



Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Επίπεδο: Προπτυχιακό Πρόγραμμα Σπουδών

Μάθημα – Ασφάλεια Κινητών & Ασύρματων Επικοινωνιών

Τίτλος – HackRF – (emulator)

Επιβλέπον Καθηγητής: Χ. Ξενάκης

Ονοματεπώνυμο	E-mail	A.M.
Mikael	mikaeltsakmak@gmail.com	E17152
Ιωάννης Στυλιανού	jsm@hotmail.gr	E17144
Ιωάννης Πιτταροκοίλης	jpitpol@gmail.com	E17125

Πειραιάς
06/08/2021

Περίληψη

Το θέμα αυτής της εργασίας και επομένως ο σκοπός της είναι να βοηθήσει στην κατανόηση της τεχνολογίας του HackRF και ανάλυση των Software Define Radio. Ο τρόπος που εξελίχθηκε η διαδικασία ανάλυσης είναι μέσω παραδειγμάτων από τον πραγματικό κόσμο ώστε να γίνει πιο κατανοητή και απλή. Στη συνέχεια του κειμένου παρουσιάζεται ο τρόπος με τον οποίο λειτουργούν τα συστήματα RFID , τι λειτουργίες παρέχουν και πως το καταφέρνουν. Λέγοντας αυτό θα ήθελα να τονισθεί ότι παρόλο που το κείμενο αυτό αποσκοπεί στην ενημέρωση των φοιτητών, με την εργασία αυτή καθένας θα μπορεί να κατανοήσει τους κινδύνους που υπάρχουν στην τεχνολογία αυτήν, καθώς και τρόπους προστασίας.

Περιεχόμενα

Τι είναι το HackRF	1
Παραδείγματα επιθέσεων	1
Brute Force Attack	1
Replay Attacks	1
Rolling code	2
Jamming Attacks.....	2
Attack on Rolling code	2
Λογισμικό που χρησιμοποιήσαμε	3
Διεξαγωγή επίθεσης	9
Τι είναι το RFID (radio frequency identification)	15
Πειράματα επάνω στις ετικέτες (NFC tags)	16
Με χρήση Arduino	17
Πειράματα επάνω στις τραπεζικές κάρτες	19
Βιβλιογραφία	21

Τι είναι το HackRF

Το HackRF One είναι ένας ραδιοφωνικός πομποδέκτης ραδιοσυχνοτήτων (SDR) με ευρεία ζώνη που δημιουργήθηκε και κατασκευάστηκε από την Great Scott Gadgets. Ο κώδικας του είναι ανοιχτής φύσης για το λογισμικό αλλά και του υλικό του. Το HackRF One έχει τη δυνατότητα λήψης και μετάδοσης σε εύρος συχνοτήτων από 1MHz έως 6GHz.

Παραδείγματα επιθέσεων

Όπως είναι λογικό, ο κάθε ένας που έχει τα απαραίτητα εργαλεία και την γνώση, μπορεί να καταγράψει και να ανάλυση όλα τα ραδιοσήματα που μεταδίδονται στον περίγυρο του. Αυτό μας δίνει την απορία, τι θα μπορούσε ένας κακόβουλος χρήστης να θα μπορούσε να κάνει ενάντιον μας. Παρακάτω θα αναλύσουμε μερικά παραδείγματα από τον αληθινό κόσμο.

Brute Force Attack

Σε μια τέτοια επίθεση ο επιτιθέμενος δεν χρειάζεται να γνωρίζει τίποτα για να επιτεθεί. Φυσικά όσα περισσότερα πράγματα γνωρίζει, τόσο περισσότεροι πιθανότητα έχει για να επιτύχει τον στόχο του, (πχ συχνότητα, μήκος κλειδιού). Ο επιτιθέμενος εδώ προσπαθεί να μαντέψει τον κωδικό με τυχαίο τρόπο δοκιμάζοντας όλους τους πιθανούς συνδυασμούς. Φυσικά αυτό δεν είναι κάτι τόσο αποτελεσματικό, καθώς θα τραβήξει πολλά βλέμματα καίοντας με μια κεραία διπλά σε μια ξένη γκαραζόπορτα. Υπάρχουν τεχνικές που μειώνουν αυτόν τον χρόνο ραγδαία (όπως η ακολουθία De Bruijn).

Replay Attacks

Ένα πολύ βασικό ερώτημα είναι, « θα μπορούσε κάποιος να καταγράψει το σήμα που ξεκλειδώνει την γκαραζόπορτα σας και να το αναμεταδώσει όποτε επιθυμεί εκείνος?». Η απάντηση είναι «Ναι» μπορεί να το κάνει. Όμως τα πράγματα δεν είναι τόσο απλά. Για αρχή θα πρέπει ο δράστης να γνωρίζει την συγγνότητα που μεταδίδει το κλειδί της γκαραζόπορτας (Υπάρχουν standards που οι κατασκευαστές ακολουθούν). Υστέρα θα πρέπει να βρίσκεται σε απόσταση που μπορεί να καταγράψει το σήμα σας, καθώς και να είναι σε ετοιμότητα να το καταγράψει μόλις εσείς το πατήσετε. Θεωρώντας ότι όλα τα παρακάτω έχουν γίνει με επιτυχία και ο δράστης έχει κατεργασμένο το σήμα σας, ακόμη και τότε δεν μπορεί απλός να το μεταδώσει και να λειτουργήσει όπως το κλειδί

σας. Σε αυτήν την φάση ο δράστης θα πρέπει να ανάλυση το σήμα, φιλτράροντας τον θόρυβο που προκύπτει από όλα τα υπόλοιπα σήματα , να ενδυνάμωση το σήμα, και άλλες επεξεργασίες που τείχος χρειαστούν. Εάν υποθέσουμε πως όλα πήγαν σωστά είναι η στιγμή που ο επιτιθέμενος θα μπορεί να ανοιγοκλείνει την γκαραζόπορτα σας όποτε επιθυμεί.

Rolling code

Οι κυλιόμενοι κωδικοί εφευρέθηκαν με σκοπό την αποτρέψει των Replay Attack. Ένας κυλιόμενος κωδικός είναι μια κρυφή συνάρτηση που εμπεριέχετε στους πομπούς και δέκτες (πχ σε μια γκαραζόπορτα και στο ασύρματο κλειδί του), και δημιουργούν νέους κωδικούς κάθε φορά που ένας χρησιμοποιείτε. Φανταστείτε πως κάθε φορά που πατάτε το κλειδί για να ξεκλειδώσετε την γκαραζόπορτα σας, εσωτερικά το κλειδί σας δημιουργεί μέσω της συναρτήσεως το νέο κλειδί και το αποστέλλει. Από την πλευρά του η γκαραζόπορτα δημιουργεί τα επόμενα κλειδιά και τα αντιστοιχεί με αυτό που στείλατε. Όταν ένα κλειδί χρησιμοποιηθεί, αυτό και όλα τα προηγούμενα διαγράφονται από την λίστα που δημιουργείτε μέσω της συνάρτησης. Έτσι όταν εσείς ανοίξετε την γκαραζόπορτα σας και ο επιτιθέμενος καταγράψει το σήμα που μεταδώσατε, δεν θα καταφέρει με κανέναν τρόπο να ανοίξει την γκαραζόπορτα με αυτό το κλειδί, δεν έχει την δυνατότητα ούτε να βρει την συνάρτηση μέσω του κλειδιού που κατέγραψε.

Jamming Attacks

Σε μια τέτοια επίθεση ο επιτιθέμενος δεν έχει (απαραίτητα) τον στόχο του να υποκλέψει κάτι από εμάς, αλλά στο να κάνει να μην μπορούμε ούτε εμείς να χρησιμοποιήσουμε αυτό που θέλουμε. Εδώ ο επιτιθέμενος μεταδίδει με πολύ μεγάλη ισχύ στην συχνότητα που μεταδίδουμε και εμείς με το κλειδί (και στις κοντινές γύρο συχνότητες), με αποτέλεσμα ο δέκτης να μην καταφέρνει να διαβάσει το καθαρό σήμα που μεταδίδουμε εμείς.

