Research Journal of Applied Sciences, Engineering and Technology 4(20): 4043-4050, 2012
ISSN: 2040-7467

Submitted: March 03, 2012 Accepted: March 16, 2012 Published: October 15, 2012

A Survey on Mobile Payment Systems Security

[1]Leila Esmaeili, [1]Zeinab Borhani-Fard and [2]Mohammad Ali Arasteh
[1]Information Technology Engineering Department, University of Qom, Iran
[2]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

Abstract: In recent years, increasing use of mobile devices and the emergence of new technologies have changed mobile commerce and mobile payment in all over the world. Although many attempts have been made to implement secure mobile payment systems and services, growing forgery, fraud and other related electronic crimes as well as security attacks and threats prove the necessity of paying special attention to security issues for development and extension of such systems. In this paper, we investigate classification of security threats and attacks in mobile payment and discuss security issues in three related areas of mobile payment; including network security, transmission security and mobile device security. Network security includes WLAN and WWAN security; transmission security includes WAP, SMS, wave channel and USSD security; and mobile device security includes hardware and software platforms and operating system security.

Keywords: Mobile commerce, mobile device, mobile payment, security, transmission, wireless network

INTRODUCTION

Today extensive use and customer acceptance of mobile payment services is a requirement for development of e-commerce and moving towards m-commerce. This depends on a high perception of security technical levels. This subject is more crucial when more payments and banking orders are carried out through mobile phones. For example in 2008 in the United Kingdom, 81% of banking orders by the total volume of 88 billion dollars were carried out by mobile phones, also fraud statistics are increasing and frauds made through mobile transactions make half of the total amount of frauds. Therefore, the identification and investigation of different security issues in mobile payment is of a great importance.

Generally, in a secure transaction and payment, the customers' privacy should not be compromised and there should be no possibility of financial losses. On the other hand for business owners, customer authentication is a crucial matter. As the general framework of any secure messaging system-confidentiality, integrity, non-repudiation, availability and authentication should be supported the m-payment services (Misra and Wickamasinghe, 2004). Despite the great efforts and security appliances in m-payment hardware design, transmission network, transaction protocols and etc, still world reports indicate a growth in the number of attacks, threats and crimes in recent years.

Reports from McAfee are related to three areas: mobile device security, transmission security and Network Security (Lopez, 2009). In this paper, we will investigate these three areas. Security issues of each of these areas along with its relation to the support layers of an m-payment system will be illustrated.

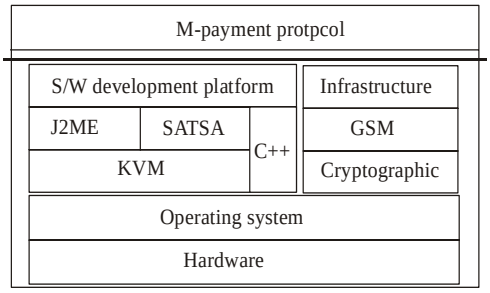

Fig. 1: Different layers of an m-payment system

INVESTIGATION OF VULNERABILITIES

M-payment system rides on underlying infrastructures like GSM and employs a technology like Bluetooth or Radio Frequency Identification (RFID). Security vulnerabilities in such underlying technologies are often ignored in analyzing the security aspects of an m-payment system. An accurate security analysis is possible only if we take a holistic view over the vulnerabilities at each dimension instead of considering only a specific dimension (e.g., protocol or platform) of the m-payment system (Fig. 1).

Layers of support for m-payment systems: At the highest level of m-payment systems we have the m-

Corresponding Author: Leila Esmaeili, Information Technology Engineering Department, University of Qom, Iran

payment protocol which rides on top of a software development platform and a wireless infrastructure. These underlying components in turn have a layered architecture comprising APIs, Operating Systems, hardware and etc. The KVM (K Virtual Machine) is a compact, portable Java virtual machine intended for small, resource-constrained devices such as cellular phones (Agarwal, 2007). To ensure the security of the m-payment system as a whole, it is necessary that every layer in the m-payment system be robust to attacks like man-in-the-middle attacks, replay attacks or impersonation attacks. Security features like authentication, authorization, confidentiality and non-repudiation are an absolute necessity for any m-payment application.

