A Report on cybersecurity issues in smartphone payments

FIN 545-WS

By:
Sri Dhanush Reddy Kondapalli
CWID: 10476150

Abstract

The report focuses on the cybersecurity risks of smartphones and digital payments. It focuses on a problem and a research structure of the study. The report includes the various potential cybersecurity threats on smartphones and digital payments. It also includes the possible outcomes and best practices to avoid these potential cyber risks. Smartphones are an integral part of our lives and payments through smartphone shave emerged as the most popular in recent years. The report focuses on the risks in the utilization of the payments through smartphones.

Contents

1. Introduction

With uses in industry, finance, administration, defence, music, education, and medicine, cell phones have evolved into an essential part of our everyday lives. Various wireless applications enable users to keep their confidential info on portable devices and carry out a variety of crucial functions, and the number of mobile phones is growing every year ([1]Bubukayr & Almaiah, 2021). Customers are more likely to attempt and download more recent or popular apps on their cell phones because of the convenience of use and intriguing aspects of these applications, while considering plenty about their security, possibly due to ignorance. These actions make them accessible victims for cybercriminals ([1]Bubukayr & Almaiah, 2021).

Approximately 230 billion applications were installed onto mobile terminals in 2021. With the aid of their cell phones or other handheld platforms like iPads and Android smartphones, many individuals use internet providers ([2]Cruz & Simoes, 2019). Apps for mobile wallets and finance are getting increasingly popular. Nowadays, almost all banks offer online payments or mobile wallet services that let their clients carry out a variety of tasks from every position using electronic services or e-wallet applications downloaded to their smartphones, including verifying individual financial accounts, funds transfers, bill payments, food and grocery money transfers, financial records, internet banking, and travel booking ([1]Bubukayr & Almaiah, 2021).

The goal of attacks is to keep the internet safe from cyber fraud. Cybersecurity refers to all things, including equipment, programming, and data, that are associated with the Internet or a system. Payment systems are the use of a cell phone or even another mobile device to manage a savings account and carry out some internet banking functions like paying bills, transferring money, paying charges or taxes, cash withdrawals from those other internet accounts, and monitoring financial accounts ([3]Taha & Dahabiyeh, 2020). Account holders benefit greatly from its ease, but it is susceptible to a range of assaults that can be launched against smartphone financial institutions. However, as mobile technology has advanced, mobile payment programs have increased in popularity, enabling users to easily keep a record of all of the economic transactions on their smartphones. To put it in another way, digital payment is a software program that enables someone to transfer or send money that used a smartphone application. The advantages of virtualized technologies, private data storage, secure data transfer, and frictionless payments make digital payment apps popular ([3]Taha & Dahabiyeh, 2020).

The safety and confidentiality of a user's data are critically impacted by mobile browser safety. To distinguish and get a competitive edge, software development businesses seem to be more enthusiastic about including as many capabilities as possible in their apps. However, this enthusiasm comes at the expense of major gadgets and privacy protection compromises ([4]Al-Turjman & Salama, 2021). Rapid software changes enhanced features, and increased usability usually have come at the cost of security technologies. Since programmers continue to generate incredibly exposed code, it has grown faster to compromise a smartphone application's privacy as amended to reflect, making it simpler to build and deploy apps as well. It is important to spread knowledge about the risks to smartphone app privacy and how to counter them ([3]Taha & Dahabiyeh, 2020).

1.1 Problem Statement

The increase in digital payment over the few years has increased security threats. Payment apps are more prone to these security threats and attacks. These cyber security risks lead to various adverse consequences such as theft, loss of integrity, leakage of confidential financial information and others. The attacks include mobile malware and viruses, phishing attack, keyloggers, trojan and fraud apps/updates and others. The causative factors of these attacks include weak and vulnerable passwords, usage of third-party apps, not enough knowledge about cyber security, clicking on harmful links and sharing confidential information such as One-time passwords with others ([4]AI-Turjman & Salama, 2021).

