2016

Mobile Payment Security, Threats, and Challenges

Yong Wang
Dakota State University, yong.wang@dsu.edu

Christen Hahn
Dakota State University

Kruttika Sutrave
Dakota State University

Mobile Payment Security, Threats, and Challenges

Yong Wang
College of Computing
Dakota State University
Madison, SD 57042
yong.wang@dsu.edu

Christen Hahn and Kruttika Sutrave
College of Computing
Dakota State University
Madison SD 57042
cjhahn15637@pluto.dsu.edu,
kruttika.sutrave@trojans.dsu.edu

***Abstract* – Mobile payment systems can be divided into five categories including mobile payment at the POS, mobile payment as the POS, mobile payment platform, independent mobile payment system, and direct carrier billing. Although mobile payment has gained its popularity in many regions due to its convenience, it also faces many threats and security challenges. In this paper, we present a mobile payment processing model and introduce each type of mobile payment systems. We summarize the security services desired in mobile payment systems and also the security mechanisms which are currently in place. We further identify and discuss three security threats, i.e., malware, SSL/TLS vulnerabilities, and data breaches, and four security challenges, i.e., malware detection, multi-factor authentication, data breach prevention, and fraud detection and prevention, in mobile payment systems.**

Keywords – Mobile payment, security, threats, remediation challenges

I. INTRODUCTION

Mobile devices have reimagined our lives [1]. They are also innovating the way of payment methods. In addition to traditional payment methods, such as cash, check, credit card, debit card, etc., payments can also be made easily on mobile devices. Transactions on a mobile device can be conducted via Short Message Service (SMS) messages, at a point of sale (POS), as a POS, and online in the Internet. Mobile payment has become much easier and convenient and gained its popularity in many regions. Apple, Google, Samsung, PayPal, etc. all developed and released their own mobile payment systems. These mobile payment systems are available either on iOS, Android, or both devices. Forrester forecasts that US mobile payments will reach $90B in 2017, compared to $12.8B mobile payments in 2012 [2].

SMS payments were adopted earlier for purchasing using a mobile device. A text message with payment information is sent to a mobile payment service provider. The mobile payment service provider processes the transaction between the customer and the merchant. The cost of the purchase is then charged on the mobile subscriber's monthly phone bill. An early example of the mobile payment via SMS messages was demonstrated by Coca Cola in 1997 using a Coke vending machine [3]. As NFC (Near Field Communication) technology advances, NFC-enabled mobile payment systems are also available. Apple announced their Apply Pay program based on NFC technology on September 9, 2014. Apple Pay lets mobile devices make payments at contactless POS using a NFC antenna and in iOS apps. In addition to the NFC-enabled mobile payment systems, many online mobile payment systems, such as PayPal and Alipay, are also available in the Apple App store and the Google Play store. These mobile payment systems can also be used to make purchases at a POS in grocery stores or at restaurants.

Security is one of the biggest concerns in payment systems. Many regulations, i.e., PCI DSS (Payment Card Industry Data Security Standard) [4], are in place and have been enforced to ensure payment data security. Mobile payment service providers must also comply with these regulations. However, it is not an easy task to protect data. PCI DSS was first released in 2004. Any merchant who accepts or processes payment cards must comply with the PCI DSS. However, data breach still occurs [5], [6]. When a data breach incident occurs, payment card information, such as, user name, credit card number, expiration date, cardholder verification value, service code for purchase, might be compromised. Users who are affected are also exposed to fraud and identity theft.

Mobile payment systems also face other threats and attacks. Unlike a POS device in a large retailer which is constantly maintained, monitored, and exclusively used as a point of sale, a mobile device is not an exclusive device for mobile payment or as a point of sale. A mobile device is often shared by multiple apps and used for multiple purposes such as managing emails, word processing, and entertainment. It is up to the users to upgrade the mobile operating systems. A mobile device may or may not have the latest security patches. Many threats and attacks have been reported on mobile devices, such as sniffing, spam, spoofing, phishing, pharming, and malware [7]. These threats and attacks must be considered in the development of a mobile payment system.

