DESIGN OF A CONTEXT AWARE SECURITY MODEL FOR PREVENTING RELAY ATTACKS USING NFC ENABLED MOBILE DEVICES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS OF
THE MIDDLE EAST TECHNICAL UNIVERSITY
BY

DAVUT ÇAVDAR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

JULY 2020

Approval of the thesis:

DESIGN OF A CONTEXT AWARE SECURITY MODEL FOR PREVENTING RELAY ATTACKS USING NFC ENABLED MOBILE DEVICES

Submitted by **DAVUT ÇAVDAR** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Information Systems Department, Middle East Technical University** by,

Prof. Dr. Deniz Zeyrek Bozşahin
Dean, **Graduate School of Informatics** ____________________

Prof. Dr. Sevgi Özkan Yıldırım
Head of Department, **Information Systems** ____________________

Assoc. Prof. Dr. Aysu Betin Can
Supervisor, **Information Systems, METU** ____________________

Dr. Emrah Tomur
Co-Supervisor, R&D, **Ericsson** ____________________

Examining Committee Members:

Assoc. Prof. Dr. Altan Koçyiğit
Information Systems, METU ____________________

Assoc. Prof. Dr. Aysu Betin Can
Information Systems, METU ____________________

Prof. Dr. Ece Güran Schmidt
Electrical-Electronics Engineering, METU ____________________

Assoc. Prof. Dr. Ahmet Burak Can
Computer Engineering, Hacettepe University ____________________

Assoc. Prof. Dr. Ihsan Tolga Medeni
Management Information Systems,
Ankara Yıldırım Beyazıt University ____________________

Date: **10.07.2020**

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Davut ÇAVDAR

Signature :

ABSTRACT

DESIGN OF A CONTEXT AWARE SECURITY MODEL FOR PREVENTING RELAY ATTACKS USING NFC ENABLED MOBILE DEVICES

Çavdar, Davut
Ph.D., Department of Information Systems
Supervisor: Assoc. Prof. Dr. Aysu Betin Can
Co-Supervisor: Dr. Emrah Tomur

July 2020, 135 pages

Near Field Communication (NFC) is a promising communication technology used in smart mobile devices. As an effective and flexible communication technology, NFC is frequently used in innovative solutions nowadays such as payment, access control etc. Because of the nature of these transactions, security is an important issue since NFC is used in critical applications such as payment and access control. There are several attacks mentioned in literature against NFC-enabled applications, yet, none of the security solutions offered provides sufficient protection for NFC enabled access control systems due to their static nature. In this context, the contribution of this work is threefold. First, we demonstrate how easy to perform such attacks implementing a relay attack in a realistic testbed. Second, we propose a context-aware security model for preventing relay attacks for NFC enabled mobile devices even if attackers compromise authentication tokens. Third, we prove the validity of our proposed security model both theoretically by formal verification and practically by the deployment of the model on a testbed infrastructure where we also analyze the performance in comparison to other approaches.

Keywords: NFC, Relay Attack, Access Methods, Security, Context-Aware

ÖZ

NFC ÖZELLİKLİ MOBİL CİHAZLARIN KULLANILDIĞI RELAY SALDIRILARINI ÖNLEYEN BAĞLAMA DUYARLI BİR GÜVENLİK MODELİNİN TASARIMI

Çavdar, Davut
Doktora, Bilişim Sistemleri Bölümü
Tez Yöneticisi: Doç. Dr. Aysu Betin Can
Ortak Tez Yöneticisi: Dr. Emrah Tomur

Temmuz 2020, 135 Sayfa

Yakın Saha İletişimi (NFC) akıllı mobil cihazlarda kullanılan ve gelecek vadeden bir iletişim teknolojisidir. Etkili ve esnek bir iletişim teknolojisi olarak, NFC günümüzde, ödeme, erişim control sistemleri vb. Çözümlerde sıklıkla kullanılmaktadır. Bu işlemlerin doğası gereği, NFC kritik uygulamalarda kullanıldığı için, güvenlik önemli bir konu hale gelmektedir. Literatürde NFC kullanan uygulamalara karşı çeşitli saldırılardan bahsedilmiş olmasına karşın, sabit yapısından ötürü, önerilen çözümlerden hiçbiri NFC kullanan erişim kontrol sistemleri için yeterli koruma sağlamamaktadır. Bu bağlamda, bu çalışmanın temel katkısı 3 aşamalıdır. İlk olarak, gerçek bir test ortamında, relay saldırısının kolaylıkla nasıl gerçekleştirilebildiğini gösteriyoruz. İkinci olarak, saldırgan yetki anahtarına sahip olsa dahi relay saldırısını önleyen bağlama duyarlı bir güvenlik modeli öneriyoruz. Üçüncü olarak ise, modelimizin geçerliliğini, teorik formal doğrulama yaparak, pratik olarak da performansını diğer yaklaşımlarla kıyasladığımız gerçek bir ortam üzerine yükleyerek ispatlıyoruz.

Anahtar Sözcükler: NFC, Ortadaki Adam Saldırısı, Erişim Modelleri, Güvenlik, Bağlama Duyarlı

To my wife, Şeyma,
To my son, Umut,
To my mother and father.

ACKNOWLEDGMENTS

First of all, I would like to thank my co-supervisor, Dr. Emrah Tomur, for his endless support, motivation, valuable guidance, and encouragement. Also, I want to thank my supervisor Assoc. Prof. Dr. Aysu Betin Can for her technical support in my studies. I appreciate and never forget their supports during my hard times.

I also thank my thesis monitoring committee members, Assoc. Prof. Dr. Altan Koçyiğit and Prof. Dr. Ece Güran Schmidt, for their valuable feedbacks. Also, I want to thank Prof. Dr. Semih Bilgen especially for his motivation at the beginning of my study.

I would like to thank the examining committee members, Assoc. Prof. Dr. Ahmet Burak Can and Assoc. Prof. Dr. Ihsan Tolga Medeni for their valuable feedback and contributions.

I acknowledge the support of The Scientific and Technological Research Council of Turkey (TÜBITAK) BIDEB for 2211 graduate student fellowship during my Ph.D. education.

I also thank Dereağzı Cilt Evi for their support in the printing of the thesis in a limited time.

I thank Özge, Samet, Burak, Üzeyir, Uğur, Onur, Oğuzhan and Ahmet Oguz for your friendship and support.

I would like to thank my mother and father for their endless support. They are always with me in my hard times.

I thank my little son, Umut Berk Çavdar. He is medicine of my wounds and his smiles keep me stronger.

Lastly, I would like to thank my dear wife, Şeyma Çavdar, for her encouragement and continues support. I feel always her love with me. Thank you, my sweet family, I love you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ASK	Amplitude Shift Keying
CSC	Context Sensitive Controls
DAC	Discretionary Access Control
DOS	Deny of Services
DPC	Dynamic Policy Controls
EMV	Europay MasterCard Visa
FWT	Frame Waiting Time
GRBAC	Generalized Role-Based Access Control
HCE	Host Card Emulation
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LLCP	Logical Link Control Protocol Specification
MAC	Mandatory Access Control
MITM	Man in the Middle Attack
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
PCE	Pervasive Computing Environments
PSK	Phase Shift Keying
RBAC	Role Based Access Control
REST	Representational State Transfer
RTD	Record Type Definition
SE	Secure Element
T-CAC	Threshold Based Collaborative Access Control
TRBAC	Temporal Role-Based Access Control

CHAPTER 1

INTRODUCTION

The popularity and usage volume of smart mobile devices have exponentially increased in the last decade. The main reasons for this situation are the functionality and convenience of mobile devices. Mark Weiser [1] described this age as the third era of computing in which electronic devices are smaller and able to interact with other devices. This era also named as "Ubiquitous Computing" or "Pervasive Computing". In this stage, standard computer perception changes in both appearance and logic.

Device diversity increased with the needs of humans for daily life activities. Besides standard computers, mobile devices, sensors, actuators etc. have started to be used by humans in daily life. The major contribution of ubiquitous computing emerges in the interaction of these devices. Unlike standard devices, these ubiquitous computing devices have effective interaction capabilities with both human and other electronic devices.

In the last decade, the communication and lifestyle of people have completely changed. People have started to use smart mobile devices for their daily routines such as mailing, dealing with documents, entertaining etc. As a result of this situation, production and sales of smart mobile devices, mobile operating systems, mobile marketing and mobile solutions have extremity increased. According to research conducted by Collins [2], there are 7.3 billion mobile devices in the world, which exceeds the world population. These numbers also show the impacts of the mobile ecosystem.

Near Field Communication (NFC), technology is one of the communication conveniences that emerge from mobility tendency and device interaction concept. The main function of NFC is to establish a connection between two mobile devices or NFC tags and reader. Data exchange or access requests can be easily performed with this concept. The detail of this communication process is described in Chapter 3.

NFC enabled smart mobile devices are used in daily applications and create smart solutions. These solutions are summarized in Figure 1[3]. For example, NFC technology is used in contactless payments, which are also the most popular NFC applications, loyalty couponing, transport systems (bus, train etc.), data exchange, gaming, location-based services and access control systems.

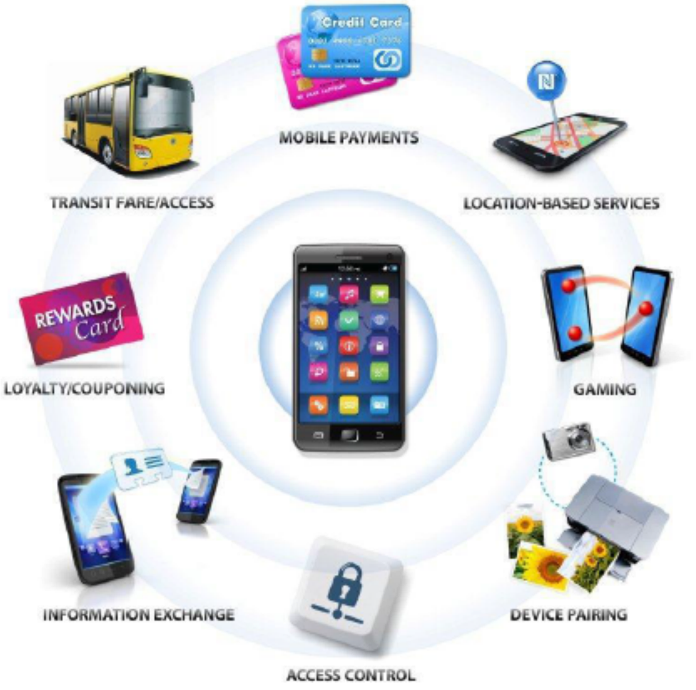


Figure 1: The Ecosystem of NFC Based Solutions [3]

Although used in critical and data sensitive solutions for quite a period, security issues in NFC technology are not completely solved and standardized yet. NFC technology is introduced with RFID ISO/IEC 14443 “Contactless Proximity Smart Cards and their technical features” standard. Although, it was standardized as ISO/IEC 18092 “Near Field Communication Interface and Protocol (NFCIP-1)” and then ISO/IEC 21481 “Near Field Communication Interface and Protocol (NFCIP-2)”, majority of NFC principles and functions are still inherited from RFID standards. Although the NFC Forum has released even NDEF and RTD based standards, security requirements and standards are not discussed. This eventually causes misconceptions in security issues of mobile solutions.

NFC enabled mobile devices to come into use in access control systems instead of using a passive card, however in the literature, the majority of studies discuss finding solutions for avoiding passive card relaying attack. Because of its complexity in comparison with passive cards, mobile devices are exposed to security attack more frequently, however, they are more powerful and flexible device and provides a more suitable environment for security solutions.

Although some partial solutions are offered, they are not applicable for NFC based access control systems working on the application layer. In former access control systems ISO/IEC 14443, based passive cards are used instead of smart mobile devices in mobile payment and access control applications. Because of their limitations, attackers, especially in relay attacks, misuse security gaps of passive cards. Also, in the literature, studies, which are discussed in Chapter 3, proved the applicability of relay attacks on passive cards.

According to the gaps in the related studies about offering a complete application-level solution to relay attacks in mobile communication environments, we have defined below objectives:

- To identify current vulnerabilities for NFC communication environment and analyze effects of them to relay attack occurrence.

- To define system requirements that can be input to our context aware security model.

- To design and build a dynamic context aware security model to prevent relay attacks in NFC enabled mobile phones.

- To provide formal and mathematical verification of the model.

- To implement a complete solution including infrastructure and mobile application in order to prove practicability of the relay attacks in the domain also apply and test the model on it.

1.1. Research Questions

In order to address the below research objectives, we have focused following research questions:

1. What are the possible vulnerabilities for NFC communication environment?

2. What are the system requirements and how can we define them properly for our context-based security model?

3. Can we prove and simulate the practicability of the relay attack in NFC communication?

4. How can we design and build a dynamic context aware security model to prevent relay attacks in NFC enabled mobile phones?

In this thesis, we have performed four tracks of studies in order to cover above research questions.

In the first study, we investigated possible vulnerabilities in the NFC environment. In addition to the vulnerabilities inherent in NFC, typical vulnerabilities found in wireless communications have been identified.

Interactions of these vulnerabilities with each other are also explained. In particular, vulnerabilities that could affect the occurrence of relay attacks were analyzed. For the second study, basic system requirements that should be met for our context aware security model are provided. They are explained in the Chapter 5 in detail. In order answer to the third question, a complete solution is developed including services, infrastructure, mobile application etc. With the help of this developed solution, firstly, it was simulated and proved the practicability of the relay attack in NFC communication environment. In addition to that, our model is applied on this implementation and performance tests are performed using this implementation.

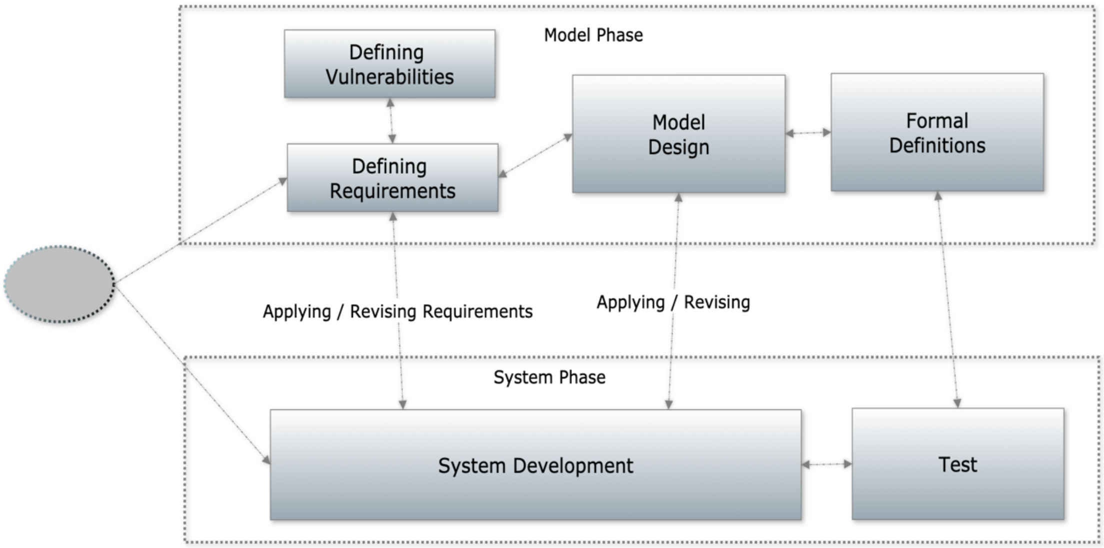


Figure 2: General Components of the Thesis Study

About the fourth question, the studies are performed in two parallel framework formats. The one is designing of conceptual security model; the other one is developing NFC based access control system and testing that security model on it. The design of security model phase consists of “Defining Vulnerabilities”, “Defining Requirements”, and “Model Design” and “Formal Definitons” sub modules. The system phase consists of “System Development” and “Test” sub modules. Because of performing parallel development of conceptual model design and system, both development phases interact each other in case of any need. The interactions between two development frameworks of our study are illustrated in Figure 2.

1.2. Contributions of the Study

The main contributions of the thesis study are:

- System-level security requirements are offered for NFC communication.
- Relay attacks in NFC enabled mobile devices is practically proved. The experience and output are used in model design and development.
- A dynamic, adaptive and context aware security model extending Role Based Access Control (RBAC) is designed to prevent relay attacks in NFC enabled mobile devices.
- The concepts of formal and mathematical verification for a context aware security model are offered.

1.3. Thesis Organization

This thesis study consists of eight chapters:

Chapter 2 presents related studies in the literature discussing the three domains, which are NFC, Access Control System and Security.

Chapter 3 describes the basics, principles, components of the NFC ecosystem.

Chapter 4 introduces practical relay attack scenario in NFC enabled mobile device and its implementation.

Chapter 5 offers dynamic, adaptive and context aware security model to prevent relay attacks in NFC enabled mobile devices.

Chapter 6 presents the formal and mathematical verification of the model.

Chapter 7 describes a complete implementation of NFC based access control system implementation, covering all high-level use case combinations and the results of performance tests of the proposed model.

Chapter 8 concludes the study with a general summarization and possible future works.

CHAPTER 2

RELATED WORK

2.1. Introduction

In this section, related studies in the literature are provided. In the first part, the studies, which describe practical relay attacks in NFC environment, are provided. We have also designed and implemented a relay attack to show the applicability and feasibility [4]. This implementation is explained in the Chapter 4 in detail. The second part presents the offered solutions for preventing relay attacks in the literature and explains why they are not suitable in terms of used methodology and their approaches.

We aim to research on three domains, which are NFC, Access Control System and Security. The researches, studies, implementations and performance analysis are narrowed and conducted on these three domains.

The Near Field Communication (NFC) technology is relatively new technology; it is introduced within the current decade [5]. The first versions of related standards have been released in the last years by NFC Forum and ISO [6] and after these developments, device manufacturers have started to develop more NFC devices.

In the market, many NFC solutions are conducted over the world, especially for mobile payment systems. All trials indicate the fact that with the development of NFC technology, mobile phone is subject to become safer, more convenient, speedier and more fashionable physical device.

Also, in parallel with developments, academic studies have started in the last years; however, there are limited number of research and articles. Also, the major problem for NFC literature is that; the conducted researches only mentions general NFC ecosystem and probable security vulnerabilities for NFC applications in a survey format.

In [7], an NFC based payment system was proposed for mobile phones. Communication between mobile operator and bank were conducted according to ECC principles, however, other aspects of important components such as mobile device secure element security were not discussed. Similar studies are conducted in [8] and [9] where RTD standard based certificates were described with ECC cryptographic principles in [8] and public, private key methodology with ECC cryptographic principles are discussed in [9], however other security aspects of important components were not discussed similar to [7].

Smart token-based access control system was offered in [10]. Mobile phone stores token data instead of acting real requester and uses them for accessing sources. They offered Kerberos based key management systems; however, they did not offer any precautions against relay attack. In addition, an access control study for cars was conducted in [11] by same researchers with the same methodology.

[12] implemented a simulation environment to analyze Relay Attacks on different distances and tried to answer what extent a relay attack can be evaluated on an NFC mobile device. However, they did not offer a solution for prevention.

Some security aspects were covered for NFC-enabled contactless payment systems in [13] such as inconsistency in resolving card collision, vulnerability to relay attacks, token implementation vulnerabilities, tradeoffs between Host Card Emulation and Secure Element-enabled Mobile Wallets.

Not only in payment solutions but also in access control systems, NFC based mobile devices are used to gain access to resources. Divya et al. [14] give a survey on various mechanisms of automatic identification and access control that have been used over the years to avoid unauthorized access. They also explained NFC based access control system including locking device, an (NFC) Near Field Communication device, a microcontroller and mobile application to show applicability of NFC in access control systems.

Chainan et al. [15] proposed an attendance application includes many essential operations, such as captured attendance records using NFC, automated time measurement, leave and overtime check-in, assessment of working hours, access to information modified in real time, and report generation. The proposed program also provides online platform that allows multiple company user accounts to be installed, needs no special software, and offers more accessible data storage. They also proved the flexibility of NFC usage in access control systems.

Wu et al. [16] presented a detailed review of the current Implantable medical devices (IMD) protection literature, focusing on control schemes to prevent unauthorized control. They also underlined that NFC based access control systems can be used in various areas.

2.2. NFC Security

General security vulnerabilities of NFC ecosystem such as eavesdropping and data modification and detection methods for these weaknesses were discussed in [17]. Similarly, general security features of NFC devices were described in [18]. Other security problems in NFC communication, namely, data corruption using jam signaling methods and their effects were discussed in [19].

[20] described also common vulnerabilities of NFC communication such as Eavesdropping, Transmission Interference and Data Distortion. Also, it offered old-fashioned strategies such as Encryption, QoS-Based Transmit

Beam forming and Faraday Cage. They were also discussed in our study and not suitable solutions mobile communication environment especially NFC.

Giese et al. [21] constructed an attack to mobile-based NFC payment systems by creating a wormhole so that they were able to make payment with a card which was in totally different location. They tested their attack with both contactless credit card and mobile payment applications Apple Pay and Google Pay. Based on their experiments, they concluded that card skimming or wormholes can breach magstripes and NFC security methods.

Singh et al. [22] investigated the NFC vulnerabilities which cause security and privacy attacks such as DOS and data corruptions. The main significant outcome of the study is presenting a ranking among several security attacks using CVSS framework and AHP model so that they provide a guideline for dealing with attacks at the highest risk. Based on their results, the best methods are ECC and AES algorithms for establishing a secure channel and preventing data corruption and DOS in NFC.

Micallef and Markantonakis [23] presented potential risks related to using smartphones in contactless payment transactions. They suggest researchers and industry to be more aware of the risks of host card emulators (HCE) which are commonly used by consumers for making payments. They recommend guaranteeing the same security level for HCE as the security provided by a physical card.

Al-Haj and Al-Tameemi [24] offered a new protocol for enhancing the security of the messages transmitted in the EMV protocol. Their solution mainly adds a new security level named "Management Authentication Server (MAS)". They showed that the protocol is able to prevent malicious network attacks.

Sethia et al. [25] introduce a novel framework for NFC secure element-based mutual authentication and attestation using Host Card Emulation (HCE) mode. They present the protocol's informal and formal security analysis with the Real-Or-Random (ROR) model.

Yan et al. [26] introduce a fingerprint authentication technique for NFC devices based on hardware differences. It includes obtaining analog signals, preprocessing data, extracting features, establishing model, and detecting an attacker device while NFC device transmits information. The simulation has an inherent complex mechanism so that the hardware intrinsic information becomes difficult for imitation. Their results show that the method has high precision and recall rate.

Kaur et al. [27] assessed three Android e-wallet applications of Canadian banks and compared them with the Android Pay. Based on their findings, the e-wallet applications in the market have security vulnerabilities regarding trivial attack vectors. They suggest a number of security recommendations based on the CBA security guidelines and the OWASP Top 10 Mobile Risks.

2.3. NFC Relay Attacks

Following the increase in the usage of NFC in payment solutions, trials of practical attacks on such critical applications started to be covered in literature [28] [29] [30]. These research works demonstrate the applicability and feasibility of security attacks against NFC-based systems, especially in the mobile payment domain. Although they demonstrate the security problem usually in the form of relay attack for NFC, these works mostly mention only security gaps and how they exploited these gaps. However, solutions to such security vulnerabilities have not been much offered in the literature.

Implementations of NFC relay attacks were conducted successively in [31] and [29]. Mobile application that installed on mobile device were used in the implementation, however, no security precautions were discussed in the study [31]. In the studies [28], [30] and [32], ISO/14443 based RFID cards were exposed to relay attack and successively relayed.

Forrester et al. [33] developed simulations of attacks on different proximity relay ranges confirming how easy it is to compromise these mobile payment devices by means of eavesdropping, and intentionally forcing unauthorized access to the point where their findings question the ISO 14443 standard concept of NFC ranges as counter-intuitive.

Jumić et al. [34] evaluate state-of-the-art NFC payment technology. Also, they assess emerging threats and seek to decide whether users are protected from such attacks.

Dang et al. [35] proposed and developed an attack on AFC cards that allows an attacker to top up his positive identification and acquired a refund also discussed possible countermeasures to defend against these attacks.

Akter et al. [36] successfully set up MITM attacks. Their physical foundations of the attack, technological architecture, and effective implementation results are discussed. They also present practical results on how a malicious user can leverage our MITM attack to compromise the security of contactless payment transactions.

Tu and Piramuthu [37] present an overview of RFID relay attacks and evaluate different research streams which have tried to deal with these attacks. Also, they evaluate distance bounding techniques and the implementation, with a special focus. Based on these evaluations, they summarize selective ambient condition-based solutions against RFID relay attacks.

2.4. Sensor Usage in NFC Transactions

In order to detect contextual changes and prevent unauthorized access, information gathered from sensors is used in the studies and solutions. Also, our proposed model uses contextual information retrieved from sensors.

