Open Access License Notice

A Study on Cyber Attacks and Vulnerabilities in Mobile Payment Applications

Oriel Rivers
Department of Computer Science
Norfolk State University
Norfolk, VA, USA
o.r.rivers@spartans.nsu.edu

Yen-Hung (Frank) Hu
Department of Computer Science
Norfolk State University
Norfolk, VA, USA
yhu@nsu.edu

Mary Ann Hoppa
Department of Computer Science
Norfolk State University
Norfolk, VA, USA
mahoppa@nsu.edu

***Abstract*—The end-to-end mobile purchase process depends on the decisions and actions of many stakeholders, including consumers, mobile application developers, mobile payment service providers, merchants, financial institutions like banks and credit card companies, and their respective data centers. This paper presents a detailed look at mobile payments as a sequence of transactions to better understand what is required to authenticate, authorize, verify and process them, and where security vulnerabilities lie. This analysis was accomplished by conducting in-depth research on three popular use cases – Apple Pay, Google Pay, and Samsung Pay – analyzing their respective potentials for being compromised, and suggesting opportunities where higher levels of security can be attained. While many mechanisms exist that can contribute to safeguarding mobile transactions, this analysis shows many ways known vulnerabilities and attacks still can be leveraged to exploit users' data within popular mobile payment solutions. Approaches for improving the security of mobile payment transactions are included as way ahead recommendations.**

Keywords—Mobile Payment, Apple Pay, Android Pay, Samsung Pay

I. INTRODUCTION

Mobile payments allow customers to complete purchases without physical payments like currency, checks or bank cards changing hands. Instead, transactions are completed using technologies built on point of sale (POS) terminals and compatible mobile devices, or by using mobile-to-mobile device options [1] [2] [3].

The first forms of mobile payment appeared over two decades ago. As early as 1997, Coca Cola customers could purchase a soda using Short Message Service (SMS). The cost of the transaction was charged to the customer's telephone company, who passed it on to the customer's monthly bill [4]. That same year, Exxon introduced a method of contactless mobile payment called "Speed pass." Customers could wave a small payment device – in this case, a key tag – in front of a sensor on a pump at any Exxon or Mobil gas station. Funds for purchases would be debited automatically from a payment account linked to the customer's key tag [5].

Several other innovations boosted the development of mobile payments including PayPal (funded in 1998) and Google Wallet (released in 2011). In recent years, mobile payment use has skyrocketed, despite consumer's concerns about the security of their data during these transactions. By now Apple Pay (launched in 2014), Android Pay and Samsung Pay (both launched in 2015) have been downloaded by millions of smartphone users [6] [7] [8].

Traditional physical payment methods like currency, checks and bank cards seem quaint and inconvenient compared to mobile payment technology. Individuals and companies who consider engaging with this technology may do so because of advantages such as security, speed, and clutter reduction.

- Security: The potential for security in the mobile payment process is a powerful selling point, with providers claiming there are many mechanisms in place to protect consumers' data during transactions. Because customers do not have to physically hand currency, bank cards or checks to a cashier, opportunities for financial and identity theft are minimized [9].
- Speed: Consumers and companies alike have remarked how mobile payment transactions take less time to process and complete than traditional purchase options. Less waiting time is a great marketing angle for encouraging the use of mobile payment applications [9] [10].
- Clutter reduction: Due to mobile payments, consumers have no need to carry around and keep track of physical currency, bank cards, checkbooks and paper receipts, which helps minimize the risk of financial and personally identifiable information (PII) loss and theft. To be fair, the shift to mobile payments also shifts the consumer's focus to maintaining physical control of their mobile devices which now may contain all the information needed to successfully fulfill purchase transactions [9] [11].

Of course, mobile payments are not without disadvantages. Human errors on the part of participants still may occur at many points during the transaction. Technical glitches can occur too, and may not come to light until days, weeks or even months after the original transaction. Other disadvantages include incompatibilities, battery failure and theft [9].