Taxonomy of vulnerabilities: Here we create taxonomy of some of vulnerabilities in different layers and their effects. We briefly describe them.

The prominent development platforms are J2ME and Symbian C++, both of which are known to have vulnerable APIs which give unauthorized access to restricted functionalities. Furthermore, some of the cryptography APIs provided by these platforms may use weak cryptographic keys or predictable random numbers which make them vulnerable to cryptanalysis and dictionary attacks. On the other hand, vulnerabilities in mobile infrastructure are generally a result of weak cryptographic algorithms or design flaws which make way for attacks like impersonation or man-in-the-middle attacks. Fixing these vulnerabilities is difficult as it would require a change in protocol design or in the cryptographic algorithms in the protocol. The most severe vulnerabilities are those related to the hardware. For example, as explained earlier, SIM cards play a very important role in an m-payment system as they uniquely identify a subscriber. If an attacker is able to clone a SIM card, then he can easily carry out malicious transactions on behalf of user. It has already been demonstrated that by using a side channel attack, it is possible to extract the 128-bit COMP128 keys used to uniquely identify a user. It is the responsibility of SIM card vendors to take steps in making the system robust against such side channel attacks. A recent development which has implications on the security of m-payment systems is the evolution of mobile malware. These malwares mainly exploit some vulnerabilities in the OS or misuse the various features (e.g., APIs) provided by the OS. The scheme of this taxonomy is demonstrated in Fig. 2.

NETWORK SECURITY

Network security is one of the three security arenas in m-payment systems. A secure mobile solution must prevent non-authentication accesses when the user is authenticated and exchanging data. This should be separately performed and embed in organizations which have firewall, influence detection and authentication

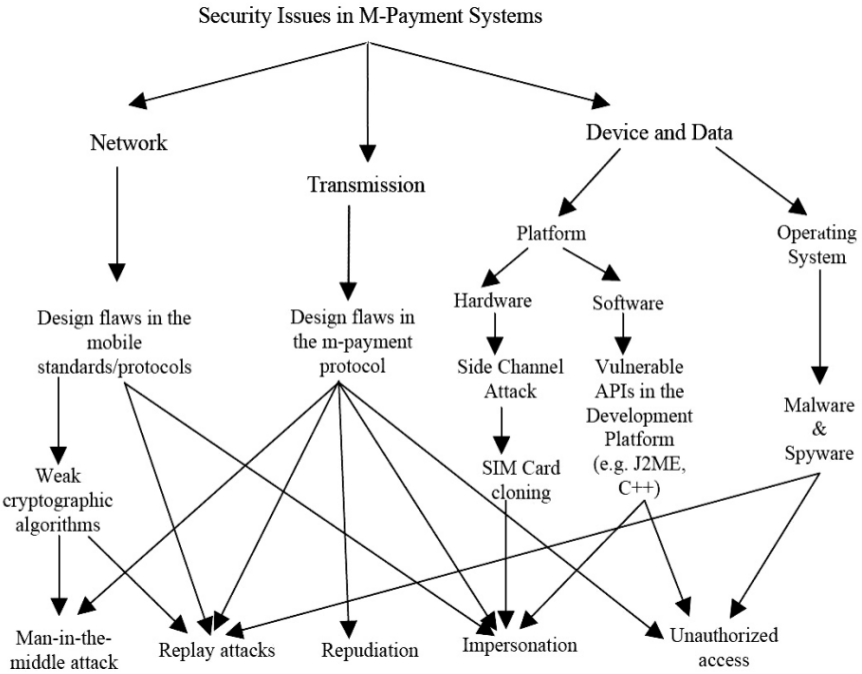

Fig. 2: Taxonomy of vulnerabilities affecting an m-payment system

systems because some of the merchants establish a VPN private network to communicate and transmit data. In the following sections, we investigate Wireless Local Area Network (WLAN) and Wireless Wide Area Network (WWAN); the WAP protocol which is related to the Internet Network will be presented in further.

