Exploitation of Radio Frequency Technologies Through the use of Microcontrollers

Daniel J. Joachim Jr.
Lord Fairfax Community College
Middletown, Virginia, United States of America
email: djj2985@email.vccs.edu

Abstract—**Radio Frequency Identification (RFID) uses a simple principle of signal broadcast by a transmission station. The signal is broadcasted to the open air and intercepted by a metallic object whose molecular structure reflects the wave being broadcasted back to the transmission station. The transmitting station can then evaluate the signal to determine the identity of the object. RFID has been around since World War I, but due to cost, research was limited. It was not until militarization during World War II that RFID research was cost effective. The RFID technology is used within offices buildings, airports, grocery stores, and academic institutions for access control. This paper is a study in which the evolution of RFID was reviewed and an attempt was made to exploit the encryption of a German Schoko Ticket and District of Columbia (D.C.) Metro MiFare card RFID signals, by using publicly available devices. The devices used were Arduino micro-controller board and an MFRC522 RFID reader. The research showed that both of the RFID cards included in the student were actually from the MiFare DESfire family and that there is a security threat to these cards that users need to be aware of.**

Keywords- RFID; cybersecurity; Microcontroller; Arduino.

I. Introduction

After the conclusion of World War I, military forces turned their attention towards technologies that would provide clairvoyance, in reference to future attacks. Research on radio technologies up to this point was expensive to facilitate an had little rate of success. This held true until a discovery by the United States Research Laboratory (NRL)[3]. The NRL had successfully broadcasted a signal towards a secondary location across the Potomac river, which was refracted by a naval vessel upon its transmission.

RFID is a technology that is used for access control purposes by people and objects. This is widely used by academic institutions and corporate business offices where tapping of the personal RFID chip based card on the tag reader will grant employees access to secure areas to aid in security of data. Similar technologies are used in keeping track of inventory at the local grocery stores and to gain access to public transportation systems. RFID helps the world meet various organizational needs and in most situations is a cost effective process.

The Pre-Pottery Neolithic Era was the first to create large scale storage facilities to store food that had been left over from their gathering season [1]. People living during this time chose a location that was remote to their villa, ensuring that their precious food was easily accessible. Their existence depended on access to food, marking the creation of the first theorized security. As mankind traversed from stone to bronze, securities shifted to follow the progression. Once mankind had established a way to produce food, they realized the need to protect their food source from danger – resulting in the erection of walls around the town villa. The concept of securing critical possessions has followed us into the world that we live in today. We have locks on the front doors of our homes, armed military guards around the white house, and access cards to control our entry to our place of work. The physical dangers of having a neighboring tribe raiding the village and stealing the village's food have been translated into the digital danger of using a weak password to protect monetary funds from cyber criminals. As civilization progresses through the Technological Age, it has created a commodity; the security of digital data. Business, organizations, governments, educational institutes and municipalities all rely on the confidentiality, availability and integrity of data to ensure continuity in their respective field of practice. The identification of this commodity has opened a wide range of opportunities for both offensive and defensive members of the Information Technology (IT) taskforce. With each defender's innovation, a challenge is posed to the offender. This affinity has been identified as *Red Team versus Blue Team* [2].

This paper is a study about RFID technology to understand its security threats and use of the German Schoko Ticket and District of Columbia (D.C.) USA Metro MiFare card for transportation systems. Cards are used to ride on public buses and trains and record the passenger travel on the system. Each time the card is swiped for entry at bus or train stations, data is transmitted that someone may intercept. The study concluded with a Red Team [2] approach to exploit, extract information contained on RIFD technologies and provide a structured understanding of inner workings of Access Control (AC) Systems. Section II provides a brief history of security technologies, while Section III provides a brief background of access control technologies. In Section IV, Microcontrollers and RFID cards will be discussed. Section V will present the exploratory research and the conclusions from the findings of the research from Section V, will be discussed in Section VI.

ISBN: 978-1-61208-764-1

II. History

A. Primitive Technologies

The origins of Radio Wave Technologies can be traced back to Scottish physicist James Clerk Maxwell. Maxwell theorized the first correlation between magnetism, electricity, and light. His discoveries can be summarized into three primary concepts:

- Electricity may penetrate most metallic objects because of movement of electrons within the atom. When electrons move, they create a magnetic field [3].
- Electromagnetic devices may be combined into one device. Fluctuating magnetic waves produce an electric current [3].
- Radio Waves share the same characteristics as light waves, but with varying frequencies [4].