A similar study was conducted in [38]. They simply performed an evaluation of mobile phone sensors as a potential relay attack countermeasure for payment solution in the research study [39]. They analyzed 12 sensors of mobile device but found five of them meaningful for this use. They found certain maximum time limitations for NFC operation to prevent relay attack.

Shepherd et al. [40] analyzed several contextual attributes for their applicability to indicate proximity in NFC payment transaction. The examined attributes were acceleration, Bluetooth, gravity, GPS, gyroscopic readings, magnetic fields, pressure, sound, WiFi, light, temperature, humidity and more.

Ma et al. [41] showed how location related data can be used to determine the proximity of two NFC mobile phones, namely using the GPS (Global Positioning System).

Halevi et al. [42] proved ambient sound and light suitability for proximity detection. The authors evaluate measurements obtained for 2 and 30 seconds periods for light and audio using a variety of comparison algorithms for similarity, respectively.

Truong et al. [43] evaluated four separate sensors over 10-120 second recording durations. Given the positive outcomes, such a long recording time renders them unsuitable for practical mobile transactions based on NFCs.

Shrestha et al. [44] used custom-made hardware known as Sensordrone, with a number of ambient sensors but with no evaluation of the generic ambient sensors available on commercial handsets, did not include the sample period and only stated that data was collected from each sensor for a few seconds.

2.5. Offered Solutions for Relay Attacks

As countermeasures, distance bounding protocols and using Frame Waiting Time were offered in [28] and [30], however they could not provide sufficient security for relay attack as explained in the below.

In the ISO/14443 standard, Frame Waiting Time (FWT) is defined for standard smart card and reader communication. FWT variable defines maximum response time after the end of the reader's data. FWT is defined as (256 · 16/ fcarrier)×2FWI , where FWI is a value from 0 (FWT = 300 μs) to 14 (FWT = 5 s) with a default of 4 (FWT = 4.8 ms). Control of this variable was offered in the literature for avoiding relay attack in [28] and [30]. Attacker can modify this variable or some additional readers may be placed between reader and card in order to overcome this variable. However, the main reason of its unsuitability is different mobile devices are used in the proposed model instead of smart cards and when a relay attack occurred, only NFC based mobile phones communicate with each other. There are no timing limitations between communication of two NFC based mobile phones, because these de-vices are active and it is different than the cases in the ISO/14443 based passive cards. Therefore, this problem needs to be solved with application layer security methods.

Location based control was also offered as another countermeasure in [30] and [45]. Distance-bounding protocols use FWT values for calculating round trip time and finally comment on requester's location. As it was already mentioned, using FWT is not suitable solution for avoiding relay attack especially where NFC enabled mobile device are used.

Drimer and Murdoch [46] offered a calculation of distance bounding security method for relay attacks based on smart cards, in particular for Chip and Pin payment cards (EMV). Based on these tests, it measures round trip times according to low level signal transmissions and attempts to detect relay attacks.

Infrared Light was offered as a countermeasure for preventing Relay Attacks in mobile transactions in [47]. Proposed solution was implemented on six different test beds, but it was found that solution is strictly dependent on infrared sensor, i.e., hardware and therefore very hard to use in general.

Chabbi et al. [48] presented an authentication protocol involving a server, a reader and an NFC Smartphone capable of capturing and converting the user iris to a secret key. Also, they performed intrusion tests to inform the cell phone's owner of attacks in order to determine the efficiency of the protocol. On the other hand, in this approach, mobile devices may not detect iris all the time because of lack of visibility also some additional processing time may be needed causing the operational problems.

Imran et al. [49] offered that Markov Chain may detect the relay attack on payment solutions using the principles of the chain, and the evaluation shows that in the case of electronic payment the Markov chain is successful in detecting anomalies in relay attacks. Consequently, they suggested that the Markov chain algorithm could also be used as a protection against an attack in NFC payment. On the other hand, although Markov chain provides suitable solutions based on the trained data, it still works on estimation approach, therefore it is risky to use it in the access control systems.

Anggoro et al. [50] proposed a method using symmetric cryptography to deliver a more accurate detection protocol against threats in mobile NFC payment applications. The method was initially implemented on wireless short-range communication using Secure Element (SE) of mobile device. Creating, encrypting and controlling of certificates were performed in the SE. However, this approach addresses low-level operations in NFC transactions. Host Card Emulation (HCE) mode enables relay attacks in application level passing all controls in low-level.

Gurulian et al. [51] conducted an analysis using sensor data obtained from 17 sensors from a test platform for an emulated relay attack to determine whether they could effectively counteract these attacks. Each sensor, where possible, was used to record legitimate 350-400 and relay (illegitimate) contactless transactions at two distinct physical sites. The research offered experimental results from which to assess the effectiveness of ambient sensing to provide a powerful anti-relay mechanism in applications that are sensitive to protection. Also, it is demonstrated that, under practical implementation environments, no single sensor evaluation is suitable for the security critical applications. In other words, raw sensor data should be analyzed and interpreted in a complete security model instead of standalone usage.

Li et al. [52] adapted the time-bound approach to detect relay transactions and present a quantitative estimate of normal transactions versus relayed transactions. A mobile prototype framework was also developed to demonstrate the feasibility of their proposed method.

Table 1: The Summary of Offered Solutions Against NFC Relay Attacks.

Studies	**Solution**	**Key findings**
Dullink et al. [28] Francis et al. [30] Li et al. [52]	Using Frame Waiting Time (FWT)	Frame Waiting Time (FWT) variable defines maximum response time after the end of the reader's data. Control of this variable was offered for avoiding relay attack.
Drimer et al. [46]	Distance Bounding Algorithm	Distance-bounding protocols use FWT values for calculating round trip time and finally comment on requester's location.
Gurulian et al. [47]	Using Infrared Light	Infrared Light is offered as a countermeasure for preventing Relay Attacks in mobile transactions. Infrared light is sent from mobile device and retrieved by reader during access request.
Chabbi et al. [48]	Converting User Iris to Secret Key	Smartphone captures and converts the mobile device user's iris to a secret key and sends that secret key within the request to the reader.
Imran et al. [49]	Markov Chain Estimation	Request is evaluated and classified according to Markov Chain algorithm based on prior trained data.
Anggoro et al. [50]	Using Symmetric Cryptography	Security certificates are created using symmetric cryptography. Creating, encrypting and controlling of certificates were performed in the Secure Element (SE) of mobile device.
Gurulian et al. [51]	Using Sensor Data	Sensor data obtained from 17 sensors from a test platform and emulated relay attack based on that data to determine whether they could effectively counteract these attacks. Finally stated that, no single sensor evaluation is suitable for the security critical applications.

Table 2: The Comparison of the Main Features of the Proposed Solutions

	M-CARBAC	Dullink et al. [28] Francis et al. [30] Li et al. [52]	Drimer et al. [46]	Gurulian et al. [47]	Chabbi et al. [48]	Imran et al. [49]	Anggoro et al. [50]	Gurulian et al. [51]
NFC Transactions	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Device Usage	✓	✓	✗	✓	✓	✗	✗	✓
Access Control Methodology	✓	✗	✗	✗	✗	✗	✗	✗
Sensor Data Usage	✓	✗	✗	✓	✓	✗	✗	✓
Context Awareness	✓	✗	✗	✗	✗	✗	✗	✗
Dynamic Adaptation	✓	✗	✗	✗	✗	✗	✗	✗
Implementation & Test	✓	✓	✓	✓	✓	✗	✗	✗
Formal Validation	✓	✗	✗	✗	✗	✗	✗	✗
Prevention of Relay Attacks in Application Layer	✓	✗	✗	✗	✗	✗	✗	✗
Proposed as a Complete Security Model	✓	✗	✗	✗	✗	✗	✗	✗

As explained in this section, most of the research works on NFC security describe potential vulnerabilities and threats, show practical attacks, compare effectiveness of existing countermeasures and offer low level solutions such as using Frame Waiting Time (FWT), distance bounding protocols, infrared light, converting iris image to encrypted key, using symmetric cryptography and evaluating raw sensor data retrieved from mobile device , however, they do not offer a complete ,context aware and dynamic security solution for NFC relay attacks. These proposed solutions are summarized in the Table 1 and 2 above.

CHAPTER 3

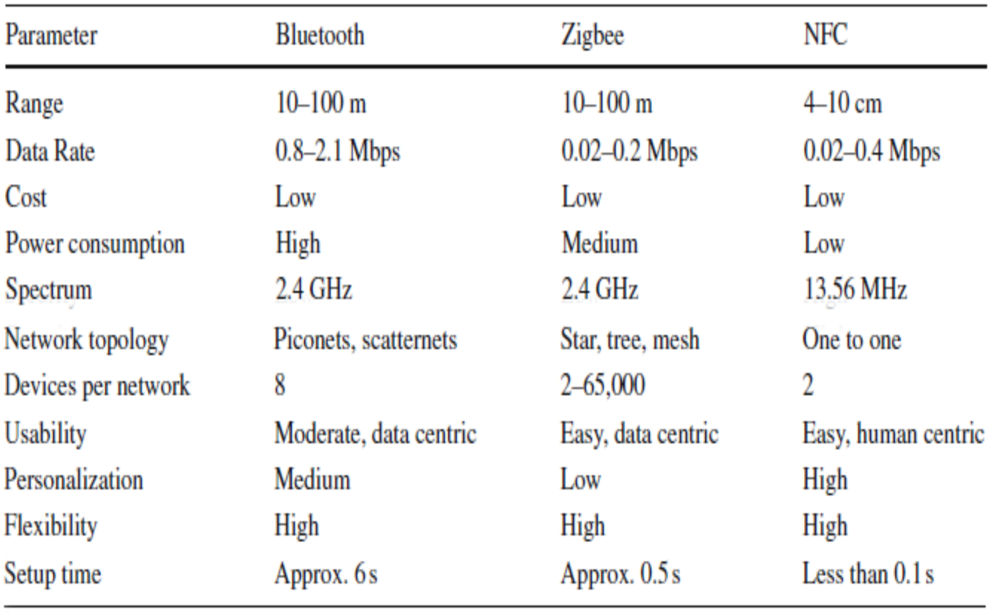
NEAR FIELD COMMUNICATION (NFC)

3.1. Overview of NFC

With the invention of mobile phones, the prior intent was to establish voice calls instead of using traditional wired phones. After Second Generation (2G) GSM technology, mobile phones have equipped with not only performing voice calls but also sending/receiving text messaging and also having internet experience capabilities. In addition to standard cellular network connection over base stations, mobile devices have started to establish connection to other electronic devices for data exchange and interaction. The infrared technology was used in first, then Bluetooth and Wi-Fi wireless technologies have been developed for connection between interactive mobile devices.

After this development phase, Near Field Communication (NFC) technology was introduced in 2002 by Philips and Nokia [17]. In 2004, Nokia, Microsoft, Sony, and Philips established NFC Forum in order to create cooperation and standardization. In early 2010s, NFC Forum has started to introduce NFC standards such as Logical Link Control Protocol (LLCP) Specification, NFC Data Exchange Format (NDEF) Specification and NFC Record Type Definition (RTD) Specification etc. After that, mobile device manufacturers have been affected from these developments and started to produce smart NFC products, which are NFC, enabled mobile devices tags and readers. Finally, NFC became a standardized short range, easy to use and set up, flexible and stable communication technology. The comparison with other communication technologies and effectiveness of NFC are indicated in Table 3[30].

Table 3: Comparison of Wireless Technologies [30]



Parameter	Bluetooth	Zigbee	NFC
Range	10–100 m	10–100 m	4–10 cm
Data Rate	0.8–2.1 Mbps	0.02–0.2 Mbps	0.02–0.4 Mbps
Cost	Low	Low	Low
Power consumption	High	Medium	Low
Spectrum	2.4 GHz	2.4 GHz	13.56 MHz
Network topology	Piconets, scatternets	Star, tree, mesh	One to one
Devices per network	8	2–65,000	2
Usability	Moderate, data centric	Easy, data centric	Easy, human centric
Personalization	Medium	Low	High
Flexibility	High	High	High
Setup time	Approx. 6 s	Approx. 0.5 s	Less than 0.1 s

According to evolution of NFC technology that is also illustrated in Figure 3, Radio Frequency Identification (RFID) technology may be interpreted as ancestor of NFC technology. Although NFC passive cards are similar technology with RFID passive cards, NFC have reformed, communication technology also combines smart cards and mobile phones for innovative and flexible solutions.

3.2. Communication Infrastructure

NFC provides short range (up to a few centimeters) wireless communication between two electronic devices. In order to establish communication, at least one active (energy provider) device should start communication process. NFC enabled mobile devices, NFC readers such as contactless payment readers are active devices, NFC tags, and NFC posters are passive devices.

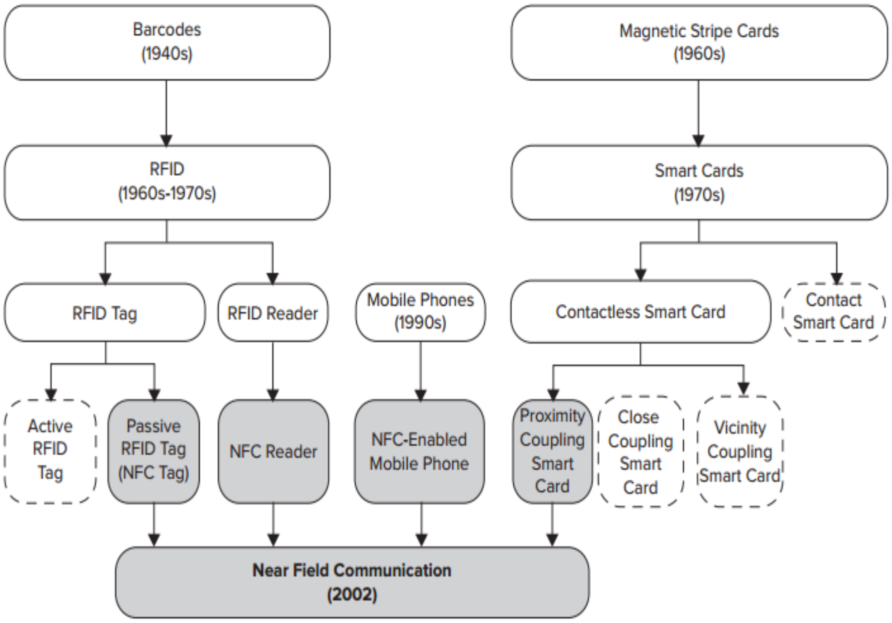


Figure 3: Evolution of NFC Technology [20]

Passive devices do not have any energy supply and they use received electromagnetic energy that is induced by active devices when they come close enough to active devices. This process is illustrated in Figure 4 [68].

NFC operates in 13.56 MHz High Frequency (HF) unlicensed frequency band that is available to all manufacturer with range of up to 4 cm, however generally devices are touched to each other. Data transfer rates are 106, 216 and up to 424 Kbps which higher than RFID data transfer rates, however much lower than 3G and Wi-Fi rates. The reason of that, the main purpose of NFC operations is not transfer to high volume data to destination. This also illustrated in Figure 5 [5].

NFC works on different modulation schemes such as ASK (Amplitude Shift Keying) with different modulation types 100% or 10% and coding techniques such as Manchester and Modified Miller coding for exchanging data.

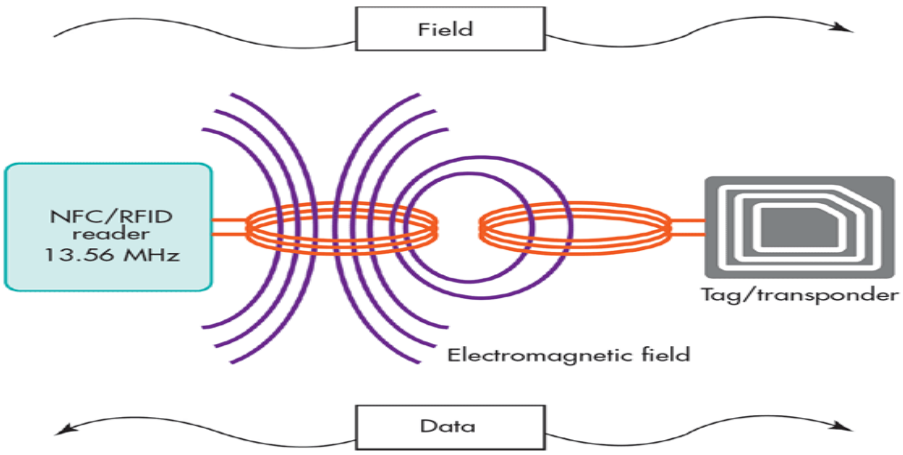


Figure 4: Electromagnetic Induction of NFC Devices [68]

According to study [8], using Phase Shift Keying (PSK) has better performance than ASK in terms of energy efficiency.

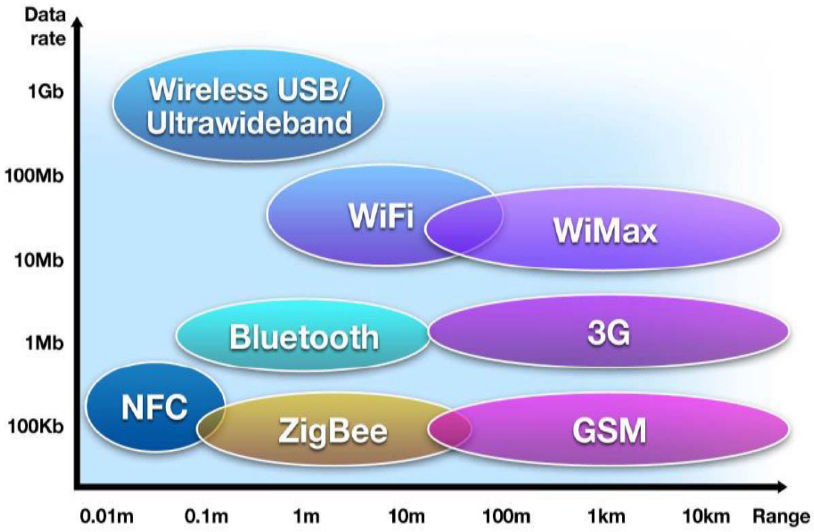


Figure 5: Data Rates and Ranges of Wireless Technologies [5]

3.3. NFC Mobile Phone Architecture

A typical NFC enabled mobile phone includes standard mobile phone equipment and NFC specific components. Mobile device in other words host controller performs its data communication through Wi-Fi or mobile network baseband via 2G/3G connection. NFC module involves NFC controller and NFC antenna, which is able to connect to NFC device. Some mobile device has electronic unit called Secure Element that aims to store critical data in secure environment. NFC module connects to host controller either directly or through Secure Element. The infrastructure of Secure Element is illustrated in Figure 6.

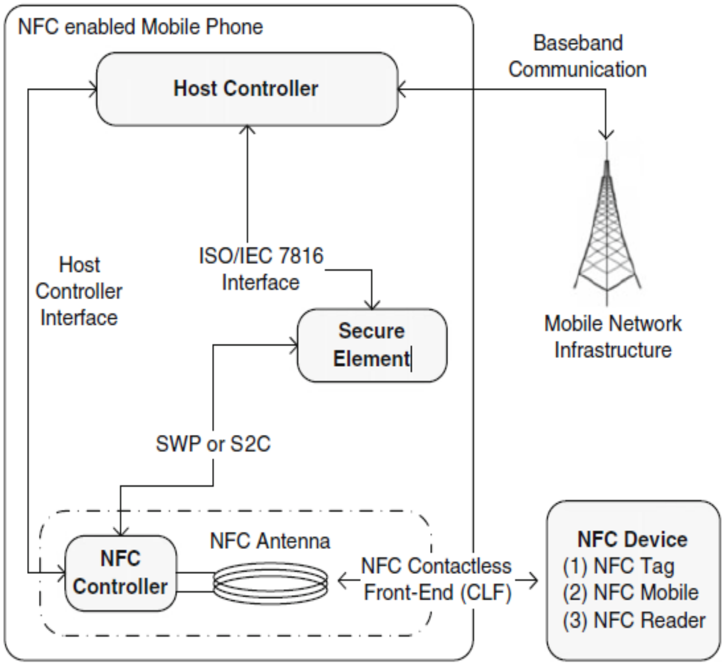


Figure 6: Structure of NFC Enabled Mobile Phone

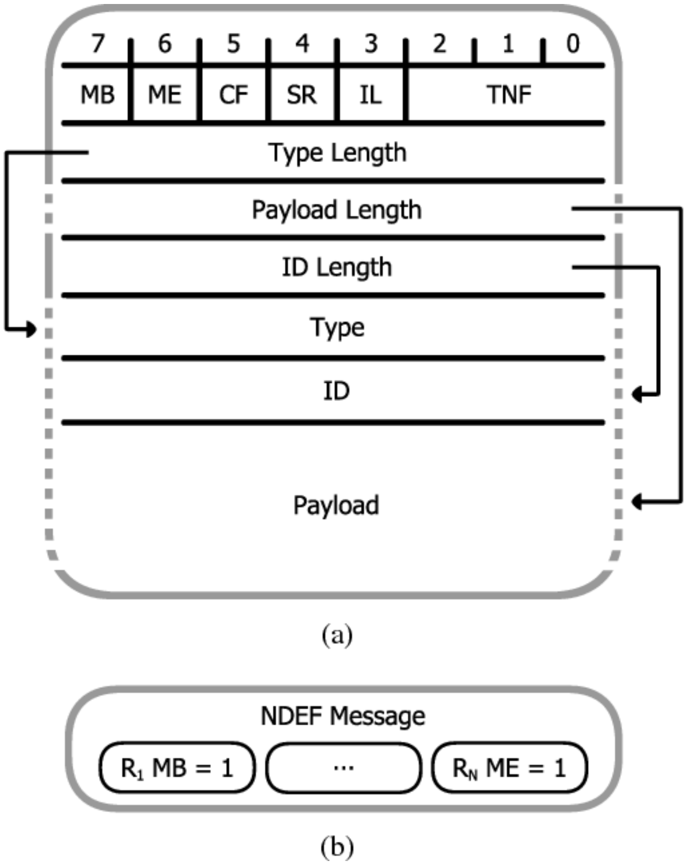
3.4. NFC Data Exchange Format (NDEF)

NFC Data Exchange Format (NDEF) is a message exchange format which is described in standard that created by NFC Forum [9]. This format regulates message content, which is sent by passive NFC device (tag) to active NFC device (mobile device or reader). With the basis of NDEF, NFC Forum has introduced four different Record Type Definitions (RTD Standard [10]) for customizable NFC applications, which are Text, URI, Smart Poster and Generic Control. There are also four different Tag Type operations named NFC Type 1-4 tag operation that must be supported by an NFC Forum device, which is based on ISO/IEC 14443A.

The NDEF message format can vary according to standards and application areas; however, common NDEF format is illustrated in Figure 7 [30]. Explanation of each fields are follows:

- MB (Message Begin): The MB flag is a 1-bit field, which indicates the start of an NDEF message.
- ME (Message End): The ME flag is a 1-bit field, which indicates the end of an NDEF message.
- CF (Chunk Flag): The CF flag is a 1-bit field, which indicates that this is either the first record chunk or a middle record chunk of a chunked payload.
- TNF (Type Name Format): The TNF field value indicates the types of the value of the TYPE field.
- TYPE_LENGTH: This field is an unsigned 8-bit integer that specifies the length in octets of the TYPE field. The TYPE_LENGTH field is always zero for certain values of the TNF field.
- SR (Short Record): The SR flag is a 1-bit field, which indicates that the PAYLOAD_LENGTH field is a single octet.
- ID_LENGTH: This field is an unsigned 8-bit integer that specifies the length in octets of the ID field.
- PAYLOAD_LENGTH: This field is an unsigned integer that specifies the length in octets of the PAYLOAD field (the application payload).

The size of the PAYLOAD_LENGTH field is determined by the value of the SR flag.



(a)

(b)

Figure 7: NDEF Message Format [30]

3.5. Operation Modes of NFC

The NFC enabled mobile phones communicates with each other using three different modes according to solution formation and requirements. These modes provide a flexible environment for developers and hardware produces. General protocol stack of operation modes is illustrated in Figure 8. [53].