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

- Incompatibilities: Mobile devices and software – including operating systems and mobile payment applications – may evolve at different rates, without cross-capability and cross-platform version release validation or synchronization. Consumers who are trying to use old or low-end smartphones often discover hardware/software incompatibilities. Mobile payment providers may be silent regarding device requirements; however ultimately there are specific capabilities users' phones must have to successfully "play" [12]. Older devices simply may not work with the latest mobile payment software and associated systems.
- Battery failure: Common causes of battery failure are prolonged application use and overcharging [9]. It may seem like an obvious statement, but if a mobile device's battery is completely drained, its owner cannot use it to make a purchase until it has been recharged. Veteran mobile device users typically avoid this problem by carrying a charge stick or extra battery. Some thought-leading businesses offer quick charges for mobile users, either free or for a small fee.
- Theft: Whether targeted or random, the theft of mobile devices that contain PII including financial data is a new consumer worry. If an individual regularly engages in mobile payment activities, an attacker who steals their device may be able to hack the on-board applications and use the financial account information associated with them. If this occurs, it then befalls the victim to undertake cumbersome corrective actions, such as canceling accounts, cards and unauthorized transactions, then reestablishing new payment methods for future use.

It is clear from the ongoing expansion of mobile payment technology that innovative applications and service providers will continue to emerge and make buying and selling increasingly streamlined. Because of significant growth in mobile payment use, it is critical that individuals and companies who engage with this technology understand vulnerabilities and threats to secure operations, and what actions must be taken to mitigate them.

The hows and whys of mobile payments reveal that consumers, merchants, financial institutions, application developers and service providers are among the many who share a chain of responsibility for securing the end-to-end process, and where better practices are needed to help mitigate security risks. The remainder of this paper is organized as follows. Section 2 presents the details of mobile payment processes as a sequence of transaction stages. Section 3 explains current security implementations and concerns associated with mobile payment transactions by exploring three popular mobile payment applications – Apple Pay, Google Pay, and Samsung Pay – as interesting use cases. Section 4 summarizes vulnerabilities and cyber-attacks that threaten the security of each stage in the mobile payment process, and suggests some approaches to mitigate them. Section 5 rolls up these recommendations for improving end-to-end mobile payment security. Section 6 concludes the paper by summarizing findings and suggesting ways to build upon this work.

II. Mobile Payment Transactions

This section explains the mobile payment process as a sequence of transactions, a level of detail needed to understand what is required end-to-end to authenticate, authorize, verify and process payments. To establish a secure connection and complete a mobile payment transaction involves six stages, each of which must communicate successfully and securely with the others. In this context, the term "secure element" refers to a tamper-resistant platform.

The first four stages are briefly summarized below. Two remaining stages – the merchant's bank to the data center, and the merchant's bank to the credit card company – are beyond the scope of this paper.

- Stage 1 – Mobile User to Mobile Payment Application: This stage involves the authentication mechanism steps that users must go through before gaining access to a mobile payment application. In the first step of the mobile payment transaction, the username and password credentials are stored and processed inside the secure element. The secure element ensures the security of the user's authentication data by making sure credentials are not easily accessible during logging in. A secure element also could be involved in the background to verify identity ("you are who you say you are") [13] [14].
- Stage 2 – Mobile Payment Application to Credit Card Company: This stage covers the communication that is needed to enroll payment cards. The security mechanism relies on the presence of a secure element that is located inside the mobile device [15].The secure element is used to unlock encrypted data used in the communication process when enrolling a debit or credit card. It maintains the integrity of the user's payment information and manages the reading of device data [14].
- Stage 3 – Mobile Payment Application to Cash Register: This stage comprises the communication mechanism that is needed to initialize and process a payment. The secure element is used to process the payment transaction. To complete a secure element transaction, the mobile device first must have Near Field Communication (NFC) capabilities [16]. After verifying the mobile device is NFC-capable, the NFC controller converts to a card emulation mode that allows such technology to take over and take the place of a payment type [13]. The secure element then performs a handshake with the terminal, sends the right responses to the right queries, authenticates the stored card, and so on [13].

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

- Stage 4 – Cash Register to Data Center of the Register: This stage covers the encryption mechanisms required to complete a secure connection [17] [18] [19]. The secure element is used to communicate using a secure Internet protocol and to pass on information that will update the transaction and the inventory.

Many different mechanisms can provide safeguards during mobile transactions such as security, prevention, payment and authentication. Each mechanism is useful to establish protections against vulnerabilities known to reside within systems and networks, or those that may be discovered weeks or even months later. Such mechanisms provide a means to assist with implementing security policies [20].

III. Security Implementations and Concerns for Mobile Payments

Using the four stages of mobile payments above as an organizing framework, this section discusses multiple security implementations and concerns that exist in solutions that fulfill such transactions. This information was coalesced by studying published details of different mobile payment application life cycles.

