International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 3, June 2018, pp. 1774~1780
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i3.pp1774-1780

The Fact-Finding Security Examination in NFC-enabled Mobile Payment System

Pinki Prakash Vishwakarma[1], Amiya Kumar Tripathy[2], Srikanth Vemuru[3]
[1,3]Department of Computer Science and Engineering, K L E Foundation, Andhra Pradesh, India
[2]School of Science, Edith Cowan University, Perth, Australia
[2]Department of Computer Engineering, Don Bosco Institute of Technology, Mumbai, India

Article Info

Article history:

Received Oct 23, 2017
Revised Jan 21, 2018
Accepted Mar 11, 2018

Keyword:

Mobile payments
NFC
Security threats

ABSTRACT

Contactless payments devised for NFC technology are gaining popularity. Howbeit, with NFC technology permeating concerns about arising security threats and risks to lessen mobile payments is vital. The security analysis of NFC-enabled mobile payment system is precariously imperative due to its widespread ratification. In mobile payments security is a prevalent concern by virtue of the financial value at stave. This paper assays the security of NFC based mobile payment system. It discusses the security requirements, threats and attacks that could occur in mobile payment system and the countermeasures to be taken to secure pursuance suitability.

Corresponding Author:

Pinki Prakash Vishwakarma,
Department of Computer Science and Engineering,
K L E Foundation,
Andhra Pradesh, India.
Email: pinki.vishwakarma@sakec.ac.in

1. INTRODUCTION

Presently, by virtue of ubiquity of mobile phones, people can perform financial payment anytime and anywhere [1]. Near Field Communication (NFC) is an emerging and neoteric technology in the field of mobile payments. It streamlines the eternity of motility and is gaining recognition in contactless payment. The time cards are being replaced by mobile phones; it is convenient to the users as there is no requirement to carry credit/debit cards along with them. With the prevalence of internet and E-commerce it has made feasible to transform the method of payment [1]. Howbeit, availability should not accord the security in mobile payments. Hence it is imperative to device security techniques to secure sensitive data at rest and data in transit.

Technology upping makes the life facile thusly it also rams the way business is consummated. In view of digitized transactions being disseminated and stored in mobile using internet it is essential to secure mobile payments. Howbeit, dissemination of electronic transaction results in cybercrimes and the security threats through mobile payments are colossal due to technology. In the face of fact that risk is associated with NFC technology, consumers find it appropriate for mobile payments. The consumers play an important role in protecting their personal information, should password protect their mobile devices and install antivirus software to defend against theft or malware attack.

Payment methods using mobile entail remote payment and proximity payment [2], [3]. In proximity payment the players involved use NFC technology to communicate, identical to contactless payment. In remote payment the players involved are not close to each other, encompass purchases from a web merchant by virtue of mobile phone. Examples of remote payment method are Electronic-commerce and Mobile-commerce transactions. Figure 1 shows the operating modes of NFC devices are reader/writer mode, peer to

peer and card emulation mode [4]-[11]. In reader/writer mode the NFC device acts as a reader for NFC tags and can perform either read or write data to the tag. In peer to peer mode the two NFC devices, initiator and target devices exchange information. In card emulation mode the NFC device acts akin a contactless smart card. The mobile phone is used instead of credit/debit cards to perform payment transaction.

