“project_doppelgänger – A Lesson in the Consequences of Trusting Unencrypted RFID”

Jimin Lee

Table of Contents

Abstract

Whether you like to pay with contactless or open doors with keycards, it's safe to say that RFID technology has cemented itself within our culture as the de facto way of authentication. But as with every technology, flaws and vulnerabilities are to be assumed if not expected and RFID is no exception. However, the critical moment that determines the security of a technology occurs when known vulnerabilities are patched and addressed especially when the costs of not doing so can grant unauthorised personnel access to buildings containing sensitive data and more importantly, vulnerable people. But with the neglected nature of enterprise systems even after the flaws of such common RFID systems have been readily disclosed, most organisations overlook the consequences of these vulnerabilities until it is too late. Within this essay, I will explore the illusion of trust fabricated by the white cards and the blue fobs, trust that I believe has been misplaced.

Introduction

Technology has this distinctive ability for exponential growth not often seen in other fields of industry. From the invention of the smartphone to the widespread growth of the personal computer, it could be said with certainty that the tech industry is like no other. Some attribute this growth to the vast potential within technology. Whilst I do mostly agree, I believe the one element that is too often overlooked is the competitive nature of the industry. Start-ups brawl with each other often using underhanded tactics in the name of increasing market share whilst established corporations knowingly take temporary losses in order to secure their names in the future of the industry.

But as with every extreme, there must be a flipside to be uncovered.

Enterprise systems include software and hardware intended for use in large-scale commercial settings and are mostly found within standardised systems intended for use to be compatible with as many pieces of pre-existing hardware as possible. However, this comes at the cost of either security or convenience and when hours spent in order to properly train staff to use systems securely is often seen by executives as a mere hindrance to their vision of exponential year on year growth, security is treated as an afterthought whilst priorities lie in having staff wear professional looking ID badges, disregarding the potential exploits that may be enabled through the use of these cards.

Within this essay, I will explore how RFID technology works, the common use cases of RFID technology within the general public, known exploits and vulnerabilities of these technologies, proposed plans to mitigate these attack vectors and finally to evaluate whether the usage of these technologies is justified considering the vulnerabilities presented.

What is RFID and How Does it Work?

RFID or Radio Frequency Identification can be dated as far back as 1973 [1] when Mario Cardullo was granted a patent (shown in Figure 1.1) that included a passive transponder device that could be powered wirelessly by an external transmitter to have the device respond with the contents of the data held within its memory. This technology was initially intended for use in automated toll booth systems so that drivers would no longer have to pay tolls tediously with cash and instead be able to have them processed automatically, ensuring a smooth flow of traffic.

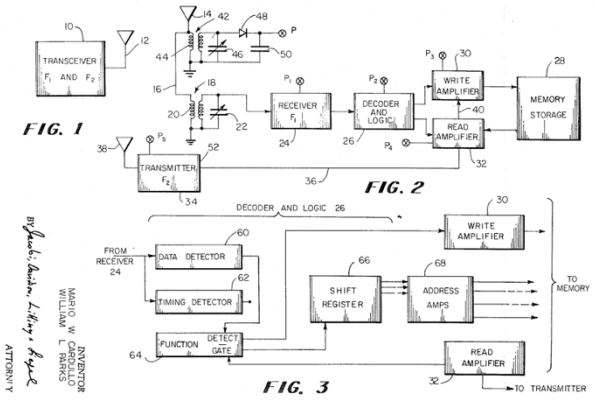

Figure 1.1
[34] 'Transponder apparatus and system' granted to M. Cardullo et al.

However, more modern implementations of RFID all stem from the ISO/IEC 14443 and ISO/IEC 18000-2 standards which outline the guidelines that manufacturers of RFID enabled technologies must follow for their products to be compatible with other RFID enabled devices. [2] Examples of physical attributes required by the standard include features such as protection from UV light at levels experienced "in ordinary daylight at sea-level". More importantly, the standards also define the operating frequencies which all standard compliant devices should run at. The ISO/IEC 14443 states that "The frequency *fc* of the RF operating field shall be 13,56 MHz" whilst [3] ISO/IEC 18000-2 states that

"Type A tags are permanently powered by the interrogator, including during the tag-to-interrogator transmission, and operate at 125 kHz." whilst

"Type B tags are powered by the interrogator, except during the tag-to-interrogator transmission, and operate at 125 kHz".

Admittedly, this raises more questions than it answers. What is a 'Type A' tag and how does it differ to a 'Type B' tag? What does the specification mean when it refers to an 'interrogator'?

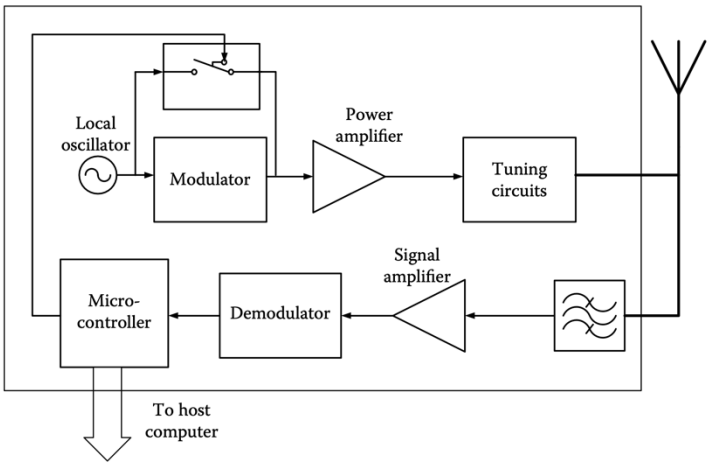

Figure 1.2
[4] Basic block diagram of a generic interrogator.

[4] An interrogator is a device that can be simplified to its two distinct functions: firstly, to generate and transmit the radio frequencies to power the tag and secondly, to receive and decode the signals generated by the tag. However, within more advanced implementations of the RFID protocol, interrogators may also can also transmit specific commands to the tag, facilitating bidirectional communication for features such as tag writing or locking. In order to both transmit and receive radio signals, bidirectional communication is achieved through the transmission of backscattered signals meaning that the tag's circuitry changes the resistance of the tag's antenna causing a transmission of RF waves that the interrogator then receives and decodes. Common examples of RFID interrogators include card machines with 'Apple Pay' support, hotel doors with contactless keycards, anti-theft pedestals commonly found within retail environments and many more.

Exploring Active and Passive RFID

As mentioned earlier, RFID tags have two main variants depending on their power source. Type A tags – more commonly known as [5] passive tags – rely on the radio frequency signals transmitted by the interrogator to transmit the contents of its memory whilst Type B tags – more commonly known as active tags – have their own power source usually in the form of an on-board battery within the tag. Due to the key differences presented within each type of tag, they both present their own unique sets of advantages and disadvantages.

