A Secure and Robust Mobile Payment System

[1]Abdullah Fahad Althumairy, [2*]Mohammed AlShehri & [3]Shaik Shakeel Ahamad
[1]a.thumairy@mu.edu.sa [2]ma.alshehri@mu.edu.sa & [3]s.ahamad@mu.edu.sa*
College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia

Summary
Current literature in the realm of mobile payments are not robust and secure. Intruders target three areas for vital information they are Mobile Payment Application (MPA), during the Transit of messages and Bank Server. This paper addresses these shortcoming and proposes a novel key management in the realm of secure mobile payments. Our proposed protocol ensures confidentiality, authentication and Integrity. Proposed protocol ensures security and freshness of the keys, overcomes reverse engineering, security of data at rest and during transit are ensured. Proposed protocol withstands replay attacks, impersonation attacks and Man-In-The-Middle attack.

Key words:
Secure Mobile Payments, Key Management, confidentiality, authentication, Integrity, Replay attacks, impersonation attacks and Man-In-The-Middle attack

1. Background

Mobile payment is payment for which data and instructions are initiated and confirmed by mobile device, so focusing attention more on procedures than on payment instruments or mediums of exchange [1]. Mobile payments are very popular and evolving very rapidly. Mobile Payment Applications (MPA) are replacing SMS and browser for transferring money using mobile phones. Despite its popularity there are some genuine concerns which are pushing back, particularly security of the transactions. A Mobile Payment Application (MPA) runs on a mobile device and contains vital information related to client's account. Intruders target three areas for getting important information such as passwords, One Time Passwords (OTP) and account information, the three areas are

i) Mobile Payment Application (MPA)
ii) During the Transit
iii) Bank Server

These assets belongs to the consumer side of mobile payments. Security of the bank server and security of the messages exchanged during the transit needs to be addressed. So our research focuses not only on the Mobile Payment Application (MPA) security but also on the bank server security and security during the transit. Existing literature in the security of mobile payments focuses on one of the three areas but in order to make it very secure we propose a secure and robust mobile payment system which ensures security.

[2] Proposes a protocol based on the concept of NFC mobile payments, an extension of NFC cloud Wallet model. The main limitation in this work is key management is not achieved, security and freshness of the keys are not ensured. In addition to these communication and application security are not ensured. [5] Claims to solve almost all the issues in the mobile payments but there is no clarity how the proposed system ensures all the security properties. [4] Proposes a Secure Mobile Payment Framework (SMPB) that relied on biometrics but has the following limitations

i) key management
ii) security and freshness of the keys are not achieved

Following are the contributions made

a) This paper addresses the limitations of the existing mobile payment solutions.
b) Proposes a novel key management in the realm of secure mobile payments.
c) Proposed protocol ensures confidentiality, mutual authentication and Integrity.
d) Proposed protocol ensures security and freshness of the keys, overcomes reverse engineering, security of data at rest and during transit are ensured.
e) Proposed protocol withstands replay attacks, impersonation attacks and Man-In-The-Middle attack.

The rest of the paper is organized as follows Section 2 presents the Proposed Mobile Payment System, Section 3 presents the Security analysis of our proposed system, Section 4 Comparative Analysis of the protocol with related work, Finally, Section 5 concludes the paper.

2. Proposed Mobile Payment System

Our proposed payment system has Payer. Payee, Bank and Certifying Authority (CA). Payer is the entity transferring money through bank to Payee. Payer and Payee has the Mobile Payment Applications (MPA) installed on their smartphones. Bank contains a Trusted Platform Module (TPM) which plays an important role in key management. Both Payer and Payee has their respective accounts in the

