A Practical Walk Through NFC Security and Evolution

Dany Bouça Nova

University of Kent
School of Computing

Msc Networks and Network Security
2016 - 2017

“

We can’t solve problems by using the same kind of thinking we used when we created them

”

Albert Einstein

ABSTRACT

Near Field Communication (NFC) technology is a subset of RFID providing a set of communication protocols. NFC offers a variety of reliable services such as payment, loyalty services, access control, ticketing... As promising as this short range wireless communication technology is, it has always been a controversial subject during its appearance until nowadays. The misconceptions about security and NFC in various applications will be cleared up. Although these misconceptions, an estimated 1.9 billion phones worldwide will be NFC-enabled by 2018. An understanding about the current status of NFC is necessary to maintain the advancement of knowledge in NFC research especially about the evolution of its security flaws. This paper will present a comprehensive analysis of the security and global evolution of the NFC technology. Indeed, a brief history, evolution and improvements, applications and usability, security and privacy will be discussed as well as further research opportunities. Practical experimentations and applications will be brought breaking the line between theory and practice. This paper will be a guide either for researchers, academicians or simply business world interested in this versatile technology. The exploding growth of NFC will make this valuable for anyone interested in that promising technology.

Keywords: Near Field Communication, NFC, NFC Technology, NFC security, NFC privacy, NFC Evolution, NFC threats, NFC Payments, NFC Profiling, MIFARE, EMVCo, Android NFC, Proxmark3, NFC Readers

World Count: 9267

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my research supervisor Budi Arief. This dissertation would not have been accomplished without his assistance, enthusiasm and involvement. I would like to thank him very much for letting me borrow special and expensive tools that I would not have in hands without his support. I also want to show my gratitude to the University of Kent for this year as a Postgraduate student on the Msc of Networks and Network Security where I have been learning so much. I will always carry positive memories about this year, the professors, the support of the University, the Library as well as all its resources available.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

Radio Frequency Identification (RFID) technologies are used since the early eighties in the industrial sector. Nowadays, RFID is everywhere as it is an easy way to transport data at low cost. An RFID system is composed of a tag (itself composed of a microchip and an antenna) and a base station (often called reader). NFC, a child of RFID, stands for Near Field Communication and allows to have communications with a working distance around 10 centimetres between the station and the tag with classic equipment. NFC works using magnetic induction between two antennas located closely from each other. The NFC forum association marked the beginning of the technology growth by creating the specifications and standards for NFC devices and tags. The frequency range of RFID systems is between 125 kHz (Low Frequency) to 2.45 GHz (High Frequency). NFC works in a subset of the high frequency (HF) range at 13,56 MHz and hence compatible with the majority of tags and readers already in place. NFC offers a data transmission rate of 106 kbit/s to 424 kbit/s.

There are several modes by which the NFC interface can communicate. These modes of communication are distinguished according to which device creates a Radio Frequency (RF) field or in the opposite retrieves the power generated by the RF field of the other device. The device which generates its own RF field is called an active tag while the other is called a passive tag. The NFC Forum defines three modes of operation [1]. The card emulation mode enables NFC devices to act like simple passive tags, smart cards allowing the user to perform transactions for example. The NFC reader or writer mode enable devices to read information of a NFC tag or write information into it. The last mode called Peer-to-Peer mode enables two devices to communicate with each other in order to share files or exchange information.
The diversity of NFC tags types (appendix NFC Tag Types) required signalling protocol to communicate and exchange data (appendix NFC Protocol Stack Overview). Technical specifications for the different operating modes are based on existing RFID standards including NFC-A (ISO/IEC 14443A), NFC-B (ISO/IEC 14444B) and NFC-F

(FeliCA JIS X6319-4). The NFC standards include the ISO/IEC 18092 dedicated to the Peer to peer mode (and also used in NFC-F) and other standards defined by the NFC Forum such as the application layer of the NFC Stack and its communication structure: NFC Data Exchange Format (NDEF) [2].

NFC has multiple advantages and that is why it is widely used nowadays, keeping growing exponentially. This very same growth has led people to naturally ask themselves about security and privacy as NFC still is deployed in more and more applications. How the evolution of NFC technology has allowed more and more people to use it? How secure has been NFC during its growth and does it protect user privacy?

This paper will present a brief NFC history, evolution and description in the second chapter. Chapter three contains a literature review, providing research contributions, signifying security research advancements as well as how this technology has overcome security issues (Confidentiality, Integrity and Authenticity) in order to become a reference for small-range communications. Chapter four presents the tools that the author used for the experimentations that are described in the chapter five. Three different approaches are explained within the experimentation chapter: Mifare and Mifare classic experience, a desktop application and an Android application. The results of these experimentations are listed in the chapter 6. The question raised by this research are treated in the chapter seven followed by the conclusion. This work has been done in the collaboration with another student, Dorian Jolivald and will be quoted when talking about his accomplishments.

1 NFC EVOLUTION

The ubiquity of the NFC today was not evident during the first years of its release. This same ubiquity is becoming more and more accentuated as the number of application is growing and also becoming more secure.

1.1 RFID AND NFC

In 1983, the first patent was recorded to Charles Walton for an object using RFID. Franz Amtmann, the NXP engineer who created NFC with his colleague Phillipe Maugars explained that NFC basically was based on a precursor technology known as MIFARE launched in 1994. MIFARE is a NXP owned trademark possessing the majority of the contactless smart cards and proximity cards chips used all around the world. MIFARE proprietary technologies are all respecting the international standard that defines smart cards protocol communication: ISO/IEC 14443. The idea of NFC was to take this MIFARE technology to the next step by "defining a device which can combine card functionality with reader functionality" according to Franz Amtmann [3]. NFC is a subset of RFID and smart card technology: it is fully compatible with most existing RFID and contactless smart card system. The main difference relies on their architecture while RFID and contactless smart cards have a reader and a tag to be working, an NFC device can be either transmitter or reader. Moreover, NFC introduces the Peer-to-Peer mode for binary data exchange communications. This feature is not described in the ISO/IEC 14443 (contactless cards) but added to the NFC standard by the ISO/IEC 18092. Figure 1 shows the three modes of operation for NFC communication.

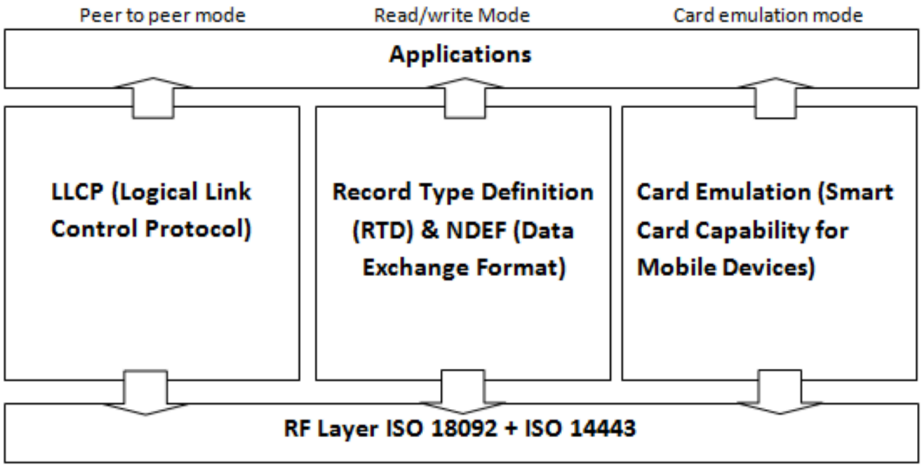


Figure 1 - NFC protocols and modes of operation

1.2 NFC BRIEF HISTORY

The NFC history begins in 2002 with Sony and NXP Semiconductors (which was spun off from Phillips in 2006 and bought by Qualcomm in 2016) when both entities established the technologies specifications and created it. NFC forum, a non-profit association created in 2004 by NXP, Sony and Nokia brings life to NFC technology advancing the use of NFC by promoting the implementation and standardization to ensure interoperability between devices. Standards brought NFC tag types or even the NFC Data Exchange Format (NDEF) that was specified in 2006 to ensure the compatibility of RFID tags and contactless smart cards with NFC applications [4]. In 2006, several specifications have been created for passive tags such as smart tags, smart posters… The same year, the Nokia 6131 NFC is the first NFC-enabled cell phone. Moreover, this fast distribution of smart phones during that period have made the NFC area expand rapidly. In 2009, the Android 2.3 version named Gingerbread brought in his API 9 the NFC support [5]. One year later, the first android phone appeared: Google Nexus S [6].