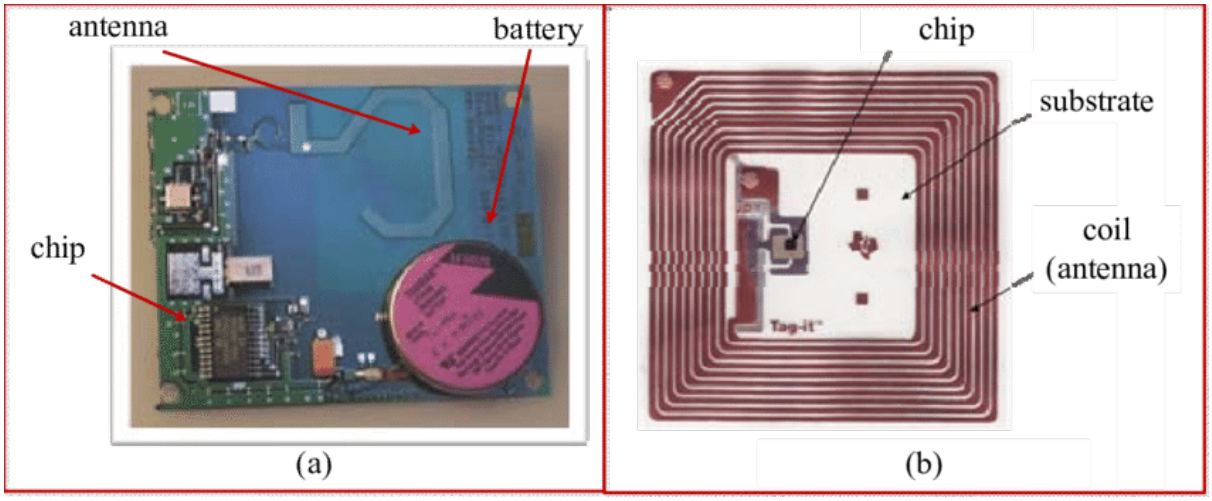

Figure 1.3
[35] Image of a disassembled active tag (left) and passive tag (right)

Active tags have the advantage of being able to transmit a much stronger signal as they have their own power source (see Figure 1.3) meaning that they do not have to rely on backscattering signals which are much weaker than signals produced by a dedicated power source thereby enabling them a greater range of operation. However, with the added circuitry required to accommodate the extended features included in an active tag along with the battery required to power it, this substantially increases both the cost and size of the overall tag which severely limits the use cases that an active tag may be appropriate for use in.

On the other hand, passive tags have the advantage of being much less expensive due to the lack of an internal power source. This also comes with the benefit of being much lighter and smaller since passive tags do not require the presence of a battery to be sealed within the structure of the tag. However, this comes at the drawback of range. Due to the requirement of backscattering present within passive tags, they can only operate at a distance of [5] “a few inches to 30 feet (**≈9.14m**)” from the interrogator whilst active tags can operate at a much greater range of [5] “20 to 100 meters”.

Furthermore, according to Fujitsu, their [6] Datasheet for the ‘High-Capacity FRAM RFID Tag’ suggests that the highest capacity RFID tag on the market is 64KB.

An Analysis of 125KHz and 13.56MHz RFID

[7] 125KHz RFID – also known as LF (low frequency) RFID – communicates at a lower frequency compared to higher frequency variants of RFID such as 13.56MHz RFID – also known as HF (high frequency) RFID – or 840MHz+ RFID – also known as UHF (Ultra High Frequency) RFID. However, since UHF RFID is intended for use within applications where higher range and data transfer speeds are paramount to the usage, they are rarely ever used within door access control systems and therefore lie outside of the scope of this project.

A distinctive advantage of LF RFID is its ability to transmit signals through water and metal due to its substantially longer wavelength compared to other variations of RFID with higher frequencies. This makes LF RFID ideal for door access control applications as it ensures that everyday items such as clothes or jewellery do not interfere with any communication between the tag and the interrogator. However, due to the lower frequencies supported by LF tags, the rate at which radio signals are turned on and off to represent high and low logic states respectively is further limited which leads to a drastically restricted data transfer speed and is therefore unsuitable for any applications that require lots of data to be stored on the tag as it would require the user to hold the tag up to the interrogator for long periods of time proving to be both ineffective and unintuitive.

[8] One of LF RFID's most significant weaknesses was its lower capacity leading to LF tags commonly only holding a 64bit serial number as the contents of its memory. This alongside its inability to be rewritten meant that any authentication with a 125KHz RFID tag lacked any encryption and therefore the security and integrity of the authentication depended on LF's inherent limitation of being read-only and most importantly, hinged on the serial number of the tag being kept unexposed.

Apparently, manufacturers didn't get the memo.

Figure 1.4
[9] [10] [11] Product images for popular LF RFID tags/cards currently sold in online retailers for enterprise hardware

On the other hand, HF RFID is a newer development which seeks to solve the issues that were present within LF RFID. Due to its higher operating frequency, HF RFID has a much higher data transfer speed, [8] enabling it to hold significantly more data with tags typically holding around 1KB of data spread over 16 sectors. Furthermore, through the advancements within integrated circuits, higher end HF RFID tags also have the capability to encrypt the contents of the tag, enabling secure authentication for use within enterprise environments. Initially, some may raise concerns at the extended operating range of 13.56MHz RFID tags as this may cause unwanted authentication which may only serve to

sabotage the superior security present in HF tags. However, this problem is easily rectified by either integrating coils with fewer turns or to decrease the current emitted by the interrogator to ensure accidental transponder communications do not occur.

Furthermore, HF tags appear to be cheaper than their LF counterparts due to their greater demand and usage, allowing the effects of economies of scale to play a leading role within the price, further lowering costs due to their [12] mass production enabling higher levels of efficiency as weaker links within the supply chain get addressed through automation and stricter quality control standards which are qualities that less likely to be seen in less established supply chains such as LF tags that are slowly being phased out for more secure alternatives such as HF.

