SECURITY MODELING OF MOBILE PAYMENT SYSTEM ARCHITECTURE

Temitope Olanrewaju, Pavol Zavarsky, Ron Ruhl, Dale Lindskog
Department of Information Systems Security Management
Concordia University College of Alberta, Edmonton, Canada
7128 Ada Boulevard, Edmonton, Alberta, Canada T5B 4E4
felixaty2k@yahoo.com, {pavol.zavarsky, ron.ruhl,dale.lindskog}@concordia.ab.ca

***Abstract*— This paper provides insight into the security of the existing mobile payment system by studying its system architecture and the security architecture. It also reviews the security vulnerabilities in some components of the architecture and studies how these vulnerabilities might be exploited. This research also applies environmental metrics values on the CVSS base scores of these vulnerabilities when considered in the context of mobile payment system architecture.**

***Keywords:* EMV, Mobile payment, NFC, CVSS, Point of sale terminal.**

1. INTRODUCTION

The growth of Near Field Communication (NFC) equipped mobile phones suggests that contactless mobile payment systems will be used widely in the near future. Mobile device experts estimated that payments using NFC-equipped mobile phones will account for $240 billion in spending worldwide in 2012 and more than $670 billion by 2015 [1]. Consequently, there is a likelihood of mobile phones replacing credit cards in the payment industry. Mobile payment is made by waving a mobile phone near merchant’s Point of Sale (POS) terminal. The ability to integrate loyalty and incentive programs into the mobile payment applications and increase in speed of processing POS payments are some of the benefits that mobile payment systems have over credit card method of payment [2]. Sensitivity and security of the payment information involved in the mobile payment systems encouraged us to conduct a modeling of its security. Security modeling refers to the description of system architecture and its security controls. It helps to analyze the security and support comparative evaluation of systems like mobile payment system [3].

Many Mobile Payment System (MPS) architectures have been developed to explain the flow of information between different entities involved in MPS. Our main focus will be on the MPS architecture developed by EMV (Europay, MasterCard, and Visa). EMV is a global standard for secure and convenient payment using bank cards and the EMV payment infrastructure. EMV technology replaces the magnetic stripes on credit cards and debit cards by inserting an electronic chip that contains strong cryptographic, dynamic, and digitally-signed payment data to ensure secured payment transaction. It provides protection against the use of counterfeit, lost or stolen cards for payment and credit card-based payment attacks [4], [5].

According to [6], EMV outlined mobile payment architecture which shows entities involved and the flow of payment information that occurs in mobile payment architecture. The contactless interface is based on near field communication technology. NFC is a short range, bidirectional wireless communication technology that extends the ISO 14443 standard for Radio Frequency Identification (RFID) technology. Therefore, any NFC-enabled device can communicate with other NFC devices and with any existing RFID infrastructures, such as readers and contactless cards. The range in which NFC devices can communicate is about 10cm; compared to RFID or even bluetooth technology that have much wider range.

There are three modes of operation for an NFC-device. The first mode is reader and writer mode in which NFC devices can access contactless smartcards, RFID transponders and NFC tags. This mode makes NFC devices compatible to existing contactless tokens. The second mode is card emulation mode, in which the NFC-device acts as proximity inductive coupling card. An NFC enabled phone acts as a tag or contactless card in card emulation mode. The most common usage is to emulate credit card which can be used at point of sale terminal for payment. The card emulation mode is the one used for mobile proximity payments [15]. The third mode is peer-to-peer mode; in this mode two NFC devices can carry out bidirectional communication to transfer data. NFC standard allows peer to peer communication between NFC-enabled devices like NFC phone and NFC-compatible point of sale [7], [8], and [9].

NFC technology presents great business opportunities when used in mobile phones for applications such as mobile payment, transport ticketing, and physical access control [10]. Google Wallet is one of the applications of NFC mobile payment system. In mobile payment system, an NFC-enabled mobile phone is provisioned with a version of a payment application - (for different payment cards such as, American Express ExpressPay, Discover Zip, MasterCard PayPass, Visa PayWave). Also, the mobile phone is personalized with a customer payment account (credit, debit or prepaid) issued by the financial institution (Issuer) using an Over the Air (OTA) process as explained by GlobalPlatform (GP) in [11]. GlobalPlatform is an independent body that identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple applications on secure chip technology. The mobile phone can then use NFC technology to communicate with a merchant’s contactless payment-capable POS system. The customer is required to hold the mobile phone in close proximity to the merchant’s POS and EMV payment information sent to the contactless POS reader.

The ISO/IEC 14443-based contactless merchant POS infrastructure that is now in place to support contactless credit and debit payment can also accept NFC-enabled proximity mobile payments, providing a head-start for broad acceptance and use [12]. The updating of mobile payment application (such as EMV scripts) on mobile phone is done through an OTA process between the issuer and mobile device. The authorization and settlement processes are similar to what is done in traditional EMV chip card-based payment system [6].

The security issues with NFC technology raised concern in mobile payment system. Embracing such mobile technology, developing applications for storing credit card information, and facilitating NFC payments also bring with it risks and concerns around privacy, theft, and regulatory compliance [13],[14].

1.1 Our Contribution

In this paper, we will provide insight into the security of the existing mobile payment system architecture and also present a review of the security vulnerabilities in some components of the architecture highlighted in Figure 1. Finally, we will examine how environmental metric group will affect the overall CVSS base scores of these vulnerabilities when applied in the context of mobile payment system architecture.