These discoveries supplied the groundwork for scientists and engineers to fabricate technologies utilizing wireless communication. “His work was later adopted by German physicist, Heinrich Hertz, refracted a 66cm radio wave off dielectric and metallic objects “ [5]. Six-teen years later, the first patent for a ship navigation device utilizing his technology was issued to German engineer, Christian Hansmeyer, who received acceptance for his patent from multiple countries [5]. Despite being awarded his patents, the complexity of the invention prevented it from becoming a tool that could be commonly utilized until its adoption by the military for approximately another 20 years.

B. Radar

Monopulse radar, which NRL developed in 1943, is the basis for all modern tracking and missile control radars in the United States [1].

III. Access Control

Resources are critical to the development of private infrastructures, government agencies and organizations alike. To ensure the continuity, integrity, and authenticity of an organization’s resources, i.e. data,, certain preventative access measures are put in to place. Access control is referenced as any mechanism used within an information system for granting or denying approval to used specific resources [6]. This may be accomplished through external perimeter defenses, internal physical access security, and physical device security.

A. Types of Physical Access Control

There are many thigs that have been used for physical access controls, such as barriers, cages, barricades, bollards, motion detection systems, security personnel, keyed door locks, deadbolt locks, and cipher locks.

B. Types of Electronic Access Control

This study focuses primarily on the components used to read and write information located within an RF identifiable object. This study will refer to that object as a tag, card or fob interchangeably. This work focuses primarily on the components used to read and write information located within an RFID identifiable object. The words: “tag”, “card”, “token” and “fob” may be used as an interchangeable reference to the device that holds the data activated by the RFID reader. RFID tags consist of four primary components that allow their data to be accessed by the RFID reader: transponder, rectifier circuit, controller and memory.

The RFID reader consists of three primary components: signal generator, Microcontroller and receiver. The signal generator and receiver are sub-derivatives of the analog circuit block, which is responsible for driving the radio signal and receiving the radio signal’s modulated voltage. This analog data is then covered by an Analog-Digital-Converter and passed to the Microcontroller to enumerate the cryptographic functions that have been performed by the tag, as seen in Figure 1 below [8].

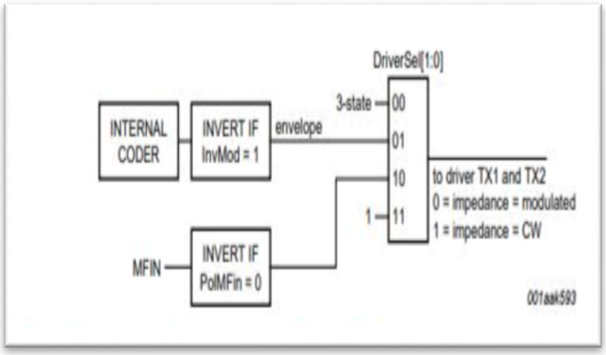
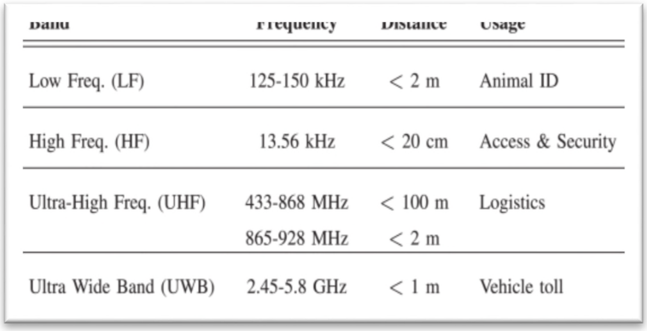


Figure 1. Serial Data Switch for p-driver Tx1 & Tx2 [8].

C. RFID

The three frequencies that tags normally operate at are Low (LF), High (HF), and Ultra High (UHF) [18][19]. Figure 2 shows the common bands that RFID operates within.