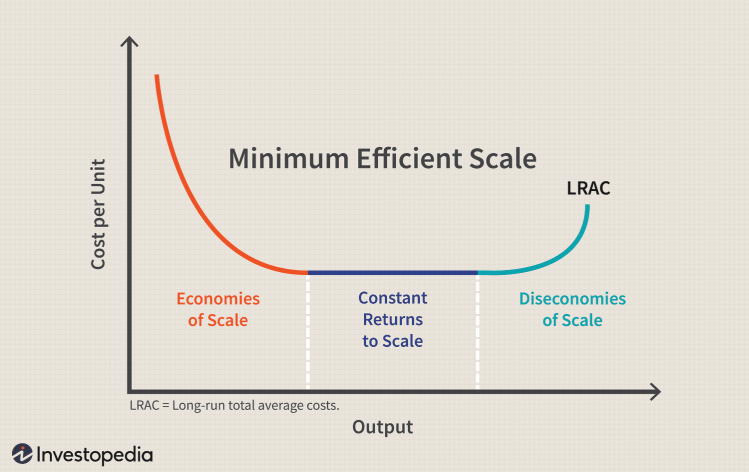

Figure 1.5
[36] A graph showing the effects of economies of scale.

As the evidence suggests, HF is a much more secure and reliable technology compared to its predecessor, LF. Therefore, I suggest that any new RFID-enabled access control systems be fitted with a control panel that supports HF at the very minimum and strongly encourage considering options that implement encryption within its authentication procedure. However, when searching for commercial applications of secure RFID to include within my research, I found systems that implement unencrypted 125KHz RFID that are listed on [13] Amazon as “the safest, closest to modern technology” and that it is suitable for “Home/ hotel/ office/ apartment/ factory” applications. Not only are these false claims both deceitful and harmful to the end user, but they are also perpetuated by Amazon’s labels such as ‘Amazon’s Choice’ and ‘Amazon Best Seller’. When such blatant lies are not only allowed but encouraged on a platform as substantial as Amazon, how will the industry ever move forward when it seems the only priority is to increase quarterly revenues and make a quick sale whilst security is a mere afterthought that can be afforded to be put on the backburner until you get caught?

Part 2 – Applications of RFID

Since RFID is only a standard defined by established organisations such as the ISO/IEC, the IC - or Integrated Circuit that is the heart of the RFID tag’s functions – is manufactured by companies that license the RFID design from the ISO/IEC and develop their own implementations of these technologies, each with their own distinct improvements and drawbacks from the standardised design. To align with the scope of this project, I will mainly be focusing on NXP’s implementations of RFID as they hold the most prominent position within the access control/authentication market.

To say that NXP has had success with their 'MIFARE' brand would be nothing short of a vast understatement. 'MIFARE' was a subsidiary of Philips Electronics that was acquired by NXP in 2006 and has enjoyed a dominant position in the market making up usage in [14] "over 750 countries" with approximately "1.2 billion" active users of their technology having shipped over "12 billion ICs" to date. NXP markets their 'MIFARE' products as a strategy to replace outdated and vulnerable technology such as [15] "magstripe, barcode and QR-code infrastructures".

'MIFARE Classic' is their original card with limited encryption features however contains 16 blocks of data each with 64 bytes of data per block to come to a total capacity of 1KB.

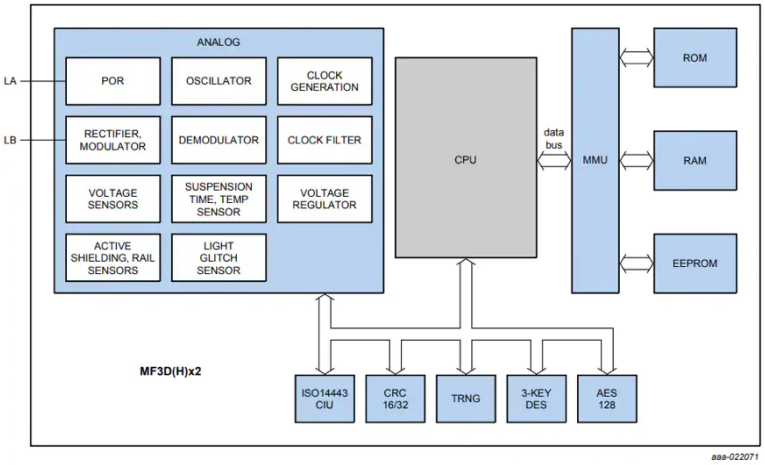

Figure 2.1
[37] Diagram illustrating the MIFARE DESFire architecture with hardware encryption on-board

'MIFARE DESFire' is NXP's latest product line where the cards introduce [14] heavy encryption into the standard with 2-key/3-key DES (Data Encryption System) as well as AES encryption to ensure the integrity of these cards. Using encryption where blocks are encrypted 2/3 times over to maximise security, NXP has cemented DESFire as the industry standard when searching for a high-security card suitable for security-critical applications where a card's integrity is not only expected but required.

However, since most high-volume contracts are given to the same select manufacturers, the element of competition between manufacturers is mostly abolished with any semblance of a laissez-faire market being unrecognisable. Since development costs are often subsidised by the conglomerates of the tech industry, manufacturers are kept wrapped around the fingers of corporate customers whilst the industry is left at a dead-end for progress as when the only products being purchased at volume are the same vulnerable, low-cost ICs with minimal security features on-board, what incentive is there for manufacturers to continue developing more secure and sophisticated tags, when costs are prioritised over security?

Case Study – Contactless Payments featuring 'Apple Pay'

Recent innovations in smartphones seem to foreshadow a future for RFID where conventional tags are not kept separately as a part of your keychain but rather a feature on your phone available for use at any time with some implementations enabling use even [16] after your phone runs out of battery. These implementations of RFID forgo [17] the use of having separate ICs for each tag but rather have a software-based emulation layer where the phone pulses a coil within its chassis to an interrogator according to the data corresponding to a user's payment card. Whilst this implementation of RFID is widely known to consumers as 'Apple Pay' or 'Google Pay' and is used to enable contactless methods of payment using a smartphone, [18] Apple has recently introduced a new variant of the 'Apple Pay' technology called 'Apple HomeKey' that intends to replace traditional house keys through the emulation of an encrypted RFID card.

