Survey on Security Mechanisms for Mobile Wallet

Atman Wagle, Sushmitha N.
Student, Assista t Professor
RV College Of Engineering, Bengaluru,

***Abstract*—In this paper, the objective is to highlight all the promising mobile wallet security mechanisms available. For the upcoming future and rapid pace of change in technology and computing, we will determine which technique is suitable when and where. With the help of our existing mainstream mechanisms, we will discuss each technique of security mechanism.**

***Index Terms*— Categories of mobile wallets, Types of mobile wallets.**

I. INTRODUCTION

The popularity of mobile wallets over the past couple of years has skyrocketed to an unbelievable extent, where we see a large section of the society is today seen using these wallets in their daily use and also aiming to reduce reliance on paper money for convenience purposes. However due to its rampant popularity in the society, there exists a section who tend to exploit these transactions for their own personal gain, which is criminal in nature. So to avoid such situations, there should be a secure environment around the transactions so that there is no scope for finding the vulnerability in the wallets and its transactions. The methodologies will be discussed about how to implement the security methods and mechanisms in detail but before discussing the possible suggestions for security, existing mobile wallets will be discussed first.

II. OVERVIEW OF DIFFERENT CATEGORIES OF MOBILE WALLETS

To begin with the identification of each technique, we classify them on various criteria to highlight each of its mechanisms. The classification is as follows:

A. Apple Pay:

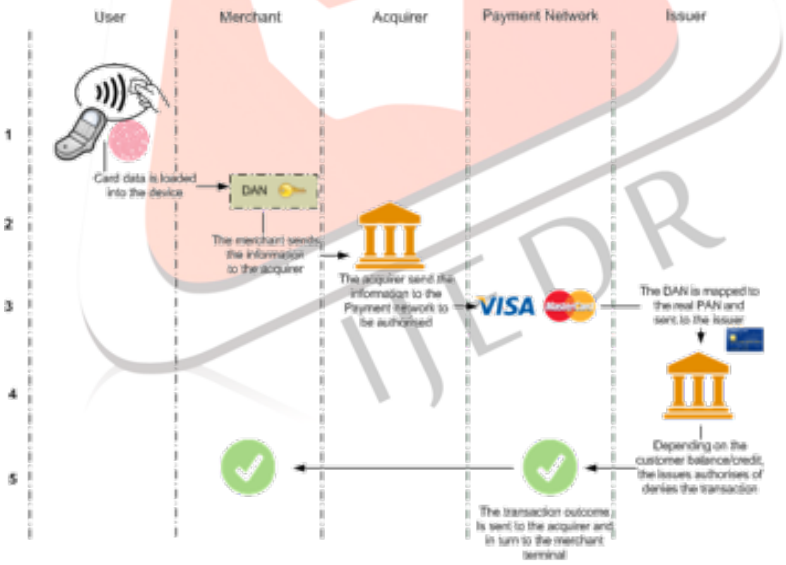

Figure 1.1: Architecture of Apple Pay

1) To start the transaction in int above Figure 1, the user places the device close to the NFC payment terminal. Apple Pay depends on TouchID (For Apple Watches its the PIN number) to identify the user. Once the card is selected, its token (DAN number) is loaded into the SE (Secure Element). EMV Contactless is being supported by Apple and therefore, in the event of being supported by the terminal, a dynamic cryptogram will be generated by the SE.
2) The information to the acquirer will be sent by the merchant. The bank is the acquirer that on the credit card transaction, it would get paid.
3) The DAN number is received by the acquirer, but it's unsure whether it is a valid PAN or a token. Apparently, the BIN (Bank Identification Number) is simply verified by the acquirer and via the payment network it is sent it to the appropriate issuer, where the network acts as a medium between the issuer and the acquirer.
4) The detection on the payment network will reveal that instead of a real PAN, it is actually a DAN and therefore the number will be forwarded to the TSP (Token Service Provider) so that the real PAN is sent back to the issuer.
5) The authorisation or denial of the transaction by the issuer prompts to relay the notification towards the acquirer, which will in turn send it back to the merchant.

