FUNDAÇÃO GETULIO VARGAS
ESCOLA BRASILEIRA DE ADMINISTRAÇÃO PÚBLICA E DE EMPRESAS
MESTRADO EXECUTIVO EM GESTÃO EMPRESARIAL

Mobile ID in Physical Access Control Applications

Dissertação apresentada à Escola Brasileira de Administração Pública e de Empresas para obtenção do grau de Mestre

Eduardo Simonetti

Rio de Janeiro – 2016

Ficha catalográfica elaborada pela Biblioteca Mario Henrique Simonsen/FGV

Simonetti, Eduardo
Mobile ID in physical access control applications / Jose Eduardo Simonetti. – 2016.
81 f.

Dissertação (mestrado) - Escola Brasileira de Administração Pública e de Empresas, Centro de Formação Acadêmica e Pesquisa.
Orientadora: Ana Paula Borges Gonçalves.
Inclui bibliografia.

1. Empresas – Redes de computadores – Medidas de segurança. 2. Comunicação por campo de proximidade. 3. Sistemas de comunicação sem fio. 4. Sistemas de comunicação móvel. 5. Segurança de informações. 6. Computadores – Controle de acesso. I. Gonçalves, Ana Paula Borges. II. Escola Brasileira de Administração Pública e de Empresas. Centro de Formação Acadêmica e Pesquisa. III. Título.

CDD – 658.478

JOSÉ EDUARDO SIMONETTI

MOBILE ID IN PHYSICAL ACCESS CONTROL APPLICATIONS.

Dissertação apresentada ao Curso de Mestrado Profissional Executivo em Gestão Empresarial da Escola Brasileira de Administração Pública e de Empresas para obtenção do grau de Mestre em Administração.

Data da defesa: 10/11/2016.

ASSINATURA DOS MEMBROS DA BANCA EXAMINADORA

Ana Paula Borges Gonçalves
Orientador (a)

Mario Couto Soares Pinto

Luis Filipe Rossi

3 Table of Contents

4 List of Illustrations

5 List of Tables

List of Abbreviations

Identity and Access Management (IAM).

Physical Access Control Systems (PACS)

Radio Frequency IDentification (RFID)

Near Field Communication (NFC)

Mobile ID in physical access control applications

(Smartphones integration into security solutions and access control systems PACS)

6 Abstract

Today there exist a myriad of different types of physical access control systems (PACS) that use a smart card or mobile device as a key. The mobile device enabled smart locks, as they are often referred to, operate using either Wi-Fi or Bluetooth. This thesis has explored the use of a third emerging wireless technology called Near Field Communication (NFC) available in mobile devices such as smartphones. Near Field Communication (NFC) technology is a relatively new technology that is on the rise and is included in almost every new mobile device. By leveraging Near Field Communication (NFC) enabled mobile devices, a highly secure access control system can be achieved and developed taking advantage of the computational power of smartphones in comparison to traditional methods the business implications are huge, Several different authentication and encryption protocols, mobile operating systems and Near Field Communication (NFC) modes of operation where analyzed and evaluated. After considerations technical considerations the Secure Remote Password authentication protocol on top of Near Field Communication (NFC) card emulation (CE) scheme with the client application running on smartphones operating system (OS) was selected. This thesis shows that Near Field Communication (NFC) enables a mobile device to act as a key in a secure access control system (PACS) and as the user base for NFC grows larger so will the likelihood that we will come to see more of these types of systems in business and organizations.

7 Introduction

Nowadays, access control systems are always in demand and are used everywhere around us. We use online services on the Internet, such as email accounts, social networks or any other cloud services. Further, the access control is used for getting access to the PC, computer networks or to a protected physical area in buildings.

In each case, it is necessary to control access of users to the required assets. The increasing amount of services brings new needs for security and privacy enhanced techniques, which provide better protection of user privacy and credentials. Current systems, which support privacy protection techniques, are only usable for online Web-services based on Logical Access Control (LAC). On the other hand, a higher computational complexity causes the fact that the schemes are not usable for Physical Access Control (PAC), because they usually use low-cost devices such as contactless smart cards, key fobs, tokens, etc. This thesis describes the current state of the most frequent technologies in the field of physical access control and a consideration of the practicalities of a broad adoption of mobiles in physical access control (PACS) and the likely impacts business.

In today's fast growing technology world, most of mobile devices are equipped with wireless modules that enables data transfer by bringing two devices in close proximity, which are a potential way of solving the problems and weaknesses of physical access control (PACS), smartphones can emulate and offer compatibility with other contactless smart card standards used in physical access controls systems (PACS). This thesis list down the basic working principles of radio frequency identification (RFID) technologies built-in in smartphones, the protocols involved, risks and vulnerabilities of integrating them in physical security applications, and comparing the traditional methods with the proposed one. By using the wireless communication features of a modern smartphone, such as Near Field Communication (NFC) as solid ground to transmit and receive information to and from various sources can be established.

This thesis work starts with an introduction to radio frequency identification (RFID) standards and how the technology works. Followed by taxonomy of known attacks and threats affecting radio frequency identification (RFID), which avoids going through too much of technical details

but provides references for further research and study for every part and attack. Then radio frequency identification (RFID) security threats are reviewed from risk management point of view, linking introduced attacks to the security principle they affect.

A market research in the physical access control landscape, predicted growth and trends, a global forecast and analysis, as well as a market research in smartphone market penetration of mobiles with biometrics capabilities, analyze the market projections and forecasts. This thesis presents a concise survey on different types of mobile access and their pros and cons. Mobility is the driving force that will unleash the long awaited biometric revolution, since the introduction of the Apple Touch ID[1] fingerprint sensor, Apple disrupted the market by opening a blue ocean of possibilities in mobile identity and authentication, allowing to evolve towards user-centric identity[2] and closing the human-machine identity gap, but the rollout of mobile identity in physical security is being slow, challenges and difficulties such as lack of standardization, proprietary protocols and lack of hardware interoperability at the physical layer, renders the adoption more difficult than in the logical access world. This thesis focus on the challenges that inhibit the integration of mobile ID into physical security, including case studies in higher education and a proposed migration strategy for businesses and organizations.

Mobility is the driving force in our daily lives and at work physical access control is not the exception. The future of access control systems will be a smartphone App and mobile technologies. Now days we use smartphones to pay for goods (Apple Pay, Android Pay, Google Wallet, etc.) in a secure and convenient way, why not use them for access control as well, since more and more people refuse to leave home without their smartphones devices. Mobile ID should work wherever a person is and goes, security systems must cater to those things. This ability will be attractive to companies whose employees frequently travel to other worksites. Employees can set up access privileges prior to their trips, alleviating the headache of having to sign into a system at the site or wait for an on-site employee to give them access to the building.

[1] "*Apple – Iphone 6 –Touch ID*", Available at http://www.apple.com/iphone-6/touch-id/, Accessed 30 March 2016

[2] El Maliki, Seigneur (2007). *"A Survey of User-centric Identity Management Technologies."* IEEE: Technology and application, 12 –17

As we go about our lives, we have the "real us" and then the things that tell the world and machines who we are (keys, passwords, PINs, ID badges etc.). The flaw in "traditional identity" is that credentials can be shared, borrowed, forgotten or even stolen leaving us with nothing more than a suspect identity. Giving access to physical spaces, logical applications or account information where it isn't warranted. The only way to mitigate this risk is by using more sophisticated authentication and encryption methods and our unique characteristics to verify who we are, biometrics are completely unique to us, cannot be shared, stolen or borrowed. They are our rightful Identity this two premises are perfectly compatible with smartphone devices[3].

There are 3 inherited weaknesses in physical security and traditional access control systems and no matter what we do; these weaknesses will never go away:

Traditional Identity	Mobile Identity
Physical objects: static objects and never up to date, can be lost, stolen and counterfeited (duplicated)	**Logical object**: dynamic software-based digital credential, never lost or stolen, always accurate and up-to-date and valid
Anonymous: impossible to verify, once stolen or shared anyone can use it.	**Digitally Verifiable**: only the owner can use the mobile identity, digital badge ID biometrically linked to the user
Most be **Presented** to the other party and can be intercepted in transit	**Encrypted**: eliminate interception (privacy protection protocols)

Table No.1[4]

Credentials, badges, tokens, password, PIN's remain common forms of identity for physical and logical access. None of those are without risks. They're easily duplicated, are prone to being lost

[3] *Corcoran, Costache (2016) "Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts." IEEE Communication surveys & tutorials, 70 - 78*
[4] *Comparative table between Traditional Identity and Mobile Identity source: Prepared by the author*

and/or shared, and often prove inconvenient. Key cards, unless they've been embedded with RFID technology, can only be tracked at access control readers; by contrast, smart phones devices can be tracked throughout the environment. Mobility is the natural outcome of the identity and access management (IAM). People want on-the-go access, and that demand applies for access control and security systems as well. When these pieces are used in tandem, physical security improves. Patterns and context, situational awareness emerges.

Tomorrow's physical security solutions must address the mobile factor or be left to languish alongside a growing pile of security badges, closed and proprietary access control systems, with proprietary software and hardware that requires a separate infrastructure and dedicated resources.

Both, mobile and cloud offerings will continue to grow in popularity. We already started to experience this trend in higher education, industry stalwarts who have continued to cling to the outmoded server-based architecture rather than investing in cloud or hosted services, as a successor will be cannibalized from several angles. New entrants with credible multi-tenant software as a service (SaaS) products will take some market share, and the few legacy companies who have kept up with the times will be rewarded for their foresight. Many organizations realize that they need to change or improve their existing physical access systems, but balk at the infrastructure costs, investment cycles, and the time it would take for a complete overhaul.

Wireless signals like Radio Frequency RFID, Near Field Communications (NFC), Bluetooth Low Energy (BLE)[5], are embedded in smartphones and allow connected devices talk with the cloud and other hardware. Mobile apps, and wearable technology make it possible to bridge physical worlds and virtual communities. Mobile technology would become a transformational power inherent with the proliferation of smartphones. Smartphones and mobile technologies are driving innovation and viable transition path to a password-free future.

[5] Sousa, Tavares, Abreu, Qintas, Reis, Restivo (2015). *"Wireless control and network management of doors"* IEEE: Technology and application, 141 –142

8 Businesses and Market Review

Looking at the robustness of the security market in general, it reflects several underlying trends. Growing economies, populations, and infrastructures have contributed strong organic growth tied to general economic prosperity. Unfortunately, unrest and the presence of various types of threats are contributing to a sense of greater need for security solutions in general.

Physical forms of identity such as PhotoID badges and key cards are easily lost, stolen, or duplicated, while usernames and passwords can be easily cracked or phished. The inherent weakness of physical IDs and passwords are primarily to blame for the $250 billions of dollars lost to fraud and the $110B lost to cybercrime every year, including damaged reputations and undermined public trust according to Verizon Data Breach Investigation Thesis 2016.[6] Physical badges are hard to manage and offer limited value, clearly, traditional forms of identity are failing and a robust solution is urgently needed to prevent cybercrime and fraud, by empower people to authenticate with credentials that are completely unique to them, such as their face, eyes, heartbeat or fingerprint. This will fundamentally change how we access applications, processes, equipment, doors, or anything else that requires proving who we are.

Businesses and organizations still rely on weak and outdated methods of authentication and too many identities are still at risk, a users identity has tremendous power and is an attempting target for cyber criminals, that's why "63% of confirmed data breaches involved leveraging weak/default/stolen passwords or compromise credentials"[7], our identities provide access to online systems and resources, credentials unlock doors, verify transactions and they help to understand who is interacting with, they are at the very heart on everything in modern business.

[6] Source: 2016 DBIR: "*Verizon Data Breach Investigation Report*" from: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
[7] Sourse: 2016, "*Security & surveillance technology - Statista Dossier"* from: https://www.statista.com/topics/2646/security-and-surveillance-technology/

But protecting and verifying these identities is not and easy task, organizations ranging from universities, state and federal government, financial institutions, retailers and everything in between need a solution that can replace outdated forms of authentication and empower users to safely and easily access physical and logical assets and provide feedback in the form of data analytics on an organization security posture.[8]

Major data breaches have something in common with the way in which the attack was accomplished, the attacker was able to steal a username and password.

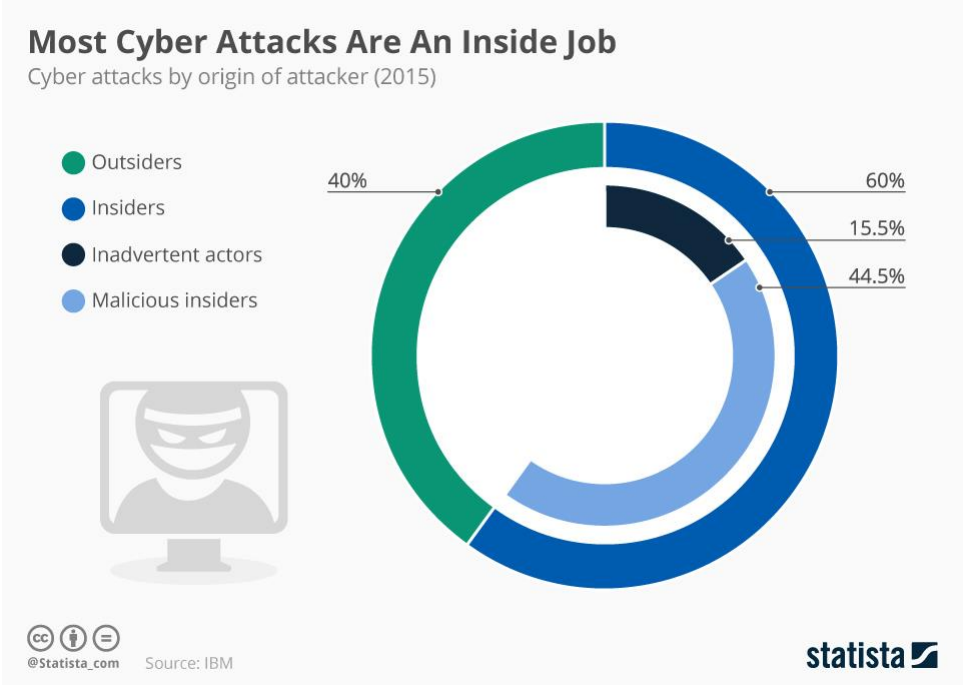

Figure No.1[9]

By leveraging the mobile platform, and its computational power a strong authentication can be implemented in a user-friendly manner. The near term trend for the mobile platform is to take advantage of secure hardware elements and trusted execution environments.

[8] "Enterprise Security Guide" Microstrategy Usher, 2015. Downloaded on December 21, 2015 from http://www.usher.com/Usher/media/documents/guides/enterprise-security.pdf

[9] Cyber Attacks by origin of attacker (2015), Source: Statista, published by: IBM

In recent breaches at major retailers, financial institutions and government agencies, a username and password was stolen early on in the attack[10]. A password is a poor secret because it is difficult to secure. In most cases the password is stolen through a form of social engineering. To make a password attack more difficult several techniques have been introduced that add a second factor to user authentication.[11]

In other words, even though these security techniques offer a higher challenge to an attacker, the difficulty is often not high enough to fully deter the attack. The strength of the authenticator should match the risk being mitigated.

Desktop operating systems do not offer the same level of application isolation as mobile operating systems. This isolation prevents mobile device malware from interfering in the memory space of critical native apps. This technique has proven itself in mobile commerce applications, giving the option to store cryptographic credentials in a very secure environment such as hardware secure elements (SE) and trusted execution environments in the phone. This is an improved method from username and password use, in terms of both security level and user experience[12].

Strong authentication has often been difficult to implement or presented a poor user experience. Today, user-friendly computing form factor that is always in our pocket can be achieved by leveraging mobile platforms for strong authentication. Mobile platforms offer us the ability to secure our digital identities in ways that are stronger than the other forms of second factor authentication, such as SMS tokens, previously mentioned.[13]

With mobile platforms, our digital identity can take the form of a cryptographic credential that never has to leave the device. Communication between backend systems and the mobile device

[10] Source: 2016 DBIR *"Veraizon Data Breach Investigation Report"*
[11] Aloul, Zahidi,El-Hajj (2009) *"Two Factor Authentication using Mobile Phones,"* in IEEE/ACS International Conference on Computer Systems and Applications, Vol. 6, pp. 641-644
[12] Ashraff, Chatta (2014), *"NFC – Vulnerbilities and defense"* Conference of information Assurance and Cyber Security (CIACS), pp. 35 -38
[13] Gripentog, Kim (2015), *"Utilizing NFC to secure Identification"*, IEEE International Conference of Identification and Security

can be encrypted and identity tokens do not have to be re-typed into user endpoints. These capabilities offer users a truly out-of-band multi-factor authentication.[14]

It should be noted that the usage of secure elements (SE) in mobile credentials is a way to offer a root of trust for devices to be able to secure their own digital identities. Encrypted communication, authentication and authorization between devices can become possible. Complex supply chains will also demand that device identities are secured throughout their lifecycle. Attackers should not be allowed to simply "become you" on your network because of a stolen credential. This is true whether we are considering traditional IT networks that run our enterprises, or device-centric operational technology networks that run our critical infrastructure. By taking advantage of credentials stored in a highly secure manner, the security of digital identities becomes possible.

With the push by many end-users to migrate their physical access control systems to the IT network in recent years has also come an increased demand for solutions that can streamline both physical and logical access in a way that is less burdensome on final users. The benefits of implementing such a solution are numerous. However, very few companies have come up with a viable enterprise solution that can function in both worlds effectively. And that will be focus or scope of my research of this thesis, the study of a framework that can integrate mobile-based technology for identification and access control purposes.

With the growing adoption of mobile access control for physical security applications, smart cards and smartphones used as credentials are converging into centralized identity and access management systems (IAM). Either of these form factors, or both, will be used to secure access not just to the door, but also to data and cloud applications, while providing a seamless user experience.[15]

[14] Nag, Dasgupta (2015). *"An Adaptive Approach Towards the Selection of Multi-Factor Authentication"* IEEE: Symposium Series, 463 – 472

[15] Dzurenda, Hajny, Zeman, Vrba (2015). *"Modern Physical Access Control Systems and Privacy Protection."* IEEE: Technology and application, 1 –5

Now that identification cards and mobile phones are starting to blend together for both physical and logical access, the convergence trend is accelerating even more quickly. With the latest solutions, the same card used to open a door can also have authentication capabilities for logical access control, it can be tapped to a laptop, tablet, phone or other NFC-enabled device to access data, cloud apps and web-based services. Plus, smartphones can be turned into a trusted credential that can be used to unlock doors and open gates. The same ID card that is used for these physical security applications can now also replace dedicated one-time password (OTP) solutions for permitting access to computers, data, applications and cloud-based services[16]. In other words, what previously was a single credential per user for opening doors might now be a half a dozen, or more, remotely provisioned credentials for both physical and logical access control.