This paper focuses on security issues in mobile payment systems. The remainder of this paper is organized as follows: Section II presents a mobile payment processing model and introduces mobile payment systems. Section III examines security mechanisms and desired security services in mobile payment systems. Section IV discusses mobile payment security threats and remediation, followed by a discussion of mobile payment security challenges in Section V. Section VI summarizes and concludes the paper.

II. MOBILE PAYMENT SYSTEMS

Mobile payment is a payment service performed from or via a mobile device. Many mobile payment systems are available on iOS and Android devices. A bank account, a credit or debit card, or a store-issued card, is often required to link to a mobile payment account before a purchase can be made.

A. Mobile Payment

A traditional card payment process is shown in Figure 1. It includes five key players, consumer (cardholder), merchant or

retailer, acquiring bank (merchant bank), issuing bank (cardholder bank), card associations (Visa, MasterCard, etc.) [8]. A cardholder presents his/her card to a merchant to make a purchase. The transaction data is collected at the merchant using a POS. The details of the transaction is sent to the acquiring bank. The acquiring bank captures the transaction information and routes it through the card network to the cardholder's issuing bank. The issuing bank receives the transaction information from the acquiring bank and responds by approving or declining the transaction. The response code is routed back to the acquiring bank and reaches the merchant's terminal. The cardholder receives the desired products or services if the transaction is approved by the issuing bank.

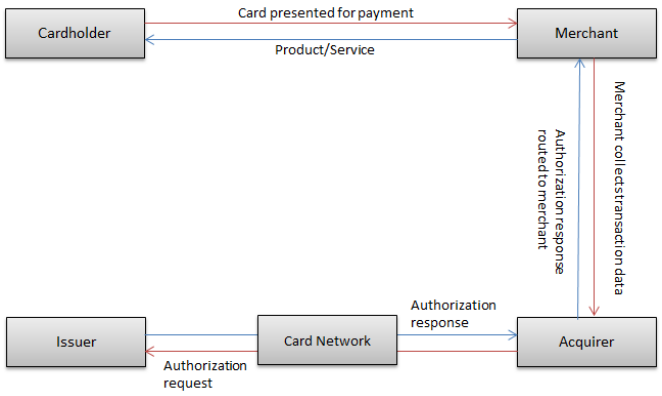

Figure 1. Traditional Card Payment Process

Figure 2 shows a process of mobile payment. In addition to the five key players in the traditional card payment process, two new players are introduced. These two new players are mobile network operators (MNOs) and mobile payment service providers (MPSPs). MNOs are mobile network carriers who offer direct carrier billing services. MPSPs are the service providers who provide mobile payment services.

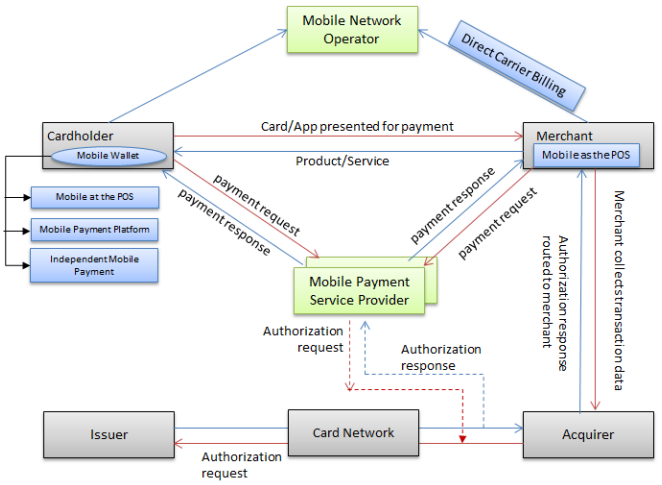

Figure 2. Mobile Payment Process

As new players are introduced, new business models are also created. A mobile payment user can now send money to another user within a mobile payment system. The process may involve only cardholders and a mobile payment service provider. There is no merchant, acquirer, card associations, and issuer involved in the process. The mobile payment service provider serves the role as an acquirer. One example is WeChat red envelope. WeChat red envelope is a program developed by Tencent and was launched on January 17, 2014. It has the functions such as delivering virtual money, withdrawing cash, checking transaction history, etc. A bank account is required to link to the WeChat account if a user wants to deposit cash or withdraw cash from the account. Otherwise, the user can deliver virtual money to peers as long as there is a balance in the user's account. During Chinese New Year in 2015, over 40 million virtual red envelopes were exchanged. In just a few days, millions of new users signed up for WeChat's red envelope program and linked their bank accounts to WeChat [9].