Since then, NFC has been growing exponentially in the area of payments where many companies saw the opportunity of facilitating user interaction especially when it comes to earn money [7]. Contactless payments became part of a new-scale mode

of consumption based on the dematerialization of money. The decrease of the effort of purchasing and the impression of spending less money[1] increases the attractive power of a product which makes contactless payments increasing your consumption motivation and could even cause over consumption [8]. There are not only contactless payments in which NFC has been brought. NFC has endless applications and both researchers and companies do not stop to explore new ones. Gaming, commerce, marketing, social networking, smartphone automation tasks, access tags and healthcare are the most significant type of application nowadays. Some of the NFC wide-range of features are listed in the Figure 2. Some amazing uses has been discovered such as this gas detection wirelessly and cheaply done by a simple smartphone NFC chip modification which can detect explosives, harmful gases or even food spoilage [9]. Other eccentric applications have born such as Pizza hut and their NFC tattoo in order to let customers order their favourite pizza. "We're always looking for innovative ways to get pizzas into people's hands" said a Pizza Hut spokesman in October 2016 [10].

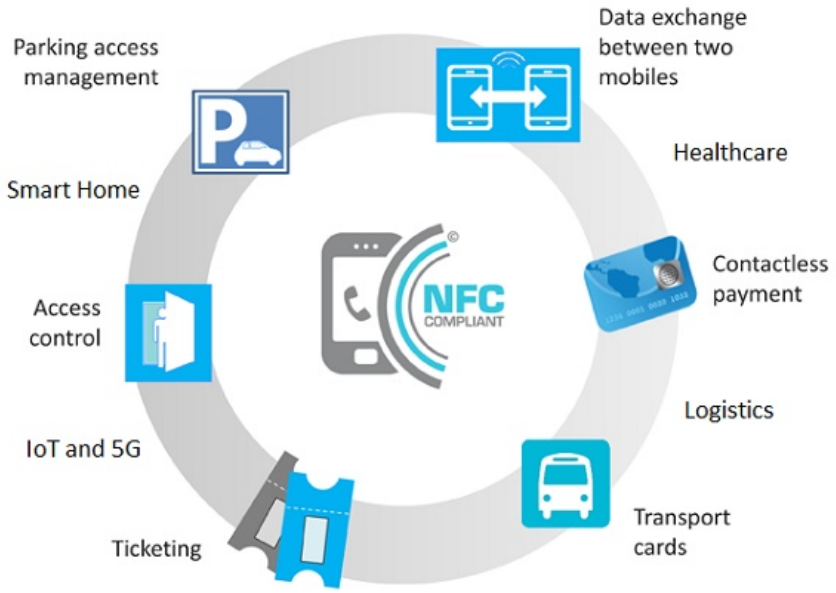


Figure 2 - Common NFC applications

[1] Virtual purchase gives you the impression of spending less money because you do not see your savings go down right away. Using cash is the most transparent payment mode and will save you money according to the Guardian [13].

1.3 CURRENT AND FUTURE NFC EVOLUTIONS

One of the major limit of NFC applications relies on manufacturers imagination as the possibilities and the number of applications are growing since the advent of the technology. Since its invention, NFC has become a very well-known and vital element for near communications and especially for the Internet of Things (IoT) where the impact of such technology is remarkable [11]. Indeed, one of the last main application of NFC remains the IoT and especially the area of smart homes that can besides help the Healthcare area. NXP blog articles [12] shows the willing of NFC application diversification. Some people were not really confident concerning the future of the NFC. However, Apple has release during its famous WWDC[2] 2017 conference a new API: CoreNFC [13]. This API will enable IPhones to use the technology underlying the Apple wireless payment system for more tasks. And that could help Apple close the Android application gap while bringing Apple consumers closer to the NFC experience. China is slowly using NFC Technology for example with Beijing opening the whole subway payment system for NFC-enabled cell phones [14]. Ofo[3] company has launched NFC enabled locks for their bike sharing solution in China and all the cities concerned replacing the QR code locks which were insecure and targeted by scammers [15].

Among other evolutions, The China cashless revolution stated by Bloomberg [16] describes the payment model used by China where most transactions are done by QR Codes. Indeed, only people in rich countries have access to credit cards and Apple Pay or other services are very likely uneconomical for these consumers. Moreover, small-scale merchants are very unlikely investing in expensive new terminals that can handle NFC technology. That is why QR Codes are likely to run in poorer

[2] WWDC stands for World Wide Developer Conference, a major event organized by Apple targeting apple products developers.
[3] Ofo is a bicycle sharing company based in Beijing and present in more than 20 cities (2016) that was founded in 2014.

countries while richer countries are more concerned with NFC technology. Furthermore, QR Codes are likely to take a larger role in payment systems by the QR code specification for payment systems published by EMVco[4] [17], slowing the NFC development.

[4] Europay MasterCard Visa Consortium (EMVCo) is an association of several companies which are responsible for technical standards for smart payments.

2 Related Work and Security overview

The unique NFC drawback relies on its ease of use where this new contactless process for communicating bypasses some well-established security steps (*e.g.*, PIN entry for credit cards) that cannot be easily forgotten. NFC benefits clearly are the ease of use, the versatility and of course, the security; element that is developed in this section. A state of the art of NFC security is described showing that NFC evolution has sometimes been slowed because of it. Few sources really talk about what could actually be done technically with NFC technology over an Android smart phone and some points are clarified in this section as well.

2.1 NFC Threats

2.1.1 NFC Viruses

Since its invention to today, many people think that NFC technology never has been secure and this common thinking is at the very first limit of NFC growth. But is this a common thinking mistake? One of the first attack that might have built that common thinking about NFC insecurity deals with RFID exploits[5]. In 2006, a paper entitled "Is your cat infected with a computer virus?" written by a group at the University of Amsterdam [18] theorizes the possibility that a RFID tag could embedded in its payload an exploit, a malware or virus that could spread via vulnerable RFID readers or middleware. This paper was reported on every media and has even won the best paper award for most impact. In fact, the virus presented in the paper could work in exceptional circumstances and the author had a special environment for the virus to work. While some researchers even said that this paper fatally failed to find an RFID

[5] NFC is based on RFID technology but is not only about identification such as RFID purpose but communication.

security issue and deliberately built a system for the virus to successfully spread, the paper still got people in mind that contactless technologies were unsecure.

In 2012, an NFC hack presented in the Black Hat conference by Charlie Miller exposed several exploits [19]. Like the previous 2006 exploits, these ones have also been over-mediated and is not quite as massive as a security flaw. The exploit used involved the use of Nokia [20] and Samsung NFC-enabled phones that allowed any hacker to "beam" (sharing content by NFC from one phone to another) malicious code or malware into the devices. The scenario used a Nexus S on an outdated Android OS version (Gingerbread 2.3) which makes the attack quite irrelevant as every Nexus device at that time was already running Android 4.0 which patched the vulnerability. Indeed, the hacker was running malicious code to take down the device by exploiting a Gingerbread's memory management flaw through an NFC tag that just carried the payload. Also, the hacker would have to beam one phone with another and so nearly touch physically the devices to work which makes the device NFC activation without your knowledge quite difficult. The other exploit presented is not an actually NFC exploit: NFC was used to redirect the device to a malicious website that exploited a browser flaw to gain privileges.

At DEF CON 21 in 2013, Wall of Sheep team turned into NFC awareness by spoofing: installing some smart posters around the conference where each scan for "free music" was in reality warning such activity that could make your phone infected with malwares in some special cases[6].