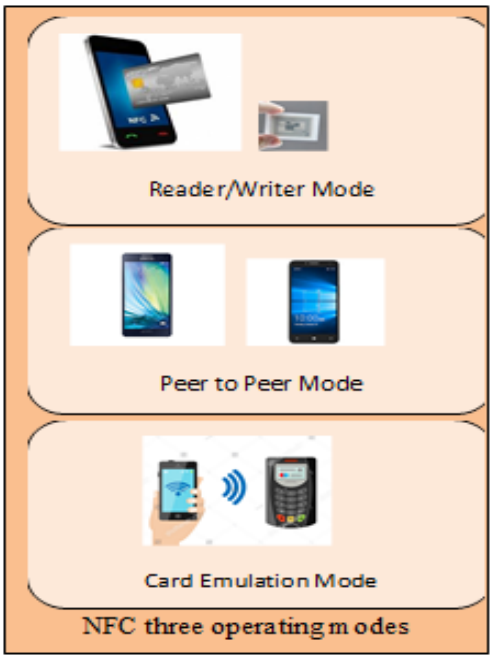

Figure 1. NFC Three Operating Modes

2. RELATED WORK

Electronic payment emerged ensuing the enrichment in the science involved and is considered as discerning field with respect to security [12]. The NFC devices operating in reader/writer mode, peer to peer mode and card emulation mode do not provide generic security protocol nevertheless reckon on application specific implementation [8]. Mobile payment acceptance by users when correlated to other traditional methods of payment is low as deficit of user trust plays a cardinal role in payment industry [13], [14]. The mobile phones are susceptible to various security threats as it contains sensitive data of payment users. The sensitive data may contain personal information or payment credentials of the users. Therefore, to secure sensitive data multifactor authentication techniques can be fancied [15].

Accessibility and Security are two factors whish persuade the users to use their smart phones for conducting financial transactions [16], [17]. The initiator and the target users of electronic banking system involved in transaction execution need determined identification. The key issues like security, privacy and authentication for securing banking transactions are necessary to be fathom [18]. With respect to secure mobile payment service, Kadambi *et al.* described a NFC-based mobile payment solution; it eliminates transmission of sensitive information over the network such as PAN and PIN [2]. End to End encryption techniques foster the sensitive data in mobile payment system [19].

3. SECURITY ASSAY OF NFC-ENABLED MOBILE PAYMENT SYSTEM

The mobile payments using NFC need evolvement of cryptographic protocols in furtherance of reconciling the desire security requirements. The security analysis of NFC-enabled mobile payment system is precariously imperative due to its widespread ratification.The NFC technology by virtue of wireless nature is susceptible to eavesdropping. It is futile to harbor across eavesdropping in NFC technology without the use of encryption, solution is to setup a secure channel. Data encryption in mobile payment imparts securing data and revitalizes mobile payment adoption.During data in transit, modification to the transaction data grounds security threats in mobile payment system.

The clover of mobile payments reckons on factors like security, faith, confidentiality and authenticity. Security and Reliability are the essential factors required for NFC technology placid to

understand prevalent ratification. To safeguard confidentiality, cryptographic mechanism can be used. The cryptographic key management forfend the mobile payment system's sensitive data from the attackers [20]. In the threat model the encrypted message cannot be encrypted without decryption key thereby preventing the attacker from performing any cryptanalysis.

Susceptibility of the payment information in mobile payment systems motivate towards security design. The security design refers to system design as free of susceptibleness and invulnerable to attack feasible through security controls. Mobile payments endeavor a scopic range of security facet nevertheless, it is the user who need to safeguard their data. Therefore, this can be consummated by using following knowledge.

a. Using unique and strong password
b. Updating anti-virus software
c. Using multifactor authentication
d. Encryption of sensitive data
e. Having remote data wipe facility in mobile phone

The innumerable transaction security is the prominent it is for all the entities involved in the mobile payment system. As NFC is a pullulating technology, cutting-edge mobile payment methods will preface new threats/risks. Consumer should ensue security measures like updating operating system on a regular basis when provided by OS provider, not using public Wi-Fi for making payments, using multifactor authentication to the mobile phone and in case of device lost/stolen having remote data wipe facility in the mobile phone.

Authentication and Authorization is critic for mobile payment system because it authenticates the consumer and authorizes the payment transaction. If there is proneness in authorization, then it might lead to impersonation attack. Security of mobile payment is vital as it affects the different entities in the payment system. In mobile payment system security threats are cognate to the business data in transit or data at rest.