A. Stage 1: Mobile User to Mobile Payment Application

To protect their valuable information during and after mobile purchases, users must be identified, authenticated, and authorized [21]. These terms sometimes are used interchangeably, but the concepts are different. Identification is the means whereby one user is uniquely distinguished from any other user (e.g., user id). Authentication is the process of confirming the identified user is, in fact, who they claim to be (e.g., the password provided corresponds to the user id). Authorization grants or blocks accesses to other resources based on the user's authenticated identity.

Due to the high-value data that is exchanged during mobile purchases, authentication is a major security concern. To a large extent, during the mobile user to mobile payment application stage, users determine the security or risk to their data and PII through their credential choices; however, service providers and developers already have added to or reduced risk by the methods and implementations they offer.

1) Security Implementation: The categories of authentication credentials are simple passwords, complex passwords, personal identification numbers (PINs) and biometrics.

- Simple and complex passwords are comprised of letters, words, digits and phrases [22] [23].
- PINs normally consist of a sequence of 4 to 8 digits.
- Bio-metrics describe methods based on physiological or behavioral traits of the authenticating individual [24].

This analysis focused on user to mobile application interactions that involve single-factor and multi-factor authentication mechanisms [25] [26].

- Single-factor authentication: This method requires users to authenticate using just one category of credentials. Many users prefer single-factor methods because they are simple, quick to use, and easy to remember; however, having just one protective layer puts the user's identity at risk [25].
- Multi-factor authentication: This method requires users to provide two or more categories of credentials to the authentication process, making it harder for bad actors to hack it.

Users first must identify, then authenticate their identity to their own mobile device by entering their credentials; this authorizes which mobile interfaces and applications they may access. Next users must be identified, authenticated and authorized by the mobile applications needed to complete transactions [21].

- One-stage Authentication: Users must authenticate their identity on their mobile device by entering their credentials to gain access to their mobile interfaces and applications.
- Two-stage Authentication: If the user's credentials are correct, their identity will be authenticated within the mobile application. This step is completed by providing a password, a PIN, or a bio-metric option [22] [23] [24].

2) Security Concerns: During this stage, it is important to maintain secure transactions to help minimize the possibility of users becoming cyberattack victims. Vulnerabilities may result from weak authentication and poor authorization, and may be exploited in both the one-stage and two-stage methods used to exchange user credentials. For example, weak password combinations are at risk from a wide variety of threats including rainbow-table and brute force attacks [27] [28] [29]. Physical credentials such as hardware tokens and smartcards are easily lost or stolen. Multi-factor authentication is ineffective if the user can opt out of using the additional modes. Users who are not attentive during transactions may inadvertently download malware to their mobile devices [30]. Phishing also can occur due to users' lack of cybersecurity awareness and knowledge.

B. Stage 2: Mobile Payment Application to Credit Card Company

Users are authenticated from the mobile payment application to the credit card company using the debit or credit card information enrolled into the mobile payment application. This process connects with the credit card company's server to ensure users can be authenticated when using a specific card. The security of the enrollment stage benefits from information being sent over a secure network for validation purposes, from encrypted card information, and from the protection of Secure Socket Layer (SSL) certificates. The enrollment processes of three major mobile payment applications – Apple Pay, Samsung Pay and Android Pay [31] – are detailed below as interesting use cases for further analysis:

1) Security Implementation: Apple Pay is only accessible to users with devices that use Apple's iOS operating system. Apple Pay enrollment consists of five steps:

- Step 1: The user loads their personal information and debit/credit card information into their mobile device.
- Step 2: The mobile device sends the card information to Apple's server, using SSL.
- Step 3: Apple encrypts the information with a payment network key and transfers the information to the bank.
- Step 4: The bank verifies that the information matches the payment network key (e.g., VISA, Mastercard, American Express). If the card and key match, the bank creates a token for the card. If the card type does not correspond with the correct information, the process will go back to the user.
- Step 5: A Device Account Number (DAN) is sent back as a token to Apple. Apple then sends the information back to the device and stores the token into the Apple Wallet [28].

Android Pay is only accessible to users with select Android or Google smartphones. Android Pay does not verify the user's identity; instead it assigns the user verification role to the acquiring bank. Android Pay offers three verification methods – text, email, and bank app. Android Pay involves two steps:

- Step 1: Android Pay designates the user's bank as being responsible for identifying the user.
- Step 2: Upon verifying the information with the bank, Android Pay stores the user's card number onto Google's cloud server [28].