Manuscript received April 5, 2020
Manuscript revised April 20, 2020
*Corresponding author Email: ma.alshehri@mu.edu.sa

bank and bank provides the MPA to both payer and payee. Certifying Authority (CA) is responsible for issuing certificates to all the entities involved in the system. We propose a secure key management in our proposed mobile payment system. A symmetric key is shared between the Mobile Payment Application (MPA) of the client's smart phone and the Trusted Platform Module (TPM) of the Bank. The authenticity of Mobile Payment Application (MPA) is verified by the Certifying Authority (CA). Client generates his/her key pairs in the smart phone which contains public key and private key. Bank server also generates key pairs containing public key and private key. Client (C) and Bank (B) requests CA to generate their respective certificates by proving the possession of the equivalent private key to public key for which X.509 certificates are generated. CA issues X.509 certificates to the Client and Bank. We assume that Bank (B) has many accounts of the customers. Client access his/her bank account using Mobile Payment Application (MPA). MPA shares a symmetric key with the Trusted Platform Module (TPM) of the Bank. Communication security is ensured using SSL/TLS protocol. So our proposed protocol ensures both application security and communication security which is very important for banking transactions. Key management is very important for the acceptance and security of the payment system. Bank installs MPA on the client's smart phone Over The Air (OTA). The main feature of ensuring security in our proposed system is by updating the symmetric key at regular intervals which ensures security of the transmitted messages. Bank's TPM plays vital role in key management as TPM is tamper resistant and cannot be compromised.

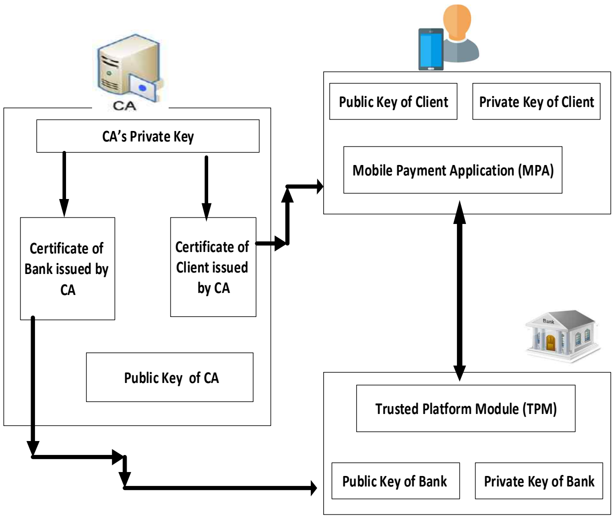
CA
CA's Private Key
Certificate of Bank issued by CA
Certificate of Client issued by CA
Public Key of CA
Public Key of Client
Private Key of Client
Mobile Payment Application (MPA)
Trusted Platform Module (TPM)
Public Key of Bank
Private Key of Bank

Fig. 1: Proposed Key Management in the Mobile Payment System

Table. 1: Notations

Notation	Full Form/Meaning
PayerID	Identity of the Payer
PayeeID	Identity of the Payee
$\mathbf{SYYKEY_{BPayer}}$	Symmetric Key Shared between Bank & Payer
$\mathbf{SYYKEY_{BPayee}}$	Symmetric Key Shared between Bank & Payee
T_B	Time Stamp generated by Bank
T_{Payer}	Time Stamp generated by the Payer
N_B	Nonce generated by Bank
N_{Payer}	Nonce generated by Payer
ACK	Acknowledgment
TID	Transaction ID
AMT	Amount

Our Proposed Protocol: There are three steps involved in our proposed protocol. Figure 2 depicts the steps involved in the proposed protocol.

$$\mathbf{Sep\ \ 1: Payer \rightarrow B: \{PayerD\ \ , AM\,T, N_{Payer}, T_{Payer}\}SYYKEY_{BPayer}}$$

Step 1: Payer authenticates himself to the MPA by inserting the PIN. He fills the MPA with$\mathbf{PayerD\ \ , AM\,T, N_{Payer}, T_{Payer}}$. MPA encrypts the message with the symmetric key shared between himself and Bank (B).

$$\mathbf{Sep\ \ 2: B \rightarrow Payer : \{PayeeD\ \ , AM\,T, ACK, TD\ , N_B, T_B\}SYYKEY_{BPayer}}$$

Step 2: Bank TPM receives the message and decrypts the message using the symmetric key shared between Payer and Bank (B). Bank verifies all the attributes in the message, if the verification is successful it transfers AMT to the Payee account and send the following message to the payer. $\mathbf{\{PayeeD\ \ , AM\,T, ACK, TD\ , N_B, T_B\}SYYKEY_{BPayer}}$ containing AMT, Transaction Identity (TID)

$$\mathbf{Sep\ \ 3: B \rightarrow Pay\,ee: \{PayerD\ \ , PayeeD\ \ , AM\,T, ACK, TD\ , N_B, T_B\}SYYKEY_{BPayee}}$$

