Journal of the Nigerian Association of Mathematical Physics
***Volume 61* (July – September *2021 Issue*), pp91 – 100**
© J. of NAMP

VULNERABILITY OF RFID TECHNOLOGY: CLONING OF LOW FREQUENCY RFID CARD

Evbuomwan E.[1,*] and Iyekekpolo E.N.[2]

[1]Department of Computer Engineering, Faculty of Engineering, University of Benin, PMB 1154, Benin City, Nigeria.
[2]Department of Electrical/Electronic Engineering, Faculty of Engineering, University of Benin, PMB 1154, Benin City, Nigeria.

Abstract

In this research, the vulnerability of an RFID access control system is shown by performing a cloning attack on a low frequency RFID card. RFID technology has been found very useful in many areas including its use in security system in offices, industries and recreational centres. However, there has been growing concerns about the strength of its security. With the increasing level of hackers and viral attack on security systems, RFID system must be subjected to fireproof test in order to ascertain its strength in being able to withstand attacks. With the increasing application of RFID technology, we carried out a cloning attack using an RFID cloner, Proxmark 3, in a Linux development environment. The attack was successful and showed the susceptibility of RFID cards to attacks.

Keywords: RFID reader, RFID cloner, RFID card, Proxmark 3, low frequency, high frequency.

1 Introduction

RFID is an acronym for "radio-frequency identification" and refers to a technology whereby digital data encoded in RFID tags or smart labels are captured by a reader via radio waves. Radio-frequency identification (RFID) [1] uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID tag consists of a tiny radio transponder; a radio receiver and transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader. An RFID system consists of both a reader and a tag. The RFID tag is attached to any object that is to be tracked or identified while the reader is used to continuously send radio waves which the tag will receive when it is within range, which will in turn cause the tag to send a feedback signal making tracking and identification possible.

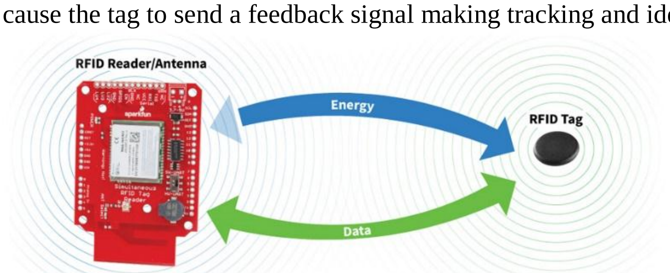

***Fig** 1: Data transfer between RFID tag and card reader*

In 2014, the world RFID market was worth 8.89 billion USD, up from 7.77 billion USD in 2013 and 6.96 billion USD in 2012. This figure includes tags, readers, and software/services for RFID cards, labels, fobs, and all other form factors. The market value is expected to rise from 12.08 billion USD in 2020 to 16.23 billion USD by 2029 [1].

As mentioned earlier, RFID technology finds applications in various areas such as [1]:

i. Access management
ii. Tracking of goods

Corresponding Author**:** Evbuomwan E., Email: eguagie.evbuomwan@uniben.edu, Tel: +2348020613656, +2347061280886 (IEN)

iii. Tracking of persons and animals
iv. Toll collection and contactless payment
v. Machine readable travel documents
vi. Locating lost airport baggage
vii. Tracking and billing processes
viii. Monitoring the physical state of perishable goods

However, this work focuses primarily on access management as RFID cards form a large part of security system in offices, industries and recreational centres such as hotels, lounges and guest houses.

Section 2 discusses the materials and related works in RFID tag emulations and Section 3 presents the methodology used in this paper for cloning a RFID card. Section 4 is the results which is presented as a comprehensive guide towards cloning with Proxmark 3 device using the API from a Github repository which was built from the source files. In the end, the conclusion on the research is given in Section 5.

2 Theoretical Analysis

Proxmark 3

The Proxmark3 device is a standard device designed solely for reading, decoding, storing and replaying information from any low frequency (125 kHz) proximity cards and high frequency (13.56 MHz) RFID cards.

Fig 2 Proxmark 3

The Proxmark3 device can collect information/data between a tag and a reader and can therefore be used to perform an attack on RFID technology. This device was originally developed by Jonathan Westhues, and the latest version of this device is called the RDV4.01.

Parts of the Proxmark3

On the Proxmark3 device there are a couple of other components as shown in Table 1

Table 1 parts of the proxmark 3

Low Frequency antenna	High Frequency antenna	Cable	2 Proxmark3 PCB protection shells
			

Ubuntu Operating System (OS)

Ubuntu is an operating system that is developed by a worldwide community of programmers as well as by employees of Ubuntu's commercial sponsor, Canonical [2]. Ubuntu is based on the concept of free or open-source software, which means it comes without any licensing fees and so one can download, use, and share the operating system free of charge. Being a Linux-based operating system, Ubuntu has a well-deserved reputation for stability and security. The potential drawbacks or challenges Ubuntu users may encounter are the availability of compatible applications, the issue of hardware support or compatibility, the fact that PC retailers don't offer a pre-installed Ubuntu, which means you must install the system yourself, whereas Windows and OS X usually come pre-installed on your PC and lastly, the fact that there are no big updates, same GUIs.