2.1.2 EAVESDROPPING

Although NFC relies on short range communications, it does not make it more secure than another communication technology. NFC Forum does not provide any protection against eavesdropping and one attacker can possibly gather private information about an NFC communication between two devices. This attack consists the listening secretly a private NFC operation and makes NFC confidentiality illusionary. As NFC communication are done through air with electromagnetic radio

[6] Some issues are pointed such as unawareness, outdated systems, no anti-malware.

waves, which is an open and accessible medium for all, eavesdropping is a logical attack. Eavesdropping can be either passive to gather information or active where the attacker acts as a middleman receiving and altering transaction information between two devices: a man in the middle attack.

The Proxmark 3 can for example snoop NFC operations at a few centimetres but many manufacturers also sell NFC long range readers with unusual large antennas that can read multiple tags at 30 centimetres away [21]. Some other researches have been made and custom equipment has achieved interceptions at a distance of 30 to 60 centimetres with nearly 100 percent accuracy [22] [23]. Most non-technical people that heard about eavesdropping issues have seen long range RFID reader such as the ones presented at the DEF CON 21 [24] or in some researches [25] [26] [27] reading cards up to 1 meter away but these devices are not NFC compliant (13.56 MHz) and can only read RFID Low Frequency (125 KHz) smart cards. “RFID Myth busting” conference by Chris Paget at the DEF CON 17 in 2009 has even tried to challenge these misconceptions about RFID technology including NFC [28].

2.1.3 Data corruption, Manipulation and Interferences

Data corruption could be seen as a Denial of Service (DOS) attack in which the attacker changes the data transited from an NFC operation into an unrecognized format. If the data stored or read is corrupted, it makes it useless. NFC Readers that do not handle the read of multiple cards at once could lead to interferences. This can also be viewed as a DOS attack. Nowadays, most of the readers include an anti-collision protocol, usually slotted Aloha or Bit collision protocol [29]. Data can either be corrupted, modified or even inserted in an NFC communication.

2.1.4 Relay Attacks

The first practical relay attack was made back in 2005 on smart cards and so ISO/IEC 14443 standard with two (quite big) hardware devices acting as the proxy and the mole [30]. NFC Peer-to-Peer relay attacks have been made back in February 2012

using mobile phones. NFC has no mechanism to ascertain whether or not a device is in proximity to the terminal which makes relay attacks susceptible for contactless transactions by using NFC mobile phones [31].

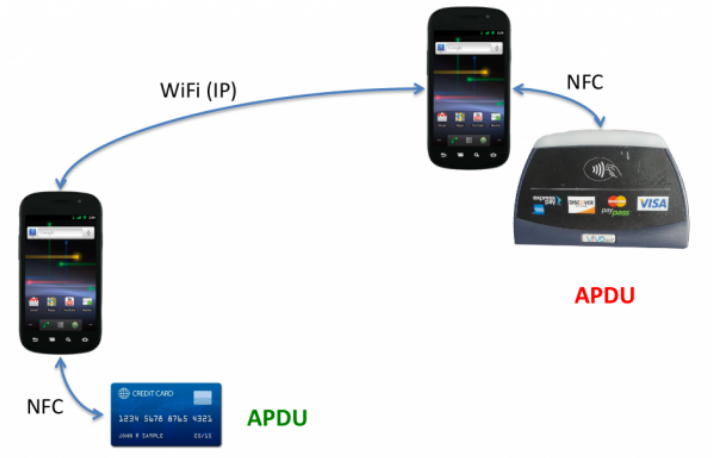


Figure 3 - NfcProxy relay attack

An example, shown in Figure 3, presents the NFC-Proxy attack that has been presented a few months later during DEF CON 20[7] by Eddie Lee [32], a security researcher at Blackwing Intelligence contributing to the reasons why standards should be fixed. This attack relies on a simple attack: two NFC-enable phones running the NFC-Proxy application in background, decide which one will run as a relay mode (near a victim credit card) and the proxy one (in contact with the terminal) and let a victim card pay with your proxy mobile phone. These attacks are very powerful and do not even need a rooted android device or a custom firmware.

Inspired by NFC-Proxy, the same attack has been presented in the DEF CON 25 [33] as “Uni Proxy” which is a hardware built tool solution highly customisable and faster. The difference relies on the way of transmitting the data, the master and slave are not android phones but a custom hardware solution communicating with radio transmitters up to 50 to 200 meters and not by Wi-Fi which was slow.

[7] The DEF CON conventions are one of the world’s longest running and largest hacking conferences held every year in Las Vegas, Nevada.

2.1.5 THEFT

This attack is the most obvious but one of the most powerful. The theft of a physical device such as a mobile phone or a smart card can theoretically lead the thief to use the stolen product to make a purchase. To avoid such attack, users have to be diligent and having a fingerprint or PIN entry authentication to access the device in order to protect their data. Google Wallet and Apple Pay hopefully implemented a default authentication factor to use the payment feature but what about contactless credit cards? One can easily buy something with credit card that has not been signalled as stolen even with some procedures remaining. Contactless payments daily limit or floor limit, depending on user location, is a result of no PIN verification or user signature (*e.g.*, Apple Pay touch ID) which brings some security. The amount of fraud on payment cards issued in France decreased in 2016 by 4% according to the observatory of means of payments under the presidency of the governor of the Bank of France [34]. Floor limits tends to increase with the reinforced security of contactless payments by the use of encryption to assure secure channels.

2.1.6 NFC NEW THREATS

NFC applications and possibilities seem endless, so do its threats. Unsuspecting threats begin to arrive. Biohacking is the exploit of genetic material through a specific purpose. Seth Wahle implanted an NFC chip in his hand, the perlicue, in order to ping Android NFC enabled device to open a link [35]. Once the user agreed to open the link and install a malicious file, the device would connect to a remote computer and pursue with other exploits. This social engineering tool is alarming as only X-Ray scans can detect it and especially if a zero-day[8] was used.

Sony is actually preparing itself for a bright new mobile feature using NFC technology. Wireless charging through NFC has been invented and described in a Sony patent [36]. The usefulness of such technology is rather obvious but what about the leach of someone else's battery phone? This technology will perhaps private

[8] Unknown security issue.

some users to access the content of their phone because of the drain of battery done by some attacker.

2.2 ANDROID NFC SECURITY

Android proposes since API 9 (Android Beam[9] in API 14) an implementation of NFC technology within your Android smartphones. Indeed, you can send and receive NFC data (NDEF messages, MIME type or URI) or even emulate an NFC chip (card) with your phone. Android only provides a HF antenna (13.56GHz) and possesses some limitations to read multiple chips simultaneously or emulate whatever card we want for some obvious security issues.

There is no way as an Android developer to see, when communicating with multiple tags, which tags have responded and then manually choose out of them. The NFC stack implemented by Android OS picks the first one and gives it to you. However, you can see the collision avoidance bit of the NFC protocol with various desktop readers and read multiple tags, but the Android NFC stack does not provide a system which can provide such multiple tag reading possibility.
Another barrier in the Android NFC implementation is the UID randomness when emulating a card. Indeed, it is not possible to force a smartphone to use a fixed or a chosen UID as Android generates a random UID for each emulation in order to avoid conflicts in reading multiple cards [37]. This also avoids critical security issues such as cloning every card and emulate it easily with your smartphone. Consequently, it is not possible to emulate the cards we want as some entities only distinguish users based on their card UID set by the manufacturer to perform specific actions. Android does not provide an API to influence the UID, anti-collision identifier.

However, if rooting or creating a custom ROM is an option, there are some possibilities to change the UID for example with a Kernel hook selecting a chosen UID when emulate a specific card in order to have no difference with the original

[9] Android Beam is a file sharing technology using NFC chips facilitating the exchange of data.

card. Other protocol parameters might be possible by changing the NFC implementation on a rooted android phone such as multiple card reader but there is no documentation or forums answering this very specific question. The SDK simply it is too limited and the unique solution involves an updated SDK that supports the reading of more than one tag.

A post on google + social media written by a NFC Tech lead at Google resumes the UID randomness: “It's not possible in the official version. (You could of course do it with some AOSP hacking).”[10] According to him, the reason is that Host-based Card Emulation (HCE) is designed around background operation and if the apps were allowed to set a custom UID, every app would have set their own and resolve the conflict would be impossible afterwards. We might expect in a close future an evolution of NFC infrastructure and move the authentication to higher levels of the NFC protocol stack instead of relying on the UID.