Attack on Rolling code

Όλα τα νέα συστήματα που χρησιμοποιούν ραδιοσυχνότητες ως βασική επικοινωνία μεταξύ τους, πλέον χρησιμοποιούν κυλιόμενους κωδικούς. Αυτό είχε ως αποτέλεσμα την εμφάνιση ενός νέου τρόπου επιθέσεις για την υποκλέψει του κλειδιού μετάδοσης. Η επίθεση λειτουργεί ως εξής, ο επιτιθέμενος παρεμποδίζει (jamming) το σήμα που στέλνουμε εμείς, ενώ ταυτόχρονα το καταγραφεί, στην συνέχεια επειδή θεωρούμε πως δεν έπιασε το σήμα αναμεταδίδουμε, και ο επιτιθέμενος καταγραφεί και το δεύτερο

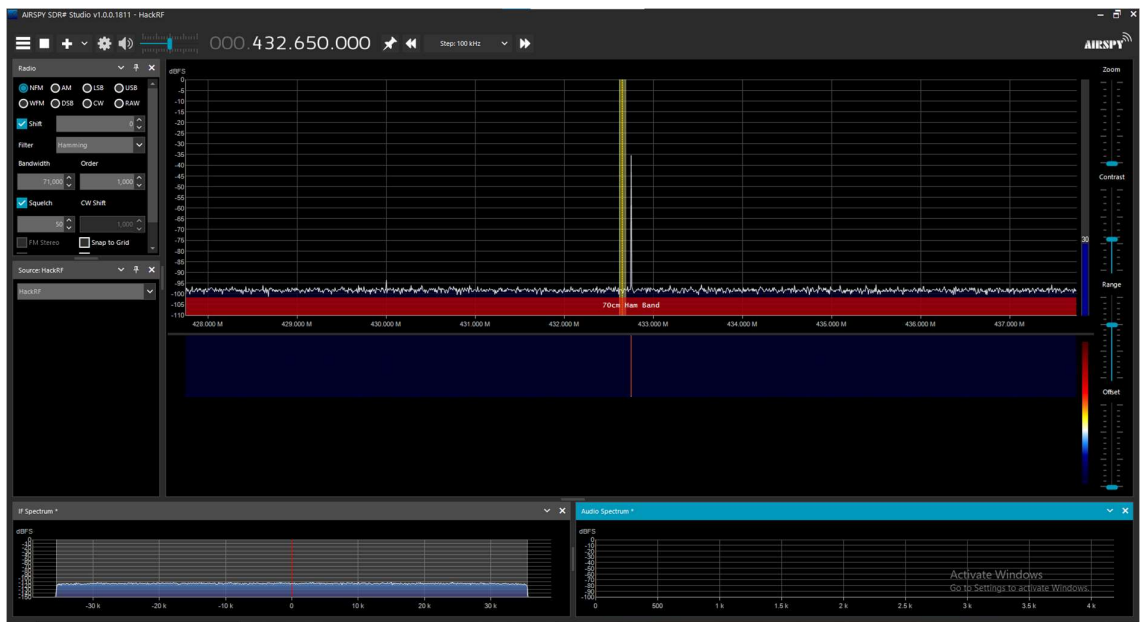
κλειδί. Ταυτόχρονα με την καταγραφή του δευτέρου κλειδιού μεταδίδει το πρώτο κλειδί που κατέγραψε, με αποτέλεσμα ο δέκτης να το λάβει και να ξεκλειδώσει. Τώρα ο επιτιθέμενος έχει καταγεγραμμένο το ακριβώς επόμενο κλειδί που ξεκλειδώνει τον δεκτή και εμείς δεν το γνωρίζουμε, καθώς πιστεύαμε πως απλώς δεν έπιασε το σήμα.

- Λυση

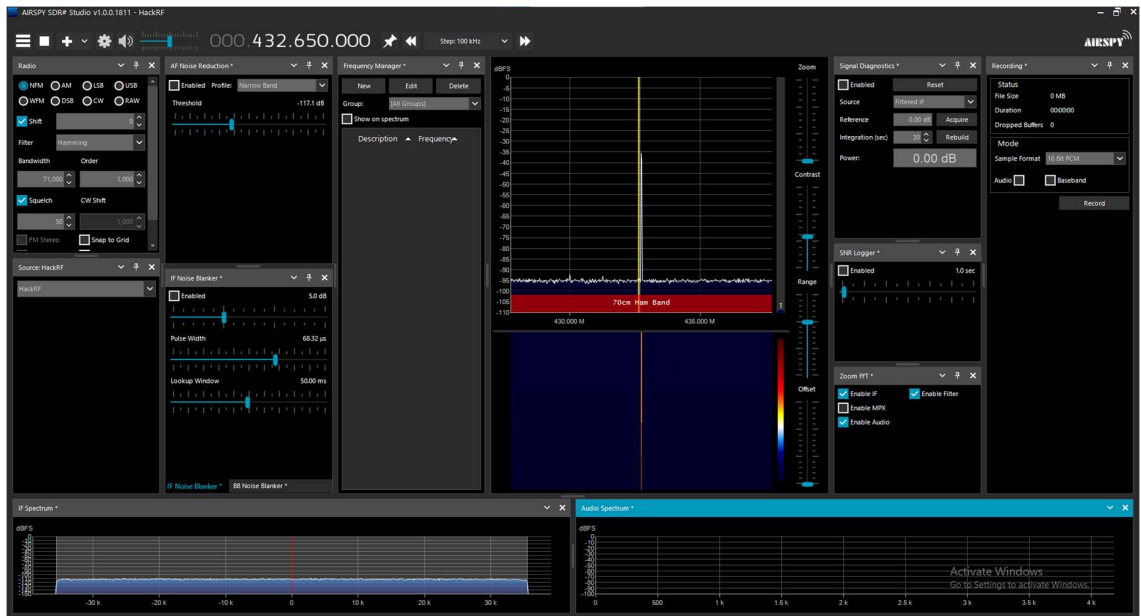
Μια λύση για το πρόβλημα αυτό θα ήταν εκτός των κυλιόμενων κωδίκων να υπάρχει και χρονικό όριο χρήσης του κάθε κωδικού.

Λογισμικό που χρησιμοποιήσαμε

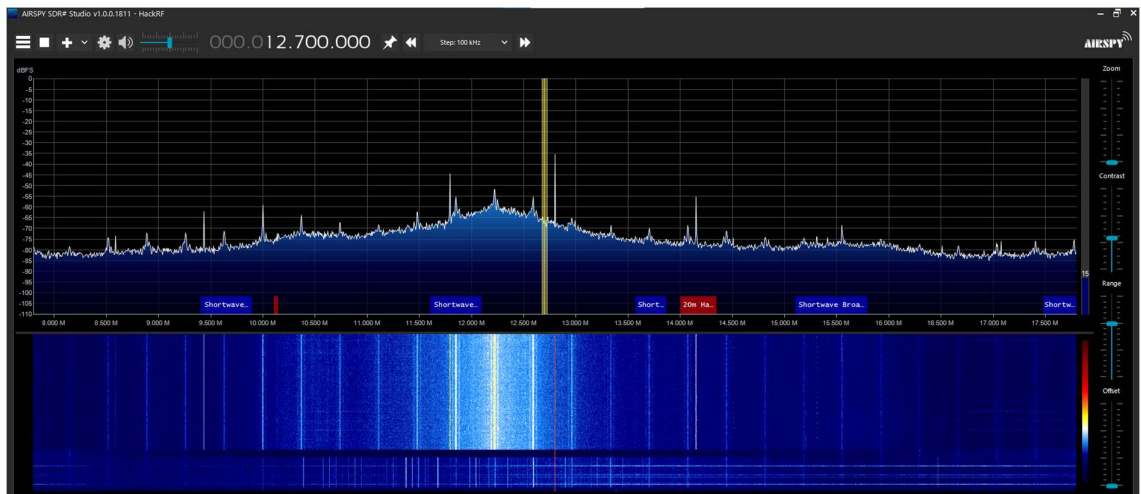
Προκειμένου να αξιοποιήσουμε τις δυνατότητες τους `hackrf` χρησιμοποιήσαμε 3 προγράμματα στο windows λειτουργικό. Αρχικά κατεβάσαμε το **SDR-SHARP** της AIRSPY το οποίο θεωρούμε πως είναι το καταλληλότερο πρόγραμμα προκειμένου να βρούμε την συχνότητα στην οποία υπάρχει η εκπομπή του σήματος που ψάχνουμε. Στο πάνω κομμάτι του προγράμματος εμφανίζεται μία μύτη όταν παρατηρείται ένα έντονο σήμα, επομένως γίνεται εμφανές σε ποια συχνότητα ακριβώς εκπέμπει. Στο μπλέ κομμάτι από κάτω εμφανίζεται ένα λευκό σημάδι το οποίο σημαίνει ότι εκπέμπεται πληροφορία. Σε περίπτωση που υπάρχει μύτη στο πάνω κομμάτι θεωρούμε πως είναι απλά θόρυβος.