1.2 Research

The structure of the report includes the topic of security issues in mobile phone payment. The report consists of the introduction of security issues. It includes a problem system regarding the complication of digital payments and cyber security risks related to it. It also includes a discussion and analysis that consists of the cyber security risks in the payments app and protection techniques with some best practices that can be undertaken by smartphone users to avoid cyber-attacks and to complete smooth payments.

2. Discussion and analysis

2.1 **Cyber security risks in smartphone payments**

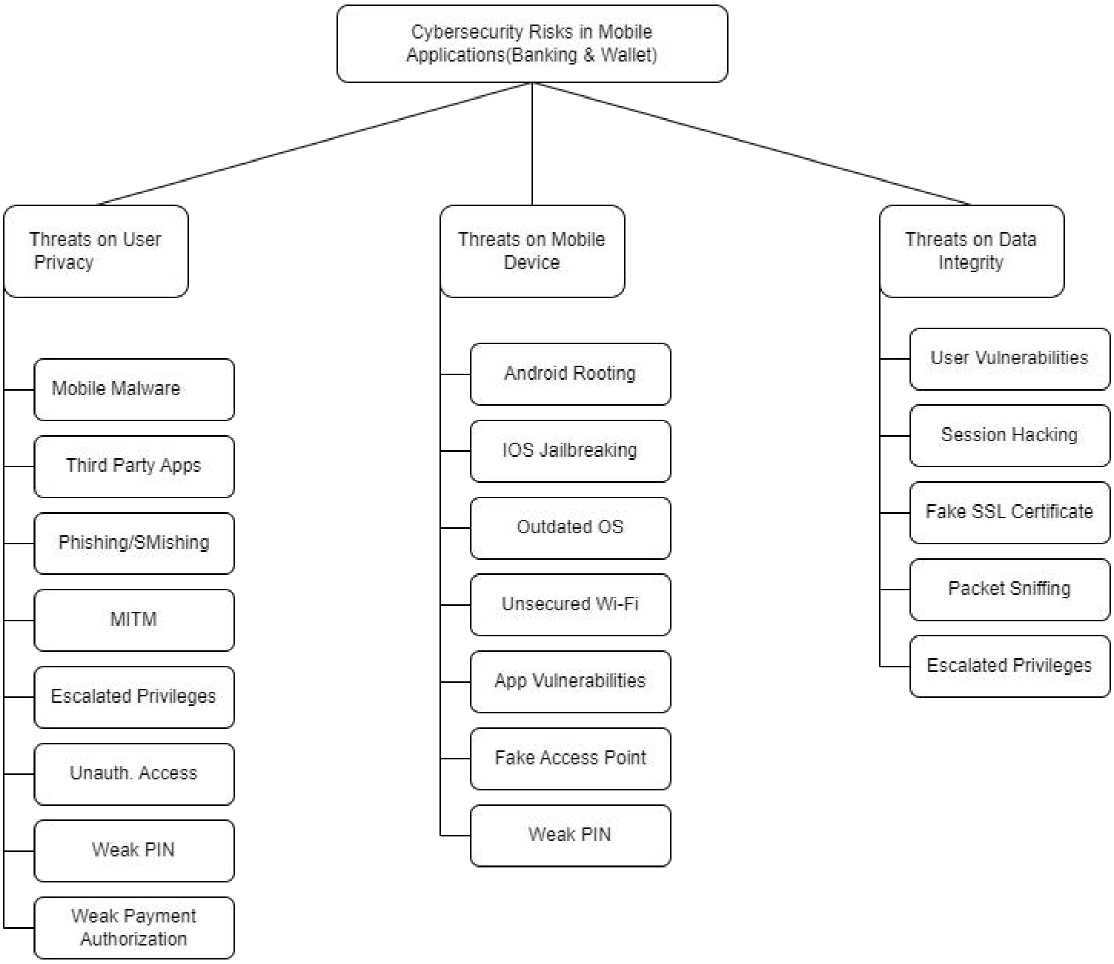

Figure 1. Cyber security risks in mobile applications

Source: ([2]Cruz & Simoes, 2019)