Bank TPM now sends $\mathbf{\{PayerD\ \ , PayeeD\ \ , AM\,T, ACK, TD\ , N_B, T_B\}SYYKEY_{BPayee}}$ to the Payee. Payee decrypts the message and gets$\mathbf{\{Payer\ D\ , PayeeD\ \ , AM\,T, ACK, TD\ , N_B, T_B\}}$.

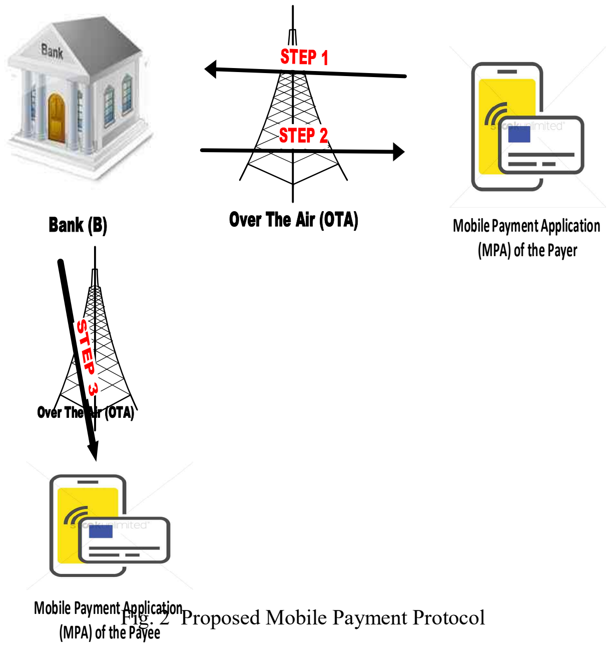

Fig. 2 Proposed Mobile Payment Protocol

3. Security Analysis

Confidentiality: Our proposed protocol ensures confidentiality as the message the message will be encrypted with the symmetric key shared between Payer and Bank (B) and moreover symmetric key is updated at regular intervals which ensures security of the symmetric and transmitted messages thereby ensuring confidentiality of the message.

Integrity: Our proposed protocol ensures integrity of the messages by both application security and communication security which is very important for banking transactions. Key management plays vital role in ensuring integrity of the messages.

Mutual Authentication: Our proposed protocol ensures mutual authentication property as MPA and TPM authenticate each other with their X.509 certificates. Bank TPM and MPA establish a secure communication layer authenticating each other ensuring mutual authentication.

Secrecy of the Keys: Our proposed protocol ensures secrecy of the keys as all the entities involved in the system share a symmetric key and the keys are stored in MPA (Payer and Payee) and in the TPM at the bank end. Symmetric key is updated at regular intervals in the TPM and in MPA which ensures security of the keys.

Replay Attacks: Our proposed protocol withstands replay attacks by nonce and timestamps exchanged messages in step 1 to step 3. In addition to these application security and communication security helps to overcome replay attacks.

Impersonation Attacks: Our proposed protocol withstands impersonation attacks because intruder cannot impersonate the payer/payee as he needs a PIN to open the MPA and intruder cannot impersonate the Bank TPM as it is protected by PIN and Biometric. So impersonation attacks are not practical in our proposed system.

Man-In-The-Middle Attacks: Our proposed protocol withstands Man-In-The-Middle attacks as it is not possible for the attacker/intruder to get the message as it is encrypted by the symmetric key shared between MPA and the Bank TPM. In addition to these application security and communication security helps in overcoming Man-In-The-Middle attacks.

4. Comparative Analysis with Related Work

Table 2 compares our proposed protocol with the related works [2, 4 & 5] discussed in section 1 and we found that our proposed system ensures Mutual Authentication, Confidentiality, Authorization and Accountability. Our proposed system ensures Freshness and Security of Keys, Application Security and implements Defense in Depth. Proposed system Overcomes Reverse engineering attacks, Replay attacks, Impersonation attacks, Man-In-The-Middle Attack. In addition to these proposed system ensures Security of the Data at Rest and during the Transit.