WLAN and security: Devices used in WLAN technologies are lightweight and quite flexible in network configuration. Therefore, WLANs are suitable for office networks, home networks, Personal Area Networks (PANs), and ad hoc networks. In a one-hop WLAN environment where an Access Point (AP) acts as a router or the switch is a part of the wired network, mobile devices connect directly to the AP through radio channels. Data packets are relayed by the AP to the other end of a network connection. If no APs are available, mobile devices can form a wireless ad hoc network among themselves and exchange data packets or perform business transactions if necessary (Hu *et al*., 2005).

In Table 1, major WLAN technologies are compared in terms of the maximum data transfer rate (channel bandwidth), typical transmission range, and modulation technique

Bluetooth security: Bluetooth is a relatively secure technology on which most of the attacks are either theoretical in nature or are possible due to a bug in implementation. Also air sniffers make it possible to sniff the raw data being exchanged between two devices. Access to this data could open several possibilities for an attacker, such as cracking the PIN. A man-in-the-middle attack can be launched by cracking the link key (Agarwal, 2007).

Bluetooth provides security by using frequency hopping in the physical layer, sharing secret keys, called passkeys, between the slave and the master, encrypting communication channels, and controlling integrity. Encryption in Bluetooth is a stream cipher called "E0", while for integrity control a block cipher called "SAFER+" is used. However, "E0" has potential weaknesses (Biryukov *et al*., 2000; Jakobsson and Wetzel, 2001) and "SAFER+" is slower than the other similar symmetric-key block ciphers (Tanenbaum, 2002).

Wi-Fi Security: Security of IEEE 802.11 WLAN standard is provided by a data link level protocol called Wired Equivalent Privacy (WEP). When enabled, each mobile host has a secret key that is shared with the base station. Encryption algorithm used in WEP is a stream cipher based on RC4. The next version, IEEE 802.11i, is expected to have a better security by employing an authentication server that separates authentication process from AP (Hu *et al*., 2005).

Table 1: Major WLAN standards (Hu *et al*., 2005)

Standard	Max data rate	Typical range (m)	Modula-tion	Frequency band
Bluetooth	1 Mbps	5-12	GFSK	2.4 GHz
802.11b (Wi-Fi)	11 Mbps	50-100	HR-DSSS	2.4 GHz
802.11a	54 Mbps	50-100	OFDM	5 GHz
HyperLAN	254 Mbps	50-300	OFDM	5 GHz
802.11g	54 Mbps	50-150	OFDM	2.4 Ghz

Max: Maximum

Table 2: Major cellular wireless networks (Hu *et al*., 2005)

Generation	Radio channels	Switching technique	Standard (examples)
1 G	Analog voice channels	Circuit-switched	AMPS
	Digital control channels		TACS
2 G	Digital channels	Circuit-switched	GSM
			TDMA
		Packet-switched	CDMA
2.5 G	Digital channels	Packet-switched	GPRS
			EDGE
3 G	Digital channels	Packet-switched	CDMA2000
			WCDMA

Wireless wide area network and security: The most important technology in this category is cellular wireless network. Cellular system users can conduct mobile commerce operations through their cellular phones. Under this scenario, a cellular phone connects directly to the closest base station, where communication is relayed to the service site through a Radio Access Network (RAN) and other fixed networks. Originally designed for voice-only communication, cellular systems are evolving from analog to digital and from circuit-switched to packet-switched networks, in order to accommodate mobile commerce (data) applications. Table 2 lists the classifications of cellular wireless networks with its specifications.