In consequence, the study has been administered to how the mobile payment system can be made secure and reliable for the consumers to use. Consumer education and knowledge is a sarcastic facet in securing mobile payments. Considering pervasive usage and adoption of mobile payment services for consumer's security, privacy, trust and reliability should be immense. For any secure mobile payment system confidentiality, authentication, integrity and non-repudiation should be endorsed [21].Tokenization, user and device authentication and whitebox cryptography when combined in sync forms a flawless solution for defending mobile payment systems.

In mobile payments security is a prevalent concern by virtue of the financial value at stave. Mobile payments are secure if the user and device identification bind to the transaction authorization [22].When an attacker attacks the mobile payment application, looks for the payment credentials, cryptography keys. Since the tokens travel over the payment network, if made manifest the attacker can request for a new token generation, man-in –the-middle attack targets the payment application residing in the mobile phone operating system. Therefore, it is imperative to congeal the application to protect facing this type of attack. The attacker gains root access of the mobile phone and looks at the payment application code for critical information like payment credentials or cryptography keys. However, the token passes through the payment network makes use of standard protocols like SSL/TLS.

The creation of the surrogate identifier is very easy as coming up with random string numbers that can be matched up back to the original string. Hence tokenization eliminates the need for payment service provider, merchant's and e-commerce sites to store sensitive payment card data on their networks.

3.1. Security techniques in mobile payments

Mobile banking application need a secure environment as they process sensitive data. As the application requires processing and storing sensitive data it pilots to the growth of secure environments [23]. The security methods which can be enforced in the mobile payment applications are:

a. In mobile payments it is imperative to identify the user as authorized user of the mobile payment system. The general methods for user identification are soft token, biometric like user fingerprint is commensurable [22].
b. The goal of tokenization process is to replace the sensitive PAN value with non-sensitive token value [22]. By replacing sensitive data with surrogate identifier the user is ensuring that if any hacker receives this information, will be unable to use it for any purpose. The security of an individual token depends on the uniqueness and the infeasibility determines the original PAN knowing only the surrogate value.
c. The sensitive data can be stored on the cloud and can be procured by using mobile applications. In tokenization process, the token generation and caching can be accomplished in the cloud. Nonetheless, it is mandatory to secure the authorization access to the cloud server for this reason; user and device authentication should be consummated.

d. Thesensitive data is maintained with encryption and decryption operations without revealing the cryptography keys and the sensitive data. A means for protecting the cryptographic operations and the data is whitebox cryptography. With the whitebox cryptography [24] the attacker cannot decrypt the key when the token passes from the secure communication channel; neither is able to inject data into the channel.
e. The data at rest requires the sensitive data to be stored securely, the payment credentials of the payment users should not reside on the mobile device. The sensitive data of the users is encrypted and stored. The cryptographic keys used for encryption and decryption must be stored securely [20]. It should be relatively difficult for the attacker to know the cryptographic keys and the encryption/decryption process. The algorithms used for implementing encryption and decryption process must elude the attacker, leaving the sensitive data in a secure state.
f. The data in transit requires a secure communication channel which can be accomplished by using a secure communication protocol between the initiator and the target user. In mobile payment system tokenization and data encryption are effective methods for securing data in transit.

3.2. Secure mobile payment transaction

The discernment and knowledge of security threats are substantial within the payment ecosystem. A payment transaction is aforesaid reliable transaction when the authenticity of the entities and confidential information of the payment credentials vanquish. It is imperative to protect the sensitive data of the payment users [20]. The payment information and process on NFC enabled mobile devices desire the amalgamation of security techniques and protocols. Security in mobile payments is a prime concern for the players of the mobile payment system, consumers, merchants and the payment processors. To bestow secure mobile payment transaction, it should ensure confidentiality, integrity, authentication and non-repudiation [16], [21].

a. Sensitive payment data in mobile payments should be secured whether the data is in transit or at rest. Withal end-to-end encryption technique is used to secure payment data to armor its confidentiality and integrity. Confidentiality of payment information can also be preserved through tokenization process in mobile payment system. The transaction data sustained and presented should be precise and persistent.
b. Authentication consummate through user password and device fingerprints. Mutifactor authentication need to be deployed in lieu to the typical PIN for mobile payments. The authentication of a transaction using mobile device is also based on the consumer behavior pattern.
c. The AES encryption technique can be used for security against eavesdropping and data modification [25].
d. In mobile payments, the payment transactions are authorized using SMS or notifications containing payment details and transaction confirmation is sent to payee and payer. The payment transaction history is maintained for future investigation. Alluding the consumer transaction history and the spending pattern will lessen the risk of fraudulent transaction [26].