B. Android Pay:

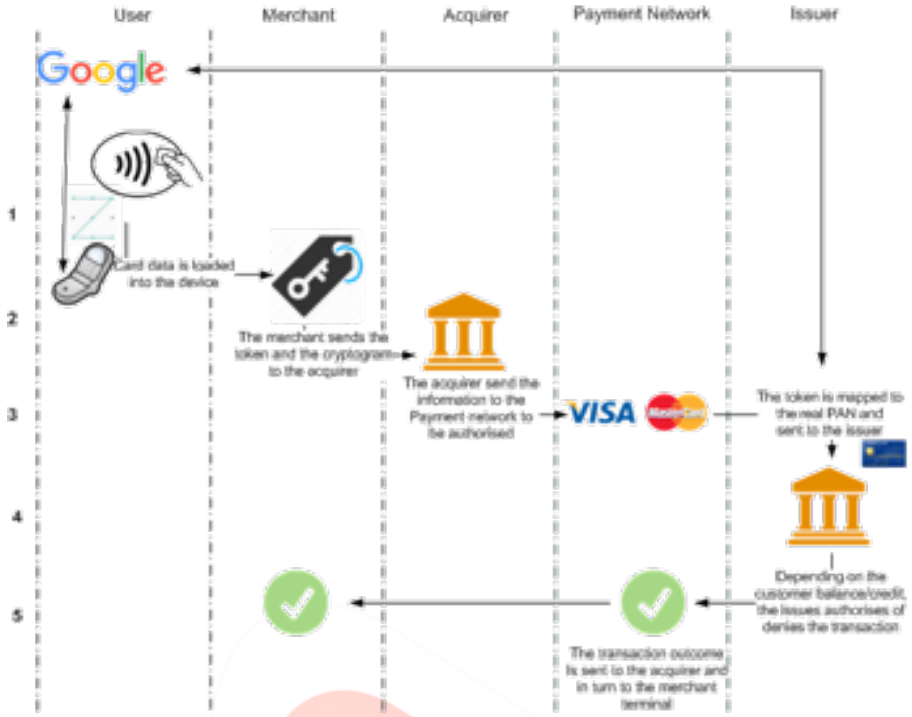

Figure 1.2: Architecture of Android Pay

1) Prior to the payment process in Figure 2, the device's connection to the Google servers has successfully done and a number of valid payment tokens has been provided. When the device is placed close to the POS terminal with NFC, NFC controller on the device will be enabled by HCE. The communication between the POS and the wallet will be handled by the NFC controller, where one of the tokens would be requested. The Cryptogram and the Dynamic Token are sent to the POS.
2) The information to the acquirer will be sent by the merchant. The bank is the acquirer that on the credit card transaction, it would get paid.
3) The token and the cryptogram is recieved by the acquirer via the payment network it is sent to the appropriate issuer, where between the acquirer and the issuer the network would act as an intermediary.
4) The real PAN will be requested by the payment network from the TSP (Token Service Provider) and for the approval it will be sent to the issuer.
5) The authorisation or denial of the transaction by the issuer will prompt to send a notification to the acquirer, which would relay it back towards the merchant.