Band	Frequency	Distance	Usage
Low Freq. (LF)	125-150 kHz	< 2 m	Animal ID
High Freq. (HF)	13.56 kHz	< 20 cm	Access & Security
Ultra-High Freq. (UHF)	433-868 MHz 865-928 MHz	< 100 m < 2 m	Logistics
Ultra Wide Band (UWB)	2.45-5.8 GHz	< 1 m	Vehicle toll

Figure 2. Common RFID Operating Bands [22].

RFID is popular because it offers improved security in access control to reduce theft, allows for tag linking, automated identification, location tracking, reduction of human interaction, improved data integrity, and range reading capability and high data transfer rate [20]. There are many applications where RFID is used, as seen in Figure 3 below.

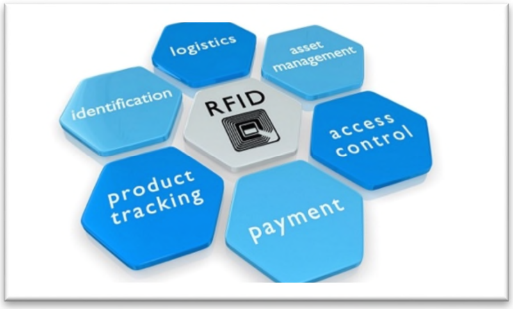


Figure 3. RFID Applications [21].

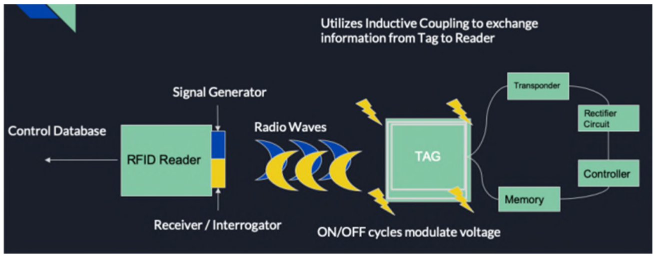


Figure 4. Access Control Systems - Component Information.

The component information for this study is found in Figure 4 above. These components consist of a database, RFID Reader, signal generator, Interrogator, and a tag.

IV. MICROCONTROLLERS & CARDS

For the sake of this study, the terms “Microcontroller”, “microprocessor” and “chip” will be used interchangeably. Microcontrollers are chips or microcomputers manufactured through Very-Large-Scale Integration (VLSI), a process where thousands of transistors are combined into a single chip. This chip may be used as an embedded component of a Real Time Operating System (RTOS). The advantages of this technology over prior semiconductor technologies are its ability to produce a chip that is smaller, less expensive, faster, requires less power and contains more logic gates than preceding chips [9]. The word “Microcontroller” is used as a misnomer for the word “Microcontroller Board”, which references the Printed Circuit Board (PCB) holding the Microcontroller, the integrated Random Access Memory (RAM) on the chip and the peripheral Input / Output (I/O) circuits that are attached to the PCB. Common Microcontroller applications include: robotics, smart home automation, car engines, computer peripherals, mobile phones, washing machines, cameras and security alarms [10].

A. Microcontrollers

The primary function of a Microcontroller is to process binary data. This is accomplished by passing electrical pulses representing data through a series of registers and transistors called logic gates to perform the desired binary arithmetic. Two common applications of computational instruction sets are Complex Instruction Set Computer (CISC) and Reduced Instruction Set (RIS). A RIS Computer (RISC) accepts only one operand per instruction cycle whereas a CISC compacts operand arguments into one instruction. CISC require more physical logic gates within the processor to execute the commands stored within the processor’s registers, therefore making this technology more expensive. RISC technologies are still used as they provide backwards compatibility to processors that have not been designed and/or capable of accepting CIS commands [9]. Common examples of Reduced Instruction Set opt codes for binary arithmetic include: ADD, AND, OR, XOR, and NOT. The density of the binary data that is being transmitted every clock cycle should be known as a “word length”. This number is often referenced by the word “bit” after the respective word size. The maximum amount of data that a Microcontroller can process is determined by the width of the registers contained within the controllers Arithmetic Logic Unit (ALU). A 8-bit Microcontroller is capable of transmitting 0x00 – 0xFF (0 – 255) per clock cycle, while a 16-bit bit processor is capable of performing arithmetic with a range of 0x000 – 0xFFFF (0-65535) per clock cycle [11].