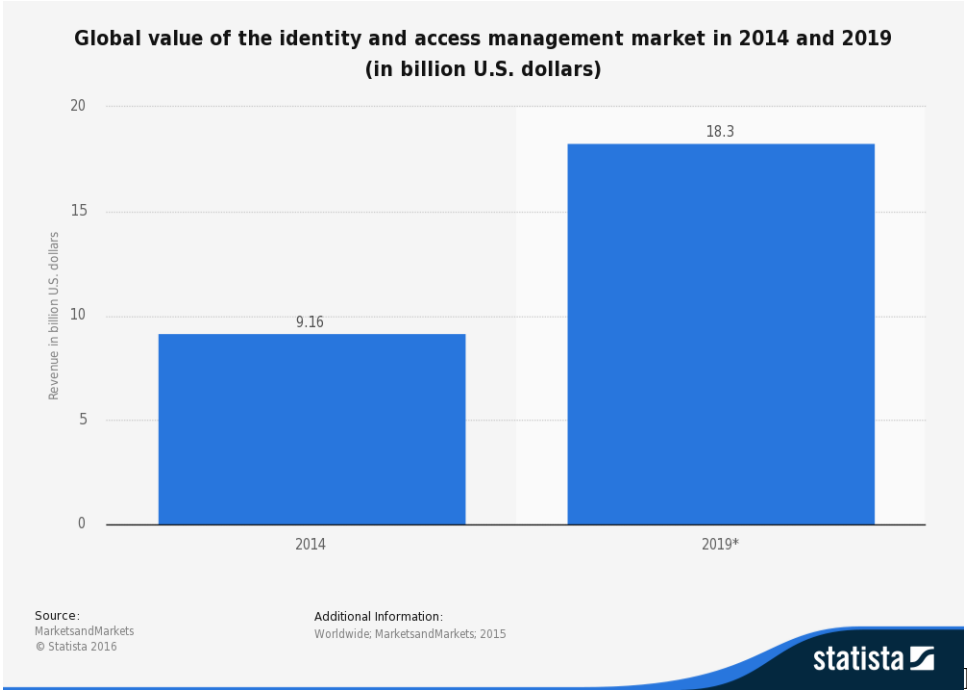

Figure No.2[17]

Cloud or off-premises hosted services, are vital for this technological transformation brought on by smartphones, as well as, for making the most out of the massive amounts of data that may be

[16] "Usher One, Usher All." *The Hoya*. January 7, 2015. Downloaded on January 5th, 2016 from http://www.thehoya.com/usher-one-usher/

[17] Source: MarketsandMarkets, published by: NBCUniversal, Februry 2015 from: http://www.statista.com/statistics/417602/global- market-forecast-identity-and-access-management/

produced by these devices. In addition to their specific functions, these connected devices act as perpetual research agents gathering useful information that can help users and administrators to enhance their capacities for action. With their plethora of sensors and personalized settings, smartphones are the wave of the future; they will change the habit of using physical keys, badges, tokes etc., and at the same time will improve mobility.

It's impossible to talk about mobile-based security and access control systems without mentioning data. Data is the backbone, we have to consider that data. Creating a data source or database it will be a must if we want mobile-based solution to be adopted. The identity and access management (IAM) receives and transmits information.

Physical security systems will store all information in the cloud[18]. With cloud-based access control, we can base credentials and privileges on people's identities and other attributes rather than a string of numbers found on a card. Those data sets will grow exponentially, meaning that custom security integrations are quickly becoming unfeasible. On-premise and proprietary systems simply can't handle the amount of data created by mobile-devices, systems, and people. The cloud is becoming a prerequisite of modern access control and physical security.

Physical access control start with one question: How do I lock my door?
There are a lot of ways to do this:

- Lock and key
- PIN pad
- Key card (magstripe, proximity, contactless smart cards, key fob, etc.)
- Biometrics

Being biometric the most ideal, there are a lot of reasons for this:

- A biometric factor can't be lost, stolen or borrowed
- A biometric factor can't be forgotten by a user, guessed by an intruder and does not need to be regularly reset
- Versatility and convenience

[18] Srividhya, Manikanthan (2015). *"An Android Based Secure Access Control Using ARM and Cloud Computing"* Electronics and Communication Systems (ICECS), 1486 – 1489

Biometric technology is playing an increasingly important role in the global access control market, which is on track to reach $10.4 billion by 2020. Driven by a need for increased security due to concerns of crime and terrorism, biometrics fit the bill when it comes to locking down critical areas.

8.1 Global Access Control Market Analysis

Growth rate 2016-2020	Market revenue by 2020
13% CAGR	**$10.4 Billion**

Table No.2[19]

Contactless Smart Card Market to See 30% CAGR to 2019, The growing need to diminish identity duplication and forgery cases has resulted in remarkable growth in the Global Contactless Smart Card Market, a new thesis from ReportsnReports.com found.

Growth rate 2015-2019	Market revenue in 2016
30% CAGR	**$1.7 Billion**

Table No.3[20]

The thesis covers the present scenario and the growth prospects of the global contactless smart card market for the period 2015-2019. To calculate the market size, the thesis considers revenue generated from the sales of contactless smart cards. The thesis also covers the global shipment details of contactless smart cards.

[19] Global Access Control Solutions Market 2016-2020, March 2016, from: http://www.reportsnreports.com/reports/514479-global-access-control-market-2016-2020.html

[20] PMR Persistence Market Research, June 2016, from: http://www.persistencemarketresearch.com/market-research/smart-cards-market.asp

According to the latest thesis, the number of fraud and forgery cases has increased as technology progresses. Contactless smart cards can provide a one-stop solution to the issue, as these cards are not easy to decode. Several government organizations are making contactless smart card technology mandatory for passports and driver's licenses, as it reduces the risk of data theft or identity duplication.

Furthermore, the latest thesis emphasizes the increased adoption of smart cards in developing countries, which is expected to support market growth. Government agencies in countries like India are increasingly adopting these cards for use as driver's licenses, e-passports, identity cards and voter ID.

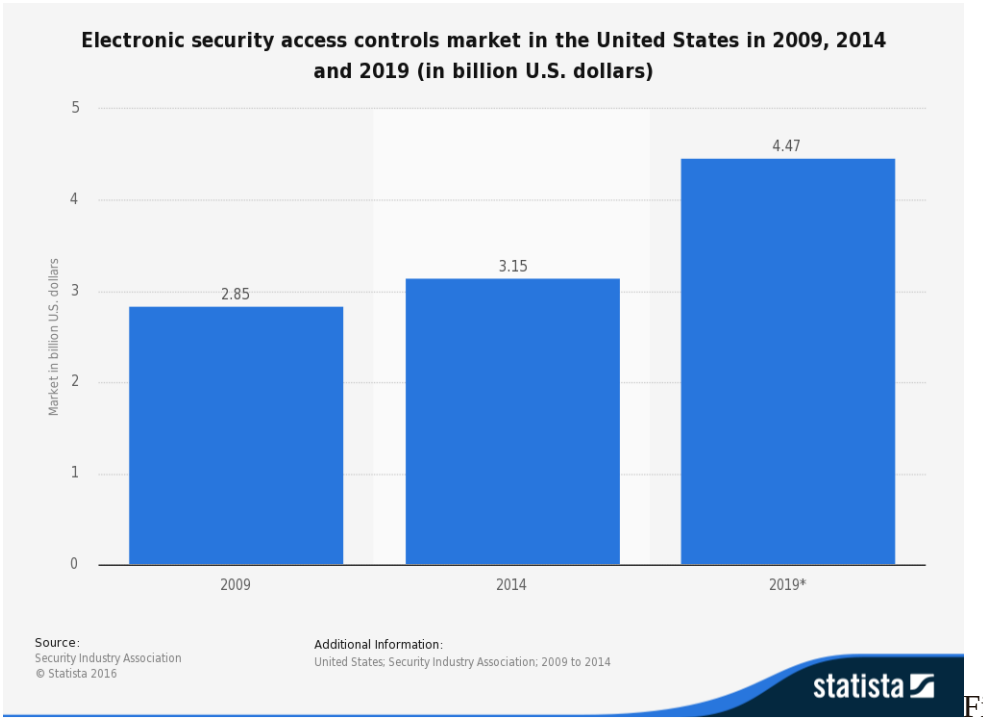

Figure No.3[21]

At the same time, new innovations in strong authentication and mobile devices have allowed for greater convenience in both implementing and using biometric security systems[22]. Of course, a balance therefore must be struck, providing an appropriate level of strong security while also

[21] Source: securityindustry.org, published by: Security Industry Association, October 2015 from:http://www.statista.com/statistics/477947/us-electronic- security-access-controls-market/

[22] Mastali, Agbinya (2010). *"Authentication of Subjects and Devices Using Biometrics and Identity Management Systems for Persuasive Mobile Computing: A Survey Paper"* IEEE, 1 – 6

meeting to a high demand in end-user convenience, allowing for governments, enterprises and even consumers to maintain a high level of efficiency while upgrading their security.

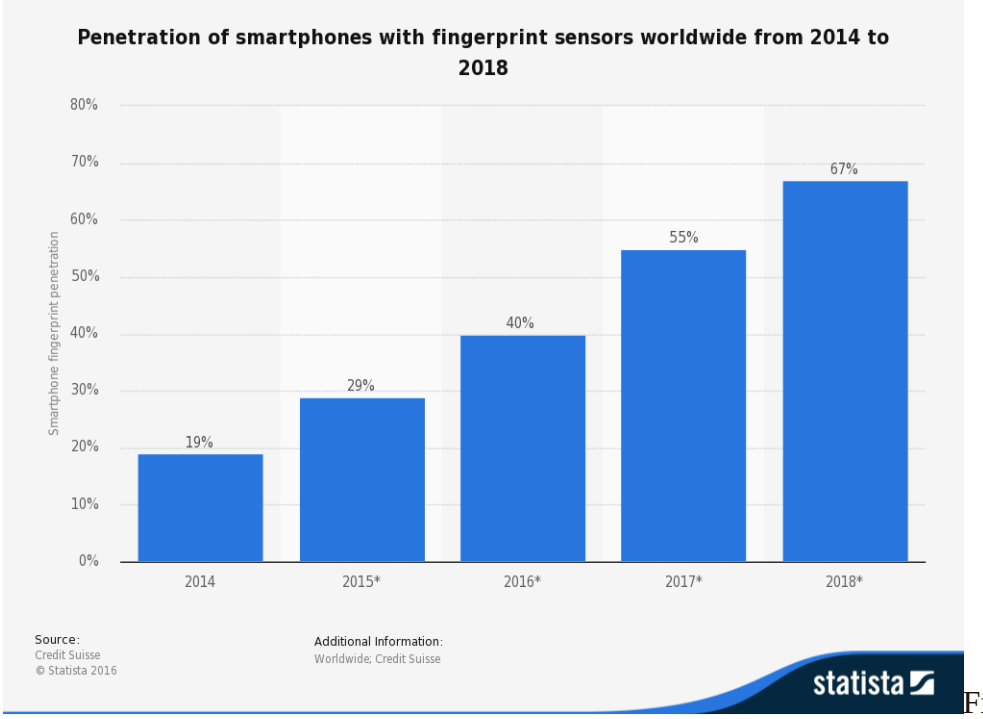

Figure No.4[23]

[23] Source: Credit Suisse , published by: Credit Suisse , January 2016 Website from:http://www.statista.com/statistics/522058/global- smartphone-fingerprint_penetration/

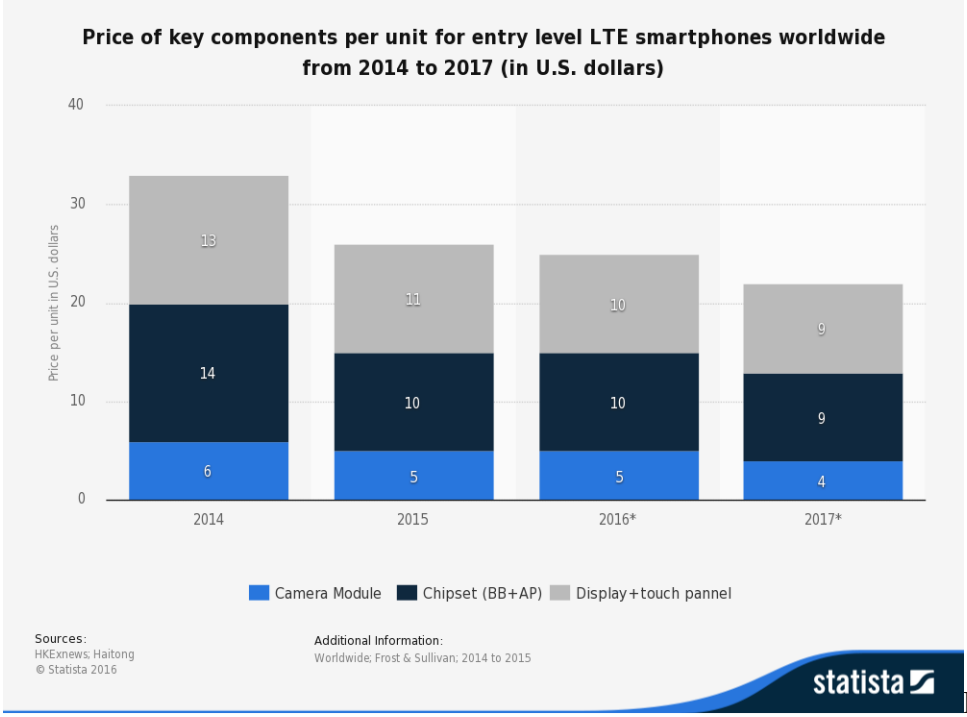

Figure No.5[24]

Biometric technology is at the heart of mobile access and identification management. When humans are constantly connected to the Internet, a biological identification trait is the best way to ensure that a user's digital identity is not abused or stolen.

Thanks to biometric applications, which can turn cameras and microphones into biometric sensors, any smartphone can be turned into a multi-factor strong authentication device. Now that fingerprint scanners are becoming standard flagship phone features too, and iris scanners are on the verge of mobile integration too[25], the options of using biological authentication factors for mobile transactions are vast. For example, anti-theft applications can take advantage of the biometric support in smartphones.

There are different biometric modalities such as vein pattern, palm geometry, behavioral etc. but given the plethora on sensors in smartphones today (microphone, cameras, GPS, etc.), the most convenient modalities are fingerprint, voice, Iris and facial recognition[26]. Mobile biometrics

[24] Source: Haitong, published by: HKExnews, June 2015 from:http://www.statista.com/statistics/484844/price-of-key- components-for-entry_level-lte-smartphones- worldwide/

[25] Counter (2016), *"The Samsung Galaxy Note7's Iris Biometrics"*, from MobileIdWolrd, source: http://mobileidworld.com/roundup-samsung-galaxy-note7-108080/

[26] Meng, Wong, Zhou (2015)"*Surveying the Development of Biometric User Authentication on Mobile Phones*" IEEE Communication surveys & tutorials, Vol. 17, No. 3

market is poised to explode. The trend indicates the cost of biometric capable sensors is going down.

Figure No.6[27]

Cloud technology, licensed through a service model, has enabled this evolving biometric ecosystem. Future proof technologies are allowing governments and enterprises to invest in mobile biometric technologies without the fear of being outdated by the time new biometric technology emerges.

> "Biometrics is a natural fit for the smart mobile devices we literally hold onto nearly every waking hour. The explosion in the use of smart devices over the past five years, along with anticipated growth over the next five -- especially in developing economies where sub $100 smart phones have begun to alter the mobile landscape -- will bring biometrics into the daily lives of half the global population. By 2020, 100% of smart mobile devices will include embedded biometric sensors as a standard feature"
>
> - C. Maxine Most Principal, Acuity Market Intelligence

[27] Source: Carnegie, published by: Carnegie, September 2015 from: http://www.statista.com/statistics/536702/asp-of- fingerprint-sensors/

Figure No.7[28]

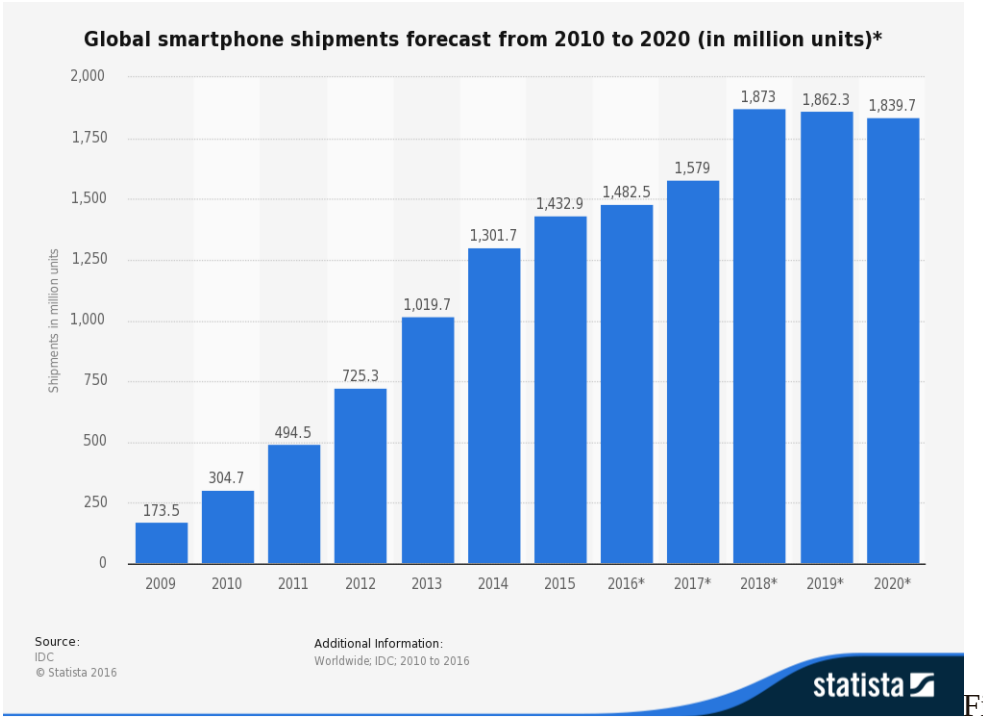

Figure No.8[29]

[28] Source: Haitong, published by: HKExnews, June 2015 URL:http://www.statista.com/statistics/484583/global-average-selling-price-smartphones/

[29] Source: IDC, published by: idc.com, June 2016 from: http://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/

If we analyze this two projection figures, it is clear that there is an inflection point in the trends, in the Figure No.7, we can appreciate the commoditization of the smartphone market where the prices are going down and in the Figure No.8, the continuous and stable increase in the smartphone shipments worldwide, this two factors plus the market penetration of built-in fingerprint capabilities in the smartphone market, will benefit adoption of mobile access control and identity management solution.

