УДК 030 https://doi.org/10.33271/ebdut/77.134

SECURITY ISSUES IN NEXT GENERATION MOBILE PAYMENT SYSTEMS

T. I. Mshvidobadze, Professor, Gori State University (Georgia),
tinikomshvidobadze@gmail.com, orcid.org/ 0000-0003-3721-9252

Methods. In the security process system the following methods are used: analysis method (generalization of the problem, elaboration of the measures to improve security procedures), comparison (to identify of the assessment of M-Payment systems), formalization (to set the problem of the mathematical modelling).

Results. The different payment schemes and their use, technology and security have been generalized. Most pay methods are account-based payment systems and their core. The focus is on security, privacy and authentication.

Models of mobile payment system (MPS) have been proposed, as well as their technologies and payment methods, various security mechanisms embedded in MPS, encryption technologies and authentication methods. Mobile payment system security mechanism is proposed in response to modern demands. It has been demonstrated that keeping in check the confidentiality, integrity and availability triad, each payment should be made with authentication and encryption because the future of MPS depends on its security features.

Novelty. Scientific novelty of the research is in the outlining of strategic prospects of the encryption technologies, authentication methods, and firewall in MPS, to provide different security aspects.

Practical value. The potential impact of digitalization on mobile payment systems makes it more difficult than just the result of modular reorganization. The practical value of the paper is to fix the dynamics that can not be found in developed countries. Findings can be applied to other mobile payment systems in developing economies.

Keywords: Electronic Commerce, Business Models, Transactions, Mobile Payment Method, Online System, Payment System, mobile Commerce, Authentication, firewall, Cyberattacks.

Statement of problem. Mobile Electronic Commerce (MEC) refers to e-commerce activities relying solely or partially on mobile e-commerce transactions. MEC operates partially in a different environment than E-Commerce conducted in fixed Internet, due to the special characteristics and constraints of mobile terminals and wireless networks and the context, situations and circumstances in which people use their hand-held terminals.

MEC has a number of business, technical and legal implications that are different from ecommerce in the fixed Internet setting. Most notably, location-based products and services is a completely new business, technical, and legal area that is typical of MEC [1, p.123]. Wireless Application Protocol (WAP) on one hand and TCP/IP+HTTP supporting mobile handsets, Communicator on the other hand.

WAP plays an important role in MEC by optimizing Internet standards for the constraints of the wireless environment and hand held terminals and thus bridging the gap between Internet and mobile world.

Analysis of recent papers. The current research in the area is focused on the usage of mobile phone to perform payment securely. However, mobile systems face different limitations [2, p.355], such as low storage and computation power, due to which they cannot perform heavy encryption operations. Different attacks are reported on mobile devices due to lack of security

patches such as spoofing, phishing, malware, and sniffing attacks [3, p. 1]. Information and communication technology (ICT) is being extensively used all around the world [4, p.247].

Aim of the paper. The purpose of this article is in the outlining of strategic prospects of the encryption technologies, authentication methods, and firewall in MPS, to provide different security aspects.

Materials and methods. Security is essential for MPS, and many security standards such as PCI DSS (Payment Card Industry Data Security Standard) [5], which was first released in 2004, is used to maintain the CIA triad. The people or merchants who use payment cards follow PCI DSS standards but security violations can still occur. When security violations occur, personal information, payment card information such as expiration date, ATM card number, security code, and transaction ID are at risk, and it can lead to fraud or illegal usage of service.

Security and payment methods for mobile commerce

A Mobile Payment is defined as a payment for product or services between two parties for which a mobile device plays a key role in the realization of payment. In an MPayment activity a mobile phone is used by the payer in one or more steps during banking or financial transactions. The ubiquity of cell phones together with the convenience it offers suggests that mobile payments will constitute an increasing proportion of electronic payments.

Mobile applications can be either be mobile web or native. Security issues in mobile web applications closely resemble those of traditional web applications because of homogeneity in underlying development technologies and protocols. [6, p.78].

Researcher Saxena and others present a few ways to overcome various security threats with online payment systems [7, p.756].