Samsung Pay is only accessible to users having select device models with designated features such as NFC. Samsung enrollment consists of three steps:

- Step 1: The user inputs their debit card or credit card information into the application.
- Step 2: The user chooses an authentication method (e.g., SMS, Email, Bank, One Time Password) and stores their PIN and fingerprint within the application.
- Step 3: The payment card network (e.g., Visa, MasterCard, American Express) verifies the given information against the authoritative information held by the card issuer. The user's device and information also are shared with the card issuer [28].

2) Security Concerns: To minimize opportunities for information leakage during the enrollment process, mobile devices must remain secure, and enrollment applications must process users' information successfully and securely. Despite the use of secure networks, encryption and SSL certificates during this stage, transactions still may be targeted and hacked using advanced persistent threats (APT) [32]], sniffing [33], and Man-in-the-Middle (MitM) attacks [34] [35].

C. Mobile Payment Application to Cash Register

Smooth and secure communications between multiple entities – the mobile application, the POS [36] (e.g., cash register), the acquirer (e.g., bank), the payment network provider, and the token service provider – are essential during this stage of the payment process. To initiate this stage, the user must place their mobile device near a merchant cash register that uses NFC and Host Card Emulation (HCE) [37].

1) Security Implementations: Security implementations of Apple Pay, Android Pay and Samsung Pay are introduced below. Apple Pay's payment mechanism is similar to its enrollment mechanisms and consists of seven steps:

- Step 1: The user places their mobile device close to the payment terminal. The user must verify their payment method using their touch ID information or a PIN.
- Step 2: The DAN is loaded into the secure element and is sent to the acquirer (i.e., the merchant's bank).
- Step 3: Upon receiving the DAN, the acquirer decides if the information is valid by contacting the issuer's bank via the payment network. Since the information is encrypted, the acquiring bank does not know whether the numbers are actual credit card numbers or if it is the token key.
- Step 4: After verifying that the information provided is the DAN, the payment network provider routes the information to the Token Service Provider.
- Step 5: The Token Service Provider sends the real primary account number (PAN) back to the issuer.
- Step 6: The issuer authorizes or denies the transaction and passes the information on to the acquirer.
- Step 7: The acquirer returns the results to the merchant [28].

The Android Pay payment process consists of five steps:

- Step 1: The user places their mobile device near the NFC-capable POS. The information stored in the wallet is sent to the POS.
- Step 2: The merchant sends the information to the acquiring bank.
- Step 3: Upon receiving the token, the acquirer passes the information to the payment service provider. The payment network is the main communication between the acquirer and the issuer.

- Step 4: The payment network provider requests the real PAN from the token service provider and sends it to the issuer.
- Step 5: The issuer authorizes or denies the transaction. The issuer will send the notification to the acquirer who will in turn forward the notification on to the merchant [28].

The seven steps in Samsung Pay's payment process are:

- Step 1: The user places their handset near the NFC- or HCE-capable POS.
- Step 2: The user chooses a card that is stored in their mobile wallet and waits for the mobile device to generate a digital token, a transaction counter, and a secret key.
- Step 3: Upon completion, the digital token, transaction counter and secret key are sent to the acquirer.
- Step 4: The acquirer identifies the payment network type and the token.
- Step 5: The payment network retrieves the real PAN from the token service provider and then forwards the payment to the issuer for execution.
- Step 6: The issuer performs the payment and notifies the payment network provider of the success or denial of the transaction.
- Step 7: In return, the merchant is notified of the results [28].

2) Security Concerns: During the mobile payment application to cash register stage, establishing a secure connection is paramount. NFC, HCE and Hypertext Transfer Protocol Secure (HTTPS) deliver security through proximity and encryption, while also providing convenience and versatility. However, even these measures do not eliminate all risk. Several known vulnerabilities during this stage are shoulder surfing [38], device misplacement or theft, and session hijacking. POS cash registers may be shipped to the merchant company with pre-existing vulnerabilities due to outdated software or undiscovered flaws or malware. In other cases, cyber-attacks and vulnerabilities initially attributed to POS machines ultimately have been traced to a lack of security structure and usage [36] [37].

D. Cash Register to Data Center

1) Security Implementations: The process between a POS and its data center is a very important stage that is needed throughout the communication process. Security between the POS and the data center is dependent upon its connecting devices and their end-to-end encryption methods. Said another way, communication between these devices must remain secure to protect the transmitted data that is received from the customer [17].