2.3 NFC Tag Types

Several tag types exist each offering advantages and inconvenient. The type of tag will mostly be chosen according to the task you need. Today, 5 type of cards exists and each is standardized and guaranteed to work with any NFC enable device. A brief figure shows the different types in the appendix NFC Tag Types.

- Tag type 1 is based on the ISO/IEC 14443A standard and is readable, re-writable and read-only. With 96 bytes of memory size and a transfer data rate of 106 kbit/s, these tags are space sufficient and costless ideal for many NFC applications.
- Tag type 2 is similar to tags of type 1 excepts that the basic memory size is 46 bytes extendable to 2 kilobytes.
- Tag type 3 is especially used in Asia as it is based on the Japanese Industrial Standard (JIS) 6319-4 known as Sony Felica and ISO/IEC 18092. These tags

[10] More information: https://plus.google.com/+MartijnCoenen/posts/iX6LLoQmZLZ

possess 2 kilobytes of memory size, transfer data rate of 212 kbit/s and are expensive.

- Tag type 4 is fully compatible ISO/IEC 14443 standard series (A and B). Pre-configured at manufacture, they are readable, re-writable or read-only. Memory size is up to 32 kilobytes and variable. Transfer data rate is variable and up to 424 kbit/s.
- Tag type 5 added in 2015 is based on ISO/IEC 15693 allowing a longer range readability, Radio Frequency technology and other features.

An NFC Tag does not offer any protection, has freely readable data and no security mechanisms implemented. Nevertheless, a tag can have its memory locked by being read-only. NFC tags contain a Unique Identifier (UID) created by the tag manufacturer. Such ID is used to identify a tag and especially avoid collision with other tags during the communication. This approach has been used commonly and still is whereas UID reprogrammable cards exists and can be used with basic hardware. These UID reprogrammable tags are often called Chinese cards as they have been introduced first in China and have a backdoor that can enable the alteration of the UID. However, some existing tags implement authentication and protection mechanism by encryption.

2.4 NFC Confidentiality, Integrity and Authenticity

To deal with most of the threats, secure channels, integrity and encryption have been brought to NFC by standards, optional and most of the times not used by resellers. The NFC Forum Signature Record Type Definition (RTD) specification released in 2010 and its 2.0 latest update in 2015 [38] brings an optional integrity protection for the content of a tag. The signature of a tag communicating with a user device is verified through a certificate chain from a trusted third party certificate authority also known as CA. This specification clearly improves user experience and users no longer have to be afraid of a hacker tampering the content of a tag as the user and its NFC-enabled device can simply verify the digital signature on the NDEF

message. A hacker could also get a digital certificate but it means that he could be track and the certificate be revoked.

Moreover, secure transport layer standards published by ECMA International protects two NFC devices communicating. The standard specifies the NFC-SEC secure channel protocol and the shared secret services NFCIP [39]. Cryptographic mechanisms such as the Elliptic Curve of Diffie Hellman (ECDH), integrity and encryption protocols such as AES are described.

To ensure authenticity and integrity, the tags manufacturer or developer needs to encrypt the payload using encryption algorithms. Encryption is at the very first NFC security level. It assures the protection of user information, the confidentiality. Cards such as the MIFARE ultralight EV1 are sensitive to sniffing attacks: a simple password mechanism to authentication through a clear text password is transmitted and then acknowledged or rejected. Mutual challenge-response authentication also exists using a shared key for tags such as the MIFARE classic (encryption and authentication protocol broken since 2008), Sony Felica Cards or even the MIFARE DESFIRE. With this approach an eavesdropper cannot retrieve the shared key. Some successful side-channel attacks have been made on MIFARE DESFIRE [40] pushing the manufacturers to release safer smart cards such as the MIFARE DESFIRE EV2 not cracked yet. Classic algorithm used are AES, DES and 3DES. Example of MIFARE tags encryption is shown in Figure 6. Some proprietary authentication and algorithms (*e.g.*, MIFARE classic CRYPTO1 algorithm) have been released but most of them are broken. Recent cards such as the MIFARE ProX and SmartX share a new approach with a microprocessor directly incorporated within the card.

3 TOOLS

This research and development project has been made possible by the use of some basic and also complex tools. A brief description of each tool used during the research is presented.

3.1 PROXMARK 3

The Proxmark 3 kit shown in Figure 1 is developed by Rysc Corp[11], a small company created in 2009 that aims to make the use of open source technologies easier.

Figure 4 - Proxmark 3 kit

The Proxmark 3 is one of the best tool for researchers in the RFID and NFC field. This RFID security research Swiss army knife [41] is composed of an hardware and a software part which makes it a great educational tool. The high level software terminal interface proposed makes low level operations easier for RFID/NFC or programming newbies by simply entering special commands. It can read, write or emulate contactless cards. It contains a High Frequency (13.56 MHz) and Low Frequency (125kHz and 134 kHz), the Proxmark 3 device and contactless cards to play with.

[11] Company designing and creating devices that helps research and development projects. More information at https://store.ryscc.com/

3.2 ACR 122U READER

The ACR 122U is one of the most common NFC reader and writer device. Shown in the Figure 5, this device developed by Advanced Card Systems (ACS)[12] is one of the most famous NFC reader writer. Its advantageous price makes this PC-linked smart card reader and writer a great tool as it is also ISO/IEC 18092 (NFC standard) compliant. Moreover, it supports all types of NFC tags.

Figure 5 - ACR 122U NFC reader

3.3 ANDROID SMARTPHONE

In the research of the android capabilities in the field of NFC technology, the author used his personal non rooted android phone: One plus 3T. The tests have been made under Oxygen OS version 4.1.7 and android Nougat, version 7.1.1. Mobiles and specifically Android is one of the major result of NFC expansion. The author naturally wanted to know what could possibly done with Android OS and what security offers the NFC stack.

[12] Advanced Card Systems is a famous Hong-Kong based company. They develop and supplies smart card reading and writing devices and other related products to over one hundred countries.

4 EXPERIMENTATIONS, FROM THEORY TO PRACTICE

The contribution made from this research can be split in three different points. A special MIFARE case is described as the author encountered these unsecure tag types constantly. To achieve the MIFARE dismantling experimentations, a desktop application has been created and is also presented. An android application is shown as a state of the art of what could be done with android and EMV-based smart cards.

4.1 MIFARE AND MIFARE CLASSIC

According to Franz Antmann, one of the creators of NFC, "NFC is based on a pre-cursor communicative technology called MIFARE Contactless" [3]. MIFARE has evolved significantly since then and is the leader of contactless products. Smart cards of course already existed before NFC technology but this last one expanded the possibilities and applications of contactless smart cards. Since the first release of the MIFARE tags shown in Figure 6, and still nowadays, the MIFARE smart tags have been in use by most of the world.

	Mifare Ultralight	Mifare Ultralight C	Mifare Classic	Mifare Plus	Mifare DESFire	Mifare DESFire EV1
Introduced in	2003	2008	1994	2008	2002	2006
Memory bytes	64	192	320 1024 4096	2048 4096	4096	2048 4096 8192
Cryptography	-	3DES	CRYPTO1	AES	DES 3DES	DES 3DES AES
UID bytes	7	7	4/7	4/7	7	4/7

Figure 6 - MIFARE family smart cards [42]

The security issues demonstrated multiples times by hackers or researchers [43] [44] [45] and the non-awareness of developers have compromised many systems securities. Indeed, the MIFARE Classic tag is one of the most used and the broken

CRYPTO1 proprietary cryptography algorithm behind still remains widely used for several type of applications: Key-fobs, e-payment… The Oyster card used on public transport in London changed the tag used from MIFARE Classic to MIFARE DESFIRE EV1 which uses a more secure algorithm (DES, 3DES). Other examples such as the Paris public transport card is also a good example but other companies do not share the same reactivity.

