Study on Mobile Payment Systems: Security with Respect to Different Technologies (Present and the Future)

Team Members: Ajay Balaji (ab10297), Johnny Lai (jyl2021), Harshil Walia (hmw5970)

1 Introduction

Our world is changing at a rapid pace with advancement in mobile communications and technologies associated with it. We are adjusting ourselves with these technologies based on simplicity and convenience. After the introduction of mobile payments, currency usage was reduced to a great extent. We are entering an era of cashless payments and transactions with the help of technologies and the internet.

Recent survey revealed that more than two-thirds of the world population are using mobile phones. In October 2022, unique mobile users reached 5.48 billion. Continued growth in mobile technologies is helping to fuel these increases in digital adoption and activity. The current research in this area is focused on the usage of mobile phones to perform payment securely. The vast development of mobile technology has enabled the growth of mobile payments. Mobile payment systems use mobile technology for communication between the entities involved in the payment process. In this research, we a group of 3 students are going to study about mobile technologies like NFC, Bluetooth and QR code which are an integral part of many schemes or models of m-payment systems.

2 Related Work

Each one of us from our group will study about a unique mobile technology and provide report on below topics

- How security is implemented in the technology
- How security can be enhanced in the future to make it more powerful for mobile payments.

2.1 Bluetooth in Mobile Payment

Bluetooth Low Energy (BLE) is a widely adopted secure communication technology for connecting mobile devices and peripherals. Its applications in mobile banking and payment systems, e.g., point-of-sale (POS) systems are becoming more popular worldwide [1]. In the early 2000's, BBVA Bancomer deployed tens of thousands of Bluetooth-based POS payment terminals in Mexico. Similarly, EUROCARD was introduced as the first Bluetooth-based wireless payment system in Sweden. In 2013, PayPal introduced the PayPal Beacon system based on BLE technology, which enables consumers to pay for their in-store purchase completely hands-free [2][3]. In this study, we investigate the security aspects of the PayPal Beacon system.

2.1.1 PayPal Beacon

When deploying PayPal Beacon in a store or at any merchant premises, the system enables consumers to pay for their purchases completely hands-free. The Beacon device broadcasts a beacon signal, which can be detected by a consumer's phone if it has the PayPal app installed. When coming into a store, consumers get prompted on their phones if they want to check in. After checking in, consumers can make their purchases and have the items paid for automatically at the POS, without taking any action. The merchant will then get paid from the consumers' PayPal accounts. For consumers, a key advantage of PayPal Beacon is that they can pay for their in-store purchases completely hands-free; that is, no need to take out a phone, a credit card, or any device. This unique advantage is unmatched by other mobile payment technologies.

We investigate the PayPal BLE Beacon security risks and potential remedies in the areas of user authentication, authorization, message confidentiality, message integrity protection, and user identity confidentiality (privacy).

User Authentication: PayPal Beacon consumers are registered PayPal users who have installed PayPal app on their phones. When walking into a store, a consumer's phone will detect PayPal Beacon's broadcast message with a request to check in. The consumer has an option to opt-in/opt-out check in. Once opted in, the store's POS system will be able to retrieve the consumer's information from PayPal's payment service. The potential security risk is for hackers to impersonate PayPal Beacon and transmit broadcast messages for check-in, and the consumer chooses to check in, triggering the phone to transmit the consumer's PayPal account information. However, in order for the hackers to go further, they need to attack the POS system as well in order to intercept the actual consumer PayPal account information from the PayPay system.

Authorization: Once the consumer is authenticated, all purchases made by the consumer will be authorized to be paid for via the consumer's PayPal account. If hackers successfully impersonate the consumer, they can make purchases to be paid for by the consumer's PayPal account.

Message Confidentiality & Message Integrity Protection: By using Security Mode 1 and Level 4, the connection between Beacon and consumer phone can achieve a high level of protection on data transmission. The application of encryption and message authentication code (MAC) in BLE achieves both message confidentiality and message integrity protection.

User Identity Confidentiality (Privacy): To provide privacy and hide the devices' permanent addresses. The BLE network can use temporary private addresses, including resolvable private address on the consumer phones and non-resolvable private address of the Beacon device.

With the above major security areas addressed, the PayPal Beacon provides a secure and convenient mobile payment service.