The structure of this paper is as follows: Section 2 shows the review of mobile payment systems. Section 3 and Section 4 describe the mobile payment system architecture and mobile payment security architecture respectively. Section 5 gives background information on Common Vulnerability Scoring System (CVSS). Section 6 examines how environmental metrics affect the CVSS base scores of these vulnerabilities in the context of mobile payment security architecture. Section 7 concludes the paper and direction of future work is also provided.

2. REVIEW OF MOBILE PAYMENT SYSTEMS

Several studies have been conducted to help improve mobile payment system models in a more secure way with different entities involved. Mobile payment is defined as payment for products or services between two parties for which a mobile device, such as a mobile phone, plays a key role in the realization of the payment. Mobile payment is divided into two types namely, proximity or remote mobile payment [15]. Proximity mobile payment is termed contactless payment in which payment information is stored on the mobile device and is exchanged based on near field communication or other wireless communication means. Remote mobile payment occurs when mobile device used to make purchase does not interact with the merchant's POS.

Different architectures have been developed to explain how mobile payment systems work. For this research, the focus will be on EMV architecture for mobile payment system based on NFC technology. NFC is a technology similar to Bluetooth that enables a radio connection between two electronic devices within proximity to each other. NFC technology is not directly associated with financial transactions like the EMV standards. One of NFC's applications however, is enabling contactless payments via mobile devices, in addition to its much broader applications for data transfer, keyless door entry and much more [16]. It is a technology which has already been adopted in Europe, Asia and gaining traction in North America [13].

The research conducted in [17] proposes a solution to overcome the security weaknesses in the mobile proximity payment by using a protocol that guarantees mutual authentication and confidentiality between the entities involved in the payment. The paper noted that the introduction of NFC payment to the EMV system opens new ways of attack that do not require physical contact between the payment token and the POS terminal.

Data between the mobile phone and the POS terminal are exchanged over the air and are susceptible to interception. Also, contactless micro payments do not require Personal Identification Number (PIN). Customers can tap their NFC mobile phones on a contactless POS terminal to make purchase. To overcome the observed security weaknesses in mobile proximity payment, they proposed a protocol that provides mutual authentication between an NFC mobile phone and a POS terminal by sharing a session key. This is made possible by means of trusted party Authentication Server (AS). This protocol makes use of symmetric keys. The POS and emulated card are provided with an identifier (ID) and a symmetric key shared with the AS. The AS has the same function of a Certification Authority but overcome the limitations of the emulated smart card as mentioned in the paper.

Another research based on a mobile payment model called Mobile Payment Consortia System (MPCS) was proposed in [18]. MPCS is a payment model used to carry out transactions between different banks and academic institutions using mobile phones. The client must have an account with a bank and the bank must be registered with the institution consortia. Each client has an institutional ID with secured mobile Personal Identification Number (mPIN) provided by MPCS, when a client request for payment service is send to MPCS. MPCS sends an encrypted message to the client for authentication. Client authentication is achieved by decrypting the message with the mPIN (stored in a personal secure environment) and responding to MPCS in encrypted format. MPCS decrypts the client response using the mPIN to validate the client's mPIN number. When the validation process is complete, clients' mPIN numbers are mapped to their respective banks and verified with their accounts. The mPIN is also mapped with the Authentication Server-Institution (AS-I) to validate request. MPCS model is developed specifically for students to make payment of fees using their mobile phone.

Unfortunately, many of these researches lack an intuitive approach to analyze the security vulnerabilities in the mobile payment architecture and underlying mobile payment application and also provide information about the severity of these vulnerabilities to help in prioritization of risk mitigation activities. It is however important to provide more contributions to the existing mobile payment system from a security perspective in order to enhance its adoption and also maintain same level of security already in place in traditional EMV card payment transaction.

3. MOBILE PAYMENT SYSTEM ARCHITECTURE

EMV mobile payment system architecture consist of the following entities namely customer's mobile device, issuer, acquirer and merchant's POS. Figure 1 shows generic mobile payment system architecture as proposed by EMV standard. Authorization is the process through which issuer approves or declines a mobile payment transaction.

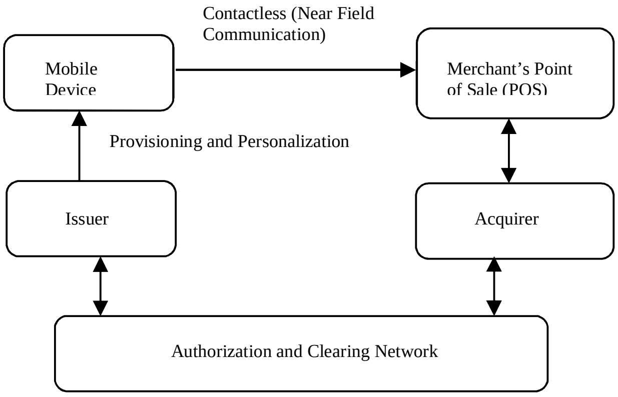
Contactless (Near Field Communication)
Mobile Device
Merchant's Point of Sale (POS)
Provisioning and Personalization
Issuer
Acquirer
Authorization and Clearing Network

Figure 1: Mobile Payment System Architecture

The authorization process helps to monitor mobile payment transactions to detect fraudulent use of mobile phone and POS terminal; and makes the decision regarding whether to approve or decline the transaction by validating the dynamic cryptogram [19]. Clearing is the process of transferring payment transaction data between processor and issuer.