GSM Security: An International Mobile Subscriber Identity (2009) or IMSI is a 15-digit unique number that contains Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Station Identification Number (MSIN). In GSM network the same authentication key and IMSI numbers are stored in both, the Authentication Center (AuC) and the Home Location Register (HLR). The security features provided between GSM network and mobile station include IMSI confidentiality and authentication, user data confidentiality, and signaling information element confidentiality. One of the security weaknesses identified in GSM is the one-way authentication. That is, only the mobile station is authenticated and the network is not. This can pose a security threat, as a compromised base station can launch a "man-in-the middle" attack without being detected by mobile stations (Hu *et al*., 2005).

UMTS Security: UMTS is designed to evolve from and reuse the existing core network components of the GSM/GPRS and fix the known GSM security weaknesses such as the one-way authentication scheme and optional encryption. Authentication in UMTS is mutual and encryption is mandatory, unless specified otherwise, to prevent message replay and modification. In addition, UMTS employs longer cryptographic keys and newer cipher algorithms which make it more secure than GSM/GPRS (Hu *et al*., 2005).

CDMA Security: CDMA use Advanced Encryption Standard, AES (Rijndael) algorithm for message encryption and have 128 bit key for confidentially and authentication. CDMA provides hashing and integrity with Secure Hashing Algorithm-1 (SHA-1). In addition, it provides anonymity, authentication and data protection. CDMA network security protocols rely on a 64-bit authentication key (A-Key) and the Electronic Serial Number (ESN) of the mobile. A random binary number called RANDSSD, which is generated in the HLR/AC, also plays a role in the authentication procedures. The A-Key is programmed into the mobile and is stored in the Authentication Center (AC) of the network. In addition to authentication, the A-Key is used to generate the sub keys for voice privacy and message encryption.

MOBILE DEVICE SECURITY

Mobile device security is guaranteed by providing data security in mobile devices and protecting them against malwares. The ideal term is when all data in the mobile device and moveable memory are encrypted. Also a secure solution might decrease the threats of malwares like viruses, Trojans and Worms. Different methods are available for securing mobile devices. A way to decrease risks is by not allowing programs to be downloaded and installed without identification and authentication; another effective method is not granting access to special programs without authorization. Finally, the use of enhanced third party programs that contain Antivirus and Firewalls is also efficacious. Some devices like RIM from BlackBerry have embedded Firewalls. Security issues in this area are related to Operating Systems and platforms which will be discussed in the following section.

Operating system security: Some of OS in mobile device are PalmOS, Windows CE, Linux on YOPY, Symbian and etc. These OSs differ greatly in architecture; so only a general comparison of these OSs is presented that we investigate PalmOS and Symbian.

PalmOS: can be considered the market-leader on PDAs. Security features of Palm OS concentrate on securing user data and authenticating users. All these features have some weaknesses in their security. Passwords can be retrieved and decoded, private data can be accessed and the encrypted data can be changed so that it becomes useless. Beginning with Palm OS 3.2, a strong security system for the "Web Clipping" technology has been implemented, containing Elliptic Curve-based key management, SSL authentication and encryption, DESX data encryption (DESX is a variant of DES that uses 128 bit of additional keying material to strengthen DES against brute force attacks), Message Integrity Check (MIC) (Kettula, 2000).

Table 3: Some of worms for mobile phone (Hypponen, 2006)

Contrast method	Functionality	Spread method	Name
Antivirus	Decrease charge battery	Bluetooth wih allowing user	Cabir
-	Change icons	Application (game or template)	Skulls
Delete from application manager	Inactivating SimWorks KasperSky	Install Antivirus.sis	Derver
Antivirus	Send SMS to contacts list.	bluetooth. MMS	Commwarrior

Symbian OS: has been subject to a variety of viruses, the best known of which is Cabir. Usually these send themselves from phone to phone by Bluetooth. So far, none have taken advantage of any flaws in Symbian OS-instead, they have all asked the user whether they would like to install the software, with somewhat prominent warnings that it can't be trusted.

