Ack: 12, Len: 45
v MQ Telemetry Transport Protocol, Publish Message
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
    Msg Len: 43
    Topic Length: 12
    Topic: test/message
    Message: 48656c6c6f2c207468697320697320d515454204578706c…
```

```
0000  ec 08 6b 54 b6 2c 10 c3  7b 96 52 1a 08 00 45 00   ··kT·,·· {·R···E·
0010  00 55 54 cc 40 00 80 06  00 00 c0 a8 01 67 4f a6   ·UT·@··· ·····gO·
0020  60 6f d9 bb 07 5b 9e 1c  d5 b9 bc 47 76 43 50 18   `o···[·· ···GvCP·
0030  01 00 72 6c 00 00 30 2b  00 0c 74 65 73 74 2f 6d   ··rl··0+ ··test/m
0040  65 73 73 61 67 65 48 65  6c 6c 6f 2c 20 74 68 69   essageHe llo, thi
0050  73 20 69 73 20 4d 51 54  54 20 45 78 70 6c 6f 72   s is MQT T Explor
0060  65 72 21                                          er!
```

Λεπτομέρειες του πακέτου No. 135. Εμφανίζεται το θέμα (topic) στο οποίο ο πελάτης είναι αποστολέας/αποδέκτης καθώς και το περιεχόμενο του μηνύματος σε απλό κείμενο. Εδώ, το μήνυμα είναι αυτό που αποστέλλεται από τον MQTT Explorer προς το κινητό τηλέφωνο Android.

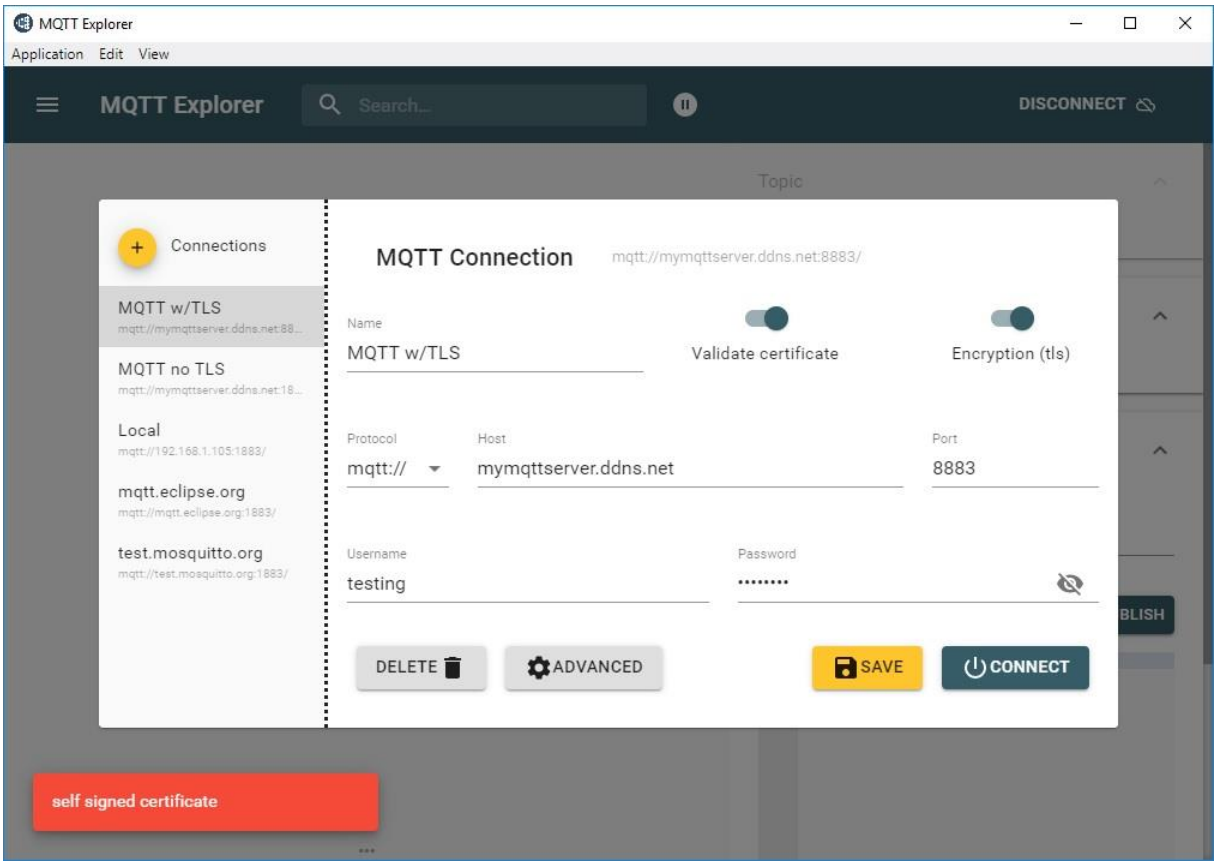
```
> Frame 253: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF_{9C02CC04-A2AB-4168-AB68-F4EFFC18C7EB}, id 0
> Ethernet II, Src: Tp-LinkT_54:b6:2c (ec:08:6b:54:b6:2c), Dst: ASUSTekC_96:52:1a (10:c3:7b:96:52:1a)
> Internet Protocol Version 4, Src: 79.166.96.111, Dst: 192.168.1.103
> Transmission Control Protocol, Src Port: 1883, Dst Port: 55739, Seq: 59, Ack: 124, Len: 47
v MQ Telemetry Transport Protocol, Publish Message
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
    Msg Len: 45
    Topic Length: 12
    Topic: test/message
    Message: 48656c6c6f2c207468697320616e20616e64726f69642064…
```

```
0000  10 c3 7b 96 52 1a ec 08  6b 54 b6 2c 08 00 45 00   ··{·R··· kT·,··E·
0010  00 57 36 a0 40 00 3f 06  92 dc 4f a6 60 6f c0 a8   ·W6·@·?· ··O·`o··
0020  01 67 07 5b d9 bb bc 47  76 72 9e 1c d5 e8 50 18   ·g·[···G vr····P·
0030  01 f6 cb 8e 00 00 30 2d  00 0c 74 65 73 74 2f 6d   ·····0- ··test/m
0040  65 73 73 61 67 65 48 65  6c 6c 6f 2c 20 74 68 69   essageHe llo, thi
0050  73 20 61 6e 20 61 6e 64  72 6f 69 64 20 64 65 76   s an and roid dev
0060  69 63 65 21 20                                    ice!
```

Λεπτομέρειες του πακέτου No. 253. Όπως και πριν, εμφανίζεται λεπτομερώς το περιεχόμενο του μηνύματος που αποστέλλεται αυτή τη φορά από το κινητό τηλέφωνο Android στον MQTT Explorer.

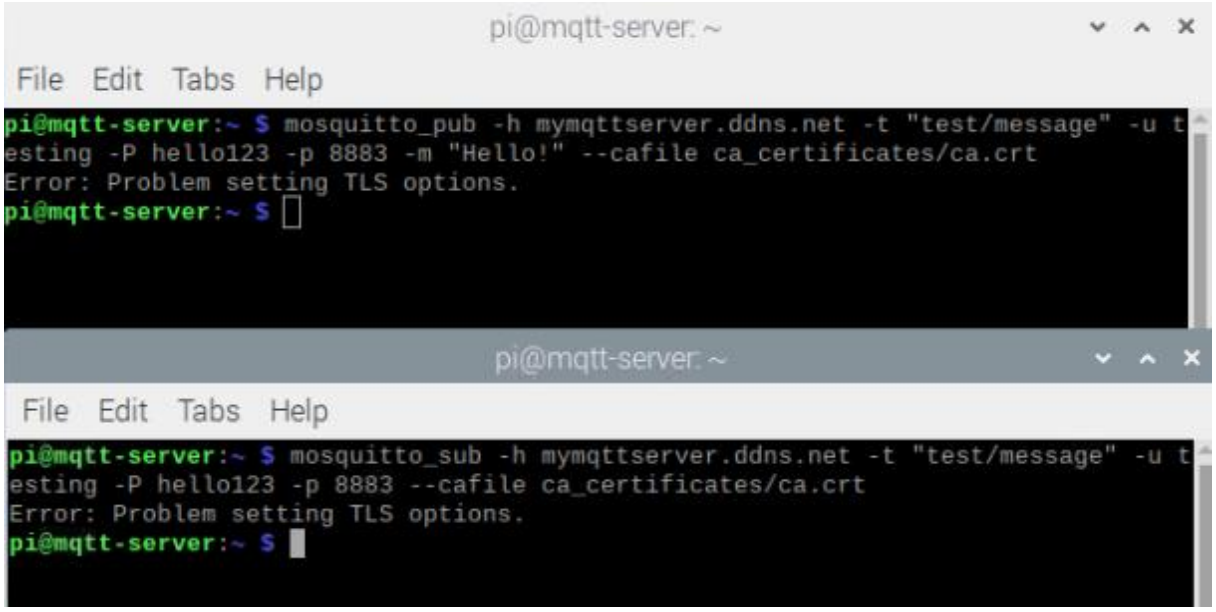
Στη συνέχεια θα ενεργοποιηθεί η κρυπτογράφηση και θα γίνει εκ νέου ανάλυση των πακέτων. Τα μηνύματα θα αποσταλούν ακριβώς με τον ίδιο τρόπο και περιεχόμενο. Για τις ανάγκες αυτής της δοκιμής δεν θα χρησιμοποιήσουμε τον ιδιωτικό broker που εγκαταστήσαμε στο Raspberry Pi. Θα χρησιμοποιήσουμε έναν δημόσιο broker που είναι διαθέσιμος για δοκιμές. Οι λόγοι για την επιλογή αυτή είναι:

ι. Τα αρχεία κλειδιών και πιστοποιητικών που δημιουργούνται μέσω της εφαρμογής openssl, είναι «υπογεγραμμένα» από τον ίδιο τον broker και όχι από κάποια έμπιστη υπηρεσία ψηφιακών πιστοποιητικών όπως η DigiCert Inc., η Google Trust Services, η GlobalSign κ.α. Υπάρχουν clients οι οποίοι δέχονται κρυπτογραφημένες συνδέσεις αλλά τα πιστοποιητικά τους, δεν πρέπει να είναι υπογεγραμμένα από τον ίδιο τον broker. Βέβαια, υπάρχουν εφαρμογές που δέχονται τέτοια πιστοποιητικά κατ' επιλογή του χρήστη. Η εφαρμογή όμως προειδοποιεί τον χρήστη πως τα αυτο-υπογεγραμμένα πιστοποιητικά είναι επικίνδυνα και η χρήση τους γίνεται με ρίσκο του χρήστη.