1. Threats to user privacy

Mobile Malware

Among the most frequent cyber defence assaults that violate the security of individuals who use smartphones and online payments are the mobile virus. The goal of cybercriminals is to violate people's security. These are seen as distinct and peculiar hazards to users of mobile devices. As more individuals use their cell phones to carry out important jobs, the potential threat will only increase. The majority of smartphone customers are ignorant of the different techniques used by MMs (assailants and raiders) to access their cell phones and other handheld platforms against their consent or permission ([5]Shah & Agarwal, 2020).

Third-party apps

The majority of cyberattacks target third-party programs. Exercise precaution when using third-party applications as they are not fully stable. Many of these apps were made by malevolent scammers and hackers, and they are typically offered for free on different mobile app shops like the iTunes and Play Store. Third-party applications serve as a conduit via which cybercriminals can access consumers' software products ([4]Al-Turjman & Salama, 2021).

Phishing attacks

Inside this attack, real people are impersonated to gain usernames and passwords or private data. Ct does this by delivering targeted recipients' emails with information about job applications and jackpot announcements. SMS Hacking is the abbreviation for SMishing. An enticing SMS is delivered to a relying party to persuade him to download and deploy spyware, such as a Trojan Horse or virus ([5]Shah & Agarwal, 2020).

Man in the middle attacks

The online hacker inserts themselves in the middle of the communication between the targets of the attempt, assumes the identities of both, and gains access to the crucial sensitive information that these parties are exchanging ([5]Shah & Agarwal, 2020).

Escalated privileges

Accessing different areas of a smartphone via a variety of techniques, among which ts barracking or unlocking the bootloader of the device.

Unauthorized Access

Unauthorized access can be obtained in several methods, including impersonating. Unauthorized entry into banking apps by a cybersecurity offender results in data spillage or theft ([6]Khera, 2018).

Weak PIN

A password or PIN is typically used to secure or unlocked a smartphone, helping to secure it from unauthorised users. One of the contributing reasons to cybersecurity incidents that allow an attacker simple entrance is a poor PIN ([6]Khera, 2018).

Weak authorization of payments

Before doing any activities, a transactional passphrase or PIN is usually needed; this is done to authorize payments. Transactions with insufficient authorisation could provide third parties access to the communications app ([5]Shah & Agarwal, 2020).

2. Threats on mobile devices

Android Rooting

It enables root privileges to the Android Software code. It let you alter a cellular phone's programming code or install additional applications that the maker normally forbids ([7]Ganesh et al., 2022).

iOS jailbreaking

It follows the same procedure as cloning an Android operating system. Customers of apple mobile phones utilize this to download free software ([6]Khera, 2018).

Outdated Operating systems

Android operating systems must be updated reguraly to prevent vulnerabilities, as attackers or fraudsters could use these openings to target financial or e-wallet software ([6]Khera, 2018).

Unsecured Wi-Fi

Unprotected Wi-Fi is a term used to describe a community or open Wi-Fi connection, like those found in coffeehouses, shopping areas, and certain other crowded places where a pass code is not required to log in. These are additionally referred to as “unsecured Wi-Fi connections” due to the risk of criminals gaining access to users’ sensitive data ([7]Ganesh et al., 2022).

App Vulnerability

Certain applications are more susceptible to assaults and much less protected. Programs from trusted stores like the Google Play Store and the Apple App Store ought to be used. Many online payment applications are susceptible to software reversing. Malicious hackers can examine software to acquire bank details, transaction records, as well as other private information ([7]Ganesh et al., 2022).

Fake Access Point

Even without the administrator of the channel's permission, a false network adapter has been installed on the system. If a criminal controls the default gateway, they can capture data travelling via the system ([7]Ganesh et al., 2022).