Analysis on NFC Wireless technology compatible with Physical Access Control Systems

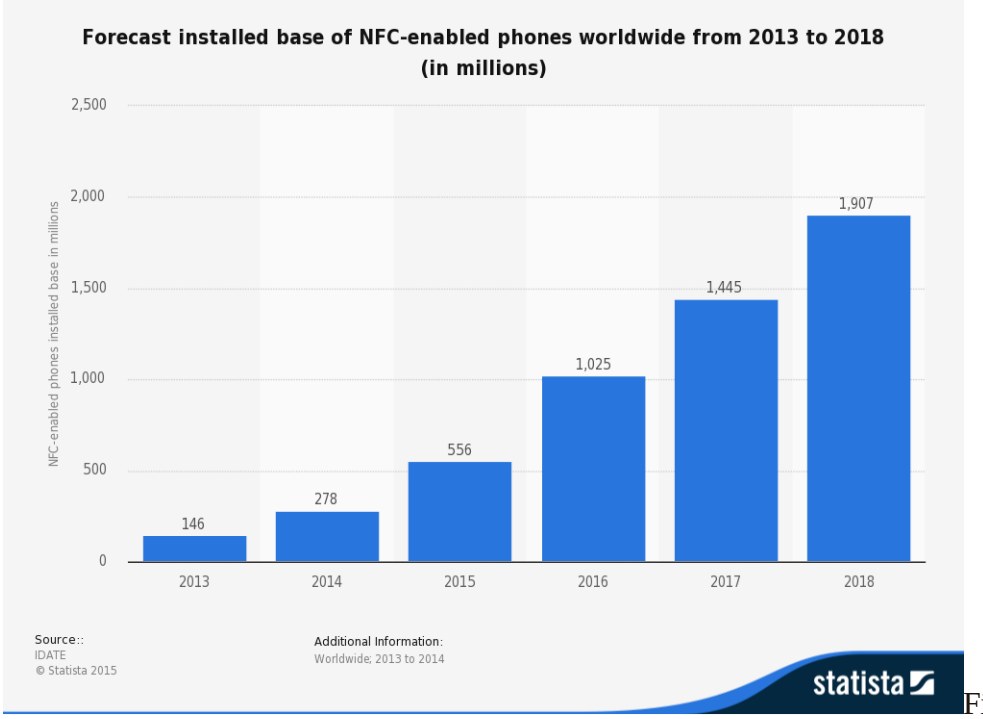

Figure No.9[30]

[30] Source: IDATE, published by: idate.com, June 2014 from:http://www.statista.com/statistics/347315/nfc-enabled-phone-installed-base/

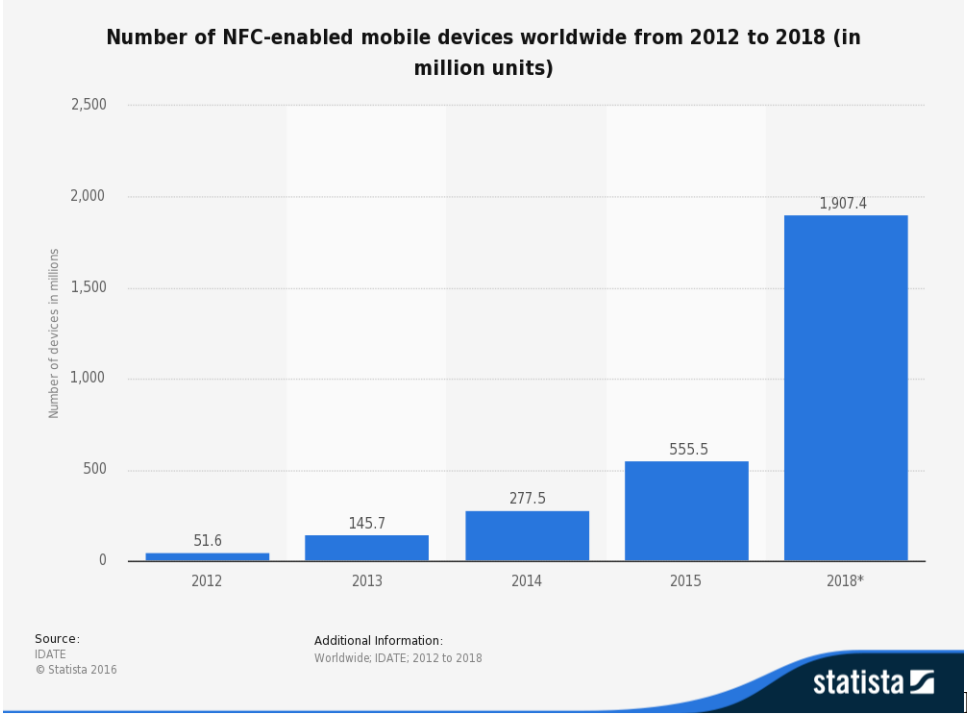

Figure No.10[31]

"*With 500 million NFC-- -enabled devices in the market, NFC is recognized as a key enabler of the connected world.*"

-NFC Forum, 2014

9 Relevance and justification

As usages of RFID become more advanced, standards became more sophisticated and more capable tags were developed. And of course the more advanced and sophisticated attacks and forgery techniques were discovered. But one simple fact still remains about the whole concept and motivation behind most of the attacks; their aim is to be able to forge and reproduce a tag data, in a form that it looks and processed as the genuine targeted tag. In some cases this attempt is as easy as rewriting a few bytes of data with known malicious values but in some other cases it means breaking into the logics of a microprocessor embedded in tags and finding flaws with advanced and heavy cryptography implementations.

[31] Source: IDATE, published by: idate.com, May 2015 from: http://www.statista.com/statistics/461494/nfc-enabled-mobile-devices-worldwide/

There are many standards and implementations of standards for RFID tags and smart cards. While many of them are based on the same few standards that are globally accepted and followed, there are always vendors and manufacturers that follow their proprietary approach to implement standards. The purpose of this is either to enhance the efficiency of their system, to make it more secure or even to define their own standard and push it to industries for competitive advantage. That is not an issue until we have to deal with compatibility of tags between different vendors produced for same standards, and of course security measures of the standard itself. In other words, just because one RFID standard has considered security in its definition and demanded manufactures to follow a certain implementation, does not necessarily means that all vendors' implementations based on that standard are secure. In fact, in many cases it has proven exactly the other way, where standards are considerably secure, but an implementation flaw and mistake makes it ineffective.

Having that in mind, there are many researchers out there that are focused on analyzing and evaluating these standards and implementations, and every now and then we see results and papers that demonstrating that a known trusted and secure brand or implementation is prone to catastrophic security failures and attacks. Considering the massive market and usage of RFID technology, each of these cases are affecting millions of end-users and businesses relying on a certain type of standard or implementation. Yet we are still seeing that many of industries and businesses are still developing their systems based on implementations that are known to have critical security issues, or even worse, not meant to be used for a case or scenario that demands security. Security in this context refers to need of protecting an asset, goods or even identity of people that are not meant to be accessible or exposed otherwise.

The physical access control market is ripe for an upgrade to modern technology; legacy physical access control systems predominantly use access badges with weak cryptography or no cryptography at all despite better building blocks being available. While strong cryptography is a necessary ingredient of a secure system, modern access control also demands continuous key/identity management and intrusion monitoring. These common security principles are virtually unknown where buildings and premises are protected. We would like for access control to become a prototype for good security reasoning built on open standards and best practice

security principles. Towards this goal, this thesis establishing security best practices in access control and provides the structure for comprehensive building access control. The design guidelines are provided as requirements such that they are directly usable in a request for proposal.

Security in an institutional environment like Universities is always a concern. According to the National Association of Campus Card Users of the roughly 231 schools they have on record 197 of them are using magstripe technology, and 62 have already moved to some form of contact-less technology[32].

Various methods have been employed over the years to meet the security needs of physical security. Some of the methods of security have included keys, badges, magstripe cards, smart cards, and currently the latest trend is NFC. Each of these methods has a role in security dependent on cost versus security.

The trend in Figures No.9 and No.10 shows how wireless near field communication (NFC) is the way of the future. This paper will focus on the deployment of NFC technology to make identification and access management (IAM) more robust and secure without affecting the end user. The motivation behind choosing NFC is based on identification needs as the industry switches to contact-less data transfer and the compatibility with existing RFID smartcard access control applications given that NFC uses the same carrier frequency of 13.56 MHz. However, as a result of switching to new identification standards, challenges such as choosing a system, cost, and administration of the system are hurdles to overcome.

Given that NFC is more accessible now than ever, new exciting areas of application can be explored. One such area is physical security and more specifically one of the main categories, secure authentication. Today there exists a myriad of different secure NFC smart cards that can be used as secure tokens in many different physical security applications. The problem is that the encryption on these smart cards is quite weak with varying degrees of security and is susceptible

[32] http://www.naccu.org,

to different attacks and exploits that have been published over the years[33]. These weaknesses will not do for more sensitive systems such as high security entry systems or data exchange systems. This thesis will focus on secure authentication and explore the benefits of using a NFC enabled mobile device as a secure token in an access control system as opposed to using a NFC smart cards.

10 General objectives

The main objective of the thesis is to evaluate different Near Field Communication (NFC) technologies, mobile devices and cryptographic authentication protocols and see, which best suits the needs of a proposed mobile-based access control system based in open standards. The open source authentication selection should meet the following requirements and design considerations based in the highest security standards and best practices[34][35]:

- ***The lock should utilize the highest available encryption standards***. Effectively making all cryptographic attacks nearly impossible or take an unforeseeable amount of time to break.
- ***The authentication process should be as fast as possible*** **low latency**. Requiring the user to hold the device at the reader for as short a time as possible. A long authentication time is tedious for the user.
- ***The authentication process requires as little user interaction as possible***. The user should not have to interact with applications on the device.
- ***The lock should not require Internet access***. Not being able to access the locked door if the Internet connection is down is not acceptable.
- ***The lock application should work on as many devices as possible***. The system should have as large a user base as possible.

[33] Garcia, Rossum, Verdult, Schreur (2009). "*Wirelessly pickpocketing a Mifare Classic card*", In *Security and Privacy, 2009 30th IEEE Symposium on.* Berkeley: IEEE.
[34] Security Industry Association, (2013)"*PACS Best Practices using PKI-Authentication*", from: http://www.securityindustry.org
[35] Roh , Noh , Plöt , (2009) *"Access Control Best Practice"* from: https://srlabs.de

The research will be performed within the time frame of a Master thesis project. This means that a proof-of-concept implementation will not be part of the scope of the thesis. One of the problem that this thesis answer, is lack of single resourceful material that covers wide range of security aspects of RFID and mobile technology in physical access control (PACS), known security issues about it and common attacks that threat various applications. While there are few similar resources available for this purpose that focuses on security, none of them found to have a balanced combination of wide coverage of domains and level of technical details that can be easily followed by consumers with moderate or low level of knowledge about RFID technology.

There are approximately 180 papers on RFID/NFC security from IEEE.org and some of them are discussed in this paper, including a categorization of how scholars have proposed addressing related security issues. The general security problems with NFC can be classified in three categories: Field extension attacks, Man-in-The-Middle attacks (MiTM), and cryptographic attacks, all these categories were analyzed in this research.

This thesis tries to combine and compare various resources and previous publications as well as case studies in related domain into a single resource, so that readers can start with it to gain a basic understanding about the subject, and if interested or necessary, also be able to follow the subject in more advanced and technical details in other resources that are referenced. Since it is necessary to understand the RFID technology and its fundamentals before going through security issues in Physical Access Control (PACS), readers are first walked through basics of radio frequency identification (RFID) technology and are introduced to relevant key protocols and standards. Followed by that, taxonomy of RFID security issues is reviewed, by classifying known attacks in different categories based on the layers and components of the RFID technology they affect in physical security implementations. For every introduced attack few external resources both from previous academic works, Followed by a review in how these attacks are related to security principles they affect and finally discuss what guidelines and best practices are available in hand to improve the security of an RFID systems in an organization.

This research describes the current state of the most frequent technologies in the field of physical access control and a consideration of the practicalities of a broad adoption of mobile access control and the likely impacts for business and organizations.

This thesis will familiarize readers with all of the publicly documented and known security issues of RFID technology applied to physical security, so that they can get a sense about the security state of their systems. Without getting involved with too much technical details about every attack vector, or going throw tens of different books and papers, readers can use this thesis as a comprehensive reference to educate themselves about all known attacks against RFID, published to the date of writing this paper.

11 Academic Review

A note on terminology: This study distinguishes between several concepts that are not always clearly separated in the literature on access control system:

A **reader** is a device to read and write RFID cards. Depending on the system, a reader has a medium amount of firmware complexity and may be able to make access decisions on its own, which leads to security problems if the reader is positioned outside of the protected area.

A **transponder** is a simple device, sometimes referred to as "active antenna" that communicates with cards with a minimal amount of firmware complexity and no security functionality. The transponder converts data between radio channel and wired communication channel.

A **controller**, sometimes also called "door controller", is placed inside the protected area and is connected to one or more readers or transceivers and one or more doors. It hosts all the security functionality and makes access decisions, potentially in cooperation with a backend system.

The **backend** system is a centralized place that hosts all data regarding access permissions and may be consulted by online controllers/readers.

A **smart card** is a pocket-sized card, made of plastic, which is embedded with integrated circuits or microchips. It is used for authentication, identification, data storage, and application processing.

11.1 Radio Frequency Identification (RFID) Background

Since the era of early and traditional barcode systems, we have always been in seek of faster, more efficient and more reliable solutions and methods to be able to track our goods and items, monitor our supply chains and stores, control buildings accesses and many more similar applications.

During Second World War (WWII) an invention named Identification Friend or Foe (IFF) started a new era in this field and is considered the root of active RFID systems[36]. IFF was a system to identify friendly or enemy airplanes by use of an automated query and response system via radio frequencies, where friendly airplanes would actively respond to received RADAR signals from ground stations with radio frequencies to identify them.

RFID systems in very simple words are a pair of transponders talking to each other over specific radio frequency bands, one preforming the role of a fixed device known as the reader, and the other work as the mobile/portable device known as the tag. The tag has some information coded into it in form of bits and bytes, strings of letters and numbers that are presented and interpreted by the reader to identify the tag.

After few decades since its invention, modern RFID tags are now completely different in form of size and their work logics. Nowadays they can be as small as a rice grain and have their own built-in microchip and memory elements, following the same drastic advancements flow of wireless infrastructures and low cost embedded computers.

With a world market estimated to worth about US$10.1 billion in 2015 IDTechEx[37] find that in 2015, the total RFID market is up from $9.5 billion in 2014 and $8.8 billion in 2013. It is not hard to ignore this pervasive technology and numerous applications it has been adopted for. RFID has improved our commerce by integration into payment systems, asset management, inventory systems, access controls and social media. It has enhanced transportation and logistics, public transports, transport payments, animal/human identification and tracking, passports, and our institutions such as hospitals, libraries or museums. As one might think, each of mentioned applications have their specific requirements. In some cases low cost of mass deployment is the main factor, and in some other security or privacy of protected assets or information and transactions are of our concern. Either way, RFID has been adopted and developed to address all of these applications by different vendors and standards and in many form factors and functionality domains. In following sections of the thesis, we will briefly review specifications of RFID systems and different types of tags, radio frequencies and standards they use.

[36] M. Rieback, 2006. "*The evolution of RFID security*," *IEEE*. pp. 66–69
[37] http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2016-2026-000451.asp

In order for the reader and the tag to be able to talk to each other both of them should operate at exact same radio frequency. Also since tags are low cost and very low power consumption devices, they cannot emit strong radio signals, thus they should be in close proximity with the reader so that the reader is able to receive their signals. Close distance in this context refers to distances from few millimeters up to about 15 centimeters. Operation only at close proximity is not only due to technical limitations. In many cases it is an intentional behavior that is intended to provide additional security by limiting the distance that a tag can be probed. Access control types of tags are also known as Remote-Coupling Systems.

Remote coupled systems are based upon an inductive (magnetic) coupling between reader and tag, therefore also known as inductive radio systems.[38] According to Klaus (2003), at least 90% of all RFID systems currently sold are among inductively coupled systems. Many of typical RFID standards like ISO15693 (contactless proximity cards) and ISO14443 (contactless smart cards) that we are usually dealing with fit into this category, which are operating at 125KHz and 13.56MHz frequencies respectively.

Contactless access control based on Radio Frequency Identification (RFID) has replaced earlier technologies such as magnetic swipe cards in almost all security applications. Two generations of RFID access cards exist: an earlier generation or proximity cards using low frequency (LF) 125khz spectrum, including Legic Prime and NXP Mifare Classic, etc. which only use basic proprietary security mechanisms, and a modern generation or contactless smart cards that leverages advances in CMOS and smart card technology to implement state-of-the-art cryptography within the resource limitations of contactless cards in high frequency (HF) 13.56Mhz spectrum. The earlier generation of RFID cards is omnipresent in access control but easy to clone, while the newer cards with more appropriate security enter the market only slowly. This study outlines the requirements for a modern access control scheme and consequently requires the use of strongly encryption mechanisms possible only with the second generation that matches 13.56Mhz spectrum.

Smart cards are classified into two types: contact-based and contactless. Contactless smart cards are embedded with integrated circuits that process and store data and communicate with a reader via Radio Frequencies Identification (RFID). Employing a radio frequency between the card and

[38] F. Klaus, *RFID handbook*. WILEY, 2003.

the reader that needs no physical insertion of the card uses these cards. Before outlining the proposed design, the next sections discuss attacks on currently used proximity card technologies to motivate the need for more secure systems.

11.2 Near Field Communications (NFC)

NFC is an umbrella term for wireless communication technologies operating in the unregulated 13.56 MHz spectrum at a range of up to 10 cm. It differs from other wireless communication technologies in that it uses inductive coupling instead of radio waves to communicate wirelessly between two devices. An NFC device manipulates the electromagnetic fields in such a way that it can transmit binary data at a very short distance. This inductive coupling makes it possible for a NFC reader to power a low power NFC tag or smart card, thus eliminating the need to have a power source on the NFC tag or smart card. NFC traces its roots back to RFID technology, sharing many of its characteristics. (Coskun and Ozdenizci, 2012)

The year 2004 was an eventful year for the RFID technology Near Field Communication (hereafter NFC). The Finnish mobile giant Nokia developed the first mobile phone equipped with NFC and came together with Samsung and Philips to start the NFC forum. (Fine, Klym, Tavshikar, & Trossen, 2006) (Vanderkay, 2004) (Coskun and Ozdenizci, 2012) The same year, ABI research predicted that 50 percent of mobile phones would be NFC equipped by 2009. (Swedberg, 2004) However, Nokia is now a former shell of what it once was, and NFC has taken longer time than predicted to reach the general public. The reasons for the slow adoption rate are many, but one major problem has been the lack of infrastructure to support NFC where where Bianchin and Nathanson argue that the key for success depends on collaboration between mobile device manufactures, mobile network operators and payment companies (e.g. Visa and MasterCard) among others. (Bianchin, Nathanson, 2008)

Now, the adoption rate start to increase and the NFC technology is starting to be incorporated into everything from bus-fare token systems, concert tickets, secure login applications and much more. (Coskun and Ozdenizci, 2012) One can also argue that the launch of the iPhone 6 and Apple Pay in 2014 marked the year that every major mobile device manufacturer incorporated NFC technology in their product lines. So despite a slow adoption rate, NFC has yet again started to

gain traction; "*With 500 million NFC enabled devices in the market, NFC is recognized as a key enabler of the connected world.*" (NFC Forum, 2016).

As mentioned above, NFC can be used in countless number of applications. For a better understanding of the different application areas where an NFC enabled mobile devices is used, these areas are usually divided into four main categories (Haselsteiner, Breitfuß, 2006) For the purpose of this paper the fourth category will be the focus of the research:

- **Contactless Token** - Grab information from NFC tags that can be attached to anything from movie posters to grocery store specials. Much like an evolved form of barcode.
- **Ticketing/Micropayments** - Used in ticketing systems to validate a purchased ticket or make payments in retail stores by swiping a NFC card or device over a NFC reader.
- **Device Pairing** - This is where NFC is used to pair two devices together and hand over further communication using a higher bandwidth/longer range communication interface i.e. Wi-Fi or Bluetooth.
- **Secure Authentication** - Makes it possible for two NFC enabled devices to establish a secure communication channel between each other. This can be used to grant access to users in a secure access control systems or when login onto a computer terminal.