B. Mobile Payment Systems

Mobile payment enriches the traditional payment methods by introducing mobile at the POS (for cardholder), mobile as the POS (for merchant or retailer), mobile payment platform, and direct carrier billing. Mobile payment systems can therefore be divided into five categories, i.e., mobile payment at the POS, mobile payment as the POS, mobile payment platform, independent mobile payment system, and direct carrier billing. Mobile wallet usually refers to mobile payment at the POS and mobile payment platform which can be used to make purchases from multiple merchants and retailers.

1) Mobile Payment at the POS: This method enables the customer to pay with a mobile phone at the POS. Many of the methods are based on built-in NFC technology, such as, Apple Pay and Google Wallet.

These built-in payment systems are easy to set up on a mobile device. To set up Apple Pay, first, either scan the card number in with the camera or enter the information manually including the card number, three digit security code, expiration date, and the name on the card. Apple Pay then contacts the card issuer to ensure the card information is correct. Once confirmed, the user needs to agree to the terms and conditions. The application then talks to the card issuer once more and confirms, sets up, and adds the card to the wallet. Android Pay and Samsung Pay have similar setups.

To use a built-in payment system, hold the phone over a NFC-enabled terminal to make a connection using NFC. Then, depending on the smartphone, either unlock the phone, double click the home button, or place your finger on the fingerprint scanner to approve the transaction. The transaction is validated with the secure element (SE) chip. This chip relays authorization back to the NFC modem, and the transaction finishes the same way a traditional credit card swipe would. The terminal sends the merchant's id number, card information, and transaction amount to the card processor. Once the processor reads the information, it sends an authorization request to the card issuing bank. The card issuing bank then checks for fraud and verifies if the card can cover the transaction amount. It either approves or declines the transaction. The merchant is then notified whether the transaction was accepted or not.

Samsung Pay works a bit different than the other built-in payment systems. In addition to the NFC technology, Samsung Pay also utilizes magnetic secure transmission (MST). MST

allows users to use Samsung Pay at almost any store, because it can talk to standard magnetic credit card readers where a retailer has not upgraded to the NFC readers. This process mimics the same signal as physically swiping a card.

2) Mobile Payment as the POS: This method allows a merchant to use mobile as the POS and process card payments. This method usually requires a mobile app downloaded to a mobile device and requires a credit card reader connected to the mobile device. The setup is easy, quick, and convenient. It can provide card payment services at any time and from anywhere.

Square Register is an example of the mobile payment at the POS. Square Register supports both transactions from a credit card reader and keyed-in transactions. Three types of credit card readers are supported currently, i.e., Square reader for magnetic stripe cards, Square reader for EMV chip cards, and Square contactless and chip reader. Square contactless and chip reader accepts NFC payments like Apply Pay. PayPal also provides similar mobile payment as the POS service.

3) Mobile Payment Platform: This method provides online payment services on a mobile device. It requires a mobile app downloaded and installed on a mobile device. This method can also be used as mobile wallet to make a payment at a POS. A bank account or a credit/debit card account is usually required to link to the mobile payment account.

PayPal and Alipay (most popular in China) are two popular online payment systems which allow individuals and businesses to transfer funds over the Internet. PayPal and Alipay act as middle man. They are mostly used for online shopping, to pay utility bills, transfer money to other accounts, and to check out on shopping apps. Customers and merchants both need to have accounts to use the services provided by these payments systems.

Both sides signup with the mobile payment platforms and provide their bank accounts to these acquirers and in turn the acquirers handle the transactions. A buyer chooses to make a payment via one of acquirers. The acquirer credits the seller's account and debits from the buyer's account, and both sides are informed about the transaction.

4) Independent Mobile Payment System: This method provides similar mobile payment services like mobile payment platforms. A company may decide to develop its own online payment service to support mobile devices. These systems are called independent mobile payment systems. Examples of these independent mobile payment systems include the mobile apps from Amazon, Starbucks, etc.