Security issues due to mobile malware and spyware: Over the past few years, computer scientists have been witnessing the evolution of a vicious species called Mobile malware. The evolution of mobile viruses started with proof-of-concept worms like Cabir. The intention of the authors of Cabir was not to cause any financial damage to the victims but to make the world aware that it was possible to write viruses that could infect mobile devices. However, this idea was further explored by some virus writers who succeeded in writing viruses which caused the phone to malfunction (e.g., Skulls) or caused financial damages to the user by sending SMS messages (e.g., Viver) from his/her phone (Table 3). Currently, every week about ten mobile phone Trojans are added to antivirus databases. Going by the current trend it is clear that this threat will only increase in the future. In light of these facts, it has become very crucial for m-payment research community to analyze the impact of such malware on the security of m-payment systems. In this section we discuss the security implications of such malware on some m-payment schemes.

Platform: What we describe as platform, in this section is a discussion on hardware and software security in m-payment systems.

Hardware security: In 1990, SIM cloning for the first time was done on fundamental information in order to have the SIM recognized in the network. The main SIM card was put in a copy device, then the information was read and raw SIM card was written on a fake SIM card, therefore, the fake SIM card could be used just like the main SIM card. After all, a special wireless device could thieve, encrypt and store information without needing to access the SIM card for cloning. Though access to Ki in wireless is difficult but it is not impossible. Since there is no way to identify the real and cloned SIM card in the network the only way to avoid forgery and SIM card cloning is removing both SIM cards from the network. Today, less cases of cloning SIM cards are reported but this threat must not be ignored in designing SIM cards (He, 2007).

Software security: In this section, among the three main mobile programming languages, J2ME, BREW and Symbian C++, we investigate the two first languages.

J2ME Security: Several researchers have developed prototypes for their m-payment systems using J2ME. Debbai *et al*. (2005) documents a vulnerability in some Java-enabled phones that can be exploited to write a malicious MIDlet that sends SMS messages without requiring the user's authorization. This could affect the security of some SMS based schemes which require the user to send a SMS message (to the payment gateway) to initiate a transaction. If a malicious MIDlet is installed on the user's phone which sends SMS messages then it would be possible to initiate a transaction without the approval of the user (Agarwal, 2007).

BREW (binary runtime environment for wireless) security: BREW is a solution provided by Qualcomm and is applied in the mobile phones to be used in downloading small softwares and contents such as games, accounting softwares and so on. This program exclusively is used in CDMA-based phones. BREW is in competition with J2ME in GSM phones and is incompatible with it.

BREW is more retroactive compared with the former methods and provides a better security by supporting secure platforms. Also, it supports secure APIs and services and applies the encrypting algorithms (Varughese and Akasapu, 2007).

TRANSMISSION SECURITY

The Most used mobile phone network is GSM. Ninty five percent of countries and 71% of mobile phone users use this network. However, infrastructure of m-commerce in many countries is GSM and therefore its facilities and specifications must be precisely investigated. GSM provides four transmission channels each of which has its own special security characteristics. The mentioned four channels are WAP, SMS, wave channel and USSD. In continue, we discuss security issues in these technologies.

WAP Security: WAP has a mechanism for displaying Internet contents on mobile phones or any other wireless device; of course the mobile phone must support WAP. Web pages, for a precise displaying are implemented with WML language. WAP implementation on GSM was unsuccessful due to difficulties such as low speed and high costs but when implemented on GPRS network, it does not face such difficulties (Hu *et al*., 2005).

A method to guarantee security throughout the path is by putting WAP gateway in the local network of the organization or service provider. However, data get decrypted and encrypted in a secure network, but implementation and maintenance of WAP gateway need large resources and cost high (including costs for selling software and certificates) when there is a low volume of transaction, the takes a longer time to reverse assets.

One security problem, known as "WAP Gap" is caused by the inclusion of WAP gateway in a security session. That is, encrypted messages sent by end systems might temporarily become clear, readable text on the WAP gateway when messages are processed. One solution is to make the WAP gateway reside within the enterprise (server) network where high security mechanisms can be enforced (Hu *et al*., 2005).