Thangamuthu introduces various types of online payments such as credit card, e-wallet, debit card, net Bank, smart card, mobile payment and Amazon payment. The authors also present certain requirements for online payments, Such as integrity and authentication, out-of-zone authorization, password authentication, signature authentication, privacy, and accessibility and reliability [8, p.86].

Saranya and Naresh have proposed a new Secure Authentication Protocol (SAP) for mobile payments. The author used cryptography techniques for authentication between server and client. The proposed technique ensures the security of the user data account and ensures the confidentiality of the payment transaction [9, p.1].

There are two methods of Mobile Payment Systems: account based payment system and token based payment system [10, p.27].

1) Account Based Payment System.

In the account-based transaction, we need cards or information cards like ATM or credit card. Using this process, the amount is charged from the user's bank account after getting the required details or getting confirmation of the transaction from the user.

Risk Factor: If any misuse of card or details is done or any forgery or identity theft is done, then it will affect this system.

2) Token Based Payment System

It is a new electronic payment method based on tokens instead of cash or credit cards. These tokens are generated by any bank, service provider, or telecom company. Moreover, it is used in the same way as cash is used. By using such tokens, users can pay to any company through mobile, and those tokens will be sent to that company which they can encash, or the provider will pay them for each token.

Risk Factor: These tokens will have no worth if the user has tokens in their account and the merchant does not accept those tokens.

M-Payment Life cycle.

Payment transaction in a mobile environment is very similar to a typical payment card transactions shown in Fig 1. It differs in the transport of payment detail involved i.e. wireless device using WAP/HTML based browser.

Mobile payment lifecycle has the following main steps.

1. Registration: Customer opens an account with payment service provider for payment service through a particular payment method.

2. Transaction: Transaction mainly comprised of following four important steps.

a) The desire of a customer is generated using a SMS or pressing a mobile phone button.

b) The content provider forwards the request to the payment service provider.

c) Payment service provider then requests a trusted third party to authenticate and authorize the customer.

d) Payment service provider informs content provider about the status of the authentication and authorization. If successful authentication of the customer is performed, content provider will deliver the requested goods.

3. Payment settlement: This operation can take place during real time, prepaid or postpaid mode.

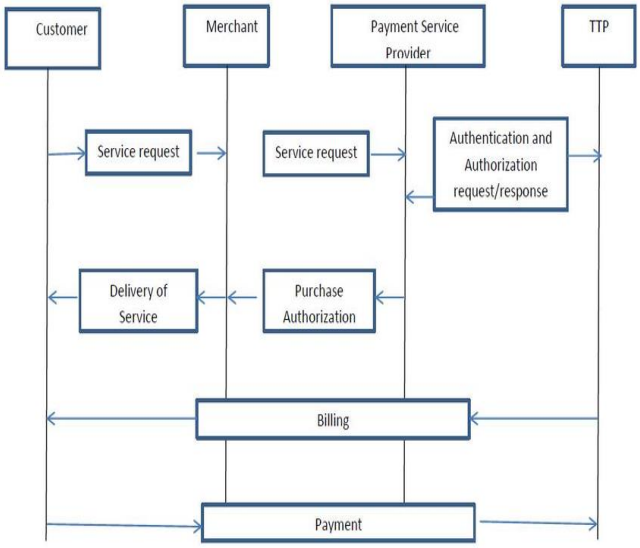

Fig 1: M-Payment life Cycle

A real time payment involves the exchange of some form of electronic currency, for example payment settlement directly through a bank account. In prepaid type of settlement customers pay in advance using smart cards or electronic wallets. In post pay mode the payment service provider sends billing information to the trusted third party, which sends the bills to customers, receives money back, and then sends the revenue to payment service provider. [11, p.3].

Mobile payment system security mechanism

MPS security mechanism included: Encryption technology, authentication, and a firewall.

Encryption technology.

Encryption technology included: Symmetric encryption and public-key encryption.

1) Symmetric Key Encryption (SKE) - SKE system uses a common key to encrypt messages, which means both sender and receiver will hold a common key for encryption and decryption.

2) Public-Key Encryption (PKE) - PKE system is a type of asymmetric encryption because the same key is not used to encrypt and decrypt the messages. In the PKE system, two different keys are used, called public and private key.

Authentication.

Authentication included: Digital signature and certificate authority.