Independent mobile payment systems are very similar to mobile payment platforms except that the independent mobile payment system is used only for the company itself. An independent mobile payment system can be transformed to a mobile payment platform if it is widely adopted and supported by merchants and retailers. For example, WeChat red envelope was a program introduced by WeChat in 2014. It became so popular and has been transformed to a mobile payment platform, WeChat Wallet, and adopted by many merchants and retailers in China.

5) Direct Carrier Billing: This method allows users to purchase products or services using their mobile devices. It does not require a credit or debit card as a payment. The cost of the purchase is charged on the mobile subscriber's monthly phone bill. Direct carrier billing usually involves charging via SMS messages. A user enters his/her mobile phone number to make purchases on a website. A transaction code is provided to the user via a text message. The user enters the code on the website to confirm the purchase.

Direct carrier billing is very popular in Europe. For example, Boku works with 250 carrier partners and provides direct carrier billing service in Europe [10]. Using the service from Boku, users can purchase products from merchants such as Facebook, EA, Sony, Spotify, Lookout, and Riot Games. The market for direct carrier billing on mobile devices alone is projected to be almost $6B by 2017 [11]. However, its growth outside of Europe is very slow due to many regulatory constraints.

III. MOBILE PAYMENT SECURITY

Mobile payment security is critical for all mobile payment users and service providers. The payment data must be protected when it is at rest, in transit, and in use.

A. Mobile Payment Security Services

The desired security services in a mobile payment system include authentication, access control, confidentiality, integrity, nonrepudiation, and availability [12].

Authentication includes two specific services, user authentication and transaction data origin authentication. A mobile payment system must provide ways to verify both the user identity and the origin of the transaction data. Access control ensures only the authorized person can gain access to the mobile payment system. In addition to the pin/passcode/screen lock pattern to gain access to a mobile device, a mobile payment may also require users to use fingerprints or enter pin/password to make a purchase. Confidentiality protects the transaction data from passive attacks. Integrity prevents the transaction data being modified when data is at rest, in transit, and in use. Nonrepudiation prevents either a user or a service provider from denying a transmitted message. Availability ensures a mobile payment system being accessible whenever users request them.

Many of these security services depend on cryptographic operations, such as encryption, hashing, digital signatures, etc. NFC-based mobile payment approaches, such as Apple Pay and Google Wallet, also utilize the secure element built-in on mobile devices for cryptographic processing.

B. Mobile Payment Security Mechanisms

Many security mechanisms have been adopted to ensure mobile payment security. These mechanisms are summarized as below:

- Fingerprint: Apple Pay and Samsung Pay have the option to use fingerprint to authorize a payment by simply touching a finger to the fingerprint scanner on the device.

- User name/password: Mobile payment platforms and independent mobile payment systems often use user name/password to verify user identities and authorize a purchase.
- Multi-factor authentication: Many mobile payment systems also use multi-factor authentication to authenticate users. For example, an authentication code is required when a user signs into the service using a new phone. The authentication code is then sent to the user via an email to the user's registered email account.
- SSL/TLS: SSL/TLS are widely used to protect data in the Internet. SSL/TLS can provide confidentiality, integrity, and authentication for mobile payment data when it transits in the Internet.
- Secure Element: NFC-based mobile payment systems also use the secure element on a mobile device to protect sensitive data and for cryptographic processing. For example, in Apple Pay, fingerprint and other sensitive material, such as the device's unique account number, are stored in the secure element.

IV. MOBILE PAYMENT THREATS AND REMEDIATION

Mobile payment systems are targets of cyber criminals. Many threats and attacks have been found on mobile devices. These threats and attacks could also target a mobile payment system. Compromising a mobile payment account may cause user privacy exposure and financial loss. Detailed discussions on mobile device threats and attacks could be found in [7]. In this section, we summarize the threats and attacks which have serious impacts to mobile payment security.