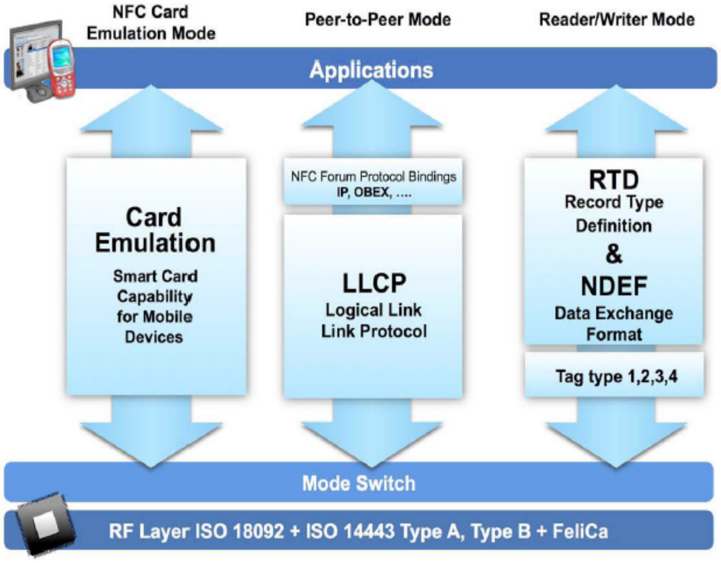


Figure 8: Operation Modes of NFC[53]

3.5.1 Card Emulation Mode

In this mode, two active NFC devices, which are mobile device and reader, are used. The mobile devices act as smart card based on ISO/IEC 14443 Type A, Type B and FelicCa standards in the application. When mobile phone gets close to reader, similar to RFID applications, reader initiates interaction and reaches mobile phone's NFC module and Secure Element if available. Payment and Access Control applications use this mode for granting access.

3.5.2 Peer-to-Peer Mode

In Peer-to-Peer mode, two active NFC enabled mobile phones interact each other in two directional data exchange paradigms. Firstly, one mobile device initiates communication set-up process using request-response mechanism, other mobile device replies its response. The connection is established according to Logical Link Control Protocol Specification (LLCP) created by NFC Forum and data exchange is performed according to Simple NDEF

Exchange Protocol (SNEP) protocol basics. The data, picture, URL exchange operations between two mobile devices use this mode of operation.

3.5.3 Reader/Writer Mode

Active mobile devices can both read and write passive NFC tags in Reader/Writer mode. Similar to RFID cards, NFC cards respond to requested data sent from initializer mobile device or write demanded data. Passive NFC tags are operated according to NDEF and RTD message format standards which described in Section 3.4. Location based services, information tags or smart posters use this operation mode.

3.6. Vulnerabilities and Attacks

In this section, the vulnerabilities and attacks that target to these parts of the overall system are analyzed.

There are two main reasons for high volume of attacks to mobile systems especially NFC based ones. Firstly, NFC mobile devices can act as credit cards so they include critical and sensitive financial data, or they can act as smart cards that are used in access control systems so they again include private data. Second reason of attacks is about customer perception of security. The customers of mobile device do not pay attention security and possible risks enough. According to survey conducted by Ponemon Institute [54], only less than half of consumers use passwords or other security patterns, only 29 percent of consumers state that they install anti-virus software, and only 10 percent of customers turn off their Bluetooth “discoverable” status when their phone is not in use.

3.6.1 NFC Tag Vulnerabilities

Passive NFC cards or tags which are also similar to RFID cards operate in Reader/Writer modes. They are generally unpowered microelectronic unit including small chip and antenna. Active devices (mobile phone or reader) initialize connection and passive tag replies with included data or function with the harvested power. The common components of NFC tag are illustrated in Figure 9 [55].

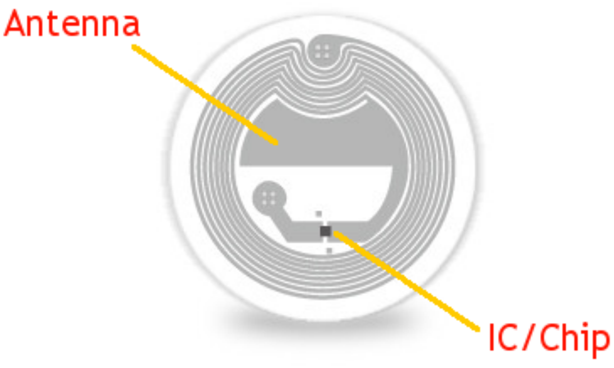


Figure 9: Components of NFC Tag [55]

The chip (EEPROM) inside of NFC tag contains NDEF based data which also described in RTD document of NFC Forum. The probable threats about tags can be grouped as data modification, URI modification and fuzzing.

NFC tags may contain ticketing data in transportation or can be used in hotels for room access. If the data inside of card or tag can be modified easily, it may result in unauthorized access. Another risk is URI modification. When the data is modified and overwritten with an unsecure web link, consumer may download some applications or files which cause security risks. These threats can be avoided with key distribution and key agreement between two sides of solutions.

3.6.2 NFC Enabled Mobile Device Vulnerabilities

In order to ensure security on mobile devices, sensitive data and credentials should be stored in secure environment [56]. In order to provide this requirement, electronic especially mobile device manufacturers have developed microelectronic chip called “Secure Element (SE)”. For example, as a popular payment solution, Google Wallet system stores debit card information in secure element of mobile device [30].

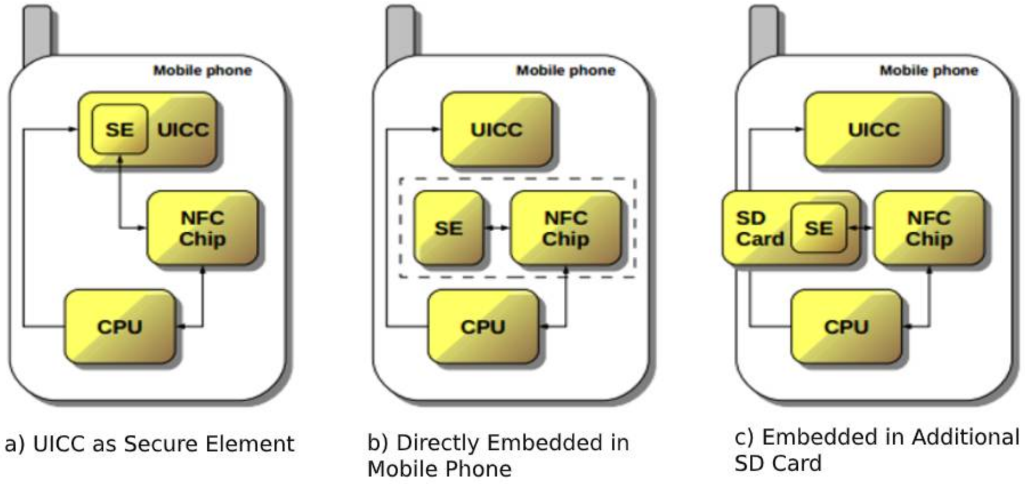

Mobile phone
SE
UICC
NFC Chip
CPU
a) UICC as Secure Element
Mobile phone
UICC
SE
NFC Chip
CPU
b) Directly Embedded in Mobile Phone
Mobile phone
UICC
SD Card
SE
NFC Chip
CPU
c) Embedded in Additional SD Card

Figure 10: Types of Secure Element [55]

Three types of secure element are offered in the literature [55], [57] according to their structure. These are SIM Card (UICC) as Secure Element that the secure element chip is located on UICC, Embedded Secure Element where the Secure Element is directly embedded in the mobile device as a separate unit and Additional Secure Element that external SD card is used as Secure Element.

- **SIM Card (UICC) as Secure Element:** The secure element chip is located on UICC. This solution is used when either mobile device does not have embedded secure element or Mobile Network Operators offering solutions. Such as, Turkcell Mobile Payment solution works on this kind of secure element.

- **Embedded Secure Element:** Secure Element is directly embedded in the mobile device as a separate unit. These kinds of secure elements provide independency and flexibility to manufacturers and developers. The majority of secure elements which produced recently are this kind of secure element. Google wallet mobile payment system uses both embedded secure element and UICC as secure element.

- **Additional Secure Element:** Less mobile solution uses secure element as inside of external SD card. This kind of secure element is likely exposed to high security risks.

Also, in the research [20], software based secure elements were added to mobile phone virtually, however, they are not applied to solutions because of their security risks in data modification in virtual secure element easily.

NFC controller is connected to SEs through either Single Wire Protocol (SWP) or NFCWired Interface (NFC-WI). In addition, secure element connects to host controller using ISO/7816 standard regulations [58]. These connections are illustrated in Figure 6. However, NFC literature does not include any comparison analysis of both physical layers in terms of security, performance and other parameters yet.

As the concept of isolating sensitive data in the mobile phone [12], software-based isolation is offered which is an extension of OS first, then a hardware unit assigned inside of mobile phones' Central Processing Unit (CPU) and memory, finally a complete dedicated hardware unit is developed for assuring high security. This development is illustrated in Figure 11.

The main security trait affecting secure element is trying to reach data stored in the secure element in unauthorized manner [59]. To do that, attacker may use hidden software, which installed to phone without knowledge of user and this software can read secure element. Additionally, an attacker can add a modified virtual secure element to the device and create security leaks. By doing that, attacker can pass over PIN based precautions. The solutions to these issues are not discussed in the literature and should be researched. Assigning SE matching ID and performing data transactions using with that ID may avoid adding modified secure element security risk, in other words integrating context aware security model with mobile device SE helps to solve these security threats. This vulnerability is out of scope of this thesis.

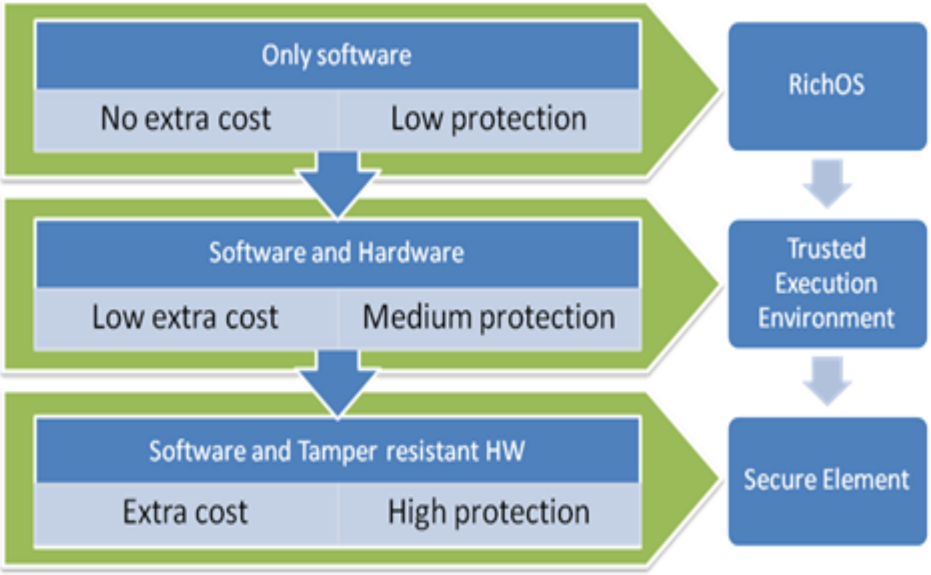


Figure 11: Stages of Secure Element

3.6.3 NFC Communication Vulnerabilities and Attacks

In addition to typical wireless communication threats, there are also threats which are specific to NFC communication. The common attack methods in NFC communication environment are eavesdropping, data modification and relay attack.

Although communication range of NFC is only a few centimeters, attacker can listen and record the communication using proper antenna system. According to study [59], there is no built-in prevention method for NFC systems, however encrypting data and creating secure data communication channel between NFC device can avoid eavesdropping and also the proximity of the communication units can be another precaution for attack realization, but it does not eliminate the risks totally.

Data corruption, data modification and data insertion type attacks have similar method and properties on radio communication. Similar to other wireless mediums, data corruption is mainly caused by jam signaling. In the research [55], reflective and pulse jamming are described and effects of jam signaling on the data modulation schemas are also analyzed. Data modification and data insertion attacks are difficult to implement than data corruption, because, attacker can interfere the communication using signaling, however, in order to modify or insert data to flowing data in the medium, first s/he should capture the packet in required small time range. Also, even if data package is captured, transaction should be in the proper modulation and encoding form. In the research [59] and [60], it is stated that; when transferring data with modified Miller coding and a modulation of 100%, only certain bits can be modified, while transmitting Manchester-encoded data with a modulation ratio of 10% permits a modification attack on all the bits.

Eavesdropping and data modification attacks are not frequently used in NFC domain as relay attacks. In the relay attack scenario, attacker captures and forwards relayed message to proxy device and this device deliver the message as if the real owner. Similar to relay attacks, man in the middle attacks also influence wireless medium, however, the method and purpose of relay attacks have completely changed. These attacks are frequently used in ISO/IEC14443 based passive smart card communication environment. Since these cards are used in critical payment and access control systems, relay attacks in this environment result in important security threat. For example, in the research [61], ISO/IEC14443 based smart contactless credit card is successfully relayed over proxy devices. In this application, relay mobile phone records debit card data in reader mode and forwards this data to other phone via wireless communication such as Wi-Fi or Bluetooth.

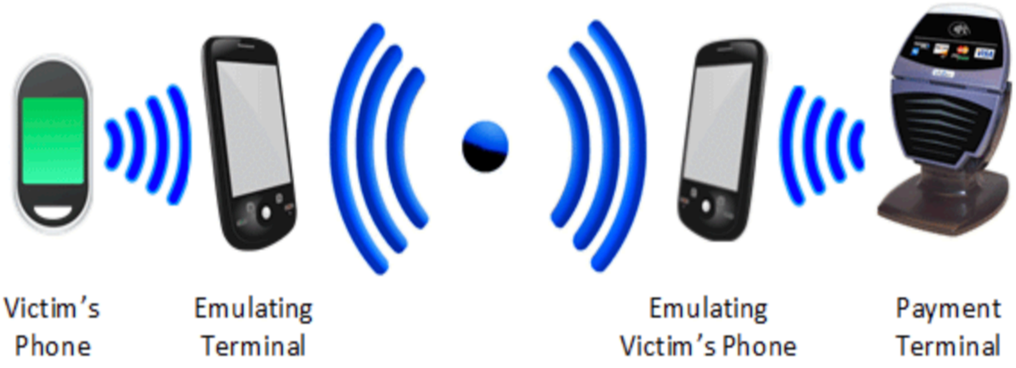


Figure 12: Example of Relay Attack Formation [62]

Proxy NFC based mobile devices sends credentials to reader as if the real owner in card emulation mode. If the reader cannot realize the fake sender, relay attack is completed successfully. The example of relay attack communication example is illustrated in Figure 12.

In the literature, NFC enabled mobile phones are generally used for relaying smart cards, in other words mobile phones read and send the data only. Credit cards, debit cards even electronic passports are used in relay attack experiences, however in the access control systems that also used in this study; mobile devices are used in card emulation mode instead of using smart cards. In our study, we give more attention to relay attack than eavesdropping and data modification because; relay attacks are encountered more frequently in transactions and can cause more damage than other threats. Also because of NFC's short communication range, other attacks generally cannot be performed successfully.

CHAPTER 4

PRACTICAL NFC RELAY ATTACK

In this chapter of the thesis, details of practical relay attack using NFC smart phones are analyzed. The relay attacks are generally occurring in wireless environments; however, it has some different characteristics in NFC domain in terms of implementation logic and methodology.

In addition to other security threats such as eavesdropping, data modifications etc. in the short-range wireless communication, relay attacks are frequently used for performing interventions.

Attacker captures and forwards relayed message to proxy device and this device delivers the message as if the real owner in a typical scenario. Similar to relay attacks, man in the middle attacks also influence wireless medium, however, the method and also purpose of relay attacks have completely changed. These attacks are frequently used in ISO/IEC14443 based passive smart card communication environment. Since these cards are used in critical payment and access control systems, relay attacks in this environment result in important security threats. For example, in the research [62], ISO/IEC14443 based smart contactless credit card is successfully relayed over proxy devices. In this application, relay mobile phone records debit card data in reader mode and forwards this data to another phone via wireless communication such as Wi-Fi or Bluetooth. Proxy NFC based mobile devices send credentials to reader as the real owner in card emulation mode.

If the reader cannot detect the fake sender, relay attack is completed successfully.

In the literature, NFC enabled mobile phones are generally used for relaying smart cards, in other words mobile phones read and send the data only. Credit cards, debit cards, and even electronic passports are used in relay attack experiences, however, in the access control systems proposal; mobile devices are used in card emulation mode instead of using smartcards. On the other hand, smart cards are limited and just reply the requested data.

4.1. Host Card Emulation Mode (HCE)

NFC devices basically operate in three different implementation modes, Reader/Writer, Peer-Peer and Card Emulation mode. Although announced three modes, developer could use two of them, Reader/Writer and Peer to Peer in Android operating systems because of limitations. Also, we have started that Peer to Peer mode in our previous test environment in implementation phase of thesis study. Only Google Wallet [63] solution could access to this operation mode in its transactions until the 4.4 version of Android (API Level 20) is released. With that release, developers have started to use Host Card Emulation Mode [64] in their solutions and users have started to use their mobile phones like smart cards, also we have moved to that operation mode in our system because of its functionality and flexibility compared to its other modes.

The use of HCE in solutions also eases the practicability of relay attacks in the domain. Shifting between Reader and Card Emulation modes provides great chance to relay attackers. We have also used HCE in our practical relay attack scenario.

4.2. Relay Attack Implementation

The relay attack setup in this study shows differences in transaction methods and relaying medium. As it is illustrated in Figure 13, the high-level components of NFC based access control systems are NFC Enabled mobile device, NFC reader, access control panel and central server.

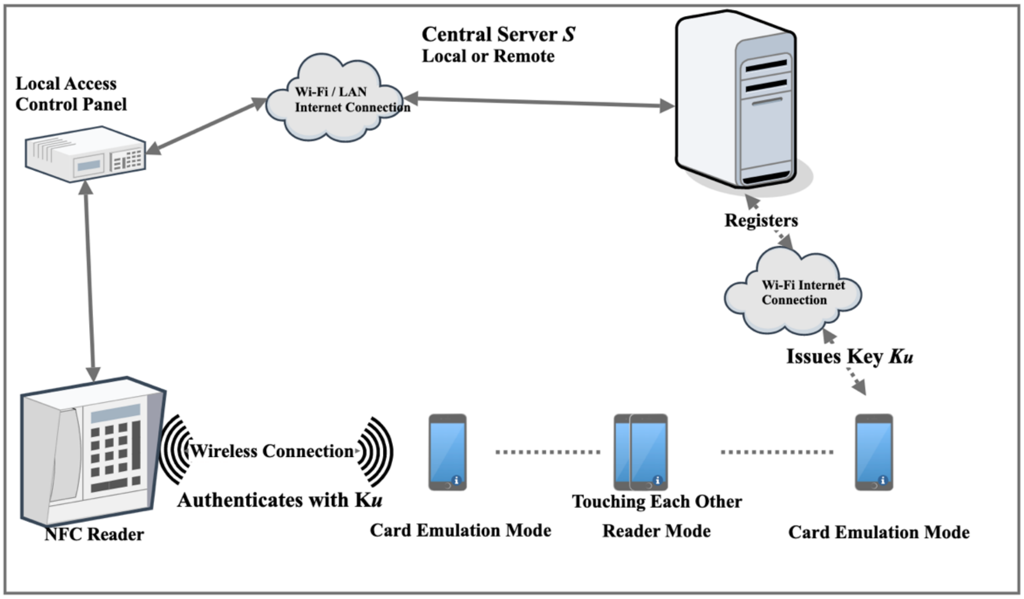
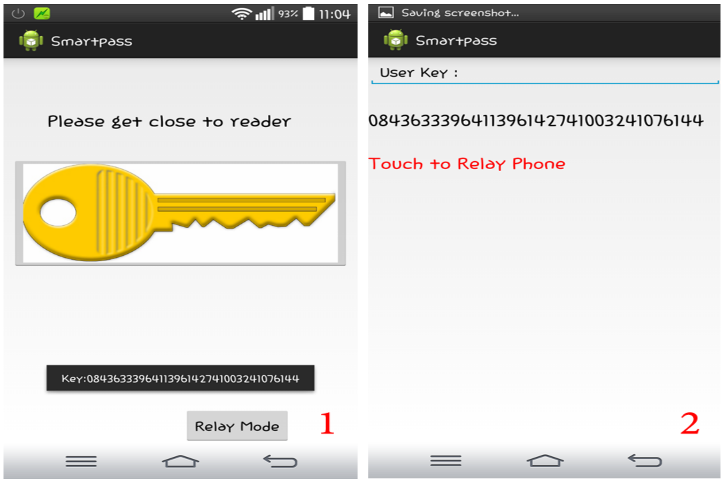


Figure 13: Relay Attack Flow for Access Control System

The general activity flow of NFC based access control system begins with controlling whether NFC unit is active or not. If NFC is enabled, user registers to system with his/her mobile operator number, username etc. via application that installed on device. Once user is registered to system, central server activates his/her authorizations if defined previously and sends to activation key to authenticated mobile device. After registration process is completed successfully, user can now send access requests with his/her user name, password and period of time parameters.

After getting key from the server using JSON based web services infrastructure, user can now send authentication requests to NFC reader with acquired key. At that time, relay phone can interfere NFC communication between reader and mobile phone. Relay phone can read the key that stored in the real mobile phone by getting close to phone in reader operation mode. In other words, relay phone imitates the NFC reader. If requester cannot identify the real NFC reader, relay phone can get the user key.



Please get close to reader

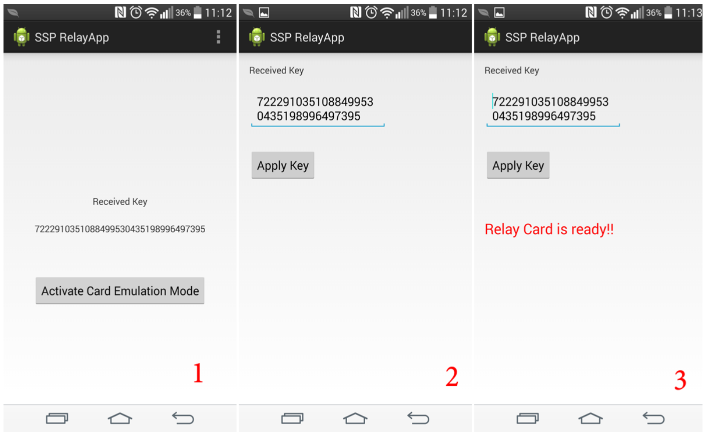
Key:0843633396411396142741003241076144

User Key :

0843633396411396142741003241076144

Touch to Relay Phone

Figure 14: The Mobile Phone Screens of the Real Sender



Received Key

7222910351088499530435198996497395

Received Key

722291035108849953
0435198996497395

Received Key

722291035108849953
0435198996497395

Relay Card is ready!!

Figure 15: The Mobile Phone Screens of the Fake Sender

In order to complete attack successively, relay phone should send access request to NFC reader with key that captured from real phone. To do that, relay phone shifts its operating mode to Host Card Emulation Mode, by doing this; it now acts as smart cards and sends requests. After these transactions, NFC reader gets the key and forwards to the server. Because of the validity of the key, unauthorized attempt access to resource. The screenshots of these operations are illustrated in the Figure 14 and 15.

The main purpose in developing this attack trial application is to show how easily relay attack can be performed especially using host card emulation mode in NFC enabled mobile devices. To overcome this security vulnerability, we have designed and developed a context-aware and dynamic security model for that medium. The details of the offered model are described in the Chapter 5.

CHAPTER 5

MOBILE CONTEXT AWARE AND ROLE-BASED ACCESS CONTROL MODEL (M-CARBAC)

5.1. Security Model

Security model generally means a schema for enforcing security policies as a term. In other words, it is formal descriptions of security policies. If a security policy states that subjects need to be authorized to access objects, the security model would provide definitions how x can access y only through the outlined specific methods. In our case, main security policy can be stated as only authorized users can access resources via NFC communication and security model describe how it can be achieved, which methods and calculations should be used etc.

There are different kinds of security models for any kind of need in applications. For example: Bell-LaPadula for confidentiality, Biba, Clark-Wilson for integrity, Chinese Wall for dynamic changes of access rights, Clark-Wilson for informal environment etc. In addition to these security models, access control security models also offered in the literature such as, Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC). Details of these access control models are explained in the Table 4.

Table 4: Access Control Models Basics

Model	Description
Discretionary Access Control (DAC)	Access control over databases based on user identities and rules
Mandatory Access Control (MAC)	Lattice based access control model. Primarily focuses on information flow of computer systems.
Role-Based Access Control (RBAC)	Access grants are given according to role status of users instead of individual authorization.
Temporal Role-Based Access Control (TRBAC)	Extension of RBAC model, time contexts can also be used in access control.
Generalized Role-Based Access Control (GRBAC)	Access roles are defined in three different concepts which are subject roles, object roles and environmental roles.
Threshold Based Collaborative Access Control (T-CAC)	Access is allowed only when total access requests reach the defined threshold value.
Context-aware access control using threshold cryptography (CAAC-TC)	Works based on "threshold cryptography" methodology and contexts. Data encryption and decryption are administered by access control rules.