C. Samsung Pay:

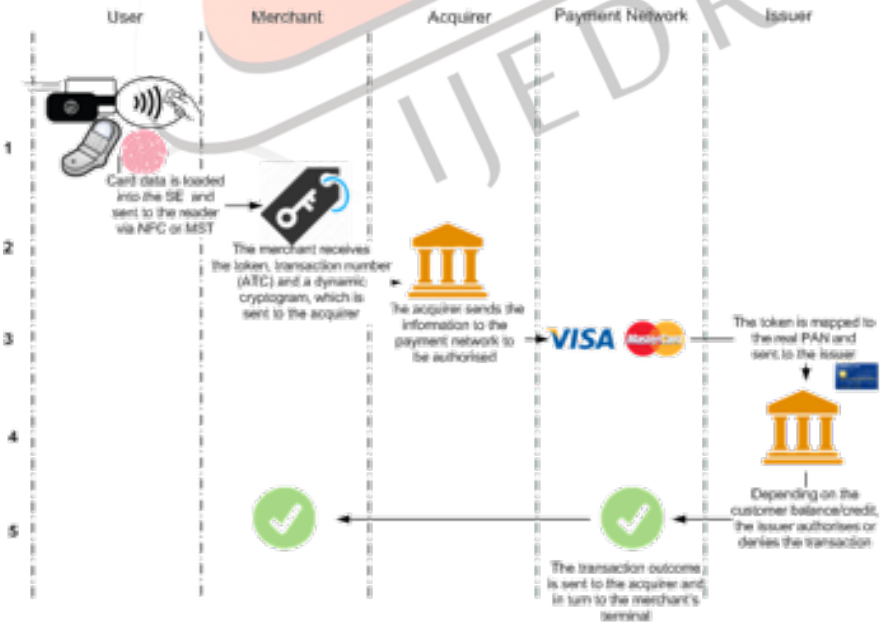

Figure 1.3: Architecture of Samsung Pay

1) In Figure 3, the payment will be initiated by the user by placing the handset close to the magnetic stripe POS or NFC. The payment process will be initiated by Samsung Pay using the MST technology or NFC transmitter. After selection of the card, 3 pieces of information are generated by the handset:

a. There is a digital linked to the card given by the payment network. Token's purpose is to hide the actual PAN and give freedom to the acquirer to route transactions to the correct payment network and issuer.
b. Incrementation of a transaction counter (ATC) on every single transaction and allowing the payment network to keep track of payment sequence.
c. A cryptogram generated with a secret key (which is known only to TrustZone), token and ATC.
2) After the information described above is received by the merchant reader, the message is conveyed to the acquirer.
3) The appropriate payment network will be identified by the acquirer and will forward the transaction information.
4) The token will be identified by the payment network and the TSP will be called to retrieve the real PAN number associated to it, which in turn be forwarded to the issuer in order to start the transaction.
5) The payment will be done only when the issues detected would clarify on the status of the transaction.
6) On the event of successful transaction the payment network will be notified, which in turn will also notify the merchant.

III. Various types of Mobile Wallet Methodologies

A. Cam-Wallet:

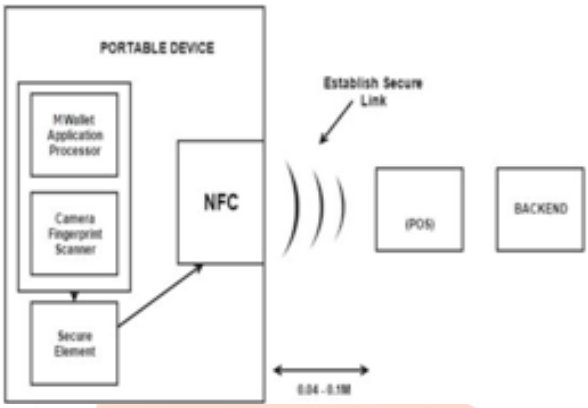

Figure 4: Architecture of Cam- Wallet

In this system, there is the approach of reading the fingerprint through the camera of the device whose ultimate aim is to reduce the device's reliance on the costly inbuilt sensor apparatus. To increase the security factors of the wallet mechanism, a shorter range of operation is chosen for which is helped by the NFC in the mobile devices. In Figure 4, the Cam-Wallet working is demonstrated where we have a scenario of it being used in a market at a POS terminal where the transaction will be made. The wallet will hold the card details and credentials of the user, where the transactions will be made via NFC. The Portable Device will hold details in it like licence details, identity details, insurance details, employee card details etc. The secure element keeps the security barrier between the internal storage and the NFC sensors to prevent any breach in data. Camera object detection algorithms can be optimized to make this proposal more effective and accurate.