Mobile device is used as payment token and it contains EMV compliant-payment application and cryptographic keys stored on tamper-resistant component of the mobile device called Secure Element (SE). Secure element in the mobile device provides a tamper-proof environment for storing payment data, performing cryptographic functions, and achieving transaction security. SE can be a dedicated microchip that is embedded into the NFC-enabled mobile device or integrated in another smartcard or security device that is used within the NFC device. It can also come in form of UICC (Universal Integrated Circuit Card) often referred to as Sub-scriber Identity Module (SIM card) or a Secure Digital (SD) memory card [9].

The issuer will provide and deliver EMV compliant-payment application to SE of the mobile device during an OTA provisioning process. Mobile device personalization stage involves customizing payment application with customer payment information. This personalization process used in mobile payment systems relies on the same foundation defined by EMVCo in terms of formatting the data using EMV Card Personalization Specifications, and ensuring the highest level of security and confidentiality by using industry-proven cryptographic standards defined by EMVCo [4]. EMVCo manages, maintains, and enhances the EMV Integrated Circuit Card (ICC) specifications for chip-based payment cards, contactless payment, mobile payment and also acceptance devices like point of sale terminals and Automated Teller Machines (ATMs) [20]. After personalization process, the mobile device is ready for use to make payment.

One of the NFC mobile payment applications is Google Wallet (GW). As of September 2012, many retail stores are accepting Google Wallet at merchant's point of sale terminals. A user must switch on the display of the mobile device that the application is stored. GW requires a four-digit Personal Identification Number (PIN) to authenticate users and grant access to the SE. The PIN is stored as a Secure Hash Algorithm, (SHA-256) hash on the mobile phone. Since the PIN can only be a four-digit value, a brute-force attack on the mobile phone will only require calculating at most 10,000 SHA-256 hashes. Five invalid PIN entry attempts is only allowed on GW before locking the user out. To make a payment, the user unlocks his mobile phone and the mobile payment application's unique PIN is entered; the mobile phone is now tapped against a NFC compatible POS terminal. Payment credentials are transferred to the merchant. The merchant receives a confirmation on the POS terminal and a receipt is printed, while the customer receives a confirmation on the mobile device [25], [26].

4. ANALYSIS OF MOBILE PAYMENT SECURITY ARCHITECTURE

Security in mobile payment system is the provision of confidentiality, integrity, authentication, authorization, assurance, and non-repudiation in every transaction. Security architecture can be defined as the design artifacts that describe how the security controls are positioned, and how they relate to the overall information system architecture. Critical data involved in financial transaction must be stored securely in the mobile device or in issuer's storage infrastructure [24].

Mobile payment security architecture examines the way security is built into mobile payment system architecture in order to achieve mobile payment security requirements. Cryptographic key management helps to prevent the mobile payment system from being compromised by an attacker. The study of this security architecture will help to identify the existing security measures built into mobile payment system; assess how these measures are able to secure the system, and also provide insight to the vulnerabilities that still need to be mitigated.

The Figure 2 shows mobile payment security architecture with placement of security controls. We assume that the existing control is similar to what we have in traditional EMV payment architecture. Payment information provisioning and personalization processes between mobile device and issuer are protected based on Public Key Infrastructure (PKI) system using Secure Socket Layer version 3 (SSLv3) or Transport Layer Security (TLS). Transport layer security and its predecessor, the secure socket layer, are cryptographic protocols that provide secure communication for Card-Not-Present (CNP) transactions over the internet. SSL is used to provision the EMV card data to the mobile phone. Subsequently, Payment information is protected by the emulated EMV certificates and the EMV secret key provisioned into the secure element in the phone by the issuer [22], [23].

A Public Key Infrastructure (PKI) is a system consisting of set of hardware and software used for the management of public key and distribution of digital certificates which are used to verify that particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed when it is not in use [21]. Figure 2 shows how security controls are placed in mobile payment system architecture.

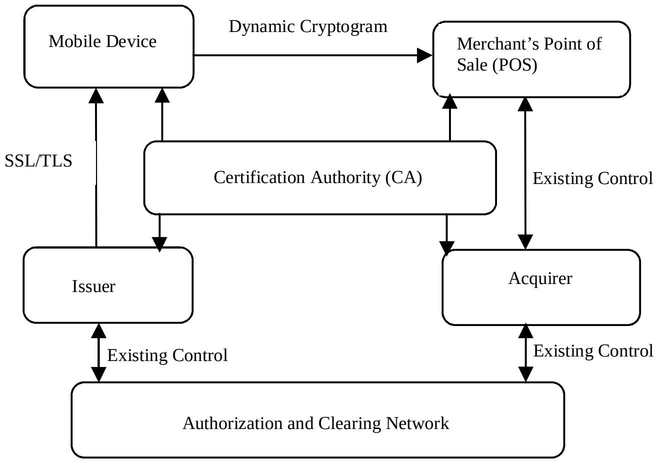

Figure 2: Mobile Payment Security Architecture

Certification Authority (CA) is trusted entity that issues digital certificates to users within a PKI system and provide status information about the certificates the CA has issued. The digital certificate certifies the ownership of a public key by the named subject of the certificate [27], [28]. Both issuer and acquirer have their individual public key pairs; therefore generates digital certificates. The CA authenticates the public keys of both the issuer and acquirer. CA certifies the public key of the issuer using its private key. The POS terminal retrieves its stored copy of the CA public key and used it to verify the issuer's public key certificate. Subsequently, the POS terminal also gets the issuer's public key from the issuer public key certificate and used it to verify the dynamically signed mobile payment data. The CA's public key is distributed to the acquirer and the POS terminal. POS terminal used the public key to verify that the issuer's public key was certified by the CA.