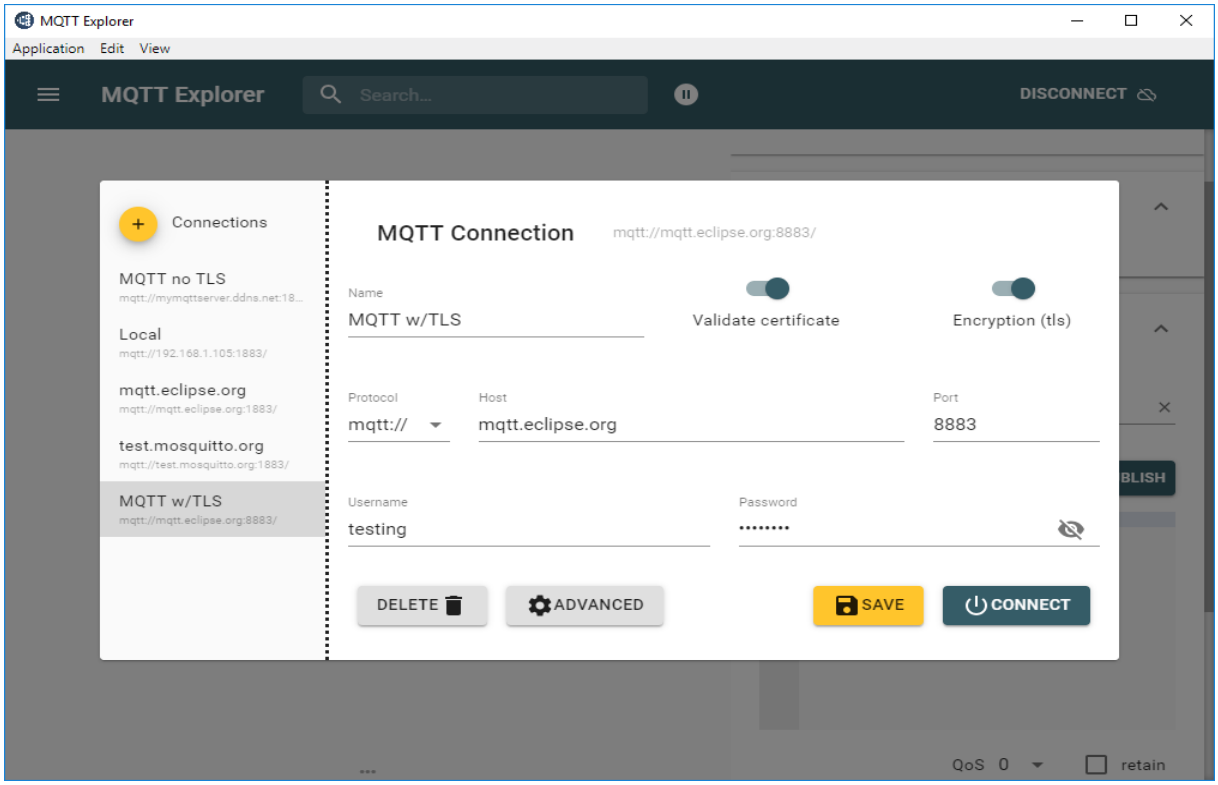
Το σφάλμα που προκύπτει όταν επιχειρείται η σύνδεση του MQTT Explorer στον ιδιωτικό broker του Raspberry Pi 4. Το μήνυμα που εμφανίζεται σε κόκκινο πλαίσιο γράφει: «self signed certificate», δηλαδή, αυτο-υπογεγραμμένο πιστοποιητικό. Η σύνδεση απορρίπτεται γιατί το πιστοποιητικό του broker δεν μπορεί να επικυρωθεί από την εφαρμογή.

ιι. Η ρύθμιση του broker για χρήση κρυπτογράφησης SSL/TLS οδηγούσε πάντα σε σφάλματα κάνοντας την διαδικασία μετάδοσης μηνυμάτων αδύνατη.



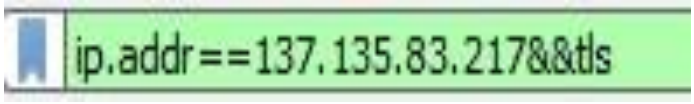
«Σφάλμα ρύθμισης επιλογών TLS».

Η δοκιμή εκτελέστηκε με τον broker του ιδρύματος Eclipse, με διεύθυνση «mqtt.eclipse.org».

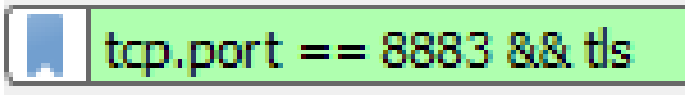


Ο δημόσιος broker του ιδρύματος Eclipse. Προκειμένου να γίνει χρήση κρυπτογράφησης πρέπει να ενεργοποιηθεί ο διακόπτης «Encryption (TLS)» και η θύρα να αλλαχθεί από 1883 σε 8883.

Γνωρίζουμε πως η τοπική διεύθυνση IP του Η/Υ είναι η 192.168.1.103 και η διεύθυνση IP του broker είναι η 137.135.83.217. Επομένως, για να προβάλλουμε στο Wireshark μόνο τα πακέτα που ανταλλάχθηκαν μεταξύ των δύο διευθύνσεων, χρησιμοποιούμε το φίλτρο:



εναλλακτικά,



με πανομοιότυπα αποτελέσματα.

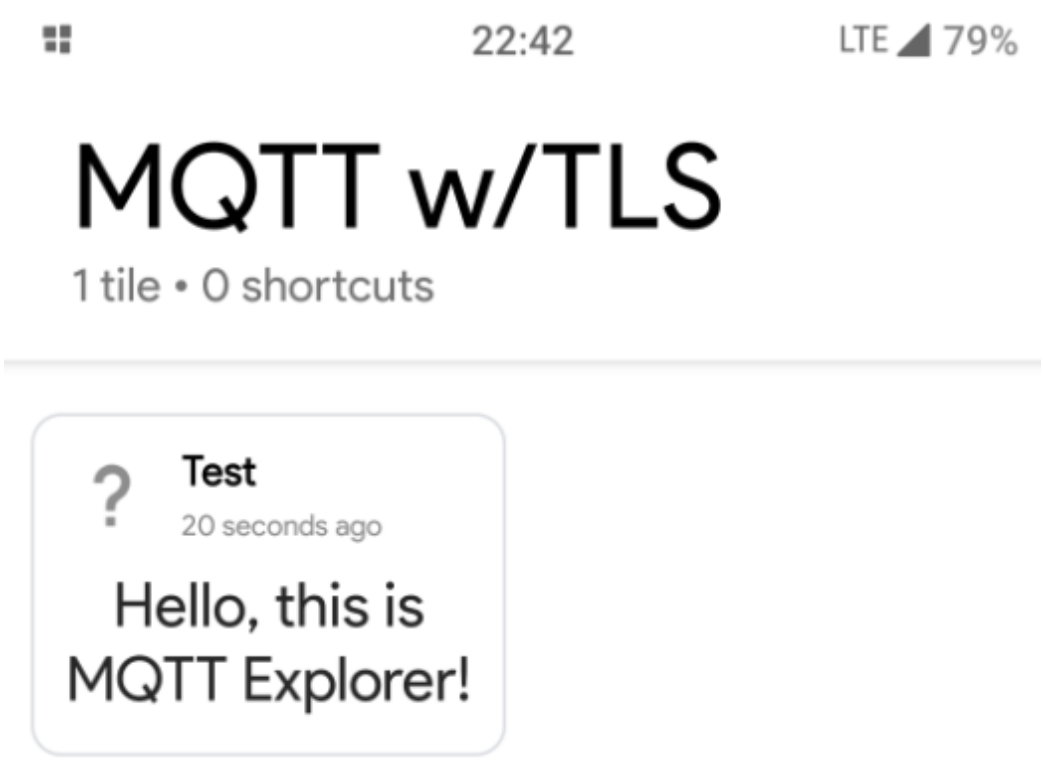
ip.addr==137.135.83.217&&tls

No.	Time	Source	Destination	Protocol	Length	Info
30	4.719514	192.168.1.103	137.135.83.217	TLSv1.2	309	Client Hello
32	4.888168	137.135.83.217	192.168.1.103	TLSv1.2	1494	Server Hello
33	4.889638	137.135.83.217	192.168.1.103	TLSv1.2	1494	Certificate [TCP segment of a reassembled PDU]
35	4.889846	137.135.83.217	192.168.1.103	TLSv1.2	150	Server Key Exchange, Server Hello Done
36	4.890131	192.168.1.103	137.135.83.217	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
37	5.055932	137.135.83.217	192.168.1.103	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
38	5.056394	192.168.1.103	137.135.83.217	TLSv1.2	486	Application Data, Application Data, Application Data, Application Data,
39	5.223214	137.135.83.217	192.168.1.103	TLSv1.2	87	Application Data
40	5.223746	192.168.1.103	137.135.83.217	TLSv1.2	247	Application Data, Application Data, Application Data, Application Data,
41	5.387060	137.135.83.217	192.168.1.103	TLSv1.2	88	Application Data
83	38.398570	192.168.1.103	137.135.83.217	TLSv1.2	244	Application Data, Application Data, Application Data, Application Data,
84	38.564030	137.135.83.217	192.168.1.103	TLSv1.2	128	Application Data
127	89.590085	137.135.83.217	192.168.1.103	TLSv1.2	133	Application Data
139	98.399491	192.168.1.103	137.135.83.217	TLSv1.2	85	Application Data
141	98.563018	137.135.83.217	192.168.1.103	TLSv1.2	85	Application Data
180	122.953132	192.168.1.103	137.135.83.217	TLSv1.2	114	Application Data, Application Data
181	122.953298	192.168.1.103	137.135.83.217	TLSv1.2	85	Encrypted Alert

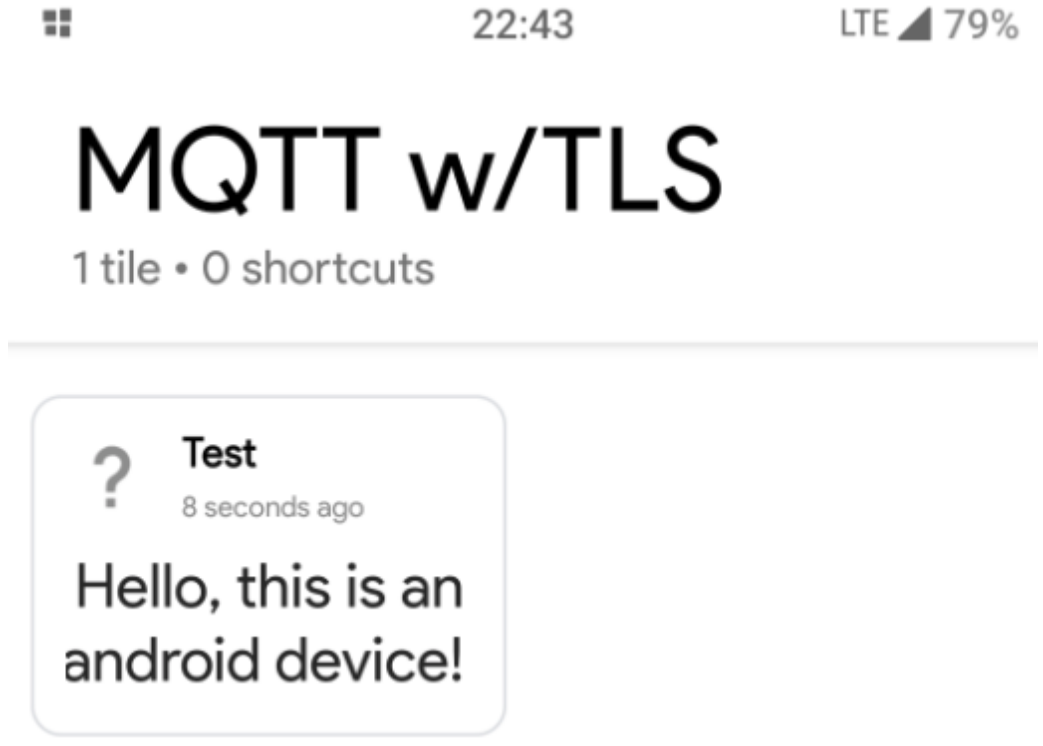
Τα πακέτα που λήφθηκαν μέσω Wireshark.