11.3 RFID versus NFC

Near Field Communication (NFC) is a newer definition for wireless communication technology that operates at 13.56 MHz frequency and is highly compatible with RFID technology, in in many cases even based and fully compatible with same ISO standards as discussed in this chapter of this thesis, namely ISO/IEC 14443 and ISO/IEC 15693. NFC can be used to transmit data between two devices with a range up to 10 cm and have different operational modes, which allows the NFC device to preform both as a read/write transponder and also simulated transponders, for example simulating an RFID tag and to perform a peer-to-peer data transfer between two NFC enabled devices. In short, we can mention the major difference between RFID and NFC to be the ability to have two-way communication between NFC devices, while in RFID roles of reader device and tags cannot be changed.

Since NFC modules are usually integrated into another device, a mobile phone for example, there is a host interface available in the module that allows communication with the host device. In typical scenarios where security is not a concern, such as transferring files or reading a smart label, data can be transferred and handled through the host controller and by the device. In security and safety sensitive NFC applications such as payments via NFC or NFC enabled ticket systems, host device is not considered secure and safe enough for storage of such sensitive information. Memory of a mobile phone for example might be subject of unauthorized malicious access, or unintentional modification or deletion of data. To prevent this, there is a different design approach called Secure-NFC where a secondary and protected and secure element (SE) is considered for storage of sensitive data or NFC applications. This storage can be integrated into NFC module as a chip, can be the phone SIM card running java applets, or certain external storage memories like secure SD cards which have built-in smartcard chip.

Lets have a closer look at the existing types of electronic access control systems that employ a wireless interface. There exists quite a few different wireless access control systems and they can be divided into two main categories. A token-based access control system, which uses a NFC smart card or tag as a key, is the first category. The second emerging category in recent years is sometimes referred to as Smart locks, here the user can unlock the door by using a mobile device.

11.4 Existing Physical Access Control Systems (PACS)

Token based Access Control Systems

The first category is those systems that use a physical token, like a smart card or tag to authenticate the user. These systems have been around for quite some time and are commonplace at office buildings, hotels and larger residential building. The most basic of these systems stores the tag ID number in a database and when the user presents its tag to the reader, the ID is read and the access if granted if the ID is valid. This is not very secure, as a malicious attacker can eavesdrop on the ID and program that ID into a new tag. These systems can be made secure using the newer versions of smart cards for instance MIFARE DESFire range of cards. These cards are what you might call “smart” as they have a microprocessor and a couple of Kbytes of storage space, where they can store one or more private keys. They use an AES pre shared key cryptographic scheme

to authenticate the card. These locks are what one might consider outdated, as they require a physical token.

Smart Locks

Smart locks are a new class of access control systems that have emerged in the last couple of years. Many of the major lock manufacturers have started to focus its R&D to develop these types of system, among them manufacturers like ASSA ABLOY and Yale. The smart locks typically use the short-to-medium length wireless technologies Bluetooth or Wi-Fi, to communicate with a mobile device, which holds the key. They usual employ one of the authentication schemes presented in this chapter; most common is the PKI scheme, which authenticates the user through an online certificate authority. These Smart locks are feature rich with advanced supervision that sends a message to the owner if it detects abnormalities. Other features include time-restricted access or granting access instantaneously even tough the owner is miles away. The popularity of these type of locks will probably increase in the near future as more and more people, see the convenience they and plethora of features they bring. At the time of writing none of these new generation smart locks employ NFC as communication medium. Using NFC is not only a very fast and reliable, but inherently safer option to use as the usage distance is very limited.

11.5 Standards and Protocols

NFC is comprised of several standards and communication protocols defined by the ISO and ECMA organizations, the two major ones being ISO-14443 and ISO-18092, which are in part compatible with each other. On top of this there are several proprietary implementations like MIFARE developed by NXP and FeliCa developed by Sony. (ISO/IEC, 2008) (ISO/IEC, 2013)

The NFC standard specifies two modes of operation and three different transfer speeds for the radio interface. An NFC device could either be active, meaning that it generates its own field or passive meaning that it relies on another device to generate a field and use load (NFC Forum, 2016). The Communication speeds are divided into two groups, one low speed and one high speed. The low speed communication is done at a rate of 106 kbps and the high speed is either 212 or 424 kbps. (ISO/IEC, 2013)

In the case of passive communication, only one device generates a carrier frequency, and all other devices uses load modulation to send data. Load modulation works by shifting the signaling level of the carrier, which is done by grounding the radio circuit thus lowering the signal level. Using this modulation scheme ones and zeros can be transmitted passively on the carrier wave. In the passive communication mode RF power is always on when communicating with targets. (ISO/IEC, 2013)

In the active case, NFC works like most other wireless technologies, only keeping RF power on while actively communicating. And shall always, before turning it back on, perform RF collision avoidance. (ISO/IEC, 2013)

ISO 14443

The ISO 14443 standard defines the physical characteristics and transmission protocols for contactless proximity identification cards. The standard consist of four parts, each specifying a layer in the protocol stack, from the physical characteristics of the air interface to the initialization and transmission protocols.

1. ISO/IEC 14443-1:2008 Part 1: Physical characteristics (ISO/IEC, 2008)
2. ISO/IEC 14443-2:2010 Part 2: Radio frequency power and signal interface (ISO/IEC, 2010)
3. ISO/IEC 14443-3:2011 Part 3: Initialization and anti-collision (ISO/IEC, 2011)
4. ISO/IEC 14443-4:2008 Part 4: Transmission protocol (ISO/IEC, 2008)

The details of these protocols are out of scope for this project, as it will focus more on the higher-level communication protocols.

MIFARE

Is a proprietary implementation of the ISO 14443 standard developed by NXP, one of the biggest manufacturers of NFC smart cards. It includes varied selection of NFC smart cards (Classic, Ultralight, DESFire) that has a wide range of applications. (Coskun and Ozdenizci, 2012) The MIFARE smart card extends the functionality of ISO 14443 by adding security. MIFARE features different kinds of advanced cryptographic methods, from the basic Single DES through triple DES up to AES. Only the most advanced MIFARE smart cards have the ability to authenticate via AES authentication, a very secure pre shared key (PSK) authentication method that belongs to the symmetric key class of cryptographic ciphers. (MIFARE, 2016)

FeliCa

Is a proprietary radio frequency identification (RFID) contactless smart card system developed by Sony. It currently meets the ISO 18092 standard, which is also known as Near Field Communication, FeliCa system has achieved ISO/IEC 15408 EAL4/EAL4+ security level. The encryption key is dynamically generated each time mutual authentication is performed, preventing fraud such as impersonation[39]. On Sept 7, 2016, Apple announced Apple Pay now features FeliCa technology. iPhone 7 and Apple Watch Series 2 users can now add and tokenize
their FeliCa cards into their Apple Pay wallets and tap their phones just like regular FeliCa cards.[40]

11.6 NFC Modes of Operation

Reader/Writer mode is the most basic form of communication, used to read from or write to a NFC tag or NFC smart card. This is used in smart posters or tollbooths ticketing system. This is supported by the ISO 14443 standard and in extension the Mifare and FeliCa standards. (Coskun and Ozdenizci, 2012)

Peer-to-peer mode In peer-to-peer mode, two NFC devices can share data between them. This could be anything from digital business cards to setup parameters for Bluetooth communication. (Coskun and Ozdenizci, 2012)

Host Card Emulation (HCE) Card emulation is a further development of the reader/writer mode, allowing a NFC enabled mobile device to emulate a NFC smart card. The external reader will not notice any difference. This enables the NFC device to be used in contactless payment or ticketing systems without needing to change the existing infrastructure. The card emulation mode is a very versatile communication mode, but one drawback is that it requires a secure element to function. A secure element is a closed encrypted chip located outside of the operating system usually on the SIM-card supplied by the network operators. All traffic being sent and received over the NFC channel in card emulation mode will be routed via the secure element that handles

[39] Overview of FeliCa: http://www.sony.net/Products/felica/business/tech-support/index.html
[40] http://www.apple.com/jp/apple-pay/getting-started/

encryption/decryption and authentication. Access to this secure element is very restricted and only available to the network operators or banking system vendors. (Coskun and Ozdenizci, 2012)

11.7 NFC and Mobile Operating Systems (OS)

The implementation of a secure access control system relies heavily on the mobile phone operating system and their support of NFC and the different reader modes. In this section we will have a closer look at the three major operating systems for mobile devices and their support of NFC and the different modes of communication.

Android

Android has long been supporting NFC ever since version 2.3 (Gingerbread) of the operating system. Combine that with the plethora of available Android smart phones that incorporate NFC and Android is a cutting edge operating system for NFC development. Android supports all three operating modes, reader/writer, peer-to-peer, card emulation (HCE).

- An Android device can be used as a NFC reader/writer when running the phone in the reader/writer operating mode. This is used for reading/writing to/from NFC tags and other NFC smart cards.
- Peer-to-peer mode on Android is called Android Beam, and is used for sending NFC data exchange format (NDEF) messages between two NFC devices. This communication is one directional, only passes a single NDEF messages per session before disconnecting the NFC channel. Usually used for sending small messages or other information in a neat and presentable manner.
- The host card emulation mode (CE) is, as stated previously, a very versatile communication mode with the drawback of requiring a secure element. But as of Android 4.4 (Kitkat), a new type of card emulation was added Host card Emulation (HCE), which enables an Android device to operate as a NFC smart card without the need of a secure element (SE). This enables third party developers to start utilizing the potential of card emulation for advanced NFC applications.

Apple iOS

Apple has included support for NFC in its latest iPhone models, iPhone 7 and iPhone 7 Plus. Unfortunately the NFC API is closed to third party developers and thus no NFC applications can be developed for iOS. Although this might change as Apple has done the same with new

technology in the past, where they later decide to release an Advanced Programing Interface (API) to developers.

Windows phone

Windows phone has two types of NFC operating modes, Wallet platform and Proximity platform. The Wallet platform is a card emulation mode, which enables the device to mimic a NFC card using secure element. This platform is used, as the name implies, for contactless payments. (Microsoft, 2015)

The proximity platform is an implementation of the NFC peer-to-peer mode, used for sending messages and picture between two NFC devices. (Microsoft, 2015)

11.8 Mobile Credential Benefits

The benefits of using a mobile device as a secure token can be summed up in the following statements (Ahson & (eds), 2012):

- **Convenience** – Request Access to the doors at your facility with a touch of your phone. Mobile Credentials are iOS and Android compatible and allows authorized users access to designated doors. A user can be remotely granted access to a system through an application on the device. By sending the access credentials through a secure channel over the Internet, the user can then have instantaneous access without having to acquire a physical token. A mobile device has far more processing power, which means more computation intensive encryption schemes can be used.
- **Increased security** - If a phone goes missing, the phone owner usually notices right away, unlike a card or fob that could go unnoticed or unreported for days. Phones are also less likely to be shared. Using a smartphone as a credential provides a layer of increased security by allowing users in a corporate setting to capitalize on their corporate mobile device policies to require authenticated device unlock by pin, gesture or biometric, effectively adding multi-factor authentication to Mobile Credential. It can be used in conjunction with other security features on the mobile device such as PIN or biometric lock.

- **Consistent credential management** – If a phone is lost or an employee is terminated the credential can be immediately and easily deactivated to prevent unauthorized access.

- **Log of events** – data collection for audit trails
- **Replace traditional forms of identity:** Plastic IDs, keys, or passwords are converted into mobile identity that contains all credentials on a person's smartphone, electronic keys can be transfers safely and for businesses will be a universal and transparent way to assign and revoke credentials. A user does not have to carry around several cards or tokens for all the different systems it needs to access, everything can be stored on one device. With other words, several authentication systems, one device.
- **Ensure user identity:** Mobile Identity can be biometrically linked to its owner, ensuring that only the true owner can activate their mobile identity and use it.

- **Use mobile identity in every business process:** lets individuals use their mobile phones to validate identity, log on to applications or computer workstations, open entryways and doors, and authorize transactions.

This subject matter will be explored in detail in this paper, finding out what level of security one could expect from a mobile device based authentication system. Different NFC modes of communication will be discussed as well as cryptographic authentication protocols that can be used over a NFC communication channel.

11.9 Authentication and Cryptography

11.9.1 Introduction to Authentication

To authenticate that a client or server is who they really claim to be, is no easy task. So how would one go about doing this authentication? All types of human authentication can be divided into three categories (FFIEC, 2001):

- The user ***is*** something (biometrics, fingerprint, voice, etc.)
- The user ***has*** something (token, ID card, smart card)
- The user ***knows*** something (Password, PIN, etc.)

All three can be used in an electronic access control system. They can also be combined for increased security, commonly referred to as two-factor authentication. (FFIEC, 2001) In this paper the focus will be on the last paragraph, that the user knows something, like a password.

11.9.2 Authentication Protocols

There are a many number of authentication protocols that can be used in an access control system, here is a closer look at the most widely used protocols. Only access control platforms based on open standards will enable the move to mobile access, converged solutions, and web-based credential provisioning that will improve customer convenience.

Public Key Infrastructure (PKI)

Public key cryptography is a widely used cryptographic scheme used on the Internet. It enables a user to establish a secure communication channel to a server over an insecure public network. It relies on the use of asymmetric keys and a certificate authority to establish a secure channel where the user can pass its credentials to authenticate. The asymmetric keys are made up of one public key that is used by anyone who wish to encrypt or sign a message and send to the server and a private key that is kept secret and used to decrypt a message or verify a signature. (Delfs Knebl, 2007)

Secure Shell (SSH)

SSH authentication is used to establish a secure connection between client and server, the client can then pass on user credentials over this secure connection to authenticate against the server. SSH can use either public key authentication or password authentication.

In the SSH public key authentication scheme the user have to generate a public/private key pair. The private key is kept hidden by the user while the public key is stored on the server. It has some vulnerabilities, which is the private key stored on the client side, which could be compromised or stolen and use by an attacker to gain access to the server. (Ylonen, 2006)

SSH password authentication is the second option when using SSH authentication. It establishes an encrypted channel and then sends the plaintext password to the server for authentication. The first time a user connects to the server, it will receive the server's public host key. This key is not

signed and is tied to the hostname or IP address of the server. If the server gets a new IP address the host key changes, and need to be sent to the clients again. This will display a warning on the client side, warning about the changed host key and that there might be a risk for a MiTM attack. (Ylonen, 2006)

Kerberos

Kerberos is commonly used in enterprise class systems to securely communicate between nodes on an unsecure network. It operates on a client/server model and requires an external Kerberos authentication server. When a client logs on to the network it first has to authenticate against an authentication server that issues a time stamped ticket, which it encrypts with the clients password and sent back to the client. When the client wants to securely access a service on the network it will send its ticket to a ticket-granting service, which will check if the ticket is valid and that the client has the correct privileges to access the requested service. If the request is granted the ticket-granting service will return a ticket along with a session key. The client can then send this ticket and session key to the service it wants to access. (Ylonen, 2006) (Cisco, 2006)[41]

Pre Shared Key (PSK)

Pre shared key authentication is a pretty simple yet very secure form of authentication protocol. It relies on a symmetric encryption scheme, i.e. encryption/decryption is performed using the same key. It uses this pre-shared key to encrypt a message containing a user's credentials together with some random elements, which it sends to the server. The server, using the same key, decrypts the received message. The server then generates its own random elements and concatenates that with the message received from the user and sends it back. This gives a mutual authentication between user and server. There are many different types of encryption schemes that can be used in PSK authentication DES, BlowFish and AES are some of the more notable. Where AES is the de facto standard for secure encryption today, and key length range from 128-bits to 256-bits. AES encryption is regarded as far the most secure encryption scheme, with no known attacks that are computationally feasible. (Delfs Knebl, 2007)

[41] Cisco. (2006, January 19). "*Kerberos Overview I An Authentication Service for Open Network Systems"*. Retrieved 2015, from Cisco.com: http://www.cisco.com/c/en/us/support/docs/securityZvpn/kerberos/16087Z1.html

Password-Authenticated Key Agreement (PAKE)

This is a group of authentication methods that lets two or more parties establish a cryptographic key using an exchange of messages. This method is based only on their knowledge of a shared password and an eavesdropper cannot gain any valuable information while engaging in the message exchange and is constrained as much as possible from brute force guessing the password. There are two main categories of Password-authenticated key agreement, Balanced PAKE and Augmented PAKE. In the Balanced PAKE a client and sever can negotiate and authenticate a shared key using the knowledge of a shared password. The Augmented PAKE works in a similar fashion as the balanced version but improves on the balanced version, as it does not need to store the password-equivalent data on the server, instead it only requires a password verifier to be stored. This makes the system more robust even if the server is compromised and the verifier data is stolen. It cannot be directly used by the attacker without first performing a brute force search for the password. The most interesting implementation of an Augmented PAKE cryptographic system is the Secure Remote Password authentication protocol. (Wu, 1998)

Secure Remote Password (SRP)

SRP belong to the Augmented PAKE family of password authentication protocols and was created by Thomas Wu, Stanford University in 1996. When authentication is performed using the SRP protocol, the client never reveals the actual password to the server. Instead the client proves the knowledge of the password through an ingenious protocol exchange. The server only stores a password verifier and not the actual user password; a verifier is like a one-way hash of the password. This makes the password reasonably secure even if the server is compromised and a malicious attacker get access to the verifier; it has to be found by brute force. The exchange between client and server is also protected from eavesdroppers by no useful information is actually transmitted. (Wu, 1998)

The SRP protocol is a mutual authentication protocol. In the original version of the SRP protocol there was six rounds of information exchange between client and server. This has been revised in later revisions to only require three rounds of exchange, by changing the order in which certain parameters are calculated and grouping them together. If not mutual authentication is required, i.e. only the user proves that it knows the password, then it can be reduced further in half, witch is the

case for access control system PACS, It shares a lot of similarities with Diffie-Hellman asymmetric key cryptography. SRP is a hybrid between pre shared key and asymmetric key cryptography. The key need so be shared between the authenticating parties ahead of time. But the actual authentication uses a Diffie-Hellman style key exchange. (Wu, 1998)

11.9.3 Cryptographic Basics

To understand the contents of the next chapters it is good to have some basic knowledge about cryptography. This section will briefly explain some core concepts in cryptography that are good to know when reading further.