RELATED WORKS

For the purpose of clarity of methodology used by researchers in RFID systems, we present a detailed review of related works in security attacks with RFID technology. Information security threats have been traditionally classified according to what is known as the CIA Triad:

i. Confidentiality. It is related to the importance of protecting the most sensitive information from unauthorized access.
ii. Integrity. It consists in protecting data from modification or deletion by unauthorized parties, and ensuring that, when authorized people make changes, they can be undone if some damage occurs.
iii. Availability. It is the possibility of accessing the system data when needed.

If any of these three principles is not met, then security can be said that it has been broken. Like other technologies, RFID is exposed to security threats and, specifically, to attacks on the confidentiality, integrity and availability of the data stored on the tags, or on the information exchanged between a reader and a tag. When these threats are associated with the probability of occurrence of an event that causes damage to an informational asset, they are known as risks.

In real life, most risks are a mixture of both security and privacy risks: they threaten RFID security in order to get access to the information stored or to the data exchanged in a transaction.

Physical Attacks

This type of threat consists in using some kind of physical medium to attack a tag or the RFID communications. There are mainly five basic attacks [3]:

i. Reverse engineering. Most tags are not tamper-proof and can be disassembled and analysed.
ii. Signal blocking or jamming. It consists of blocking tag communications to avoid sending data to a reader.
iii. Tag removal. It consists of removing an RFID tag or replacing it with another one.
iv. Physical destruction. In this case the attacker destroys the RFID tag by applying pressure, tension loads, or high/low temperatures; by exposing the tag to certain chemicals; or by just clipping the antenna off.
v. Wireless zapping. RFID zappers are able to send energy remotely that, once rectified, is so high that certain components of the tag might be burned.

Software Attacks

These attacks are related to software bugs or vulnerabilities found in tags or in the RFID reader. Researchers have found that it is possible to misuse the kill password in some tags (EPC Class-1 Gen-2) with a passive eavesdropper and then disable the tags [4]. Another such attack is the tag cloning. In this attack, the Unique Identifier (UID) and/or the content of the RFID is extracted and inserted into another tag [5]. It has been found that some readers are vulnerable to remote code execution by just reading the content of a tag [6] or SQL injection such that some reader middleware are vulnerable to the injection of random SQL commands.

There is also the possibility of Virus/Malware injection. Although difficult to perform in the vast majority of RFID tags due to their low storage capacity, it is possible in certain tags to insert malicious code that is able to be transmitted to other tags [6].

Channel Attacks

Channel attacks refer to threats related to the lack of security on the communications between the reader and the tag. Researchers have performed unauthorized reading with most RFID tags without leaving a trace [7,8]. Also, the channel attacks take the form of Denial of Service (DoS) attacks whereby the channel is flooded with such a large amount of information that the reader cannot deal with the signals sent by real tags [9].

Another such attacks are Signal replaying – it consists in recording the RFID signal in certain time instants with the objective of replaying it later, Man-in-the-Middle (MitM) attacks –They consist in placing an active device between a tag and a reader in order to intercept and alter the communications between both elements [7,10], Relay/amplification attacks – They consist in amplifying the RFID signal using a relay, so the range of the RFID tag is extended beyond its intended use [11,12].

3 Experimental work

In this paper, we carried a cloning attack on an RFID card that was used to gain access into a building using the materials discussed in Section 2 which can be summarized as:

i. Test cards (one active RFID card and one empty RFID card)
ii. Proxmark 3 (RFID card cloner)
iii. USB cable
iv. Ubuntu OS

The research starts with the visual inspection of the tag for information such as an external sign that might indicate the manufacturer, the model, or the RFID standard. One of the most relevant external signs for determining the internal parameters of a tag is its FCC ID (or its equivalent in other parts of the world). The FCC is an agency of the United States that regulates radio communications. Each FCC-approved radio device receives a unique FCC ID that must be marked permanently and has to be visible to the buyer at the time of purchase. Such an FCC ID is composed by 4–17 alphanumeric characters. The first three characters are the Grantee Code, which identifies the company that asks for the authorization of the radio equipment. The rest of the characters (between 1 and 14) are the Product Code. If there is an FCC ID label on an RFID tag or on a reader, it is possible to obtain through the FCC ID search page [13] information like the name of the company that has applied for the authorization, the lower and upper operating frequencies, block diagrams, schematics, and even external/internal photos of the device.