Microcontroller families may be identified by one of the following characteristics: bit depth, memory architecture, simple / complex instruction or memory devices [11]. Microcontroller boards are simply small form factor Printed Circuit Boards (PCB) that are designed to handle a single operation or program. They operate in the same way that the computer’s PCB is being used to view this journal. Microcontroller boards or, single-board Microcontrollers, are comprised of a Microcontroller that is implanted or imbedded on to a PCB. These boards have low power draw, are small formfactor and contain I/O systems that enable the use of multiple sensory devices. They are inexpensive -- currently as of March 2019, the Arduino Uno REV3 costs $22.00 excluding tax and shipping [12]. Controller boards are manufactured by a wide range of vendors [9]. some such as Arduino and Raspberry Pi, provide open source documentation to the controller board, as well as source code for projects of any application [10].

Microcontroller boards share some of the same characteristics as Microcontrollers but are to be considered the component that hosts the embedded Microcontroller rather than the component being embedded into the Real Time Operating System. Microcontroller boards share the following characteristics:

- They must contain a way to preform binary arithmetic via a processing unit. These Microcontrollers may be embedded or modular.

- They must have a means to load a program into memory. This is typically done through a Easily Programmable Read Only Memory (EPROM) chip, or Electrically Erasable Programable Read-Only Memory E2PROM chip that is stored on the Microcontroller board.

B. *Arduino*

Arduino is an easy to use, open source, project-oriented Microcontroller board developed by Interaction Design Institute Ivera in Ivera, Italy [8]. Its sources can be traced back to Hernando Barragán, who laid the schematic foundation of the Arduino project [8]. Missimo Banzi and David Cuartielles sought to build from Hernando's work, creating user friendly programmable device geared towards design and interactive art [8]. David Mellis thereafter joined the development team, created the Arduino Independent Development Environment that was designed paralleled with the board's schematics. Gianluca Martino and Tom Igoe were the last two members to join the Arduino project [8]. These five members are known to be the original creators of Arduino [8]. The purpose of Arduino's creation was to provide an inexpensive, easy-to-use tool that allowed designers interoperability between hardware components. This resulted in the Atmel AVR 8-bit processor (Atmega8) to be selected during the board's prototyping phase [17].

C. *MiFare Card*

The Mifare RFID card was used in this study has an internal memory of 1 kB. This memory is divided into sixteen sections, each section composed of four blocks of sixteen bytes, see Figure 5 below.

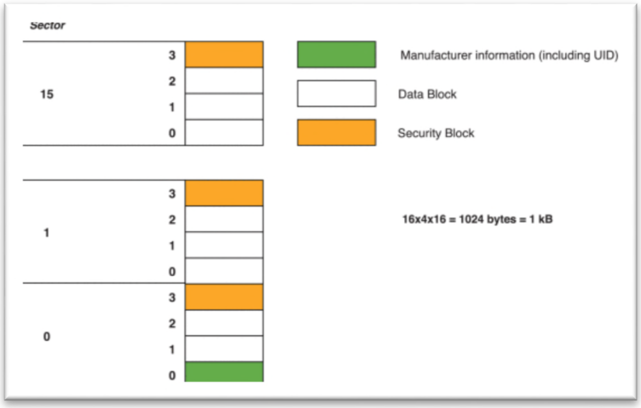

Sector
15
3
2
1
0
1
3
2
1
0
0
3
2
1
0
Manufacturer information (including UID)
Data Block
Security Block
16x4x16 = 1024 bytes = 1 kB

Figure 5. Details of the memory organization of the Mifare RFID [9].

The first block of the first section includes the card Unique IDentifier (UID) and the rest of the blocks are reserved for application data that can be read and written by the user, e.g. usually user-related information [22].