3. Threats on payment

Security Vulnerability of users

The usage of an inadequate or no password, the storing of confidential documents, and a lack of adequate understanding and skills about security precautions are some examples of user weaknesses that cybercriminals may exploit to infiltrate networks and obtain confidential and personal information ([8]Williams et al., 2020).

Session hijacking

Ethical hacking is yet another kind of network assault that occurs when the perpetrator modifies the conversation between two or more authenticated persons in an attempt to gain access to resources or material used by authorized people. Man-in-the-middle (MITM) assaults and TCP account hijacking are two examples ([8]Williams et al., 2020).

Fake SSL certificate

It is crucial to protect the I ines of interaction between both the user and the banking institutions. Proper Encrypted File technology is used to carry out this operation (SSL). The main factor contributing to this assault with the use of illegitimate, unlicensed, or hacked programmes. Circumventing the Secure sockets layer, the assailant will try to initiate a conversation in an illegal way ([8]Williams et al., 2020).

Packet sniffing

The observation and fault identification for particle data flowing through a network is called packet sniffing. Although criminals may use comparable technologies for illicit operations,system administrators utilise packet sniffing tools to track and analyze traffic on the network ([9]Tervoort et al., 2020).

Scams

One of the most typical DFS frauds involves transaction cancellation demands and advance fee frauds. A user is fooled into submitting money in a money-laundering scam to play bogus lotteries or obtain a fake prize or present. An improper payment which has been deposited into a user's account is asked to be reversed in a reversing demand ([9]Tervoort et al., 2020).

Social engineering attack

A scammer uses social networking to deceive a client or a company's worker into disclosing personal data or granting access to company networks and data. Phishing is a technique used by criminals to call, email, or contact their victims to obtain identifying infom1ation data including credit card details, PINs, and user usemames and passwords. The user's identities can then be stolen, their assets can be taken over, and client monies can be accessed ([9]Tervoort et al., 2020).

2.2 Protection techniques and practices

Users who use smartphone programs like financial and payment apps can benefit from a variety of benefits. Nevertheless, a significant obstacle to the mass acceptance of these apps is the confidentiality of critical information. People need to be aware of such vulnerabilities, possible hazards, and actions they can take to minimize these since using mobile applications comes with a variety of privacy risks ([2]Cruz & Simoes, 20 I 9). The security breaches regarding mobile devices have not yet been systematically discussed in the literature. Some significant security issues in this study were presented to highlight by this research. In the part that follows, several user security methods and practice guidelines are also recommended ([10]Peng et al., 2018).

Build and maintain a secure network

To create and keep up a reliable connection, safeguard credit card information, and configure and operate a firewall. An institution's originally issued security measures are used to detect and classify inbound and outbound traffic through a firewall, and information security equipment. A firewall is a barricade that stands between such a proprietary local network and open internet even at the most basic level. The basic function of a firewall is to let safe traffic in while blocking harmful traffic ([10]Peng et al., 2018).

Avoiding distributor settings for computer credentials as wells as other encryption keys is part of setting up and maintaining a private connection on the smartphone for the payment method. The supplier may supply security holes, thus they shouldn't be relied upon to complete the payment. Vendors of smartphones keep developing security features the can keep thieves or hackers from breaking into your digital payment ([10]Peng et al., 2018). To access the phone using multiple authentications, you need two different identification documents. Typically, a PIN is used in conjunction with a fingerprint or face identification system. When a completely random transaction certificate is generated instead of critical credit card info, a smart contract assures that the credit information is never viewed by retailers ([11]Algarni et al., 2021).

Protect cardholder Data and use VPN

Securing the software products where cardholders' data is stored and encryption of the transfer of such data over public, open wifi. One of the safest ways to prevent espionage is to employ a VPN or private network. With the help of a VPN, the gadget and the internet surfing are encrypted to the point where any data sent across them cannot be decode without the need for a special key ([11]Algarni et al., 2021).