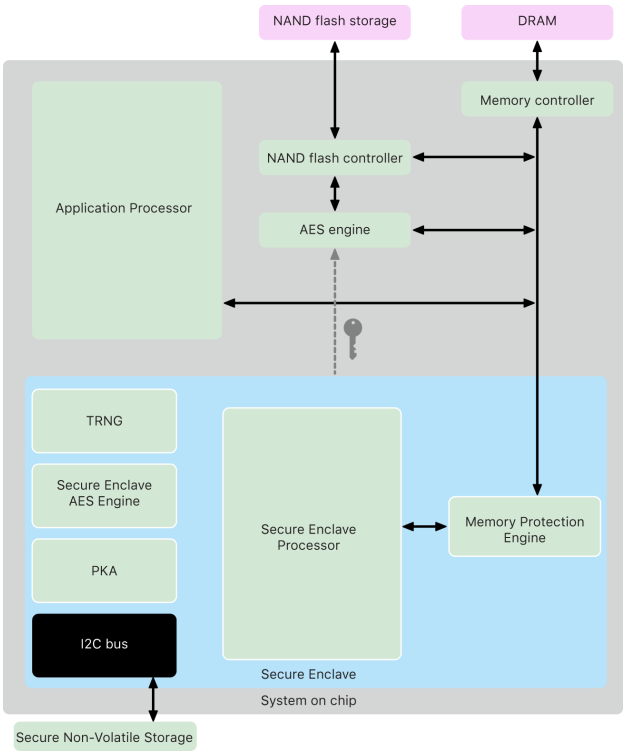

Figure 2.2
[38] Diagram of Apple's Secure Enclave Architecture

Furthermore, Apple's contributions to the RFID industry seem to be indispensable in terms of increasing security standards. By using the 'Secure Enclave' to invoke any procedures that require access to sensitive data such as 'Apple Pay' or 'Apple HomeKey', Apple solidifies integrity throughout the authentication process. Apple's modular approach to security eliminates the ever-common singular point of failure throughout the chain of components involved in a transaction by spreading the processes out between as many parts of the iPhone as possible from the side button to the RFID coil that whilst all connected to the same main logic board of the iPhone, are physically unable to communicate with each other which is a conscious hardware limitation designed by Apple to ensure that even if one component is compromised, it cannot affect the integrity of the 'Secure Enclave' authentication chain.

At the beginning of the chain is the side button featured in iPhones from the iPhone X onwards. The iPhone's side button is physically connected to the iPhone's 'Secure Enclave' which ensures that all calls made to the 'Secure Enclave' for sensitive data to be accessed can only be made by the iPhone's user physically clicking the button. Apple brands this step as the [19] 'Secure intent' and whilst it may seem unnecessary at first, it is quite imperative to the chain of security built into every 'Secure Enclave' call made as it ensures that malicious actors cannot access the 'Secure Enclave' through software regardless of how high their privileges may have been escalated to as a physical circuit must be closed by the button to access any data from the 'Secure Enclave'.

When a 'Secure Intent' has been approved by the user through a double-click of the side button, the 'Secure Enclave' transmits your Device Account Number [20] alongside a transaction-specific random security code generated by the Secure Enclave (to ensure that software on your iPhone can neither access this random number or affect its value - potentially predicting it) to the Point of Sales system to finalise contactless payment in the case of 'Apple Pay'.

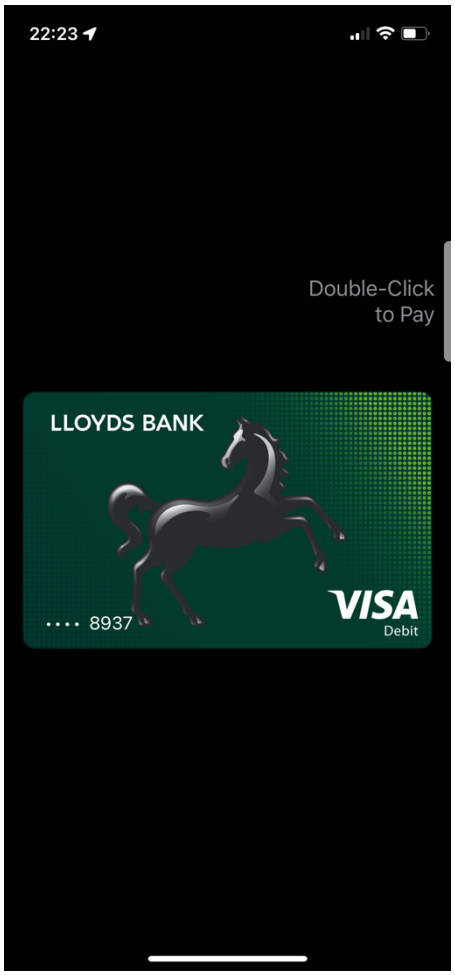

Figure 2.3
Screenshot of a 'Secure Intent' request made by iOS to be approved by the user

Whilst at first this may seem like nothing more than a gimmick, due to Apple's leading role in smartphone market share, competitors are likely to catch up and match leading to the weak encryption standards holding back technologies such as 'MIFARE Classic' to be replaced for more secure approaches with implementations of randomised UIDs and 2-way encryption being standard.

Case Study – Disney MagicBands

By exploring the [21] public FCC filings for Disney's 'MagicBand', we discover that the MagicBands run on the 2.4GHz frequency band - as stated in the 'RF Exposure' document - which we can assume to be responsible for the long-range functions of the MagicBand due to its active characteristics.
Furthermore, Disney is able to access a parkgoer's approximate location at any time by utilising [22] ADIC (Automatic Data Identification and Capture) operating on the 2.4GHz frequency band. This data is then used by Disney's Cast Members to [22] predict and anticipate rushes of parkgoers at any given time and is also a cleverly disguised way to help ensure the safety of children by tracking the location of any lost children.

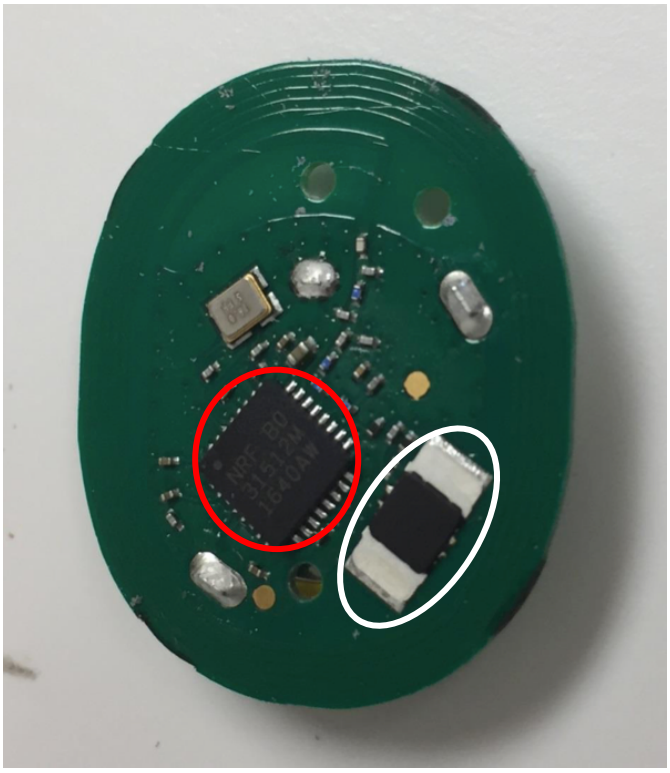

Figure 2.4
[39] Teardown of a Disney 'MagicBand' highlighting the 13.56MHz HF IC (circled white) and the 2.4GHz UHF IC (circled red)

Whilst research on the passive HF implementation of the MagicBand is scarce due to the proprietary and secretive nature of the wristbands and the systems running to support them, we can deduce that these ICs are likely within MIFARE DESFire specifications of encryption since they hold access to sensitive parts of data such as payment information or hotel door access keys. However, the most interesting part of Disney's implementation of RFID lies in the ingenious use of multi-factor authentication and how MagicBands serve as an additional security measure rather than a convenient replacement.