B. Parasitic Authentication:

It involves the involvement of a an intermediary secondary device attached to the existing payment system to add an extra layer of security to the transaction process overall. As long as the secondary device remains in proximity with the primary device and can verify if the connected secondary device is a valid recognized device, then the main device has the authorization to complete the payment transaction. The identification protocols help distinguish the recognized secondary devices from the unknown ones so that security is maintained in the transaction process. The session for the transaction due to this mechanism can end in multiple ways for security reasons, i.e. when the transaction times out and there is no further relay from the secondary device, the transaction being cancelled by the secondary device and most importantly the transaction interruption due to the proximity levels between the two devices crossing the maximum range. All these add up to the security factors of the parasitic authentication. Here, the limitations are only the fact that hackers may try to bypass the secondary device authentication to compromise the overall device security.

C. E-Wallet Using E-Cheque:

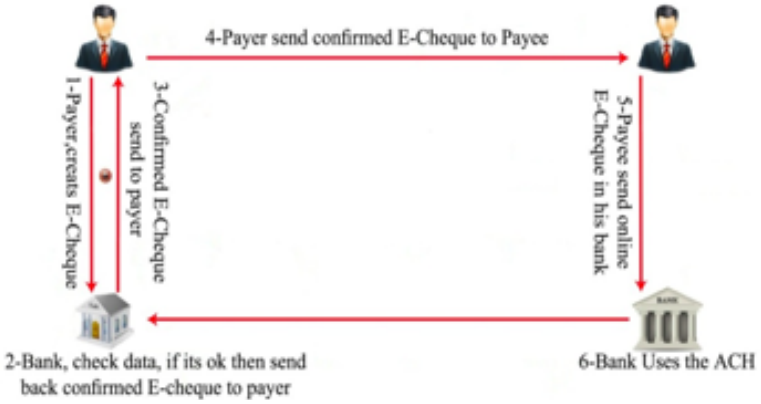

Figure 5 A sample E-Cheque implementation

During the ongoing transactions, the security of the transactions can be made more stronger with the adoption of the E-Cheque mechanism. It has all the features as that of a normal paper cheque. E-cheque has important fields like the Cheque Number, which is a unique and a rather big random number to identify E-cheque, payer's account number, beneficiary name, cheque amount, and date of payment etc.. But E-cheque fields depend on cheque regulations in each country, can could vary across regions. The E-Cheque security mechanism is facilitated by mathematical algorithms like digital signatures and since it is a form of cheque, it is also secured through the clauses of Confidentiality, Anonymity, Non-repetition, Generality and Non-repudiation. The above Figure 5 shares some insight about the proposed process.

D. Localized Assisted Server Mobile Wallet:

Traditional credential transfer models shown below in Figure have the shortcoming of misuse of credentials by the credential acquirer, who may not be a trusted party where the credentials can easily be accessed by a third party entity as there is no layer if security between them. Also this model makes the credential holder hold many of its credentials simultaneously which is rather inconvenient and finally the psychological factor of loss-tolerance which each individual may not have during the event of theft or misplacing the credentials issued.

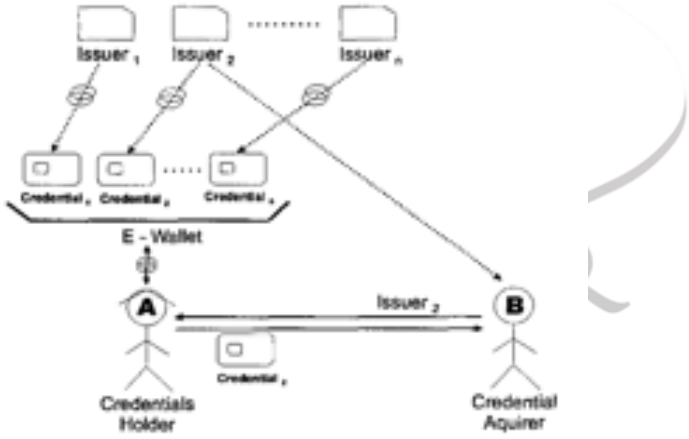

Fig 6 The mobile credential system assisted by distributed keeper-servers.