Digital Signature (DS) is a string value calculated using text value to a Hash value.

Certificate Authority (CA) is a trusted organization that publishes and manages network security public keys infrastructure (PKI) and credentials for message encryption. As part of the PKI, the CA will use the registry for verification.

Firewall

The firewall can simultaneously protect the system/local network against network-based threats. The firewall allows access to the outside world to the local network. In most scenarios, a firewall is necessary because it is difficult to equip all devices with different security devices. [12, p.201].

Cyber attacks on mobile payment system

Attacks of various levels on MPS can be by unauthorized malicious users. The first attack is aimed at mobile money users. It involves users accessing the PIN via shoulder surfing when it does not have a mask with a four- to five-digit PIN [13, p.798]. This PIN can allow attackers to commit fraudulent transactions.

The second type of attack involves accumulating money Communication channels. Breaking and control MMS traffic and account manipulation for transactions can be done using these items.

The third type of attack is on a mobile money server Application. Access to the server for both mobile money agents and users is suspended when such an attack is carried out on the server.

The fourth point of attachment is the IT Administrator. The administrator computer can

be hacked by an unauthorized person, making it inaccessible to the administrator.

Technologies used in the M-PAYMENT process

The M-Payment system uses mobile technology to communicate between individuals involved in the payment process.

Near Field Communication (NFC) [14, p.1] is communication a protocol that allows communication between two devices. The Mobile Global System (GSM) [15, p.54] is the standard mobile communication system. Radio Frequency Identification (RFID) [16, p.54] uses electromagnetic field or tags attached to an object for identification. Short Message Service (SMS) [17, p.62] is a text messaging service used to communicate via mobile phone. Bluetooth is the standard for wireless technology; Using this we can connect devices to fix short distances.

An Identity-Based Signature (IB-Signature) [18, p.229] is a type of Public Key Infrastructure (PKI) in which a string representing an individual is publicly used as a public key, e.g., an email address.

Wireless Application Protocol (WAP) [19, p.397] is a standard protocol used to access information over a wireless network. Universal Factor 2 (U2F): This is an open authentication standard that provides two-factor secure authentication.

Processing the query on encrypted data is the solution To solve the additional overhead caused by using encryption, and such a technique leads to a significant improvement in the scenario where data needs to be processed in almost real time [20, p.120].

Security analysis includes various services: Confidentiality, Authentication, integrity, Customer Anonymity and others.

Confidentiality.

Privacy is provided using Java components, cryptography, OTP and PKI infrastructure, GSM security mechanism, A5 and A8, RSA encryption mechanism, DES and ECC, AES algorithm.

Authentication.

Authentication is performed by reading the RFID tag, which is embedded in the SIM card. RFID reader authenticates the user in this scheme. In authentication is provided by asking for a PIN and account number.

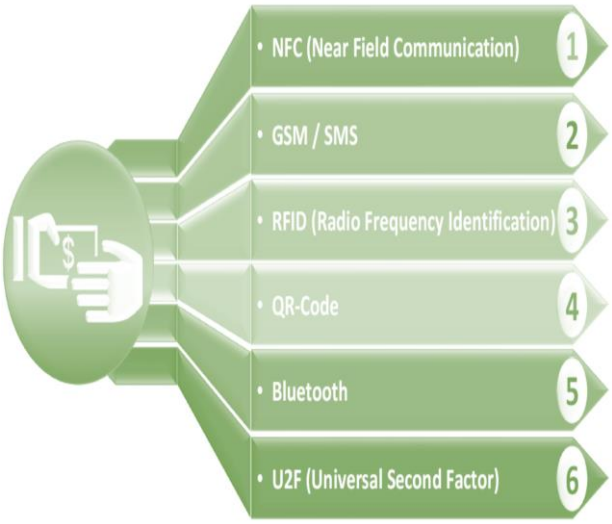

Fig. 2. M-Payment system based Technology

Customer anonymity

Do not need to re.gister with a merchant either before or during the transaction of any third party to ensure the anonymity of the client. According to W. Chen, a client's long-term ID card is not disclosed to the merchant, which ensures the client's anonymity [21, p.83].