5.2. Threat Modeling

Threat modeling is a set of activities for improving security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of risks. There are lots of offered threat modeling methodologies [65] in the literature. Such as STRIDE, PASTA, LINDDUN, CVSS, Attack Trees, Persona Non Grata, Security Cards, hTMM are the examples of the most used ones. We analyzed the STRIDE threat modeling basics and created the Elements of NFC Relay Attack Threat Model. STRIDE is a model of threats offered by Praerit Garg and Loren Kohnfelder at Microsoft for identifying security threats [66]. Basically, STRIDE stands for "Spoofing", "Tampering", "Repudiation", "Information disclosure", "Denial of service", and "Elevation of privilege". The main purpose of STRIDE is to allow researchers to classify threats according to its categories.

Table 5: STRIDE Threat Categories

	Threat	**Violated Property**	**Explanation**
S	Spoofing Identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, network, memory or else
R	Repudiation	Non-Repudiation	Claiming that you did not do something or were not responsible
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of Service	Availability	Exhausting resources needed to provide service
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do

The categories of STRIDE model are presented in the Table 5. Although STRIDE model is generally used for analyzing software threat modeling, it can be also used for other systems. At first glance, Tampering, Repudiation, Information Disclosure and Denial of Service threat categories are not related with Relay Attack threat methodology. Although "Spoofing Identify" seems to be category of Relay Attack, in fact, it is a tricky way of pretending someone or something such as phishing etc. Elevation of Privilege is defined as allowing someone to do something they are not authorized to do. With this perspective, it is the closest category of Relay Attack scenarios.

After that, we have defined Asset, Vulnerability, Threat, Adversary, Type of Adversary, Attack Vector, Motivation, Successful Result and Countermeasure of NFC Relay Attack Threat Models. They are explained in the Table 6.

First of all, threat is having access of unauthorized subjects with authorized credentials in mobile access control systems using NFC technology which means Relay Attack. Moreover, the main target is to get critical data (credentials and contextual) of mobile device. In other words, attacker targets to get this information to perform his attack successfully.

The main vulnerability in the NFC Relay Attacks is unable to detect real owner of mobile critical data. If the system/model could not detect the real requester than Relay Attack is successfully performed. The attacker can be defined as a person with unauthorized mobile device. In other words; someone having a mobile device including critical data of someone else. An adversary type is active and mobile, according to the contextual data used in the requests, it may be static or dynamic. The main motivation source of attackers for Relay Attacks is that, they can easily obtain sensitive and critical data and reach sensitive applications such as access control, financial etc. To prevent successful Relay Attack threats and ensure authentication validity, we have offered a context-aware prevention model.

Table 6: The Elements of NFC Relay Attack Threat Model

Element	**Property**
Asset (Target)	Critical data (credentials and contextual data) on mobile device.
Vulnerability	Unable to detect real owner of mobile critical data.
Threat	Having access of unauthorized subjects with authorized credentials in mobile access control systems using NFC technology (Relay Attack).
Adversary (Attacker)	Person with unauthorized mobile device.
Adversary (Attacker) Type	Active, static or dynamic, mobile.
Attack Vector	Mobile devices → (wireless communication) → reader of resource.
Motivation	Attacker can get the authorization access easily in critical access control systems.
Successful Result	Is authorized to resources.
Countermeasure	Using context-aware prevention to ensure authentication and authorization validity.

5.3. The Model Basics

The pervasive computing environments (PCE) include different kinds of hybrid devices, infrastructures and applications. In the study [55], components of a typical PCE described as devices, pervasive networks, middleware and applications. In our proposed system and model, following matchings can be applied; NFC enabled mobile phone as device, NFC communication as middleware and access control system as application.

Our proposed model is an access control model based on predefined security policies and principle in order to ensure secure end-to-end NFC communication. The three main security policies that define security model based on our research questions are;

1. What are the possible vulnerabilities for NFC communication environment?
2. What are the system requirements and how can we define them properly for our context-based security model?
3. Can we prove and simulate the practicability of the relay attack in NFC communication?
4. How can we design and build a dynamic context aware security model to prevent relay attacks in NFC enabled mobile phones?

We are planning to create a context sensitive security model, which ensure and satisfy these questions and policies. Our main security principle in the proposed access control model; the credential data should be meaningless even it is captured and it should be no longer valid even if it is read. According to that principle, validity has more importance than confidentiality, which is one of the main principles of security. Because the key in the NFC access control, systems need not to be confident, when validity of keys satisfies the conditions. Based on these requirements that defined in this section, we interpret the context aware methodology for new domain with innovative perspective.

With the help of these basics, our model provides application layer security mechanisms for NFC based access control systems. In addition to traditional and static security models, it provides dynamic and adaptive context aware security model principles. The offered model covers the NFC based access control systems, other NFC based solutions such as NFC payment solutions or EMV based NFC card solutions are out of scope in this study although the model can be applicable on them as well.

5.4. Context Aware Methodology

Context as a term is described in studies and by researchers in many different ways. The five "W" descriptions of context include definitions that are "Who", "What", "Where", "When" and "Why". An answer of each of these questions generates a context. Location description of context mainly focuses on the person's current location and descriptions of surrounding location. Also, nowadays, additional parameters are used in context aware systems. For example; average value of daily usage or other parameters such as IMEI number of mobile devices etc. can be used for access control systems.

Context categories are:

- User context: the status of the user making a request.
- Resource context: the status of the resource (object) being requested.
- Environment context: the status of any entities relevant to the specific request (resource's environment).
- History context: specific previous events and situations, which constitute an additional dimension of context information, including user, resource and environment history.

A system can be defined as a Context Aware System as long as it senses the environment and reacts accordingly. It can be described as context aware systems as collecting required contexts in order to create meaningful information for users or systems. Another description of context aware system underlines adaptation of systems behaviors and reactions according to sensed changes of the environment. In addition, context aware systems are grouped as “active” and “passive” context aware systems. Both of them monitor changes in the environment, however, active context aware systems adapt their reactions according to context and pre-defined rules, on the other hand, passive context aware systems sense the changes in the environment and send them to system users.

5.5. Dynamic and Adaptive Security

Access control systems are always needed for any kind of resource throughout to history. This need exponentially increased in the digital age which is also defined as “third era of computing” by Weiser [1]. In this era resources and devices are extremely distributed in the environment. This concept also named as “Pervasive Computing” in the literature.

Although conventional static security models are still used in digital systems, innovative access control models are becoming more popular. In fact, this popularity is result of needs about efficiency, simplicity and durability. Number of devices, interactions between devices and people who use these devices are extremely increased in pervasive computing environments. Therefore, MAC (Mandatory Access Control), DAC (Discretionary Access Control) and other conventional model do not satisfy these needs.

As a result of this period, dynamic security models in which permissions and assignments are changed according to changes in the environment are developed, and still studies are conducting on this topic. Our model is also planned and designed based on dynamic and adaptive security model methodology.

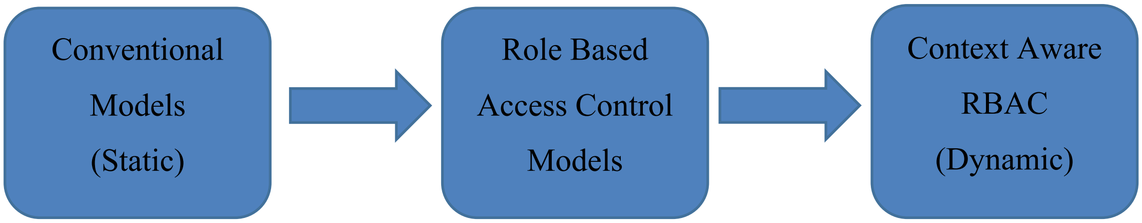


Figure 16: Evolution of Access Control Models

5.6. Mobile Context Aware and Role-BasedAccess Control Model (M-CARBAC)

The important part of our model is to ensure security in mobile environment especially in NFC communication. In addition to common encryption techniques, we suggest a context aware security model. Unlike the typical RFID based smart cards, NFC mobile phones can act as both a reader and smart cards. This mainly causes Relay Attack. This attack occurs in application layer, therefore suggested Data Link Layer precautions such as calculating Frame Waiting Time (explained in proposal report in detail) for RFID based cards do not solve this problem. The Proposed context aware security model is mainly suggested in order to overcome this type of attack. Based on mentioned requirements, context aware parameters are added to generated key in mobile device before sent and encrypted. With the help of this logic, even the data can be relayed to another location or any device, it will not be valid and attack will not be successful. This logic also validates our main security principle which is the credential data should be indecipherable even it is captured and also it should be no longer valid even if it is deciphered.

The major valuable and conceptual properties of the model as follows:

- **Context Layer Abstraction**: Using different kinds of contextual information with defining entities and activities in authentication period.

- **Two Layer Capsulation**: In addition to standard encryption, contexts are added to packet before sending access requests.

- **Runtime Creation**: Transactions and contexts used in authentications are created in runtime. This becomes a necessity in mobile environment in order to prevent relay attacks.

- **Undescriptive Key Format**: According to our main security principles, data may be captured, however it should be meaningless in other words; contextual information and keys should not be identified.

- **Dynamic Adaptation**: Unlike the traditional authentication methods, permission activations and revocations are performed accordingly with the context changes.

5.7. Role Based Access Control (RBAC)

Role Based Access Control model is suggested by Sandhu and his colleagues [69] in 1996 as an alternative access control model to Mandatory Access Control (MAC) and Discriminatory Access Control (DAC) models. Majority of access control models are developed based on its main principles. It is also accepted and published as a standard by National Institute of Standards and Technology (NIST).

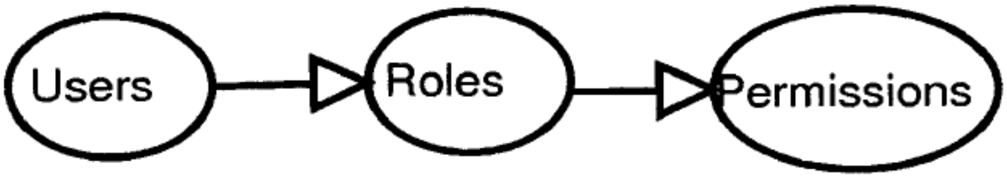


Figure 17: Structure of Basic RBAC

Table 7: Authentication Methods of Models

Approach	**Subject Identity Sid**	**Token T**	**Authentication**	**Mapping**	**Access Policy - Permission P**
Conventional Access Control	User-name	Password	Is S_{ID} a valid username, given T?	-	(S_{ID}, P)
Public Key Based Access Control	Certificate (public key)	Signature (private key)	Does S_{ID} represent a valid user, given T?	-	(S_{ID}, P)
Role-Based Access Control	Username	Password	Is SID a valid user, given T?	$S_{ID} \rightarrow Role_{ID}$	(Role $_{ID}$, P)
Context-aware Role Based Access Control	Username	Password	Is SID a valid user name, given T?	$S_{ID} \rightarrow Role_{ID}$ $S_{ID} \rightarrow$ Ctx	(Role $_{ID}$, Cxt, P)

RMAC is developed in order to manage complex access control procedures in the companies and systems. Basically, it contains four main components which are users, roles, permissions and sessions. Instead of using traditional control mechanisms such as passwords or access control lists, it is based on User-Role (U-R) assignments. This flow is illustrated in Figure 17. In addition, it separates permission management from user and role mechanisms with Role-Permission (R-P) assignments. The first version of RBAC only provide a flat assignment from user to permissions then other improved versions of RBAC are offered. The development process of RBAC is described in below.

- RBAC0: the basic model in which users are associated with roles (U-A) and roles with permissions (P-A).

- RBAC1: RBAC0 with role hierarchy.

- RBAC2: RBAC0 with constraints on role and permission assignments.

- RBAC3: combination of RBAC1 and RBAC2.

In the last version of RBAC, role hierarchy and constraints are added to the model in order to manage level of roles with respect to permission activation and define constraints that affect U-R and R-P assignments. As a result, RBAC became one of the most popular and convenient access control models in terms of efficiency, administrative costs and easiness.

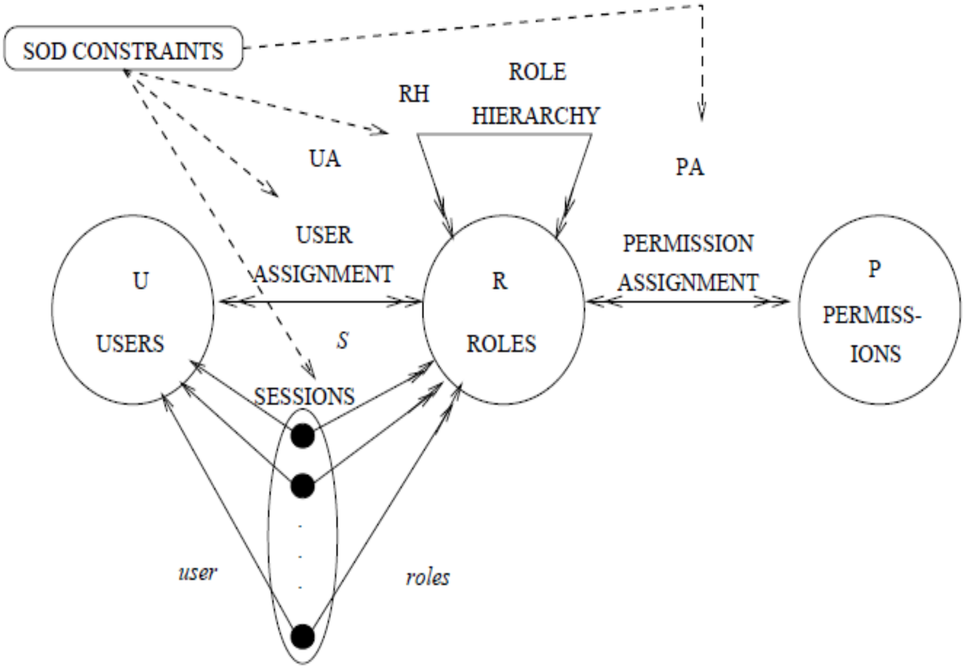


Figure 18: Structure of RBAC3 [69]

Although majority of systems use RBAC, it cannot meet all requirements of today’s systems and applications. The parameters of devices, users and applications changes frequently in pervasive computing environments (PCE), therefore roles and permissions change accordingly. In order to develop access control systems with this perspective, researchers tend to extend RBAC by adding new parameters, mechanisms or components. Our model (M-CARBAC) also extends the RBAC in order to make it appropriate for mobile environments.

5.8. Conceptual Requirements of the Model

Near Field Communication (NFC), technology takes part of access control solutions. Almost all these kinds of solutions are critical and data sensitive solutions because of their roles and functions. Although general information security requirements which are described below can be applied to NFC based communication, NFC specific security requirements have not been offered in the literature up to now.

- **Data Confidentiality:** Because of its nature, data confidentiality is one the most important requirement. The basic principle in NFC based access control systems is securing sensitive credentials from unauthorized individuals

- **Data Integrity:** Integrity means to be correct or unchanged the intended state of data. In NFC communication, the data is not tolerated to even small changes; therefore, data integrity principles should be applied to NFC based solutions. It also includes authenticity and non-reputation schemas

- **Availability:** This principle guarantees the service reachability for all required time and conditions. Because of wireless communication of NFC, it may be affected from DDOS attacks that are created by jam signaling and other interferences.

NFC technology is a multi-functional technology and includes hardware, software and communication domains. Because of that, NFC security issue deals with not only traditional information and communication security issues but also NFC specific security issues.

Least Privilege, Role Hierarchy, Separation of Duties and Role Conflicts are core requirements that will be considered in implementation part of our model as an infrastructure.

a) **Least Privilege:** The principal of least privilege also known as the principal of minimum privilege regulates the minimum required rights in order perform desired action on an object. According to this requirement, each user, function or application should not have more permissions than minimum level of right for an action.

b) **Role Hierarchy:** The role hierarchy defines a structure of levels of roles in the systems. Similar to inheritance of object-oriented programming (OOP) in software development, it provides bottom-up role tree of organization. This structure decreases role complexity and eases to manage of roles. Basically, it describes that the role has all permissions of roles from all below levels. For example; IT managers have all privileges of DB admins and also officers, because IT managers are in the top and officers are in the bottom in role tree. The tentative role hierarchy of our model is illustrated in Figure 19.

c) **Separation of Duties:** This requirement mainly aims to prevent one role having whole permissions to perform an action. It is based on at least two or more role or users are needed to complete a transaction. For example, a confirmation of a critic money transfer transactions in a bank should be performed by at least two officers.

d) **Role Conflicts:** Role definitions and role hierarchy should be designed carefully in case of any role conflicts. A user may have two roles that have conflicting permissions. For example; a research assistant can have “instructor” and “student” roles at same time, however they may have some conflicting permissions. To prevent these kinds of conflicts, roles should be atomic as much as possible or predefined rules should be addressed in case of any conflict’s occurrence.

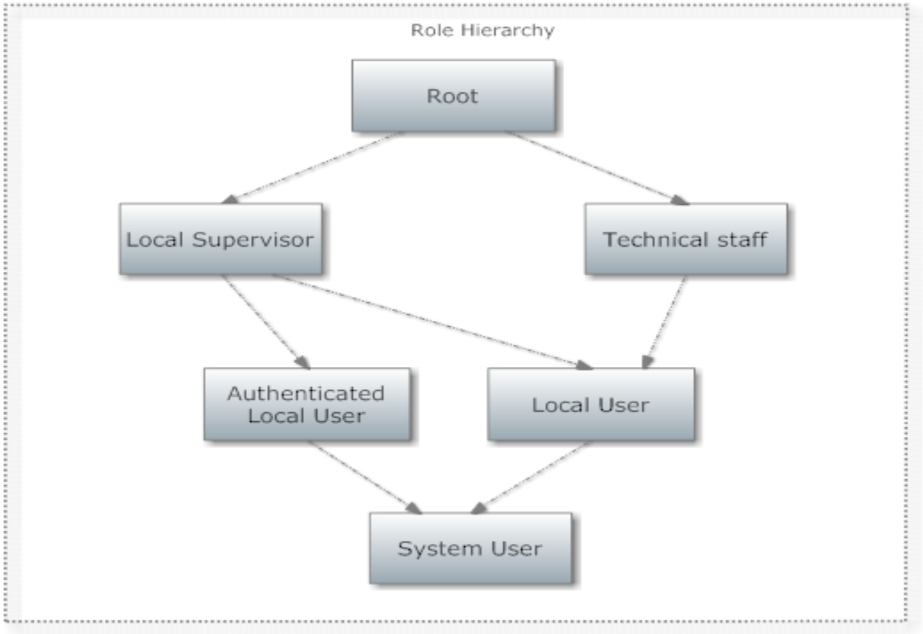


Figure 19: Role Hierarchy of MCARBAC

5.9. Principles and Components of the Model

Access control systems mainly regulate access requests from subjects on an object. When a user (subject) wants to reach a resource (object), access controller mechanism evaluates this request based on access policies and predefined rules. On the other hand, these types of static access control mechanisms become out of use because of its inflexible and inefficient structure. Not only static credential information but also supportive contextual information is started to be used in access control evaluation periods in order to create more efficient decisions and make assignments accordingly.

We try to extend RBAC model with contextual additions. By doing that we aim to both prevent relay attacks in mobile environments and also provide a dynamic security model for applications.

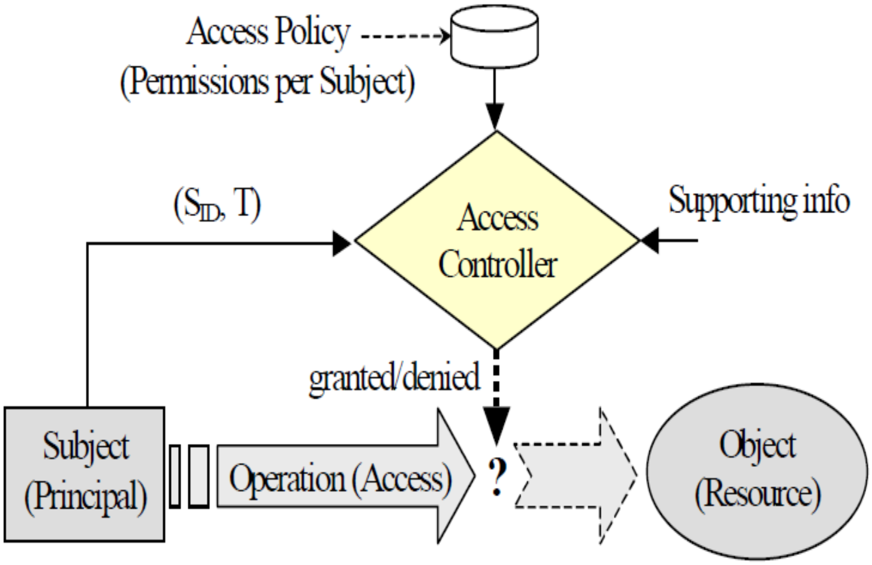


Figure 20: Typical Access Control Mechanism

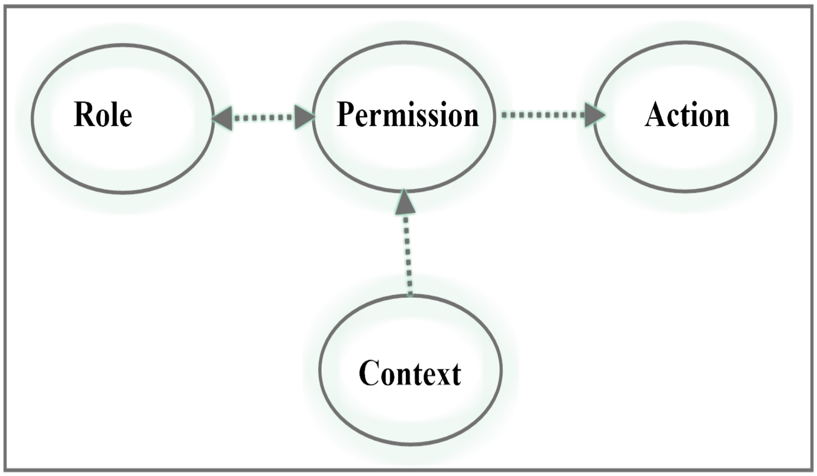


Figure 21: Conceptual Context Relationship

The main components of our model are;

Subjects (SS) set consists of current systems users.

Roles (SR) set includes predefined system roles and match with Subjects and Permissions sets.

Objects (SOb) set describes system Objects.

Operations (SO) set describes system Operations on Objects.

Permissions (SP) set describes system Permissions for given objects and operations.

Context (SC) set describes the sum of Static Mobile Context (SMC) and Dynamic Mobile Context (DMC).

These components are explained in the Chapter 6 in detail.

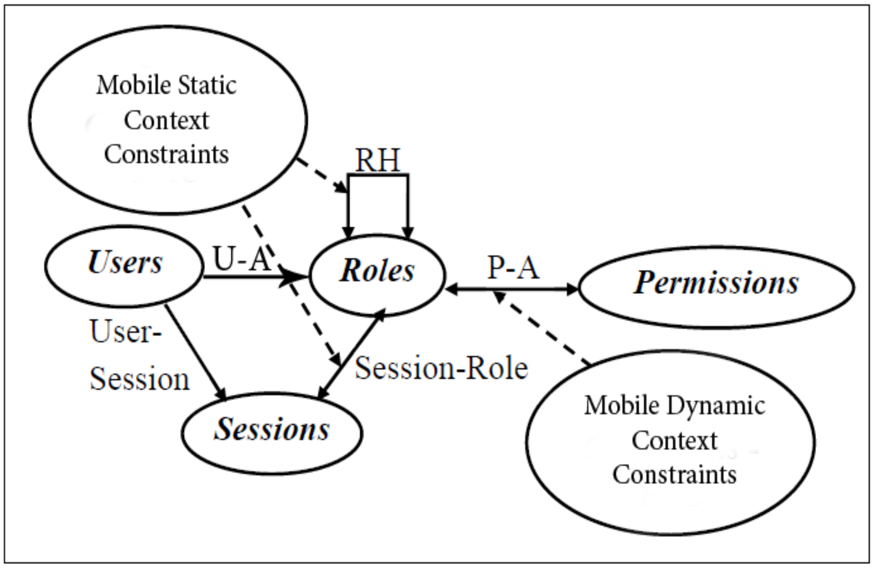

Mobile Static Context Constraints
RH
Users
U-A
Roles
P-A
Permissions
User-Session
Session-Role
Sessions
Mobile Dynamic Context Constraints

Figure 22: Structure of the Proposed Model

5.10. Access Control Mechanisms of the Model

The M-CARBAC security model which provides context sensitive access control provides layered control orders. The layers from bottom to top are Standardizes Controls (SC), Context Sensitive Controls (CSC) and Dynamic Policy Controls (DPC). The layered infrastructure is provided in Table 8.