Sector	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Block (1block = 16byte)	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	
	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	
	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62	
	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59	63	1K
Sector	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
Block	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	
	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125	
	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126	
	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123	127	2K
Sector	32	33	34	35	36	37	38	39									
Block	128	144	160	176	192	208	224	240									
	129	145	161	177	193	209	225	241									
	130	146	162	178	194	210	226	242									
	131	147	163	179	195	211	227	243									
	132	148	164	180	196	212	228	244									
	133	149	165	181	197	213	229	245									
	134	150	166	182	198	214	230	246									
	135	151	167	183	199	215	231	247									
	136	152	168	184	200	216	232	248									
	137	153	169	185	201	217	233	249									
	138	154	170	186	202	218	234	250									
	139	155	171	187	203	219	235	251									
	140	156	172	188	204	220	236	252									
	141	157	173	189	205	221	237	253									
	142	158	174	190	206	222	238	254									
	143	159	175	191	207	223	239	255									4K

Figure 7 - MIFARE Classic Memory Layout

A Mifare Classic tag can either be 1, 2 or 4 Kilobytes as shown in Figure 7. They contain sectors where each has blocks of data storage and among these blocks, one block for storing the secret access keys and access controls (ACL). The reader must authenticate each time to the tag with a secret key before reading a sector and its content. Each sector contains two keys conventionally named A and B. Of course, each sector can define its own access rights in order to perform specific operations. The sector 0 block 0 contains a Unique Identifier (UID) and some manufacturer data. This section can only be re-writeable on special Chinese tags containing a backdoor. To successfully read or clone such card, an attacker needs to know all the A and B keys of each card sectors.

4.2 Desktop Application: card cracking and data extraction

In order to exploit MIFARE or other tags, myself and especially my colleague Dorian worked on a C++ project using the ACR122U reader writer. The high level interface given by the Proxmark 3 gives less flexibility than necessary for this work.

This project used LibNFC which is a NFC controller library giving access to the NFC interface. PC/SC smart card API provides a standard interoperability over readers and computer platform from different manufacturers. The implementation of this interoperability layer, pcsclite was used. The author tested both libraries LibNFC and LibFreefare (which is a higher level library based on LibNFC) and the LibNFC was preferred as it comes with most powerful possibilities (*e.g.*, some cards were not read with libFreefare but was recognized with LibNFC).

This easy tool helped both of us in our experiments on NFC technology by simplifying them. It allows successfully the clone of a tag, listing of all NFC tags near the reader and the binary dump of the content tag as described in the - Desktop application usage. To dump a tag, a file containing the keys of that very same tag is needed.

```
./nfc --mode=[MODE] [OPTIONS]
Available modes : clone-tag, clone-file, list, dump
Options :
        --keyfile=[FILE]  the file containing the keys of the tags for cloning
        --tagfile=[FILE] the MFD file containing the representation of a tag
        --clone-keys            enable the cloning of the keys areas
        --clone-acl             enable the cloning of the acl areas
        --clone-uid             enable the cloning of the uid areas

Modes :
Clone Tag :
        Clone a tag present on a reader         Need the option [--keyfile]. Options [--
clone-keys], [--clone-acl],[--clone-uid] can be added to modify behaviour.
Clone File : Same as Clone Tag, where the tag is read from a parameter (binary) file
List: List the tags on the reader
```

DUMP: DUMP ONE OF THE TAGS ON THE READER

Figure 8 - Desktop application usage

This application could be seen as an equivalent to the Mifare Classic Tool android application.

In order to have the secret keys of the tag you want to dump, the author used two very well-known open-source programs: MFOC and MFCUK. MFOC[13] stands for Mifare Classic Offline Cracker and allows an attacker to recover the keys of a tag with an Offline nested attack. MFOC is useful to retrieve the keys of a tag when a unique or a few keys are already known. A well-known list of default keys set by the manufacturer are not reset and still remains int the tag. These default manufacturer keys are taken into account by MFOC such as 0xFFFFFFFFFFFF at NXP chip deliveries. Changing all these default keys before using a tag could already be a first security step trying to avoid MFOC and MFCUK which are powerful software. When MFOC do not succeed finding a key, Mifare Classic Universal Toolkit (MFCUK)[14] timeout attack can be used. Both software need first the installation of pcsclite and LibNFC in order to work.

4.3 ANDROID APPLICATION: EMV AND CREDIT CARDS

NFC is most of the times mingled with contactless payments. Indeed, it is one of the very first NFC application and also the one that pushed the NFC to the worldwide technology it is nowadays. Many services have been created for users such as Apple Pay or Google Wallet. Renaud Lifchitz, a French computer security engineer have been the first in 2012 to warn banks, French ministry of Finance and the National Commission on Informatics and Liberty (CNiL) about the available data that could be read from a EMV-based contactless credit card [46]. Because of his researches back then, investigations have been made by responsible organizations and law enforcement. Cardholder's name can no longer be accessed during contactless

[13] MFOC Source code: https://github.com/nfc-tools/mfoc
[14] MFCUK Source code: https://github.com/nfc-tools/mfcuk

exchanges for example for the vast majority of cards issued. The idea was to compare French subway Navigo smart card heavily secured as well as RFID passport chips and the credit card authentication and encryption avoidance by the EMV standard. EMVCo, formerly EMV, is an association of several companies which are responsible for technical standards for smart payments. EMV is therefore responsible for the poorly designed proposed. Indeed, the communication between the contactless card and the terminal is not encrypted.

The purpose of the NFC-Exploration android application written uniquely by the author is the scan of an EMV-based credit card to see if some measures have been taken since 2012. A java library[15] has been written also by a French security engineer Julien Millau. This low level library still needs a good understanding of EMV protocol and a wrapper has been developed by the author to provide a higher level library. Once done, a brief front-end interface presents the most useful data retrieve for all EMV-based credit card which represents in 2016, 97.75% transactions in Europe [47].

[15] Source code of the library could be fine here: https://github.com/devnied/EMV-NFC-Paycard-Enrollment

5 Results and Analysis

Some critical security issues have been discovered during this research. The result of the work is explained in this section as well as an analysis and possible ways to counter these security flaws.

5.1 MIFARE And Card Cracking

First test the author has done is the clone of its personal university accommodation room NFC tag (appendix UNIVERSITY ACCOMMODATION ROOM TAG AND DOOR SYSTEM). The tag used is a simple Mifare classic 1K which is either not secure or read-only. The tag keys were all default manufacturer ones and therefore effortless to break. The access of at least one University of Kent College accommodation student's rooms relies on poor security. Only the Unique Identifier (UID) is verified to access a building. Some data present in the sector 0 block 1 of the tag was especially written to only access its personal room once entered. Dorian reversed engineered the data present in the this very same block and could open with its own key multiples rooms. This is a critical security as an attacker could clone a student tag, reverse engineer it and possibly access all rooms of the college. Moreover, College accommodation proposes a cleaning service every week. The cleaners all had tags that could open all the doors from every single residence. With this total absence of security, one could possibly clone such tag and have access everywhere without being noticed. The clone of such tag only takes few seconds especially because of default manufacturer keys which are the first keys tried to recover a tag.

A considerable security issue was discovered by the author concerning the smart contact MIFARE 1k student card, appendix KENT CARD CLONING. Cloning the University contactless card was done using the same process as the university accommodation room access tag seen before. Two elements were found inside the card: the DHL lending number in sector 12 and the Student number in the sector 10 and 11. The critical security issue concerns the ability to pay for goods within the

University. Indeed, a student can do its groceries, buy a coffee or a beer with its student card. Top up the card is done with a web application in which you can see your credit, transactions and other information. At least, the balance cannot be influenced as it is handled by a remote server so an attacker could not steal money unlike the Selecta food and drinks distributors in Paris that is broken since 2015 for example [48].

According to the University of Kent website [49], “This multi-functional card enables you to borrow books from the library, become a member of Kent Sport, purchase items at Blackwell’s on the Canterbury campus and offers access to specific areas of the University”. The website even ensures you that “your KentOne card is a quick, easy and safe way to buy food and drink”. The appendix PAYING A COFFEE WITH A CLONED KENT CARD shows the payment terminal used to buy a coffee in the University campus. This blue tag is a Chinese MIFARE tag that contains the dump of the author KentOne card (topped with 5£) was copied with the desktop application developed and the keys were found with MFOC software. Privacy is illusory as shown by the appendix PRINTING WITH A KENT CLONNED CARD as one attacker can discover the name of a student by accessing a University printer and also see the print jobs awaiting (confidential documents could also be stolen). An attacker can also steal books by using the Kent card of a student without turning them back as the loan was not register to the attacker name. The Kent Sport subscription could be also bypassed by impersonate a student that is already subscribed (this use case has not been tested and will depend on the security system of the Kent Sport department: two accounts logically cannot be in the gym at the same time if the system is well-implemented).