The three main factors of authentication widely accepted by the [23] industry include:

1. Something you know (e.g. a password)
2. Something you have (e.g. a smart card)
3. Something you are (e.g. biometrics such as fingerprints)

With Disney's MagicBand system requiring two out of the three factors of authentication, we can conclude Disney's MagicBands to be a highly secure implementation of RFID-based approach to security that serves to combat most attacks that may plausibly occur at a Disney Park. Since purchases require both the presence of a MagicBand and authentication through fingerprints alongside the witness of a member of Disney staff, parkgoers are

deterred from going on a joyride with a lost MagicBand found on the floor. I believe that this multi-factor approach to security is one that more access control systems could take advantage of, treating RFID tags as additional part of authentication rather than the sole key.

Figure 2.5
[42] Demonstrating the multi-factor authentication achieved through Disney's MagicBands

However, in the pursuit of a 'magical' experience for every Disney parkgoer through the MagicBand system, several questions and concerns are raised at the privacy implications this system may bring. As raised by [22] Sadler et al, when all activity throughout the Park is being recorded at all times alongside the location of any parkgoer on site, it is imperative that this data is stored safely and securely and whilst the RFID tags themselves may no longer be the weak point in the system, the onus is now shifted onto the databases holding this information which if compromised could expose the payment details, hotel room number, personal location, purchase history and likely many more pieces of telemetry data that could be used to co-ordinate an attack on an individual onsite. Furthermore, with Disney's development costs totalling over $1 billion, it would be foolish to expect this technology to be limited to select Disney parks when the potential for such technologies in enterprise environments such as public transport or government surveillance is not only vast but highly sought-after.

Known Vulnerabilities in RFID – Current Strategies for Mitigation

As mentioned earlier, 125KHz RFID hinges on the expectation that consumers do not have access to writable blank cards and that the serial number of LF tags stay unexposed. However, this expectation has been broken. When the initial strategy to secure LF RFID was security through obscurity and yet various manufacturers mass produce 125KHz 'cloning devices' to be used with such tags, it is safe to say that LF RFID is inherently unsecure and is quite literally a lost cause.

Figure 3.1
[43] A mass produced 'RFID Cloner' device that is readily available to be purchased through sites such as Amazon or eBay

However, one defence mechanism that could be implemented purely through software could be to identify whether the tag detected by the interrogator is a read-only card. Since there are two types of LF tags, the first being the T5577 produced by [24] Atmel (formerly Microchip) that supports both reading and

writing to the tag and the EM4100 produced by EM Microelectronics that only supports reading to the IC, this could be achieved by sending the write command to the tag and detecting whether it transmits a response or not. If the tag sends a backscattered response, the card should be immediately rejected as it is likely a fraudulent card whilst if no response is given to the write command, authentication should proceed as usual.

When considering HF RFID, we soon discover MIFARE Classic to be the most widely used IC even after the introduction of secure alternatives such as MIFARE DESFire. Ironically enough, MIFARE Classic's biggest weakness comes from the misconfiguration of these cards when being initialised for onsite use. The architecture of MIFARE Classic cards contains 16 blocks of data counted from block 0 to block 15 where block 0 is a readable block by an interrogator without the encryption key whilst blocks 1-15 are hidden from the interrogator without authentication using the private key. [5] Block 0 is designed to only be writable by the manufacturer at fabrication of the tag as it contains the manufacturer assigned serial number (UID) and the manufacturer identifier (SAK). However, technicians and engineers have opted to configure their authentication systems to only check for a matching UID and SAK rather than checking the entire contents of the card as it heavily decreases read times – leading to less authentication failures on legitimate cards but also means that the security has now been reduced to 125KHz LF RFID standards.

However, too often overlooked is the fact that all MIFARE Classic cards come from the factory with a default key of "FF:FF:FF:FF:FF:FF". Not only is this default key almost never changed, but due to the widespread nature of MIFARE Classic, a list of all publicly known default keys mentioned in NXP datasheets has been compiled [25].

Secondly, even if the private key has been changed from the manufacturer defaults, retrieving the key from the card itself is now a heavily documented process thanks to Nohl et al and their paper 'Reverse-Engineering a Cryptographic Tag' [26]. Within the paper, Nohl et al illustrate that by inspecting the tag at a silicon level using microscopes, the cipher can be reconstructed by using image analysis then cracked by influencing the numbers generated by the weak RNG (Random Number Generator) hardware to then find the key by comparing results of influenced RNG numbers to a pre-computed rainbow table of results that can reveal the key in a matter of seconds.

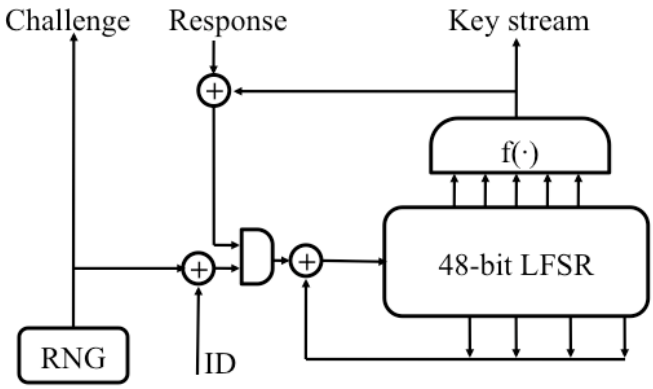

Figure 3.2
[26] A diagram to show how the RNG (Random Number Generator) plays a role into the encryption behind MIFARE Classic

After the publishing of this research, NXP issued a statement [27] stating that “NXP does not recommend to design in MIFARE® Classic in any security relevant application” and that “NXP therefore is recommending that existing MIFARE Classic® systems are upgraded” but after acknowledging that doing so is likely costly and is therefore likely that “countermeasure[s] will not be extensively deployed”, NXP has effectively given up on MIFARE Classic as a secure technology.