3.3. Security threats

Security threats and attacks aim the mobile payment system thereby causing financial loss [16].

a. Using untrusted network like Wi-Fi connection to make mobile payments can cause some accidental installation of fraud application on the mobile device, facade security risk for the consumer mobile devices. Jailbreaking and gaining root access of mobile device can break the default security provisioned by the mobile device manufacturer. The solution to malware threat is using sandboxing of mobile application on the device.
b. The attacker modifies the data that is being sent to reader device; relinquish the data in such a way that the transaction is not successfully executed. The explication to this attack is to establish a secure channel between the two NFC devices i.e. initiator device and target device and using a standard key protocol.
c. Losing the NFC mobile phone will be an asset to the discoverer and can constitute single factor authentication. The attacker makes effort to bypass PIN or fingerprint locks. It can make use of forensic tools to jailbreak the mobile device OS thereby, gaining access to the file system to steal data. The solution to this is remote data wipe out.
d. Despite of having a secure system, there's always a measure to invade. The victim node can impersonate a genuine node as a result of the deficit of authentication. Authentication is the key to impersonation attack. The sensation of user identity is important so it is imperative to always authenticate the user identity in the payment system.

4. RESULTS AND ANALYSIS

Viable countermeasures are bestowed in this section that will help to abate the security threats.

4.1. Threat analysis in mobile payment system

The mobile payment model players as shown in Figure 2 are the mobile device, POS, payment server, acquirer, issuer and fraud detection and prevention.

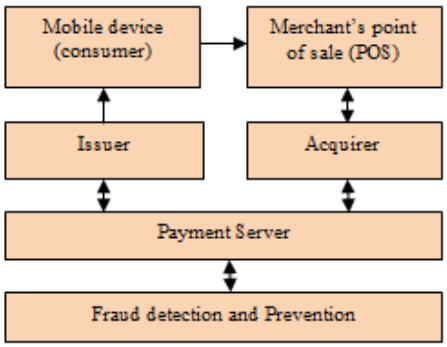

Figure 2. Mobile Payment Model

In mobile payment model consumer is a person who wants to buy goods or services from the merchant with a NFC enabled mobile phone.A merchant is an entity who has products or services to sell with a NFC reader.Issuer is the consumer's bank which interacts between the payment server and the consumer.Acquirer is the merchant's bank which interacts with the payment server and the merchant's POS. The payment server is an intermediate entity between the acquirer and the issuer, responsible for payment authorization and clearing. The fraud detection and prevention entity monitors transaction activities, identify and verify whether a transaction is fraudulent or legitimate. The threats and the viable countermeasures of the mobile payment system are described.

a. Malware Threat: The threats associated with the mobile device are malware and illegal access in case of lost/stolen device. Viable countermeasures are remote data wipe, multifactor authentication like PIN, password, biometric etc., OS updation time to time and antivirus.
b. Impersonation Threat: The threats between the mobile device and POS is impersonation and replay attack. The possible countermeasures are Encryption and use of secure protocols.
c. Relay Attack: The threats conjoin with the POS are malware and relay attack. The viable countermeasures are software updation, firewall and use of SSL/TLS connection.
d. Data Leakage and Access Control: The threats associated with acquirer/issuer are malware, data leakage, dataset hacking, access control and payment fraud. The viable countermeasures are multifactor authentication for access, fraud prevention strategy, data at rest encryption and use of SSL/TLS connection.
e. Data Modification: The threats associated with payment service provider are data modification and replay. The viable countermeasures are use of secure protocols and encryption.