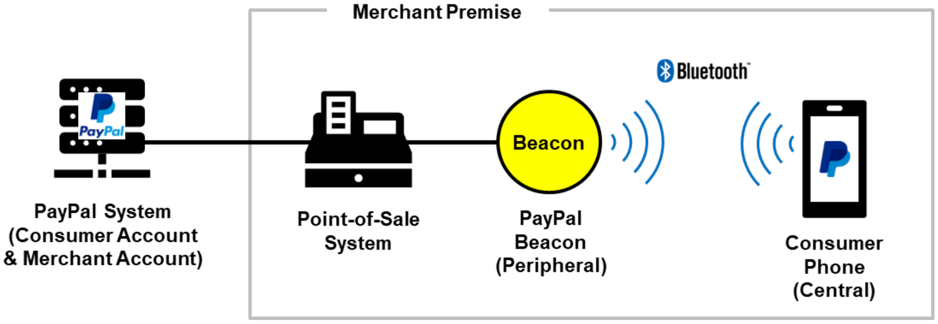


Figure 1 - PayPal Beacon Architecture

2.1.2 Future Opportunities and Challenges

The convenience, speed, and security offered by Bluetooth-based mobile payments help them to continuously gain popularity among merchants and consumers. However, the increasing number of Bluetooth-based mobile payment system infrastructures will become potential security liabilities in the future. We have learned that infrastructure and backward compatibility are forever, and hackers' tactics are constantly evolving. Going forward, the installed system legacy issues create major challenges for Bluetooth-based mobile payment system providers to ensure the security of their installed system base for a long time to come.

2.2 NFC Payment

Near Field Communication (NFC) payment is one of the mobile payment technologies for cashless transactions. NFC enables mobile phones and other devices to communicate and identify themselves in close proximity. Furthermore, the use of NFC for short-range communication allows for possible integration with existing point-of-sale equipment and merchants. A mobile phone or tablet with an NFC chip could make an NFC payment possible. Some of the major stakeholders who support NFC payment in the form of mobile wallets are Apple pay, Android pay, and Samsung pay. Figure 2 shows how an NFC payment will happen between a customer and a merchant.

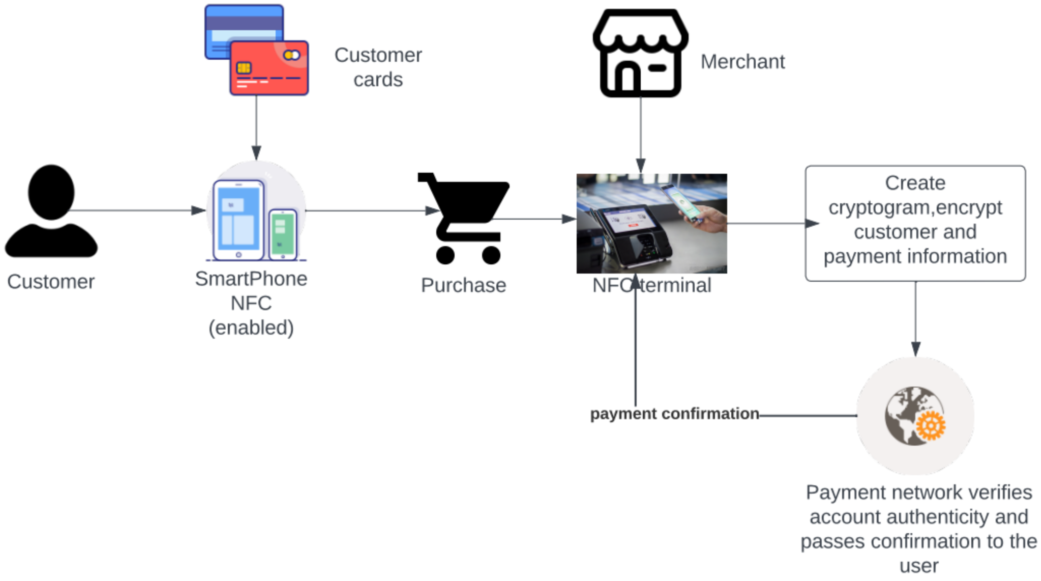

Customer cards
Merchant
Customer
SmartPhone NFC (enabled)
Purchase
NFC terminal
Create cryptogram,encrypt customer and payment information
payment confirmation
Payment network verifies account authenticity and passes confirmation to the user

Figure 2 - NFC payment process

2.2.1 NFC payment Architecture and Security Concerns:

In NFC mobile payment, if an end user wants to make payment, bank will check users' mobile phone and secure element using Mobile network operator (MNO). Bank will ask information like IMEI and SE from MNO. After verification, if user SE and mobile device meet the requirements for NFC payment, we can add our cards to the payment apps. There will be multiple actors involved in NFC payments, some of them are Secure Element (SE): Used to facilitate authentication and security, Bank: holds the funding account for consumer payment, payment network: authorization processing and the settlement of bank card transactions, MNO: highly active part of the NFC payment system when the UICC is the SE, TSM: facilitate management of the NFC payment application on the consumer's phone.

There are 3 different communication modes in NFC. 1) Reader/Writer mode, 2) Card Emulation mode, 3) Peer-to-Peer Mode. Card Emulation mode is mainly used for payment transactions. When a card is added to a mobile device, it will be stored in the safe place SE. This data can be accessed only when high level of security permission is granted for the payment application. Card Emulation mode helps NFC mobile to function as contactless smart card.