In most commercial systems it is not common to show external clues about the characteristics of a tag, so, in these cases, a detailed analysis has to be carried out. The first parameter to determine is the operation frequency of the tag. Most tags use LF, HF or UHF bands. So, if the preceding steps that have been discussed do not suffice, the process towards determining the operation frequency involves two steps. First, we dissemble and analyse the tag or reader, then perform radio spectrum analysis to detect the operation frequency. In the radio spectrum analysis, the objective is to detect the resonant frequency of the passive RFID tag which is done by modelling the tag as a simple RLC parallel resonant circuit. Through Thomson's equation the obtained frequency is

$$f_r = \frac{1}{2\pi\sqrt{LC}}. \quad (1)$$

Where L is the inductance and C is the capacitance. The key to measuring the resonant frequency is that the impedance of the measuring antenna as well as the reflection and transmission coefficient vary significantly at frequencies in the vicinity of the resonant frequency of the RFID tag. If it is verified that the RFID system is LF or HF, the next step of the methodology requires determining the modulation and the coding scheme used by the tag. These tasks involve the use of the appropriate tool to perform a detailed analysis of the radio signals. Such a tool may be a bench oscilloscope with a measuring antenna or similar hardware (e.g., Proxmark 3) that allows for acquiring the RFID signals and then showing the wave received through a display. However, if it is detected that the tag is UHF, the study can become difficult because, although most passive tags are compliant with the EPC Gen 2 standard, there are a number of companies that make use of proprietary protocols. In such a case, reverse engineering may require using software-defined radio platforms like USRP, MyriadRF [14] or HackRF One [15] to study and then emulate the RFID communications protocol. Once the frequency, the modulation, and the coding scheme have been obtained, it is straightforward to determine whether there exists an RFID standard compliant with such a configuration. If there is not, the research may involve reverse engineering a proprietary protocol. However, due to compatibility purposes, most massively commercialized LF, HF and UHF tags follow well-known RFID standards. Lastly, the trial-and-error process that requires to sniff and emulate communications to perform security tests. Sniffing is not only useful for reverse engineering a communications protocol, but also when trying to understand a well-documented standard protocol. Eventually, once the communications protocol is understood, it may be emulated with the appropriate hardware. For instance, Proxmark 3 official firmware offers off-the-shelf emulation of different standards (i.e., ISO/IEC 14443-A and 14443-B, ISO/IEC 15693) and specific tags (e.g., iClass, MIFARE, HID, Hitag, EM410x, Texas Instruments LF tags, or T55XX transponders). The methodology discussed can be summarized as follows:

i. Visual Inspection
ii. Federal Communication Commission (FCC) ID or equivalent
iii. Frequency Band detection
iv. LF/HF tag parameter analysis
v. UHF tag parameter analysis
vi. Standard analysis
vii. Sniff and Emulate

4 Results and discussion

The following steps (i) to (viii) are the comprehensive setup procedure for interfacing the Proxmark 3 device.

i. Installation of the Ubuntu Software. We used the Ubuntu 18.04 LTS version for the project.
ii. Next, we get the build dependencies for the Proxmark 3 software Application Programming Interface (API). Fig 3 presents the installation of the dependencies.

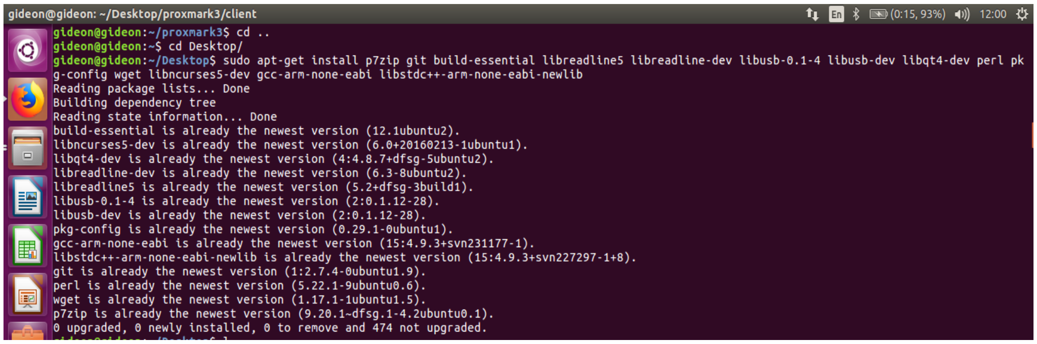

Fig 3 Command line to build proxmark3 source files

iii. Afterwards we clone the Proxmark repository on Github for the latest version of the API using the command git clone https://github.com/proxmark/proxmark3.git

iv. There are a couple of steps to take to build the source files that have been cloned which are outlined as follows [16]:

cd
cd proxmark3
git pull
sudo cp -rf driver/77-mm-usb-device-blacklist.rules /etc/udev/rules.d/77-mm-usb-device-blacklist.rules
sudo udevadm control --reload-rules
sudo adduser $USER dialout

v. Do logout and login after the last step to ensure the user privileges are changed.