The mobile payment exposures with respect to players of mobile payment system andassociated threats alongwith countermeasures are bestowed to abate the security threats.

5. CONCLUSION

The comfort to pay by using mobile device is convenient for the consumers rather than carrying their credit/debit cards. Howbeit, using a mobile device for performing financial transactions is not outside fortuity. With consumer aspect security, faith and accessibility are the pivotal elements in mobile payments. Thus in end-to-end process of mobile payments, beginning from transaction initiation by a consumer for purchase, authentication, verification and payment successful/declined should guarantee a secure environment. The mobile payment exposures with respect to players of mobile payment system are discussed along with the associated threats. Viable countermeasures are bestowed that will help to abate the threats.

ACKNOWLEDGEMENTS

The authors thank our colleagues from K L E Foundation who provided discernment and assistance that conspicuously assisted the research carried by us.

REFERENCES

[1] W. Jianping, "The Analysis and Optimization on M-commerce Secure Payment Model," 2011 *Third International Conference on Communications and Mobile Computing*, Qingdao, 2011, pp. 41-44.

[2] K. S. Kadambi, *et al.*,"Near-field communication-based secure mobile payment service," ICEC '09 Taipei, Taiwan, August 12 - 15, 2009, pp. 142-151.

[3] Richard Kemp, "Mobile payments: Current and emerging regulatory and contracting issues", *Computer Law & Security Review*, vol. 29, no. 2, April 2013, pp. 175-179.

[4] S. K. Timalsina, *et al.*, "NFC and its application to mobile payment: Overview and comparison," *2012 8th International Conference on Information Science and Digital Content Technology (ICIDT2012)*, Jeju, 2012, pp. 203-206.

[5] S. M. Shariati, *et al.*, "Investigating NFC technology from the perspective of security, analysis of attacks and existing risk," *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, Tehran, 2015, pp. 1083-1087.

[6] A. Armando, *et al.*, "Trusted host-based card emulation," *2015 International Conference on High Performance Computing & Simulation (HPCS)*, Amsterdam, 2015, pp. 221-228.

[7] 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, 2015, pp. 1308-1312.

[8] Michael Roland and Josef Langer, "Comparison of the usability and security of NFC's different operating modes in mobile devices," *Elektrotechnik undInformationstechnik*, November 2013, vol. 130, no. 7, pp. 201-206.

[9] Bangdao C.and Roscoe A.W, "Mobile Electronic Identity: Securing Payment on Mobile Phones" *In: Ardagna C.A., Zhou J. (eds) Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication.* WISTP 2011. Lecture Notes in Computer Science, volume 6633. Springer, Berlin, Heidelberg, pp. 22-37.

[10] VedatCoskun, *et al.*, "A Survey on Near Field Communication (NFC) Technology," *Wireless Personal Communications*, August 2013, vol. 71, no. 3, pp. 2259-2294.

[11] Ferina Ferdianti, *et al.*,"Utilization of Near Field Communication Technology forLoyalt Management," *TELKOMNIKA (Telecommunication Computing, Electronics and Control)*, vol. 11, no. 3, September 2013, pp. 617-624, ISSN: 1693-6930.

[12] N. E. Tabet and M. A. Ayu, "Analysing the security of NFC based payment systems," *2016 International Conference on Informatics and Computing (ICIC)*, Mataram, 2016, pp. 169-174.

[13] M. R. Hashemi and E. Soroush, "A Secure m-Payment Protocol for Mobile Devices," *2006 Canadian Conference on Electrical and Computer Engineering*, Ottawa, Ont., 2006, pp. 294-297.

[14] Lingling Gao and KeremAkselWaechter, "Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation," *Information Systems Frontiers*, June 2017, vol. 19, no. 3, pp. 525-548.

[15] Soonhwa Sung, *et al.*, "User authentication using mobile phones for mobile payment," *2015 International Conference on Information Networking (ICOIN)*, Cambodia, 2015, pp. 51-56.