```
> Frame 40: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface \Device\NPF_{9C02CC04-A2AB-4168-AB68-F4EFFC18C7EB}, id 0
> Ethernet II, Src: ASUSTekC_96:52:1a (10:c3:7b:96:52:1a), Dst: Tp-LinkT_54:b6:2c (ec:08:6b:54:b6:2c)
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 137.135.83.217
> Transmission Control Protocol, Src Port: 56254, Dst Port: 8883, Seq: 814, Ack: 3268, Len: 193
v Transport Layer Security
  > TLSv1.2 Record Layer: Application Data Protocol: mqtt
  > TLSv1.2 Record Layer: Application Data Protocol: mqtt
  > TLSv1.2 Record Layer: Application Data Protocol: mqtt
  > TLSv1.2 Record Layer: Application Data Protocol: mqtt
  > TLSv1.2 Record Layer: Application Data Protocol: mqtt
  v TLSv1.2 Record Layer: Application Data Protocol: mqtt
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 25
      Encrypted Application Data: 00000000000001322f003464a634ee0d048fcbd2b32ad0a…
```

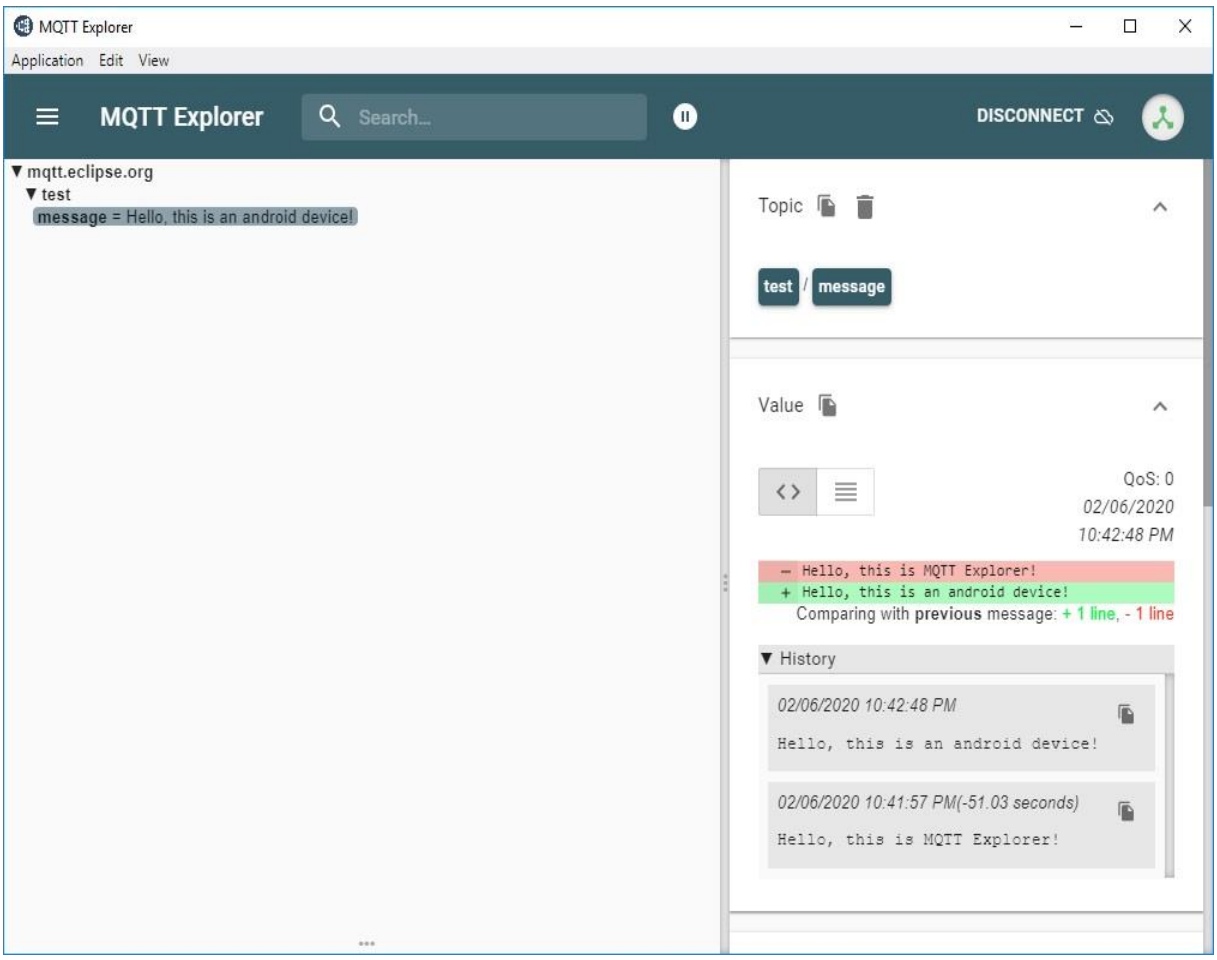
Οι λεπτομέρειες του παραπάνω επιλεγμένου πακέτου (No. 40). Είναι εμφανές πως αυτή τη φορά, η ανάγνωση του περιεχομένου είναι αδύνατη. Είναι άγνωστο το θέμα στο οποίο είναι εγγεγραμμένος ο client, άγνωστο το QoS, το περιεχόμενο των μηνυμάτων και τα στοιχεία ταυτοποίησης (όνομα χρήστη/κωδικός πρόσβασης).



Επιτυχής λήψη μηνύματος από το κινητό τηλέφωνο Android.



Το κινητό τηλέφωνο απαντά στον MQTT Explorer.

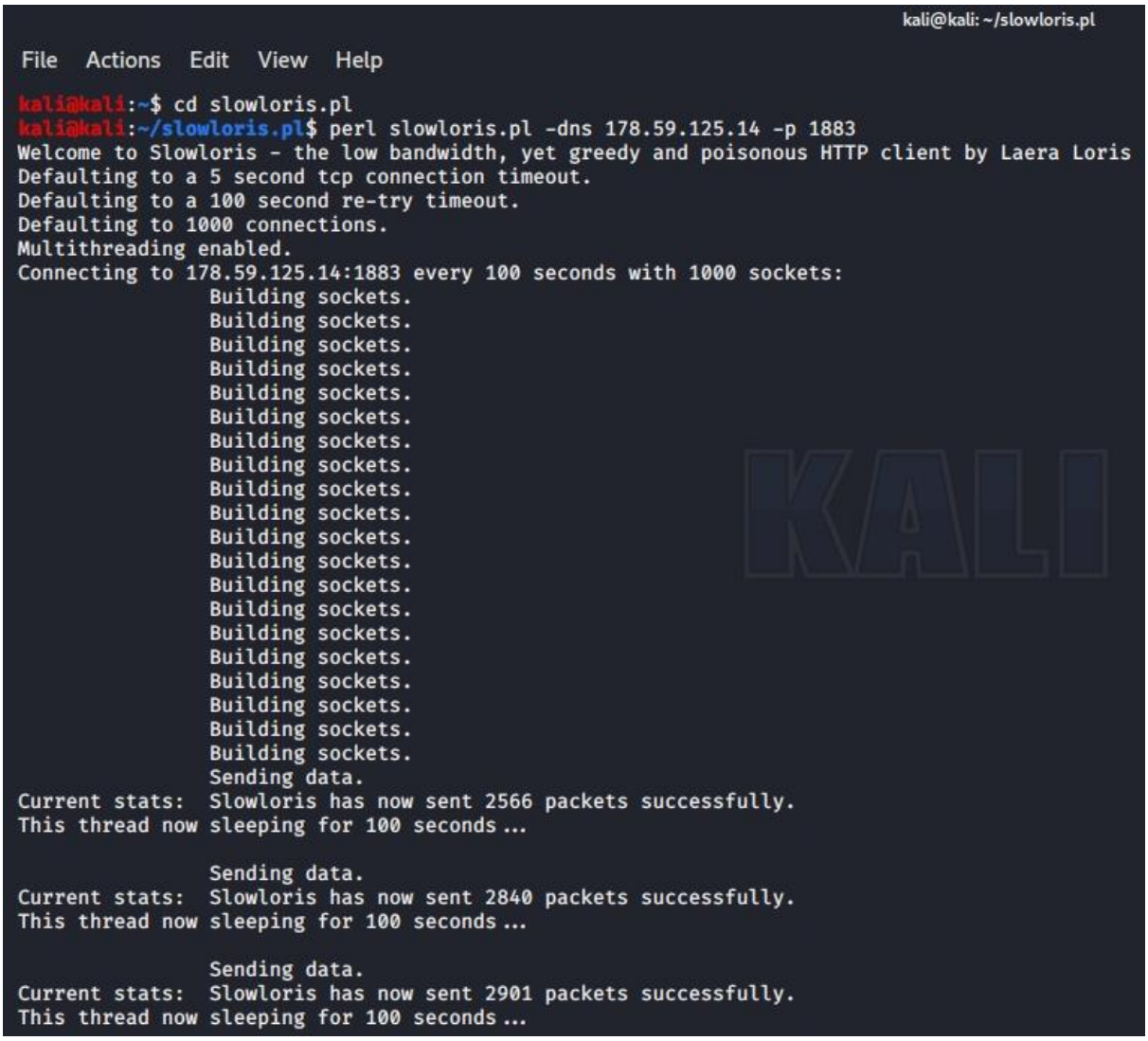


Η ανταλλαγή μηνυμάτων από την πλευρά του MQTT Explorer. Με πράσινο (+) συμβολίζεται η λήψη μηνύματος από τον MQTT Explorer, ενώ με κόκκινο (-) η αποστολή μηνύματος προς το κινητό τηλέφωνο.