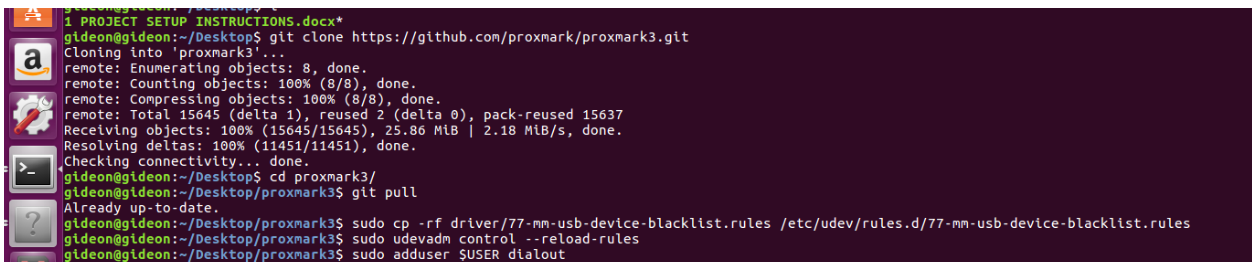

Fig 4 Command for git pull and to install all blacklist rules

vi. Next, we compile the Proxmark 3 API with a clean and complete compilation using the commands shown in Fig. 5.

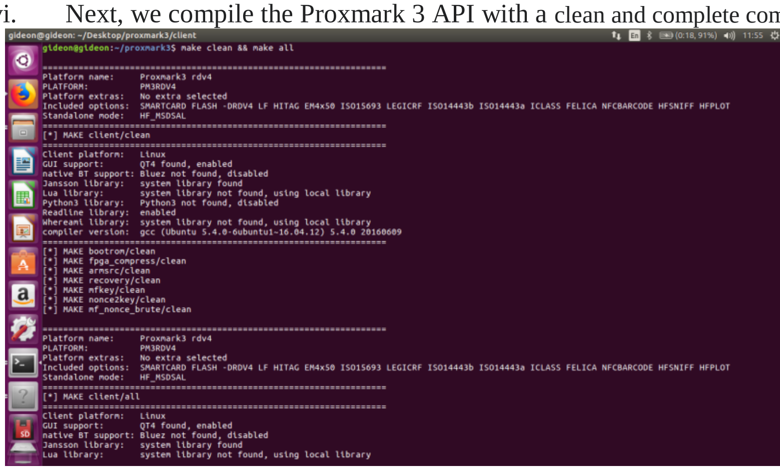

Fig 5 Command line to clean and complete the compilation.

vii. Compilation is done so the Proxmark3 device can be plugged in to the Host Computer. Do check the dmesg using the command dmesg | grep -i usb

viii. Flash the BOOTROM, FULLIMAGE with the command: sudo client/flasher /dev/ttyACM0 -b bootrom/obj/bootrom.elf armsrc/obj/fullimage.elf [16].

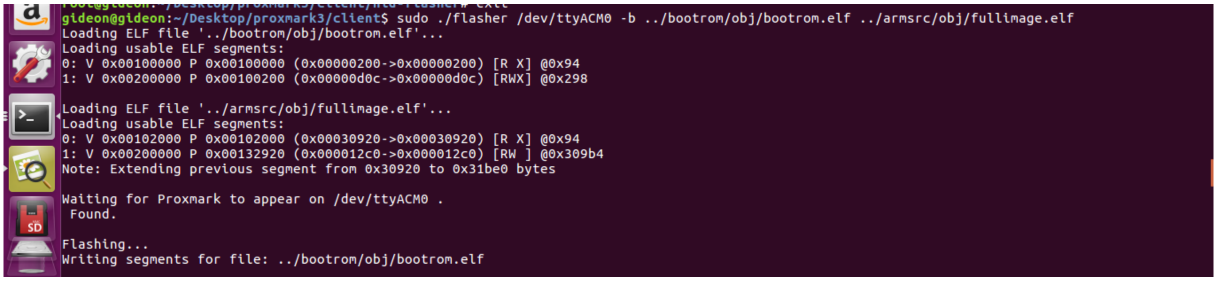

Fig 6 Command line for the bootrom and full image flashing

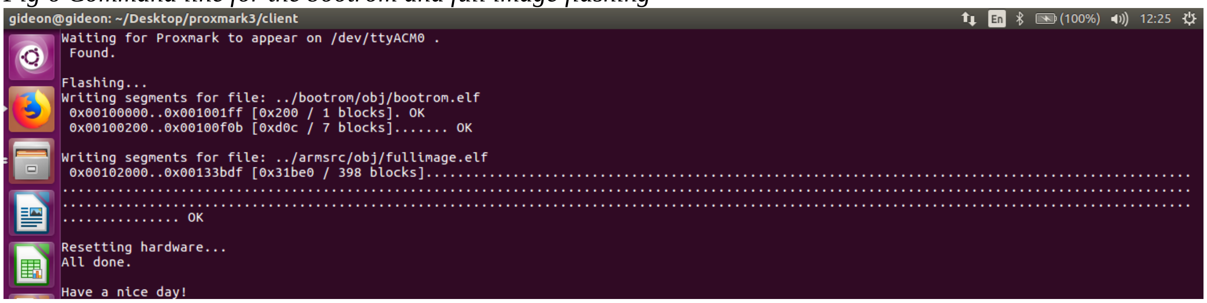

Fig 7 Command line for the bootrom and full image flashing (Continuation)