Mobile phone (emulated EMV card) authentication to merchant's POS terminal is similar to EMV card authentication. Dynamic Data Authentication (DDA), Combined Dynamic Data Authentication (CDA) and Fast Dynamic Data Authentication (FDDA) are authentication methods that can occur in mobile payment system. DDA makes each mobile payment transaction unique to protect payment data from customer phone to POS terminal. For each transaction, the POS terminal requests that the mobile phone generate a cryptogram based on a random data element sent to it, a valid cryptogram is generated and verified when the transaction is authorized. This cryptographic value and transaction-specific data is validated by the POS terminal to protect against data breach. The mobile phone must be present to generate a valid cryptogram which is verified offline or online during transaction authorization stage. Dynamic data authentication method used by mobile phone will lower payment fraud because stolen payment card information will not be used to make counterfeit cards or fraudulent online transaction. Dynamic cryptogram provided by issuer improves mobile payment security [21], [22]. The Figure 3 shows description of dynamic data authentication process [29].

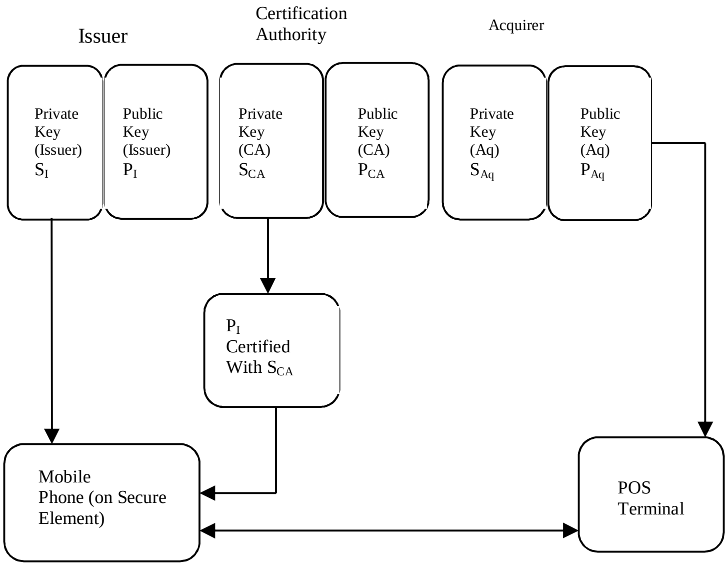
Issuer
Certification Authority
Acquirer
Private Key (Issuer) S_I
Public Key (Issuer) P_I
Private Key (CA) S_{CA}
Public Key (CA) P_{CA}
Private Key (Aq) S_{Aq}
Public Key (Aq) P_{Aq}
P_I Certified With S_{CA}
Mobile Phone (on Secure Element)
POS Terminal

Figure 3: Dynamic Data Authentication in Mobile Payment System

- P_I is the public key of the issuer certified by the certification authority's private key.
- The POS terminal uses the CA public key (P_{CA}) to verify the signature on the issuer's public key.
- The public key of the CA (P_{CA}) is distributed to the acquirer and resides on the POS terminal.

Combined Dynamic Data Authentication (CDA) is a variation of DDA. It is also known as Combined DDA with Application Cryptogram (AC) generation. CDA combines a request for dynamic signature calculation and application cryptogram in one command. This offers an extra layer of security to ensure payment token validity when performing offline transactions. Certain payment brands require CDA for offline contactless transactions. MasterCard PayPass contactless payment uses CDA. CDA protects against static data authentication certificate cloning, card skimming, and counterfeiting [32].

Visa PayWave uses a new variant of DDA named Fast Dynamic Data Authentication (FDDA). FDDA transactions use a new protocol sequence which significantly speeds up the processing of Visa NFC transactions [33]. FDDA puts a digital signature on the transaction details including the amount and this signature can be use to verify the amount. The FDDA dynamic signature is generated at the early stage of the transaction to complete the transaction before the customer's payment device moves away from the POS terminal [34].

Additional layer of security is provided by using pin authentication on both customer's mobile phone and EMV compliant-payment application stored on the mobile phone. By comparing the mobile payment system and security architectures, we can see that the confidential payment information exchanged through NFC contactless interface in the system architecture is protected using dynamic cryptogram as shown in the security architecture. With all these security controls, mobile payment systems are still vulnerable to different security threats ranging from vulnerabilities in the mobile device as payment token, vulnerabilities in the use of SSL/TLS, and vulnerabilities in the mobile payment application provisioned on the mobile phone. An open framework like CVSS is needed to generate consistent scores that will accurately represent the impact of these vulnerabilities on the security requirements of mobile payment systems [35]. The following sections provide more information about CVSS and its application to mobile payment systems

5. INTRODUCTION TO COMMON VULNERABILITY SCORING SYSTEM

Providing a list of vulnerabilities is all well and good but without any ranking of risk factors, it is difficult task to decide which vulnerability is more critical than other to assist in the prioritization of risk mitigation process. Common Vulnerability Scoring System (CVSS) provides an open framework for communicating and documenting the major characteristics of vulnerabilities, and also for measuring potential impacts of exploitation of these vulnerabilities. It applies a severity level, or CVSS score to each information system vulnerability. CVSS scores range from 0 to 10, where 10 represent the most critical score [36].