Το μεγάλο πρόβλημα βρίσκεται στην εφαρμογή κρυπτογραφημένων επικοινωνιών στις συσκευές κατώτερου επιπέδου στο δίκτυο IoT, όπως είναι αισθητήρες και στοιχειώδεις ενεργοποιητές, των οποίων τα κυκλώματα είναι μικρά και απλά προκειμένου η κατανάλωση ενέργειας και το κόστος κατασκευής να είναι χαμηλά. Η απλότητα των κυκλωμάτων σημαίνει ότι τέτοιες συσκευές δεν έχουν τους απαραίτητους υπολογιστικούς πόρους (επεξεργαστική ισχύ, μνήμη RAM) που χρειάζονται για τη λειτουργία αλγορίθμων κρυπτογράφησης.

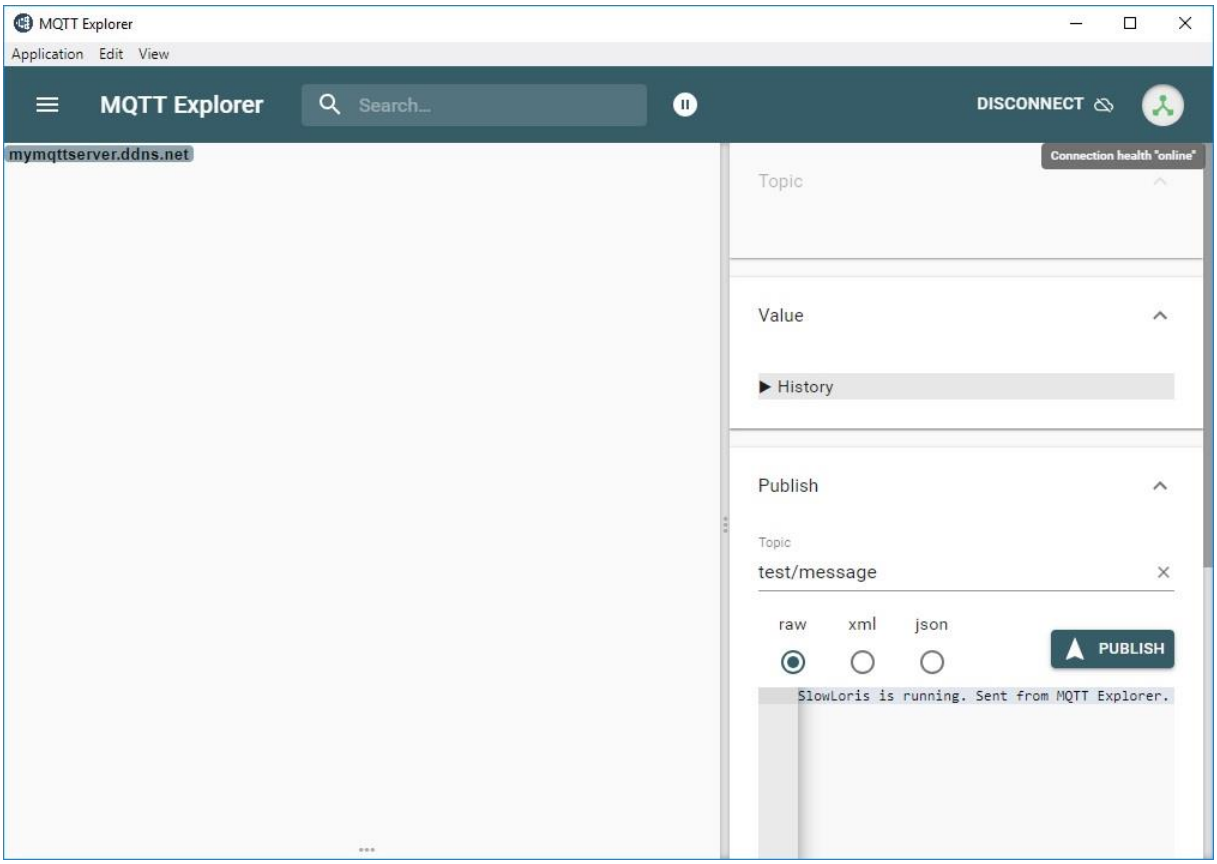
Επίθεση No. 2: SlowLoris Denial Of Service Attack (Επίθεση Άρνησης Υπηρεσιών).

Σε αυτό το σενάριο θα εξεταστεί η ικανότητα ενός broker να διαχειριστεί μία επίθεση άρνησης υπηρεσιών. Το είδος της επίθεσης που θα χρησιμοποιηθεί είναι η SlowLoris της οποίας δημιουργός είναι ο Robert "RSnake" Hansen. Η επίθεση αυτή επιτρέπει σε ένα μόνο μηχάνημα να διακόψει τη λειτουργία ενός εξυπηρετητή με χρήση ελάχιστων πόρων από την πλευρά του επιτιθέμενου. Για την υλοποίηση αυτής της δοκιμής θα χρησιμοποιηθεί ο broker του Raspberry Pi και η διανομή Kali Linux της Offensive Security.

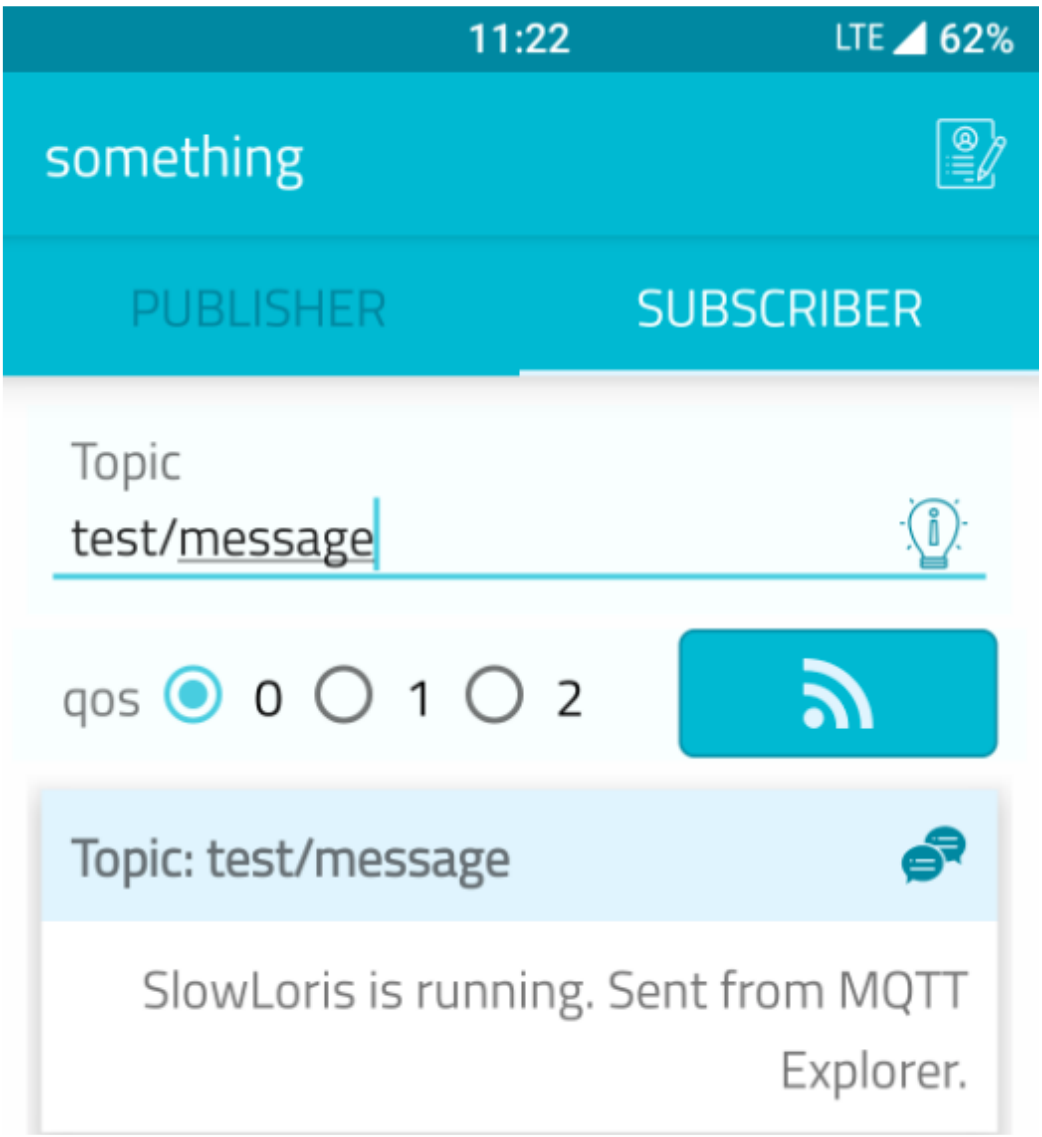


Εκτέλεση της επίθεσης. Η διεύθυνση IP της εικόνας αντιστοιχεί στον broker του Raspberry Pi με όνομα «mymqttserver.ddns.net» και η θύρα 1883 είναι η προεπιλεγμένη θύρα για μη κρυπτογραφημένη μετάδοση μηνυμάτων MQTT.