Running the proxmark 3 client

After the previous steps for cloning and compiling the source codes for the proxmark 3 libraries, we can run a shell to test simple commands.

i. Access the client directory in Desktop/proxmark3/client on the host computer and run the client using the command: ./proxmark3 /dev/ttyACM0. The command opens the proxmark3 shell as shown in Fig. 8

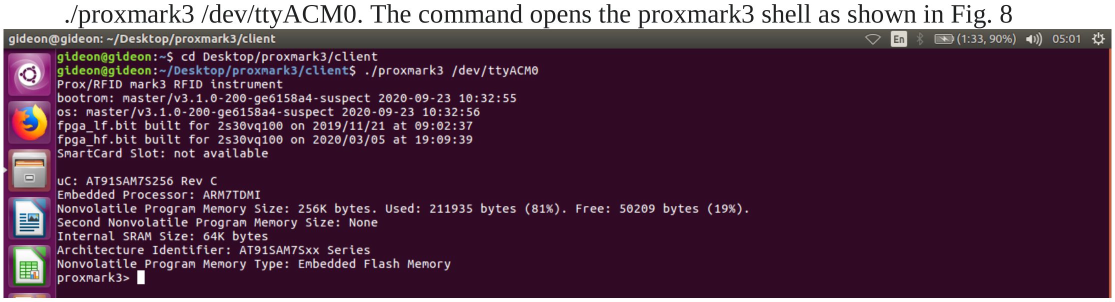

Fig 8 Command line to run the proxmark3 client.

ii. In the shell run the *hw status* and *hw version* to check the status of the connected device and as shown in Fig. 9 and 10 respectively.

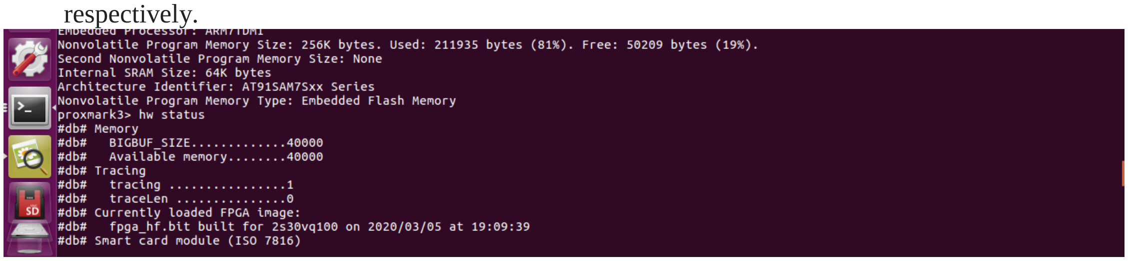

Fig 9 Commands to verify the functionality of the proxmark3 (1)

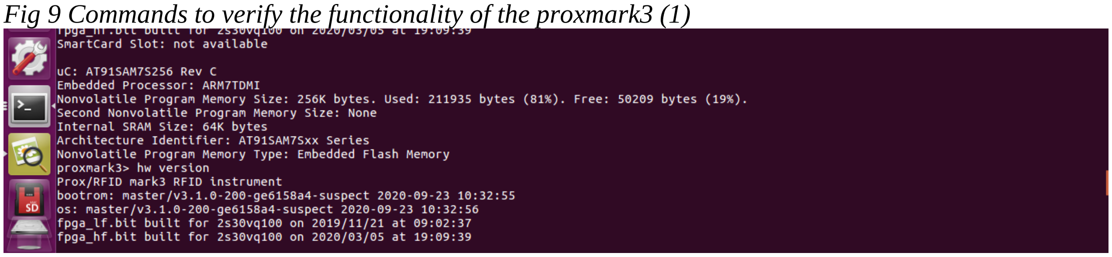

Fig 10 Commands to verify the functionality of the proxmark3 (2)