The author is not sure about the authentication of the devices and the Kent One card as either the UID, the Student Number or both can be verified to authenticate a student. If only the student number is verified, it means that a simple tag (not UID changeable) is necessary and that you could even pay with your mobile phone by emulating the student number at the good sector. Moreover, it could be even easier to impersonate someone else just by knowing its student number.

5.2 ANDROID APPLICATION

The appendix NFC-EXPLORATION ANDROID APPLICATION INTERFACE shows the author credit card read by the application developed. This application developed by the author is capable of recognizing any type (VISA, MASTERCARD ...) of contactless EMV-based credit cards. Although you cannot read an entire wallet and read a specific card with Android NFC stack, you can scan one by one a credit card and retrieve interesting information. Since 2012 and the revelation of EMV security flaws [46], nothing changed except the cardholder's name that is no longer retrievable.

Although the CVV is not retrieved from EMV cards, a research in 2017 conducted by some researchers shows how easy to obtain details about your Visa using online purchases [50]. It is shown that online merchants only require Primary Account Number (PAN) and the expiry date. The attack consists of a distributed guessing attack over multiple online merchant's websites to guess the expiry date, and even the CVV. According to the paper, a bot configured with 30 websites can only took 4 seconds to obtain all information from a card.

With such knowledge of online purchase, having the PAN and the expiry date provided by the application is enough and you can even get the CVV easily with such attack.

5.3 COUNTERMEASURES

Recording EMV-based credit card data is not enough to clone a credit card as some information such as the private key (certificate) to sign transactions that are not transmitted during a transaction and cannot be accessed. Nevertheless, valuable information still can be retrieved and abused: linking one piece of information in such cards can often quickly be escalated into leak everything. EMV design should be reconsidered to avoid an attacker to retrieve remotely valuable available data. Secure measures and not illusory ones such as the very secured dynamic pictograms transmitted in clear text. Contactless accesses should be authenticated, protocol has

to define encryption to avoid eavesdropping valuable data as we saw and integrity should be insured to avoid injection. Such security already exists, protocols just have to change, EMV should be modified or even rewrite.

In the other hand, systems should not base their security upon the UID of a tag. From the University accommodation access room tag and especially for payments like the Kent One card. The cards whose security has been compromised such as MIFARE classic card must not be used for payment application. Encryption should be used to avoid the guess of secret keys and therefore the clone of tags. Secure cards such as MIFARE DESFIRE EV2 exists and should be used for payment transaction ensuring the confidentiality, integrity and authenticity.

6 FUTURE WORK

The research seems to have raised more questions that it can answer as the field of NFC technology is quite endless. There are multiple areas of research that should be pursued each arising from this research. There are plenty opportunities for extending the scope of this work that are described in this section.

The announce of the new NFC API for IOS developers [13] has been released during the writing of this research and have not been studied neither used. The capabilities of this new API could be used for multiple purposes and hence should be exploited.

In this work, the author stayed on an unrooted Android device. A rooted device would have offered way more possibilities. Modifying directly the android NFC stack could lead to the read of multiple NFC cards at once for example. Another very interesting option could be the modification of the very same NFC stack in order to modify the compulsory random UID [51]. That could lead to the centralization of all the smart cards right into your phone, emulating every tag you dumped (including the UID) and then no longer need physical tags. The android proof of concept developed could be pursued to ensure a more user-friendly interface with useful features such as the record of the cards scanned and many others.

A few more tests could be run to check the authentication of the Kent One card terminals of each good (library, coffees, Kent Sport and printers) in the University of Kent in order to know which information is taken into account to authenticate a student: the UID, the student number or both.

Profiling almost has not been discussed in the work. Indeed, most of the hackable tags do not carry important information. These tags are generally identified from a remote server that only verifies the tag UID. There might be some tags with interesting data such as the name of a person, its birthday… Identifying patterns on smart cards could lead to the identification of what kind of card it is (*e.g.*, gym card from a specific company) at the scan of an entire wallet.

7 CONCLUSION

This work provides a comprehensive and recent review of NFC technology concerning its evolution, security issues and practical applications illustrating the current NFC security status. Today, companies and developers have not been clear-sighted about the dangerousness of some security flaws as such presented in this research. A first approach of what is NFC, its history and its current and future evolution was described. Also an explanation of its mode of operation according to the standard protocols put in place by different entities. A literature review clarified some misconceptions about NFC technology security and some real flaws, that were for most of them patched by standards, assuring the confidentiality, the authenticity and integrity of the communication through encryption. NFC communication security standards are mostly optional and are not fully respected and rather ignored. This can be observed by the practical experiments and the applications developed. This contribution has shown the current status of NFC security and what has changed over the years. EMV-based credit cards are studied through a state of the art of Android NFC stack possibilities. The work of this research is constantly in progress as the NFC technology, its standards and security continues to evolve.

REFERENCES

[1] N. Forum, "NFC Modes of Operation," [Online]. Available: https://nfc-forum.org/what-is-nfc/what-it-does/.

[2] N. Forum, "Tag Format Support release," 2006 June 5. [Online]. Available: https://nfc-forum.org/newsroom/nfc-forum-unveils-technology-architecture-and-announces-initial-specifications-and-mandatory-tag-format-support/.

[3] F. Amtmann and P. Maugars, "A Brief history of NFC," NXP Semiconductors, 17 September 2015. [Online]. Available: http://www.newelectronics.co.uk/.

[4] N. Forum, "Home ›Newsroom ›NFC Forum Press Releases ›NFC Forum Unveils Technology Architecture And Announces Initial Specifications And Mandatory Tag… NFC Forum Unveils Technology Architecture And Announces Initial Specifications And Mandatory Tag Format Support," NFC Forum, 5 June 2006. [Online]. Available: https://nfc-forum.org.

[5] A. Developers, "NFC Connectivity," Google, 2009. [Online]. Available: https://developer.android.com/.

[6] N. World, "Google Unveils first Android NFC Phone," 7 December 2010. [Online]. Available: https://www.nfcworld.com.

[7] S. C. A. P. C. w. paper, "Contaactless EMV Payments: Benefits for consumers, Merchants and Issuers," EMV Connection, 2016.

[8] "Cashless payments could cause over consumption," The New Economy, 22 December 2014. [Online]. Available: https://www.theneweconomy.com.

[9] T. Anne, "Wireless Chemical Sensor for Smartphone," MIT News Office, 8 December 2014. [Online]. Available: http://news.mit.edu/.

[10] C. Brown, "Pizza Hut offers NFC tattoos that let customers order favourite takeaway," NFC World, 21 October 2016. [Online]. Available: https://www.nfcworld.com/.

[11] N. Forum, "Simplifying IoT: Connecting, Commissioning, and Controlling with Near Field Communication (NFC)," NFC Forum, June 2016.

[12] NXP Semmiconductors, "Blog," 2006-2017. [Online]. Available: https://blog.nxp.com/.

[13] A. Developer, "Core NFC," Apple, 5 June 2017. [Online]. Available: https://developer.apple.com/documentation/corenfc.

[14] L. Liu, "Beijing subway line support bush mobile phone ride," Beijing Youth Daily Internet Communication Technology, 14 August 2017. [Online]. Available: http://epaper.ynet.com.

[15] S. Timmy, "Ofo to launch NFC-enabled smart locks," Technode, 22 August 2017. [Online]. Available: http://technode.com.

[16] M. Adam, "China's Cashless Revolution," Bloomberg, 19 July 2017. [Online]. Available: https://www.bloomberg.com/.

[17] C. Sarah, "EMVCo standarsizes QR codes for mobile payments," 19 July 2017. [Online]. Available: https://www.nfcworld.com.

[18] R. R. Melanie, C. Bruno and S. T. Andrew, "Is your cat infected with a computer virus?," Vrije Universiteit Amsterdam, Amsterdam, 2006.

[19] C. Ryan, "NFC Hacks revealed at Black Hat," SecureIdNews, 26 July 2012. [Online]. Available: https://www.secureidnews.com.