[16] Y. Wang, *et al.*, "Mobile pent security, threats, and challenges," *2016 Second International Conference on Mobile and Secure Services (MobiSecServ)*, Gainesville, FL, 2016, pp. 1-5.

[17] Amir Herzberg,"Payments and banking with mobile personal devices,"*Communications of the ACM*, New York, USA, vol. 46, no. 5, May 2003, pp.53-58.

[18] AyangbekunOluwafemi J., *et al.*,"Analysis of Security Mechanisms in Nigeria E-Banking Platform," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 4, no. 6, December 2014, pp. 837- 847.

[19] Tracey Caldwell, "Securing the point of sale," *Computer Fraud & Security*, vol. 2014, no. 12, pp. 15-20.

[20] Pinki Vishwakarma, *et al.*, "Cryptosystem: Securing Data at Rest in Mobile Payment System," *Third International Conference on Computing, Communication, Control and Automation ICCUBEA 2017*, 17-19 August 2017 Pune, India.

[21] W. Feifei, "Research on Security of Mobile Payment Model Based on Trusted Third Party," *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, Wuhan, Hubei, 2010, pp. 442-445.

[22] Pinki Vishwakarma, *et al.*, "A Hybrid Security Framework for Near Field Communication Driven Mobile Payment Model", *International Journal of Computer Science and Information Security*, USA, vol. 14 no. 12, Dec 2016, pp. 337-348.

[23] Mohamed Amine Bouazzouni, *et al.*, "Trusted mobile computing: An overview of existing solutions," *Future Generation Computer Systems*, June 2016, ISSN 0167-739X.

[24] Brecht Wyseur, 2017, August 30, WBC: Protecting Cryptographic Keys in Software Applications, [Online]. Available: http://www.whiteboxcrypto.com/

[25] Kevin Curran, *et al.*, "Near Field Communication," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 2, no. 3, June 2012, pp. 371- 382.

[26] SadiqAlmuairfi, *et al.*, "Anonymous proximity mobile payment (APMP)," *Peer-to-Peer networking and Applications*, December 2014, vol. 7, no. 4, pp. 620-627.

BIOGRAPHIES OF AUTHORS

Pinki Prakash Vishwakarma has received B.E (Computer Engg.) degree in 1997 from University of Mumbai and M.E (Computer Engg.) degree in 2005 from B.V.D.U.C.O.E Pune, India. Currently she is a PhD Scholar in K L E Foundation, Andhra Pradesh, India. Her area of interest includes Mobile Commerce, Data Mining, Databases, Data analytics in secure transaction, etc.

Amiya Kumar Tripathy has received the PhD degree from the Indian Institute of Technology Bombay, India in 2013. He is a professor in the Department of Computer Engineering, Don Bosco Institute of Technology Mumbai, affiliated to University of Mumbai, India and adjunct professor to School of Science, Edith Cowan University, Perth, Australia. His general area of research includes data mining, Opinion Mining. Spatio-Temporal data analytics, Health-Informatics, Data mining in Agriculture, Data analytics in secure transaction, etc. Currently he is working on Remote Sensing and GIS based data analytics in Agriculture. He is member of IEEE and ACM. He has published several papers in refereed Journal amd Conference Proceedings. He is a program committee member to many international conferences and workshops.

Srikanth Vemuru received his B.E. and M. E. degrees in 1998 and 1999 from University of Madras, Tamil Nadu, India. After his masters, he worked in Software Industry on Web-based projects. Later on, he joined K L E Foundation as a faculty member in Computer Science and Engineering Department. He received his Ph.D. degree from Acharya Nagarjuna University (ANU) in 2011. He ishaving over 13 years of research experience and actively participating in projects related to Wireless Sensor Networks, Cognitive Networks, and Network Security. He published over 23 papers in major International journals and flagship conferences. He received best teacher award for more than three times. He is currently serving as the head of the department for Computer Science and Engineering. He is currently guiding 8 Ph.D. scholars and 8 M. Tech. students. He is an active member in professional societies like CSI, Indian Science Congress.