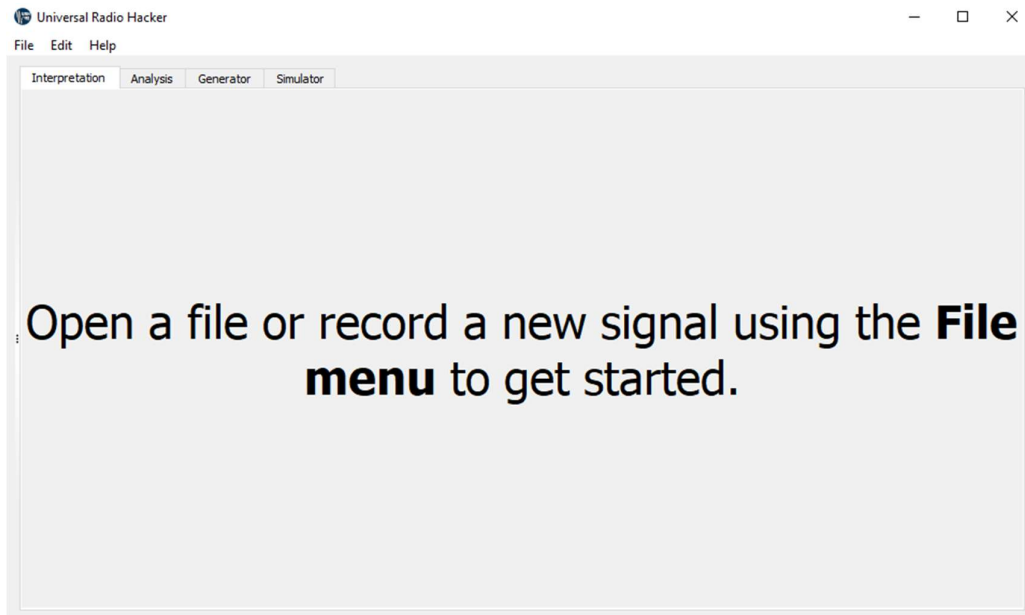
Για περαιτέρω ανάλυση υπάρχουν και διάφορες ρυθμίσεις όμως εμείς δεν χρειάστηκε να πειράζουμε κάποια ρύθμιση για να βρούμε την συχνότητα του σήματος μας.



Ενδεικτικά παρακάτω εμφανίζεται μία χαμηλή συχνότητα που περιέχει πολύ θόρυβο.

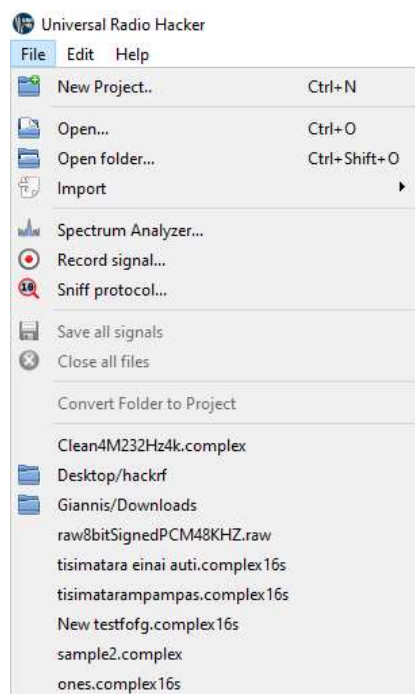


Το δεύτερο πρόγραμμα που χρησιμοποιήσαμε είναι το **Universal Radio Hacker**. Από μόνο του, μπορεί να χρησιμοποιηθεί αποκλειστικά προκειμένου να πραγματοποιηθεί μία ανάλυση και επίθεση όμως θεωρήθηκε πως ο συνδυασμός προγραμμάτων είναι πιο σωστός για ευρύτερη κατανόηση.

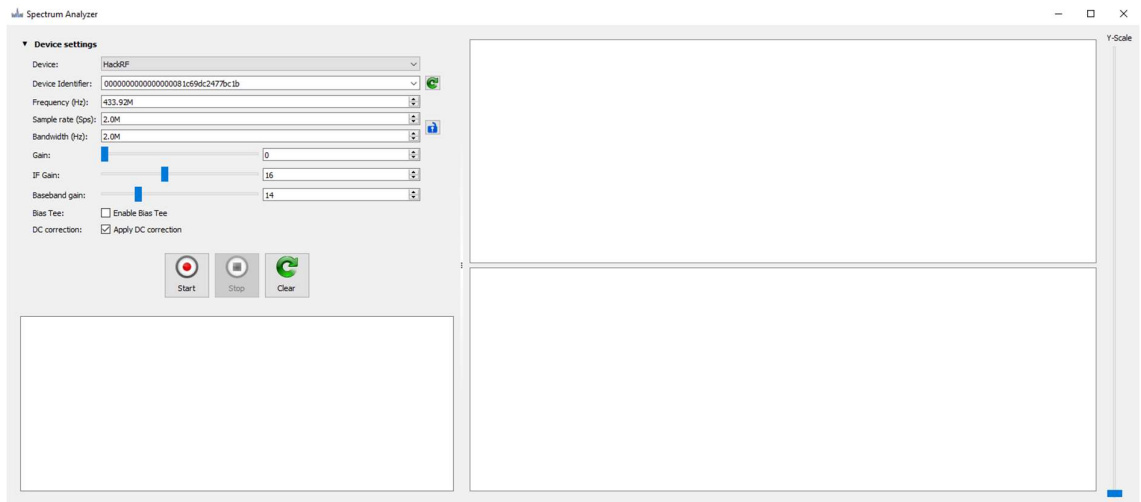


Πηγαίνοντας στο tab file μπορούμε να δούμε τις λειτουργίες του. Μπορούμε να δημιουργήσουμε ένα project, να ανοίξουμε ένα αρχείο/φάκελο αλλά και να import αρχείων. Ωστόσο οι σημαντικές λειτουργίες είναι το Spectrum Analyzer και το record analyzer.

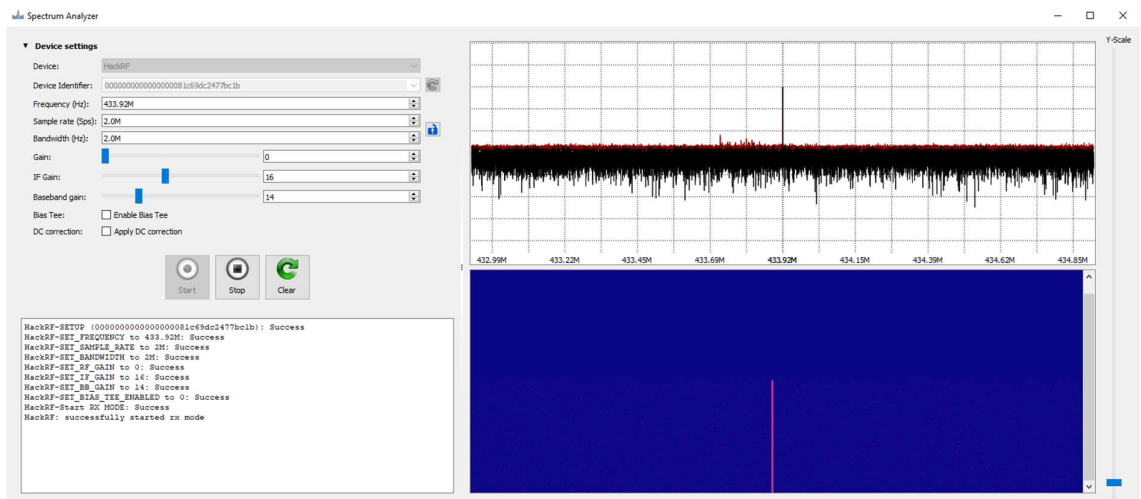
Πηγαίνοντας στο tab file μπορούμε να δούμε τις λειτουργίες του. Μπορούμε να δημιουργήσουμε ένα project, να ανοίξουμε ένα αρχείο/φάκελο αλλά και να import αρχείων. Ωστόσο οι σημαντικές λειτουργίες είναι το Spectrum Analyzer και το record analyzer.