According to the technical and operation requirements of the Payment Card Industry Data Security Standard (PCI DSS) guidelines in [37], for a component to be considered compliant, it must not contain any vulnerability that has been assigned a CVSS base score equal to or higher than 4.0. The PCI DSS is a mandatory requirement for all the entities involved in payment card processing such as the merchants, acquirers, issuers, service providers and all other entities that store, process or transmit cardholder data [47]. Any CVSS base scores between 0.0-3.9, 4.0-6.9, and 7.0-10.0 are considered as “Low”, “Medium”, and “High” respectively in term of severity ranking.

To properly and effectively quantify vulnerabilities for prioritization purposes, it is not advisable to rely mainly on the base score generated by the National Vulnerability Database (NVD). Instead, organizations are required to add the environmental information so as to have a true picture and properly prioritize the response process that can be selected to mitigate the vulnerabilities [38].

5.1 CVSS METRIC GROUPS

CVSS scores are composites derived from the following three categories of metrics [35]. The three metrics groups are defines as follows:

- Base metric group - This group represents the properties of vulnerability that do not change over time. Six different metrics are classified under this group: access vector (measures whether a vulnerability can be exploited locally or remotely), access complexity (measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system), authentication (measures the level of authentication needed to exploit the vulnerability), confidentiality impact (measures the impact on the confidentiality of a successful exploit of the vulnerability on the target system), integrity impact (measure the impact on the integrity of a successful exploit of the vulnerability on the target system), availability impact (measures the impact on availability of a successful exploit of the vulnerability on the target system)
- Temporal metric group - This group represents the vulnerability characteristics which change over time but not through the user environment. Three metrics are defined under this group: exploitability (measures the level of exploitability of the vulnerability), remediation level (measures the level of an available solution or remedy), and report confidence (measures the degree of confidence in the existence of the vulnerability and the credibility of its report).
- Environmental metric group - This represents the implementation and environmental specific qualities of vulnerability. These are user defined qualities that reflects the characteristics of vulnerability with reference to a specific environment. Two metrics are used here: Collateral Damage (CDP) (measures the potential for a loss of physical equipment, property damage or loss of life), Target of Distribution (TD) (what percentage of the systems is susceptible to the vulnerability). The Confidentiality Requirement (CR), Integrity Requirement (IR), and Availability Requirement (AR) increases or reduces the impacts of the base metrics group according to the importance of these security requirements [36].

6. ANALYSIS OF CVSS ENVIRONMENTAL METRICS ON THE VULNERABILITIES IN MOBILE PAYMENT SECURITY ARCHITECTURE

This section examines vulnerabilities in some components of the mobile payment security architecture. We studied and found some vulnerabilities in mobile device (NFC mobile phone), SSL implementation, and the mobile payment application used to store customer payment information as recorded in NVD. We also look at the impact of the environmental metrics on the CVSS base scores of these vulnerabilities using CVSS calculator to generate some scores. These vulnerabilities and their associated CVSS analysis are described in the following subsections.

6.1 VULNERABILITY SUMMARY FOR CVE-2008-5827 (NOKIA 6131 NFC PHONE)

The NVD entry in [39] CVE-2008-5827 describes vulnerability in the Nokia 6131 NFC phone. This explains vulnerability in the mobile device as a mobile payment token. This mobile phone is used in cooperation with MasterCard and Citibank as a wireless or debit card to transfer payment information to merchant’s POS [40]. This vulnerability could allow a remote attacker to execute arbitrary code on the system. This is caused by an error when handling NFC Data Exchange Format (NDEF) tags. Software installation automatically occurs after the download of a Java ARchive, JAR file. By persuading a victim to download a .JAR file containing a specially-crafted Uniform Resource Identifier, URI record in an NDEF tag, an attacker can exploit this vulnerability to execute arbitrary code.

Exploitation of vulnerability leads to unauthorized access, disruption of service, and unauthorized disclosure of confidential customer’s payment information. No remedy is available as of February 1, 2013 for this vulnerability [41]. The CVSS base score of CVE-2008-5827 is 7.5, Impact Subscore of 6.4, and Exploitability Subscore of 10.0. The Tables 1 below shows effect of different 20 possible combinations of environmental metrics on the CVSS base score as generated by CVSS calculator.

From the overall CVSS scores generated for CVE-2008-5827 in Table 1, it shows that the overall CVSS scores can range from value 0.0 up to 9.2; that is from ”Low” to ”High” in term of severity ranking. Table 1 shows that when the environmental metrics are considered in the context of mobile payment system, the Overall CVSS score can actually be as high as 9.2, and as low as 0. These values further show that the CVSS base score value alone may not reveal the true picture of the state of the vulnerability when considered in the user environment (mobile payment environment).