Lastly, we must consider the human.

The ‘mere ownership effect’ [28] is a phenomenon in psychology and behavioural economics that suggests that people are more likely to think more positively of an object and the ideas represented by it when they own it compared to when it is not in their possession. This alongside the ‘Endowment effect’ – the tendency for people to be more willing to keep an object than acquire the same object when they are not in ownership of it – presents a rather interesting view into the psychology behind the illusive white ID badge and the perceived value it may represent to someone who has one and actively uses it compared to the analysed value of that card in the eyes of a security researcher.

“project_doppelgänger”

"if I have seen further [than others], it is by standing on the shoulders of giants."
-Issac Newton

Throughout the course of my research for this project, I came across many forum posts on the internet with code that individually did parts of what I wanted to achieve in project_doppelgänger. After editing them for my own needs, I built three mainboards to communicate with my Arduino. One to facilitate the programming and erasing of my microcontroller, another to act as a 125KHz RFID emulator when my microcontroller is embedded onto the board and lastly an interface board to interface the commercial RFID access control panel I purchased to demonstrate the weaknesses of LF RFID.

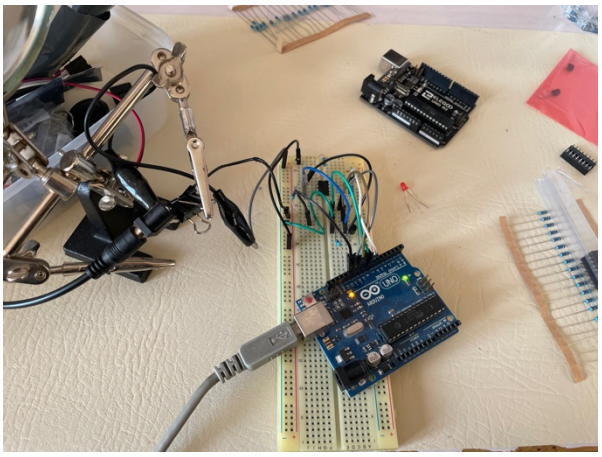

Figure 4.1
My ATTiny85 Programmer/Eraser in its prototyping stage

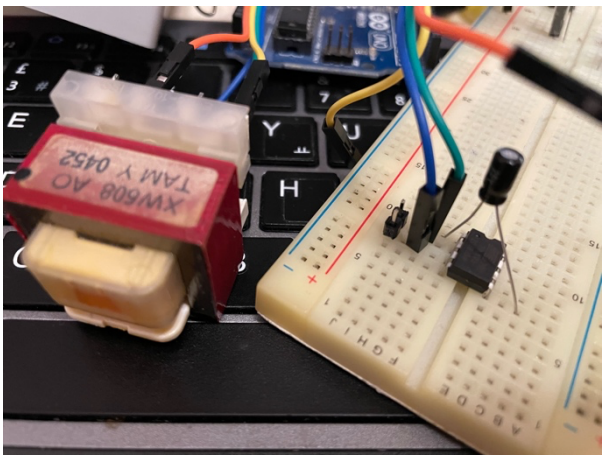

Figure 4.2
The RFID Emulator in its prototyped on a breadboard

Firstly, I prototyped my Arduino ISP using official code found in the [29] Arduino IDE to flash an Arduino to act as an ISP to my microcontroller. However, since the microcontroller I chose to use (the ATTiny85) requires high-voltage programming through a 12V programmer to set fuses to choose the clock source, I had to build a second part to the programmer which was the eraser. Normally, the microcontroller is erased by the programmer however due to the requirement of an external clock source - the interrogator’s clock pulses - the programmer is unable to interface with the microcontroller and therefore requires the high-voltage programmer.

Secondly, I implemented the eraser part of the mainboard I built was based off instructables user dmjlambert’s [30] ‘HV Rescue Simple’ designs which allowed me to integrate their high-voltage circuitry to be used in my own board designs which heavily expedited the process of building the programmer/eraser. This also meant that since their code was open-source, I was able to adapt the code to be usable with my microcontroller as it was already compatible with Atmel microcontrollers.

After prototyping each element and ensuring that the circuit designs were both stable and functional, I soldered each component down onto its perfboard (a type of PCB populated with holes used by electronics hobbyists to create their own PCBs) to make the circuits look more professional and to make them more permanent.

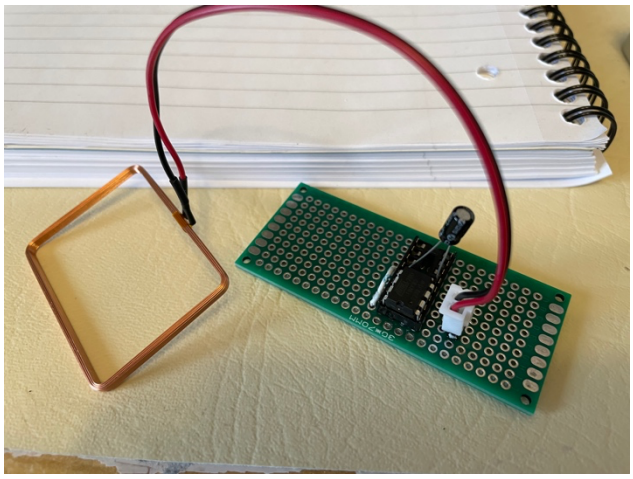

Figure 4.3
The LF RFID Emulator built with support for a capacitor to ensure that the microcontroller is powered even during pauses without pulses

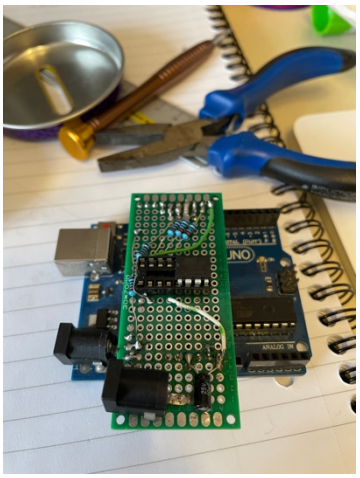

Figure 4.4
My ATTiny85 Programmer/Eraser after being soldered down onto a perfboard

Next, I registered my 125KHz tag onto the access control panel to have a test tag that I can clone to demonstrate my proof of concept. After that, I connected my Arduino to an RDM6300 module that is capable of reading LF tags and scanned my sample key onto it.

Figure 4.5
[44] Screenshot of an Arduino Tool being used to read the serial number and manufacturer code of 125KHz RFID tags.