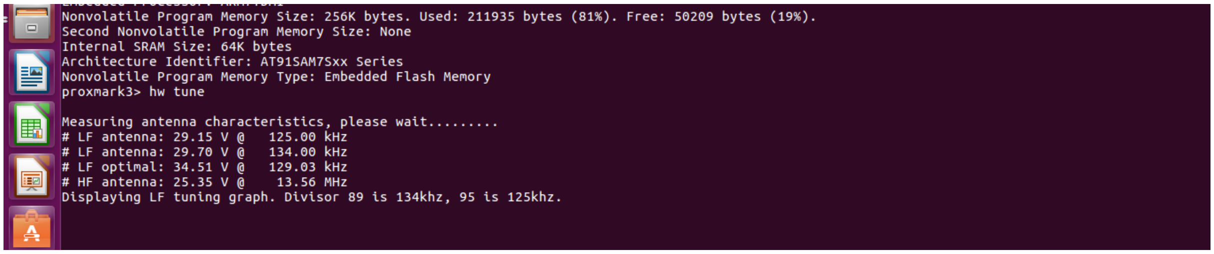

Fig 11 Commands to verify the functionality of the proxmark3 (3)

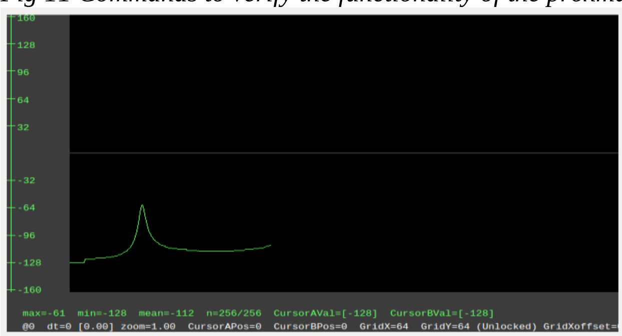

Fig 12 Graph generated after running the "hw tune" command.

These steps round up the development setup for the research. The steps (i) to (v) taken to clone an RFID card are as follows:

i. With the proxmark 3 device connected to the host computer, we run the watch command [1] to check if an external device is connected to it as shown in Fig. 13. If the proxmark 3 device is connected properly then the result is as shown in Fig. 14 after about 2 seconds.

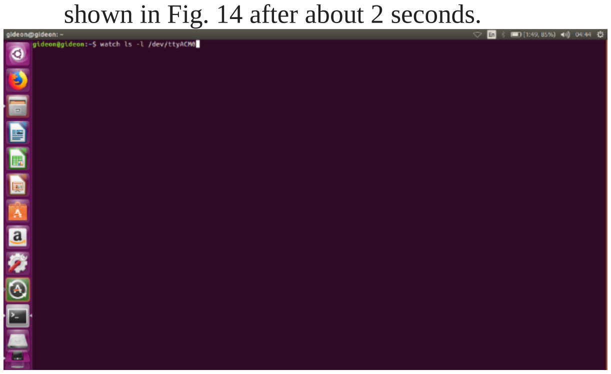

Fig 13 Steps taken in cloning a RFID card

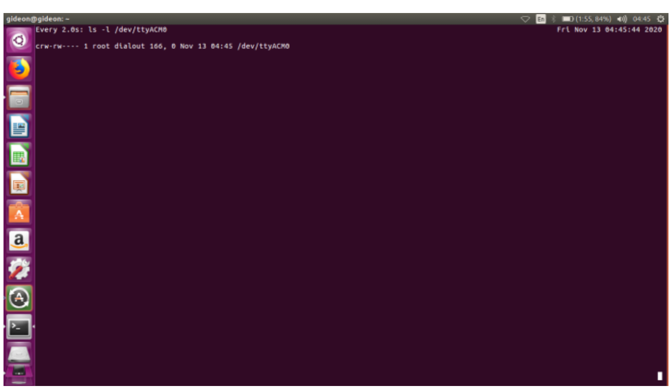

Fig 14 Proxmark 3 detected

ii. Next, we run the client which is located in the client directory **cd Desktop/proxmark3/client**. This opens the proxmark interface so that we can interact with it.

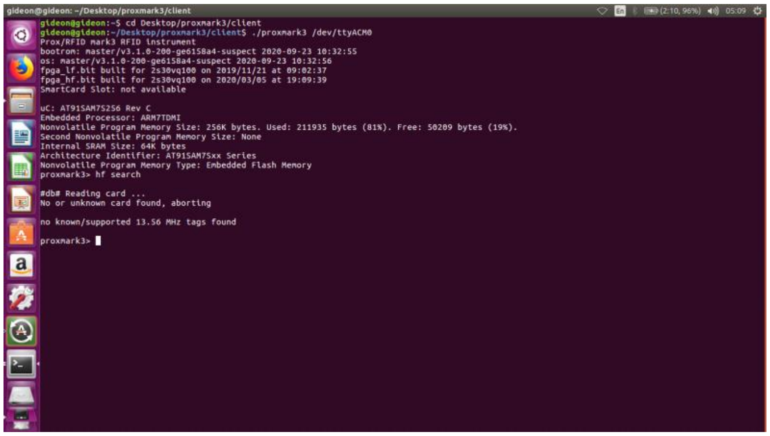

Fig 15 Running the client

iii. Place the unknown card on the proxmark 3 and run commands from the list of commands in Table 2 to determine what kind of card it is. Whichever card it is the details showing its tag identification number will be displayed after the command is ran. Fig. 17 shows the result for low frequency search for the unknown card showing the tag identification number.