Maintain a vulnerability management program

The client would be required to control the susceptibility of their cellphones and the payments software to keep a vulnerability management programme. Utilizing and maintaining anti-virus technology on all computers frequently harmed by spyware A type of application called anti virus is used to stop, scan for, find, and remove infections from a device ([11]Algarni et al., 2021). Several anti virus programmes are fully automated in the backdrop after installation to offer adequate defence from malware and viruses. Sophisticated anti-virus systems can provide extra security features like customized routers and site monitoring in addition to supporting safeguarding both data and equipment from spyware like viruses, Keygens, and malware. It aids in keeping the cell device's infrastructure and applications secure ([12]Buldakova, 20 I 9).

Implement strong access control

Utilizing password protection for both mobile apps. One method of putting phrase management into practice is by limiting who has entry to the cardholders and card information. The procedure also entails unauthorized users being prevented from entering by using multiple identifications, and client payment's private data being compromised. A person's identities and the assets they can view are both adequately insulated with the implementation of 2FA ([12]Buldakova, 2019).

When compared to identification techniques that rely on solitary identification (SFA), where the client supplies only one element, usually a passcode or fingerprint, multiple verifications offers a better degree of security. To employ multiple verifications, a user must supply a passcode as the very first factor and another, distinct element, typically a safety chip or a biometrics factor like a fingerprint or face scanning ([12]Buldakova, 2019). By reducing the ability for assailants to obtain a user's gadgets or account information, multiple verifications add a layer of protection to the verification process. This happens because, regardless of whether the suspect's account is compromised, a login alone will not be sufficient to throw the verification check ([13]Hartmann & Carmenate, 2021).

2.3 Some other best practices

- To safeguard themselves against multiple security risks, smartphone nodes must refrain from jail breaking or bypassing their smartphones. Such tapping methods get over safety and permissions restrictions, giving module interfaces to any confidential information on the phone.
- Only reputable and safe sites, such as original bank webpages, should be used to download applications for mobile banking ([13]Hartmann & Carmenate, 2021).
- If one has to utilize a mobile banking app, stay away from free WiFi.
- People should refrain from relying on just about any hyperlinks received through Text from dubious addresses, in addition to accepting SMS/MMS communications from unknown sources.
- Upgrade the application for mobile banking whenever the latest iteration becomes accessible.
- Update the mobile Operating system as quickly as is practical after the patch is issued. The emphasis lies that should not be overlooked is an obsolete OS ([13]Hartmann & Carmenate, 202 l).
- Particularly when the message or caller requests confidential info like account information, a Password, or other confidential material, do not open the message or respond to the call. Such letters or emails are very likely to involve spoofing or Spear phishing.
- Sensitive material should indeed be kept in safe facilities with good protection, and also to prevent unauthorized access, a powerful passcode must be utilized ([2]Cruz & Simoes, 2019).

Conclusion

The report focuses on cybersecurity issues in smartphone payment. People depend on android smartphones to preserve everywhere from texts, personal documents, contact information, and online network account names to online payments, internet ordering, and general merchandise money transfers with the help of specialized smartphone platforms. Smartphones are quickly getting increasingly indispensable components of everybody's life. evertheless, the rise in mobile phone users also brings with it an escalation of security risks. These technologies have attracted a large number of immoral malicious hackers who are ready to utilize them for their benefit, including stealing, devastation, duplication, and a range of many other things. This study looks at numerous cyber threats to smartphone devices including wallets and financial apps.