Afterwards, I downloaded the [31] ‘avrfid’ project – a project that aims to emulate LF RFID tags using AVR microcontrollers – and edited the source code so that the tag data and manufacturer ID being emulated corresponded to the data held in the sample key. Usually, most microcontrollers can be programmed through the Arduino IDE software however since I am compiling C++ code from source, I had to manually compile the code using the terminal tool ‘make’ and then flashed the software onto the microcontroller using the Arduino’s internal command line tool ‘avrdude’.

```
jiminlee@Jimins-MacBook-Air try % avrdude -v -p attiny85 -P /dev/cu.usbmodem1101 -c stk500v1 -b 19200 -U lfuse:w:0xC0:m -U flash:w:avrfid.hex

avrdude: Version 7.0
         Copyright (c) Brian Dean, http://www.bdmicro.com/
         Copyright (c) Joerg Wunsch

         System wide configuration file is "/opt/local/bin/../etc/avrdude.conf"
         User configuration file is "/Users/jiminlee/.avrduderc"
         User configuration file does not exist or is not a regular file, skipping

         Using Port                    : /dev/cu.usbmodem1101
         Using Programmer              : stk500v1
         Overriding Baud Rate          : 19200
         AVR Part                      : ATtiny85
         Chip Erase delay              : 4500 us
         RESET disposition             : possible i/o
         RETRY pulse                   : SCK
         Serial program mode           : yes
         Parallel program mode         : yes
         Timeout                       : 200
         StabDelay                     : 100
         CmdexeDelay                   : 25
         SyncLoops                     : 32
         PollIndex                     : 3
         PollValue                     : 0x53
         Memory Detail                 :

                                  Block Poll               Page                       Polled
           Memory Type Alias    Mode Delay Size  Indx Paged  Size   Size #Pages MinW  MaxW   ReadBack
           ----------- -------- ---- ----- ----- ---- ------ ------ ---- ------ ----- ----- ---------
           eeprom                65     6     4    0 no        512    4      0 4000  4500 0xff 0xff
           flash                 65     6    32    0 yes      8192   64    128 4500  4500 0xff 0xff
           signature              0     0     0    0 no          3    1      0    0     0 0x00 0x00
           lock                   0     0     0    0 no          1    1      0 9000  9000 0x00 0x00
           lfuse                  0     0     0    0 no          1    1      0 9000  9000 0x00 0x00
           hfuse                  0     0     0    0 no          1    1      0 9000  9000 0x00 0x00
           efuse                  0     0     0    0 no          1    1      0 9000  9000 0x00 0x00
           calibration            0     0     0    0 no          1    1      0    0     0 0x00 0x00
```

Figure 4.6
Screenshot of ‘avrdude’ flashing the ATTiny85 with the compiled ‘avrfid.hex’ file using the Arduino as ISP flag

After the microcontroller had been successfully flashed, I tapped the emulator onto the control panel for the moment of truth.

Figure 4.7
Success found at last with the transformer coil accurately emulating the credentials of the sample key shown by the access control panel granting entry by enabling the relay usually responsible for powering the door solenoid.

Afterword

As we have successfully demonstrated practically in “project_doppelgänger” and theoretically in Chapters 1-3, RFID is still a relatively vulnerable protocol with plenty of attack vectors and potential exploits. However, through the recent work of substantial technology companies such as Apple or Google, the future for RFID seems bright even if it isn’t used in its conventional keyfob-like form. Although, this puts us in a difficult position where secure RFID protocols and designs are locked behind closed-source doors of the technology conglomerates and as we have demonstrated already, a monopoly is never a favourable thing for the wider industry but only serves to line the wallets of the few elites at the top.

Not only do monopolies hinder the rate of innovations within the industry, but they also serve to incentivise a strategy where profits and investor relations are prioritised over security and technological advancements. Furthermore, companies such as Apple have been found ignoring security flaws disclosed by [32] independent security researchers until journalists and news outlets were informed of the presence of these bugs by the researcher, causing the incident to be publicised, subsequently hurting public image and stock prices, forcing Apple to then acknowledge and patch the bugs.

One proposal I would like to make to improve the security of all RFID-based security systems would be to be stricter about tag frequencies and backscattered response timings. Whilst legitimate ICs are almost instant in their response as they are ASICs (Application Specific Integrated Circuit), emulators such as the one I built as part of “project_doppelgänger” require CPU cycles to compute and transmit the responses which inevitably bring an emulation overhead and therefore delayed responses which could be detected by the interrogator through a well-written firmware update as this improvement wouldn’t require any extra hardware.

To evaluate, I would also like to acknowledge that a lot of the improvements suggested in this paper are both difficult and costly to implement in reality. In the enterprise world, software updates are a constant gamble that often require downtime to check whether any new bugs have been surfaced in the recent update which may potentially break infrastructure if rolled out to the entire site at once. Therefore, whilst it may be easy to point fingers and shift the responsibility onto others, as with all matters involving people, please try and remember the human.

Lastly, I’d like to say a thank you for reading this paper. I had lots of fun not only building the project but also doing the research and writing this paper and ultimately, I hope that my efforts have served to help you grasp a fuller picture in the world of enterprise and more specifically, RFID hardware.

Works Cited

[1] M. W. Cardullo, “RFID Journal,” 21 April 2003. [Online]. Available: https://www.rfidjournal.com/genesis-of-the-versatile-rfid-tag. [Accessed 25 February 2023].

[2] ISO/IEC, *ISO/IEC 14443-1 Identification cards - Contactless integrated circuit(s) cards - Proximity cards Part 1: Physical characteristics,* 2008.

[3] ISO/IEC, *ISO/IEC 18000-2:2009 Information technology — Radio frequency identification for item management — Part 2: Parameters for air interface communications below 135 kHz,* 2009.

[4] A. Lozano-Nieto, RFID Design Fundamentals and Applications, CRC Press, 2010.

[5] R. Weinstein, “RFID: A Technical Overview and Its Application to the Enterprise,” *IEEE Computer Society,* pp. 27-28, 2005.

[6] Fujitsu, “Datasheet - World's Largest-Capacity 64KByte FRAM Metal Mount RFID Tag,” 2014. [Online]. Available: https://www.fujitsu.com/jp/group/frontech/en/imagesgig5/brochure-ait64k.pdf. [Accessed 26 February 2023].

[7] atlasRFIDstore, “A Guide to RFID Types and How They Are Used,” [Online]. Available: https://www.atlasrfidstore.com/a-guide-to-rfid-types-and-how-they-are-used/. [Accessed 26 February 2023].

[8] S. News, “Proximity Access Readers: 125kHz or 13.56Mhz?,” 16 October 2018. [Online]. Available: https://sen.news/proximity-access-readers-125khz-or-13-56mhz/. [Accessed 26 February 2023].