The functional areas related to security in WAP include Wireless Transport Layer Security (WTLS), Wireless Identity Module, WAP Public Key Infrastructure, WML Script signText and End-to-End Transport Layer Security (Nambiar *et al*., 2004).

WTLS: WTLS protocol is a PKI-enabled security protocol, designed for securing communications and transactions over wireless networks. It is used with WAP transport protocols to provide security on transport layer between the WAP client in mobile devices and the WAP server in WAP gateway. Security services that are provided by WTLS protocol are authentication, confidentiality and integrity. WTLS provides functionality similar to Internet transport layer security systems, TLS (Transport Layer Security) and SSL (Secure Sockets Layer), and is been largely based on TLS, but has been optimized for narrow-band communications and incorporates datagram support. WTLS is implemented in most major micro-browsers and WAP servers. WAP 1.x series use the WTLS protocol to protect messages in the wireless network and in some way into the wired network, that is, between the wireless device and WAP Gateway. The WAP gateway transforms WAP 1.x stack to/from the wired TCP/IP stack, relays the data between the wireless and wired network, and communicates with the Web

Server that the mobile device is accessing (Nambiar *et al*., 2004).

Currently WTLS class 3 supports client/server authentication over a secured channel and mutual authentication between the server and consumer by an exchange of certificate. WTLS class 3 is secure enough to transmit the transaction information (Jonker, 2003).

WPKI: WPKI is an optimized extension of a traditional PKI for wireless environment (Raina and Harsh, 2002). WPKI requires the same components as a traditional PKI: an End-Entity Application (EE), a Registration Authority (RA), a Certification Authority (CA) and a PKI Repository. In WPKI, the End Entities (EE) and the Registration Authority (RA) are implemented differently, and a new entity, referred to as the PKI Portal, is introduced. The EE in WPKI runs on the WAP device. It is responsible for the same functions as the EE in a traditional PKI. The PKI Portal can be a dual-networked system, like a WAP gateway. It functions as the RA and is responsible for translating requests of WAP clients to the RA and interacts with CA over wired network. The RA validates the EE's credentials to approve or reject the request to receive a digital certificate (Nambiar *et al*., 2004).

The WAP PKI defines three levels of transport layer session security; WTLS classes 1, 2 and 3, and a sign Text--WMLScript functionality for digital signatures. WTLS Class 1 provides encryption; WTLS Class 2 provides encryption and gateway authentication; WTLS Class 3 provides encryption and a two-way authentication. The WMLScript sign Text is a functionality that the user interface can utilize for creating digital signatures. The sign Text uses the underlying security element WIM (Wireless Identity Module) that actually performs the cryptographic procedures and stores the secret keys securely. Basically, WPKI is concerned with the requirements on a PKI imposed by WTLS and the sign Text function.

WIM: Wireless Identity Module (WIM) is used in performing functions related to WTLS and application level security by storing and processing information; information such as secret keys and certificates needed for authentication and non-repudiation. To enable tamper resistance, WIM is implemented as software, performing on a microprocessor-based smart card.

WML script signText: WMLScript signText includes support for digital signatures of WML (display data format in wireless world analogous to HTML) coded content. SignText function allows a wireless user to digitally sign a transaction in a way that can be verified by a content server. This provides end-to-end authentication of client, together with integrity and non-repudiation of the transaction.

SMS security: SMS is sent through a separate signal path from voice channel and it has the capability of synchronizing transmission with voice, data and fax.

To protect the messages, SMS uses GSM encrypting mechanism and messages are maintained or exchanged in an unencrypted form in the other parts of the network. Storing messages in a SMS or SMSC center could bring about some problems like the offering a possibility to view or make a change in the messages by attackers. One of the risks threatening the SMS system is fake SMSs, usually sent through Internet which is also cheap and very easy to carry out (Ki Chong, 2006). When SMS is selected as a channel for m-Commerce, useful mechanisms such as STK are used to support security.