Our model aims to provide end to end complete security solution for access control systems using smart mobile devices whose infrastructure is illustrated in Figure 13. The system includes both standardized hardware technologies (server, local access control panels), wireless and wired communication technologies (Ethernet, 802.11 wireless) and non-standardized relatively new technologies (NFC communication, mobile device hardware and software).

Table 8: Layered Control Mechanisms of the Model

Process	Steps			Countermeasure
Authorization	Dynamic Policy Controls			**M-CARBAC**
	S	G	R	
Authentication	Context Sensitive Controls			**M-CARBAC**
	1st Cycle	2nd Cycle		
	Standardized Controls			**Standard**
	Encryption / Decryption			

We mainly focus on NFC (wireless) communication security that occurs between mobile device and system. Therefore, we try to develop a security model that regulates this communication and eliminates relay attack types unauthorized attempts from mobile devices to resources. On the other hand, we included all standardized system components and communications although they are not in scope our study. The reason is that; we try to provide end-to-end security solution for our environment and develop security solution for gaps of the whole system and finally offer a complete solution.

The standardized security issues of wired (Ethernet) and wireless (802.11) communications between devices and systems and also security issues of server hardware and software components and also network based attacks such as DOS, DDOS etc. are not in the scope of our study. These concerns are studied in the literature in detail and well known and standardized security solutions developed and offered for these environments.

However, we included these modules in both layered control mechanism of the conceptual model also in the system infrastructure of the model to make sense of integrity.

We have designed layered control mechanism of our model similar to layered structure in computer networks in order to illustrate control order in a regular manner. It is illustrated in Table 8. At the bottom of layers, Standardized Controls take place. Above of that controls Context Sensitive Controls and Dynamic Policy Controls perform authentication and authorization processes respectively.

Encryption / Decryption, Authentication and Authorization processes generally play important role in almost all access control models. They are natural standard processes for access requests to resources and used in different ways and concepts. Approaches and procedures of the model for these processes differentiate our security model. Our major contributions to these processes are offering context sensitive innovative credentials as new two-cycle methodology in authentication and evaluation periods. The details of authentication and authorization processes are explained in the following sections.

5.10.1. Context Sensitive Controls (CSC)

This part of our proposed model explains the authentication process of access control mechanism. Based on dynamic security and two-phase authentication philosophy, an innovative context sensitive methodology is offered.

In this methodology, not only traditional static credentials but also dynamic context parameters are used for both role and permission decisions. As stated in the requirements parts of our model, two-layer capsulation is also applied to user key with context parameters. In this phase, static security model is extended with context parameters in order provide dynamic control. Both user key and received context parameters are evaluated together. These operations are performed in the 1st cycle of controls.

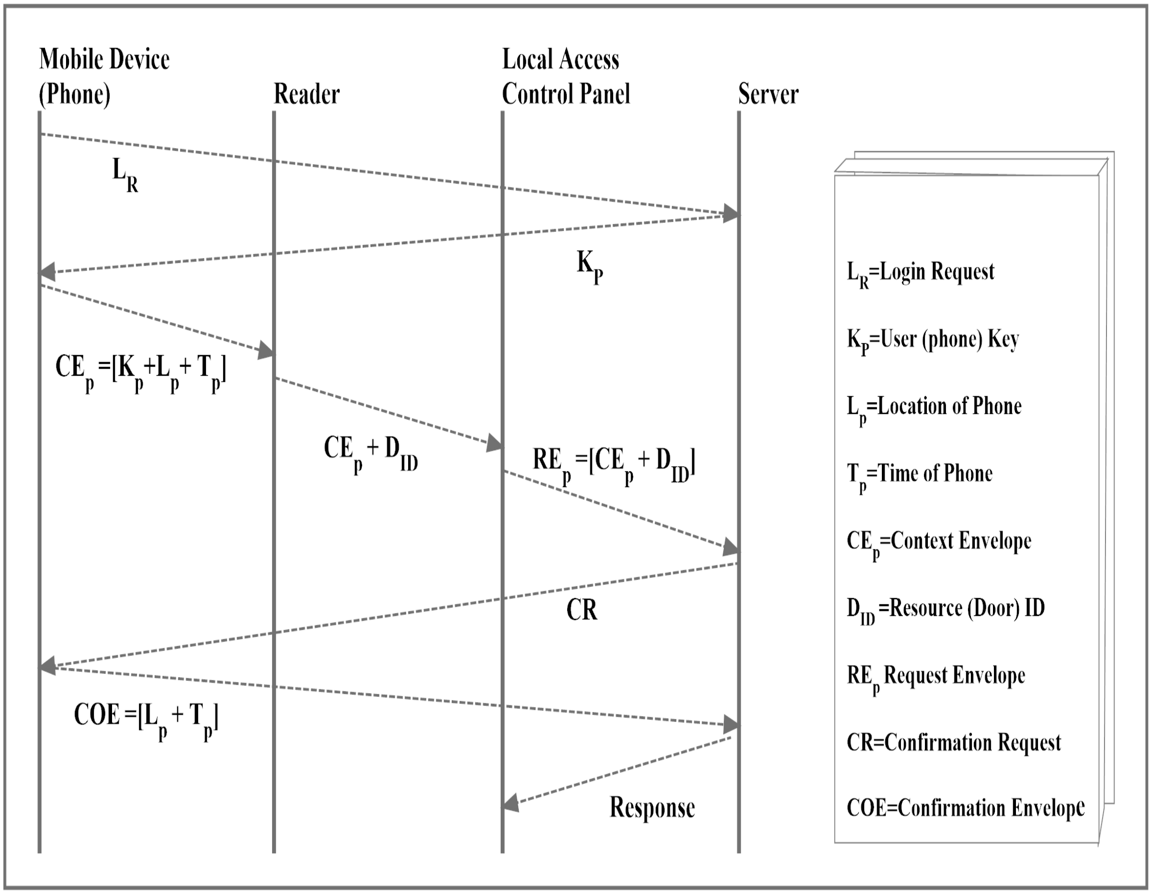


Figure 23: Conceptual Flow in Authentication Process

In the 2nd cycle, the verification of context parameters is performed by central server with the real sender phone in order to prevent relay attack. This verification is crucial operation because as it is stated; Our main security principle in the proposed access control model; the credential data should be meaningless even it is captured and also it should be no longer valid even if it is read. According to that principle, validity has more importance than confidentiality which is one of the main principles of security. By doing this we ensure that; even user key is captured by unauthorized person and relayed. System is able to detect this attempt and identify its validity even key is confirmed and finally blocks access to resources.

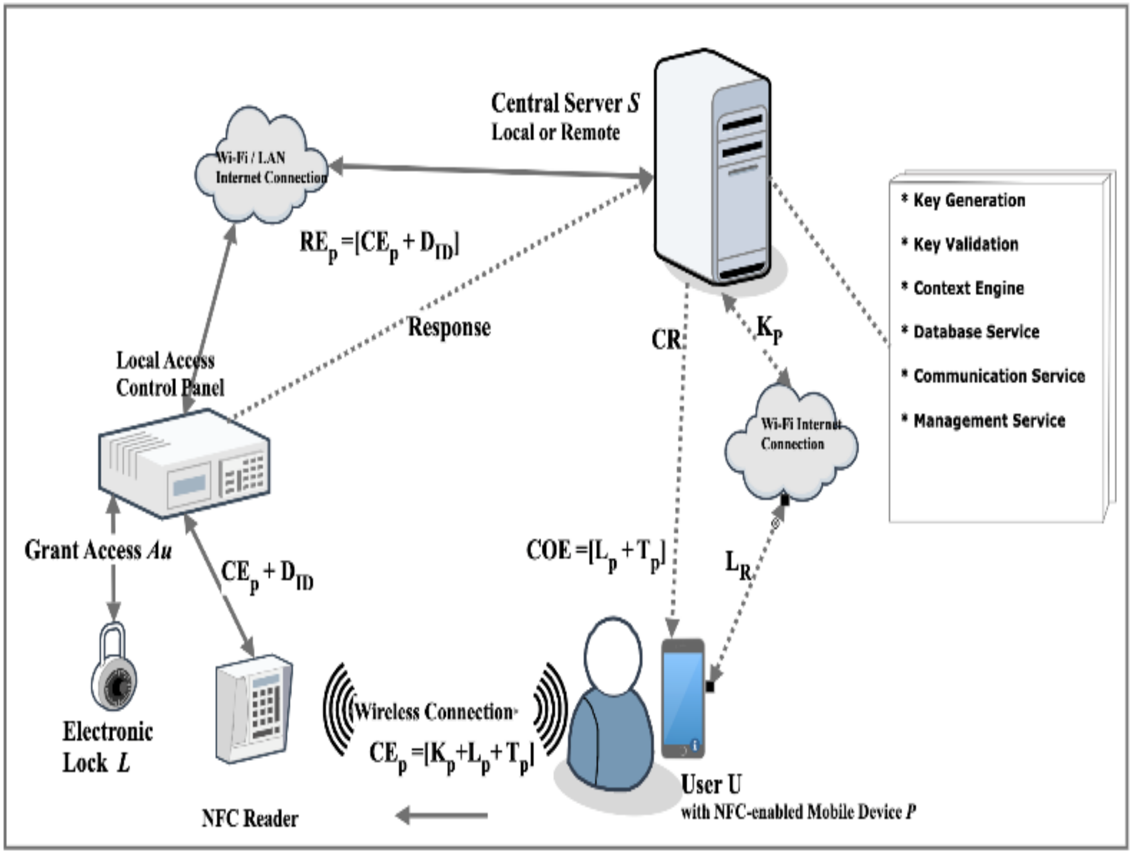


Figure 24: Credentials Flow of System Components

The process of access control and authentication firstly begins with mobile device user to login (LR) to the server. After logging in successfully, user-specific random key (KP) generated by the server is sent to the user's mobile device. The generated key is valid for the duration specified by the user in the login process.

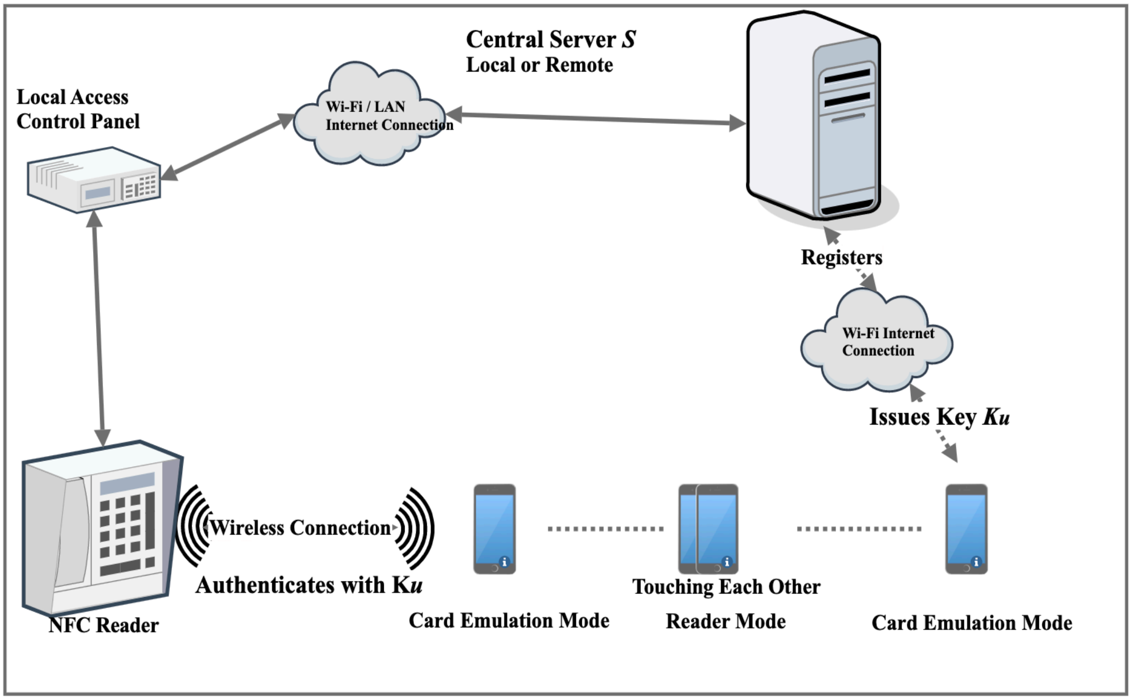


Figure 25: Credentials Flow of System Components (Relay Attack)

At the end of this duration, the validation of the key is expired. The key obtained by the user who wants to access the sources, the time (Tp) and the location (Lp) information obtained automatically in background create the Context Envelope (CEp =[Kp+Lp+ Tp]). This envelope is sent to the reader. The reader adds to the envelope its own DID which describes the resource and send them to the Access Control Panel. The Local Access Control Panel converts these information as the Request Envelope (REp =[CEp + DID]) and sends it to the server. The server opens the packet arrived and controls the key

(Kp), the time (Tp) and the location (Lp) information in the packet. If the key generated by the server and is not expired, then the time (Tp) and the location (Lp) parameters are evaluated. If the request time is in the time intervals specified in the policies, the location parameter is then controlled. Similarly, if the location information generated automatically in background by the mobile device is in the range specified in the policies before, then the first control cycle is completed.

The server either makes a decision or performs the second control cycle processes based on the parameters. In this phase, the verification is performed in order to prevent relay attacks. The server sends the Confirmation Request (CR) to the real mobile user logged and requests the location and the time information from the user in background. The real mobile user generates the Confirmation Envelope (COE =[Lp+Tp]) with the time and the location information calculated in background, and sends it to the server. The server compares these time and location information with the ones arrived in first cycle. The time spent for communicating is considered while comparing the time information. If the time and the location information are consistent with the ones arrived in the first cycle, and they are in the time interval specified in the policies, then the generated response is sent to the Access Control Panel. The Access Control Panel either gives authorization physically or denies depending on the answer arrived. These steps are illustrated in Figure 23 and Figure 24.

In the second phase, a risk-based method can be used. These authorization mechanisms can be used when the application is critical, or when there is a user who has a suspicious process history, or when the location information is very close to the range limit specified. However, this method should be used for every request in the situations that relay attack may occur.

In the relay attack scenario, even though the attacker imitates the real user as it is close to the reader (when it isn't in fact) by changing the Lp value in the message that it will send, it will be denied in the second phase of confirmation. If the attacker sends the location information of the real user in the Request Envelope in order to pass the second phase, the request will be denied because it is not close enough to the reader in this time. In this situation, the only condition that surpass the method is that the real user brings user mobile phone to a nearby place to the source and requests an access authorization. In this situation, it can pass the location control in the second phase of confirmation. It is an exceptional and non-controllable situation that can be occur in any access control system. In such a case, the software which runs on the real user's device can answer to the request sent by the server in the second phase only when it is run by the user actively. Thus, even though the attacker brings the mobile device of the real user to resource close enough, it cannot pass the second control phase.

5.10.2. Dynamic Policy Controls (DPC)

Generally, authentication process is performed in order to determine who is the requester exactly. This authentication process is crucial because for access control systems, permission and roles are assigned according to these results based on authentication process. This flow is also explained in the layered control mechanisms of the model.

After authentication process is performed successfully, authorization process is initiated with parameters coming from authentication level. Also both authentication and authorization transactions use system and context policies which created based on application priorities and organization decisions.

Context parameters and user credential (key) are used both in authentication and authorization process but in different methods and different purposes. In the authentication period, process tries to define the identity of requester on the other hand in the authorization period, these parameters are used for assigning verified requesters to predefined roles and permissions with the help of policies. The key produced by server and location and time contexts are extracted from Context Envelope (CEp=[Kp+Lp+ Tp]) in authentication period and then these parameters are evaluated in the upper authorization layer.

Also stated in the Principles and Components of the Model dynamic and static context information take part in role and permission assignments. In our model, location (Lp) and time of phone (Tp) are dynamic contexts and User Key (Kp) and Resource ID (D_{ID}) can be stated as static context. Also stated in the Figure 22, role assignments are performed based on static contexts, permission assignments are performed based on dynamic contexts. In other words, after authentication period, user (Kp) is assigned to predefined role within the role hierarchy and whether permission is granted or not to requested resource is evaluated based on dynamic time and location contexts within predefined access policies.

The levels and types of policies may change according to the application and its priorities. The high-level conceptual policy patterns of our model are described Chapter 6 in detail. In addition, low-level derived policies are used in implementation of the model.

CHAPTER 6

FORMAL DEFINITIONS

Mobile Context Aware and Role Based Access Control Model (M-CARBAC) is explained with formal definitions in this chapter. First, sets and functions of the model are created then context and policy evaluations are explained and finally claims which verifies the formal definitions of the model are provided.

6.1. Set and Functions

Following sets and functions describe the formal representation of the proposed model:

Subjects (SS) set consists of current system users. It is primarily related with context and role sets. It consists of mobile users who use NFC based mobile application for requesting access.

Roles (SR) set includes predefined system roles and matches with Subjects and Static Mobile Context sets. As it is also stated in the Role Hierarchy section of Chapter 5, our main roles are Root, Local Supervisor, Technical Staff, Local User and System User. There is a mapping between subject and context combination and elements of set of Roles. In other words, subjects having different contexts address at least one predefined role (See Equation 1).

$$(s{:}SS,\ c{:}SMC) \rightarrow 2^{SR} \qquad (1)$$

Objects (SOb) set describes system elements where subjects want to get an access over them. For example, conceptual Objects set can be defined as follows: {Door, Device}

Operations (SO) set describes system Operations on Objects. Conceptual operations set is as follows:

Operations: {Login, Lock Door, Unlock Door, Register, Activate}

Permissions (SP) set describes system Permissions for given objects and operations. As SP is defined in the Equation 2, it consists of object, operation and decision (allow/deny) combination.

$$SP \subseteq SO \text{ x } SOb \text{ x } 2^{\{Allow/Deny\}} \qquad (2)$$

Context (SC) set describes system contexts and includes Static Mobile Context (SMC) and Dynamic Mobile Context (DMC) subsets. Context set is defined in the Equation 3.

$$\text{ContextSet } (SC) = SMC \cup DMC \qquad (3)$$

Static Mobile Context ***(SMC)*** set consists of static contextual information that retrieved from current user before requesting an access. An example of SMC is defined as follows:

SMC = {PhoneNumber,Key}

Dynamic Mobile Context ***(DMC)*** set includes dynamic contextual information which is collected from internal and external domains. Such as ID of secure element of mobile device may be internal, relative location or time may external DMCs. Contexts are defined as tuple {ContextType,Value}.

A typical context sets of models are as follows:

$DMC = ExtDMC \cup IntDMC$ (4)

ExtDMC = {RelativeLocation, Time, Date, etc.}

IntDMC = {Device ID, SecureElementID, AvarageUsage, Hash Value, etc.}

User-Role Function (URF) defines and regulates User-Role assignments based on SMCs. As URF is defined in the Formula 5, it consists of subject, role and context combination.

$URF \subseteq SS \times SR \times 2^{SMC}$ (5)

$getUserRole (s, smc) = \{r \in SR \mid s \in SS, smc \in SMC(s,smc,r) \in URF \}$(6)

Role-Permission Function *(RPF)* describes Role-Permission assignments based on DMCs. As URF is defined in the Equation 7, it consists of role, permission and context combination.

$RPF \subseteq SR \times SP \times 2^{DMC}$ (7)

$getRolePermissions (r ,dmc, obj, op) = \{p \in SP \mid (r,dmc,p) \in RPF$

$\text{and } p.obj = obj \text{ and } p.op = op \}$ (8)

Evaluate Permissions Function (EPF) evaluates permissions for given role and contexts and creates a set of Allow/Deny responses for permissions.

$$\text{EPF} \subseteq \{\text{Allow/Deny}\} \tag{9}$$

$$\text{evaluatePermissionss (P)} = \bigcup_{\text{Pi} \in \text{P}} \left(\prod_{\text{allow/deny}} \text{Pi} \right)$$

$$\text{where P} \subseteq \text{SP} \tag{10}$$

6.2. Evaluation of Access Granting

Evaluation of access granting based on our model includes policy evaluation, context verification and risk function evaluation operations.

Our main evaluation function is provided as follows:

$$\text{GrantPermission}(\text{r}, \text{p}, \text{c}) = \{\text{pe}(\text{r}, \text{p}, \text{c}) \land \text{vc}(\text{c}) \land \text{erf}(\text{r}, \text{p}, \text{c})\} \tag{11}$$

where;

pe (r, p, c): Policy Evaluation Function

vc (c): Verify Context Function.

erf (r, p, c): Evaluate Risk Function which is calculated dynamically in the run time, such as evaluating suspicious request history or reaching threshold values etc. These functions are explained in below in detail.

6.2.1 Policy Evaluation

Security policies define the rules and procedures for all subjects accessing resources (objects). In the proposed model, policy evaluation is the first step of access granting evaluation and consists of two main functions which are getRolePermissions and evaluatePermissions. This evaluation function is defined in the Equation 12.

$$\begin{aligned} pe(r,p,c) = (getRolePermissions(r,dmc,obj,op) = P) \\ \wedge (evaluatePermissions(P) = R) \wedge \neg\exists q \in R(q = deny) \\ \wedge \left(\exists q \in R(q = allow)\right) \end{aligned} \tag{12}$$

Within this evaluation process, first getRolePermissions and then evaluatePermissions function is executed. Although this policy evaluation function uses r,p,c (r ∈ SR, p ∈ SP, c ∈ SC) parameters, because dmc is the projection of c (context) ($\prod_{dmc} c$), and also obj (object) and op (operations) parameters are the projection of p (permission) ($\prod_{obj,op} p$) , they are used in getRolePermissions (r, dmc, obj, op) function directly as parameters. These two functions are explained in below.

getRolePermissions (r, dmc, obj, op): Retrieves active permission set ($P \subseteq SP$) for given role(subject), dynamic context information(dmc), object(obj) and operation(op).

evaluatePermissions (P): Evaluates permissions based on their Allow/Deny fields described in Formula 2 and creates a response set for each set of permissions.

6.2.2 Context Verification

Given a context c, let L_p be the location of the requester device extracted from c and let T_p be the current time of the requester device retrieved from the context c. Also, as a contribution of proposed model, confirmed contextual information (CL_p and CT_p) are retrieved from context of Confirmation Envelope (CE) that is executed in the second cycle control of the model, which is described in the Section 5.10 in detail.

Context verification process has four control steps. Control of confirmation contextual parameters are performed in the first two steps to prevent relay attack. Initially, it is checked that whether L_p (Location of requester device) is equal to CL_p (Confirmed location value). Similar to that control, then it is checked that whether T_p (Current Time of the Requester Device) is equal to CT_p (Confirmed Time Value). After checking relay parameters in the first two controls, standard context control is performed in the last two phases. Location of requester device (L_p) is expected to locate within the predefined threshold distance value (T_d) and finally, current time value of the requester device (T_p) should be between start and end time of related predefined rule. Verify context function creates a successful (true) response when all these four control steps are successfully verified, otherwise context verification is failed.

We define the verify context function as follows.

vc(c) $= ((L_p = CL_p) \wedge (T_p = CT_p) \wedge (|x - L_p| \leq T_d) \wedge (T_s \leq T_p \leq T_e))$ (13)

where;

x : Location value of predefined rule (such as location of source (door, vending machine etc))

L_p: Location of requester device

T_d: Threshold distance value for evaluation

T_s: Start time value of predefined rule (Unix Time Stamp, such as 1561556024)

T_e: End time value of predefined rule (Unix Time Stamp, such as 1561556424)

T_p : Current time value of the requester device

CT_p : Confirmed time value retrieved from Confirmation Envelope (CE) that is executed in the second cycle control of the model

CL_p : Confirmed location value retrieved from Confirmation Envelope (CE) that is executed in the second cycle control of the model

```
1.1 if (c == Ø) return false
1.2 Roles = getUserRole (s, $\prod_{smc} c$)
  1.2.1 if (Roles == Ø) return false
1.3 for each r ∈ Roles do
  1.3.1 P = getRolePermissions (r, $\prod_{dmc} c$, $\prod_{obj,op} p$)
          R = evaluatePermissions (P)
    1.3.1.1 if $\exists q \in R(q = deny)$ return false
    1.3.1.2 if $\neg\exists q \in R(q = allow)$ return false
    1.3.1.3 if (vc (c) = false) return false
1.4 if (erf (r, p, c) = true)
      then return true else return false
```

Figure 26: Access Granting Algorithm

The first part of vc() aims to prevent relay attacks. It ensures that confirmed context values, which are retrieved in the second cycle of controls, should match with the contextual information of the requester device. If Lp is not equal to CLp., there may be a relay attack attempt because the time value of requester and confirmed value from authenticated user are different. A similar argument is valid for the time context. The model validates the confirmed context parameters in the background in second cycle of transactions to prevent relay attack instead of evaluating the context provided in the request envelope. The second part of context verification can vary for different system requirements. System designers may employ different dynamic context elements with different control mechanisms such as using biometric values.