CDP	TD	CR	IR	AR	Overall CVSS Score
None	None	Low	Low	Low	0.0
None	Low	Low	Low	Medium	1.6
None	Low	Not Defined	High	Medium	2.0
None	Medium	Low	Low	Low	4.1
None	Medium	Low	Low	High	5.2
None	Not Defined	High	Low	High	7.9
Low	High	High	Low	Medium	7.7
Low-Medium	High	Low	High	High	8.5
Medium-High	High	Not Defined	High	High	8.9
High	Low	High	Not Defined	Not Defined	2.2
High	High	Medium	High	High	9.1
High	Not Defined	Medium	Low	High	8.7
High	Not Defined	Low	High	High	9.0
Medium-High	High	High	High	High	9.2
Low-Medium	Medium	High	Low	High	6.4
None	High	Not Defined	High	High	8.2
Not Defined	Low	Not Defined	Medium	High	2.0
Not Defined	Not Defined	High	Not Defined	High	8.2
Not Defined	Not Defined	Not Defined	Not Defined	Not Defined	7.3

Table 1: Possible Combinations of Environmental metrics for CVE-2008-5827

6.2 VULNERABILITY SUMMARY FOR CVE-2012-5810 (CHASE MOBILE BANKING APPLICATION)

The NVD entry CVE-2012-5810 in [42] describes vulnerability in Chase mobile banking application for Android operating system. This describes vulnerability in the mobile payment application used in mobile payment system. The SSL connections established by this mobile payment application on Android mobile phones are insecure against man-in-the-middle attack; which is exactly an attack that SSL is intended to protect against. This allows a network attacker to capture credentials, such as username and password, of any Chase customer using this application, along with the rest of their session. It was found that this application and the SSL libraries examined did not reject self-signed or third-party digital certificates as they would be expected to do for ensuring secure communications.

According to research conducted in [43], it was noted that chase mobile banking application overrides default x509TrustManager which causes the application to fail to check the requesting server’s certificate. This allows man-in-the-middle attacker to spoof SSL server via an arbitrary valid certificate due to broken SSL certificate validation in many applications and libraries. The CVSS base score of this vulnerability is 5.8, Impact Subscore of 4.9 and Exploitability Subscore of 8.6. The Table 2 below shows 20 possible combinations of environmental metrics on the CVSS base score as generated by CVSS calculator. Table 2 shows that an estimated number of vulnerable endpoint mobile devices can affect the Overall CVSS score. For example, from the Table 2, we can see that when the Target of Distribution (TD) changes from “Low” to “High”, the Overall CVSS score increases from 1.0 to 7.2 respectively.

CDP	TD	CR	IR	AR	Overall CVSS Score
None	None	High	High	High	0.0
None	Low	Low	Low	Low	1.0
None	Medium	Low	Low	High	3.1
None	Medium	Low	High	Low	4.4
Low	None	High	Low	High	0.0
Low	Medium	Low	High	Not Defined	4.7
Low	High	Medium	Not Defined	High	6.0
Low	High	High	High	Low	7.2
Low	High	High	High	High	7.2
Low-Medium	Medium	High	High	Low	5.9
Low-Medium	High	Low	Not Defined	High	6.4
Low-Medium	High	Medium	Low	Low	6.4
Medium-High	None	High	Medium	High	0.0
Medium-High	None	High	High	High	0.0
Medium-High	Medium	Low	Low	Low	4.8
High	Not Defined	High	High	High	8.4
High	Not Defined	Not Defined	Not Defined	Medium	7.8
Not Defined	Not Defined	Not Defined	Low	Not Defined	4.9
Not Defined	Not Defined	High	High	Low	6.9
Not Defined	Not Defined	Medium	Medium	Not Defined	5.6

Table 2: Possible Combinations of Environmental Metrics for CVE-2012-5810

6.3 VULNERABILITY SUMMARY FOR CVE-2010-2913 (CITIBANK MOBILE APPLICATION)

Another vulnerability is recorded in NVD entry CVE-2010-2913 [44] which describes vulnerability in Citibank mobile application. This flaw can allow a local attacker to obtain sensitive information, caused by the storing of account data in a hidden file. This vulnerability can be exploited by a local attacker by using the mobile device or a synchronized computer to obtain security access codes, PIN, account numbers, and other sensitive financial information. Once the attacker gets the PIN, they have full access to the credit card information stored on the mobile payment application and they can use the phone to make purchase [45], [46].

This low risk vulnerability has a CVSS base score of 2.1, Impact Subscore of 2.9, and Exploitability Subscore of 3.9. Table 3 below shows 20 possible combination of CVSS environmental metrics for CVE-2010-2913. Based on the values generated in the Table 3, it shows that the Citibank mobile application is not PCI-DSS compliant because it contains vulnerability with CVSS score equal to or high than 4.0. Also, when possible combinations of CVSS environmental metrics was put into consideration, the Overall CVSS score increased from 2.1 up to 6.5. This increases the severity ranking of this vulnerability from ”Low” to ”Medium” when considered in the context of mobile payment environment.