SAT: SIM toolkit is a specification of SIM and terminal functionalities that allow SIM to take control of the mobile terminal for certain functions. SIM Application Toolkit (SAT) is used to create Short Message Service (SMS) based mobile payment applications. In SIM Application toolkit based systems, the communication between mobile clients and the payment server occurs using SMS. SMS is used to initiate and authorize payments. The user is identified and authenticated by GSM authentication service and hence the GSM mobile network operator acts as an intermediary between the mobile client, the payment server, and the merchant (Mjølsnes and Rong, 2003).

SAT provides confidentiality, authentication, integration, and message replay protection, but does not provide denial of service or non-repudiation. This lack of support for non-repudiation is a major hindering factor for adopting SAT mobile commerce applications. SAT has built in support for data encryption standards including triple DES. The service provider places the encryption key before the SIM is issued to the customer. This ensures that the secret key never goes over the air interface. Authentication is provided by strong authentication algorithms, which can be chosen by the payment provider. Data integrity is realized using message digests like SHA and MD5. Other than not providing support for prevention of non-repudiation, the SAT also has another flaw caused by its using mobile clients' PIN code. PIN codes are usually 4 digit numbers, which can be guessed and entered into stolen or lost mobile phones, and undo the security provided by encryption algorithms or large keys.

Wave channel: This method is used for proximity payments and contains technologies like Bluetooth, RFID, NFC, Infrared, voice channel and so on. Bluetooth security was described in section 3.1.1.

RFID security: Generally, RFID with the objective of receiving information from static or dynamic objects is used by specific devices. This information can be about the identity of a person, location or any other entity-related information.

There should be reliability in all processes, components and equipments of RFID project. In these systems, provided the human errors decrease, reliability will drastically increase. Errors are mainly due to errors in data inputting like those in the selling process, transportation and distribution. To attain the 100% reliability we must overcome this problem. Still, the equipments sometimes do not work with the expected preciseness and the accuracy of readers is even sometimes less than 90% (Rothfeder, 2004).

Reliability in RFID depends on several factors. Generally, these factors are divided into two areas; subversive attacks and risks of technology. The subversive attacks which affect reliability are classified as organized spyware activities, Destroying and damaging tags, Sending parasite. The risks of technology that affect reliability also include Reading data wrongly, Collision and damaged tags.

NFC security: Near Field Communication or NFC, is a short-range high frequency wireless communication technology which enables the exchange of data between devices of about 10 centimeter distance. The technology is a simple extension of the ISO/IEC 14443 proximity-card standard (contactless card, RFID) that combines the interface of a smartcard and a reader into a single device. An NFC device can communicate with both existing ISO/IEC 14443 smartcards and readers, as well as with other NFC devices, and is thereby compatible with existing contactless infrastructure already in use for public transportation and payment. NFC is primarily aimed at usage in mobile phones.

NFC offers no protection against eavesdropping and is also vulnerable to data modification. Applications have to use higher-layer cryptographic protocols (e.g., SSL) to establish a secure channel.

Voice channel: Voice channels can be used to identify the customer. Mechanisms such as DTMF make transmission of data, such as passwords, through the channel possible. Voice can operate as a signal for identification with a mechanism like fingerprint. Also by using a speech to text software, one could use the voice to transmit the password. However, since this exchange of information is among a high traffic of thousands of other phone calls, there is a very low risk of having the secret data stolen (Katugampala, 2004).

USSD (unstructured supplementary service data): USSD is a GSM technology that like SMS is based on GSM capabilities for transmitting information on the signal channel and is regarded as a channel that could replace SMS to exchange information and authentication information. USSD is used in two modes:

- User starts communication; All mobile phones support this capability
- A program starts a communication with the mobile phone; this is implemented with quite different approaches in different phones

CONCLUSION

M-Commerce possesses many advantages like portability of data, generalization, network communication, ease in carrying out operations and etc; all of which have facilitated the development of commerce and have brought comfort in dealing with it. Among the most crucial infrastructures in this area are m-payment services in which security plays a very important role since assuring customers with security of a business is an important factor in the success and acceptance of the m-payment services. According to statistics, in developed countries like America, England, Japan and etc, although commerce has reached maturity and is widely used in these countries, still there are risks and security threats. Generally, technological progresses make it more difficult to sustain security. Therefore, this should not interrupt societies with their entering and progressing in m-Commerce.