When we are using a new technology, the best way for protection is to know the risk associated with them. Figure 3 will show some of the possible security attack on NFC payment and its prevention

Security Issues	Description	Protection solutions
Over the air (OTA) transmission between phone and Point of sale (POS) - Interception of traffic	In this issue a person will acts as a man in the middle between two NFC devices and later the information from mobile will be altered before reaching POS.	TPM, secure protocols, encryption.
Installation of malware on mobile phone - Download app without knowing of malware	When any malware was installed in mobile app. There is a possibility that card information can be compromised.	proper software management and permission management.
Message modification and reply of transaction	Same transaction can be replayed again which will deduct amount again	Mutual authentication both on mobile side and POS side.
Cryptanalysis and dictionary attack	Breaking cryptographic algorithm	Strong cryptographic key implementation.

Figure 3 - NFC payment security

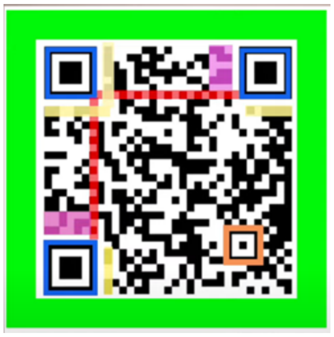
2.2.2 Future Opportunity and Challenges:

High infrastructure requirements – backend systems need to interact with SE in real time and TSM are required to download card credentials securely over the air to mobile phones. This will create an insecurity in consumer minds. In addition to that NFC wallet payment requires SE in mobile device, some of the headset will have NFC and not SE. This will limit the functionality and its expansion. We can implement a cloud-based NFC payments to overcome the above-mentioned challenges. Cloud based NFC payment uses the concept of mobile cloud computing (MCC) which stores the payment information in a remote server instead of mobile device. In managing sensitive data for an NFC transaction, SE acts as a single secure component. By storing data in the cloud rather than the mobile phone, the NFC cloud-based approach introduces a new method of storing, managing, and accessing sensitive transaction data. In this case the NFC phone is used to establish communication between the cloud provider and the vendor terminal. A cloud-based NFC technique appears to need a few more years to become economically viable based on the pace of the current generation of mobile data services.

2.3 QR Code

Quick Response code, popularly known as QR code is one of the most used modes of payment via mobile phones. A QR (figure 1) code is very similar to a barcode but a barcode is single dimensional and whereas a QR code is two dimensional which allows it to store a lot more information. QR codes break all the traditional limitations of a barcode, for example a barcode is static, once a barcode is generated for specific information, it cannot be changed and a barcode cannot be customized to look beautiful, its just black lines. On the other hand, a QR code is of 2 types, static and dynamic. A static QR code is similar to a barcode but with more information while a dynamic QR code can change its structure for the same type of information and along with that, we can also track the number of scans, their geolocations and other logistic information about it.

A QR code has 7 types of information.



1. Quiet Zone (Green marks)
2. Detection markers (Blue marks)
3. Alignment pattern (Orange marks)
4. Timing pattern (Red marks)
5. Version information (Purple marks)
6. Format information (Yellow marks)
7. Data and Correction keys

The Quiet Zone is the white space that separates the code from the background.

The Detection markers are the three huge blocks located at bottom left, top left and top right corners of the code. These markers tell the scanner in which direction to scan since it can be scanned in top-down manner and left-right manner.

The alignment pattern is a tiny box with a single black bit inside it which aligns the code even when it is scanned at an angle. The QR code shown in the figure 2 is a small one which needs only one alignment pattern but there can be more if the code is huge.

The timing pattern is the L shaped series of blocks that is used to determine the size of the matrix.

There are a total 40 QR code versions and the Version information markers represent one of those 40 versions.

The format information contains information about the error tolerance and data mask pattern making it easier to scan the code.

Data and correction keys are the rest of the code that contains all the information.

As fascinating the QR codes are, they come with their own vulnerabilities and exploits. QR code is extremely popular in Asian countries like China and India where the merchants stick a static QR code on the wall for people to scan or the payments for other purposes like renting a public bicycle have static QR codes on them. Many times, people replace these static QR codes with QR code with their own banking details and make the transactions go to their account rather than the original merchant. If we think about it in terms of security, this is an “Authentication” flaw. Out of various ways of solving this problem, we’ll talk about 2 solutions, one is using dynamic QR codes and the other one is to use split QR codes.