6.2.3 Steps of Formal Verification

Based on defined sets, functions, policy evaluations and context verification basics, granting algorithm is defined as illustrated in the Figure 26 in order to represent formal definitions of the model. By tracing steps of the algorithm, it is ensured that, model answers all possible access requests accurately according to the predefined policy and rules.

6.2.4 Claims

Claim 1: The request is granted only if the context is verified.

This claim ensures the main contribution of the model. Instead of the evaluation of the context that provided in the request envelope, the model validates the confirmed context parameters in the background as second cycle of transactions to prevent relay attack.

For that claim, all steps in the algorithm are confirmed until the step 1.3.1.3. Step 1.1. ensures that context is provided within the request. If there is no provided context, the request will not be granted, therefore it supports the claim. Then roles of the subject (user) are retrieved using $\prod_{smc} c$ projection. If the subject is not assigned to any role, then request is denied based on the principles of Role Based Access Control principle, i.e. each subject should be assigned to at least one role. Also, each role should be member of set of roles (SR) otherwise request is denied. Once roles of subject are retrieved, the permissions for the rules are checked according to the requested role (r), context ($\prod_{dmc} c$), and permission ($\prod_{\text{obj,op}} p$) parameters in the step 1.3.1. There should be no "deny" result and at least one "allow" result in the set of result (R) as explained in the step 1.3.1.1 and 1.3.1.2

According to these evaluations, until the steps 1.3.1.3, all steps are confirmed successfully, however, the Formula 13 states that:

$$\mathbf{vc(c)} = ((L_p = CL_p) \wedge (T_p = CT_p) \wedge (|x - L_p| \leq T_d) \wedge (T_s \leq T_p \leq T_e)) \quad (13)$$

This formula ensures that, confirmed context values, which retrieved in the second cycle of controls, should match with the contextual information of the requester device. If L_p is not equal to $CL_{p.}$, this situation can be assumed as one of relay attack attempts because the time value of requester and confirmed value from authenticated user are different. Also same evaluation is valid for location context. Under these evaluations, vc () function returns false response, once this function returns false whole evaluation process is broken and permission is not granted. Our model ensures that access is granted only if context is verified by evaluating the result of vc() function which guarantees contextual verification.

Claim 2: The request is granted only if result set contains at least one "allow" result and no "deny" result.

This claim ensures the applicability of the "deny overrides the allow" principle for the model. In this perspective, once any "deny" result is defined for the case, request is denied although it has some "allow" results.

For that claim, all steps in the algorithm are confirmed until the step 1.3.1.1. These steps are explained in detail in the Claim 1. Context is provided and roles of the subject (user) are retrieved using $\prod_{smc} c$ projection. If the subject is not assigned to any role, then request is denied based on the principles of Role Based Access Control principle, i.e. each subject should be assigned to at least one role. After roles of subject are obtained, the permissions for the rules are defined according to the requested role (r), context ($\prod_{dmc} c$), and permission ($\prod_{obj,op} p$) parameters in the step 1.3.1. There should be no "deny" result and at least one "allow" result in the set of result (R) as explained in the step 1.3.1.1 and 1.3.1.2.

The step **1.3.1.1** states that:

"if $\boldsymbol{\exists q \in R(q = deny)}$ ***break, return false"***

This statement reflects the general policy evaluation principal. Not only in NFC, but also in wireless or other network communication, deny rules always override the allow rules. Therefore, this function returns false and whole evaluation process is broken and permission is not granted. Our model ensures that request is not granted unless at least one "allow" result and_no "deny" result exist in the set of permission result (R).

Claim 3: **The request is not granted if the risk assessment fails.**

Although the implementation of the risk assessment is out of scope of the thesis, this claim ensures that the proposed model contains risk assessments in the evaluation processes.

For that claim, all steps in the algorithm are confirmed until the last step 1.4. As all clarified in the Claim 1 in detail, context is provided, roles of the subject (user) are retrieved and the permissions for the rules are defined according to the requested role (r), context ($\prod_{dmc} c$), and permission ($\prod_{obj,op} p$) parameters in the step 1.3.1. Based on the principle of "deny overrides the allow" principles, step 1.3.1.1 and 1.3.1.2 ensure this principle. Also, context is verified in step 1.3.1.3 in terms of both provided context and retrieved ones from model in the background to prevent relay attack. The vc() function guarantees contextual verification.

However, the step 1.4 states that:

“if (erf (r, p, c) = true) then return true; else return false”

This statement ensures that the model does not create a positive response when risk assessment fails. Since communication of NFC takes place in a short distance and fast, making an instant risk assessment is an important step for access evaluation.

Assessment can be made based on suspicious transaction history, different forms of behavior or previously defined risk factors. Also, AI algorithms and machine learning principles can take place in risk evaluation. Although it is applicable in our model, a complete risk evaluation study is decided as future work.

CHAPTER 7

IMPLEMENTATION AND TEST

Based on requirements and principals of the offered model, a complete NFC infrastructure and framework are developed in order to apply and verify the model. Within scope of this study, mobile application running on NFC enabled mobile device is developed to perform access requests. In addition, backend infrastructure, Arduino microcontroller, database and communication services (REST) are provided in a complete manner. For the implementation, high level uses cases, sample scenario, rule set and implemented access requests are provided in order to prove the coverage of the model in terms of addressing all possible request combinations. Also, performance tests of the model are provided in this chapter.

7.1 NFC Access Control System

In order to protect valuables in daily life, access control systems are offered throughout history. Although purpose is same for all access control systems, control methods have changed radically. Physical keys have been used for doors, also still they are used. Passive RFID cards have started to be used in offices or public buildings then. Fingerprint and retina-based access control have been developed for high security.

In last decade, with the increase of mobile device popularity and easiness, these devices have been preferred in access control. For example, SMS based mechanisms are used in banking application, also barcode and QR codes have been placed for granting access.

Finally, NFC based smart solutions have been started to use in access control. These kinds of systems provide great facilities both for consumers and manufacturers. The traditional RFID based solutions offer limited functions in terms of flexibility in access control. Because of using passive RFID cards, different cards are needed for each different door or building. On the other hand, with using NFC based smart mobile devices, different doors or different kind of control points can be easily accessed by only one single mobile device. For example, consumer can use his/her mobile phone for both home and office door entrance access, s/he does not need to carry extra different keys for each door.

In addition, traditional physical key systems are not secure enough; keys can be copied easily and when keys have been lost, all lock system should be renewed. The passive RFID cards and tags are not secure enough too; the data inside of cards can be modified easily and also copied to another card or tag.

NFC based access control solution provide more flexible and secure solution to these problems. When mobile phone is lost or stolen, the related authorization can be revoked instantly from another mobile device or web-based management panel without any need for physical intervention. The general infrastructure of NFC Based Access Control System is illustrated in Figure 27.

7.2. Components of NFC Access Control System

This test bed infrastructure consists of two types of structure which are physical and software components. Physical part includes Central Server, Local Access Control Panel, NFC Reader and Mobile Device. Other part consists of development of central software and database, mobile application, wireless communication structure based on JSON web service basics. Researchers need to deploy backend server and mobile application and install hardware components to simulate and validate our offered model.

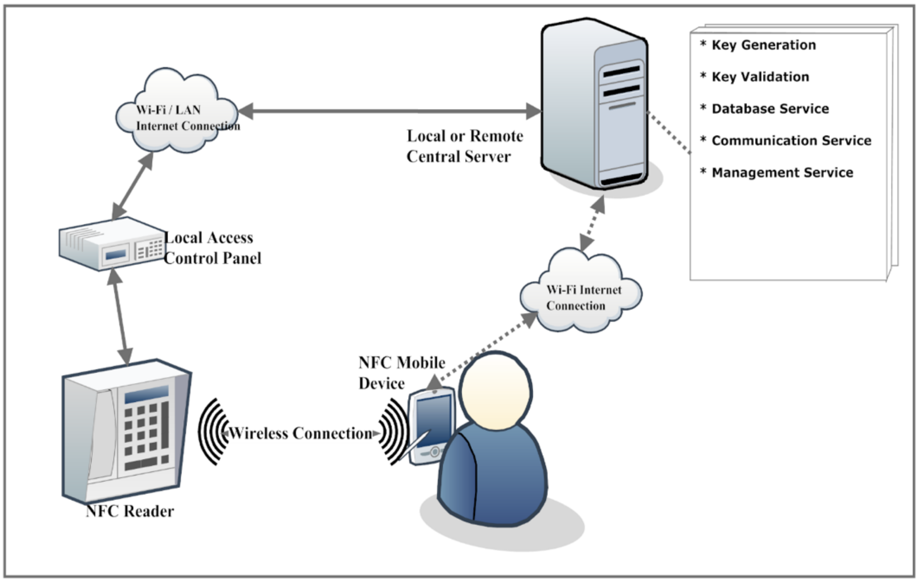


Figure 27: NFC Based Access Control System

The high-level components of NFC based access control systems are:

- **NFC Enabled mobile phone:** Stores credentials in secure environment and establish NFC connection with NFC reader with card emulation mode and sends encapsulated credentials with required headers. Also establishes connection with server via secure web service for registering and getting credentials.

- **NFC Reader:** Initiates connection with mobile phone reads and forwards the key to control panel.

- **Access Control Panel:** Acts as local management forwards the credentials to Central Server in secure manner or controls credentials locally according to application if it has authority table in its local memory. Establishes connection with reader according to Wiegand protocol principles via RS232 or USB connections. Supports more than one NFC reader connections.

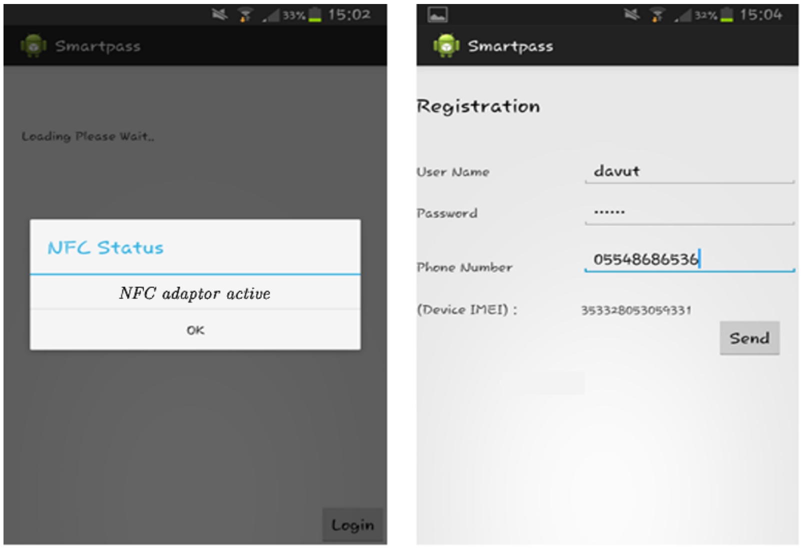
- **Central Server:** Administers authentication, authorization, encoding, storing, managing and other related operations. Establishes connections with access control panel and mobile devices in secure web service message mechanisms. Includes Key Generation, Key Validation, Database Service, Communication Service and Management modules.

7.3 Flow of Operations

The general activity flow of NFC based access control system begins with controlling whether NFC unit is active or not. If NFC is enabled, user registers to system with his/her mobile operator number, username etc. via application that installed on device. Once user is registered to system, central server activates his/her authorizations if defined previously and sends to activation key to authenticated mobile device in the form of encrypted manner. Mobile device stores them into its operating system isolated hardware unit (Secure Element).

After registration process is completed successfully, user can now send access requests with his/her user name, password and period of time parameters. The system remembers the choice and does not generate new key until the end of the time period that is defined during login session.

When user wants to have an access to door, s/he touches the mobile phone screen close enough to reader and sends request using mobile application interface. The mobile phone applies two-layer static and dynamic encapsulation to user access key before sending. The mobile transactions are illustrated as screenshots in Figure 28 and 29. Local access control panel forwards to access request that comes from NFC reader to central server. Two-layer encapsulated access key is opened and it is evaluated according to pre-defined functions, context aware rules, algorithms and encryption techniques. According to evaluation, access is granted or denied.



Loading Please Wait..

NFC Status

NFC adaptor active

Registration

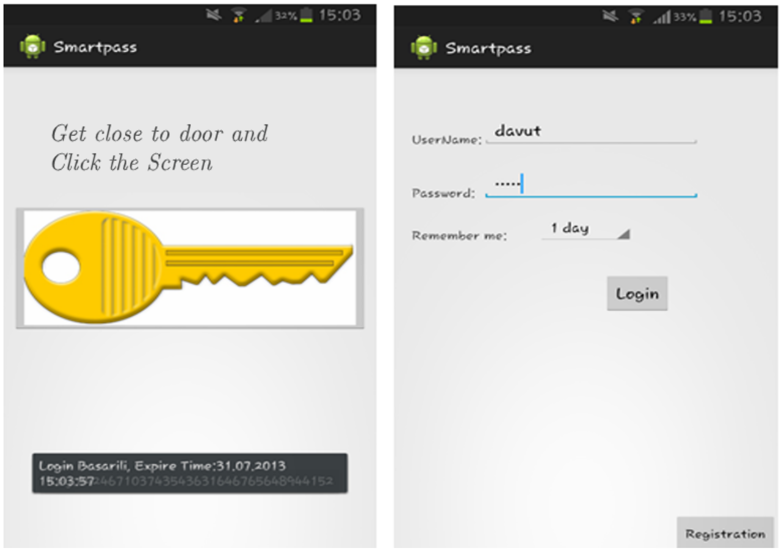
User Name davut

Password ······

Phone Number 05548686536

(Device IMEI) : 353328053059331

Figure 28: Registration Screen of Mobile Application



Get close to door and
Click the Screen

Login Basarili, Expire Time:31.07.2013 15:03:572467103743543631646765648944152

UserName: davut

Password: ·····

Remember me: 1 day

Figure 29: Request and Login Screens of Mobile Application

Table 9: Description of Services of the Implementation

In order to complete system cycle, microcontroller is also connected to computer and after local access control panel receive a request, it forwards to central server and gets the response. According to response, control panel gives an order to microcontroller about whether door will be opened or not. The microcontroller gives 5V to predefined output port which also electronic lock is connected.

Service Name	Endpoint Interface	Description
Login	serverIp:serverport/smartpassApplication-2.0/rest/authentication/login/{username}/{password}/{activeDayCount}	response format: {"expireTime":"dateTime", "status":"0 or 1","key":"rule based generated"}
Lock Door	serverIp:serverport/smartpassApplication-2.0/rest/doorOperation/lockDoor/{key}/{doorId}	response format: {"response":"-1, 0 or 1"} "1" means that user has an authorization "0" means that user doesn't have authorization "-1" means that door has not been registrated before
Unlock Door	serverIp:serverport/smartpassApplication-2.0/rest/doorOperation/unlockDoor/{key}/{doorId}	response format: {"response":"-1, 0 or 1"} "1" means that user has an authorization "0" means that user doesn't have authorization "-1" means that door has not been registrated before
Registration	serverIp:serverport/smartpassApplication-2.0/rest/registration/sendRegistrationRequest/{username}/{password}/{phoneNumber}/{imei}	response: {"status":"0 or 1", "key":"0 or rule based genetated"} "status": "0" means that username has already used "status": "1" means that username has already used
Activation	serverIp:serverport/smartpassApplication-2.0/rest/registration/sendUserActivationRequest/{username}/{password}/{phoneNumber}/{imei}/{key}	response format: {"status":"0 or 1"} 0 means that activation has failed 1 means that activation has been successful.

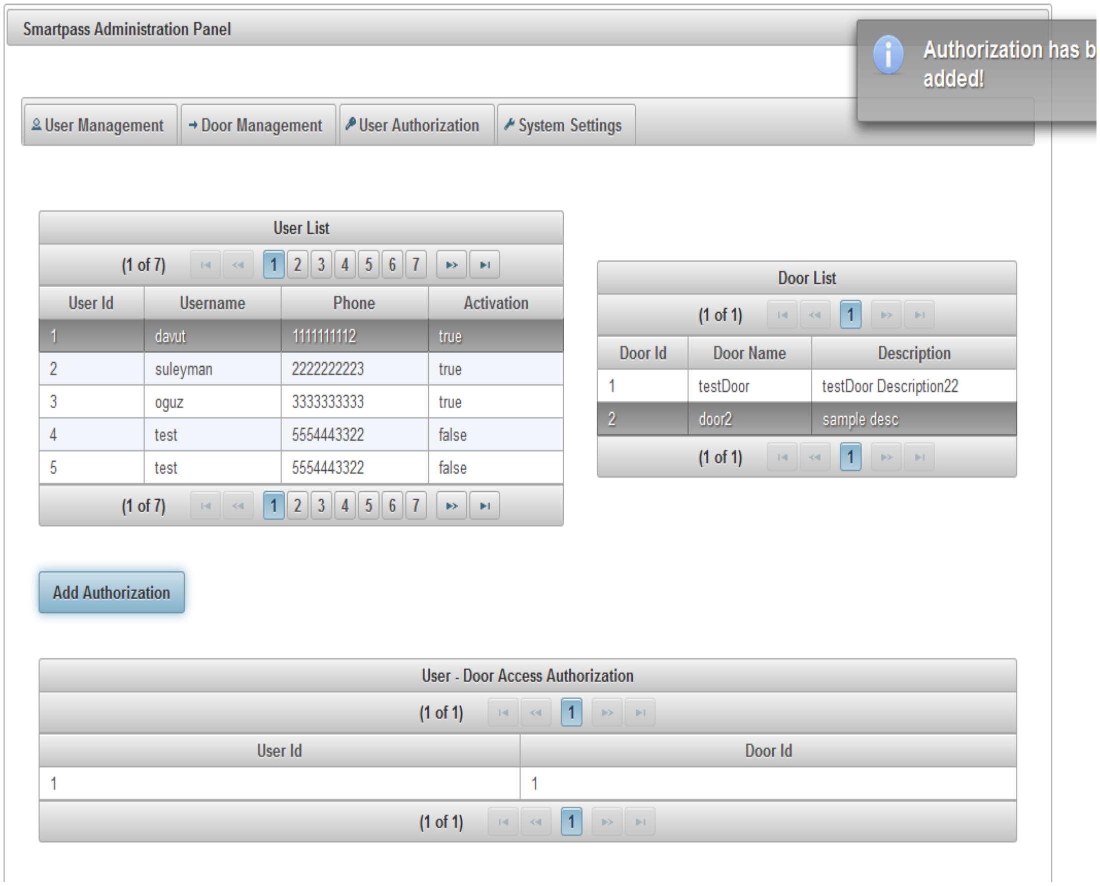
The communication between mobile device – server and access control panel-server are performed via web services. As a web service infrastructure, JSON infrastructure is used because of its flexibility, interoperability and communication speed. The services, required parameters and response formats are described in Table 9.

Majority of system transactions are performed by central server software. It is designed in modular based. The modules are Database Service, Communication Service, Session Manager, Role Manager, Permission Manager, Context Engine, Conflict Engine and Key Engine. After logging onto system, key engine generates user key and sent it through communication service based on JSON web service. User creates request package with his key and contextual information and sent it through NFC reader when he wants to access resource. Context engine interprets and verifies the retrieved context in the package in its sub-modules. According to XML based predefined rules, conditions and tuples that are retrieved from database service, required assignments are sent to role and permission manager. Also, according to mentioned conditions, context engine may revoke these assignments when needed. Finally, response is sent to both physical access control component and mobile device again through communication service in wired connection and web service.

7.4 Implementation

7.4.1 High-Level Use Cases of the Implementation of the Model

Although variety of scenarios can be implemented in the testbed to show validity and coverage of the model, the high-level use cases can be categorized into the four main groups. The first group is Relay User which includes relay attack tries using contextual parameters. Because proposed model aims to detect and prevent the Relay Attacks in the proposed scope, this use case group is studied and implemented in order to show the validity of the model. The other two groups include the tries of the normal users.



Authorization has b
added!

User List

(1 of 7) 1 2 3 4 5 6 7

User Id	Username	Phone	Activation
1	davut	1111111112	true
2	suleyman	2222222223	true
3	oguz	3333333333	true
4	test	5554443322	false
5	test	5554443322	false

(1 of 7) 1 2 3 4 5 6 7

Door List

(1 of 1) 1

Door Id	Door Name	Description
1	testDoor	testDoor Description22
2	door2	sample desc

(1 of 1) 1

User - Door Access Authorization

(1 of 1) 1

User Id	Door Id
1	1

(1 of 1) 1

Figure 30: Web Management Panel of Implementation

The proposed model is developed at the top of the Role Based Access Control Model (RBAC), therefore the main principles of the RBAC also should be verified in the implementation. Based on the principles of the RBAC and the proposed model, the requests of the normal users are evaluated using their contextual information like Relay Users and “Deny” and “Allow” responses are generated after applying policy rules. These high level uses cases are provided in the Table 10.

Table 10: High Level Use Cases of the Implementation

Group	Use Case Identifier	Description of Use Case	Formal Representation	Result
Initial Checks	IC1	No contextual information is not provided within the request envelope.	c == null	Deny
	IC2	Subject is not assigned to any role.	getUserRole (s, $\prod_{smc} c$) == Ø	Deny
	IC3	No rule is defined for requested role, context and permission.	getRolePermissions (r, $\prod_{smc} c$, $\prod_{obj,op} p$) == Ø	Deny
Relay User (Attack)	RU1	The Relay Attack use case. The location context in the user request is different than the	Lp !=CLp	Deny

		confirmed by the system in the second cycle of the model.		
	RU2	The Relay Attack use case. The time context in the user request is different than the confirmed by the system in the second cycle of the model.	$Tp!=CTp$	Deny
Normal User - Context Control (Deny)	NUD1	The time and location context in the user request are same with the confirmed by the system in the second cycle of the model, however the distance from the object is higher than the threshold defined in the policy therefore the validation of verify context () function fails.	$Lp=CLp$ and $Tp=CTp$ and $\lvert x-Lp \rvert > Td$	Deny

	NUD2	The time and location context in the user request are same with the confirmed by the system in the second cycle of the model, however the time of the request is before the time defined in the policy therefore the validation of verify context () function fails.	$Lp=CLp$ and $Tp=CTp$ and $\|x-Lp\| <=Td$ and $Tp<Ts$	Deny
	NUD3	The time and location context in the user request are same with the confirmed by the system in the second cycle of the model, however the time of the request is after the time defined in the policy therefore the validation of verify context () function fails.	$Lp=CLp$ and $Tp=CTp$ and $\|x-Lp\| <=Td$ and $Tp>Te$	Deny
	NUD4	Access is not granted if only even one “deny” result received	$\exists q \in R(q = deny)$	Deny

		from getRolePermissions function although it has “allow” results.		
Normal User - Context Control (Allow)	NUA1	The time and location context in the user request are same with the confirmed by the system in the second cycle of the model also, the contextual information is validated and validation of verify context () function passes, as a result access is granted.	Lp=CLp and Tp=CTp and |x-Lp| <=Td and Ts<=Tp<=Te	Allow

7.4.2 Sample Scenario

In order to demonstrate validity and coverage of the model, we have created a sample Security Research Centre scenario based on the RBAC principles. The main components of the scenario are listed in Table 11.

Table 11: The Components of Sample Scenario

Name	**Components**
Objects (door of)	• 5G Laboratory • Administrative Office • Library • Social Room • Lobby
Operation	• Unlock Door
Roles	• Researchers • Graduate Students • B.Sc. Students • Administrative Staff • Visitors • Security Guards
Subjects	• David: (assigned to Researchers Role) • John: (assigned to Graduate Students Role) • Diana: (assigned to B.Sc. Students Role)

	• Barbara: (assigned to Administrative Staff Role) • Alex: (assigned to Visitors Role) • Morpheus: (assigned to Security Guards Role)
Context	**Dynamic Context:** • Location (Lp): Location value of the phone during request • Time (Tp): Time value of the phone during request **Static Context:** • Phone Number • User Key

7.4.3. Rule Set for the Scenario

The following set describes the rules that used in the evaluation of the requests. In addition to description of the rule set, an additional formal description table including the role, operation, object, context, related use case and result of the rule set is provided for each one.

1) The subjects (users) cannot open any door if the contextual information is not provided.

2) The subjects (users) cannot open any door if the subject is not assigned to any role.

3) The subjects (users) cannot open any door if no rule is defined for requested role, context and permission.

4) The subjects (users) cannot open any door even if only one deny result received from getRolePermissions function although it has allow results.

5) The subjects (users) cannot open any door unless attack parameters are successfully verified.