V. Exploitation Research

In October 2008, the Netherland educational institute, Radboud Universität Nijmegen, announced its intentions to publish the complete reverse engineering of the CRYPTO-1 algorithm used by NPX Semiconductor's MiFARE Classic cards. NPX Semiconductor is an American Dutch semiconductor manufacturer who responded by placing the publication under judicial process in hopes to prevent it from being published, eventually being overruled by legislature under constitutional freedom of speech [23]. Libraries may be built around to aid the exploitation of the ~3.5 billion MiFARE cards are in circulation around the world [24]. Shortly after, security research company "Nethemba" published "MFOC", a package for nested offline attacks on MiFARE Classic cards. Andrei Costin, an assistant professor at University of Jyvaskyla in Finland, also received a great benefit from the research conducted was the development of the MiFare Classic Universal Toolkit now known as "MFCUK" [25]. These tools allow for the complete enumeration and replication of cards that implement the CRYPT0-1 encryption algorithm aided by Microcontrollers with RFID reader-writers. These software libraries, among others, have been combined to form the first multi-platform low level RFID Application Programing Interface known as Near-Field Communications (NFC) tools provides functionally between a multitude of RFID reader-writers. NFC-Tools is integrated by default with downloading the latest platform of Kali Linux and is considered the de-facto library for cracking MiFARE Classic cards.

In this study, cloning to a blank and re-writable RFID card is a relatively inexpensive and easy approach to execute two main types of attacks known as card skimming and unauthorized use. RFID card skimming captures the data without the card owner's knowledge and then the attacker uses the data to clone a new card to impersonate the legitimate user's authentication systems. RFID card unauthorized use is when a card is replicated to give the attacker authenticated access to specific services such as ability to ride a Metro train or bus.

With these vulnerabilities in mind, a model attack was setup with a clone RFID card. The writing block is composed of an Arduino RC522 RFID reader. To complete this cloning process, the test cards were written to blank tags. Then the card information is directly obtained from the application layer and must be inserted manually on the Arduino sketch. The Arduino UNO was coded in Arduino C using the MFRC522 open source library [26] to interact with the rC522 RFID reader.

VI. Conclusions and Future Work

There are several known vulnerabilities associated with the use of RFID technology that have major impact on card owners, who become victims. The use of RFID-based cards in the context of Public Transportation Systems, such as Metro, presents several vulnerabilities that compromise their effective use for authentication and balance tracking. Current use of the tested cards provides an opportunity for attackers to easily and successfully carry out card cloning attacks.

This research was paired with an attempt to break the encryption of the German “Schoko Ticket” and District of Columbia “Metro” MiFARE cards. The Arduino Uno Rev3 was the Microcontroller board that was supplied paired with the RFID-RC522 RFID reader-writer to conduct tag enumeration and reading/writing. The MFRC522 was the Arduino library used to control the RC522 reader. The results showed that by using low-cost commercial-off-the-shelf hardware and open-source source software, it is easy and simple for cyber criminals to perform attacks. These vulnerabilities allowed for cloning of any RFID card within the testing RFID reader range. This means that if an attacker can get close enough to any Metro RFID card with a RFID reader, the card maybe cloned and then used to ride for free on the public transportation system.

Methods of reducing these types of attacks include changing the authentication from the default, applying cryptographic algorithms on transmitted data to hide information, employ encrypted access tokens on data blocks to identify the RFID owner, add a privacy bit controlled, or employ random numbers to identify the card.

Future research may be using the RFID device around campus to see if able to obtain and clone fob data that faculty, maintenance staff, and security use to enter into restricted areas.

Acknowledgment

The author would like to thank Dr. Melissa Stange for providing the Arduino Kit. I also want to thank Lord Fairfax Community College and Dr. Melissa Stange for their support with this work.

References

[1] CompTIA. Are You Red Team or Blue Team? How Your Skills Fit into a Cybersecurity Career. [Online]. Retrieved November, 2020 from https://certification.comptia.org/it-career-news/post/view/2018/09/28/cybersecurity-red-team-or-blue-team, 2018.

[2] I. Kuijt & B. Finlayson. Evidence for food storage and predomestication granaries 11,000 years ago in the Jordan Valley . PNAS,07-Jul-2009. [Online]. Retrieved November, 2020 from https://www.pnas.org/content/106/27/1096

[3] J.C. Maxwell. Discoveries - James Clerk Maxwell - Science Hall of Fame - National Library of Scotland. Retrieved November, 2020 from https://digital.nls.uk/scientists/biographies/james-clerk-maxwell/discoveries.html#electro, 2019.

[4] P. Higgs. Electromagnetic Theory. Electromagnetic Theory. [Online]. Retrieved November, 2020 from http://www.clerkmaxwellfoundation.org/html/electromagnetic_theory.html, 2020.