Symmetric cryptography

This is the classic definition of encryption, where two parties share a common secret key. When one party wants to send a secret message to the other party it uses the common secret key to encrypt the message, which can later be decrypted by the other party when it is received. (Delfs Knebl, 2007)

Asymmetric cryptography

Public key algorithms are based on hard to solve mathematical problems that have no known efficient solutions. One such mathematical problem is prime number factorization, which is very hard to do. Take two very large prime numbers that are multiplied together and produce a product. Given that multiplication product find the two original prime numbers by factoring the product; the only known way to do this is try every single combination, a very processor intensive task. This is the core principle behind many of the existing public key algorithms, such as Diffie-Hellman and RSA. (Delfs Knebl, 2007) In recent years, as the available computational power increases exponentially, so do the need to use larger and larger prime numbers to guarantee security. (Moore, 1965) The recommendation today is to use 4096-bit prime numbers, but as the key sizes increases so does the computational power used by the client and server, as will the size of messages passed between client and server, which will make handshaking more and more cumbersome. To overcome this need of ever-larger key sizes, new mathematical problems have been introduced, that does not require large key sizes but still remains equally secure. One such new category of mathematical problems is the elliptic curve problem, or more precisely the elliptic

curve discrete logarithm problem, where an elliptic curve with a set of starting points are used to make a traversal of the curve in an arbitrary amount of rounds. This traversal is very hard and computationally intensive to reverse. (Delfs Knebl, 2007)

Zero Knowledge Proof

In cryptography zero knowledge proof is when one party (the prover) proves to the other party (the verifier) that it knows a shared secret and this proof is done without divulging any information about the shared secret. This can be achieved by having the verifier issue challenges in an arbitrary amount of rounds that if answered correctly shows that the prover has to knowledge of the secret with a very high probability. Goldwasser, Micali, Rackoff, 1989) (Schneier, 1996)

Forward Secrecy

When talking about forward secrecy in cryptography it means that if an encrypted message sent between two parties is intercepted and brute force decrypted by a malicious attacker. Then the key that was found during the brute force attack cannot be used on future messages between the two communicating parties. This is a sought after property for a cryptographic system to have. (Diffie, van Oorschot, Wiener, 1992)

Entropy

Entropy is a very important characteristic in cryptography when it comes to defining password strength. One could say that entropy defines how hard a password or random key is to guess. The entropy of a simple password like `cat` is very low and easy to guess. The entropy for a long random string is on the other hand very high, and takes a long time to break through brute force techniques. (Schneier, 1996) Entropy is also vital when generating a random number using a computer. Computers cannot generate true random numbers, and have to settle for pseudo random numbers. These pseudo random numbers are generated using a random function that takes a seed, to start the generation. This seeds needs to be of high entropy, else an attacker could easily guess the seed and run the same random function. Computers can not just rely on using the current time stamp and use that as a seed for the random function, a time stamp has terrible entropy on its own, therefore several different system parameters are collected to construct a high entropy seed that can be used in the random function and in extension in a cryptographic system. (Schneier, 1996)

11.9.4 Attacks on Cryptographic and Physical Security systems

Any cryptographic system is susceptible to attacks from third parties wanting to (Haselsteiner Breitfuß, 2006):

- Disrupt or interfere with the communication between server and client.
- Gain unauthorized access to a system or location.
- Obtain classified information.

There are many different attacks that can be performed on a cryptographic authentication system using a communication channel that is transmitting through the air. Lets us explore these different attacks that a security system must sustain, before delving deep into the different cryptographic protocols.

Eavesdropping/Skimming

A malicious attacker can listen in on the communication between client and server. This is the most basic form of attack and is very easy to deploy, the good thing is that it is also easy to counter act. By encrypting the communication between client and server the attacker will not be able to obtain any useful information. (Haselsteiner Breitfuß, 2006).

There have been cases though, which encryption and authentication is flawed, leading to partial discovery of key stream. As an example, a practical attack as been introduced by Garsia [29] in 2008 against MIFARE Classic from NXP[42], which allows extraction of session encryption key. Discovery of session encryption key stream leads to farther attacks, which is extraction of encryption keys used to protect data stored in affected memory section of tag.

Offline Attack and Data Manipulation

This attack is typically used in conjunction with an eavesdrop attack, where the attacker eavesdrops on the messages exchanged between the two parties and then runs an offline attack on the encrypted messages to try to break the encryption. These attacks can employ a wide range of

[42] Garcia, Gans (2008) "*Dismantling mifare classic*," *Secur.* pp. 97–114, 2008.

techniques, where the most basic technique is the brute force attack, where every possible combination of crypto key is tried to unlock the message. Another variant is the dictionary attack, where the attacker tries crypto keys from a dictionary of commonly used key values. A more sophisticated technique is the use of rainbow tables; these rainbow tables are pre-computed tables of password hashes for a finite amount of passwords using a given limited character set. Rainbow tables shift the space-time correlation of the brute force attack, by trading processing time for storage space. Rainbow tables require huge amount of storage, as they can grow very large. (Oechslin, 2003)

Data Corruption

This is when an attacker is corrupting or disturbing the communication channel between client and servers, making communication impossible, which is commonly known as a Denial of Service attack. It has fast become one of the most common forms of attacks on the Internet and is very hard to guard against. The attacker does not gain any information but it will make it hard for the clients to use the server. (Haselsteiner Breitfuß, 2006)

Data Modification

In this scenario the attacker tries to modify the data passed between client and server in such away that it may gain access to the server. A cryptographic authentication protocol must be able to either sense that someone is trying to manipulate the data that it receives or not be susceptible to this form of attack. (Haselsteiner Breitfuß, 2006)

Data Insertions

This is another form of data manipulation where an attacker inserts data at precise instances, thereby authenticating itself to the server instead of the client. (Haselsteiner Breitfuß, 2006)

Man-in-the-middle (MiTM)

Commonly referred to as MiTM, is when an attacker tries to impersonate the server and tricking the client to send its user credentials to what the client thinks is the server. The communication channel can be as secure as anything, but if the other party is not whom the client thinks it is, it does not matter. (Haselsteiner Breitfuß, 2006). Is one of the most powerful attacks against RFID technology, since attackers are simply relying information in this attack, understanding or decrypting transferred data is not necessary, thus making MiTM attack defeat even some advanced cryptographic RFID cards. Implementation of such attack does not require expensive hardware devices and attackers with average skill sets can build such a system.

Nowadays having smart phones equipped with NFC technology, one can use the Internet connection over mobile phone networks to pass data during this attack. A sample of effective relay attack is presented by (Kfir and Wool, 2005)[43]. As discussed in the paper, one of the main difficulties in this type of attack is the transmission delay. In ISO14443 standard for example, the timeout for a handshake query from the tag in vicinity is 5 milliseconds and up to 5 seconds for data transfer. While it might sound a limited and tight timing window, modern communication channels allow fast-enough bidirectional communication that meets this limitation. MiTM attack implementations can be very powerful and hard to detect by victims.

There are countermeasures available though, that can be used to prevent or limit such attacks. Measurement of the delay between query and response, introduced as distance-bounding protocol by (Brands and Chaum, 1993) shows how prevention mechanisms can be implemented[44]. This method later proved to be practically feasible as presented in (Hancke and Kuhn, 2005)[45] (Rasmussen and Capkun, 2010)[46] While mentioned countermeasure technically works, it has never become popular or used in consumer market due to its complexity and extra expenses. A different approach for detection and prevention of MiTM attacks against RFID is also presented in (Yong, Na-Na, and Tao, 2008)[47] (Bosley and Nicolosi, 2011)[48] as HB protocol, however according to the

[43] Z. Kfir and A. Wool, "*Picking virtual pockets using relay attacks on contactless smart card," Secur. Priv. Emerg. Areas ...*, 2005.
[44] S. Brands and D. Chaum, "*Distance-bounding protocols," Adv. Cryptology— EUROCRYPT'93*, 1993.
[45] G. Hancke and M. Kuhn, *"An RFID distance bounding protocol," ... Priv. Emerg. Areas ...*, pp. 67–73, 2005.
[46] K. Rasmussen and S. Capkun, *"Realization of RF Distance Bounding.," USENIX Secur. Symp.*, 2010.
[47] G. Yong, L. Na-Na, and Z. Tao, "*An Improved HB++ Protocol Against Man-in- Middle Attack in RFID System," ... Commun. Netw. ...*, pp. 1–4, 2008.
[48] C. Bosley and A. Nicolosi, "*HB N : An HB -like protocol secure against man-in- the-middle attacks,"* pp. 1–18, 2011.

later paper this solution works only against passive relay attacks. Later enhancements to this protocol named HB+ and HB++ has addressed this limitation though. Latest researches in the field for defense against relay and MiTM attack, suggests involving measurement and analysis of physical elements such as ambient and surface temperature (Urien and Piramuthu, 2013)[49] during the authentication phase.

MiTM attack can be performed as a passive or active attack. If attacker is simply relaying data during attack without any modification, it is considered as a passive MiTM attack. In more advanced form, attacker might manipulate captured data before transmitting them to targeted reader device.

Replay/Spoofing

An attacker can record the messages being sent between client and server during the authentication handshake and later resend (replay) the same data without modification to mimic a legitimate tag. In case of RFID tags that are not involving advanced cryptography, it will be impossible to distinguish a replied tag data from a legitimate one. Even if transmitted messages between legitimate devices are encrypted but strong authentication is not in place, a successful attack may still be possible. In such scenarios, attacker blindly record and reply tag data without need of decoding or decryption of them. To guard against such an attack, secure authentication methods such as Message Authentication Code (MAC) or even involving random number generators in authentication phase can prevent such attacks. It is important that the authentication protocol has a random part, usually this is done using a unique session token, making the messages used in different authentication sessions unique, i.e. the exact same message will never be sent again. (Aura, 1997)

The recorded information can also be manipulated and falsified prior to reply, allowing spoofing and impersonation. This attack allows bypassing many of simple RFID based solutions such as low frequency (LF) tags used for physical security. In case of basic RFID tags that are authenticated only with their UID, replay and spoofing attacks can be very effective, yet simple.

[49] P. Urien and S. Piramuthu, "*Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks,*" *Decis. Support Syst.*, vol. 59, pp. 28– 36, 2013

For more complicated implementations that random variables are involved in the protocol, by analyzing several legitimate messages and studying changed data it may still be possible to analyze and predict such changes, thus spoofing a properly modified reply. This is also referred as message reconstruction. Spoofing and replay attacks usually involve an emulator device, which is a customized reader device capable of emulating and sending arbitrary data to another reader. Emulators can function and be controlled with a computer, or built in form of a portable and independent device. There are many commercial or open-source devices are available specifically built for this purpose such as which is an open source hardware design capable of emulating ISO14443 tags[50].

Relay

In the relay attack, a malicious third party uses an intermediary medium to physically connect two parties. By creating an artificial bridge between, between two devices making it appear as if they are in close proximity of each other, when in reality they can be miles away. The attacker employs two relay devices that can seamlessly relay the traffic between the two parties without them even knowing it. A device is placed at each end of the bridge and the attacker can initiate a secure authentication session between for example a NFC smart card and a secure access control system, by holding the relay device close to an unsuspecting victims pocket and initiate the authentication session with the access reader at the other end of the bridge. This could possible lead access being granted to the unsuspecting victim, that is currently miles away from the system. This sophisticated attack has been proven effective against NFC enabled devices. (Francis, Hancke, Mayes, Markantonakis, 2012)

Another interesting practice of relay attack is presented in (Francillon, Danev, and Capkun, 2011)[51] which demonstrates attack against RFID technology used in cars to authenticate the key. In a more simplified implementation of relay attacks (van Dullink and Westein,2013)[52] evaluates using a computer with two off the shelf NFC readers communicating over network to implement

[50] "OpenPICC RFID Emulator Project - OpenPCD." Accessed: 17- Mar-2016. Source: http://www.openpcd.org/OpenPICC_RFID_Emulator_Project

[51] A. Francillon, B. Danev, and S. Capkun, "*Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars.*," *NDSS*, 2011.

[52] W. van Dullink and P. Westein, "*Remote relay attack on RFID access control systems using NFC enabled devices*," 2013.

the attack, targeting tags based on ISO14443-4 and focusing on RFID backend systems communication for the attack. Combined with sniffing techniques that increases the effective working distance between a tag and reader.

Denial of Service (DoS)

DoS attacks are referred to type of attacks that may target radio frequency range, affecting reader and tag device or the tag itself by affecting data, or even the backend systems in a RFID scenario, such as backend software or users. In any of cases the aim is to render some or all parts of the system malfunction or completely stop functioning to reach a goal. As well described in in (Bochum and Kasper, 2011)[53] DoS attacks can be in one of below categories:

- **Jamming:** In this type of attack, the goal is to jam the signal that targeted RFID system functions in, so that no further communications between tags and readers are not possible. In malicious scenarios, attackers might use jamming techniques to block a tag owner to use it for identification
- **Blocker Tag:** Another approach for DoS and prevention of communication with a particular RFID (reader) device is to flood it with large number of fake and virtual tags, in a way that it cannot identify legitimate tags anymore. If there is too much collision, there is no chance for a legitimate tag to communicate with targeted reader. Blocker Tag (Juels, Rivest, and Szydlo, 2003)[54] and RFID-Guardian (Rieback, B. Crispo, and A. Tanenbaum, 2005)[55] use this concept. A patent for a jammer[56] specifically built for RFID smart tags is another example for a DoS for good intentions, where it is built to protect individuals from unwanted RFID smart tag systems functioning around them, which is more of a privacy concern. Unlike simply jamming the RF, this patent presents a solution that floods the reader device with large amount of fake responses in a form that it cannot identify the genuine and legitimate reply from a smart tag.

[53] R. Bochum and T. Kasper, "*SECURITY A NALYSIS OF P ERVASIVE Physical and Protocol Attacks in Practice*," no. September, 2011.
[54] A. Juels, R. Rivest, and M. Szydlo, "*The blocker tag: selective blocking of RFID tags for consumer privacy*," *Proc. 10th ACM Conf. ...*, pp. 103–111, 2003.
[55] M. Rieback, B. Crispo, and A. Tanenbaum, "*RFID Guardian: A battery-powered mobile device for RFID privacy management*," *Inf. Secur. Priv.*, 2005.
[56] "Jamming device against RFID smart tag systems." 22-May-2007.

- **Destruction:** RFID tags are electronic circuits that are subject to intentional or unintentional damage caused by mechanical forces, heat or strong electromagnetic field. While physically breaking and destroying a tag might not be always the option, using string electromagnetic field can permanently damage tag while keeping physical shape of it intact. "RFID Zapper"[57] is a sample of such attack, which is built from off the shelf items, a disposable camera in this case.
- **Shielding:** By placing a tag in specific shielded area (Faraday`s case) for example in aluminum coated protective covers, it is possible to prevent any RF communications with the tag. While categorized under DoS, as discussed in previous Jamming section, it is mainly used for maintaining privacy and to prevent accidental or unexpected exposure of the tag to readers. Another use case is protection of security sensitive tags from being queried by attackers when tag is not being used

Side-Channel Analysis

The side-channel attack is a very sophisticated attack where the attacker records physical parameters and characteristics of the target system. These parameters could be minuscule fluctuation in power drawn by the CPU during decryption, signal crosstalk from system busses or measuring the time it takes the system to perform a specific task. Basically any measurable information leaking out of a side-channel, hence the name, could glean some clues as to what the system is doing and how it is doing it, for example during sensitive operations such as decrypting/encrypting. The system must be designed in such a way that makes these attacks very hard to perform or rather, makes the information obtained from these attacks useless. This is usually done by not running the exact same pattern every time the system decrypt/encrypt a message, because if the system is to consistent executing the exact same processor instructions every time a cryptographic function is run, then the attacker could gather information from this and exploit any weakness found. (Zhou Feng, 2005)

One of the most interesting attacks against proprietary RFID systems based on this concept is the published research paper about attacking Hitag2 implementation (Verdult, Garcia, and Balasch,

[57] "*RFID-Zapper - 22C3."* [Online]. Available: https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html.

2012)[58] which affects at least 34 vendors and about 200 car models as stated in the paper. Hitag2 was a very popular RFID microcontroller used in car immobilizer systems around the world since its introduction in 1996, but after revelation of its vulnerabilities is nowadays being replaced by more secure alternatives, such as Megamos which are also proved to be vulnerable in 2013 It should be noted that presented attack against Megamos is actually based on reverse engineering of a 3rd party licensed implementation of crypto system, and not side-channel analysis[59].

Cloning

Cloning attack refers to a process in which, reading data from a legitimate and genuine tag creates an identical and functional copy of a tag. Since UID of tag is not protected and can be queried prior authentication even in secure tags, any adversary with an off the shelf reader can read targeted tag, and later create a clone of the tag with same UID. Reverse engineering can be performed by different means. Of the most common techniques are etching the integrated circuit (IC) and analyzing implemented hardware layouts, extracting and reading contents of the device and trying to reconstruct its functionality.

Reverse Engineering

It is the concept that focuses on retrieving the content or functionality of a system or chip, to obtain proprietary cryptography algorithms, encryption keys or other forms of intellectual properties (IP). A paper published by Nohl in 2008 is a great example and demonstration of such attacks, which targets MIFARE Classic RFID microcontrollers[60]. While referred method in the paper is considered to be expensive and time consuming, it can be mostly automated. There are even multiple commercial companies available, which can provide this service to customers. Another recent example of successful attack is the research on Megamos (Carolina and Paterson, 2013),[61] which is based on reverse engineering firmware and software implementation of a proprietary cryptosystem assumed to be secure in its chip design. Megamos is the crypto system

[58] R. Verdult, F. Garcia, and J. Balasch, "*Gone in 360 seconds: Hijacking with Hitag2," 21st USENIX Conf.* 2012.
[59] R. Carolina and K. G. Paterson, "*Megamos Crypto, Responsible Disclosure, and the Chilling Effect of,"* pp. 1–15, 2013
[60] K. Nohl, "*Reverse-Engineering a Cryptographic RFID Tag," Proc. 17th USENIX Secur. Symp.*, 2008.
[61] R. Verdult, "*Dismantling Megamos Crypto : Wirelessly Lockpicking a Vehicle Immobilizer • Due to a recent injunction by the High*."

that multiple high-end and luxury car manufacturers have designed their car immobilizers based on it.

Reverse engineering of proprietary cryptosystems have historically proven that security through hiding the logic of system from attackers is usually doomed to fail, and adversaries eventually find their way to understand implemented algorithms and reveal vulnerabilities in them. In case of Megamos, Volkswagen followed a poor practice of disputing the researchers and prohibiting them by court order from publishing their paper.

12.0 Methodology

In order to prepare this thesis work a wide range of techniques and previous researches had to be reviewed. Beside few published book titles that have been mentioned before, tens of academic papers, news articles, whitepapers, security projects and presentations have been reviewed. Having multiple resources covering the same topic provided two main advantages. First, it help to have more than one point of view about a specific subject, thus giving us a better understanding and more complete overview. The second advantage is being able to review different solutions and answers to a certain problem. Moreover, academic community usually follows slightly different approach and way of researching and releasing information in comparison to the so-called hackers community. There are also some domains that may have not been researched by both communities, which in such cases by not having this dual point of view, we will completely miss them. After collecting all related materials related to topics related to this thesis work, they have been reviewed, important parts of each paper has been marked and tagged and classified properly. Another point that has been in mind while preparation of this work was to have a few external references and citations for every single topic that is introduced in this report, so that readers can study them for gaining farther and better understanding of the subject.

12.1 Thesis Structure and Explanations

In the academic review this research start familiarizing the reader with basics of radio frequency identification (RFID) technology followed by, and introducing in how different RFID standards work. Followed by, a review of some of the most popular RFID tags and card brands that are currently in use around the world. By reviewing this section readers should be able to understand

how RFID works, without getting involved with too much technical details, and understand different purposes of using RFID tags and cards.

A description of common attacks and abuse scenarios affecting RFID systems. Attacks are categorized based on their objective, parts of the RFID system they target, and expected outcomes of attacks. For every introduced attack type, where possible, relevant previous works and researches are presented in form of a short summary. This helps readers to be aware of possible threats, without need of going through entire research details of that specific case. Of course, readers that are interested in fine technical details are supposed to follow presented materials in order to have a complete grasp of the presented attack or problem.