[20] M. Charlie, "Exploring the NFC Attack Surface," Accuvant Labs, Denver, 2012.

[21] Gao RFID Inc., "13.56 MHz reader writer," Gao Group, 2006. [Online]. Available: http://gaorfid.com/.

[22] P. Tereza, "Hacking Contactless with homemade antennas shortcoming of NFC," 8 November 2013. [Online]. Available: https://terezapultarova.wordpress.com/.

[23] F. M. Stig and S. K. Henning, "Eavesdropping Near Field Communication," The Norwegian Information Security Conference (NISK), Trondheim, 2009.

[24] Marsh, "RFID reader snoops cards from 3 feet away," HackADay, 3 November 2013. [Online]. Available: https://hackaday.com.

[25] K. Ilan and W. Avishai, "How to Build a Low-Cost, Extended-Range RFID Skimmer," Tel Aviv University, Ramat Aviv, 2006.

[26] P. D. Thomas, A. B. Johann, W. C. B. Tim and W. Stephan, "Eavesdropping Near Field Contactless Payments: A Quantitative Analysis," University of Cambridge, Cambridge, 2014.

[27] P. H. Gerhard, "Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens," University of London, London, 2010.

[28] DEF CON, "DEFCON 17 Archives," DEF CON Communications, 2 August 2009. [Online]. Available: https://defcon.org/.

[29] J. Wehr, "understanding anticollision processing multiple cards at the same time," 1 January 2003. [Online]. Available: https://www.secureidnews.com.

[30] H. Gerhard, "A Practical Relay Attack on ISO 14443 Proximity Cards," University of Cambridge, Cambridge, 2005.

[31] F. Lishoy, H. Gerhard, M. Keith and K. Markantonakis, "Practical NFC Peer-to-Peer Relay Attack using Mobile Phones," University of London, Egham Hill, 2010.

[32] L. Eddie, "NFCProxy," in *DEFCON 20*, Las Vegas, 2012.

[33] S. Haoqi and Y. Jian, "Man in the NFC," in *DEF CON 25*, Las Vegas, 2017.

[34] observatoire de la sécurité des moyens de paiement, "Premier rapport annuel de l'Observatoire de la sécurité des moyens de paiement," Banque de France, 18 July 2017. [Online]. Available: https://www.banque-france.fr.

[35] F.-B. Thomas, "Implant android attack," Forbes, 27 April 2015. [Online]. Available: https://www.forbes.com/.

[36] J. R. Milne, T. Xiong and C. McCoy, "Configuration of Data and Power Transfer in Near Field Communications". United States of America 9 November 2016.

[37] G. A. Developers, "NFC HCE ProtocolParams," Google, 2013. [Online]. Available: https://developer.android.com/.

[38] NFC Forum, "The practical uses of the nfc signature RTD 2.0 specification," 24 April 2015. [Online]. Available: https://nfc-forum.org.

[39] B. Rian, "ECMA updates NFC Security standards," NFC World, 11 August 2015. [Online]. Available: https://www.nfcworld.com.

[40] T. Kasper, v. M. Ingo, O. David and P. Christof, "Cloning Cryptographic RFID Cards for 25$," Ruhr-University, Bochum, 2010.

[41] G. d. K. G. R. V. Flavio D. Garcia, "Tutorial: Proxmark, the Swiss Army Knife for RFID Security Research," Radboud University, Nijmegen, 2012.

[42] D. K. G. Gerhard, "Outsmarting Smart Cards," Institute for Programming research and Algorithmics, Nijmegen, 2013.

[43] d. K. G. Gerhard, H. Jaap-Henk and D. G. Flavio, "A Practical Attack on the MIFARE Classic," Radboud University Nijmegen, Nijmegen, 2008.

[44] G. d. K. G. R. M. P. v. R. Flavio D. Garcia, V. Roel, W. S. Ronny and B. Jacobs, "Dismantling MIFARE Classic," Radboud University Nijmegen, Nijmegen, 2008.

[45] D. G. Flavio, v. R. Peter, V. Roel and W. S. Ronny, "Wirelessly Pickpocketing a Mifare Classic Card," Radboud University, Nijmegen,, 2009.

[46] L. Renaud, "Hacking the NFC credit cards for fun and debit ;)," Hackito Ergo Sum, Paris, 2012.

[47] EMVCo, "Worldwide EMV® Deployment Statistics," EMVCo organization, 2017.

[48] Dyrk.org, "Faille NFC Distributeur Selecta," 3 September 2015. [Online]. Available: https://dyrk.org/2015/09/03/faille-nfc-distributeur-selecta/.

[49] University Of Kent, "Kent One Card," 09 September 2015. [Online]. Available: https://www.kent.ac.uk/kentonecard/.

[50] A. A. Mohammed, A. Budi, E. Martin and v. M. Aad, "Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?," Newcastle University, Newcastle, 2017.

[51] M. Roland, "Host-based Card Emulation with fixed card ID," 15 February 2015§. [Online]. Available: https://stackoverflow.com.

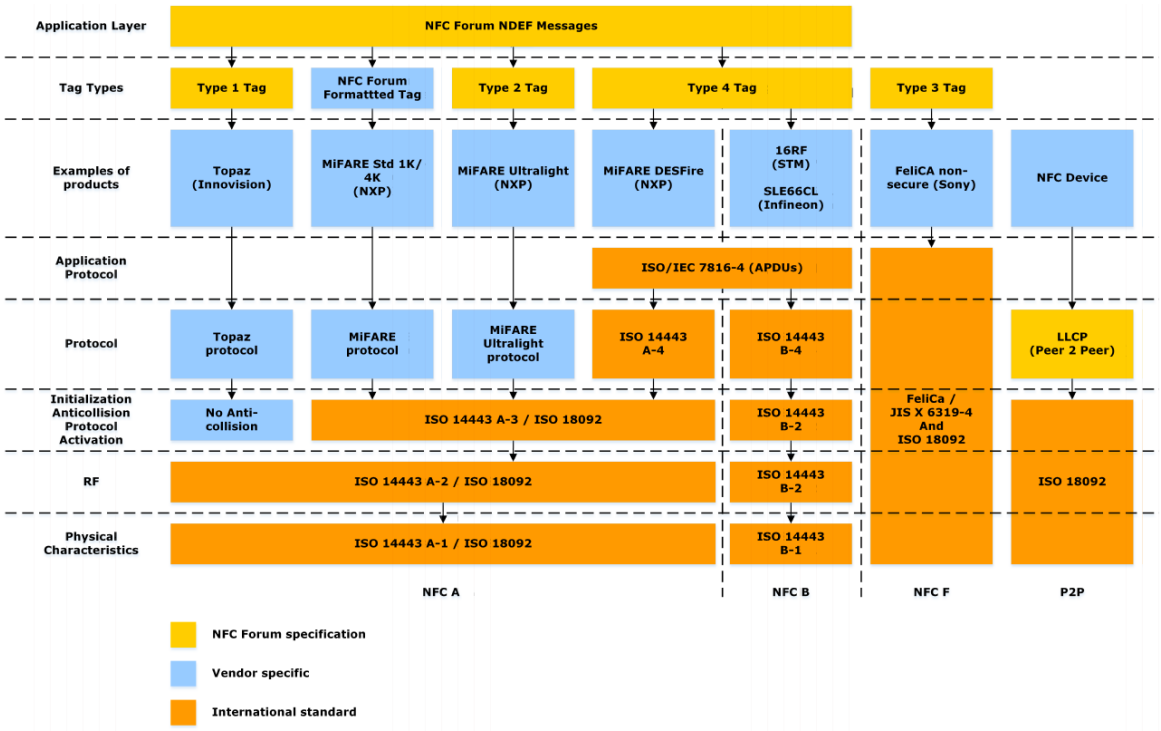
[52] B. Olivier, "Cash versus credit save money," The Guardian, 1 June 2012. [Online]. Available: https://www.theguardian.com.