[9] YARONGTECH, “Amazon UK,” YARONGTECH, [Online]. Available: https://www.amazon.co.uk/YARONGTECH-Proximity-125Khz-EM4100-Orange/dp/B071GN3BD7. [Accessed 26 February 2023].

[10] Soldered Electronics, “Soldered,” Soldered, [Online]. Available: https://soldered.com/product/125khz-rfid-tag/. [Accessed 26 February 2023].

[11] Armata, “Armata Shop,” Armata, [Online]. Available: https://www.armata.fi/en/rfid-cards/35-125khz-rfid-cards-em4200.html. [Accessed 2023 February 2023].

[12] C. Banton, “Investopedia,” 29 September 2020. [Online]. Available: https://www.investopedia.com/terms/m/mass-production.asp. [Accessed 26 February 2023].

[13] Yavis, “Amazon,” [Online]. Available: https://amzn.eu/d/6GWbwdV. [Accessed 26 February 2023].

[14] NXP, “Mifare,” [Online]. Available: https://www.mifare.net/en/. [Accessed 11 March 2023].

[15] NXP, “Mifare Ultralight,” [Online]. Available: https://www.nxp.com/products/rfid-nfc:RFID-NFC. [Accessed 11 March 2023].

[16] Apple Inc, “Express Cards with power reserve,” 13 May 2022. [Online]. Available: https://support.apple.com/en-gb/guide/security/sec90cd29d1f/web. [Accessed 13 March 2023].

[17] E. Kazan, “The Innovative Capabilities Of Digital Payment Platforms: A Comparative Study Of Apple Pay & Google Wallet,” *International Conference on Mobile Business,* vol. 4, 2015.

[18] Apple Inc, “Access Credential Types,” [Online]. Available: https://support.apple.com/en-gb/guide/security/sec30bdef041/web. [Accessed 11 March 2023].

[19] Apple, “Secure intent and connections to the Secure Enclave,” [Online]. Available: https://support.apple.com/en-gb/guide/security/sec7a94f7d1e/web. [Accessed 11 March 2023].

[20] A. S. J. a. J. S. Park, “A Security Analysis on Apple Pay,” *2016 European Intelligence and Security Informatics Conference,* 2016.

[21] Disney Inc, *FCC Filing - FCC ID Q3E-MB-R1G1,* Washington DC: FCC, 2013.

[22] D. P. M. S. V. C. Madeleine Sadler, “Magic or Mischief: A look into Disney’s adaptation of IoT,” *Big Data,* vol. Fall, 2016.

[23] Pearsons IT Certification, “Understanding the Three Factors of Authentication,” 6 June 2011. [Online]. Available: https://www.pearsonitcertification.com/articles/article.aspx?p=1718488. [Accessed 12 March 2023].

[24] Microchip, “ATA5577C – Read/Write LF RFID IDIC Datasheet”.

[25] mfcuk, “Mifare Classic Default Keys,” 3 April 2010. [Online]. Available: https://code.google.com/p/mfcuk/wiki/MifareClassicDefaultKeys. [Accessed 12 March 2023].

[26] N. e. al., “Reverse-Engineering a Cryptographic Tag,” *ACM Computer and Communications Security,* 2015.

[27] J. G. -. N. P. M. Manager, *Security Statement on Crypto1 Implementations,* 2015.

[28] J. Beggan, “On the social nature of nonsocial perception: The mere ownership effect.,” *Journal of Personality and Social Psychology,* 1992.

[29] Arduino, “Arduino as ISP and Arduino Bootloaders,” 9 March 2023. [Online]. Available: https://docs.arduino.cc/built-in-examples/arduino-isp/ArduinoISP. [Accessed 12 March 2023].

[30] dmjlambert, “HV Rescue Simple,” [Online]. Available: https://www.instructables.com/HV-Rescue-Simple/. [Accessed 12 March 2023].

[31] scanlime, “Github 'avrfid',” 15 June 2010. [Online]. Available: https://github.com/scanlime/navi-misc/tree/master/avrfid. [Accessed 12 March 2023].

[32] P. Masiliauskas, “Apple ignores multiple security issues on iOS 15, researcher claims,” 9 June 2022. [Online]. Available: https://cybernews.com/news/apple-ignores-multiple-security-issues-on-ios-15-researcher-claims/. [Accessed 13 March 2023].

[33] Cisco, “What Is a Cyberattack?,” [Online]. Available: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. [Accessed 24 February 2023].

[34] W. P. M Cardullo, “Transponder apparatus and system”. United States of America Patent US3713148A, 23 January 1973.

[35] H. Doğan, “Use of Radio Frequency Identification Systems on Animal Monitoring,” *SDU International Journal of Technological Science,* 2016.

[36] C. Tardi, “Investopedia,” 3 October 2021. [Online]. Available: https://www.investopedia.com/terms/m/minimum_efficiency_scale.asp. [Accessed 26 Febuary 2023].

[37] NXP, “MIFARE DESFIRE EV2,” [Online]. Available: https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire/mifare-desfire-ev2:MIFARE_DESFIRE_EV2_2K_8K. [Accessed 11 March 2023].

[38] Apple Inc, “Secure Enclave,” [Online]. Available: https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web. [Accessed 11 March 2023].

[39] J. Brunk, “Disney MagicBand Teardown,” [Online]. Available: http://www.pemnet.net/files/design_info/teardowns/Disney.pdf. [Accessed 11 March 2023].

[40] C. Kuang, “Disney's $1 Billion Bet on a Magical Wristband,” 10 March 2015. [Online]. Available: https://www.wired.com/2015/03/disney-magicband/. [Accessed 12 March 2023].

[41] C. Wang, “Disney's $1 Billion Bet on a Magical Wristband,” 10 March 2015. [Online]. Available: https://www.wired.com/2015/03/disney-magicband/. [Accessed 12 March 2023].

[42] Mike, “Blog Mickey,” 23 August 2021. [Online]. Available: https://blogmickey.com/2021/08/biometric-finger-scanning-returns-to-disney-world-theme-parks-following-covid-19-suspension/. [Accessed 12 March 2023].

[43] Dangerous Things, “Store,” [Online]. Available: https://dangerousthings.com/product/blue-cloner/. [Accessed 12 March 2023].

[44] A. M. Shojaei, “Interfacing RDM6300 RFID Reader Module with Arduino,” [Online]. Available: https://electropeak.com/learn/interfacing-rdm6300-125khz-rfid-reader-module-with-arduino/. [Accessed 12 March 2023].