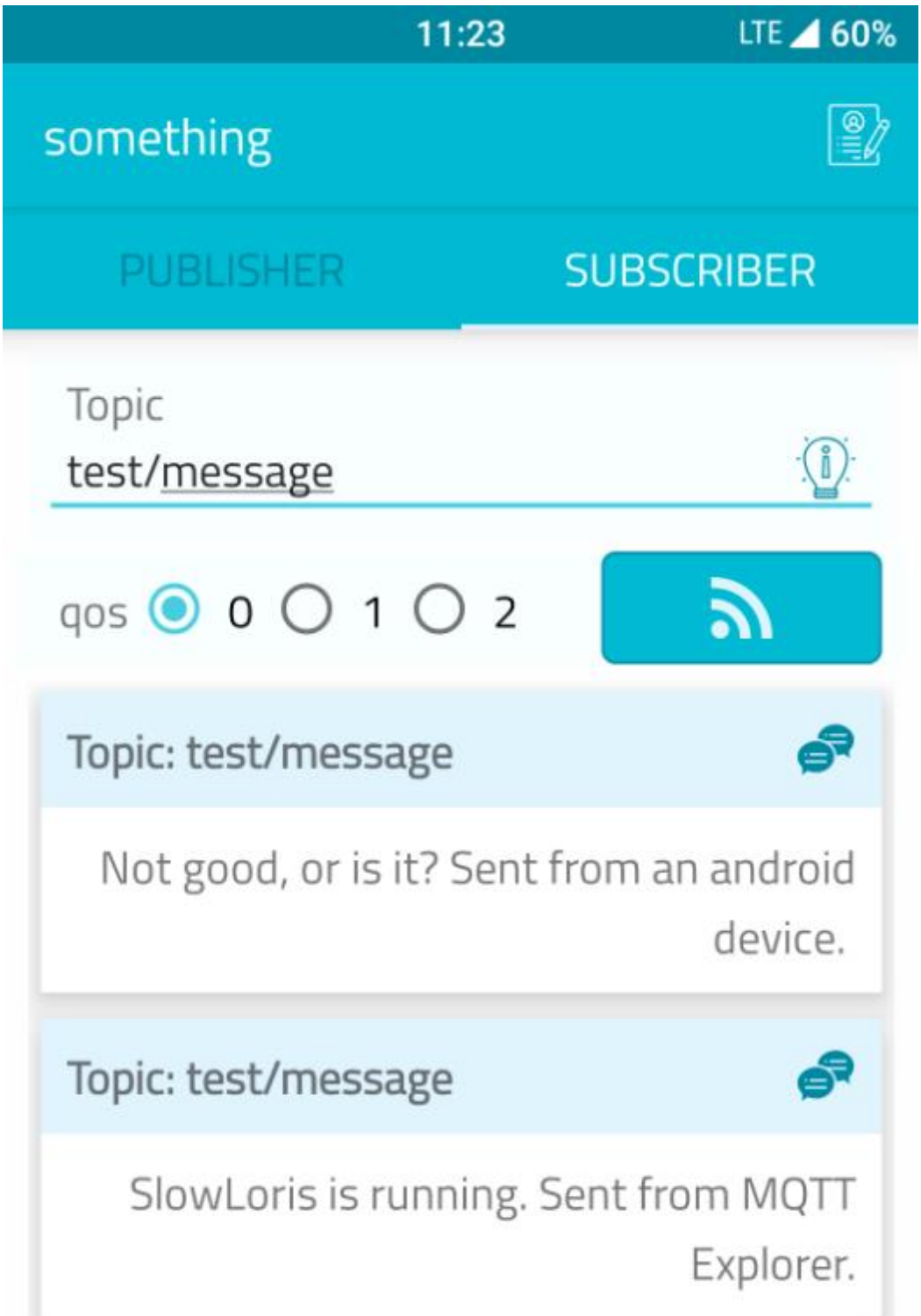
Αφού ξεκινήσει η επίθεση, επιχειρούμε να συνδεθούμε στον broker με το MQTT Explorer και το κινητό τηλέφωνο Android. Τυπικά, όταν ένας εξυπηρετητής βρίσκεται υπό την επήρεια της επίθεσης SlowLoris αδυνατεί να απαντήσει σε νέα αιτήματα συνδέσεων και κατά συνέπεια να τις εξυπηρετήσει.



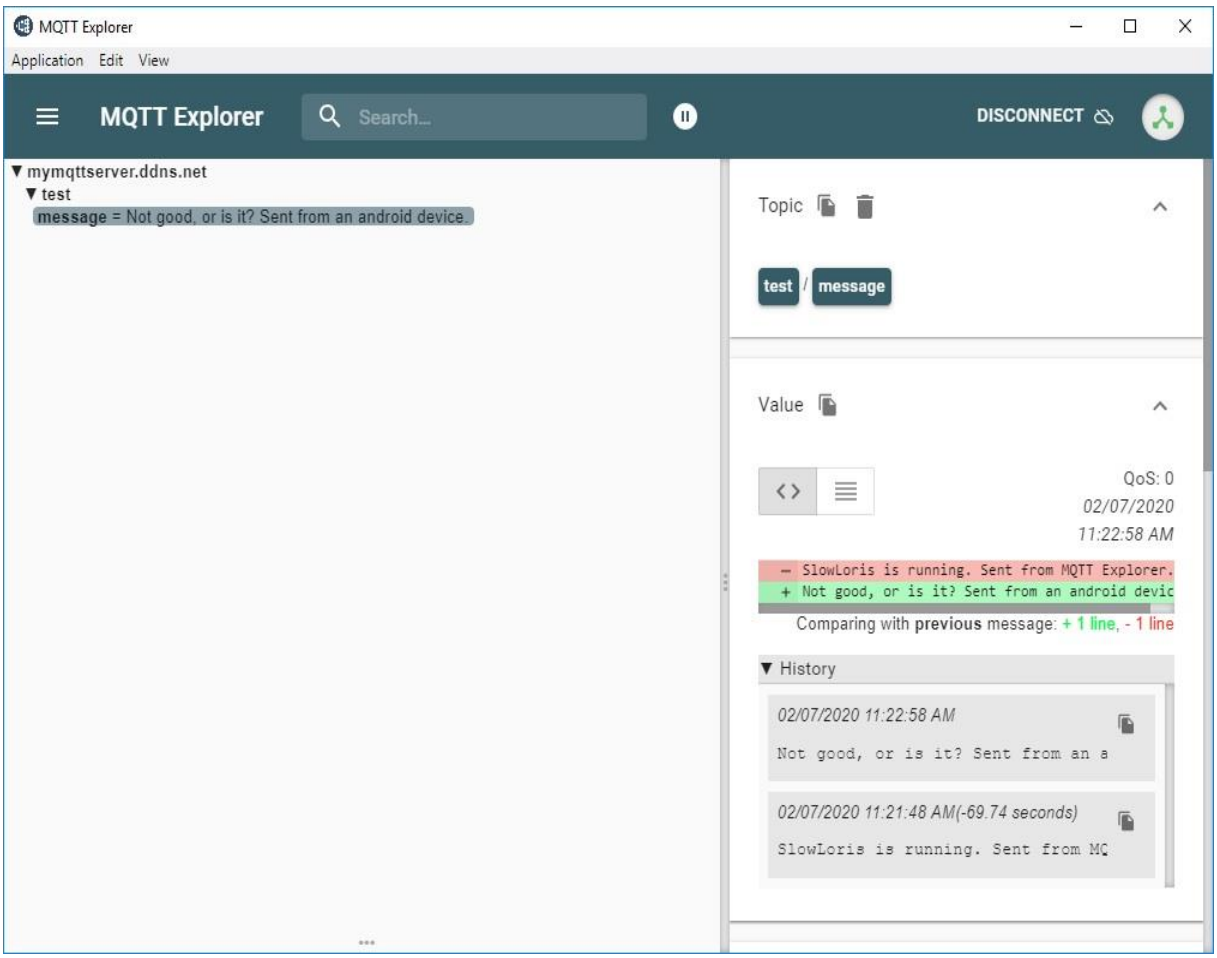
Ο MQTT Explorer συνδέεται αμέσως και στην επάνω δεξιά γωνία της εικόνας διακρίνεται το μήνυμα «Connection health = "online"». Πατώντας «Publish», το μήνυμα «SlowLoris is running. Sent from MQTT Explorer» είναι έτοιμο να αποσταλεί στον broker.



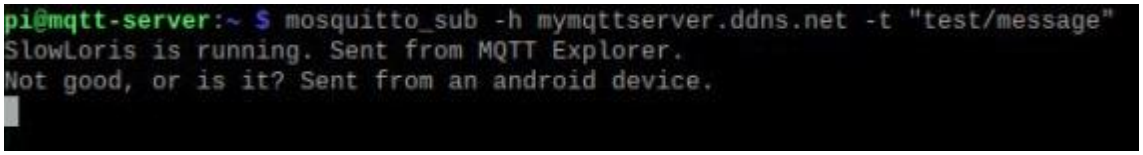
Ούτε το κινητό τηλέφωνο αντιμετώπισε προβλήματα σύνδεσης στον broker και λαμβάνει το μήνυμα του MQTT Explorer.



Το κινητό τηλέφωνο απαντά στον MQTT Explorer μέσω του broker.



Τα μηνύματα ανταλλάχθηκαν επιτυχώς από την πλευρά του MQTT Explorer.



Επιβεβαίωση της μετάδοσης μηνυμάτων και από τον ίδιο τον broker.

```
max_connections 5

allow_anonymous true

#password_file /etc/mosquitto/passwd
```

Οι ρυθμίσεις του αρχείου «mosquitto.conf» επιτρέπουν τις ανώνυμες συνδέσεις χωρίς να απαιτείται συνδυασμός ονόματος χρήστη/κωδικός πρόσβασης. Επίσης ο αριθμός των μέγιστων συνδέσεων έχει τροποποιηθεί, με μέγιστο όριο τις πέντε (5). Οι ρυθμίσεις αυτές έγιναν με σκοπό τη μεγιστοποίηση του αποτελέσματος της επίθεσης.

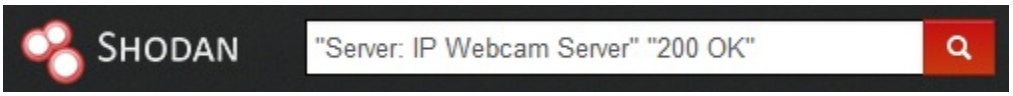
Όπως γίνεται αντιληπτό, ο MQTT broker δεν συνάντησε κανένα εμπόδιο στην εκτέλεση των εργασιών του. Το κινητό τηλέφωνο και ο MQTT Explorer συνδέθηκαν ταχύτατα, αφού φυσικά είχε ξεκινήσει να εκτελείται πρώτα η επίθεση. Αυτό οφείλεται στο γεγονός πως το MQTT λόγω της φύσης του ως ελαφρύ πρωτόκολλο επικοινωνίας, επιτρέπει θεωρητικά τη διαχείριση απεριόριστου αριθμού συνδέσεων. Ακόμη, στην περίπτωση που υπήρχε πρόβλημα για τον broker λόγω του ορίου συνδέσεων που μπορεί να τεθεί, η σουίτα MQTT προσφέρει τη ρύθμιση «max_connections -1» που αλλάζει το όριο του μέγιστου αριθμού συνδέσεων σε άπειρες.