Since there are many different sets and combinations of attacks that can be used to achieve one result, this research is more focused to explain what authors has found suitable and most efficient in long term for the purpose of research and evaluation of attacks. Further more 5 other real world case studies such Georgetown University GOcard mobile pilot and campus student accommodation tags are briefly evaluated and presented.

12.2 Evaluation of attacks against RFID technology

Radio Frequency Identification (RFID) is a technology that has been around for more four decades now. It is being used in various scenarios in technologically modern societies around the world and becoming a crucial part of our daily life. But we often forget how the inner technology is designed to work, or even if it is as trustable and secure as we think. While the RFID technology and protocols involved with it has been designed with an acceptable level of security in mind, not all implementations and use cases are as secure as consumers believe. A majority of implementations and products that are deployed suffer from known and critical security issues.

This thesis work started with an introduction to RFID standards and how the technology works. Followed by that a taxonomy of known attacks and threats affecting RFID is presented, which avoids going through too much of technical details but provides references for further research and study for every part and attack. Then RFID security threats are reviewed from risk management point of view, linking introduced attacks to the security principle they affect. We also review (lack thereof) security standards and guidelines that can help mitigating introduced threats, and what materials we are currently missing, that can be used to raise awareness and increase security of

RFID technology for consumers. This thesis will not focus on and cover all attacks against NFC systems, but only cover attack vectors and scenarios that are shared with RFID systems in physical security applications.

12.3 Attackers Classification

Different types and classes of attacks require different level of knowledge, prerequisite resources such as hardware and software tools and different budgets. While some simple attacks might be feasible to impalement, other class of attacks might require thousands of dollars of equipment, knowledge and experience in the field and weeks of work to succeed. That is why we often calculate the risk of attacks based on the amount of damage or loss they might cause, and also considering which class of attackers they meant to protect from[62]. (Kasper, 2011) has defined three classes of attackers, and similar classification will also be introduced in this thesis, which are as follow:

Class I (Individual Attackers)

This class represents those groups of attackers whom are mostly consisted of individuals who are interested in the subject and have enough base knowledge to understand concepts of moderately advanced attacks and are often the knowledge that are previously published or introduced by later class of attackers. The motivation for these attackers is usually personal interest or simple attack scenarios that can be part of a self-motivated attack or part of an ordered security evaluation of a system. Attackers of this class use off the shelf tools, software and devices for their attacks or often develop their attack tools and scripts based on public knowledge about vulnerabilities.

The budget and amount of funding behind attacks that are conducted by this group is usually very limited. Students, individual so-called hackers/crackers or enthusiast experimenters are samples of this class.

Class II (Professional Attackers/Researchers)

[62] T. Kasper, "*Security Analysis of Pervasive Wireless,*" Ruhr-University Bochum, September 2011.

Attackers or researchers in this class are much more experienced and have solid background and deep knowledge about the field. Unlike previous class, they produce their own novel and new set of attack techniques and tools, or discover new type of vulnerabilities. This also usually results in design and build of custom hardware devices or software tools, where off the shelf devices and equipment are not capable of handling expected behaviors. Customized RFID reader devices or card emulator devices are examples fit in this category. Motivations and funding are also much higher in this class. Result of researches or attack methodologies discovered by this class usually affects a wide range of products and not an individual case or certain limited scenario. Individual or small team of researchers whom their works are published in communities, or professional attackers who use their skills to conduct sophisticated attacks against targets are samples of this class. Attackers in this class are skilled enough to case sever damages or compromise sensitive scenarios such as sophisticated frauds or forgeries.

Class III (Funded Organizations)

While previous class of attackers might look like most advanced and serious threats, level of expertise and sophistication can still drastically grow. Government backed or well-funded organized criminals with support of great funding resources fit into this category. Government or intelligence agencies arrange dedicate group of highly skilled professionals, often hired among previous class, for their researches. Results of work of this class are the most advanced and sophisticated attacks that are not possible to achieve by previous class. Well-funded Intelligence agencies such as NSA or similar commercial companies for example, have large teams of specialists and cryptographers working together that make such advanced and focused researches possible, capable of breaking many cryptographic systems.

12.4 Taxonomy of Attacks and Security Issues with existing PACS

Wide range of technologies, standard, protocol's, hardware devices and software's are integrated together to form the RFID technology. For the same reason, many different types of attacks or attack objectives exist against it. Every part of the system should be considered as an attack surface, with possible relevant weaknesses and attacks against it. While different components are usually studied and attacked researched for possible attacks separately, the result and successful attack

against one component might affect other components and parts of the system, even if they are not vulnerable on their own and when inspected individually. Consider a scenario where working logic of an RFID system that involves advanced cryptography features is secure. But during manufacturing design process, mistakes result in a weakened cryptography scheme, or exposure of otherwise assumed secure cryptographic keys. In other example, an RFID implementation might be considered secure against cryptography attacks or design flaws, but lack of physical security considerations allows execution of powerful Man-in-The-Middle (MiTM) attacks that effectively bypass even some of the most secure RFID implementations. In this part of the thesis, possible attack vectors and methods are discussed and divided into different categories where possible. Some of the classifications and categories introduced in this thesis are based in previous works presented in[63] each focusing on different aspects for classification. While the first two references focus more on technical aspects of threats, later reference[64] focuses more on principle aspects of security threats, and also covering complexity and cost of different attack types.

12.5 Security Status and Vulnerabilities of Major Smart Card Brands

Being familiar with RFID technology basics and common attack types and scenarios against this technology, in this section we can have a summarized and recap version of known attacks and researches that has been published to the date of publishing this thesis. It should be noted that not all types of RFID cards, models or brands are covered in the table. Moreover due to simplicity of attacks against non-cryptographic and ID only tags, they are not covered in this section. All of these types of tags can simply be cloned and emulated with off the shelf and cheap equipment and available open-source software. The focus in this section is more on most known and widespread brands and models that are used by consumers and in commercial market. Moreover there might be multiple versions and publications for same or similar types of attacks against a class of card, but only the major or most complete ones are cited. For farther variants of attacks against each specific tag family, reader is advised to go over relevant and cited papers in mentioned references.

[63] T. Kasper, "*Security Analysis of Pervasive Wireless,*" Ruhr-University Bochum, September 2011.
[64] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, "*Classification of RFID Threats based on Security Principles*," engr.sjsu.edu

For a much more detailed and complete list of brands and models among their specific security features, readers can refer to a comprehensive list of tag chip models and their security and protection features in[65] which covers over 350 models from different brands. As one might notice, not all chip models that provide security features are publicly discussed as broken, however this is only the case if those features are used properly. For instance, some of models provide password protected read/write operations, but if this option is not used, cloning those tags is as simple as any other ID only tag model.

In the presented table the first column indicates the brand or specific RFID (microcontroller) model. Second column indicates if the tag type is (partially) broken or not. It means if part or all of security measures provided by the tag are vulnerable or not. Third column indicates if existing vulnerabilities or attacks are practical to lunch or not. Fourth column shows cost of known attacks (considering lowest cost possible) in form of budget or requirement of advanced/expensive lab equipment. Finally the last column lists (most interesting) known attacks or research works published related to the tag.

Brand/Type	Broken/ Partially	Attack Probability	Cost of the Attack	References and Papers
MIFARE Classic	YES	Practical	Low	[29] [30] [31] [44]
MIFARE DESfire	YES	Practical	Medium	[32] [33]
MIFARE Ultralite	YES	Practical	Low	[34]
HID iClass	YES	Practical	Low	[35]
HID iClass Elite	YES	Practical	Low	[36]
KeeLoq	YES	Practical	Medium	[37]
MEGAMOS	YES	Practical	Low	[38] [39] [40]
Legic	YES	Practical	Low	[41]
Hitag2	YES	Practical	Low	[42] [43]

Table No.4[66]

[65] A. Quagliarini, "RFID General Table." sourse: http://goo.gl/vYDbqT Accessed: July, 2016
[66] Security Status and Vulnerabilities of Major Smart Card Brands source: Prepared by the author

As we can see in presented Table No.4, all listed proprietary protocols have been successfully analyzed and broken. It might be worth mentioning that some of those proprietary standards are still widely used nowadays in sensitive applications. For example the MEGAMOS technology is used by some of the high-end and luxury automobile industry companies to protect latest models of cars such as some of Porsche or Volkswagen models. In other cases, there are still dozens of manufactures and tens of car models that are affected by these broken technologies.

For example the protection implemented in MIFARE Classic cards has a long history of known security issues, which are discussed in many papers and can be exploited to retrieve these protection keys. This thesis briefly reviews some of these papers and attacks they introduce. Among the more interesting ones ”Dismantling MIFARE Classic” (Garcia and Gans, 2008)[67] can be mentioned that described practical attack techniques that can recover keys by capturing and analyzing only 2 handshakes between tag and a legitimate reader (aware of the key) in about one second, or more sophisticated and quicker attacks described in paper titled “The dark side of security by obscurity” which are a card-only attack (Courtois, 2009)[68]. It means by having access to only the card, attacker can successfully extract all protection keys practically in less than a minute. The later paper actually describes and combines three known attacks from previous works (Garcia, Rossum, Verdult and Schreur, 2009)[69] (Nohl, 2008)[70] to achieve the first card-only attack against MIFARE Classic, which to date is still the fastest and most reliable attack.

As presented in section 7 of (Bochum and Kasper, 2011), implementation attacks can be successfully used against even the most secure and advanced cryptography system implementations, in this case Mifare DESfire (based on 3DES algorithm) leading to successful key-recovery from smart cards. This work is based on a previous research presented by Kimo in 2009 (Kasper, Oswald, and Paar, 2009)[71] introducing new methods of side channel analysis attack by analyzing electromagnetic field using low cost equipment.

---

[67] F. Garcia and G. D. K. Gans, “*Dismantling mifare classic,” ... Secur. 2008*, pp. 97–114, 2008.
[68] N. Courtois, “*The dark side of security by obscurity,” Int. Conf. Secur. Cryptogr.*, 2009.
[69] F. D. Garcia, P. Van Rossum, R. Verdult, and R. W. Schreur, “Wirelessly pickpocketing a Mifare Classic card,” *2009 30th IEEE Symp. Secur. Priv.*, pp. 3– 15, May 2009.
[70] K. Nohl, “Reverse-Engineering a Cryptographic RFID Tag,” *Proc. 17th USENIX Secur. Symp.*, 2008.
[71] T. Kasper, D. Oswald, and C. Paar, “New Methods for Cost-Effective Side- Channel Attacks on Cryptographic RFIDs,” *Work. RFID Secur. RFIDSec09*, no. 3, 2009.

12.6 Case Studies

This section reviews college/university campus pilots:

Georgetown University is teaming up with Enterprise Security providers, an mobile technology companies, to deliver secure logical and physical access to bring mobile credentials on campus, in these context, limited pilots with different vendors are under consideration.

For physical access control applications, Georgetown IT department can increase the efficiency of security administrators by helping to implement a robust mobile identity management system with proven processes for managing users and the entire life cycle of mobile identities. For instance, HID Global Security and Microstrategy, Inc. identity services enable integrators to help manage the entire process of how an employee is on-boarded and issued a mobile identity. Simply adding a user's name and email triggers the process to send out an invitation email to the employee with instructions on how to install the Mobile App. When the App is installed and configured, the correct mobile identity is provisioned to the mobile device and the security administrator is notified when the process is complete. For larger organizations it is possible to mass upload user data from a file.

Universities are on the side of the equation focused on protecting data and physical spaces[72]. One way to accomplish both is to work from the other side of the equation; that is, developers design solutions that blend data with physical security systems. Administrators are focusing on the possibility, particularly in the education sector. Security personnel and public safety departments also have an interest in mobile applications. They can access video, data, and security credentials without having to be at "home base". Physical security is as much an issue of access as it is of data. With data, security personnel are better able to understand the context of a situation and respond accordingly. The system itself understands the situation better, and can perform functions of either locking down an area or granting access.

[72] Using Usher at Georgetown" *University Information Services*. Downloaded on January 6th, 2015 from http://uis.gudrupalstg.georgetown.edu/accounts/usher-faq#Who2

With ongoing pressure to reduce IT capital expenditure and operating expense, the Mobile Credential solution helps eliminate the need for physical smart cards, card-printing and personalization systems, as well as the complex IT processes to enroll and provision user accounts. Georgetown smart campus initiatives[73] leverage the power of mobile computing and over-the-air (OTA) provisioning, as well as rich policy and workflow capabilities, to eliminate manual processes and empower end-users to easily enroll and recover credentials as required.

Since last year Georgetown University is piloting a mobile identity platform that combines several forms of physical identification into a consolidated mobile identity credential on smartphones. This Enterprise security solution still on beta testing and risk-assessment and supplements traditional forms of identity on campus, such as plastic ID cards, usernames, and passwords, with a secured mobile identity on smartphones, to reduce identity fraud and cybercrime.

The new mobile credential or GOCard app, is still in its piloting phase and can only be used by freshmen, incoming transfer students and is also available to selected Georgetown employees via email invitations only. Once the mobile GOCard app is downloaded on smartphones, beta testers can quickly and securely use the mobile GOCard app to sign in to websites, make purchases at locations around campus (students only), Submit a photo for your GOCard, and so on. You can pay for things on campus; you can use it to pay for printing, and also for swapping contacts with each other.

In the past, deployment credentials involved one major round of on-site card provisioning at the beginning of each semester and periodic follow-on provisioning for new students, hires or to replace lost or stolen cards. This model will not go away anytime soon because of the visual identification capabilities that only physical cards can deliver; however, on top of this model, there is the new opportunity to remotely provision physical access credentials to smartphones and other mobile devices, and to provision credentials to both cards and phones not just for opening doors,

[73] "*UIS introduces LiveSafe, Usher, and Campus Quad mobile apps to campus*." *Georgetown Voice*. January 2015. Downloaded on January 5th, 2016 at http://georgetownvoice.com/2014/09/04/uis-introduces-livesafe-usher-and-campus-quad-mobile-apps-to-campus/

but also for secure print management, time-and-attendance and cashless payment applications, among others.

Georgetown University will consider adding more features to the mobile GoCard app based on how the results of the pilot program. If it goes well, GU will consider expanding the app to the rest of the entire community as well.

Universities are in need for a cost-effective migration plan to replace its outdated and vulnerable ID card system with a more secure and comprehensive "one card" solution. 5 Case studies in higher Education included in this paper:

Five pilot projects illustrate the benefits of using smartphones to open doors on a campus. In projects at Georgetown, George Mason, Villanova, Arizona and the University of San Francisco, groups of students and staff access campus residence halls, facilities, and selected rooms using a variety of popular smartphones connected to all major mobile networks.

Participants use their phones to access residence halls, and some are also using them with a unique digital key and PIN to open individual dorm room doors. To open locked doors, participants present the phone to a door reader, just as they would a student ID card.

The technology can also support over-the-air provisioning and management of digital keys, which simplifies administration of the PACS. Approximately 80 percent of the student participants reported that using a smartphone to unlock a door was just as convenient as using their campus ID card. Nearly 90 percent said they would like to use their smartphones to open all doors on campus.

While these pilots are focused on physical access, nearly all participants also expressed interest in using their smartphones for other campus activities, including access to the student recreation center and laundry, transit fare payment, and meal, ticket, and merchandise purchases.

University	Case Study Scope	Solution Provider

Georgetown University[74]	Phase 1: Student dormitories/offices	Microstrategy Blackboard
George Mason University[75]	Phase 1: facilities, residence halls, library and cafeteria	HID Global
Villanova University[76]	Phase 1: 30 students; 12 staff; 6 dormitories/offices Phase 2: Over 100 students and staff; two major residence halls with 80 locks (with four people per room, resulting in over 200 residents) Campus-wide deployment: 4,000 doors in dormitories, offices and classrooms now implemented with locks, with 6,000 doors implemented when complete. Use has expanded to check attendance using NFC-enabled tablets; establish a loyalty points program for sports arena seating; enable POS terminals to use Wildcard Bucks; NFC-enable vending machines, laundry facilities and library copier locations.	Allegion
University of San Francisco[77]	Phase 1: 12 main doors; 3 elevators with floor control. Enable access control and laundry. Phase 2: Explore alternate student demographics and feedback; implement with executive MBA graduate students at branch campus	Allegion
Arizona State University[78]	Phase 1: Palo Verde main hall; 32 student phones controlling 22 selected resident room doors	HID Global

Table No.5

12.6.1 Combined results and Lessons Learned From Case Studies

[74] "Usher One, Usher All." *The Hoya*. January 7, 2015. Downloaded on January 5th, 2016 from http://www.thehoya.com/usher-one-usher/

[75] Migrating to a Smart, "One Card" Student ID, George Mason University, HID Global case study, from: https://www.hidglobal.com/case-studies/george-mason-university

[76] Villanova University Conducts Most Comprehensive NFC Access Control Trial to Date," Ingersoll Rand press release, March 21, 2012, from: https://investor.shareholder.com/ir/releasedetail.cfm?releaseid=658725

[77] Using NFC to replace campus one-cards with smartphones," University Business, March 2013, http://www.universitybusiness.com/article/using-nfc-replace-campus-one-cards-smartphones

[78] Arizona State University Mobile Access Pilot, HID Global case study, from: https://www.hidglobal.com/sites/hidglobal.com/files/resource_files/hid-asu-mobile-access-cs-en.pdf

Combined campus pilot and students feedback included:

- 70%-80% of student physical keys and student access cards are lost or stolen
- 91% of students said ease-of-use or convenience was the best part of NFC.
- Over 70% preferred using a smartphone to enter buildings over using their student ID (smart card).
- 100% of students surveyed would be interested in owning NFC technology built into their own smartphone

The main benefits identified by students and their relative importance is shown in Table No 6.

Student Benefit	Percent Reported Benefits
More Convenient/ and easy to use	43%
Faster issuing process	15%
Less likely to loose or break credential	14%
Innovative technology	11%
Easier replacement	6%
More secure	6%
Reduced environmental wate	5%

Table No.6: Benefits from University/Campus Implementations

The ability to issue identification credentials immediately and carry them on a smartphone (i.e., as a mobileID) has compelling advantages for both the users and Universities. The smartphone with a mobileID becomes a door opener, a mobility ticket, and a time and attendance tracker, among other functions. A Students does not have to wait for their badge to open doors or pay for food. Universities can streamline their ID (GOCard) issuing processes, saving costs and increasing convenience. Users benefit because it is convenient to have all of their ID cards always at hand. And a mobileID already works with many current reader infrastructures.

Although a high percentage of students have smartphones, there are still students who do not (adoption is increasing every semester). I think that's one issue we need to constantly keep in the back of our minds, We have brought up the issue with our enterprise security provider and they

have reassured us that there is an HTML code, a way that through a non-smartphone you can still use the basics of the app. As these apps continue to expand their reach on campus, GU says it will continue to look for ways to make sure all students are included in the technological improvements.

Universities will need the IT departments or systems integrators support not only for deploying the overall solution but also for provisioning and managing a broader range of credentials that can now be issued remotely for a wider range of applications. Even the best IT organizations experience difficulty managing the sheer volume of identities within their organization, for example at the beginning of semesters where we experience a large amount of students waiting to move into our campus, quick pre-registration, simple provisioning and email distribution of electronic badges will allow them to skip the physical GOCard pick-up line on move-in day. This means we can use mobile GoCard credentials for quick check-in in residence dorms. These multipurpose credentials securely access computer workstations, network resources, data, cloud applications, physical doors or buildings, and also enable users to digitally sign transactions and encrypt data. It's more convenient, easier to use, cost-effective to deploy and provides support for a number of authentication and information-protection needs.