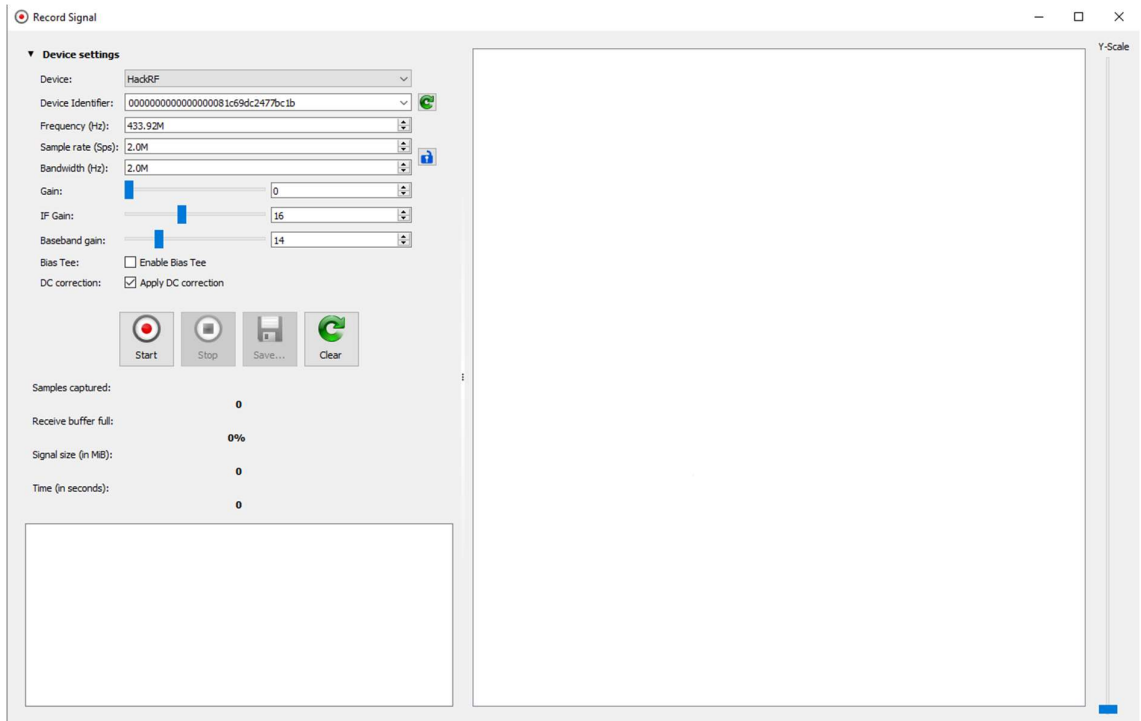
Στο **Spectrum Analyzer** πραγματοποιούμε ότι και στο **airspy** δηλαδή βρίσκουμε την συχνότητα του σήματος που μας ενδιαφέρει.



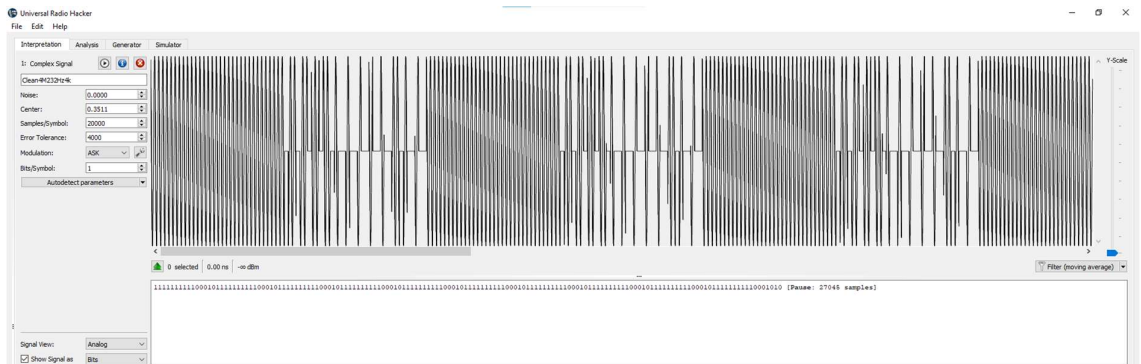
Παρακάτω φαίνεται το **spectrum analyzer** ενώ χρησιμοποιεί το **hackrf**.



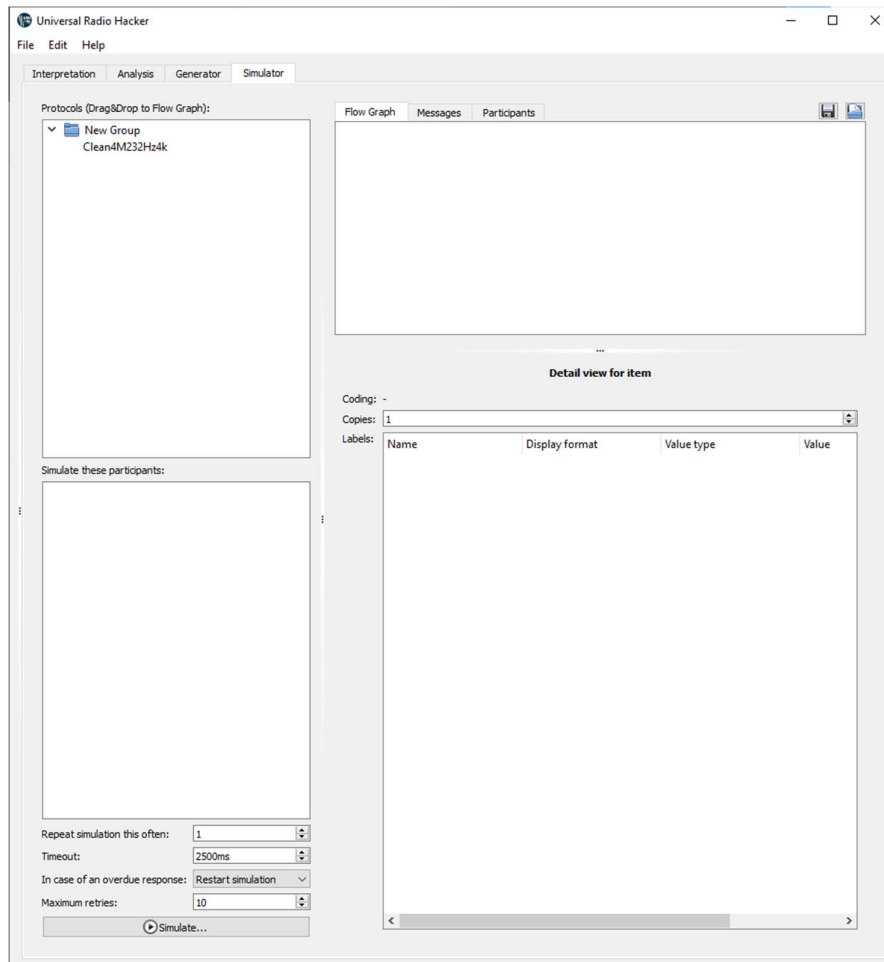
Στο **record signal** εισάγουμε την συχνότητα στην οποία βρήκαμε προηγουμένως το επιθυμητό σήμα και ορίζουμε τις παραμέτρους που επιθυμούμε.



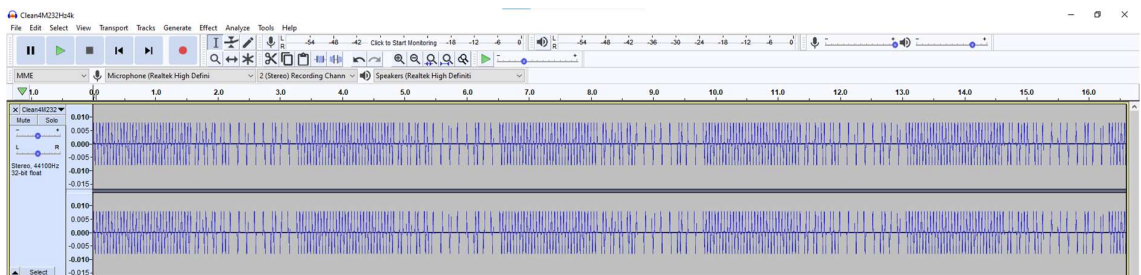
Αφού κάναμε capture το σήμα που επιθυμούμε μπορούμε να πραγματοποιήσουμε ανάλυση, να χρησιμοποιήσουμε φίλτρα και γενικά να το αλλάξουμε όπως επιθυμούμε.