Dorking (Shodan/Google dorks).

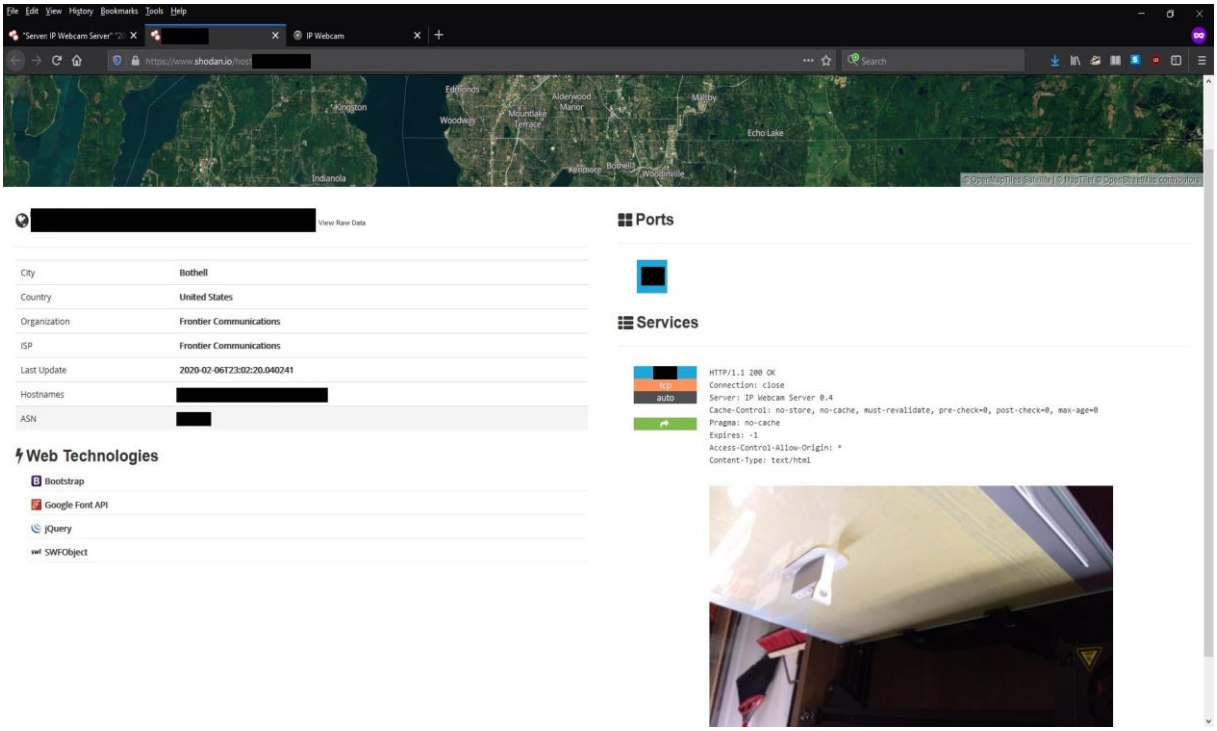
Τα παραπάνω πειράματα δεν σημαίνουν ότι οι συσκευές IoT είναι άτρωτες. Όπως αναφέρθηκε και νωρίτερα στην εργασία, το IoT υποφέρει από τις δικές του δικτυακές αδυναμίες, συν τις αδυναμίες του πρωτοκόλλου TCP στο οποίο έχει τα θεμέλιά του. Πολλές από αυτές τις διασυνδεδεμένες συσκευές είναι αναζητήσιμες και μπορούν να ευρεθούν από κατάλληλες μηχανές αναζήτησης με κατάλληλα κριτήρια.

Μηχανή αναζήτησης Shodan (Shodan search engine, https://www.shodan.io).

Το Shodan σχεδιάστηκε από τον John Matherly το 2009. Είναι μια μηχανή αναζήτησης για συσκευές συνδεδεμένες στο Διαδίκτυο αλλά διαφέρει πολύ από μηχανές αναζήτησης περιεχομένου όπως το Google, το Bing, το Yahoo κ.α. Οι τυπικές μηχανές αναζήτησης ανιχνεύουν δεδομένα σε ιστοσελίδες και τοποθετούν αυτά τα δεδομένα σε ένα ευρετήριο προς αναζήτηση. Το Shodan, κάνει αναζήτηση σε θύρες και λαμβάνει τις σημαίες (flags/banners) που προκύπτουν, και μετά τοποθετεί τις σημαίες σε ευρετήριο αντί του περιεχομένου. Οι σημαίες είναι πληροφορίες σε μορφή κειμένου που περιγράφουν τις υπηρεσίες/χαρακτηριστικά μιας συσκευής. Το περιεχόμενο της σημαίας διαφέρει ανάλογα με τις υπηρεσίες/χαρακτηριστικά της συσκευής. Ένα παράδειγμα μιας αναζήτησης μέσω του Shodan φαίνεται παρακάτω.



Πεδίο αναζήτησης του Shodan. Το κριτήριο που έχει τεθεί θα εμφανίσει όλες τις κάμερες που είναι συνδεδεμένες με εξυπηρετητές Android.



Ένα από τα αποτελέσματα αναζήτησης. Πρόκειται για μία κάμερα η οποία δεν έχει κανενός είδους προστασία και μεταδίδει ζωντανά στιγμιότυπα. Για λόγους προστασίας του κατόχου, οι διευθύνσεις IP και η θύρα είναι κρυμμένες στην εικόνα.

Η σημαία HTTP του συγκεκριμένου αποτελέσματος είναι:

- HTTP/1.1 200 OK
- Connection: close
- Server: IP Webcam Server 0.4
- Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
- Pragma: no-cache
- Expires: -1
- Access-Control-Allow-Origin: *
- Content-Type: text/html

Είναι δυνατή και η χρήση τελεστών άλγεβρας Boole για να συμπεριληφθούν ή να εξαιρεθούν όροι αναζήτησης. Εκτός από τη σημαία HTTP, το Shodan περιλαμβάνει και μετά-δεδομένα (metadata) σχετικά με τη συσκευή όπως γεωγραφική θέση, τη διεύθυνση IP, το όνομα της συσκευής στο δίκτυο, τη θύρα, το λειτουργικό σύστημα κ.α. Το Shodan επιτρέπει την ταξινόμηση των αποτελεσμάτων σύμφωνα με τους παραπάνω όρους. Τα μετά-δεδομένα του παραπάνω αποτελέσματος αναζήτησης φαίνονται παρακάτω.

City	**Bothell**
Country	**United States**
Organization	**Frontier Communications**
ISP	**Frontier Communications**
Last Update	**2020-02-06T23:02:20.040241**
Hostnames	[redacted]
ASN	[redacted]

Ορισμένα από τα στοιχεία τοποθεσίας της κάμερας που βρέθηκε μέσω του Shodan.

Μία από τις πιο τρομακτικές χρήσεις του Shodan είναι η εύρεση συστημάτων SCADA (Supervisory Control And Data Acquisition) τα οποία έχουν δικτυακή διεπαφή (web interface). Τέτοιες συσκευές ρυθμίζουν τη λειτουργία του δικτύου ηλεκτροδότησης, το πότισμα φυτών, εργοστάσια πυρηνικής ενέργειας κ.α. Τα συστήματα SCADA είναι οι πιο πιθανοί στόχοι σε περιπτώσεις κυβερνο-τρομοκρατίας, όπου οι αντίπαλοι προσπαθούν ο ένας να απενεργοποιήσει την υποδομή του άλλου και αντίστροφα, το να έχει κάποιος ανεμπόδιστη πρόσβαση στις ρυθμίσεις παροχής ηλεκτρικής ενέργειας κάνει την διαδικασία αυτή πάρα πολύ εύκολη. Το Shodan, παρόλο που είναι ένα επικίνδυνο εργαλείο, αποτελεί ζωντανή απόδειξη του τι μπορεί να συμβεί όταν συσκευές με ελλιπή μέτρα ασφαλείας έρχονται στη ζωή μας. Με μία γρήγορη αναζήτηση μπορεί κάποιος να ανακαλύψει ευπαθείς web κάμερες από σχολεία μέχρι εργοστάσια ή κάμερες για την επίβλεψη μικρών παιδιών. Η ανεπαρκής ασφάλεια που υπάρχει σε αυτές τις συσκευές, έγκειται στο ότι οι καταναλωτές προκειμένου να κάνουν τη δουλειά τους, αγοράζουν τις φθηνότερες συσκευές και αυτό συχνά έχει αρνητική επίπτωση στην ασφάλειά τους.

Google Dorks

Μία ακόμα κοινή μέθοδος για την εύρεση ευάλωτων συσκευών, είναι η χρήση της μηχανής αναζήτησης Google. Είτε χρησιμοποιώντας ειδικούς όρους αναζήτησης στο περιβάλλον του Google, είτε χρησιμοποιώντας ήδη δημοσιευμένα αποτελέσματα από Google Dorks, γίνεται δυνατή η ανακάλυψη και απόκτηση πρόσβασης σε τρωτές συσκευές IoT. Το Google Dorking ή αλλιώς γνωστό ως Google Hacking επιτρέπει στο χρήστη να αποκτήσει πληροφορίες που θα ήταν δύσκολο να βρεθούν με απλούς όρους αναζήτησης. Αυτό περιλαμβάνει πληροφορίες που δεν προορίζονται για προβολή στο κοινό αλλά δεν έχουν προστατευθεί επαρκώς. Το Google Dorking είναι μια παθητική μέθοδος επίθεσης και είναι ικανή να ανακτήσει ονόματα χρηστών, κωδικούς πρόσβασης και πληροφορίες για τρωτά σημεία. Παρακάτω, φαίνονται μερικές από τις προχωρημένες παραμέτρους αναζήτησης:

- intitle, allintitle
- inurl, allinurl
- filetype
- allintext
- site
- link
- inanchor
- daterange
- cache
- info
- related

Και μερικά παραδείγματα χρήσης αυτών:

- «intitle:Google» Αυτός ο όρος αναζήτησης επιστρέφει αποτελέσματα σελίδων που έχουν τη λέξη «Google» στον τίτλο τους.
- «Example Query site:Google.com» Με αυτόν τον όρο αναζήτησης γίνεται έρευνα αποτελεσμάτων για τον όρο «Example Query» μόνο από την ιστοσελίδα Google.com.