Although the mobile GOCard app has been downloaded by thousands of students in previus semesters, not all the users have found the app to be completely beneficial. The mobile GoCard is useful for certain things, like Pay for things around campus with just your phone, Check in when students arrive on-campus without waiting in long lines, Log in to Georgetown websites without entering usernames and passwords, Connect with friends and add their contact info directly to the phone address book, but it cannot be taken as a form of credential physical access control. In order to make the mobile GOCard app more useful, we need to allow more features and making it interoperable with the large amount of physical access control infrastructure, so students can get into their dorms or the library, etc. with our mobile GOCard.

Of course, having a single app or digital credential that provides so many access rights is a security concern in and of itself, that's why a multi-factor authentication will be necessary, any single factor of authentication is never secure by itself, whether it is biometrics or your password,

which is a secret. For example, Touch ID (Apple's fingerprint technology) is one form of biometrics on the phone that can be explored for this purpose as a dual factor to provide that extra layer of security. Some businesses might not yet be comfortable with using mobile devices as a primary form of identity and authentication. Georgetown can design a solution that assuages these concerns. Instead of the mobile device or wearable acting as the primary token, it becomes a secondary one.

Using two forms of authentication is a best practice; the employee uses a traditional card or other token, and then uses the mobile device to confirm his identity and gain access. Dual authentication is of interest some departments at the Law Center, such as Financial Aid and Registrar Offices, needing an extra security layer. For example, all the employees within the Financial Aid department could access the computer room, but only ones with the correct mobile credentials could access the computer.

Finally in this thesis after all case studies have been reviewed, in which we see and analyze the results of this pilots and the difficulties of implementation in real-world scenario, in some cases it is an practical way. As we can see, in all cases the descriptions highlight the variety of benefits that can accrue from implementing mobileID applications while illustrating associated implementation challenges. While some challenges are unique to a particular application, others are common and require solutions at the industry or ecosystem level before applications can truly become mainstream.

Challenges during implementation can be categorized as follows:

- **Infrastructure challenges**: The lack of maturity and consistency across the NFC ecosystem, coupled with the lifecycle lengths of current infrastructure assets, may result in refresh cycles being carried out without NFC as the primary mobile strategy.

- **Credential security model challenges**: The market is therefore faced with potentially supporting two different security models (SE and HCE)
- **Absence of consistency across device types**: lack of consistency in how NFC functions behave across device types. (Antenna placement, read-write performance, etc.)
- **NFC accessibility or availability challenges**: differing levels of support for NFC features and security approaches
- **Lack of industry-wide standards**: many of the non-payment applications have no industry standards or have standards that are only just emerging.

13 Analysis of results

This chapter will analyze which mobile device, mode of operation, authentication protocol and cryptographic library that will best suit and fulfill the requirements and goals presented in this research. It will also analyze different attack vectors and if they are valid and meet the requirements of the research.

Mobile devices (Smartphones)

When choosing the mobile device to use in the proposed framework several factors have to be taken into consideration.

- Are there any NFC enabled devices for the OS?
- How open is the OS when it comes to API access, documentation and source code?
- How large is the potential user base?
- Which modes of operations does the OS support?

Apple's iOS and Microsoft's Windows Phone have a long way to go, both in regards to functionality and openness. The iOS operating system is completely closed for third party developers, disqualifying it as a viable choice in this project. Windows Phone on the other hand is a competitor to Android, but it loses to Android's richer NFC library API and market share penetration, Android having a market share of 85.3% for the year 2016[79], according to IDC,

[79] IDC.(2016, September 1st). source: *Worldwide Quarterly Mobile Phone Tracker*. Retrieved: 2016, from: idc.com: http://www.idc.com/tracker/showproductinfo.jsp?prod_id=37

compared with Windows Phone's 0.5 percent. (IDC, 2016) Android stands out when it comes to NFC functionality. Developers have full access to all APIs regarding NFC. Android is also open source that's why all libraries and APIs are available for review, which can be very helpful during development where library features are sometimes poorly documented. Android has by far the most mature NFC libraries and widest array of NFC enabled devices supporting all modes of operation.

Modes of Operation

Most secure authentication protocols require the server and client to exchange several request/response messages during the authentication process. This means that the communication has to be bidirectional i.e. both the server and client have to be able to both send and receive messages during one session. The transfer speed is also important, as lower speeds translates into longer authentication times.

The only real option when wanting bidirectional NFC communication when using an Android device is to make the device emulate an NFC smart card. Android has the ability to emulate a NFC smart card by using the Host Card Emulation (HCE) Framework as presented in chapter? From the access control reader's perspective it will communicate with the Android device as if it where an ordinary NFC card or tag, using exactly the same protocols and parameters. This will enabled a bidirectional, half duplex communication channel, well suited for authentication protocol message exchange.

Open Standard Authentication Protocol

Some manufacturers and vendors try to evade from being audited or challenged for security by going the proprietary product and protocol, which is known as security through obscurity. It means that vendors try to hide technical details and specifications of their products, so that attackers have no ground information about them to attack their product. This has been proven multiple times to be a wrong assumption and it actually has never worked. In almost all the so called secure tags that has been researched and broken so far, key parts and protocols of the chip or technology were considered a safely guarded business secret of the vendor and some vendors have even tried to sue

researchers working on their products to break them. Yet we can see in previous research papers that all of those vendors and products have been successfully attacked and their products are now considered 'Broken' and unsafe, even though they have never released any technical details to consumers.

Another commonly seen security issue is about vendors that try to reinvent their own security protocols, or when they copy a known standard and protocol, but just modify it slightly so that it is not standard and compatible with similar products anymore. This is also considered a sample of security through obscurity. A good example of this case in RFID industry is vendors that try to present their own secure proprietary tags that are not compatible with other manufacturers. This can be either for branding and marketing goals, or to just give a (false) sense of security to consumers that, just because other brands and vendors cannot understand and communicate with their devices, you are safe.

When choosing an authentication protocol for the access control system, naturally the system requirement has a huge impact on the selected protocol. Below the different authentication protocols will be evaluated with regards to the requirements.

PKI

This is the most widely used authentication protocol on the Internet and could be a usable protocol here as well. It is very secure, especially when using one of the newer Elliptic Curve asymmetric keys. Unfortunately the PKI protocol has two major drawbacks that make it incompatible with the system requirements for a physical security application. The first one is that it requires access to the Internet; it has to be able to verify the servers and/or users certificate using a third party certificate authority that will verify the authenticity of the certificate. The second draw back is, that it costs money to register the certificate with a certificate authority. Self-signed certificates can be used, but that defeats the purpose of using PKI in the first place. Since you have no way of knowing if the signed certificate is sign by the server or a malicious attacker.

Kerberos

Not really an option in this system. It requires many external system components and is not a good fit for a lightweight, standalone access control systems. It also needs all connected systems to have a precisely synchronized time, which requires a Network Time Protocol (NTP) Server or similar, which further increases the complexity and number of required systems.

SSH

Since the certificate is not signed, a MiTM attack is very easy to perform. If the user does not heed the warning about possible MiTM attacks, it will send its plain text password to the attacker.

Pre Shared Key (PSK)

AES keys are typically between 128-bit and 256-bit long, depending on the required security level. The server and client need to exchange this secret key in order to communicate securely over an open network. This is not a trivial task, the server and client has to be at the same physical location exchanging the keys in a manner that no one can eavesdrop and gain access to the key. Once the key has been exchanged it has to be kept hidden, which poses the second problem with PSK; how to securely store AES keys, they are nearly impossible for a human to memorize, since they consist of a random string of 32 bytes. This means that they have to be stored locally on a mobile device, which make them susceptible to theft or other malicious attacks. This limits the usefulness of the PSK authentication protocol, even though it is very secure.

SRP

SRP is a strong password authentication protocol that is starting to gain considerable attention in both the open source community and in commercial products. SRP does not require an Internet connection, and its protocol is very lightweight comparing to some of the others that have been evaluated. The SRP protocol does not expose passwords to either passive or active network intruders, making it impossible for an eavesdropper to gain knowledge about the secret password. The passwords are also stored as a one-way hash on the server, making it resilient even if the server is compromised. It is secure even when using low entropy passwords, thanks to the salt that is added when creating the SRP verifier.

With SRP one can weighting convenience vs. security, effectively choosing the level of security a particular system needs. By forcing the user to enter the password in every authentication session, one gets a very high level of security with SRP. On the other hand, the password can be entered once and stored on the device for future use. Then the level of security will drop significantly since the plaintext password is only protected by the device's PIN code. This level of flexibility is not given in the other PSK protocols that use a long random key with a length of at least 128 bits, making it nearly impossible for a user to memorize.

Security analysis

From the authentication protocol analysis in the previous chapter, the choice was between using PSK and SRP, they are similar in some sense, and they both fulfill the requirements:

- They are both very secure and lightweight protocols.
- They both use a shared secret that needs to be shared between server and client before authentication can be performed.
- They do not require any Internet access.

In the end the SRP protocol is the one that best fulfills the system requirements. Its ability to use memorizes low entropy passwords favored the SRP protocol over PSK which uses long random password strings. Let's have a look at how susceptible the SRP protocol is to different cryptographic attacks.

Some experts argue that the attack vectors on a NFC system are very limited due to the closely coupled nature of NFC, where the communication range is less than 10 cm. This attitude towards security in NFC could be dangerous, and lead the system designers to neglect certain situations and thereby creating security holes.

Eavesdropping

SRP has been designed to counter the threat of password sniffing, as well as preventing a determined attacker equipped with a dictionary of passwords from guessing at passwords using captured network traffic.

Offline Attack

The SRP protocol allows the server to store passwords in a form that is not directly useful to an attacker. Even if the servers' password database were publicly revealed, the attacker would still need an expensive dictionary search or brute force search to obtain any passwords. The exponential computation required to validate a guess in this case is time-consuming.

Data Corruption

A denial-of-service attack is hard to fend against, and this system will be no different. An attacker could always, corrupt the communication, and make the system unusable, though it is not a threat to the integrity of the system. Due to the closely coupled nature of NFC, where the communication range is less than 10 cm, denial-of-service attacks would be tough to implement in a real scenario.

Data Modification

The SRP protocol resists active network attacks such as data modification attacks. It would not help the attacker in any way to modify the contents of the exchanged protocol messages.

Data Insertions

Likewise it is not affected by precisely timed data insertions. This attack does not really make sense as the attacker would have to be standing next to the victim, who will probably notice the stranger standing close by, trying to gain access.

Man-in-The-Middle (MiTM)

A MiTM attack does not really make sense, as the communication range is very short distance. There might be situations where this is possible but a correctly implemented SRP protocol should not be susceptible to this kind of attack. Even if someone tries to pose as a Server trying to steal the password, no actual password information is ever passed from the client to the server.

Replay

Mounting a replay attack on a SRP authentication system would not be possible, since the protocol uses random elements that are unique to each session. Therefore using the messages from a previous session would not be possible.

Relay

The SRP protocol has no built-in guards against a relay attack, which means that the system could be susceptible to such an attack. This has to be considered when designing the system.

Side-Channel

A side-channel attack I very hard to guard against. But the attacker needs a to have complete access to the system to be able to study it in detail.

14 Conclusions

Deployed access control technologies fall short of the protection level that modern RFID smart cards and mobiles smartphones can provide. They use cryptographically insecure encryption often in combination with predictable secret keys. A modern system must use standardized encryption and a multi-tier key management scheme that protects valuable master keys in secure hardware modules. Managing such a centralize access control scheme becomes a group responsibility rather than the responsibility of individual divisions or facility management teams. Consequently, access control and identity management (IAM) by the IT security group or corporate security team and held up to the same requirements and risk management procedures as other IT assets.

Besides these organizational changes, migrating to a modern access control system requires controllers to be equipped with secure key storage chips and access cards to be replaced. Through the use of dual interface cards, the migration is stretched over a manageable time period, starting at the most valuable locations.

Even with a strong technology base, incidents should be expected. Update procedures for reader software and keys assure keeping the time period affected by a data leak small. Intrusion monitoring provides a vehicle to detect access attempts from stolen cards.

The access control market is ripe for a change and ready to gain the same protection level that we have been experiencing in IT systems for years. Common among many mobileID applications is the need to provision a credential to the smartphone device, store the credential on the mobile

device and use the credential to effect a transaction at the point of service (POS) or access control system. As described in this paper, NFC uses cases face several common challenges in achieving market adoption.

A requirement to support the large number of disparate smartphone makes, models and configurations in the market will inhibit adoption. However, a small number of manufacturers are driving the vast majority of new handset sales. Samsung and Apple both offer devices with an embedded SE, and Android mobile devices support HCE for applications. If common architectural approaches and sets of commercial parameters could be established with these leading firms, NFC use cases will be more straightforward to implement and new deployments and adoption will grow.

While there are a large variety of applications that can take advantage of NFC, those with an established compatible contactless infrastructure (e.g., transit, access) will be more straightforward to implement and those early adopters could help to drive adoption. In the past decade, contactless infrastructure has grown from access control to hotel door locks to transit access to automotive control to payments. Establishing best practices for the implementation approach for non-payments use cases that leverage this contactless infrastructure could help to drive progress with OEMs and all NFC ecosystem participants.

The lack of standardization, RFID different standards and the lack of hardware interoperability is delaying the adoption of mobile ID in physical security. Not all the past problems have been solved specially in the physical security and access control integration where a large ecosystem of different vendors, protocols and standards needs to communicate, interoperate and integrate with the security enterprise platform being developed.

The lack of NFC capabilities on some smartphones, particularly the iPhone particularly the iPhone is delaying the Mobile ID integration with PACS. [80]

[80] *"Apple iPhone 7 "* NFCwold.com, *Downloaded on February, 2016 from* http://www.nfcworld.com/nfc-devices/apple-iphone-7/

"The NFC problem still has not been solved as Apple has not allowed third parties to use the NFC secure element, but the industry has got around this problem by moving towards Bluetooth Low Energy. The major challenge that will immediately affect the development of mobile credentials will be getting the compatible hardware installed as end-users can be reluctant to upgrade a reader part way through its lifecycle."[81]

- Alexander Derricott, market analyst, digital security and access control, HIS

The risk of approaching physical security as a silo is that one incident in one physical area can correlate to one or more incidents across the logical network, if we don't have converged visibility to physical and cyber threats we can waste efforts investigating one area that will be related to another incident. The physical space will continue to have a larger role within IT since access control can flag anomalies, which can create a chain reaction to protect intellectual property and other assets. This ability to flag anomalies will become even more powerful as mobile access adoption increases. Security integrators will be able to provide analytics generated from smartphones that are connected and always delivering important data throughout the infrastructure.

By combining logical and physical security we can really breakdown the silos and gain a complete visibility of what is happening in our environment, smart campus initiatives at Georgetown University is trying to close the gap by merging in a single enterprise solution the logical and physical security campus wide.

Although widespread adoption of mobile access solutions has failed to materialize as of yet in the enterprise sector, there is a total different reality on the Smart-Homes business where there is a big trend for smart-locks that allow people to access their homes through virtual keys on their smartphones and move through their environment in a way that hasn't been possible before, Mobile keys are becoming a mega trend globally[82]. Recently the bulk of the installations are

[81] Joel Griffin, "Roundtable: The state of mobile access control", Securityinfowatch.com, downloaded on July 20th, 2016 from http://www.securityinfowatch.com/article/12234552/roundtable-the-state-of-mobile-access-control

[82] Chong (2016),*"Top 4 Trends Shaping The Future Of Physical Security"* Vidsys article written by CEO, James Chong on SourceSecurity, from: http://www.vidsys.com/news/top-4-trends-shaping-future-physical-security-information-management-psim/

coming in the hospitality/resorts and residential markets. But also we expect that Universities will be early adopters as well, while SMEs and large enterprise continue to learn how to deploy the technology among existing workers most efficiently.

The solution blueprint proposed in this document is guided by the principles of openness, upgradability and interoperability. The proposed solution requires best practice design in three dimensions: First, strong encryption need to be implemented with unique cryptographic keys for each card, which only newer contactless chips built-in smart cards and smartphone with better processing power can provide. Second, strong key storage should be used to protect the critical master keys of the system, Lastly; all keys can be updated in response to incidents.

"A cryptosystem should be secure even if everything about the system,
except the key, is public knowledge"
– Kerckhoffs's principle

The lock should utilize the highest available encryption Standards. Thanks to the ingenious SRP authentication protocol security would be high, especially when comparing with other contemporary authentication protocols. It should be immune to most cryptographic attacks or they would at least take an unforeseeable amount of time to break. There are additional measures that can be taken that can make the system even more secure by using other cryptographic hash functions (SHA1, SHA254, SHA384) or varying the length of the cryptographic keys (1024/2048/4096 bits) this would theoretically make the system harder to break, but it would also increase the amount of data needed to be exchange, computational power and in extension lengthen the execution time of an authentication session. To increase the security even further, one could ask the user to enter the password at the beginning of every authentication attempt. This would mean that no password information have to be stored on the phone. As with all secure system it has to be peer review before anything definite can be said about how secure it is.

The authentication process should be as fast as possible. This is a very subjective parameter, but I would argue that anything less than half a second is considered to be reasonably fast as the

measured of result of response time showed in previous works (Saefulloh, Michrandi, Dirgantara, 2015)[83], based on the analysis and results of testing well below that half-second mark; therefore the system fulfills this parameter too.

The authentication process requires as little user interaction as Possible. The user does not need to do anything other than to unlock the mobile device. The Android background service will then automatically engage when the Reader sends the select message.

The lock should not require Internet access. This is a very important parameter consideration, because here is where the majority of the commercially available mobile access solutions on the market fail to meet, their agnostic RFID approach requires to connect online in order to bypass the mobile and the reader interoperability, but this a security flaw right at the RFID edge that totally defeat the purpose of a physical security system (PACS), By choosing to base the authentication protocol on SRP protocol, no Internet access is required. Many of the other researched authentication protocols requires a connection with a third-party server that is usually connected to the Internet. The ability to run the system in an offline environment enables deployment virtually anywhere and anytime.

The lock application should work on as many devices as Possible. This requirement was fulfilled when deciding to base the client side software on the Android OS, which has by far the largest global market share and based on the host card emulation (HCE) support. Ideally all major mobile devices should be supported.

15.0 Recommendations

This chapter outlines a typical migration path from existing industry standards to the best practice standard:

[83] Rochman Saefulloh Basyari, Surya Michrandi Nasution, Burhanuddin Dirgantara (2015), *"Implementation of Host Card Emulation Mode Over Android Smartphone as Alternative ISO 14443A for Arduino NFC Shield"*, International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)

The security of all popular access control cards including Mifare Classic, Legic Prime and HID Prox, has been shown to be weak. Businesses and Organizations using these cards now need to revise their risk analysis. The risk analysis typically leads to the need of upgrading and replacing the installed technology. They will consequently need a strategy for migrating to new access control architecture. In some cases, the best route is to deploy gradually, upgrading readers on a phased basis. In other cases, it is more economical to upgrade everything at once rather than dedicating the time and expense to evaluate each reader and panel and make a case-by-case decision.