Table 2 List of commands for identifying cards

List of commands	**Meaning**
hf search	Find a high frequency card
lf search	Find a low frequency card

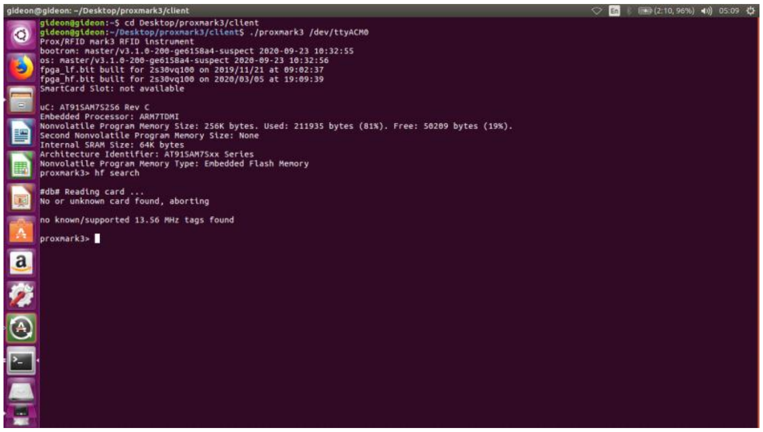

Fig 16 Running hf search command

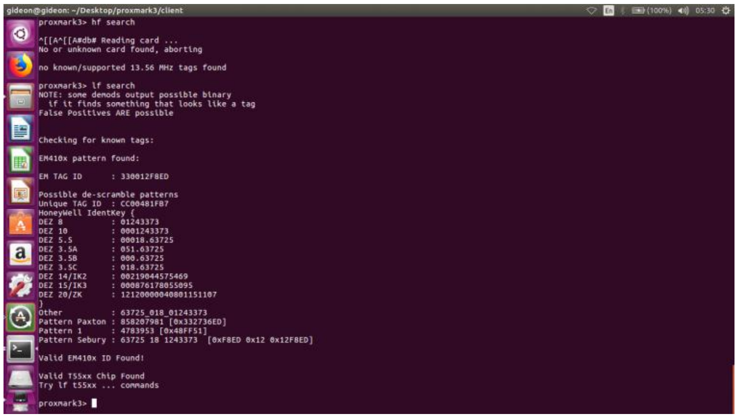

Fig 17 Running lf search command

iv. The steps are also repeated for an empty card as shown in Fig. 18.

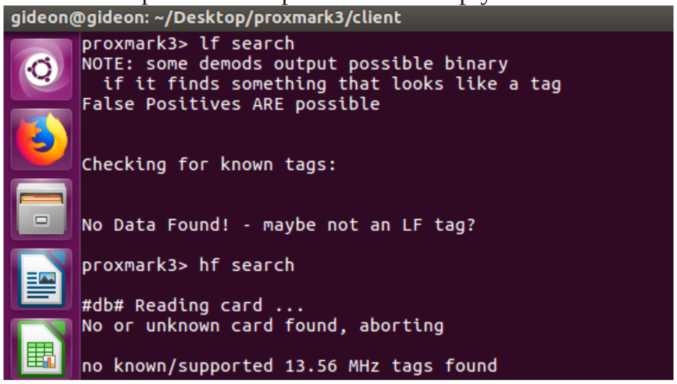

Fig 18 Checking for tags in an empty card

v. The cloning of the unknown card (LF card) is accomplished when its contents are copied into the empty card. This is done with the command: *lf em 410xwrite*. Confirmation can be done with the *lf search* command on the clone card as shown in Fig. 20.