APPENDICES

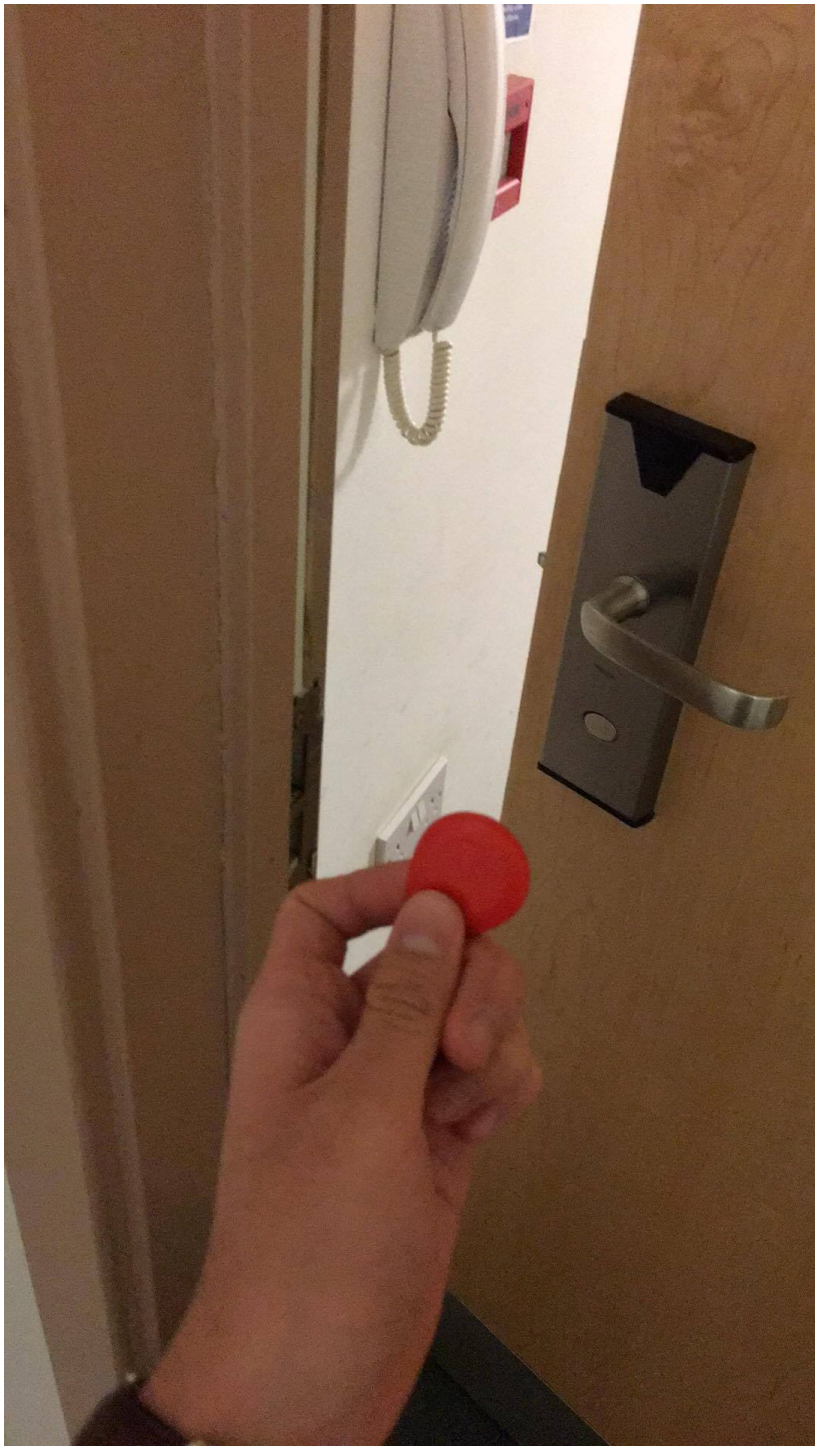
NFC Tag Types

Tag Type	Use Case	Chip Examples	User Memory (bytes)*	UID Length (bytes)	Cost
Forum Type 1	Specialized	Innovision Topaz	90 - 454	4	$
Forum Type 2	Most common, low cost, single application like smart poster, personal label etc.	NXP MIFARE UL, MIFARE UL-C, NTAG 203, 210, 212 etc.	46 – 142	7	$
Forum Type 3	Specialized, Asian markets	Sony FeliCa (Lite)	224 – 3984	8	$$$
Forum Type 4	High memory applications, high security (in non NFC mode)	NXP MIFARE DESFire EV1 -2K, 4K, 8K, Inside Secure VaultIC 151/161, HID Trusted Tag™	1536 - 7678	7	$$$
Forum Type 5 (NFC-V / ISO 15693)	If longer read range is required, industrial rugged tags – added as forum tag type June 17, 2015.	NXP ICODE SLIx family, EM4233, Fujitsu FRAM MB89R118C, MB89R112, HID Vigo™	32 – 8192 (112 for ICODE SLIx)	8	$ - $$$
MIFARE Classic	Very common, high memory Not compatible to all devices!	NXP Mifare Classic 1K, 4K	716 - 3356	4 or 7	$$

NFC Protocol Stack Overview

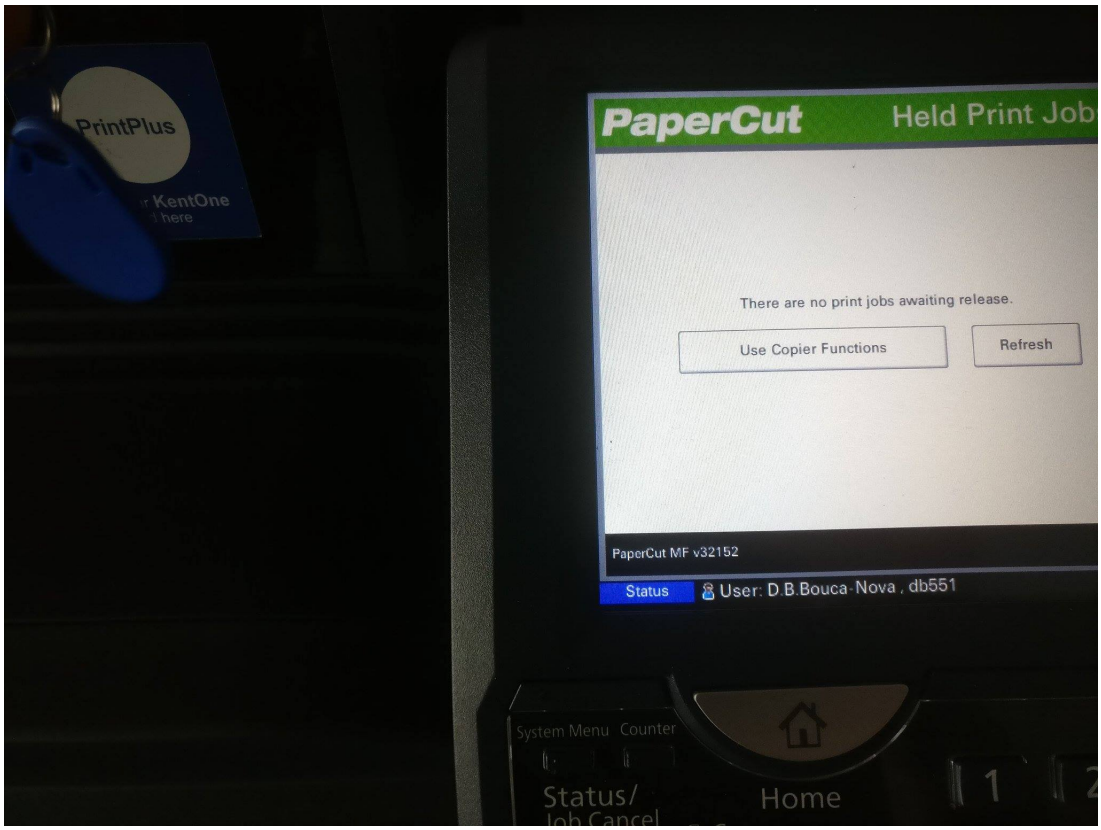


University Accommodation Room Tag And Door System



KENT CARD CLONING

PRINTING WITH A CLONED KENT CARD



PAYING A COFFEE WITH A CLONED KENT CARD

NFC-EXPLORATION ANDROID APPLICATION INTERFACE