- «intitle: “index of” “backup files”» Αυτός ο όρος εμφανίζει αποτελέσματα που στον τίτλο τους περιλαμβάνουν τη λέξη «index of» (κατάλογος του) στον τίτλο, και τη λέξη «backup files» (αντίγραφα ασφαλείας) οπουδήποτε στη σελίδα. Δηλαδή ο όρος «intitle» εφαρμόζεται μόνο στην πρώτη λέξη/φράση που τον ακολουθεί. Ο όρος «backup files» μπορεί να είναι σε οποιοδήποτε σημείο της σελίδας π.χ. στον τίτλο, στην διεύθυνση, στο κείμενο κ.ο.κ.

Η επίθεση στον πάροχο υπηρεσιών DNS, Dyn το 2016.

Την 21η Οκτωβρίου του 2016, ο πάροχος υπηρεσιών DNS Dyn δέχτηκε επίθεση άρνησης εξυπηρέτησης από συσκευές botnet (δίκτυο αυτοματοποιημένων υπολογιστών) μολυσμένες με το κακόβουλο λογισμικό Mirai. Η επίθεση έγινε σε τρεις χρονικές ζώνες της ίδιας ημέρας με συνολική διάρκεια περίπου πέντε (5) ωρών. Η επίθεση έγινε αισθητή σε μεγάλη έκταση των Ηνωμένων Πολιτειών της Αμερικής, με μεγαλύτερο αντίκτυπο στην Ανατολική Ακτή και σε πολύ μικρότερο βαθμό, στην Ευρώπη. Οι συσκευές που αποτέλεσαν το botnet ήταν στο μεγαλύτερο μέρος, συσκευές IoT όπως εκτυπωτές, web κάμερες, ενδοεπικοινωνίες επιτήρησης μικρών παιδιών, οικιακοί δρομολογητές κ.α. Το κακόβουλο λογισμικό Mirai αφού εγκατασταθεί σε μια συσκευή, η συσκευή αυτή μετά θα αποστείλει πολλαπλά πακέτα TCP SYN σε ψευδο-τυχαίες διευθύνσεις IPv4 στις θύρες 23 και 2323. Το λογισμικό διαθέτει λίστα διευθύνσεων IPv4 τις οποίες απαγορεύεται να μολύνει π.χ. ιδιωτικών δικτύων και διευθύνσεις που χρησιμοποιούνται από το Υπουργείο Αμύνης των Η.Π.Α. και την Ταχυδρομική Υπηρεσία των Η.Π.Α. Εάν μια συσκευή IoT απαντήσει στο TCP SYN, η επίθεση περνά στην φάση της βεβιασμένης απόκτησης πρόσβασης (Brute-Force Login Mode), όπου δοκιμάζονται προδιαγεγραμμένοι συνδυασμοί ονομάτων χρηστών και κωδικών πρόσβασης από μία λίστα στοιχείων εισόδου. Εάν η είσοδος του Mirai στην συσκευή είναι επιτυχής τότε το Mirai στέλνει στον εξυπηρετητή συλλογής στοιχείων τη διεύθυνση IP του θύματος καθώς και τον συνδυασμό ονόματος χρήστη/κωδικού πρόσβασης που του επέτρεψαν πρόσβαση. Η λίστα στοιχείων εισόδου περιέχει περισσότερους από 60 γνωστούς συνδυασμούς εργοστασιακών ονομάτων χρήστη/κωδικών πρόσβασης από μεγάλη γκάμα κατασκευαστών και συσκευών. Εκτιμάται πως περισσότερες από εκατό χιλιάδες (100.000) συσκευές έλαβαν μέρος σε μία οργανωμένη και πολύπλοκη επίθεση, δημιουργώντας σύμφωνα με ισχυρισμούς, έναν χείμαρρο δικτυακής κίνησης της τάξεως του 1,2 Tbps (1,2 Terabits per second) που προκάλεσε υπερχείλιση των εξυπηρετητών της Dyn και εκτιμώμενες οικονομικές ζημιές περίπου εκατόν-δέκα εκατομμυρίων δολαρίων Αμερικής (US $110.000.000).

Η «έξυπνη» παιδική κούκλα «My Friend Cayla».

Τον Φεβρουάριο του 2017 η Γερμανική Ομοσπονδιακή Υπηρεσία Τηλεπικοινωνιών (Bundesnetzagentur), προειδοποίησε γονείς που είχαν αγοράσει την κούκλα «My Friend Cayla» να την καταστρέψουν ειδάλλως θα πλήρωναν βαρύτατα πρόστιμα. Ερευνητές ασφαλείας ανακάλυψαν πως οι επιτιθέμενοι μπορούσαν να χρησιμοποιήσουν την μη ασφαλή συσκευή Bluetooth που βρίσκεται ενσωματωμένη στο παιχνίδι, ώστε να ακούσουν αλλά και να μιλήσουν στο παιδί που χρησιμοποιεί το παιχνίδι. Το παιχνίδι όμως έχει δυνατότητα σύνδεσης στο Διαδίκτυο προκειμένου να απαντά σε ερωτήσεις των παιδιών. Ευπάθειες στο λογισμικό του παιχνιδιού εμφανίστηκαν για πρώτη φορά τον Ιανουάριο του 2015.

Επιθέσεις σε συστήματα «έξυπνων» κλειδαριών.

Ο χρήστης του YouTube, LockPickingLawyer δοκίμασε να παρακάμψει δύο συστήματα: το ένα, μία «έξυπνη» κλειδαριά και το δεύτερο, ένας «έξυπνος» συναγερμός. Όπως φαίνεται και στα βίντεο που ακολουθούν, καταφέρνει με επιτυχία να υπερνικήσει τους μηχανισμούς που είχαν σχεδιάσει οι κατασκευαστές με τρομακτική ευκολία και χωρίς να χρειάζεται ειδικός εξοπλισμός ή γνώσεις. Σημειώνεται πως ο χρήστης εκτέλεσε τα πειράματα στο χώρο της οικίας του με σκοπό να εξετάσει την ασφάλεια των συστημάτων και να προτείνει τρόπους με τους οποίους μπορεί να βελτιωθεί:

[935] SimpliSafe Alarm Bypassed With a $2 Device From Amazon
[1040] Fingerprint/RFID Lock Defeated With a Paperclip (Mengqi-Control)

Affected services [edit]

Services affected by the attack included:

- Airbnb[12]
- Amazon.com[9]
- Ancestry.com[13][14]
- *The A.V. Club*[15]
- BBC[14]
- *The Boston Globe*[12]
- Box[16]
- *Business Insider*[14]
- CNN[14]
- Comcast[17]
- CrunchBase[14]
- DirecTV[14]
- *The Elder Scrolls Online*[14][18]
- Electronic Arts[17]
- Etsy[12][19]
- FiveThirtyEight[14]
- Fox News[20]
- *The Guardian*[20]
- GitHub[12][17]
- Grubhub[21]
- HBO[14]
- Heroku[22]
- HostGator[14]
- iHeartRadio[13][23]
- Imgur[24]
- Indiegogo[13]
- Mashable[25]
- National Hockey League[14]
- Netflix[14][20]
- *The New York Times*[12][17]
- Overstock.com[14]
- PayPal[19]
- Pinterest[17][19]
- Pixlr[14]
- PlayStation Network[17]
- Qualtrics[13]
- Quora[14]
- Reddit[13][17][19]
- Roblox[26]
- Ruby Lane[14]
- *RuneScape*[13]
- SaneBox[22]
- Seamless[24]
- *Second Life*[27]
- Shopify[12]
- Slack[24]
- SoundCloud[12][19]
- Squarespace[14]
- Spotify[13][17][19]
- Starbucks[13][23]
- Storify[16]
- Swedish Civil Contingencies Agency[28]
- Swedish Government[28]
- Tumblr[13][17]
- Twilio[13][14]
- Twitter[12][13][17][19]
- Verizon Communications[17]
- Visa[29]
- Vox Media[30]
- Walgreens[14]
- *The Wall Street Journal*[20]
- Wikia[13]
- *Wired*[16]
- Wix.com[31]
- WWE Network[32]
- Xbox Live[33]
- Yammer[24]
- Yelp[14]
- Zillow[14]

Υπηρεσίες που χτυπήθηκαν από μερίδα συσκευών IoT του Mirai botnet. (Πηγή: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack)

Συμπεράσματα.

Το IoT παρουσιάζει μία πληθώρα απειλών που πρέπει να ληφθούν υπόψιν από τους σχεδιαστές ασφαλείας και τους κατασκευαστές. Παρουσιάστηκαν οι τομείς που πρέπει να λαμβάνονται υπόψη, καθώς επίσης και τα πιθανά μοντέλα επίθεσης σε ένα σύστημα IoT από το επίπεδο δικτύου μέχρι το φυσικό επίπεδο. Δόθηκε περισσότερη έμφαση στο δικτυακό μέρος της ασφάλειας διασυνδεδεμένων συσκευών IoT σε σχέση με τους τομείς της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Το Shodan ως μία μηχανή αναζήτησης IoT συσκευών, μπορεί εύκολα να εκθέσει ευπαθείς συσκευές, στις οποίες μπορεί κάποιος επιτιθέμενος να προξενήσει ζημιές ή να εκμεταλλευτεί χωρίς να απαιτούνται πολλές γνώσεις. Το IoT είναι πολύ κοντά στο να εφαρμοστεί στην καθημερινότητα, περισσότερο από όσο μπορεί κάποιος να φανταστεί. Οι περισσότερες τεχνολογίες που το θεμελιώνουν έχουν βρεθεί και εφαρμοστεί, και μερικοί κατασκευαστές έχουν ήδη υλοποιήσει ένα μικρό κομμάτι του. Οι κύριοι λόγοι που δεν έχει βρει πλήρη εφαρμογή είναι η επίπτωση που θα έχει στα νομικά και ηθικά ζητήματα καθώς και στο κομμάτι της ασφάλειας. Για παράδειγμα, οι εργαζόμενοι μπορούν εύκολα να κάνουν κατάχρηση των συσκευών, οι επιτιθέμενοι να αποκτήσουν πρόσβαση σε αυτές, οι εταιρείες να μην θέλουν να διαμοιραστούν τις πληροφορίες τους και το καταναλωτικό κοινό να είναι ενάντια στην πλήρη έλλειψη ιδιωτικότητας. Συνεπώς, η πλήρης εφαρμογή του IoT μπορεί να καθυστερήσει παραπάνω από όσο χρειάζεται.

Πηγές.

Επιστημονικά άρθρα, βιβλία και case studies:

1. "A Lightweight Multi-tier S-MQTT Framework to Secure Communication between low-end IoT Nodes" των Shanto Roy, M. Shamim Kaiser και Md. Shahidul Islam.