Επιπλέον, υπάρχει η δυνατότητα σύγκρισης 2 σημάτων η οποία αποδείχτηκε άκρως σημαντική για την υλοποίηση της επίθεσης μας.



Τέλος, υπάρχει το **audacity** το οποίο αν και πρόγραμμα μουσικής βοηθάει στην κατανόηση των σημάτων τα οποία κάναμε capture.

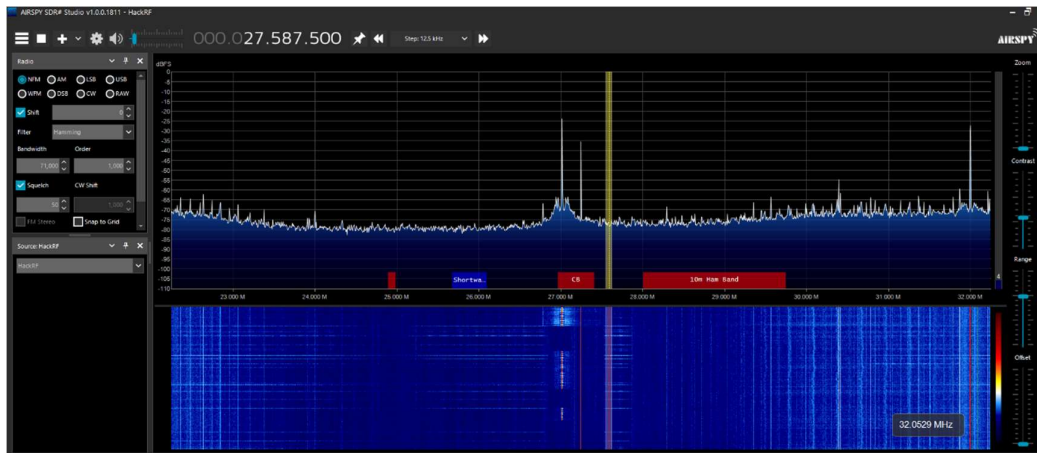


Διεξαγωγή επίθεσης

Το test-case που εξετάσαμε αφορά μια γκαραζόπορτα που χρησιμοποιεί δύο ασύρματα κοντρόλ με τεχνολογία dip switches.



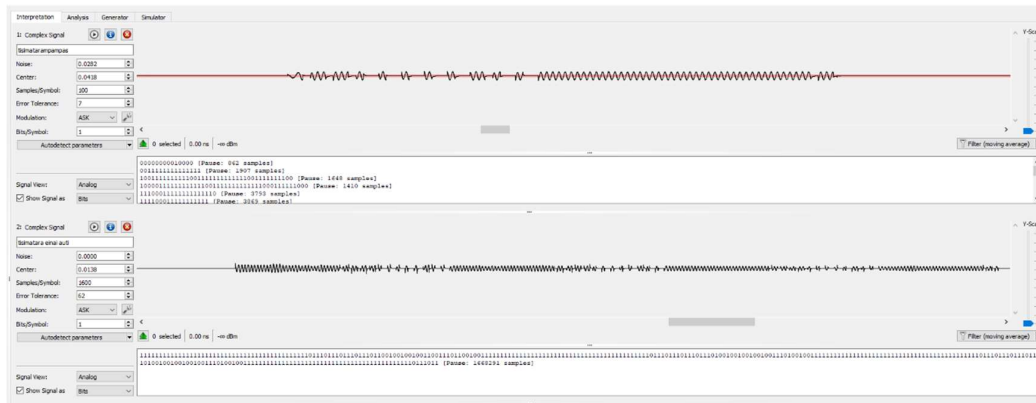
Αυτοί οι διακόπτες καθορίζουν το σήμα που εκπέμπεται για το ξεκλείδωμα της πόρτας. Μπορούμε να εντοπίσουμε τη συχνότητα που εκπέμπουν αυτά τα remotes μέσω του προγράμματος SDR#.



Από την παραπάνω εικόνα συμπεραίνουμε ότι η συχνότητα μετάδοσης των κοντρόλ είναι τα 27.015Mhz.

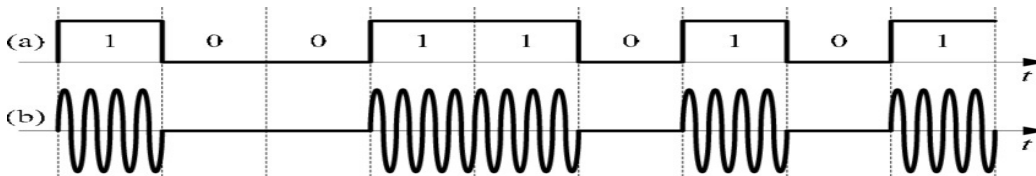
Κάνουμε capture σήμα από κάθε κοντρόλ μέσω του Universal Radio Hacker με Sample Rate - 2MHz και Bandwidth – 2MHz και παρατηρούμε ότι είναι το ίδιο σε κάθε capture και μεταξύ των κοντρόλ, συνεπώς δεν χρησιμοποιεί κάποιο μηχανισμό rolling code και



έχει στατικό κωδικό για κάθε χρήση. Τα 12 DIP switches επιτρέπουν τη δημιουργία 212 κωδικών, δηλαδή 4096. Για σύγκριση, ένας κωδικός 2 ψηφίων (αλφαριθμητικά και σύμβολα) είναι πιο ισχυρός. Με αλφαριθμητικά (26 μικρά, 26 κεφαλαία και 10 αριθμοί) και σύμβολα του πληκτρολογίου (τα 10 που αντιστοιχούν στους αριθμούς 0-9), υπάρχουν 72 χαρακτήρες διαθέσιμοι για κάθε ψηφίο του κωδικού. Ένας διψήφιος κωδικός λοιπόν θα έχει 722 πιθανούς συνδυασμούς, δηλαδή 5184.



Η μεγάλη συνεχής περίοδος αποτελεί ένα preamble, δηλαδή ένα introduction του controller που δηλώνει την ύπαρξη του. Είναι το αντίστοιχο με το header των πακέτων αλλά για τα σήματα.

Το παραπάνω σήμα είναι σε ASK modulation, το οποίο σημαίνει ότι γίνεται μετάδοση σήματος όποτε τις στιγμές που εμφανίζεται σήμα αποστέλλονται δεδομένα

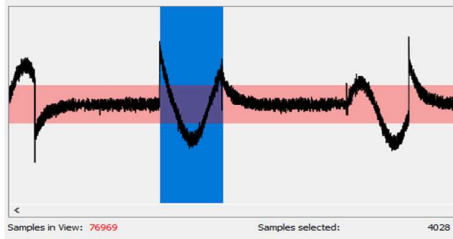


Από τα σήματα μεταξύ των preambles, βλέπουμε δύο είδη σημάτων. Τα σήματα με το μεγαλύτερο μήκος και αυτά με μικρότερο:  ,  . Τα σήματα αυτά είναι τα bits 11 και το bit 1 όπως στην εικόνα παραπάνω. Το σήμα έχει τη μορφή **11 11 11 11 1 1 1 1 1 1**.

Αν αντιστοιχήσουμε τα δύο σήματα με τα σύμβολα 0 και 1 αντίστοιχα για τα DIP switches σχηματίζουμε τον κωδικό 0 0 0 0 1 1 1 1 0 **1 1**. Τα πρώτα δέκα ψηφία του κωδικού ταιριάζουν με το κοντρόλ. Το γεγονός ότι τα δύο κοντρόλ έχουν διαφορετικό αριθμό DIP switches (10 και 12 αντίστοιχα) υποδεικνύει ότι ο κωδικός που χρησιμοποιείται είναι μάλλον 10 ψηφίων.