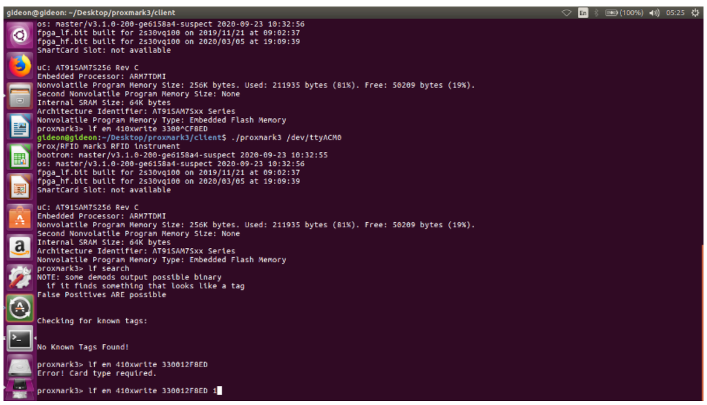

Fig 19 Cloning the card content of the LF card

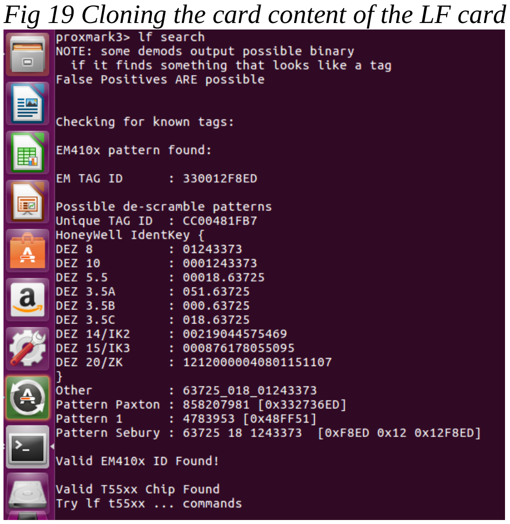

Fig 20 Output of lf search on the clone card

As it has been shown above, the attack was successful and the RFID access card was cloned to gain access to a security door lock system. This research has shown the vulnerabilities that confronts the RFID industry, which finds application in many spheres of endeavour, especially security. This calls to question, how safe personal belongings of customers who stay in hotels are, how secure goods and services in our warehouses are, and how safe records in academic institutions are. The

RFID industry is a fast-growing industry as security is transitioning from mechanical to electronic. Hence, efforts should be made to increase its integrity as much as possible.

5 Conclusion

The RFID card system is one of the most widely used access control system in the world, but unfortunately, it is also one of the most vulnerable system due to the ease with which it can be breached via cloning. Improvements such as encryption of the high frequency cards make it a little bit safe but more ways to make it safer should be implemented so as to safeguard information and properties of users of this security system.

6 Acknowledgment

The authors wish to acknowledge the assistance and contributions of the staff of Departments of Computer and Electrical/Electronic Engineering, University of Benin, Benin City toward the success of this work.

7 References

[1] TECHNOLOGY RFID/NFC Webpage. Available on https://www.freaquent.com/technology-rfid-nfc.php (accessed on November 2020)

[2] Connecting Up Webpage. Available on https://www.connectingup.org/learn/articles/introduction-ubuntu#:~:text=Ubuntu%20is%20based%20on%20the,reputation%20for%20stability (accessed on November 2020)

[3] Fernández-Caramés, T.M., Fraga-Lamas, P., Suárez-Albela, M. and Castedo, L., 2017. Reverse engineering and security evaluation of commercial tags for RFID-based IoT applications. Sensors, 17(1), p.28.

[4] Lim, T.L. and Li, T., 2008, September. Exposing an effective denial of information attack from the misuse of EPCglobal standards in an RFID authentication scheme. In 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (pp. 1-6). IEEE.

[5] Bu, K., Liu, X., Luo, J., Xiao, B. and Wei, G., 2013. Unreconciled collisions uncover cloning attacks in anonymous RFID systems. IEEE Transactions on Information Forensics and Security, 8(3), pp.429-439.

[6] Suliman, A., Shankarapani, M.K., Mukkamala, S. and Sung, A.H., 2008, May. RFID malware fragmentation attacks. In 2008 International Symposium on Collaborative Technologies and Systems (pp. 533-539). IEEE.

[7] Halevi, T., Li, H., Ma, D., Saxena, N., Voris, J. and Xiang, T., 2013. Context-aware defenses to RFID unauthorized reading and relay attacks. IEEE Transactions on Emerging Topics in Computing, 1(2), pp.307-318.

[8] Ayoade, J., 2006. Security implications in RFID and authentication processing framework. Computers & Security, 25(3), pp.207-212.

[9] Weiß, M., 2010. Performing relay attacks on ISO 14443 contactless smart cards using NFC mobile equipment. Master's Thesis in Computer Science, University of Munich.

[10] Guizani, S., 2015, August. Implementation of an RFID relay attack countermeasure. In 2015 International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 1318-1323). IEEE.

[11] Hancke, G.P., Mayes, K.E. and Markantonakis, K., 2009. Confidence in smart token proximity: Relay attacks revisited. Computers & Security, 28(7), pp.615-627.

[12] Francillon, A., Danev, B. and Capkun, S., 2011. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS). Eidgenössische Technische Hochschule Zürich, Department of Computer Science, pp.4-6

[13] FCC ID Search Webpage. Available online: https://www.fcc.gov/general/fcc-id-search-page (accessed on 1 November 2020).

[14] Myriad-RFWebpage. Available online: https://myriadrf.org (accessed on 1 November 2020).

[15] HackRF One Webpage. Available online: https://greatscottgadgets.com/hackrf (accessed on 1 November 2020).

[16] Kevin Chung – 'Rfid Hacking with The Proxmark3 Available on *https://blog.kchung.co/rfid-hacking-with-the-proxmark-3.*