[5] M.I. Skolnik. Radar. Encyclopedia Britannica, Encyclopedia Britannica, Inc., [Online]. Retrieved November, 2020 from www.britannica.com/technology/radar/History-of-radarI. 2020.

[6] M. D. Ciampa. 9-2a External Perimeter Defenses, 6th ed, 2018.

[7] Bosnianbill. Kaba Simplex Door Combination Lock Defeated w/Sparrows MAGNETO. YouTube. Retrieved November, 2020 from https://www.youtube.com/watch?v=2KSoPIeN9wY, 2015.

[8] NXP Semiconductors. Retrieved November, 2020 from https://investors.nxp.com/news-releases/news-release-details/nxp-semiconductors-reports-fourth-quarter-and-full-year-2017.

[9] MFRC522 Microchip Technology Inc. [Online] Retrieved Novemer, 2020 from “http://ww1.microchip.com/downloads/en/DeviceDoc/Microchip 8bit mcu AVR ATmega8A data sheet 40001974A.pdf, 2017.

[10] J. M. Hughes. Arduino: A Technical Reference, O'Reilly. [Online]. Retrieved November, 2020 from https://www.oreilly.com/library/view/arduino-a-technical/9781491934319/ch01.html, 2016.

[11] VLSI. Development and Basic Principles of IC Fabrication, Electronics For You, [Online]. Retrieved Novemer 2020 from https://electronicsforu.com/resources/learn-electronics/vlsi-developments-ic-fabrication, 2017.

[12] Types and Applications of Microcontrollers, Engineering Institute of Technology. [Online]. Retrieved November, 2020 from https://www.eit.edu.au/cms/resources/technical-resourses/types-and-applications-of-Microcontrollers

[13] S. D. Burd. Chapter 6 System Integration and Performance in Systems Architecture, 7e ed., Boston, MI: Cengage, pp. 120–121, 2015.

[14] Microcontrollers, Introduction Microcontrollers Types and Applications, ElProCus. [Online]. Retrieved November 2020 from: https://www.elprocus.com/Microcontrollers-types-and-applications/, 2018.

[15] What is a Raspberry Pi?,” Opensource.com. [Online]. Retrieved November 2020 from https://opensource.com/resources/raspberry-pi, 2020.

[16] Microchip, ATmega8A - 8-bit AVR Microcontrollers. [Online]. Retriveved Novemer 2020 from https://www.microchip.com/wwwproducts/en/ATmega

[17] S. Jacoband C.P. Bean. Fine particles, thin films and exchange anisotropy in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, pp. 271-350, 1963.

[18] A. Hagl and K. Aslanidis. RFID: Fundamentals and applications, RFID Security, pp. 3-26, 2008.

[19] R.K. Mota. Role of Cryptographic Welch-Gong (WG-5) Stream Cipher in RFID Security, 2012.

[20] Y.Z. Mehrjerdi, "RFID enabled healthcare systems: risk□benefit analysis", International Journal of Pharmaceutical and Healthcare Marketing, 2010

[21] RFIDHY Technology. [Online]. Retrieved November 2020 from https://www.rfidhy.com/how-is-rfid-used-in-real-world-applications/, 2019.

[22] H. Pereira, R. Carreira, P. Pinto and S. I. Lopes, "Hacking the RFID-based Authentication System of a University Campus on a Budget," 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Sevilla, Spain, pp. 1-5, doi: 10.23919/CISTI49556.2020.914094, 2020.

[23] E. Mills. Dutch chipmaker sues to silence security researchers. [Online]. Retrieved Novemer, 2020 from https://www.cnet.com/news/dutch-chipmaker-sues-to-silence-security-researchers, 2008.

[24] M. Almeida. Hacking Mifare Classic Cards. [Online]. Retrieved November, 2020 from https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf, 2014.

[25] A. Costin. Firmware.re and Jyu.Fi. [Online]. Retrieved November, 2020 from https://www.blackhat.com/us-18/speakers/Andrei-Costin.html, 2018.

[26] Arduino Library List. [Online]. Retrieved November, 2020 from https://www.arduinolibraries.info/libraries/mfrc522.