6) The subjects (users) of the “Researchers” group can open the doors of the all buildings (objects) at all times of the day (7x24).

7) If the distance value to the doors is higher than the predefined threshold value (Td= 0.001, 0.001 (~10m)), access is not granted. |x-Lp| > Td.

8) Only subjects (users) of the “Administrative Staff” can open the door of the administrative office after the working hours (6PM - 8AM). Others cannot (deny).

9) The subjects (users) of the “Graduate Students” group can open the doors of the all buildings (objects) at the working hours (8AM- 6PM).

10) The subjects (users) of the “B.Sc. Students” group can open the doors of library, social room and lobby (objects) at the working hours (8AM- 6PM).

11) The subjects (users) of the “Administrative Staff” group can open the doors of administrative office, library, social room and lobby (objects) at the working hours (8AM- 6PM).

12) The subjects (users) of the “Visitors” group can open the doors of social room and lobby (objects) at the working hours (8AM- 6PM).

13) The subjects (users) of the “Security Guards” group can open the doors of social room and lobby (objects) at all times of the day (7x24).

14) The door of the library is closed in maintenance week (Aug 1 - Aug 8) and Christmas period (Dec 24 – Jan 2) each year.

15) Only subjects (users) of the “Researchers” and “Graduate Students” can open the door of the laboratory after the working hours (6PM - 8AM). Others cannot (deny).

16) The door of the social room is closed in maintenance hour (6PM – 7PM) each day.

Table 12: Formal Description of Rule Set for Scenario

#	Role	Operation	Object	Contextual Description	Use Case	Result
1	Any	Unlock Door	Any	c == null	IC1	Deny
2	Any		Any	getUserRole(s, $\prod_{smc} c$) == Ø	IC2	Deny
3	Any		Any	getRolePermissions (r,$\prod_{smc} c$, $\prod_{obj,op} p$)== Ø	IC3	Deny
4	Any		Any	$\exists q \in R(q = deny)$	NUD4	Deny
5	Any		Any	Lp != CLp	RU1	Deny
6	Any		Any	Tp != CTp	RU2	Deny
7	Any		Any	$\lvert x\text{-}Lp \rvert > (0.001, 0.001)$	NUD1	Deny
8	Researchers		Any	(Tp != null) $\wedge$ ($\lvert x - Lp \rvert$ $\leq$ (0. 001, 0.001))	NUA1	Allow

9	Administrative Staff		Administrative Office	$(6PM < Tp < 8AM) \wedge$ $(\lvert x - Lp \rvert \leq (0.001, 0.001))$	NUA1	Allow
10	$\neg$ Administrative Staff		Administrative Office	$(6PM < Tp < 8AM)$	NUD2 and NUD3	Deny
11	Graduate Students		Any	$(8AM < Tp < 6PM) \wedge$ $(\lvert x - Lp \rvert \leq (0.001, 0.001))$	NUA1	Allow
12	B.Sc. Students		Library	$(8AM < Tp < 6PM) \wedge$ $(\lvert x - Lp \rvert \leq (0.001, 0.001))$	NUA1	Allow
13	B.Sc. Students		Social Room	$(8AM < Tp < 6PM) \wedge$ $(\lvert x - Lp \rvert \leq (0.001, 0.001))$	NUA1	Allow
14	B.Sc. Students		Lobby	$(8AM < Tp < 6PM) \wedge$	NUA1	Allow

				(|x − Lp| ≤ (0.001, 0.001))		
15	Administrative Staff		¬ 5G Laboratory	(8AM < Tp < 6PM) ∧ (|x − Lp| ≤ (0.001, 0.001))	NUA1	Allow
16	Visitors		Social Room	(8AM < Tp < 6PM) ∧ (|x − Lp| ≤ (0.001, 0.001))	NUA1	Allow
17	Visitors		Lobby	(8AM < Tp < 6PM) ∧ (|x − Lp| ≤ (0.001, 0.001))	NUA1	Allow
18	Security Guards		Social Room	Tp != null ∧ (|x − Lp| ≤ (0.001, 0.001))	NUA1	Allow
19	Security Guards		Lobby	Tp != null ∧ (|x − Lp| ≤ (0.001, 0.001))	NUA1	Allow
20	Any		Library	((Dec 24 < Tp < Jan 2) ∨	NUD2 and NUD3	Deny

				(Aug 1 < Tp < Aug 8))		
21	Researchers and Graduate Students		5G Laboratory	$(6PM < Tp < 8AM) \wedge (\lvert x - Lp \rvert \leq (0.001, 0.001))$	NUA1	Allow
22	¬ Researchers and Graduate Students		5G Laboratory	(6PM < Tp < 8AM)	NUD2 and NUD3	Deny
23	Any		Social Room	(6PM < Tp < 7PM)	NUD2 and NUD3	Deny

7.4.4 Access Requests

Although calculation of the indoor positioning is out of scope of the study, we have used geographic coordinates in decimal degrees to define the location of the requester in calculation. We assume that the location of the scenario is at 41.082630 (latitude) 28.633028 (longitude) and the threshold value (Td) is 0.001, 0.001 (~10m).

Some requests may cover multiple use cases such as request 1 addresses the use case 5 and 6. In daily rules of the policies, the request time may be both after the end time current day and before the start time of the following day. Another multiple coverage occurs when requests have multiple rule in the given context such as request 2. In some requests, multiple coverage would not be possible. The high-level use cases 1, 2 and 3 have priority in the rule check in the evaluation and when they fail then no need to check another case and rule. Use case 1 and 2 describe relay attack cases and use case 3 identifies the context existence in the request.

Access Request 1 (Use Case NUD2 and NUD3)

Description: Diana wants to open the door of the 5G Laboratory at 08:00PM in the location 41.082630, 28.633028:

getUserRole (diana, “key”) = **B.Sc. Students**

CLp = 41.082630, 28.633028

CTp = 08:00PM

Given rule set for the request:

getRolePermissions (B.Sc. Students, {08:00PM, (41.082630, 28.633028)}, {5G Laboratory, unlock door}) =>

¬Researchers and Graduate Students	Unlock Door	5G Laboratory	(6PM < Tp < 8AM)	Deny

Permission Set (P) = {deny}, therefore permission is **not** granted.

Access Request 2 (Use Case NUA1, NUD3, NUD4)

Description: David wants to open the door of the Social Room at 06:30PM in the location 41.082630, 28.633028:

getUserRole (david, “key”) = **Researchers**

CLp = 41.082630, 28.633028

CTp = 06:30PM

getRolePermissions(Researchers, {06:30PM, (41.082630, 28.633028)}, {Social Room, unlock door}) =>

Given rule set for the request:

Researchers	Unlock Door	Any	$(Tp \mathrel{!=} null) \land (\lvert x - Lp \rvert \leq Td)$	Allow
Any	Unlock Door	Social Room	(6PM < Tp < 7PM)	Deny

Permission Set (P) = {allow, deny}, therefore, permission is **not** granted.

Access Request 3 (Use Case IC3)

Description: Morpheus wants to open the door of the Library at 04:30PM in the location 41.082630, 28.633028:

getUserRole(morpheus, “key”) = **Security Guards**

CLp = 41.082630, 28.633028

CTp = 04:30PM

getRolePermissions(Researchers, {04:30PM, (41.082630, 28.633028)}, {Social Room, unlock door}) =>

Given rule set for the request: None

Permission Set (P) = Ø, therefore, permission is **not** granted.

Access Request 4 (Use Case NUA1)

Description: John wants to open the door of the 5G Laboratory at 10:00AM in the location 41.082630, 28.633028

getUserRole(john, “key”) = **Graduate Students**

CL_p = 41.082630, 28.633028

CT_p = 10:00AM

Given rule set for the request:

getRolePermissions(Graduate Students,{10:00AM, (41.082630, 28.633028)}, {5G Laboratory, unlock door}) =>

Graduate Students	Unlock Door	Any	$(8AM < Tp < 6PM) \wedge$ $(\lvert x - Lp\rvert \leq (0.001, 0.001))$	Allow

Permission Set (P) = {allow}, therefore, permission is **granted.**

Access Request 5 (Relay Case, RU1)

Description: Barbara wants to open the door of the Library at 09:00AM in the location 41.082630, 28.633028

getUserRole(barbara, “key”) = **Administrative Staff**

CL_p = 41.095630, 28.583028

CT_p = 09:00AM

Given rule set for the request:

getRolePermissions(Administrative Staff,{09:00AM, 41.082630, 28.633028}, {Library, unlock door}) =>

Administrative Staff	Unlock Door	$\neg$ 5G Laboratory	$(8AM < Tp < 6PM) \wedge$ $(\lvert x - Lp\rvert \leq (0.001, 0.001))$	Allow

Because of location of the phone is not equal to confirmed location of the phone (L_p != CL_p), this case assumed as relay attack case. Although subject is authorized on the object in this context, permission is **not** granted**.**

Access Request 6 (Relay Case, RU2)

Description: Barbara wants to open the door of the Social Room at 9:00AM in the location 41.082630, 28.633028

getUserRole(barbara, “key”) = **Administrative Staff**

CL_p = 41.082630, 28.633028

CT_p = 9:28AM

Given rule set for the request:

getRolePermissions(Administrative Staff,{9:00AM, (41.082630, 28.633028)}, { Social Room, unlock door}) =>

Administrative Staff	Unlock Door	¬ 5G Laboratory	$(8AM < Tp < 6PM) \wedge$ $(\lvert x - Lp \rvert \leq (0.001, 0.001))$	Allow

Because of time of the phone is not equal to confirmed time of the phone (T_p != CT_p), this case assumed as relay attack case, although subject is authorized on the object in this context, permission is **not** granted**.**

Access Request 7 (Use Case IC1)

Description: David wants to open the door of the 5G Laboratory with no contextual information.

The function of getUserRole cannot return any role because no contextual information is provided. Also, according to the Use Case IC1 and Rule Set 1 state that “The subjects (users) cannot open any door if the contextual information is not provided.” Based on these principles, context parameters should be provided with the request in order to validate access requests, therefore, permission is **not** granted**.**

Access Request 8 (Use Case NUD1)

Description: Morpheus wants to open the door of the Social Room at 09:00AM in the location 42.082630, 28.633028

getUserRole(morpheus, “key”) = **Security Guards**

CL_p = 42.095630, 28.583028

CT_p = 09:00AM

Given rule set for the request:

getRolePermissions(Security Guards,{09:00AM, 41.082630, 28.633028 }, { Social Room, unlock door}) =>

Any	Unlock Door	Any	|x-Lp| > (0.001, 0.001)	Deny

The location value of the request does not meet to location threshold calculation. The location of the door is in 41.082630, 28.633028 and the threshold value is Td= 0.001, 0.001 (~10m) on the other hand provided location value is 42.082630, 28.633028, therefore it does not meet the Rule 7 (x-Lp| > Td), therefore, permission is **not** granted**.**

Access Request 9 (Use Case IC2)

Description: Bob wants to open the door of the Library at 11:20AM in the location 42.082630, 28.633028

getUserRole(bob, “key”) = **null**

CL_p = 42.095630, 28.583028

CT_p = 11:20AM

According to the Use Case IC2 and Rule Set2 (getUserRole(s, $\prod_{smc} c$)== Ø), the subjects (users) cannot open any door if the subject is not assigned to any role. The subject “Bob” who is included in the request is not assigned to the any role according to the predefined User-Role function of the scenario. Because user-role assignment check is one of the initial checks of the implementation, other contextual controls are not performed and request is denied, therefore, permission is **not** granted**.**

7.4.5 Coverage Analysis of the Model

Based on the high-level use cases of the model which described in this chapter, we have created a sample scenario for the implementation. Then we have created rule set addressing the high-level use cases. In order to cover all high-level use cases of the model and common security principles of access control systems, we have designed and implemented 8 different access requests.

We have identified 3 sets; Use Cases **(UC)**, Rule Set **(RS)** and Access Requests **(AR)** in order to evaluate and show the coverage of the access requests that implemented in the study. The set of UC includes high-level use cases described in this chapter based on four different usage groups. AR set includes 9 access requests trying to address all high-level Use Cases **(UC)** and Rule Set **(RS).**

In order to demonstrate all request combinations, attributes are identified and grouped as categories. The sets of categories are as follows:

Role Category (RoC)

1) No Role - getUserRole(s, $\prod_{smc} c$) == Ø
2) Role(s) Exist – Dependent to other categories (RuC, CoC)

Rule Category (RuC)

1) No Rule - getRolePermissions (r, $\prod_{\mathrm{d}mc} c$, $\prod_{obj,op} p$) == Ø
2) Rule(s) Exist – At Least One Deny - $\exists q \in R(q = deny)$
3) Rule(s) Exist - No Deny - At least One Allow – Dependent to other categories (CoC)

Context Category (CoC)

1) Context not provided (null)
2) Not Confirmed Location of Phone – Clpi
3) Not Confirmed Time of Phone – Ctpi
4) Relay Context Confirmed but Invalid Location of Phone Context - Lpi
5) Relay Context Confirmed & Valid Location but Time of Phone Context not Confirmed - Lpv, Tpi
6) All Contexts are confirmed - CLpv, CTpv, Lpv, Tpv

CoC = {null, {(CLpi, c) | c ∈ NUC}, {(CTpi, c) | c ∈ NUC}, {CLpv, CTpv, Lpi}, {CLpv, CTpv, Lpv, Tpi}, {CLpv, CTpv, Lpv, Tpv}}

Where;

CLpi = Not Confirmed Location of Phone

CLpv = Confirmed Location of Phone

CTpi = Not Confirmed Time of Phone

CTpv = Confirmed Time of Phone

null = No context is provided

NUC (NormalUserContext) = {Lpi, Lpv, Tpi, Tpv}

Where;

Lpi = Not Confirmed Location of Phone Context

Lpv = Confirmed Location of Phone Context

Tpi = Not Confirmed Time of Phone Context

Tpv = Confirmed Time of Phone Context

Finally, all request combinations are the cartesian product given as;

RoC X RuC X CoC = { (a,b,c) | a $\in$ RoC, b $\in$ RuC and c $\in$ CoC }, the number of the elements in the cartesian product is;

s(RoC X Ruc X CoC) = s(RoC) * s(RuC) * s(CoC) = 2 * 3 * 6 = 36 elements. These 36 requests combinations are all covered by 9 access requests described in this chapter because of the controls of initial checks. According to these initial checks, when context is not provided, role or rule is not defined then implementation does not evaluate other parameters in the requests. Based on this approach, one access request can cover many combinations.

All the combinations and access requests which cover these combinations are illustrated in the Table 13.

Table 13: All the Possible Combinations of the Requests

	Role Category (RoC)	**Rule Category (RuC)**	**Context Category (CoC)**	**Covered By**
1	No Role (RoC1)	No Rule (RuC1)	Context not provided (CoC1)	Access Request 7
2	No Role (RoC1)	No Rule (RuC1)	Not Confirmed Location of Phone – Clpi- (CoC2)	Access Request 9
3	No Role (RoC1)	No Rule (RuC1)	Not Confirmed Time of Phone – Ctpi- (CoC3)	Access Request 9
4	No Role (RoC1)	No Rule (RuC1)	Relay Context Confirmed but Invalid Location of Phone Context - Lpi- (CoC4)	Access Request 9
5	No Role (RoC1)	No Rule (RuC1)	Relay Context Confirmed & Valid Location but Time of Phone Context not Confirmed - Lpv, Tpi - (CoC5)	Access Request 9
6	No Role (RoC1)	No Rule (RuC1)	All Contexts are confirmed - CLpv, CTpv, Lpv, Tpv- (CoC6)	Access Request 9
7	No Role (RoC1)	Rule(s) Exist – At Least One Deny (RuC2)	Context not provided (CoC1)	Access Request 7
8	No Role (RoC1)	Rule(s) Exist – At Least One Deny (RuC2)	Not Confirmed Location of Phone – Clpi- (CoC2)	Access Request 9

9	No Role (RoC1)	Rule(s) Exist – At Least One Deny (RuC2)	Not Confirmed Time of Phone – Ctpi- (CoC3)	Access Request 9
10	No Role (RoC1)	Rule(s) Exist – At Least One Deny (RuC2)	Relay Context Confirmed but Invalid Location of Phone Context - Lpi- (CoC4)	Access Request 9
11	No Role (RoC1)	Rule(s) Exist – At Least One Deny (RuC2)	Relay Context Confirmed & Valid Location but Time of Phone Context not Confirmed - Lpv, Tpi - (CoC5)	Access Request 9
12	No Role (RoC1)	Rule(s) Exist – At Least One Deny (RuC2)	All Contexts are confirmed - CLpv, CTpv, Lpv, Tpv- (CoC6)	Access Request 9
13	No Role (RoC1)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Context not provided (CoC1)	Access Request 7
14	No Role (RoC1)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Not Confirmed Location of Phone – Clpi- (CoC2)	Access Request 9
15	No Role (RoC1)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Not Confirmed Time of Phone – Ctpi- (CoC3)	Access Request 9
16	No Role (RoC1)	Rule(s) Exist - No Deny - At least	Relay Context Confirmed but Invalid Location of	Access Request 9

		One Allow (RuC3)	Phone Context - Lpi- (CoC4)	
17	No Role (RoC1)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Relay Context Confirmed & Valid Location but Time of Phone Context not Confirmed - Lpv, Tpi - (CoC5)	Access Request 9
18	No Role (RoC1)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	All Contexts are confirmed - CLpv, CTpv, Lpv, Tpv- (CoC6)	Access Request 9
19	Role(s) Exist (RoC2)	No Rule (RuC1)	Context not provided (CoC1)	Access Request 7
20	Role(s) Exist (RoC2)	No Rule (RuC1)	Not Confirmed Location of Phone – Clpi- (CoC2)	Access Request 3
21	Role(s) Exist (RoC2)	No Rule (RuC1)	Not Confirmed Time of Phone – Ctpi- (CoC3)	Access Request 3
22	Role(s) Exist (RoC2)	No Rule (RuC1)	Relay Context Confirmed but Invalid Location of Phone Context - Lpi- (CoC4)	Access Request 3
23	Role(s) Exist (RoC2)	No Rule (RuC1)	Relay Context Confirmed & Valid Location but Time of Phone Context not Confirmed - Lpv, Tpi - (CoC5)	Access Request 3
24	Role(s) Exist (RoC2)	No Rule (RuC1)	All Contexts are confirmed - CLpv, CTpv, Lpv, Tpv- (CoC6)	Access Request 3

25	Role(s) Exist (RoC2)	Rule(s) Exist – At Least One Deny (RuC2)	Context not provided (CoC1)	Access Request 7
26	Role(s) Exist (RoC2)	Rule(s) Exist – At Least One Deny (RuC2)	Not Confirmed Location of Phone – Clpi- (CoC2)	Access Request 2
27	Role(s) Exist (RoC2)	Rule(s) Exist – At Least One Deny (RuC2)	Not Confirmed Time of Phone – Ctpi- (CoC3)	Access Request 2
28	Role(s) Exist (RoC2)	Rule(s) Exist – At Least One Deny (RuC2)	Relay Context Confirmed but Invalid Location of Phone Context - Lpi- (CoC4)	Access Request 2
29	Role(s) Exist (RoC2)	Rule(s) Exist – At Least One Deny (RuC2)	Relay Context Confirmed & Valid Location but Time of Phone Context not Confirmed - Lpv, Tpi - (CoC5)	Access Request 2
30	Role(s) Exist (RoC2)	Rule(s) Exist – At Least One Deny (RuC2)	All Contexts are confirmed - CLpv, CTpv, Lpv, Tpv- (CoC6)	Access Request 2
31	Role(s) Exist (RoC2)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Context not provided (CoC1)	Access Request 7
32	Role(s) Exist (RoC2)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Not Confirmed Location of Phone – Clpi- (CoC2)	Access Request 5

33	Role(s) Exist (RoC2)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Not Confirmed Time of Phone – Ctpi- (CoC3)	Access Request 6
34	Role(s) Exist (RoC2)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Relay Context Confirmed but Invalid Location of Phone Context - Lpi- (CoC4)	Access Request 8
35	Role(s) Exist (RoC2)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	Relay Context Confirmed & Valid Location but Time of Phone Context not Confirmed - Lpv, Tpi - (CoC5)	Access Request 1
36	Role(s) Exist (RoC2)	Rule(s) Exist - No Deny - At least One Allow (RuC3)	All Contexts are confirmed - CLpv, CTpv, Lpv, Tpv- (CoC6)	Access Request 4

7.5 Performance Tests

We have performed some performance tests in order to evaluate model’s live performance in our test bed. The results may change according to environment such as hardware and software solutions, programming languages or database types. In order to avoid these affects, we performed this performance test in identical environments.

Two separate test sets have been performed to compare performance of response times of the proposed model. First test set has a composition of mixed types of different use cases. This composition is %10 IC1 - %10 IC2 - %10 IC3 - %15 NUD1 - %15 NUD2 - %15 NUD3 - %15 NUD4 - %15

NUA1. The second set composition consists of %50 RU1- %50 RU2. We aim to analyze the performance of the model for both mixed compositions of different types of access requests and relay requests.

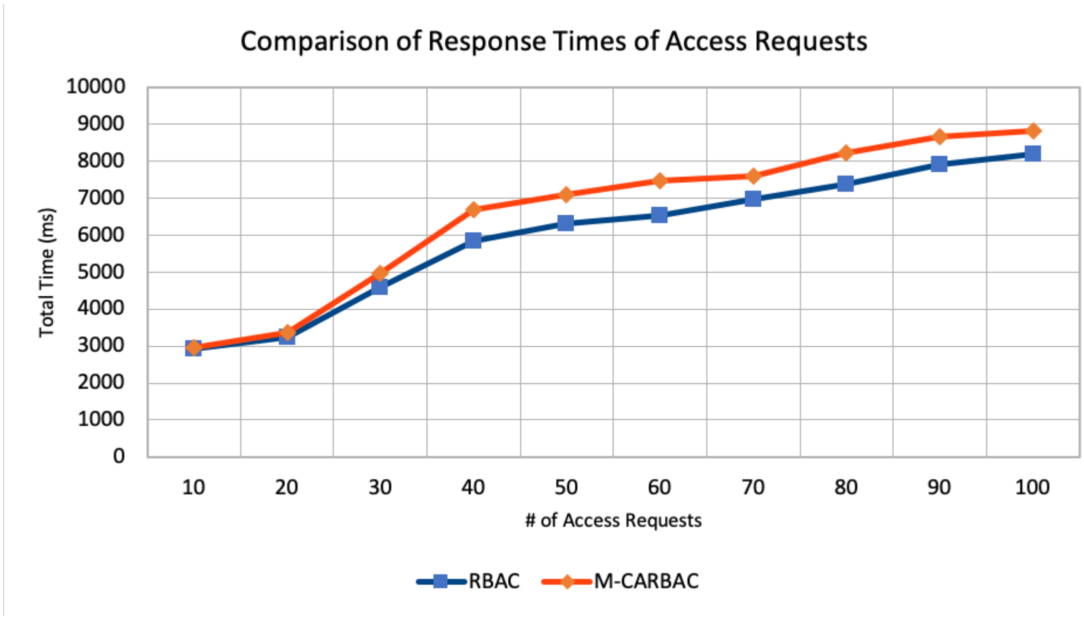


Figure 31: Comparison Response Times of RBAC and MCARBAC (Mixed Use Cases)

The results of first test set which includes mixed types of use case requests are illustrated in the Figure 31 and the results of second test set which includes mixed relay attack use case requests are illustrated in the Figure 33 as line graphs in terms of number of access requests and times required for these evaluation operations based on the principals of the models RBAC and the proposed model.