Security analysis of M-Payment systems

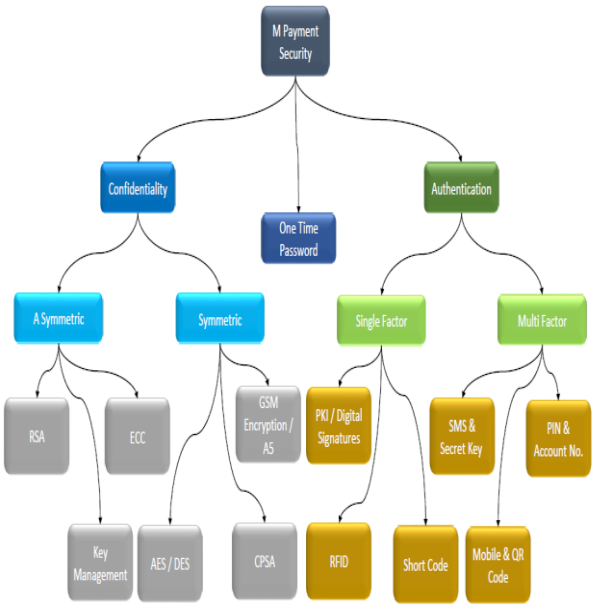

Fig. 3. M-Payment Security

According to Singh and Jasmine, anonymity of the user is guaranteed as it requires only the user's mobile, the number provided by their payment application or a short code [22, p.143].

Conclusion. Due to the increase in technology used worldwide to ease daily life activities, mobile payment systems also emerged rapidly for the same reasons.

This paper discusses the different payment schemes and their use, technology and security provided. Most pay methods are account-based payment systems and their core. The focus is on security, privacy and authentication.

The paper provides analysis of the encryption technologies, authentication methods, and firewall in MPS.

However, the main point is that keeping in check the confidentiality, integrity and availability triad, each payment should be made with authentication and encryption because the future of MPS depends on its security features.

In the future, research needs to be conducted on current delays using less mobile payment solutions and network remediation measures.

References

1. Pitoura, E., & Samaras, G. (1998). Data Management for Mobile Computing. Kluwer Academic Publishers, 1998, p. 123-127.

2. Cimato, S. (2001). Design of an authentication protocol for gsm javacards. Proceedings from MIIM ’01: International Conference on Information Security and Cryptology, (pp. 355-368). Springer.

3. Wang, Y., Hahn, C., & Sutrave, K. (2016). Mobile payment security, threats, and challenges. Proceedings from MIIM ’16: Second international conference on mobile and secure services (MobiSecServ), (pp. 1-5), IEEE.

4. Baza, M., Lasla, M, Mahmoud, M., Srivastava, G., & Abdallah, M. (2019). B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain. IEEE Transactions on Network Science and Engineering, pp. 247-250.
doi.org/10.1109/wcnc.2019.8885769

5. Securing the future of payments together. (2020).

6. Kumar, A., & Shanbhaug, J. (2012). Addressing Security and Privacy Risks Mobile applications.
IEEE Computer society. Pp. 78-83.

7. Saxena, S., Vyas, S., Kumar, B., & Gupta, S. (2019). Survey on online electronic paymentss security. Proceedings from MIIM ’19: Amity International Conference on Artificial Intelligence (AICAI), (pp. 756-751), IEEE.

8. Thangamuthu, A. (2020). A survey on various online payment and billing techniques. Humanities, vol. 7, no. 3, (pp. 86-91).

9. Saranya, A., & Naresh, R. (2021). Efficient mobile security for e health care application in cloud for secure payment using key distribution. Neural Processing Letters, pp. 1-12.

10. Téllez, J., & Zeadally, S. (2017). Mobile Payment Systems. Springer, pp.27-30.

11. Tian, F., et al. (2009). Application and Research of Mobile E-commerce security based on WPKI. Proceedings from MIIM ’09: IEEE Internatioal Conference on Information Assurance and Security, (pp. 3-7).

12. Sun, J., & Zhang, N. (2019). The mobile payment based on public-key security technology. Journal of Physics: Conference Series, p. 201, IOP Publishing.