Table. 2: Comparative Analysis of our proposed work with related work

Protocols Features	[2]	[4]	[5]	OURs
Mutual Authentication	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes
Authorization	Yes	Yes	Yes	Yes
Accountability	Yes	No	No	Yes
Integrity	Yes	No	No	Yes
Freshness and Security of Keys	No	No	No	Yes
Application Security	No	No	No	Yes
Defense in Depth	No	No	No	Yes
Overcomes Reverse engineering attacks	No	No	No	Yes
Replay attacks	Yes	Yes	Yes	Yes
Impersonation attacks	Yes	Yes	Yes	Yes
Man In The Middle Attack	Yes	Yes	Yes	Yes
Security of the Data at Rest	No	No	No	Yes
Security of the Data during Transit	No	No	No	Yes

5. Conclusion

Existing solutions in mobile payments do not provide security at all the targets made by intruders so this paper addresses these shortcoming and proposes a novel key management in the realm of secure mobile payments. Our proposed protocol ensures confidentiality, authentication and Integrity. Proposed protocol ensures security and freshness of the keys, overcomes reverse engineering, security of data at rest and during transit are ensured. Proposed protocol withstands replay attacks, impersonation attacks and Man-In-The-Middle attack.

References

[1] European Commission, Towards an integrated European market for cards, internet and mobile payments, Green Paper, Brussels, 11 January 2012.

[2] Pardis Pourghomi, Muhammad Qasim Saeed and Gheorghita Ghinea, "A Secure Cloud-Based NFC Mobile Payment Protocol" International Journal of Advanced Computer Science and Applications (IJACSA), 5(10), 2014.

[3] B.Ratnakanth and P.S.Avadhani. "A Review of Secure Authentication based e-Payment Protocol" International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 3, 2017.

[4] S. S. Ahamad, V. N. Sastry, and M. Nair, "A Biometric based Secure Mobile Payment Framework," in Proceedings - 4th IEEE International Conference on Computer and Communication Technology, ICCCT 2013, 2013, pp. 239–246.

[5] Liping Du, Guifen Zhao, Ying Li. Building a Secure Mobile Payment Protocol in the Cloud. Open Journal of Social Sciences, 2016, 4, 59-63 http://www.scirp.org/journal/jss

Abdullah Fahad Althumairy is currently pursuing his Master in Cybersecurity and Digital Forensics at College of Computer and Information Sciences, Majmaah University Majmaah, Saudi Arabia. His research areas include Network security and Digital Forensics. He can be reached at a.thumairy@mu.edu.sa

Dr. Mohammed Abdulrahman Alshehri is currently working as a Dean and Associate Professor at College of Computer and Information Sciences, Majmaah University Majmaah, Saudi Arabia. His research areas include Computer Networks and applications, Network Security, Cyber Security, with specialization in Information Technology. He can be reached at ma.alshehri@mu.edu.sa

Dr. Shaik Shakeel Ahamad is currently working as an Assistant Professor in CCIS, Majmaah University, Kingdom of Saudi Arabia. He holds a PhD in Computer Science from the University of Hyderabad (a Central University which ranks second in India) and IDRBT (Institute For Development and Research in Banking Technology), Hyderabad, India in the realm of secure mobile payments protocols and formal verification. He has published more than 25 research papers in reputed International journals / Proceedings indexed by ISI, Scopus, ACM Digital Library, DBLP and IEEE Digital Library. He is serving as a Review Committee Member in many ISI indexed journals. He is CEI (Certified EC Council Instructor), ECSA (EC Council Certified Security Analyst), CHFI (Computer Hacking Forensic Investigator), Certified Threat Intelligence Analyst (CTIA) and Certified Application Security Engineer (CASE) – Java. His research interests include cloud-based mobile commerce, secure mobile healthcare frameworks, Block chain technology, Application Security and Smart Grids. He is a member of IEEE, Association for Computing Machinery (ACM), ISACA and OWASP (Open Web Application Security Project). He can be reached at ahamadss786@gmail.com & s.ahamad@mu.edu.sa