Regarding the importance of security issues, this paper aimed at discussing security issues in m-payment in three areas; Network, m-Device and m-Transmission. In the area of Network, the security of WWAN and WLAN and in the area of m-Devices the security of Platforms and OSs were discussed. Finally the security issues in USSD, SMS, Wave Channel and WAP in Transmission were investigated.

REFERENCES

Agarwal, S., 2007. Security Issues in Mobile Payment Systems. Indian Institute of Technology, Bombay, India.

Carr, M., 2008. Mobile Payment Systems and Services: An Introduction. IDRBT Hyderarbad, India.

Debbai, M.S., M. Talhi and C. Zhioua, 2005. Security analysis of mobile Java. Proceedings of 16th International Workshop on Database and Expert Systems Applications. pp: 231- 235.

He, S., 2007. SIM Card Security. Ruhr-University, Bochum.Hu, W.C., C.W. Lee and W. Kou, 2005. Advances in Security and Payment Methods for Mobile Commerce. IDEA Group Publishing, Hershey, London, Melbourne, Singapore, ISBN: 1591403456.

Hypponen, M., 2006. Malware Mobile. Scientific American, INC. International Mobile Subscriber Identity, 2009. Retrieved from: www.en.wikipedia.org/wiki/International-Mobile-Subscriber-Identity.

Jakobsson, M. and S. Wetzel, 2001. Security Weaknesses in Bluetooth. In: Topics in Cryptography: CT-RSA 2001. Springer-Verlag, Berlin, Germany, pp: 176-191.

Jonker, J., 2003. M-commerce and M-Payment, Combining Technologies. BMI Papers Online, Bedrifs Wiskunde and Informatica, VU University, VU University, Amsterdam.

Katugampala, N.N., 2004. Real time data transmission over GSM voice channel for secure voice and data applications. Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN, the 2nd IEE (Ref. No. 2004/10660).

Kettula, A., 2000. Security Comparison of Mobile OSes. Helsinki University of Technology Telecommunication Software and Multimedia Laboratory, Swedish.

Ki Chong, M., 2006. Security of Mobile Banking: Secure SMS Banking. Data Network Architectures Group, Department of Computer Science, University of Cape Town, South Africa.

Lopez, M.D., 2009. Successful Mobile Deployments Require Robust Security. Lepoz Research LLC, San Francisco, CA.

Mjølsnes, S.F. and C. Rong, 2003. On-line E-Wallet System with decentralized Credential Keepers. Mobile Networks and Applications, Springer Netherlands.

Nambiar, S., C.T. Lu and L.R. Liang, 2004. Analysis of payment transaction security in mobile commerce. Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, Las Vegas, Nevada, pp: 475-480.

Misra, S.K. and N. Wickamasinghe, 2004. Security of mobile transaction: A trust model. Electron. Commer. R., 4(4): 359-372.

Raina, K. and A. Harsh, 2002. Commerce Security: A Beginner's Guide. 1st Edn., McGraw-Hill Co., Berkeley, Calif.

Rothfeder, J., 2004. What's Wrong with RFID? Retrieved from: www.cioinsight.com.

Varughese, P. and V. Akasapu, 2007. BREW Security: A Carriers' Perspective. Qualcomm.

Shamir, A., A. Biryukov And D.Wagner, 2000. Real time cryptanalysis of A5/1 on a PC. Proceedings of the 7th International Workshop on Fast Software Encryption.

Tanenbaum, A.S., 2002. Computer networks. 4th Ed., Prentice Hall PTR, Upper Saddle River, NJ.