Με την επιλογή autotdetect parameters του Universal Radio Hacker το σήμα αποκωδικοποιείται με τον ακόλουθο τρόπο:

Το samples/symbol που καταλήξαμε ήταν 4000 εφόσον ένα σύμβολο θέσης 1 είχε περίπου 4000 samples μήκος όπως φαίνεται παρακάτω. Παρατηρούμε επίσης ότι το σύμβολο του DIP switch σε θέση 0 έχει μήκος περίπου το διπλάσιο (8000 samples). Το error tolerance που χρησιμοποιήσαμε ήταν 2:



Το γεγονός ότι κάθε επανάληψη του ίδιου σήματος κωδικοποιείται με τον ίδιο τρόπο υποδεικνύει πως οι παράμετροι είναι σωστοί.

Σε αυτό το σημείο, οφείλουμε να αναφέρουμε πως με μία αναζήτηση μόνο της συχνότητας του κοντρόλ βρίσκουμε αμέσως ένα ίδιο με το κοντρόλ για την πόρτα:

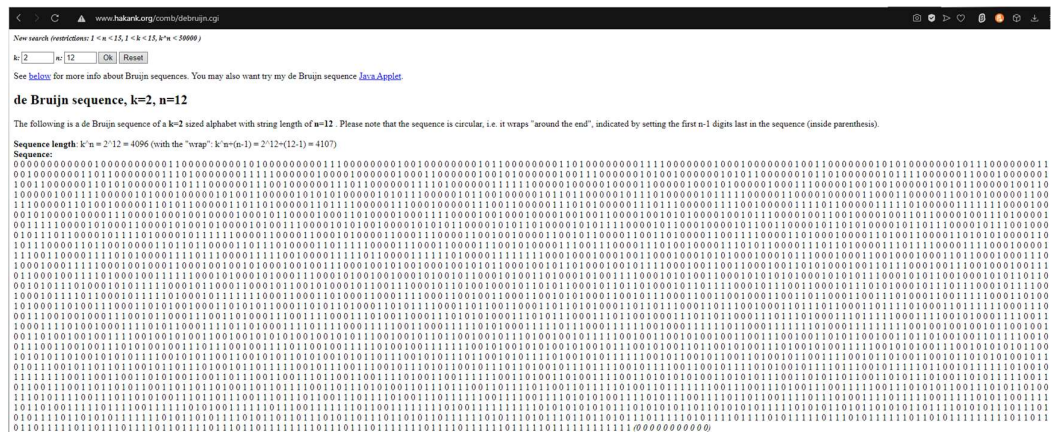
Ο επιτιθέμενος, θα μπορούσε να αγοράσει το κοντρόλ και να θέσει τα DIP switches στις θέσεις 0000111110 σύμφωνα με το σήμα και να ανοίξει την πόρτα.

Παρ' αυτά, δεν σταματήσαμε σε αυτό το σημείο. Προσπαθώντας να κάνουμε replay το σήμα αποτυχημένα, γνωρίσαμε το Generator tab του Universal Radio Hacker, από το οποίο μπορεί κανείς να δημιουργήσει ένα νέο σήμα με τις ίδιες παραμέτρους με το αρχικό. Ο τρόπος με τον οποίο γίνεται αυτό, είναι η εύρεση των κατάλληλων παραμέτρων, ώστε το 3ο και 4ο panel που είναι αντίστοιχα το generated σήμα και αυτό που έχουμε καταγράψει να είναι όσο το δυνατόν πανομοιότυπα. Η δυνατότητα του

The screenshot displays the Audacity 2.4.2 interface with the 'Modulation' panel active. The 'Carrier' section shows a sine wave with a frequency of 122.098320311 and a phase of 0.000°. The 'Data (new bits)' section shows a binary sequence of 1000 bits. The 'Modulation' section shows a square wave with 1 bit per symbol and 100 amplitudes. The 'Original Signal (drag/drop)' section shows a complex waveform. The 'New Group' section shows a list of generated files. The 'Lock view to original signal' checkbox is checked. The 'Show Only Data Frequency' checkbox is checked. The 'Samples in View' is 70000 and 'Samples selected' is 4000.

Τα συστήματα για τις πόρτες αυτές χρησιμοποιούν συχνά τεχνολογία bit shifting για να διαβάζουν το σήμα. Αυτό σημαίνει ότι σε περίπτωση που ο κωδικός είναι 5 bit, και ο επιτιθέμενος μεταδώσει σήμα 0011100, το receiver θα διαβάσει τα πρώτα 5 bit (00111), και στη συνέχεια θα «πετάξει» το πρώτο bit, και θα κάνει append στο τέλος του κωδικού το επόμενο, διαβάζοντας τον κωδικό 01110, και έπειτα 11100 κ.ο.κ. έναντι της αναμενόμενης συμπεριφοράς να διαβάσει τα πρώτα 5 bit, έπειτα να τα πετάει και να διαβάσει τα επόμενα 5.

13



Με αυτόν τον τρόπο μειώνουμε το keyspace στο 4.178% του αρχικού. Στα παραπάνω bits, εάν εκπέμπामε 12 bits κάθε φορά ολισθαίνοντας κατά 1 προς τα δεξιά, θα εκπέμπामε όλα τα δυνατά κλειδιά για μια πόρτα με 12 DIP switches. Επιπλέον, στα παραπάνω bits εμπεριέχονται όλα τα κλειδιά μήκους 1-11 εκτός από αυτά μήκους 12 ψηφίων, κάνοντας την επίθεση ακόμα πιο αποτελεσματική σε περισσότερες εγκαταστάσεις ή συσκευές.

Τι είναι το RFID (radio frequency identification)

Τα συστήματα RFID απαρτίζονται από δύο κύρια μέρη. Το πρώτο είναι οι πομποδέκτες (transponders) που συχνά αναφέρονται και ως ετικέτες RFID (RFID tags). Οι ετικέτες RFID είναι μικρά chips που αποτελούνται από ένα ολοκληρωμένο κύκλωμα, το οποίο περιλαμβάνει μνήμη ώστε να αποθηκεύει δεδομένα, και μία κεραία. Το δεύτερο μέρος είναι οι αναγνώστες ή αισθητήρες (readers), οι οποίοι ανακτούν τα δεδομένα από τις ετικέτες RFID. Οι αναγνώστες RFID έχουν ενσωματωμένα μια κεραία και μια μονάδα ελέγχου.

Οι ετικέτες

Οι ετικέτες RFID κατηγοριοποιούνται σε τρεις τύπους ανάλογα με τον τρόπο επικοινωνίας Ένα ολοκληρωμένο κύκλωμα στις ετικέτες RFID μπορεί να περιέχει μνήμη μόνο για

- ανάγνωση
- ανάγνωση και εγγραφή
- εγγραφή μιας και ανάγνωση.

Τα δεδομένα

Τα δεδομένα που αποθηκεύονται στις ετικέτες αποτελούνται από ένα μοναδικό αναγνωριστικό και μπορούν, επίσης, να περιλαμβάνουν ένα λειτουργικό σύστημα, μία αποθήκη δεδομένων και έναν ηλεκτρονικό κώδικα προϊόντων. Το μέγεθος των δεδομένων, που μια ετικέτα RFID έχει την δυνατότητα να αποθηκεύσει, καθορίζεται από τον εκάστοτε προμηθευτή.

Οι αναγνώστες

Οι αναγνώστες RFID αποτελούνται από μία κεραία, η οποία αναλαμβάνει την επικοινωνία μέσω ραδιοσυχνοτήτων με τις ετικέτες. Καθώς και μία μονάδα ελέγχου, για καθορισμό των διάφορων ενεργειών (αποστολή/ λήψη σημάτων, ανάγνωση/ εγγραφή ετικετών κ.ά.).