In the below proposed model in Figure 7 , it suggests the addition of a component to the existing model, which is called the distributed server keeper. It is responsible for the keeping the issued credentials safe from the third party acquirers and hackers by storing them in a separate tamper resistant and well protected location. Here, the credential keeper server helps in the movement of credentials across various entities to make sure they are not misused by acquirers. Even the channel between the credential holder and the credential keeper is secured and the credentials stored in it are encrypted to give a higher level of security. Only acknowledgement is shared to the credential acquirer and not the credentials itself by the server keeper to prevent credential misuse.

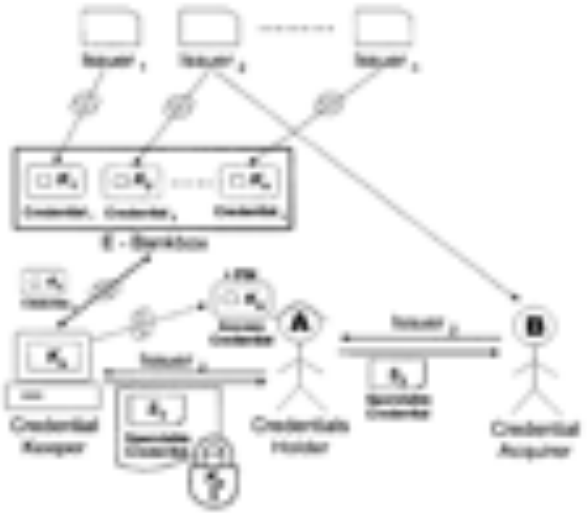

Fig 7 The mobile credential system assisted by distributed keeper-servers.

Conclusion

The paper exhibits an examination on different Mobile Wallet Security methods. We have mentioned different kinds of security mechanisms and have compared them with among themselves. Significant work has been done in the domain of data transaction and security methods, yet there is very insignificant work done on Mobile Wallets. The main motivation of the draft is to provide further references to the development of the mobile wallet security methods.

REFERENCES

[1] ENISA(2016), "Security of Mobile Payments and Digital Wallets", European Union Agency For Network and Information Security 2016, pp. 1-47, ISBN: 978-92-9204-199-1

[2] Obinna Stanley Okpara, Girish Bekaroo(2017), "Cam-Wallet: Fingerprint-based authentication in M-wallets using embedded cameras", 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS) Europe, pp. 1-5, ISBN: 978-1-5386-3917-7

[3] T. Ebringer , P. Thorne , Y. Zheng(2000),"Parasitic authentication to protect your e-wallet", Computer Volume: 33 , Issue: 10 , Oct 2000, pp. 54-60, ISSN: 0018-9162

[4] Shaghayegh Bakhtiari , Ahmad Baraani , Mohammad-Reza Khayyambashi(2009), "MobiCash: A New Anonymous Mobile Payment System Implemented by Elliptic Curve Cryptography", 2009 WRI World Congress on Computer Science and Information Engineering, pp. 286-290, ISBN: 978-0-7695-3507-4

[5] Behzad Yahid , Assadollah Shahbahrami , Mohammad Bagher Nobakht(2013), "Providing security for E-wallet using E-cheque", 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, 17-18 April 2013, pp. 1-14, ISBN: 978-1-4799-0393-1

[6] S.F. Mjolsnes , Chunming Rong(2001), "Localized credentials for server assisted mobile wallet", Proceedings 2001 International Conference on Computer Networks and Mobile Computing, 16-19 Oct. 2001, pp. 203-208, ISBN: 0-7695-1381-6