Encryption works by rendering transmitted information incomprehensible to anyone other than the intended recipient. It is important to have encryption mechanisms in place that protect users' identity and their credit card information from eavesdropping and leakage [19]. Communication between the cash register and its data center uses HTTPS to maintain the integrity and availability of resources. Apple Pay uses tokenization as a form of encryption. Android Pay uses SSL encryption, and Samsung Pay uses a one-time code as additional encryption [39].

Two standard encryption mechanisms are used within mobile payment applications to prevent unwanted information leakage and to harden the transmission against brute-force and MitM attacks: Triple Data Encryption Standard (3DES) and Point-to-Point Encryption (P2PE). 3DES involves encrypting the information from one end, while simultaneously decrypting it from the other end [18]. P2PE encrypts the data before it reaches the payment terminal, and decrypts the data after it has reached the data center [40].

2) Security Concerns: Secure communication between the POS and its data center is important to the user as well as the merchant. The merchant's cash register devices communicate with the data center servers during the payment transaction phase. The cash register communicates with the backend data center to ensure a payment has been processed and handled appropriately. These data transfers are vulnerable to cyber-attacks. Several vulnerabilities are known to be exploitable within Domain Name System (DNS) applications as part of distributed denial of service (DDoS) attacks [41] [42]. Additional threats include zero-day attacks and session hijacking [43] [44].

IV. Approaches to Improving Mobile Payment Security

This section summarizes vulnerabilities and cyber-attacks that threaten security at each stage in the mobile payment process, and some approaches to mitigate them.

A. Stage 1: Mobile User to Mobile Payment Application

Mobile users are at risk from brute force attacks, unauthorized access, and malware during the mobile user to mobile payment application stage. Table I in the Appendix lists vulnerabilities that enable such attacks, and some ways to detect and prevent them [27] [28] [30] [45].

B. State 2: Mobile Payment Application to Credit Card Company

The mobile payment application to credit card company stage is vulnerable to intruders trying to intercept valuable PII. APTs may lurk undetected on a system or network for a long period of time, waiting for an opportunity to steal financial or personal data in transit. Intruders also can sniff network packets, or conduct MitM attacks to capture credit or debit card information any time after the user scans their mobile device until the purchase is completed [32]. Table II in the Appendix lists vulnerabilities that enable attacks

during this stage, ways to detect them and some preventative measures.

C. Stage 3: Mobile Payment Application to Cash Register

Mobile payment users should be aware of their surroundings when conducting payment transactions. Although shoulder surfing is normally thought of as a close-proximity social engineering exploit, it also can be completed by a distant bad actor using simple equipment such as binoculars [46], a cheap web camera or even a drone. During this stage, hackers may attempt – via unauthorized access – to make a purchase using a lost or stolen mobile device [28]. MitM attacks also can put a user's identity in harm's way by intercepting valuable information while it is being exchanged. [35]. As a basis for providing better security between the mobile payment application and the POS, relevant vulnerabilities, attacks, detections and preventions are summarized in Table III in the Appendix.

D. Cash Register to Data Center of the Register

When disruption and delays are attack objectives, DoS can be effective during the fourth stage of processing by targeting the data center's Internet connection [41]. Zero-day attacks are another way to negatively affect computers on a network. In this case they could be aimed at a POS operating system to exfiltrate users' PII, or to erase backed-up data [43] as part of a long-planned ransom scheme. Cross-site scripting (XSS) also could be used strategically to inject malicious code into a web application involved in the transaction [44]. Table IV in the Appendix summarizes these possibilities along with some detection and prevention measures.

V. Recommendations

This research serves as a baseline to better understand vulnerabilities and attacks that threaten the security of mobile payment transactions.

Secure mobile payment processes rely on many stakeholders each contributing secured functionality and good cybersecurity practices.

A. Users

Users should:

- Create strong and complex passwords.
- Use biometric authentication options whenever available.
- Be aware of their surroundings and safeguard their personal data when completing purchases.
- Not jailbreak their mobile devices.
- Enable remote lock and wipe on their mobile devices.
- Only download trusted applications.

B. Mobile Device Companies

Mobile device companies should offer remote device lock and remote wipe options on their products.

C. Mobile Application Developers

Mobile application developers should subject their products to rigorous automated and manual security-facing testing, using the latest "left-shift" practices.

D. Merchants

Merchants should ensure that:

- Users' PII is encrypted before transmitting it over the internet.
- Their virus and malware software is up to date.
- All incoming and outgoing traffic is monitored.