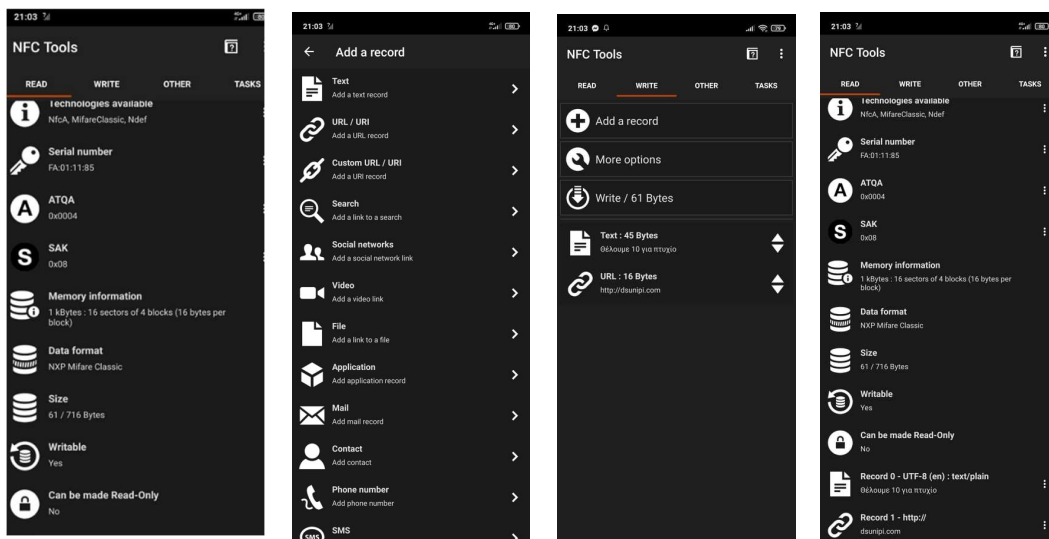
Πειράματα επάνω στις ετικέτες (NFC tags)

Για την εκτέλεση των πειραμάτων μας χρησιμοποιήσαμε ένα Arduino uno και έναν rfid reader (RC522), καθώς και το κινητό μας τηλέφωνο που υποστηρίζει την τεχνολογία nfc. Το λογισμικό που χρησιμοποιήσαμε είναι το Arduino ide και το NFC Tools. Επιπλέον τις ετικέτες που χρησιμοποιήθηκαν ήταν ανάγνωσης και εγγραφής.

Αφού έχουμε εγκαταστήσει την εφαρμογή NFC Tools στο κινητό μας τηλέφωνο, μπορούμε πολύ ευκολά πλησιάζοντας την ετικέτα στο κινητό να σκανάρουμε και να διαβάσουμε την πληροφορία που έχει, όπως φαίνεται παρακάτω.

Αναλύοντας το περιεχόμενο της ετικέτας μπορούμε να διακρίνουμε πως έχει ένα serial number, τι τεχνολογίες χρησιμοποιεί (NfcA, MifareClassic, Ndef), το μέγεθος του, τα δεδομένα που έχει αποθηκευμένα και τον τύπο της ετικέτας.

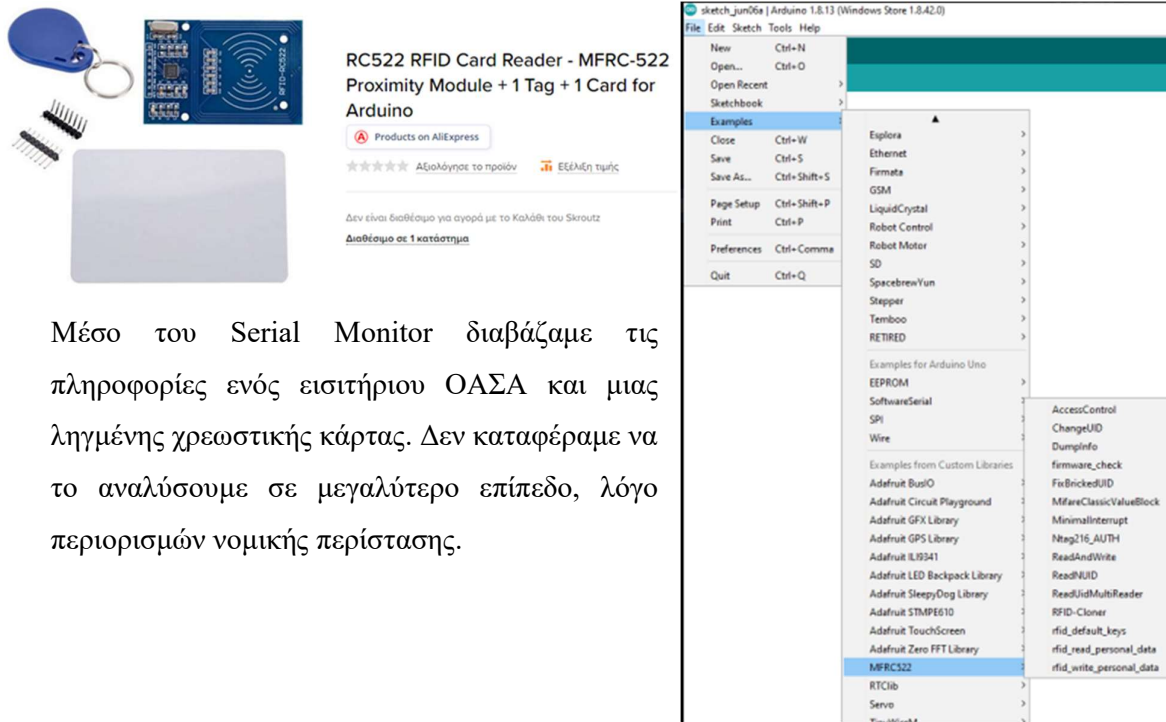
Εφόσον η ετικέτα που κατέχουμε έχει και την δυνατότητα εγγραφής, επιλέγουμε να κάνουμε μια εγγραφή στην ετικέτα. Εδώ μας δίνετε μια πληθώρα γκάμα από επιλογές που μπορούμε να κάνουμε. Εμείς διαλέξαμε να προσθέσουμε ένα κείμενο “θέλουμε 10 για πτυχίο” και ένα url “dsunipi.com”, περάσαμε ξανά την ετικέτα και αυτόματος έγραψε ότι πληροφορία είχαμε στην ετικέτα.



Ενώ η δυνατότητα υπάρχει στην τεχνολογία, λόγω μη επαρκούς λογισμικού δεν μπορέσαμε να αντιγράψουμε είδη υπάρχον κλειδωμένες ετικέτες, όπως είναι τα εισιτήρια του ΟΑΣΑ και χρεωστικές - πιστωτικές κάρτες.

Με χρήση Arduino

Για την ανάλυση των ετικετών μέσω του Arduino χρησιμοποιήσαμε το “RC522” που φαίνεται στην εικόνα παρακάτω και την βιβλιοθήκη “MFRC522”.



Μέσο του Serial Monitor διαβάσαμε τις πληροφορίες ενός εισιτηρίου ΟΑΣΑ και μιας ληγμένης χρεωστικής κάρτας. Δεν καταφέραμε να το αναλύσουμε σε μεγαλύτερο επίπεδο, λόγω περιορισμών νομικής περίπτωσης.

```
COM3
Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: FA 01 11 85
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 AccessBits
15 63 PCD_Authenticate() failed: Error in communication.
14 59 PCD_Authenticate() failed: Error in communication.
13 55 PCD_Authenticate() failed: Error in communication.
12 51 PCD_Authenticate() failed: Error in communication.
11 47 PCD_Authenticate() failed: Error in communication.
10 43 PCD_Authenticate() failed: Error in communication.
9 39 PCD_Authenticate() failed: Error in communication.
8 35 PCD_Authenticate() failed: Error in communication.
7 31 PCD_Authenticate() failed: Error in communication.
6 27 PCD_Authenticate() failed: Error in communication.
```

Εισιτήριο

```
COM3
Send

Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: 04 A5 1B 82 82 58 80
Card SAK: 00
PICC type: MIFARE Ultralight or Ultralight C
Page  0  1  2  3
0    04 A5 1B 32
1    82 82 58 80
2    D8 48 08 00
3    1A 39 DE 6E
4    10 90 38 67
5    78 69 00 00
6    00 00 00 00
7    41 C0 B7 C0
8    AE 13 65 E7
9    81 79 E3 BF
10   D4 27 16 64
11   01 40 4B 50
12   00 00 00 01
13   03 EA 04 17
14   20 91 1D 8D
15   00 00 00 00

☒ Autoscroll ☐ Show timestamp
Newline 9600 baud Clear output
```