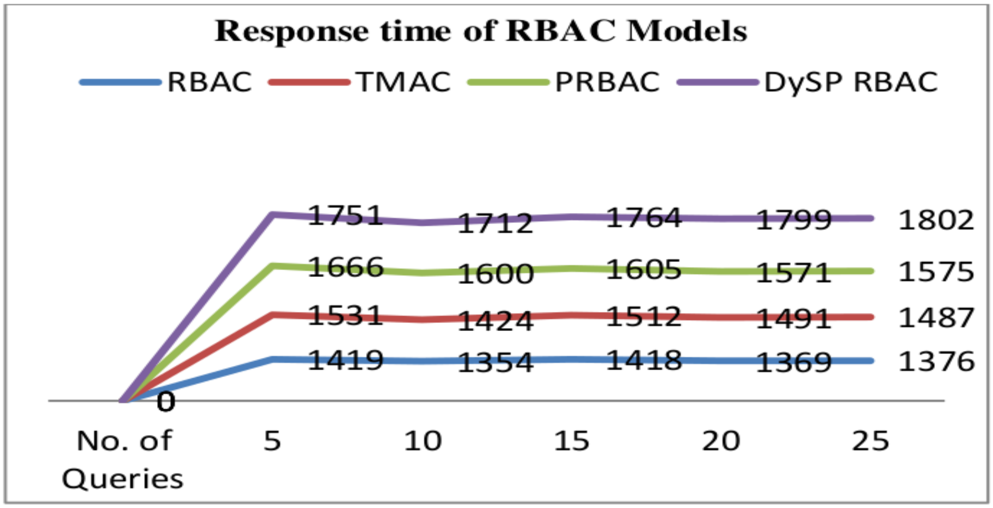


Figure 32: Response Times of RBAC Models [67]

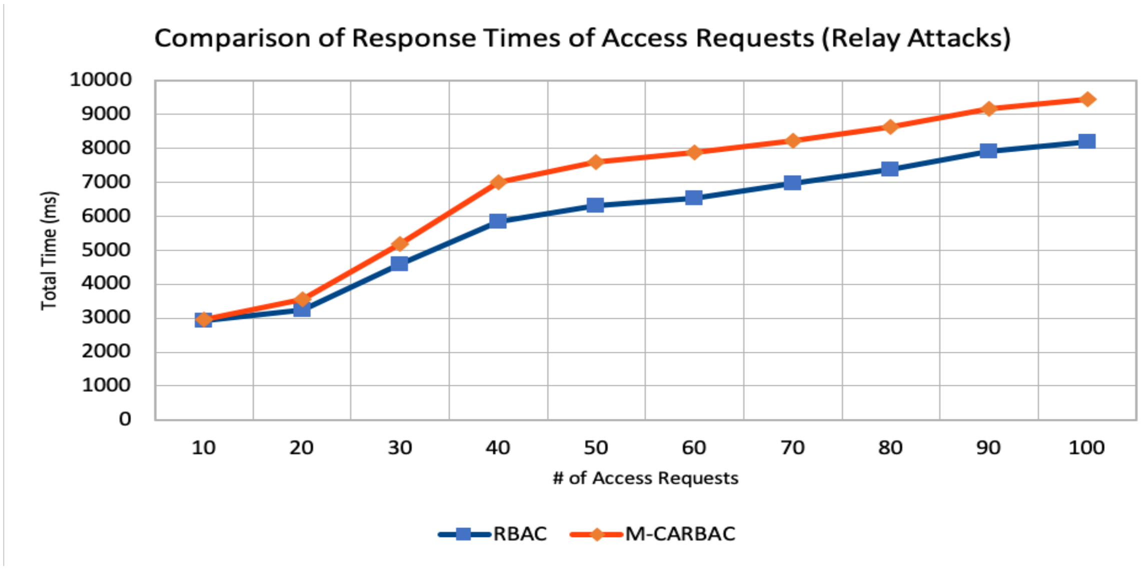


Figure 33: Comparison Response Times of RBAC and MCARBAC (Relay Attacks)

The performance of our model is acceptable although a bit lower than RBAC model. According to the study [67], the performance of RBAC is better than all its derivatives like our model, which illustrated in Figure 32. The increase in the number of queries result in increase of the response time of the both models as natural. According to the results, a little bit more time is needed for requests containing only relay attack, than those containing a mixed request composition. Because, each relay attack requests are evaluated in the both first and second cycle of the controls, on the other hand, some normal user requests can be denied in the initial controls such as requests including no context etc.

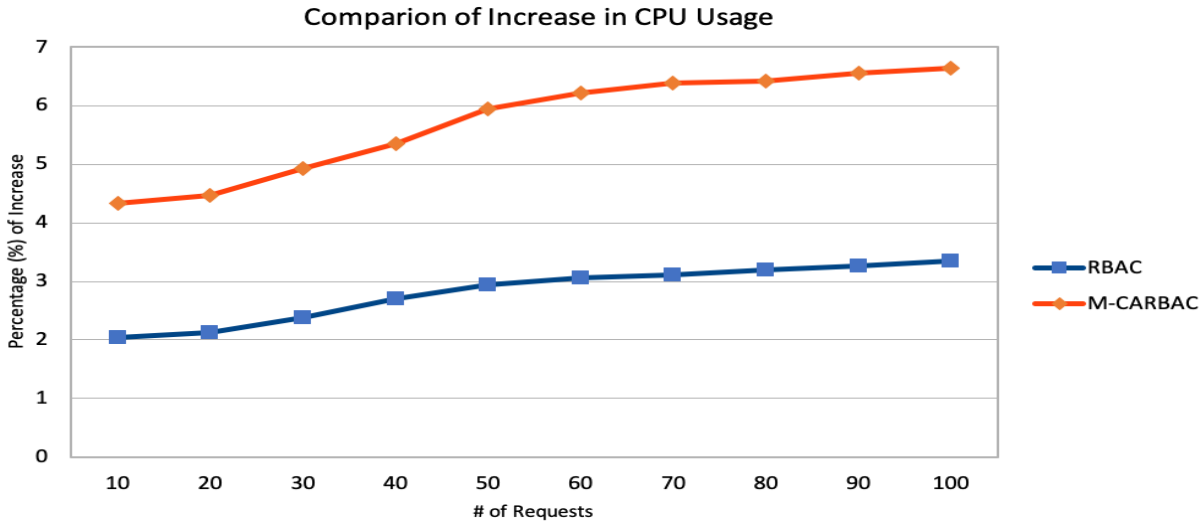


Figure 34: Comparison of Increase in CPU Usage of RBAC and MCARBAC (Mixed Use Cases)

In addition to test response and process times of queries, we have also performed and analyzed increase in CPU usage comparing RBAC, which our model is based on, and M-CARBAC. These CPU usage tests are performed on the Intel seventh generation 8 Core CPU with 25, 50, 75 and 100 queries using first test set which includes requests of mixed-use cases. Then, average CPU usages during request handling are calculated automatically based on the data retrieved from benchmark of system hardware.

The results of the CPU usage of models is illustrated in the Figure 34 as a line graph. According to the results, our model needs more CPU power for all numbers of requests then RBAC. For the maximum case, our model needs %3 more CPU. This difference is a relatively an acceptable difference because it is relatively small and our model performs more evaluations and controls with evaluation functions therefore, they need some extra CPU source.

CHAPTER 8

CONCLUSION

In this thesis, we offer a context-aware security model extending role-based access control model in order to prevent relay attacks in NFC enabled mobile devices with both theoretical and practical approach.

With the huge amount of mobile device usage and increase in their functional capabilities in the current era, they started to be used frequently in many smart solutions. One of these solutions is access control solutions. At this point NFC allows mobile devices to be used in access control systems.

Near Field Communication technology creates communication between NFC compatible devices in a short range easily. Mobile devices use its capabilities with their embedded NFC chips. In addition to being used in solutions that make life easier, it is also used in critical solutions such as access control systems. Because of the nature of these solutions, NFC communication is exposed to security attacks. Relay attacks are the most common security attacks for the NFC communication medium, which allows unauthorized access to the resources.

We proposed a context aware security solution to that critical security problem described above. Based on the research gaps presented in the Chapter 1, we answered the research questions. We have answered first research question and defined the possible vulnerabilities and attacks of NFC communication in Chapter 3. Then system level and conceptual requirements of the proposed model are described.

In Chapter 2, we presented related studies in the literature discussing various vulnerabilities of NFC communication, successful relay attacks and possible countermeasures to relay attacks. In addition, we realized that offered prevention methods provides solutions for low level applications and do not solve relay attacks occur in application layer.

An overview of NFC and comparison of wireless technologies are presented in Chapter 3. In addition, basics of NFC transmission are described in order to underline how communication is performed between two parties in NFC ecosystem. Based on this knowledge, we designed and implemented a practical relay attack in order to prove how it is easily performed in NFC enabled mobile phones with the help of host-card emulation mode. Chapter 4 describes this implementation and results also answers the third research question.

We offer Mobile Context Aware and Role Based Access Control Model (M-CARBAC) as a countermeasure for relay attacks occurred in NFC communication in Chapter 5. First, we introduce security model description and classify the threat using STRIDE threat modeling. As main characteristics of our model, context-aware methodology, dynamic security principles and role-based access control basics are described. Stages on how to prevent relay attacks are described as layered architecture. Context sensitive control (CSC) and dynamic policy controls (DPC) are offered in that layers to provide actions for authentication and authorization process. The second and fourth research questions are also answered in Chapter 5. In order to verify theoretical approach of the proposed model, sets and functions of the model are provided. Based on that, policy evaluation, context verification and steps of formal algorithm are created. Finally, we formally proved three claims on formal algorithm.

In addition to theoretical approach, we provide practical approach of proposed model. In order to apply and evaluate the model, we developed complete infrastructure of NFC based access control system including mobile application, backend and communication services and hardware setups. Lastly, required additional time and processor power with respect to standard role-based access control systems are evaluated. Test results shows that our offered model has acceptable results although it needs small amount of extra time and CPU source.

To sum up, this study has four major contributions. Firstly, security requirements are offered for NFC access control systems. Secondly, we have proved practically relay attack using NFC enabled mobile devices. Thirdly, a complete, dynamic, adaptive and context aware security model extending Role Based Access Control (RBAC) is designed and developed to prevent relay attacks using NFC enabled mobile devices. Finally, formal definitions and verification for offered system are provided to show validity of the model in all possible request combinations.

Studying on the applicability of the proposed model in other wireless technologies and for other types of NFC solutions such as payment etc. might guide researchers as future work. In addition, risk evaluation instantly during access requests can be improved using machine learning algorithms and artificial intelligence principles.

REFERENCES

[1] Mark Weiser, “The computer for the 21st Century”. Scientific American. Vol. 265, No. 3, pp.66 -75 1991.

[2] J. Collins, “ABI Research Insight: No OTA, No NFC,” accessed from http://www.abiresearch.com, on 10 2007.

[3] Romen, G. Presentation, NFC and the NFC Forum, 2010.

[4] D. Cavdar and E. Tomur, "A practical NFC relay attack on mobile devices using card emulation mode," 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, pp. 1308-1312, 2015.

[5] NFC forum accessed from http://nfc-forum.org/ on January 2, 2014.

[6] NFC Forum. (NFC data exchange format (NDEF). Technical specification, version 1.0, 2006.

[7] Master thesis, Dolgorsuren Byambajav “Secure Nfc Enabled Mobile Phone Payments Using Elliptic Curve Cryptography (Snfcmp)”, August 2011 California State University

[8] T. Rosati, G. Zaverucha: Elliptic Curve Certificates and Signatures for NFC Signature Records, NFC Forum, 2013.

[9] Hasoo Eun, Hoonjung Lee and Heekuck Oh. “Conditional privacy preserving security protocol for NFC applications”. Consumer Electronics, IEEE Transactions on, 2013, 59, 1, 153-160

[10] Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Sandeep Tamrakar, and Christian Wachsmann. “SmartTokens: delegable access control with NFC-Enabled smartphones”. In Proceedings of the 5th international conference on Trust and Trustworthy Computing (TRUST'12), 2012.

[11] Christoph Busold, Ahmed Taha, Christian Wachsmann, Alexandra Dmitrienko, Hervé Seudié, Majid Sobhani, and Ahmad-Reza Sadeghi. “Smart keys for cyber-cars: secure smartphone-based NFC-enabled car immobilizer”. In Proceedings of the third ACM conference on Data and application security and privacy (CODASPY '13) , 2013.

[12] Forrester, La-Dene & Shaw, Rupert & Thorpe, Sean. “Assessing Relay Attacks in NFC Enabled Devices A Three Factor Relay Test Environment (RATE) Approach”. 1-8, 2018.

[13] Nicholas Akinyokun and Vanessa Teague. “Security and Privacy Implications of NFC-enabled Contactless Payment Systems”. In Proceedings of ARES ’17, Reggio Calabria, Italy, August 29-September 01, 2017, 10 pages. 2017.

[14] R. S. Divya and M. Mathew, "Survey on various door lock access control mechanisms," International Conference on Circuit ,Power and Computing Technologies (ICCPCT), Kollam, pp. 1-3, 2017

[15] S. B. Oo, N. H. M. Oo, S. Chainan, A. Thongniam and W. Chongdarakul, "Cloud- based web application with NFC for employee attendance management system," 2018 International Conference on Digital Arts, Media and Technology (ICDAMT), Phayao, pp. 162-167, 2018.

[16] L. Wu, X. Du, M. Guizani and A. Mohamed, "Access Control Schemes for Implantable Medical Devices: A Survey," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1272-1283, Oct. 2017.

[17] Dakota Nelson, Mengyu Qiao, and Andrew Carpenter. "Security of the near field communication protocol: an overview" J. Comput. Sci. Coll. 29, 2 (December 2013), 94-104, 2013.

[18] Gerald Madlmayr, Josef Langer, Christian Kantner, and Josef Scharinger. "NFC Devices: Security and Privacy". In Proceedings of the Third International Conference on Availability, Reliability and Security (ARES '08). IEEE Computer Society, Washington, 2008,

[19] J. Gummeson, B. Priyantha, D. Ganesan, D. Thrasher, P. Zhang: "EnGarde: Protecting the mobile phone from malicious NFC interactions" MobiSys, 2013.

[20] Wang, Zining "Information Security Vulnerabilities of NFC Technology and Improvement Programs". 196-199, 2018.

[21] Giese, D., Liu, K., Sun, M., Syed, T., & Zhang, L. "Security Analysis of Near- Field Communication (NFC) Payments". ArXiv, abs/1904.10623, 2019.

[22] Mahinderjit Singh, Manmeet (Mandy) & Adzman, Ku & Hassan, Rohail. "Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures." International Journal of Engineering and Technology. 7. 298-305. 10.14419/ijet.v7i4.31.23384, 2018.

[23] S.Micallef,K.Markantonakis,"Mobile payments using Host Card Emulation with NFC: security aspects and limitations", ISG MSc Information Security thesis series 2018.

[24] A. Al-Haj and M. A. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," 2018 4th International Conference on Information Management (ICIM), Oxford, pp. 184-187, 2018.

[25] D. Sethia, D. Gupta and H. Saran, "NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access," in IEEE Transactions on Consumer Electronics, vol. 64, no. 4, pp. 470-479, Nov. 2018.

[26] B. Yan, A. Xu, Y. Cao, Y. Jiang, W. Xu and X. Ji, "Hardware-fingerprint Based Authentication for NFC Devices in Power Grids," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chengdu, China, pp. 1147-1154, 2019.

[27] R. Kaur, Y. Li, J. Iqbal, H. Gonzalez and N. Stakhanova, "A Security Assessment of HCE-NFC Enabled E-Wallet Banking Android Apps," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, pp. 492-497, 2018.

[28] Wouter van Dullink, Pieter Westein “Remote relay attack on RFID access control systems using NFC enabled devices”, 2013.

[29] Hancke, Gerhard.”A Practical Relay Attack on ISO 14443 Proximity Cards”, 2005.

[30] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis “Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones,". Workshop on RFID and IoT Security (RFIDsec 2012 Asia), November 8 - 9, 2012, Taipei, Taiwan. 2012.

[31] Zhao Wang, Zhigang Xu, Wei Xin, and Zhong Chen. “Implementation and Analysis of a Practical NFC Relay Attack Example”. In Proceedings of the 2012 Second International Conference on Instrumentation,

Measurement, Computer, Communication and Control (IMCCC '12), 2012.

[32] Master thesis, Henning Siitonen Kortvedt, “Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment” May 17, 2010 Der Technischen Universit At Munchen, 2010.

[33] L. Forrester, R. Shaw and S. Thorpe, "Assessing Relay Attacks in NFC Enabled Devices A Three Factor Relay Test Environment (RATE) Approach," SoutheastCon 2018, St. Petersburg, FL, pp. 1-8, 2018.

[34] J. Jumić and M. Vuković, "Analysis of credit card attacks using the NFC technology," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, pp. 1251-1255,2017.

[35] F. Dang, P. Zhou, Z. Li and Y. Liu, "NFC-enabled attack on cyber physical systems: A practical case study," 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, pp. 289-294, 2017.

[36] S. Akter, T. Chakraborty, T. A. Khan, S. Chellappan and A. B. M. Alim Al Islam, "Can You Get into the Middle of Near Field Communication?," 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, pp. 365-373, 2017.

[37] Yu-Ju Tu, Selwyn Piramuthu, “On addressing RFID/NFC-based relay attacks: An overview, Decision Support Systems”, Volume 129, 2020 (online)

[38] Haken, Gareth & Markantonakis, Konstantinos & Gurulian, Iakovos & Shepherd, Carlton & Akram, Raja Naeem. Evaluation of Apple iDevice Sensors as a Potential Relay Attack Countermeasure for Apple Pay. 2017.

[39] Gurulian, C. Shepherd, E. Frank, K. Markantonakis, R. N. Akram and K. Mayes, "On the Effectiveness of Ambient Sensing for Detecting NFC Relay Attacks," 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, pp. 41-49, 2017.

[40] C.Shepherdetal.,"TheApplicabilityofAmbientSensorsasProximityEvi dence for NFC Transactions" IEEE Security and Privacy Workshops (SPW), San Jose, CA, pp. 179-188, 2017.

[41] D. Ma, N. Saxena, T. Xiang, and Y. Zhu, "Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing," Dependable and Secure Computing, IEEE Transactions on, vol. 10, no. 2, pp. 57–69, March 2013.

[42] T. Halevi, D. Ma, N. Saxena, and T. Xiang, "Secure Proximity Detection for NFC Devices Based on Ambient Sensor Data," in Computer Security – ESORICS 2012, ser. LNCS, S. Foresti, M. Yung, and F. Martinelli, Eds. Springer, pp. 379–396, vol. 7459,2012 (Online)

[43] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Comparing and Fusing Different Sensor Modalities for Relay Attack Resistance in Zero-Interaction Authentication," in Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on. IEEE, pp. 163–171, 2014.

[44] B.Shrestha, N.Saxena, H.T.T.Truong, and N.Asokan,"Dronetotherescue: Relay-resilient authentication using ambient multi-sensing," in Financial Cryptography and Data Security. Springer, pp. 349–364, 2014.

[45] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. “Practical NFC peer-to-peer relay attack using mobile phones”. In Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues (RFIDSec'10) 2010.

[46] S. Drimer and S. J. Murdoch, “Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks.” in USENIX Security, N. Provos, Ed. USENIX Association, 2007.

[47] Iakovos Gurulian, Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes. “Preventing relay attacks in mobile transactions using infrared light”. In Proceedings of the Symposium on Applied Computing (SAC '17). ACM, New York, NY, USA, 1724-1731, 2017.

[48] S. Chabbi, R. Boudour and F. Semchedine, "A secure protocol, based on iris technology, for NFC phone applications," International Conference on Mathematics and Information Technology (ICMIT), Adrar, pp. 78-83, 2017.

[49] M. I. Isnan Imran, A. G. Putrada and M. Abdurohman, "Detection of Near Field Communication (NFC) Relay Attack Anomalies in Electronic Payment Cases using Markov Chain," 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, pp. 1-4, 2019.

[50] O. Anggoro, M. Dzulfikar, B. Purwandari and M. Mishbah, "Secure Smartphone-Based NFC Payment to Prevent Man-in-the-Middle Attack," 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, pp. 109-114, 2019.

[51] I. Gurulian, C. Shepherd, E. Frank, K. Markantonakis, R. N. Akram and K. Mayes, "On the Effectiveness of Ambient Sensing for Detecting NFC Relay Attacks," 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, pp. 41- 49, 2017.

[52] P. Li, H. Fang, X. Liu, B.Yang "A countermeasure against relay attack in NFC payment." proceeding of Internet of things and Cloud Computing (ICC '17), pp.1-5, 2017.

[53] Main, J. Presentation, "NFC Technology Overview", 2019.

[54] Harley Geiger "NFC Phones Raise Opportunities, Privacy And Security Issues" accessed from https://cdt.org/blog/nfc-phones-raise-opportunities-privacy-and- security-issues/ on May 19, 2014.

[55] Mobey Forum. "Alternatives for banks to offer secure mobile payments". Available at: http://www.mobeyforum.org/Press-Documents/Press-Releases/Alternatives-for-Banks-to-offer-Secure-Mobile-Payments, 2010.

[56] Finkenzeller, K. RFID handbook: "Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication". London: Wiley. ISBN: 978-0-470- 69506-7, 2010.

[57] Reveilhac, M. and Pasquet, M. "Promising secure element alternatives for NFC technology". In Proceedings of the first international workshop on near field communication, Hagenberg, Austria, pp. 75–80, 2009.

[58] Vedat Coskun, Kerem Ok, and Busra Ozdenizci. "Near Field Communication: From Theory to Practice (1st ed.)". Wiley Publishing. 2012.

[59] Madlmayr, G. “NFC devices: Security and privacy”. In Proceedings of third international conference on availability, reliability and security, Barcelona, pp. 642–647, 2008.

[60] Google Inc. accessed from https://support.google.com/wallet/answer/3026245?hl=en&ctx=go on January 3, 2014

[61] Lee, E. Presentation, NFC Hacking: The Easy Way, 2010.

[62] Hancke, Gerhard P. "A practical relay attack on ISO 14443 proximity cards." Technical report, University of Cambridge Computer Laboratory, 1-13, 2005.

[63] Google Inc. accessed from https://www.google.com/wallet/ on January 15, 2015

[64] Google Inc. accessed from https://developer.android.com/guide/topics/connectivity/nfc/hce.html on January 15, 2015

[65] Nataliya S. (2018, December 3). Threat Modeling: 12 Available Methods. Retrieved, from https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12- available-methods.html on July 6, 2019

[66] Kohnfelder, Loren, and Praerit Garg, The threats to our products, Microsoft Interface Available at http://blogs.msdn.com/sdl/attachment/9887486.ashx on April 1, 1999

[67] A.K Malik, M. A.Ali, A, Mateen et al.A Comparison of Collaborative Access Control Models, (IJACSA) International Journal of Advanced Computer Science and Applications, pages 290-296 Vol. 8, No. 3, 2017.

[68] Electronic Design accessed from https://www.electronicdesign.com/ technologies/communications/article/21800606/nfcrfid-ripe-for application-expansion on June 18, 2020.

[69] H. Feinstein R. Sandhu, E. Coyne and C. Youman.Role-based access control models. IEEE Computer, 29(2):38–47, 1996.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Çavdar, Davut
Nationality: Turkish
Date and Place of Birth: 22.08.1984 / Bakırköy
Marital Status: Married
Email: davutcavdar@gmail.com

EDUCATION

Degree	**Institution**	**Year of Graduation**
Ph.D.	Information Systems, METU	2020
M.Sc.	Information Systems, METU	2011
B.Sc.	Computer Science, METU	2008

WORK EXPERIENCE

Year	**Place**	**Enrollment**
2020-Present	Mercedes Benz- DAIMLER	Software Engineer
2016-2019	ANT	Software Engineer
2008-2016	METU	Research Assistant
2007-2008	SIMSOFT Inc.	Software Engineer

HONORS / AWARDS

- One of the 2014-1 2211-C Doctorate Scholar Supported by TUBITAK
- One of the 2012 Teknogirişim Supported of Ministry of Science, Industry and Technology
- Scholarship of Alumni Association of METU Istanbul Branch
- 2003 ÖSS Türkiye 1310. Ranking
- 2007 ALES Türkiye 1076. Ranking
- Middle East Technical University, Honor Student;
    - 2006-1 2006-2 terms
- Middle East Technical University, High Honor Student;
    - 2007-1 2007-2 terms

PUBLICATIONS

International Peer-Reviewed

D. Cavdar, E.Tomur , A.B.Can "*A Context-Aware Security Model for Preventing Relay Attacks in NFC Enabled Mobile Devices*" Security and Communication Networks 2020 (SCI-E, submitted)

D. Cavdar, E.Tomur *"A Practical NFC Relay Attack on Mobile Devices Using Card Emulation Mode"* The 38th International ICT Convention MIPRO, 25-29 May, Croatia

D. Cavdar, A.Yortanlı, P.Eren, A. Kocyigit *"A Certificate-based Context-Aware Access Control Model For Smart Mobile Devices In Ubiquitous Computing Environments"* The Eighth International Conference on Mobile

Ubiquitous Computing, Systems, Services and Technologies, 24-28 August, Italy

D. Cavdar, E.Tomur, N. Baykal “*Using Contexts as Precaution for Relay Attacks in Near Field Communication”* IS'CYDES 2016, International Symposium on Cyber Defence and Security, 13/05/2016,

National Peer-Reviewed

Ş.Küçüközer E.Akkurt, D.Çavdar, A.Temizel, T.T.Temizel. “UBDroid: Kullanıcı Davranış Analizi için Akıllı Telefon Uygulamaları Kullanım İzleme Aracı” 10. Ulusal Yazılım Mühendisliği Sempozyumu UYMS'16 - Çanakkale (24-25-26 Ekim 2016)

Book Chapters

D. Cavdar, “Near Field Communication” Android Mutfağından Seçmeler (Turkish) ISBN: 605-9129-12-1