E. Bank

Acquiring and issuing banks should ensure that the correct information is being transferred and sent across networks.

F. Data Center

Data center computers should host the minimum essential authorized software needed to support services.

G. Protocol

HTTPS should be used instead of HTTP to the maximum extent possible throughout mobile payment processes.

VI. Conclusions and Future Work

The security implementations and concerns explored through the processes of major mobile device and service providers like Apple, Android and Samsung confirm that today's mobile payment options are not perfectly secure, despite some mechanisms already in place to protect consumers' data. The detailed analysis presented in this paper highlights how intentional actions like APTs and other classic cyber-attacks, coupled with oversights like weak authentication methods, outdated software, unencrypted data and unsecured networks/protocols, still are leaving mobile payment transactions vulnerable to compromise and exploitations.

The successful implementation of measures that hamper intruders trying to exploit financial transactions depends on many individuals involved in the end-to-end payment process, including consumers, mobile application developers, mobile payment service providers, merchants, financial institutions like banks and credit card companies, and their respective data centers. The vulnerability analysis and mitigation recommendations presented in this paper focused on the first four stages involved in mobile payment transactions; the last two stages – the merchant's bank to the data center, and the merchant's bank to the credit card company – remain for future work. A similar approach can be taken to discuss the key technologies and methods involved during their respective transaction steps, the kinds of exploits that may compromise them given known vulnerabilities, and some ways to prevent or avoid risk as part of a holistic, multi-layer security approach.

Demonstration videos and guidebooks can be useful resources for increasing understanding of mobile payment functions and for building cybersecurity risk awareness. Beyond simply sharing how-to steps for downloading and using their applications, service providers like Apple, Google and Samsung bear some accountability to their customers: to explain the security limitations of the underlying mechanisms they are using to support mobile financial transactions; and to admit to risks these choices may intentionally or unintentionally introduce at each step in every transaction stage. Service providers and other stakeholders must act as cooperative security stewards to help minimize the cyberattack surfaces in end-to-end mobile payment solutions.

REFERENCES

[1] M. Pinola, "How to Pay with Your Phone or Tablet", https://www.lifewire.com/mobile-payments-4103869

[2] J. Rampton, "The evolution of the mobile payment," Crunch Network, https://techcrunch.com/2016/06/17/ the-evolution-of-the-mobile-payment/

[3] F. Hayashi, "Mobile Payments: What's in It for Consumer," Federal Reserve Bank of Kansas City, pp. 35-66, 2012.

[4] F. Martins, "The History of the Mobile Payment Experience #INFOGRAPHIC," http://winthecustomer.com/ technology-changing-the-mobile-payment-customer-experience/

[5] "History of Mobile & Contactless Payments Systems," http://nearfieldcommunication.org/payment-systems.html

[6] V. Rajaraman, Essentials of e-Commerce Technology, Bangalore, 2010.

[7] S. Congdon, "What's in Your Wallet? Addressing the Regulatory Grey Area Surrounding Mobile Payments," Journal of Law, Technology and the Internet, vol. 7, pp. 95-115, 2016.

[8] "Mobile payments will be the standard by 2020," Visa,https://usa.visa.com/visa-everywhere/innovation/ mobile-payment-technology-the-new-standard.html

[9] Y. Kumari, "7 Pros and Cons of Mobile Payments You Must Know," TechGYD, http://www.techgyd.com/ 7-pros-cons-mobile-payments-must-know/17057/

[10] "Consumer expect speed, convenience when mobile shopping," https://www.mobilepaymentstoday.com/news/ consumers-expect-speed-convenience-when-mobile-shopping/

[11] J. Miller, "Why You Should Invest in Mobile Payment Technologies," https://centricconsulting.com/why-invest-in-mobile-payments digital/

[12] "Compatibility is the key for new mobileapps," https://tender-retail.acceo.com/blog/ compatibility-is-the-key-for-new-mobile-payment-apps/

[13] G. Marwaha, "Mobile Payments: What is a Secure Element," http://www.gmarwaha.com/blog/2014/09/01/ mobile-payments-what-is-a-secure-element/

[14] "What is a Secure Element," https://www.justaskgemalto.com/us/what-is-a-secure-element/

[15] "Security of Proximity Mobile Payments," Smart Card Alliance, Princeton Junction, 2009.