A. Malware

Mobile malware is one of the main threats to a mobile payment system. In 2014, Symantec has identified more than 1 million apps that are classified as malware [13]. Most malware on mobile devices is related to activities such as recording calls, instant messages, locating via GPS, forwarding call logs and other vital data. Zeus is an infamous Trojan malware designed to steal one-time passwords sent by banks to authenticate mobile transactions. It appears to be part of Trusteer's Rapport software and assures that users are securely logged into their banks' online portal. However, in the background, Zeus monitors all incoming SMS messages and forwards them to a remote malicious website. A Zeus criminal can intercept the banking credentials and drain the victim's bank accounts. ZitMo, a mobile version of Zeus, has been found in Symbian, BlackBerry and Android and could be used to steal one-time passwords sent by banks to authenticate mobile transactions.

B. SSL/TLS Vulnerabilities

Many mobile payment systems depend on SSL/TLS to protect data in the Internet. However, SSL/TLS and its implementation may also have vulnerabilities which could be leveraged by malicious users to breach the security. The Heartbleed Bug is a serious vulnerability found in the OpenSSL cryptographic library [14]. Malicious users can use the bug to steal information protected by the SSL/TLS encryption. The Heartbleed Bug was exposed in April 2014. However, the bug has been out in the wild since OpenSSL release 1.0.1 on March 14, 2012.

SSL/TLS is also vulnerable to man-in-the-middle (MITM) attack. In a SSL/TLS MITM attack, a malicious user sits transparently in the middle between a client and a SSL/TLS server. All the network traffic between the client and the server, which should be encrypted to prevent network sniffing, is exposed to the attacker in plain text. The sensitive information, such as a username/password and credit card number, is all at risk. The attacker can steal money from compromised user accounts or use the compromised accounts to make fraudulent transactions.

C. Data Leakage

Compared to the traditional payment card process, two new players are involved in the mobile payment process. In a typical scenario, for example, when a user makes a purchase using a mobile wallet at a mobile as POS, five players are involved in the process, i.e., mobile wallet service provider, mobile payment as POS service provider, merchant, acquiring bank, and issuing bank. All the players require to collect the transaction data to make a purchase.

The regulations requires all the parties in the payment process to comply with standards to secure payment data. However, incidents may still occur. In the incidents of data breaches in Target [5] and Home Depot [15], criminals gained access to the payment card information including names, mailing addresses, phone numbers, etc. Millions of customers were affected. In both breaches in Target and Home Depot, custom-built malware, Backoff, was deployed to the POS systems [16]. Mobile payment service providers can learn valuable lessons from these data breaches and prevent such incidents from occurring.

D. Mobile Payment Threats Remediation

To mitigate mobile payment risks, mobile payment users and service providers both need to take security measures to protect data security and prevent data breaches. Security measures for mobile payment users to take include, but are not limited to, use strong pin/password/screen lock pattern to protect mobile devices, upgrade mobile operating systems and apply all security patches as suggested, prevent downloading malware on mobile devices, use cautions when receiving suspected SMS messages and emails, do not connect to untrusted hotspots for Wi-Fi access, and do not proceed if receiving messages such as "can't verify the identity of the website". Mobile payment apps may require users to sign in only once and cache the password for future use. Users need to use cautions if this is the case since a pin/password/screen lock pattern is the last security mechanism to prevent unauthorized transactions.

Mobile payment service providers must take all the necessary steps to ensure mobile payment app security, protect payment data, and prevent data breaches on the backend. Many mobile payment apps use SSL/TLS to protect data security in the Internet. These mobile payment apps must validate certificates from the server. If a mobile payment system receives an invalid certificate, it should stop right away and alert users that a potential attack is likely happening.

V. Mobile Payment Security Challenges

Many security mechanisms have been adopted to ensure the security of mobile payment. However, mobile payment also faces security challenges such as malware detection, multi-factor authentication, data breach prevention, and fraud detection and protection.

A. Malware Detection

Malware is one of the main concerns of mobile payment security. Many cautions have been used to detect and prevent malware spreading. However, malware still finds a way to propagate on mobile devices [17]. Mobile malware detection is a challenging issue [18]. Existing malware detection methods include mobile forensic, static analysis, dynamic analysis, etc. However, none of them are effective to detect malware on mobile devices. Effective malware detection method is desired.