15.1 Migration Target

Especially in large-scale installations, access cards and door controllers cannot be migrated all at once. Access cards must support two technologies for the duration of the migration. The two technologies can either be provided by a dual-antenna card that, hosts two independent chips. This option is needed for Legic Prime migrations since no other card is compatible with the lower levels of Legic Prime communications. For other card technologies, in particular Mifare Classic, the legacy card can be realized as an applet in a newer card, such as Mifare DESFire, Plus, or SmartMX.

For the time being it is difficult to implement a Legic Prime migration scenario in conjunction with the Mifare DESFire technology, since its relay/replay attack detection scheme leads to a high probability to be triggered when such a hybrid card is used in a Legic Prime environment. After a couple times of usage the Mifare DESFire chip reaches the upper limit for the attack detection counter and disables itself. To mitigate this, there exists a recommended special antenna layout to reduce the probability of triggering the false attack detection significantly. However, this problem does not apply to dual-antenna cards with Legic Prime/Mifare Plus and Legic Prime/SmartMX combinations.

15.2 Migration Dependencies

In higher education for example, access cards are often used to enable third party applications, such as cafeteria payment, proprietary RFID-based offline door cylinders not managed by the

online access control management system in Student dorms, billing systems, and locker keying for example. If an organization is migrating to a new card, these dependencies have to/need to be solved transparently to the user. In other words, the user should not need to care about the card generation and whether it is working for a specific application.

Typically, the additional functions of an access card are owned by third parties, which are independently organized and feel responsible for their own system only. From their point of view, the access card technology and data structure is considered as a steady foundation, which is never going to be changed. Thus, additional time for adjusting to the new technology must be given and a good rationale provided to get their support for a migration scenario. If it is necessary to replace the backend system due to a vendor or integrator change, a second layer of applications can have dependencies to those backend structures. An example is the integration with an ERP system, where external companies are paid according to polled time stamps of their access card usage for service functions.

Analyzing the data collected from the mobile GOcard pilot project, useful for metric and patterns of use and resenting it as a case study and comparing other case studies in higher education in order to create a migration strategy and model that can be used as a roadmap migration path.

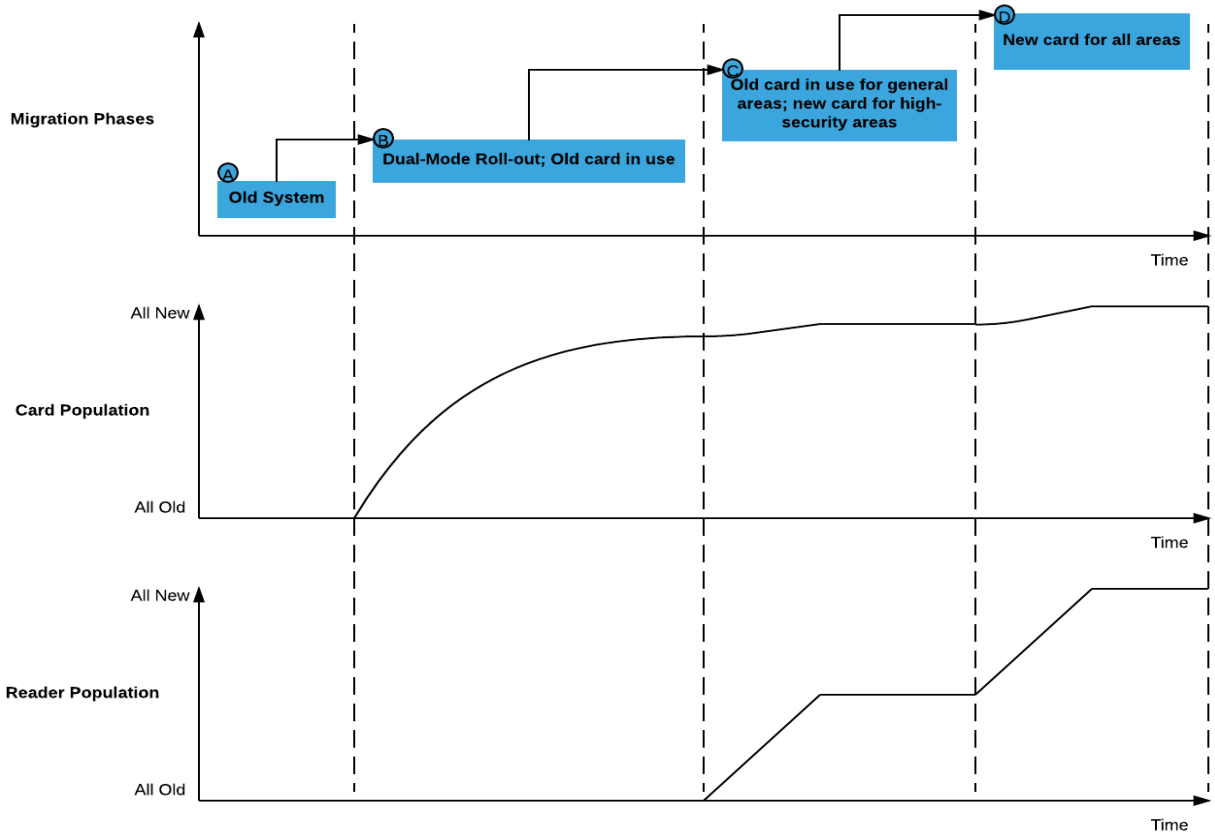

Figure No.11[84]

15.3 Migration strategy

A migration is typically executed in four phases as shown in Figure No.11 During the planning and preparation phase, **Phase A**, decisions on the new card layout, third party dependency issues, and a roll-out prioritization according to a risk assessment of access controlled areas are made. In addition, card production has to adapt the new technology to handle the dual interface cards (encoding) and incorporate the new credential management.

In **Phase B** a roll-out/card replacement with the new hybrid access card for all affected users of the access-controlled areas that are going to be upgraded next is performed. According to the

[84] Migration Strategy *"Cards and door controllers are upgraded to the secure target platform in four stages"* source: Preparred by the author

prioritization list of phase A, an access controlled area wise exchange takes place in **Phase C**. It is obvious that once an area is equipped with the new technology, door controllers should not grant access any more using the old (insecure) technology.

Phase D finalizes the migration by replacing the remaining door controller instances and stopping the production of hybrid access cards. All future access cards will not be equipped with the old RFID chip technology. Clearly, all dependent third party systems must have been transformed at this time to work with the new technology and card layout.

> "The technology and end-user understanding are ready for mobile credentials. The current projects are moving from the pilot stage to implementation. The feedback from the market suggests that more and more end-users are demanding the inclusion of this technology in their projects; maybe not for immediate use but as a way of future-proofing their systems"
>
> - **Alexander Derricott, market analyst, digital security and access control, HIS**

Another decision-making is whether to provision mobile access only to company-issued devices, or to support a Bring Your Own Device (BYOD) model, and how to do that. Many organizations have a mobile device management platform where corporate Apps are published and run in a specific container on the mobile device. Making sure the mobile access solution is interoperable with the Mobile Device Management (MDM) platform can make sense, especially if security settings are controlled by that platform.

16 Glossary

PACS	Physical access control systems
OTP	One time password
BYOD	Bring your own device
BLE	Bluetooth Low Energy
PIN	Personal Identification Number
NFC	Near Field Communication
BLE	Bluetooth Low Energy
RFID	Radio-frequency identification
OSDP	Open Supervised Device Protocol
SaaS	Software as a service
MiTM	Man-in-The-Middle type attack
DoS	Denial-of-Service Attack

MDM	Mobile Device Management
API	Application Programming Interface
SE	Secure Element (SIM Card)
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ISO	International Organization for Standardization
P2P	Peer-to- Peer
UID	Unique Identifier

17 Bibliography

[1]Meng, Wong, Zhou (2015)"*Surveying the Development of Biometric User Authentication on Mobile Phones*" IEEE Communication surveys & tutorials, Vol. 17, No. 3

[2]Corcoran, Costache (2016) "*Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts.*" IEEE Communication surveys & tutorials, 70 - 78

[3] Fine, Klym, Tavshikar & Trossen (2006). "*The Evolution& of RFID Networks."* Cambridge University Communications Research Network

[4] Diffie, van Oorschot, Wiener (1992, June) "*Authentication and authenticated key exchanges*" *Designs, Codes and Cryptography 2* (2), pp. 107Z125.

[5] Delfs, Knebl (2007). "*Introduction to Cryptography: Principles and Applications"* (2nd Edition ed.). Springer

[6] Alariki, Manaf, Khan (2016). *"A Study of Touching Behavior for Authentication in Touch Screen Smart Devices"* IEEE, 216 – 221

[7] Coskun, Ok & Ozdenizci (2012). "*Near Field Communication: From Theory to Practice.* Chichester: John Wiley & Sons Ltd

[8] Bianchin, Nathanson (2008). "*NEAR FIELD COMMUNICATION (NFC) I Emerging Market Analysis"* Automatic Identification and Data Collection Practice VDC Research Group, Inc

[9] Aura (1997) "*Strategies against replay attacks."* Computer Security Foundations Workshop, *10*, pp. 59 Z 68

[10] Francis, Hancke, Mayes & Markantonakis (2012). "*Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones"* London, UK: Royal Holloway University of London

[11] Cao, Yang (2010). *"A Survey of Identity Management Technology"* Information Theory and Information Security (ICITIS), 287 - 293

[12] Garcia, Rossum, Verdult & Schreur (2009) "*Wirelessly pickpocketing a Mifare Classic card*." In *Security and Privacy, 2009 30th IEEE Symposium on.* Berkeley: IEEE

[13] Haselsteiner & Breitfuß (2006) "*Security in Near Field Communication (NFC)."* Gratkorn, Austria: Philips Semiconductors

[14] Oechslin (2003) "*Making a Faster Cryptanalytic Time-Memory Trade-Of".* Lausanne, Switzerland: Ecole Polytechnique Federale de Lausanne.

[15] FFIEC (2001, August 8) "*Authentication in an Internet Banking Environment"*. Retrieved 2015, from ffiec.com: http://www.ffiec.gov/pdf/authentication_guidance.pdf

[16] Steiner, Tsudik & Waidner (1995, July). "*Refinement and extension of encrypted key exchange"*. *ACM Operating Systems Review ,29* (3)

[17] Ylonen (2006) "*The Secure Shell (SSH) Authentication Protocol".* Network Working Group of the IETF

[18] Wu (1998). "*The Secure Remote Password Protocol" Internet Society Network and Distributed System Security Symposium*, (pp. 97Z111) San Diego, CA

[19] Saparkhojayev, Dauitbayeva, Nurtayev, Baimenshin (2014). *"NFC-enabled access control and management system"* Web and Open Access to Learning (ICWOAL), 1 - 4

[20] Chattha (2014). *"NFC-enabled access control and management system"* Information Assurance and Cyber Security (CIACS), 35 – 38

[21] Mulliner (2009). *"Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones"* IEEE, 695 – 703

[22] Oh, Doo, Ko, Hong (2015). *"Countermeasure of NFC Relay attack with Jamming"* IEEE:Emerging Technologies for a Smarter World (CEWIT), 695 – 700

[23] Cavdar, Tomur (2015). *"A practical NFC relay attack on mobile devices using card emulation mode"* IEEE, 1308 – 1312

[24] Malone, Barkie, Fletcher, Wei (2013). *"Mobile Optimized Digital Identity (MODI): A framework for easier digital certificate use"* IBM Journal of Research and Development, 9:1 - 9:11

[25] Urien, Kiennert (2012). *"A New Keying System for RFID Lock Based on SSL Dual Interface NFC Chips and Android Mobiles"* IIEE, 42 – 43

[26] Gripentog, Kim (2015). *"Utilizing NFC to secure identification"* IIEE, 101 – 105

[27] Bellido, Canales, Cruz, Perez (2010). *"Universal Bluetooth Access Control and Security System for e-Keys Enviroments"* IIEE, 240 –250

[28] Dzurenda, Hajny, Zeman, Vrba (2015). *"Modern physical access control systems and privacy protection"* IIEE: Telecommunications and Signal Processing (TSP), 1 – 5

[29] Garcia, Gans (2008) "*Dismantling mifare classic*," *Secur.* pp. 97–114, 2008.

[30] Courtois (2009) "*The dark side of security by obscurity*," *Int. Conf. Secur. Cryptogr*

[31] M. Morbitzer, "*The MIFARE Hack"*

[32] Oswald and Paar (2011) "*Breaking MIFARE DESFire MF3ICD40: power analysis and templates in the real world*" Hardware Embedded. Systems

[33] Kasper (2011) "*Security Analysis of Pervasive Wireless Devices*" Bochum University

[34] Kasper, Von Maurich (2010) "*Cloning Cryptographic RFID Cards for 25$,"* Benelux Work

[35] *"Heart of Darkness - exploring the uncharted backwaters of HID iCLASSTM security."* Available: http://www.openpcd.org/images/HID-iCLASS- security.pdf. [Accessed: 17-Mar-2016].

[36] Garcia, Gans, Verdult, and Meriac (2012) *"Poster: Dismantling iClass and iClass Elite," cs.ru.nl*

[37] Indesteege, Keller, Dunkelman (2008) *"A practical attack on KeeLoq"* Adv. Cryptol

[38] Verdult, *"Dismantling Megamos Crypto : Wirelessly Lockpicking a Vehicle Immobilizer • Due to a recent injunction by the High."*

[39] Carolina and Paterson (2013) *"Megamos Crypto, Responsible Disclosure, and the Chilling Effect of,"* pp. 1–15

[40] Verdult, Garcia, and Ege (2013)*"Dismantling Megamos Crypto : Wirelessly Lockpicking a Vehicle Immobilizer,"* p. 91880

[41] Plötz and Nohl (2012) *"Peeling away layers of an RFID security system," Financ. Cryptogr. Data Secur.*

[42] Tembera and Novotn (2011)*"Breaking Hitag2 with reconfigurable hardware"* Euromicro Conf. Digit. Syst. pp. 558–563,

[43] Verdult, Garcia, and Balasch (2012) *"Gone in 360 seconds: Hijacking with Hitag2,"* 21st USENIX Conf

[44] Garcia, Rossum, Verdult, Schreur (2009). "*Wirelessly pickpocketing a Mifare Classic card*", In *Security and Privacy, 2009 30th IEEE Symposium on.* Berkeley: IEEE

[45] Coskun, V., Ok, K., & Ozdenizci, B. (2012). "*Near Field Communication: From Theory to Practice".*Chichester: John Wiley&Sons Ltd.

[46] Fine, C., Klym, N., Tavshikar, M., & Trossen, D. (2006). "*The Evolution of RFID Networks"* Cambridge University Communications Research Network.

[47] Vanderkay, J. (2004, March 18). *Nokia, Philips And Sony Establish The Near Field Communication (NFC) Forum*. Retrieved 2016, from NFC Forum: http://nfc-forum.org/newsroom/nokia-philips-and-sony-establish-the-nearfield-communication-nfc-forum/

[48] Swedberg, C. (2004, July 9). "*Developing RFID Enabled Phones"*. Retrieved 2016, from RFID Journal: http://www.rfidjournal.com/articles/view?1020

[49] Oechslin, P. (2003). *Making a Faster Cryptanalytic TimeIMemory TradeIOf.* Lausanne, Switzerland: Ecole Polytechnique F´ed´erale de Lausanne.

[50] Schneier, B. (1996). *Applied Cryptography* (2nd Edition ed.). John Wiley and Sons.

[51] Steiner, M., Tsudik, G., Waidner, M. (1995, July). Refinement and extension of encrypted key exchange. *ACM Operating Systems Review , 29* (3).

[52] Cisco. (2006, January 19). "*Kerberos Overview I An Authentication Service for Open Network Systems"*. Retrieved 2015, from Cisco.com: http://www.cisco.com/c/en/us/support/docs/securityZvpn/kerberos/16087Z1.html

[53] Ylonen, T. (2006). *The Secure Shell (SSH) Authentication Protocol.* Network Working Group of the IETF.

[54] Zhou, Y., & Feng, D. (2005). "*SideIChannel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing".* Institute of Software, State Key Laboratory of Information Security. Beijing, China: Chinese Academy of Sciences.

[55] Ahson, S. A., (eds), M. I. (2012). "*Near Field Communications Handbook" .* Auerbach Publications.

ISO/IEC. (2008). *ISO/IEC 14443I1:2008 Identification cards II Contactless integrated circuit cards II Proximity cards II Part 1: Physical characteristics.* Geneva, Switzerland: International Organization for Standardization.

ISO/IEC. (2010). *ISO/IEC 14443I2:2010 Identification cards II Contactless integrated circuit cards II Proximity cards II Part 2: Radio frequency power and signal interface.* Geneva, Switzerland: International Organization for Standardization.

ISO/IEC. (2011). *ISO/IEC 14443I3:2011 Identification cards II Contactless integrated circuit cards II Proximity cards II Part 3: Initialization and anti-collision.* Geneva, Switzerland: International Organization for Standardization.

ISO/IEC. (2008). *ISO/IEC 14443I4:2008 Identification cards II Contactless integrated circuit cards II Proximity cards II Part 4: Transmission protocol.* Geneva, Switzerland: International Organization for Standardization.

ISO/IEC. (2013). *ISO/IEC 15693:2013 Information technology II Telecommunications and information exchange between systems II Near Field Communication II Interface and Protocol (NFCIPI1).* Geneva, Switzerland: International Organization for Standardization.

Additional Sources (Business Articles, Case studies, whitepapers, press releases)

Gomes (2015). *"Tech giants bet on biometrics"* IEEE Spectrum, 52-55

"*Why Mobile Will Transform Enterprise Authentication*" Entrust, Inc. 2015. *Downloaded on December 21, 2015 from* https://www.entrust.com/wp-content/uploads/2015/07/6256-EntrustWP-5Reasons-DataCard_WEB4.pdf

" *Mobile Security Solutions: Securing & Leveraging the Mobile Enterprise* " Entrust, Inc. 2013. *Downloaded on December 21, 2015 from* http://img.en25.com/Web/EntrustInc/%7Bfccc1e3a-6c18-47d9-9fab-ae2508facd63%7D_24317_DS_MobileSecurity_web_Feb13.pdf?utm_campaign=&utm_medium=email&utm_source=Eloqua&elqCampaignId=

"*Enterprise Security Guide*" *Microstrategy Usher*, 2015. *Downloaded on December 21, 2015 from* http://www.usher.com/Usher/media/documents/guides/enterprise-security.pdf

"*Enterprise security: tradeoffs, trends, a key dynamics*" Microstrategy Usher, 2015. *Downloaded on December 21, 2015 from* http://www.usher.com/Usher/media/documents/white-papers/enterprise-security.pdf

"*UIS introduces LiveSafe, Usher, and Campus Quad mobile apps to campus.*" *Georgetown Voice*. January 2015. Downloaded on January 5th, 2016 at http://georgetownvoice.com/2014/09/04/uis-introduces-livesafe-usher-and-campus-quad-mobile-apps-to-campus/

"Using Usher at Georgetown" *University Information Services*. Downloaded on January 6th, 2015 from http://uis.gudrupalstg.georgetown.edu/accounts/usher-faq#Who2

"Usher One, Usher All." *The Hoya*. January 7, 2015. Downloaded on January 5th, 2016 from http://www.thehoya.com/usher-one-usher/