[16] "NFC Guide: All You Need to Know About Near Field Communication," Square, https://squareup.com/guides/nfc

[17] L. Zaichkowsky, Point of Sale System Architecture and Security, Access Data.

[18] J. Callas, "Triple DES: How strong is the data encryptionstandard?" http://searchsecurity.techtarget.com/tip/ Expert-advice-Encryption-101-Triple-DES-explained

[19] "Encryption Basics: How It Works & Why You Need It," UpWork, https://www.upwork.com/hiring/development/ introduction-to-encryption-data-security/

[20] M. Bishop, Computer Security, Boston: Pearson Education, 2003.

[21] R. Meyer, "Secure Authentication of the Internet," San Institute, 2007.

[22] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," IEEE, vol. 91, no. 12, pp. 2019-2040, 2019-2040.

[23] Abie, Habtamu, Different Ways to Authenticate Users with the Pros and Cons of each Method, Norwegian: Norsk Regnesentral, 2006.

[24] A. Ross and A. Jain, "Human Recognition Using Bio-metrics: An Overview," https://pdfs.semanticscholar.org/427f/26b2a4410babbbf039abf5de2a9e8e6f625b.pdf

[25] M. Rouse, "Single Factor Authentication," http://searchsecurity.techtarget.com/definition/one-factor-authentication

[26] M. Rouse, "Two-Factor Authentication," http://searchsecurity.techtarget. com/definition/two-factor-authentication

[27] B. Sullivan, "Preventing a Brute Force or Dictionary Attack: How to Keep the Brutes Away from Your Loot," Addison-Wesley, 2007.

[28] ENISA, "Security of Mobile Payments and Digital Wallets," ENISA, Heraklion, 2016.

[29] A. O'Donnell, "Rainbow Tables: Your Password's Worst Nightmare," https://www.lifewire.com/rainbow-tables-your-passwords-worst-nightmare-2487288

[30] T. Chen and C. Peikari, "Malicious Software in Mobile Devices".

[31] P. Viswanathan, "Most Popular Mobile Payment Apps," Lifewire, https://www.lifewire.com/most-popular-mobile-payment-apps-2373179

[32] S. King, "APT Advanced Persistent Threat," https://www.netswitch.net/ apt-advanced-persistent-threat-what-you-need-to-know/

[33] M. Chapple, "How to prevent network sniffing and eavesdropping," http://searchsecurity.techtarget.com/answer/ How-to-prevent-network-sniffing-and-eavesdropping

[34] F. Callegati, W. Cerroni and M. Ramilli, "Man-in-the-middle attack to the HTTPS protocol," 2009.

[35] R. Publico, "What is a Man-in-the-Middle Attack and How Can You Prevent It?" https://www.globalsign.com/en/blog/ what-is-a-man-in-the-middle-attack/

[36] W. Whitteker, "Point of Sale (POS) Systems and Security," A SANS Whitepaper, 2014.

[37] Host Card Emulation (HCE), Smart Card Alliance, https://www.securetechalliance.org/downloads/HCE Webinar FINAL 061815.pdf

[38] M. Rouse, "Shoulder Surfing," http://searchsecurity.techtarget.com/definition/shoulder-surfing

[39] J. Rampton, "Your Security Concerns About Using Mobile Payment Are Valid," Entrepreneur, https://www.entrepreneur.com/article/282722

[40] "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," Smart Card Alliance, Princeton Junction.

[41] M. Qadir, "4 Popular DNS Attacks and Ways to Prevent Them," https://www.purevpn.com/blog/dns-attacks-and-prevention/

[42] "3 Common DNS Attacks and How to Fight Them," Calyptix, https://www.calyptix.com/top-threats/ 3-common-dns-attacks-and-how-to-fight-them/

[43] D. Hammarberg, "The Best Defense Against Zero-day Exploits for Various-sized Organizations," GIAC (GSEC) Gold Certification SANS Institute, pp. 1-20, 2014.