13. Lakshmi, K., Gupta, H., & Ranjan, J. (2017). Ussd-architecture analysis, security threats, issues and enhancements. Proceedings from MIIM ’17: International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), (pp. 798-802), IEEE.

14. Tamazirt, P., Alilat. F., & Agoulmine, N. (2017). Nfc-based ubiquitous monitoring system for e-industry. Proceedings from MIIM ’17: Third International Conference on Mobile and Secure Services (MobiSecServ), pp. 1-4, IEEE.

15. Bhatta, A., & Mishra, A. (2017). Gsm-based commsense system to measure and estimate environmental changes. IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 2, pp. 54-67.

16. Tsao Y., Zhang Q., & Zeng, Q. (2016). Supply chain network design considering rfid adoption. IEEE Transactions on Automation Science and Engineering, vol. 14, no. 2, pp. 977-983.

17. Dix, S., Phau, I., Jamieson, K., & Shimu, A. (2017). Investigating the drivers of consumer acceptance and response of sms advertising. Journal of Promotion Management, vol. 23, no. 1, pp. 62-79.

18. Deng, L., Huang, H., & Qu, Y. (2017). Identity based proxy signature from rsa without pairings. IJ Network Security, vol. 19, no. 2, pp. 229-235.

19. Kizza, J. (2017). Security in wireless networks and devices. Proceedings from Guide to Computer Network Security, pp. 397-427, Springer.

20. Shahzad, F., Iqbal, W., & Bokhari, F. (2015). On the use of cryptdb for securing electronic health data in the cloud: A performance study. Proceedings from MIIM ’15: 17th International Conference on E-health Networking, Application Services (HealthCom), pp. (120-125).

21. Chen, W., Hancke, G., Mayes, K., Lien, Y., & Chiu, J-H. (2010). Nfc mobile transactions and authentication based on gsm network. Proceedings from MIIM ’10: Second International Workshop on Near Field Communication, (pp. 83-89), IEEE.

22. Singh, B., & Jasmine, K. (2012). Comparative study on various methods and types of mobile payment system. Proceedings from MIIM ’12: International Conference on Advances in Mobile Network, Communication and Its Applications, (pp. 143-148), IEEE.

ПРОБЛЕМИ БЕЗПЕКИ В МОБІЛЬНИХ ПЛАТІЖНИХ СИСТЕМАХ НОВОГО ПОКОЛІННЯ

Т. І. Мшвідобадзе, професор, Горійський державний університет (Грузія)

Методологія дослідження. У системі дослідження процесу безпеки використовуються такі методи: метод аналізу (узагальнення проблеми, розробка заходів щодо покращення процедур безпеки), порівняння (для виявлення оцінки систем M-Payment), формалізації (постановка проблеми математичне моделювання).

Результати. Узагальнено різні схеми оплати за їхнім використанням, технологією та безпекою. Більшість способів оплати – це платіжні системи на основі рахунку з ядром. Основна увага приділяється безпеці, конфіденційності та аутентифікації.

Запропоновано моделі мобільних платіжних систем (МПС), а також їх технології та способи оплати, різні механізми безпеки, вбудовані в МПС, технології шифрування та методи аутентифікації. У відповідь на сучасні вимоги запропоновано механізм безпеки системи мобільних платежів.

Продемонстровано, що, зберігаючи тріаду конфіденційності, цілісності та доступності, кожен платіж має здійснюватися з аутентифікацією та шифруванням, оскільки майбутнє MPS залежить від його функцій безпеки.

Новизна. Наукова новизна дослідження полягає в окресленні стратегічних перспектив технологій шифрування, методів аутентифікації та брандмауера в MPS для забезпечення різних аспектів безпеки.

Практична значущість. Потенційний вплив діджиталізації на системи мобільних платежів дещо складніший, ніж просто результат модульної реорганізації. Практична цінність роботи полягає в тому, щоб зафіксувати динаміку, якої не можна знайти в розвинених країнах. Висновки можуть бути застосовані до інших систем мобільних платежів у країнах, що розвиваються.

Ключові слова: електронна комерція, бізнес-моделі, транзакції, мобільний спосіб оплати, онлайн-система, платіжна система, мобільна комерція, аутентифікація, брандмауер, кібератаки.

Надійшла до редакції 03.02.22 р.