CDP	TD	CR	IR	AR	Overall CVSS Score
None	None	Low	Low	Low	0.0
None	Low	Low	Low	Low	0.3
None	Low	Medium	Low	High	0.5
None	Low	High	High	Low	0.8
None	Low	High	Not Defined	Not Defined	0.8
None	Medium	Medium	High	High	1.5
None	Medium	High	Low	Low	2.2
None	High	Low	High	Low	1.1
None	High	Medium	Low	Low	2.0
None	High	High	Medium	Low	3.0
None	High	High	Medium	Not Defined	3.0
Low	Low	High	Medium	High	0.9
Low	Medium	High	High	Medium	2.8
Low	High	High	High	Medium	3.7
Low-Medium	High	Medium	Medium	High	4.4
Low-Medium	High	High	Medium	High	5.1
Medium-High	High	High	Low	Medium	5.8
High	High	Medium	Low	Low	6.0
High	High	High	Low	Low	6.5
High	High	High	Medium	Not Defined	6.5

Table 3: Possible Combinations of Environmental Metrics for CVE-2010-2913

7. CONCLUSION AND FUTURE WORK

We have been able to provide security insight into existing mobile payment system and reviewed some of the vulnerabilities that can be still be exploited by an attacker. The focus is on the vulnerabilities in the mobile phone as the payment token and the mobile payment application. Possible combinations of environmental metrics are considered and are applied to mobile payment system vulnerabilities stored in NVD database. These results can be used for prioritization of risk mitigation activities and in making decision about selection of mobile phones and mobile payment applications. This research raises security awareness in mobile payment system. The future work can be done in the area of digital wallet payment in which payment information is stored with the cloud service provider. This means that cardholders' account details will no longer be stored on a secure element within a mobile phone, but will instead be maintained online with a cloud service provider (in the case of PayPal payment system).

8. ACKNOWLEDGEMENT

The first author will like to thank the research team of Concordia University College of Alberta for their positive criticism, support and guidance in the completion of this research. He will also like to thank his wife, parents, and siblings for their support and love throughout his studies and also his profound thanks to God Almighty for the gift of life.

REFERENCES

[1] University of Alabama, “UBA system improves mobile payment security, protects personal information”, [Online]. Available:http://www.newswise.com/articles/uab-system-improves-mobile-payment-security-protects-personal-info

[2] Open Forum, “Five Major Benefits of Mobile payments”, [Online]. Available: http://www.openforum.com/articles/5-major-benefits-of-mobile-payments/

[3] J. Bau and J. C. Mitchell, “Security Modeling and Analysis” IEEE Security and Privacy, Stanford University, May/June 2011

[4] Smart Card Alliance, “EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value Added Functionality”, October, 2012, [Online]. Available: http://www.smartcardalliance.org/resources/pdf/EMV_and_NFC_WP_102212.pdf

[5] EMV Chip Technology to Process Credit Card Payments Coming Soon, [Online]. Available: http://www.americaoutdoors.org/america_outdoors/files/pdf/EVMChipTech.pdf

[6] EMV Mobile Contactless Payment: Technical Issues and Position Paper, [Online]. Available: http://www.emvco.com/best_practices.aspx?id=162

[7] C. Mulliner,”Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones,” Proc. of International Conference on Availability, Reliability and Security (ARES ’09), pp. 695-700, Mar. 2009

[8] T. Ali, and M.A. Awal,”Secure Mobile Communication in m-payment system using NFC Technology”, Proc. of IEEE/OSA/IAPR International conference on Informatics, Electronics and Vision, 2012

[9] M. Roland, ”Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?”, Fourth International Workshop on Security and Privacy in

Spontaneous interaction and Mobile Phone use (IWSSI/SPMU), Newcastle, UK, June 18, 2012

[10] GlobalPlatform Inc., “GlobalPlatform’s Proposition for NFC Mobile: Secure Element Management and Messaging” [Online].Available: http://www.paymentscardsandmobile.com/research/reports/GlobalPlatform_NFC_Mobile_White_Paper.pdf

[11] GlobalPlatform Inc., “GlobalPlatform Card Specification, Remote Application Management over HTTP Card Specification” Version 2.2 - Amendment B. [Online]. Available: http://www.globalplatform.org/ specificationscard.asp

[12] Smart Card Alliance, “Security of Proximity Mobile Payment”, May 2009, [Online]. Available:http://www.smartcardalliance.org/resources/pdf/Security_of_Proximity_Mobile_Payments.pdf

[13] Security Compass Inc., “Near Field Communication (NFC) for Mobile Payment application”, 2012. [Online].Avaliable:http://www.securitycompass.com/media/datasheets/nfc-mobile-payments-datasheet.pdf

[14] Mobile Payments - Safer than Cards? [Online]. Available:http://www.tmforum.org/ArticleMobilePayments/8745/home.html

[15] ISACA, Emerging Technology White Paper, “Mobile Payments: Risk, Security and Assurance Issues” November, 2011. [Online]. Available: http://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf

[16] Datacard Group, “EMV versus NFC Technology: Setting the record straight”, Oct 18, 2012. [Online]. Available: http://datacardedge.com/articles/emv-vs-nfc-technology-setting-the-record-straight/

[17] U. B. Ceipidor, C. M. Medaglia, A. Marino, S. Sposato, A. Moroni, “ KerNeeS - A Protocol for Mutual Authentication between NFC phones and POS terminals for Secure Payment Transactions”, Proc of 9th International ISC Conference on Information Security and Cryptology. 2012.

[18] S.Britto R.Kumar, A.A Gnana Raj, and S.A Rabara, “A Framework for Mobile Payment Consortia System (MPCS)”, 2008 International Conference on Computer Science and Software Engineering, Bishop Wuhan, Hubei, China Dec. 2008.