[44] M. Cobb, "Cross-site scripting explained: How to prevent XSS attacks," http://www.computerweekly.com/tip/ Cross-site-scripting-explained-How-to-prevent-XSS-attacks

[45] M. Rouse, "Dictionary Attack," http://searchsecurity.techtarget.com/definition/dictionary-attack

[46] M. Divya and A. Janani, "Defending Shoulder Surfing Attacks in Secure Transactions using Session Key Methods," International Journal of Science, Engineering and Technology Research, vol. 4, no. 2, p. 6, 201

APPENDIX

TABLE I. VULNERABILITY, ATTACK, DETECTION AND PREVENTION BETWEEN MOBILE USER AND MOBILE PAYMENT APPLICATION

Vulnerability	Attack	Detection	Prevention
Weak credentials	Brute Force/Rainbow Attack	Excessive number of failed authentication attempts	• Rate-limit lockout • Require long strong passwords • Implement page response delay
Mobile device lacks remote lock/wipe	Unauthorized Access	Mobile device is lost, stolen or otherwise not under the owner's physical control	• Mobile device owner should enable remote lock so device can be rendered inoperable ("bricking") • Mobile device owner should enable remote • wipe so all contents can be erased if lost/stolen
Corrupted application	Malware/Spyware	OS or application freezes, noticeably slows down or behaves erratically	Use anti-malware software (*e.g.*, McAfee, Norton) to detect/quarantine/remove spyware, Trojans, and viruses

TABLE II. VULNERABILITY, ATTACK, DETECTION AND PREVENTION BETWEEN MOBILE PAYMENT APPLICATION AND CREDIT CARD COMPANY

Vulnerability	Attack	Detection	Prevention
Networks that can be surreptitiously penetrated from within or without	APT	Anomalous network traffic or behavior	• Implement antivirus software and firewalls that focus on APT scanning • Monitor traffic ingress/egress • Locate/block detected APTs; sanitize compromised devices • Upgrade perimeter and network-based security • Focus protection strategies on malicious content
Weak authentications, unsecured protocol, unencrypted information transfers that occur within attacker reception range	MitM	Mobile application is unexpectedly re-routed to another website	• Ensure mobile application is directing to an HTTPS web address • Intrusion/tamper detection software
Unencrypted information transfers over unsecured connections	Sniffing	Alarm from monitoring software	• Use HTTPS instead of HTTP to the maximum extent possible • Use SSL to encrypt personal information transmissions • Encrypt information transfers • Network scanning and monitoring

TABLE III. VULNERABILITY, ATTACK, DETECTION AND PREVENTION BETWEEN MOBILE PAYMENT APPLICATION AND CASH REGISTER

Vulnerability	Attack	Detection	Prevention
Careless body positioning while entering PII	Shoulder Surfing	• Strangers attempting to stand too close during financial transactions • Unexpected presence of • vision-enhancement devices	• Users should use their body, hand or another opaque item • to shield the POS device/keypad and any other physical elements involved (e.g., fingers, screens) from external viewing [46] • Users should use complex passwords, biometrics and non-obvious keystroke patterns
Device misplacement or theft	Unauthorized Access	Remote software can detect if someone has used the missing device	• Users should maintain positive physical control of their devices • Users should use complex passwords, biometrics
Session Hijacking	MitM	• Unusual amount of application hanging • Alarm from packet sniffer or • Intrusion Detection Software	Users should not allow pre-filled forms, saved credentials, or tracking online activity

TABLE IV. VULNERABILITY, ATTACK, DETECTION AND PREVENTIO N BETWEEN CASH REGISTER AND DATA CENTER OF THE REGISTER

Vulnerability	Attack	Detection	Prevention
Open/poorly configured DNS resolvers exposed to the Internet	DNS Amplification for DDoS	• Persistent traffic volume disparity between requests and responses • Network traffic overflow	• Forbid the installation of • non-essential/unauthorized/pirated software on data center computers • Scan hard drives regularly • Ensure all security patches are kept up-to-date • Install/monitor reliable firewalls • Increase network capacity; use offsite protective services to handle overflow traffic • Detect/eliminate spoofed IP addresses
Undiscovered software/hardware vulnerabilities	Zero-Day Attack	• Breach effects • Code irregularities • May go undetected	• Forbid the installation of • non-essential/unauthorized/pirated software on data center computers • Install/monitor a reliable firewall • Update OS and other software as often as needed • Identify exploits in real time; quarantine immediately to control damage
Inadequately tested websites/web applications/client-side scripts and forms	Cross Site Scripting (XSS)	• Evidence of stolen accounts, credentials, sessions • Malware delivery detected • Keylogging activity	• Automated XSS and/or rigorous [manual] testing guided by XSS cheat sheets to detect/remove client-side security-related design and coding flaws • Use HTTPS instead of HTTP to the maximum extent possible • Use protected wireless connections • Require (re-)authentication before certain services • Avoid exposing the backend computer directly to the Internet