Κωδικός ανέπαφης πιστωτικής

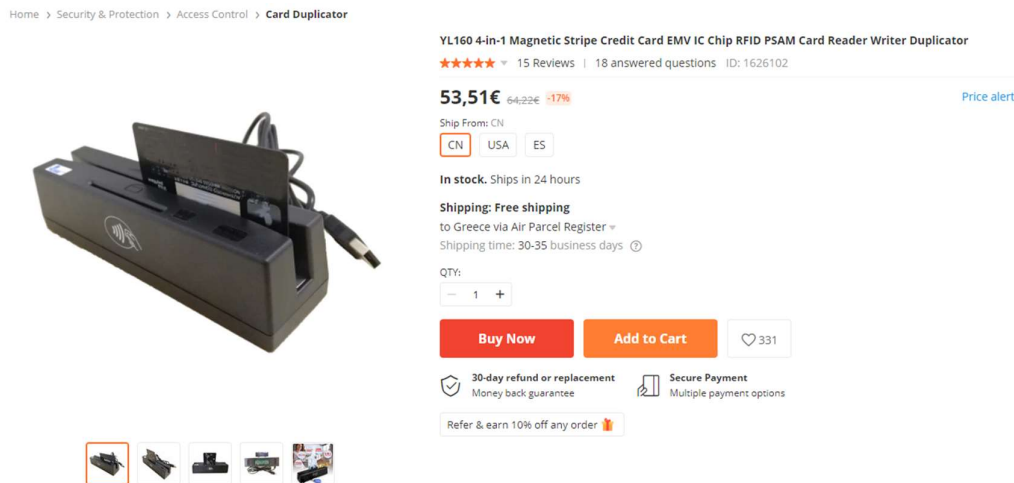
```
COM3
Send

Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: BF 3C 64 51
Card SAK: 28
PICC type: Unknown type

☒ Autoscroll ☐ Show timestamp
Newline 9600 baud Clear output
```

Πειράματα επάνω στις τραπεζικές κάρτες

Εκτός από το rfid reader σε συνδιασμό με το Arduino υπάρχει η δυνατότητα ο επιτιθέμενος να αγοράσει ολοκληρωμένο μηχανήμα το οποίο απλά συνδέεται σε θύρα usb και λειτουργεί χωρίς κάποιο πρόγραμμα.



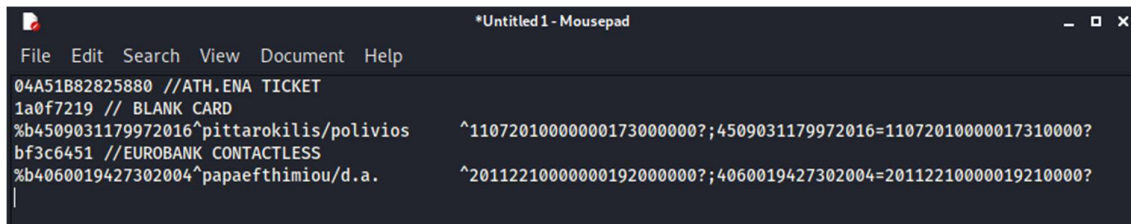
Αφού συνδέσουμε το μηχανήμα στην θύρα usb αρκεί να ανοίξουμε ένα text editor σε οποιοδήποτε λογισμικό και μας εμφανίζει τις αναγκαίες πληροφορίες. Υπάρχει η δυνατότητα αγοράς εξειδικευμένου προγράμματος από το dark web το οποίο μας επιτρέπει με αυτό το μηχανήμα όχι μόνο να διαβάζουμε αλλά και να γράφουμε πληροφορία.

Το μηχανήμα αυτό έχει 3 διαφορετικές λειτουργίες:

1. Contactless reader (rfid)
2. Διάβασμα του chip της κάρτας
3. Magnetic stripe reader

Πραγματοποιήσαμε scanning 4 διαφορετικών καρτών. Η πρώτη κάρτα είναι το ATH.ENA TICKET το οποίο μέσω rfid μπορούμε να δούμε τον κωδικό του. Η δεύτερη είναι μια κλασσική πλαστική κάρτα όπως αυτές των ξενοδοχείων για την είσοδο στο δωμάτιο ή εταιριών για πρόσβαση σε συγκεκριμένους χώρους. Η τρίτη κάρτα είναι μία παλιά πιστωτική που δεν έχει την δυνατότητα contactless payment και η τέταρτη επίσης μία πιστωτική που έχει την δυνατότητα contactless payment. Όπως δείχνουμε και παρακάτω στις πρώτες 2 κάρτες και στην πιστωτική με το contactless υπάρχει ένας

απλός κωδικός που αν αντιγραφεί είναι αρκετός για αυθεντικοποίηση. Επομένως, ένας επιτιθέμενος έχει την δυνατότητα να υποκλέψει τον κωδικό και να αποκτήσει πρόσβαση ή να πραγματοποιήσει συναλλαγή αποκλειστικά από αυτά τα στοιχεία. Αυτός είναι και ο λόγος που τα contactless payments έχουν όριο ανά συναλλαγή. Όσον αφορά το magnetic stripe μπορούμε να δούμε πως περιέχονται σχεδόν όλες οι αναγκαίες πληροφορίες. Πιο συγκεκριμένα, περιέχονται με την σειρά ο αριθμός της κάρτας, το όνομα του ιδιοκτήτη (σε άλλες περιπτώσεις εμφανίζεται μόνο το όνομα της τράπεζας), η ημερομηνία λήξης της κάρτας (YY/MM) κάποιες πληροφορίες που δεν μας χρειάζονται και μετά από τα ?; ο πίσω κωδικός της κάρτας εκτός από τα τελευταία 3 ψηφία του.



```
*Untitled1 - Mousepad
File Edit Search View Document Help
04A51B82825880 //ATH. ENA TICKET
1a0f7219 // BLANK CARD
%b4509031179972016^pittarokilis/polivios ^11072010000000173000000?;4509031179972016=11072010000017310000?
bf3c6451 //EUROBANK CONTACTLESS
%b4060019427302004^papaefthimiu/d.a. ^20112210000000192000000?;4060019427302004=20112210000019210000?
```

Εκτός αυτών, βρήκαμε και πρόγραμμα το οποίο αποδείχτηκε να έχει malware επομένως δεν καταφέραμε κάνουμε proof of concept για την αντιγραφή των δεδομένων αυτών.

Συνολικά είδαμε πως η πληροφορία είναι εύκολο να διαβαστεί, όμως στην περίπτωση των πιστωτικών/χρεωστικών καρτών έχουν παρθεί ορισμένα μέτρα προκειμένου να γίνεται πιο δύσκολη η ολική κλοπή καρτών. Εάν κάποιος επιθυμεί να πραγματοποιήσει ηλεκτρονική συναλλαγή του ζητείται και ο τελευταίος 3ψηφιος κωδικός ενώ πολλές φορές υπάρχει και 2factor authentication μέσω κινητού ή εφαρμογής. Στην συναλλαγή σε POS ή ATM χρειάζεται και το pin του χρήστη για την αξιοποίηση της κάρτας. Τέλος για τα contactless payments δεν υπάρχει κάποιος τρόπος για να μην πραγματοποιηθεί η συναλλαγή, όμως για την καθημερινή χρήση μικρών ποσών θεωρείται αμελητέος ο κίνδυνος και ορίζεται το όριο στο ποσό που επιθυμεί ο κάθε χρήστης ανά συναλλαγή χωρίς pin. Επιπλέον, ορισμένες κάρτες επιθυμούν pin ανά ορισμένο αριθμό ανέπαφων συναλλαγών.

Βιβλιογραφία

1. Universal Radio Hacker - Replay Attack With HackRF
https://www.youtube.com/watch?v=uIVBVd6yi_A
2. Transmitting With A HackRF One Via My Local Ham Radio Repeater
https://www.youtube.com/watch?v=qx_orXHiQk8
3. I Hacked Into My Own Car
<https://www.youtube.com/watch?v=5CsD8I396wo>
4. Radio Hacking: Cars, Hardware, and more! - Samy Kamkar - AppSec California 2016
<https://www.youtube.com/watch?v=1RipwqJG50c>
5. Unlocking Car Doors with the HackRF Replay Attack
<https://www.youtube.com/watch?v=CA3XnGyD-SQ>
6. Credit card cloning is too easy!
<https://www.youtube.com/watch?v=eyd24FIJCFg>
7. Security Access using MFRC522 RFID Reader with Arduino
<https://randomnerdtutorials.com/security-access-using-mfrc522-rfid-reader-with-arduino/>
8. What is RFID? How It Works? Interface RC522 RFID Module with Arduino
<https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/>