The report includes the cybersecurity risks in the smartphone payment application such as phishing attacks, SMS and email frauds, weak and poor passwords and PJN, fake access points, the vulnerability of the apps, scams, social engineering attacks, packet sniffing, fake SSL certification, session hijacking, the vulnerability of the users, android and iOS rooting, outdated operating systems, unauthorized access into the phone and escalated privileges. These cybersecurity risks are based on the threats to the privacy of the users, mobile devices and security of the payments. The report also undertakes the best protection techniques for smartphones and financial payments. The outcome of the study is to analyse and evaluate the cybersecuriry risks in mobile phones and digital payments. The report analyses possible risks and security issues of mobile phone payments and provides the best possible solutions and techniques to avoid these attacks and secure digital payments.

References

[1] M. A. S. Bubukayr and M. A. Almaiah, "Cybersecurity Concerns in Smart-phones and applications: A survey," 2021 International Conference on Information Technology (ICIT), 2021, pp. 725-731, doi: 10.1109/ICIT52682.2021.9491691.

[2] European Conference on Cyber Warfare and Security Tiago Cruz Paulo Simoes and Universidade de Coimbra. 2019. Proceedings of the 18th European Conference on Cyber Warfare and Security : Eccws 2019 : Hosted by University of Coimbra Portugal 4-5 July 2019. Reading UK: Academic Conferences and Publishing International Limited.

[3] Taha, N., Dahabiyeh, L. College students information security awareness: a comparison between smartphones and computers. Educ Inf Technol 26, 1721–1736 (2021). https://doi.org/10.1007/s10639-020-10330-0

[4] Al-Turjman, F., and Salama, R. (2021, January 1). Chapter 3 - Cyber security in mobile social networks (F. Al-Turjman and B. D. Deepak, Eds.). ScienceDirect; Academic Press, pp. 55-81, doi: 10.1016/B978-0-12-821599-9.00003-0.

[5] P. R. Shah and A. Agarwal, "Cybersecurity Behaviour of Smartphone Users Through the Lens of Fogg Behaviour Model," 2020 3rd International Conference on Communication System, Computing and IT Applications (CSCITA), 2020, pp. 79-82, doi: 10.1109/CSCITA47329.2020.9137773.

[6] Khera, V. (2018). A study of cybersecurity for telecommunication services concerning Smartphone users in Thailand. Researchrepository.murdoch.edu.au. https://researchrepository.murdoch.edu.au/id/eprint/42126/

[7] Ganesh, A., Ndulue, C., Orji, R. (2022). Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory. In: Baghaei, N., Vassileva, J., Ali, R., Oyibo, K. (eds) Persuasive Technology. PERSUASIVE 2022. Lecture Notes in Computer Science, vol 13213. Springer, Cham. https://doi.org/10.1007/978-3-030-98438-0_7

[8] Williams C, Chaturvedi R, Chakravarthy K
Cybersecurity Risks in a Pandemic
J Med Internet Res 2020;22(9):e23692
URL: https://www.jmir.org/2020/9/e23692
DOI: 10.2196/23692

[9] T. Tervoort, M. T. De Oliveira, W. Pieters, P. Van Gelder, S. D. Olabarriaga and H. Marquering, "Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review," in IEEE Access, vol. 8, pp. 84352-84361, 2020, doi: 10.1109/ACCESS.2020.2984376.

[10] Peng, C., Xu, M., Xu, S., &amp; Hu, T. (2018). Modelling multivariate cybersecurity risks. Journal of Applied Statistics, 45(15), 2718-2740. https://doi.org/10.1080/02664763.2018.1436701

[11] Algarni AM, Thayananthan V, Malaiya YK. Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. Applied Sciences. 2021; 11(8):3678. https://doi.org/10.3390/app11083678

[12] Buldakova, T.I. (2020). Cybersecurity Risks Analyses at Remote Monitoring of Object’s State. In: Kravets, A., Bolshakov, A., Shcherbakov, M. (eds) Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control, vol 260. Springer, Cham. https://doi.org/10.1007/978-3-030-32648-7_15

[13] Caroline C Hartmann, Jimmy Carmenate; Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. Current Issues in Auditing 1 September 2021; 15 (2): A9–A23. doi: https://doi.org/10.2308/CIIA-2020-034