B. Multi-factor Authentication

Mobile payment systems may use multi-factor authentication to prevent user fraud when a user signs into the service using a new mobile device. Users are required to enter an authentication code which is distributed to the user using another communication channel, e.g., emails. However, mobile devices could also be lost or stolen. Malicious users may have access to the email account and thus spoof the multi-factor authentication process.

C. Data Breach Prevention

Data breach may occur. In an incident of a data breach, sensitive information such as mobile phone numbers, credit card accounts, and purchase records are exposed. User privacy is at risk. It may also cause identity theft.

D. Fraud Detection and Protection

Mobile payment provides payment services at any time from everywhere. This also allows criminals to use mobile payment services for their benefits. Criminals may use stolen payment cards or compromised mobile payment accounts to steal money or make fraudulent transactions. When a fraudulent transaction happens, it must be detected and prevented. If a user has financial loss due to fraud, a clear definition of mobile payment assurance policy may help the user build confidence to use a mobile payment system.

VI. Summary

Mobile payment has gained its popularity in many regions due to its convenience. However, it also faces many threats and security challenges. Malware is one of the main threats to a mobile payment system. Mobile payment users need to increase security awareness to prevent malware on mobile devices. SSL/TLS vulnerabilities and data breaches are two other main concerns of mobile payment security. Mobile payment also faces security challenges such as malware detection, multi-factor authentication, data breach prevention, and fraud detection and prevention. To remediate mobile payment risks, mobile payment users and service providers both need to take security measures to protect data security and prevent data breaches.

References

[1] M. Meeker, "INTERNET TRENDS 2015 – CODE CONFERENCE," 2015.

[2] Forrester, "Forrester Forecast: Mobile Payments To Reach $90B By 2017," 2013. [Online]. Available: https://www.forrester.com/Forrester+Forecast+Mobile+Payments+To+Reach+90B+By+2017/-/E-PRE4544.

[3] Intuit, "The History of Money and Payments," 2015. [Online]. Available: http://payments.intuit.com/history-of-money-and-payments/.

[4] PCI Security Standards Council, "PCI Standards and Documents." [Online]. Available: https://www.pcisecuritystandards.org/index.php.

[5] Target, "Response & resources related to Target's data breach," 2014. .

[6] HomeDepot, "The Home Depot Reports Findings in Payment Data Breach Investigation," 2014. .

[7] Y. Wang, K. Streff, and S. Raman, "Smartphone Security Challenges," *Computer (Long. Beach. Calif).*, vol. 45, no. 12, pp. 52–58, Dec. 2012.

[8] M. Blochlinger, "Mobile Payment Systems," in *Internet Economics VI - Technical Report No. IFI-2012.02*, B. Stiller, K. Farkas, F. Hecht, G. S. Machado, P. Poullie, F. Santos, C. Tsiaras, A. Vancea, and M. Waldburger, Eds. 2012, pp. 41–62.

[9] D. Yin, "Tencent's WeChat Sends 1 Billion Virtual Red Envelopes On New Year's Eve," *Forbes*, 2015. [Online]. Available: http://www.forbes.com/sites/davidyin/2015/02/19/tencents-wechat-sends-1-billion-virtual-red-envelopes-on-new-years-eve/.

[10] boku, "We Care About Payments." [Online]. Available: http://www.boku.com/about/.

[11] Boku, "The Future of Direct Carrier Billing in Europe and e-Money," 2014.

[12] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th Editio. Pearson, 2013.

[13] Symantec, "Internet Security Threat Report," 2015.

[14] Codenomicon, "The Heartbleed Bug," 2014. [Online]. Available: http://heartbleed.com/.

[15] HomeDepot, "The Home Depot Reports Findings in Payment Data Breach Investigation," 2014. [Online]. Available: https://corporate.homedepot.com/MediaCenter/Documents/Press Release.pdf.

[16] NCCIC, "Backoff: New Point of Sale Malware." Department of Homeland Security, pp. 1–10, 2014.

[17] Apple, "XcodeGhost Q&A," 2015. [Online]. Available: http://www.apple.com/cn/xcodeghost/.

[18] Y. Wang and Y. Alshboul, "Mobile Security Testing Approaches and Challenges," in *First Conference On Mobile And Secure Services*, 2015.