2.3.1 Dynamic QR codes

Unlike static QR codes that cannot be changed once the information is stored in it, the structure of the dynamic QR code can be changed without changing its contents. This mitigates the risk of someone replacing the original static QR code with their own since a QR code once used can be changed to a new matrix and the previous matrix would be useless. Dynamic QR codes can be generated using different cryptographic algorithms like SM2, SM3 and SM4. All these cryptographic algorithms are based on a very popular cryptographic algorithm SHA-256. Generating a dynamic QR code using SM2 will use the elliptic curve public key algorithm, SM3 is the cryptographic hash algorithm and the SM4 is the block-symmetric cryptographic algorithm. While talking about payment using a dynamic QR code, these algorithms can be used to generate a different matrix of the same information after every transaction or after every 5 - 60 seconds that will gradually reduce the attack of replacing the static QR code.

2.3.2 QR code and Visual Cryptography

In this method, the original QR code is split into 2 QR codes QR1 and QR2 using visual cryptography. One of the two QR codes (QR2) will be a static QR code that will be available to scan at the merchant’s location that will be scanned by the customer which will redirect the customer to the cloud location where the second part of the QR code (QR1) is available and downloaded and again with the help of visual cryptography, both the QR codes (QR1 and QR2) are stacked on top of each other to create the original QR code that has all the required information. The beauty of this technique is that we can authenticate the merchant with the help of a static QR code.

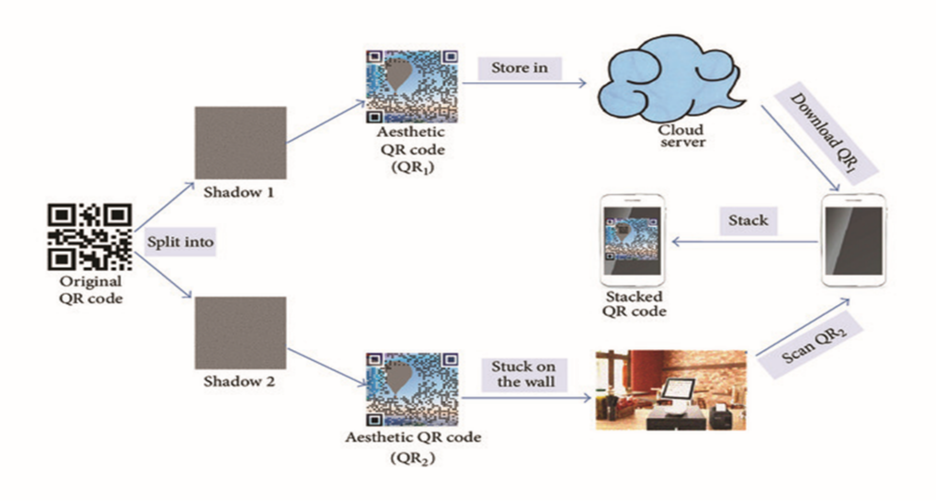


Figure 4 - QR Code Architecture with Visual Cryptography

2.3.3 Future improvements

I would suggest a method of infusing both the suggested methods into one by using visual cryptography with SM2, SM3 or SM4 to create dynamic QR codes that can be split into two and thus we can have a more robust system to authenticate the real merchants.

3 References

[1] K. Zolfaghar and S. Mohammadi, "Securing Bluetooth-based payment system using honeypot", 2009 International Conference on Innovations in Information Technology (IIT)

[2] PayPal Press Release, "PayPal Beacon To Reinvent the In-store Shopping Experience", Sep 9, 2013

[3] "How does PayPal Beacon work", Medium website, https://medium.com/paypal-tech/how-does-paypal-beacon-work-227dd70742bc

[4] W. Ahmed et al., "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 115932-115950, 2021, doi: 10.1109/ACCESS.2021.3105450.

[5] M. Al-Tamimi and A. Al-Haj, "Online security protocol for NFC mobile payment applications," 2017 8th International Conference on Information Technology (ICIT), 2017, pp. 827-832, doi: 10.1109/ICITECH.2017.8079954.

[6] Roland, Michael. Security Issues in Mobile NFC Devices, Springer International Publishing AG, 2015. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/nyulibrary-ebooks/detail.action?docID=1974132.

[7] Téllez, Jesús, and Sherali Zeadally. Mobile Payment Systems : Secure Network Architectures and Protocols, Springer International Publishing AG, 2017. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/nyulibrary-ebooks/detail.action?docID=5086669.

[8] https://www.freecodecamp.org/news/how-apple-pay-works-under-the-hood-8c3978238324/

[9] Raina, Vibha Kaw. NFC Payment Systems and the New Era of Transaction Processing, IGI Global, 2017. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/nyulibrary-ebooks/detail.action?docID=4827591.

[10] Y. Zhou, B. Hu, Y. Zhang and W. Cai, "Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance," in IEEE Access, vol. 9, pp. 122362-122372, 2021, doi: 10.1109/ACCESS.2021.3108189.

[11] Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, Chin-Chen Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography", Mobile Information Systems, vol. 2017, Article ID 4356038, 12 pages, 2017. https://doi.org/10.1155/2017/4356038