2. "Attack scenarios and security analysis of MQTT communication protocol in IoT system" του Bagus Hanindhito.
3. "Introducing Usage Control in MQTT protocol for IoT" των Αθανάσιου Ρίζου, Paolo Mori, Andrea Saracino, Antonio La Marra και Fabio Martinelli.
4. "Detecting Attacks Against The Internet of Things" του Adam Kliarsky.
5. "IoT from cyber security perspective" του Ville Sulkamo.
6. "IoT – OAS: An Oauth-Based Authorization Service Architecture for Secure Services in IoT Scenarios" των Simone Cirani, Pietro Gonizzi, Marco Picone και Gianluigi Ferrari.
7. "Διάλεξη MQ Telemetry Transport (MQTT)" του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.
8. "Mitigating DoS attacks in publish-subscribe IoT networks" των Bogdan-Cosmin Chifor και Victor-Valeriu Patriciu.
9. "New approach for securing communication over MQTT protocol. A comparison between RSA and Elliptic Curve" των Abdessamad Mektoubi, Hicham Lalaoui Hassani, Hicham Belhadaoui και Mounir Rifi.
10. "On the Security of the MQTT Protocol" του Benjamin Aziz.
11. "Secure MQTT using AES for Smart Homes in IoT Network" των B.K.S. Rajaram και Krishna Prakash N.
12. "Security analysis for MQTT in Internet of Things" του Diego Salas Ugalde.
13. "Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices" των Dan Dinculeana και Xiaochun Cheng.
14. "A comprehensive Study of Security and Privacy. Guidelines, Threats and Countermeasures: An IoT Perspective" των Δημήτριου Κωνσταντά και Hezam Akram Abdul-Ghani.
15. "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms" των Tariq Ahamed Ahanger και Abdullah Aljumah.
16. "Security Issuew in the Internet of Things (IoT): A Comprehensive Study" των Mirza Abdur Razzaq, Sajid Habig Gill, Saleem Ullah και Muhammad Ali Qureshi.
17. "Towards Security on Internet of Things: Applications and Challenges in Technology" των Kazi Masum Sadique, Rahim Rahmani και Paul Johannesson.
18. "Internet of Things. Security and Data Protection" του Sebastien Ziegler για τις εκδόσεις Springer (2019).
19. "Internet of Things for Smart Cities. Technologies, Big Data and Security." των Waleez Ejaz και Alagan Anpalagan για τις εκδόσεις Springer (2019).
20. "Security Challenges and Approaches in Internet of Thinhs" των Sridipta Misra, Muthucumaru Maheswaran και Salman Hashmi για τις εκδόσεις Springer (2019).
21. "Internet of Things. From Hype to Reality. The Road to Digitization." των Ammar Rayes και Samer Salam για τις εκδόσεις Springer (2019).
22. "Managing Access Control for Things: a Capability Based Approach" των Domenico Rotondi και Salvatore Piccione.
23. "Federated Identity and Access Management for the Internet of Things" των Paul Fremantle, Philip Scott και Benjamin Aziz.

24. “The Fragility of Industrial IoT's Data Backbone” των Federico Maggi, Rainer Vosseler και Davide Quarta.
25. “Lightweight & Secure Industrial IoT Communications via the MQ Telemetry Transport Protocol” των Σωτήριου Κατσικέα, Ανδρέα Μιαουδάκη, Κωνσταντίνου Φυσαράκη και Amaury Van Bemtem.
26. “Usage control in computer security: A survey” των Aleksandr Lazouski, Fabio Martinelli και Paolo Mori.
27. “Security and Fault Tolerance in Internet of Things” των Rajat Subhra Chakraborty, Jimson Mathew και Αθανάσιου Β. Βασιλάκου για τις εκδόσεις Springer (2019).
28. “Internet of Things Security. Challenges, Advances and Analytics” των Patel Chintan και Nishant Doshi για τις εκδόσεις CRC Press (2019).
29. “Security and Privacy Challenges in the Internet of Things” του Christoph P. Mayer.
30. “Internet of Things Security: Layered classification of attacks and possible Countermeasures” των Otmane El Mouaatamid, Mohammed Lahmer και Mostafa Belkasmi.
31. “Towards A Layered and Secure Internet-of-Things Testbed via Hybrid Mesh” των Tyler Jones, Aniket Dali, Manoj Ramesh Rao, Neha Biradar, Jean Madassery και Kaikai Liu.
32. “Computer Security and Cryptography” του Alan G. Konheim για τις εκδόσεις Wiley (2007).
33. “Computer Networks – Fifth Edition” των Andrew S. Tanenbaum και David J. Wetherall για τις εκδόσεις Prentice Hall (2010).
34. “Data Communications And Networking – Fourth Edition” των Behrouz A. Forouzan και Sophia Chung Fegan για τις εκδόσεις McGraw Hill (2007).
35. “Cryptography and Network Security – Seventh Edition” του William Stallings για τις εκδόσεις Pearson (2017).
36. “Cryptography Engineering: Design Principles and Practical Applications” των Neils Ferguson, Bruce Schneier και Tadayoshi Kohno για τις εκδόσεις Wiley (2010).

Ιστοσελίδες:

1. https://en.wikipedia.org/wiki/Personal_computer#History
2. http://openbookproject.net/courses/intro2ict/history/history.html
3. https://en.wikipedia.org/wiki/Internet
4. https://en.wikipedia.org/wiki/History_of_the_Internet
5. https://en.wikipedia.org/wiki/Global_Internet_usage
6. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-018-0123-6
7. 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
8. https://en.wikipedia.org/wiki/Internet_of_things
9. https://el.wikipedia.org/wiki/%CE%9C%CE%BF%CE%BD%CF%84%CE%AD%CE%BB%CE%BF_%CE%B1%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82_OSI
10. http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/diktya_ypolog_G_2018_final/m_osi.html
11. https://el.wikipedia.org/wiki/TCP/IP
12. https://www.digitalocean.com/community/tutorials/an-introduction-to-networking-terminology-interfaces-and-protocols

13. https://www.liveaction.com/docs/glossary/glossary-of-network-terms/
14. https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B5%CF%8D%CE%B8%CF%85%CE%BD%CF%83%CE%B7_IP
15. https://el.wikipedia.org/wiki/IEEE_802.11
16. https://en.wikipedia.org/wiki/Wi-Fi
17. https://www.microcontrollertips.com/terminology-used-in-the-internet-of-things/
18. https://www.link-labs.com/35-top-iot-terms-you-need-to-know
19. https://dzone.com/articles/iot-glossary-terms-you-need-to-know
20. https://el.wikipedia.org/wiki/NFC
21. https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/
22. https://el.wikipedia.org/wiki/%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CF%8C_%CE%BD%CE%AD%CF%86%CE%BF%CF%82
23. https://www.smartcitiesworld.net/news/news/smart-cities-services-worth-225bn-by-2026-1618
24. https://www.researchgate.net/figure/An-illustration-of-traffic-modeling-for-an-IoT-based-smart-city_fig2_316240064
25. https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building
26. https://twitter.com/humanwareonline/media
27. https://www.industryweek.com/technology/dawn-smart-factory
28. https://www.researchgate.net/figure/Shows-an-example-of-product-and-data-flow-in-a-Smart-Factory-Product-carries-RFID-tag_fig1_327884684
29. http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/#show_infographic
30. https://www.ibtimes.com/cisco-internet-everything-ioe-16-trillion-retail-opportunity-1542910
31. https://blogs.intel.com/iot/2015/09/02/intelligent-driving-experience-a-ride-with-intel-internet-of-things/
32. https://www.rfpage.com/scope-rf-technology-internet-of-things/
33. https://www.sierrawireless.com/iot-blog/iot-blog/2016/05/top-3-keys-for-automakers-to-succeed-in-connected-services/
34. https://smartamerica.org/teams/closed-loop-healthcare/
35. https://blog.phoenixcontact.com/marketing-sea/2017/04/smart-grids-how-automation-empowers-the-future-of-electricity/
36. https://en.wikipedia.org/wiki/Smart_grid
37. https://www.nesta.org.uk/feature/precision-agriculture/
38. https://pdfs.semanticscholar.org/4459/f33ccaea17c0e4896accd0bc59da182ccb74.pdf
39. https://en.wikipedia.org/wiki/Cross-site_scripting
40. https://elinux.org/images/f/f8/Common-Attacks-on-IoT-Devices-Christina-Quast.pdf
41. https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot/
42. https://www.channelpartnersonline.com/blog/iot-insecurity-6-common-attacks-and-how-to-protect-customers/
43. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
44. https://www.allot.com/blog/brute-force-attacks-iot/
45. https://www.intellectsoft.net/blog/biggest-iot-security-issues/
46. https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained
47. https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
48. https://jarv.is/notes/shodan-search-queries/

49. https://www.iotworldtoday.com/2017/09/23/iot-device-security-comprehensive-look-edge-cloud/
50. https://blog.malwarebytes.com/101/2017/12/internet-things-iot-security-never/
51. https://el.wikipedia.org/wiki/SYN_flood
52. https://en.wikipedia.org/wiki/TCP_reset_attack
53. https://el.wikipedia.org/wiki/UDP_flood_attack
54. https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle
55. https://www.postexplo.com/forum/security-in-general/terms/510-blind-hijacking
56. https://www.contextis.com/en/blog/server-technologies-https-beast-attack
57. https://en.wikipedia.org/wiki/Padding_oracle_attack
58. https://en.wikipedia.org/wiki/FTP_bounce_attack
59. https://www.cyclonis.com/what-is-ssh-how-hackers-attack/
60. https://en.wikipedia.org/wiki/Cross-site_request_forgery
61. https://en.wikipedia.org/wiki/Slowloris_(computer_security)
62. http://www.iot-vienna.at/global-iot-day-event/2015/lib/exe/fetch.php?media=talks:gieshofer_juergen:owasp_iot_top10.pdf
63. http://events19.linuxfoundation.org/wp-content/uploads/2017/11/Common-Attacks-on-IoT-Devices-OSS-Christina-Quast.pdf
64. https://2017.appsec.eu/presos/Developer/Don%E2%80%99t%20Get%20Caught%20Em-bedFinding%20and%20Preventing%20Vulns%20at%20its%20Lowest%20Level%20-%20Aaron%20Guzma-%20OWASP_AppSec-Eu_2017.pdf
65. http://blog.catchpoint.com/2017/07/06/dissecting-mqtt-using-wireshark/
66. https://www.bbc.com/news/world-europe-39002142
67. https://en.wikipedia.org/wiki/Mirai_(malware)
68. https://www.kaspersky.com/blog/attack-on-dyn-explained/13325/