[19] Ashutosh Saxena, Manik L. D., and Anurag Gupta, “MMPS: A Versatile Mobile-to-Mobile Payment System”, Proc of the International Conference on Mobile Business (ICMB’05), 2005. [Online]. Available: http://www.it.iitb.ac.in/~tijo/seminar/a%20little%20world.pdf

[20]EMVCo,[Online].Available:http://www.emvco.com/default.aspx

[21] Balachandra Muniyal, Krishna Prakash and Shashank Sharma, “Wireless Public Key Infrastructure for Mobile Phones”. In International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, November 2012. [Online]. Available: http://airccse.org/journal/nsa/1112nsa08.pdf

[22] Transport Layer Security, [Online]. Available:http:en.wikipedia.org/wiki/Transport_Layer_Security

[23] Xianping Wu, “Security Architecture for sensitive information systems”, Faculty of Information Technology, Monash University, Australia, pg. 33, 2009

[24] Open Security Architecture, “IT Security Architecture”. [Online].Available: http://www.opensecurityarchitecture.org/cms/definitions/it-security-architecture

[25] O. Ghag and S. Hegde, ”A Comprehensive Study of Google Wallet as an NFC Application”, Proc of International Journal of Computer application, Volume 58- No.16, November 2012

[26] Google Wallet's PIN System can be easily cracked from rooted devices [Online]. Available: http://www.ehackingnews.com/2012/02/google-wallets-pin-system-can-be-easily.html

[27]Certificate Authority, [Online]. Available: http://en.wikipedia.org/wiki/Certificate_authority

[28] Rokhsareh Sakhravi, “Secure Mobile Payment Model Based on WAP”, March, 2009. [Online]. Available: http://www.site.uottawa.ca/~casteig/files/csi5169-rokhsareh-sakhravi.pdf

[29] C. Markantonakis and K. Rantos, “On the lifecycle of the Certification Authority Key Pair in EMV 96”, [Online]. Available: http://www.rantos.com/Papers/EMV_CA.pdf

[30] Darin Contini, Marianne Crowe, Cynthia Merritt, Richard Oliver, and Steve Mott. “Mobile Payment in the United States: Mapping out the road ahead” March 25, 2011. [Online].Available: http://www.frbatltanta.org/documents/rprf_pubs/110325_wp.pdf

[31] MasterCard Worldwide, “Security considerations for mobile point-of-sale acceptance”. [Online]. Available: http://www.mastercard.com/us/wce/PDF/PSI_Magazine_SecurityMatters_US.pdf

[32] Smart Card Alliance, “Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?” September, 2012 [Online]. Available: http://www.smartcardalliance.org/resources/pdf/Payments_Roadmap_in_the_US_091512.pdf

[33] Emms M, Arief B, Defty T, Hannon J, Hao F, and Van Moorsel A, “The Dangers of Verify PIN on Contactless

Cards", May, 2012. [Online]. Available: http://www.cs.ncl.ac.uk/publications/trs/papers/1332.pdf

[34] Visa, "Transaction Acceptance Device Guide", Version 2.0, March 2011. [Online]. Available: https://technologypartner.visa.com/Download.aspx?id=32

[35] Ramaswamy Chandramouli, Tim Grance, Rick Kuhn, and Susan Landau, "Common Vulnerability Scoring System" IEEE Security and Privacy, 2006

[36] Laurent Gallon, "On the impact of environmental metrics on CVSS scores", IEEE International Conference on Social Computing/ IEEE International Conference on Privacy, Security, Risk, and Trust, 2010

[37] Payment Card Industry Data Security Standard (PCI DSS), "Technical and Operational Requirements for Approved Scanning Vendors", September 2006, [Online]. Available:https://www.pcisecuritystandards.org/pdfs/pci_dss_technical_and_operational_requirements_for_approved_scanning_vendors_ASVs_v1-1.pdf

[38] Ayodele Ibidapo, Pavol Zavarsky, Dale Lindskog, and Ron Ruhl, "An Analysis of CVSS v2 Environmental Scoring" IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, 2011

[39] National Vulnerability Database, "Vulnerability Summary for CVE-2008-5827". [Online]. Available: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5827

[40] PCMag, "Nokia Intros NFC Phone That Doubles as Credit Card", [Online]. Available: http://www.pcmag.com/article2/0,2817,2079922,00.asp

[41] IBM Internet Security Systems Ahead of the threat, "Nokia 6131 NFC Data Exchange Format (NDEF) tag Code Execution",[Online].Available:http://xforce.iss.net/xforce/xfdb/44528

[42] National Vulnerability Database, "Vulnerability Summary for CVE-2012-5810". [Online]. Available: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5810

[43] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software," in ACM Conference on Computer and Communications Security, 2012.

[44] National Vulnerability Database, "Vulnerability Summary for CVE-2010-2913". [Online]. Available: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2913

[45] IBM Internet Security Systems Ahead of the threat, "Citibank Citi Mobile data Information disclosure", [Online]. Available: http://xforce.iss.net/xforce/xfdb/60855

[46] IT BusinessEdge, "Google Wallet Vulnerabilities Highlight Mobile Payment Security Concerns". [Online]. Available:http://www.itbusinessedge.com/cm/blogs/poremba/google-wallet-vulnerabilities-highlight-mobile-payment-security-concerns/?cs=49753

[47] Oludele Ogundele, Pavol Zavarsky, Dale Lindskog, and Ron Ruhl, "The Implementation of a Full EMV Smartcard for a Point-of-Sale Transaction and its Impact on the PCI DSS" ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust, 2012