JPSI : JURNAL PENELITIAN SISTEM INFORMASI
Vol.1, No.2 Mei 2023
e-ISSN: 2985-7759; p-ISSN: 2985-6310, Hal 49-64
DOI: https://doi.org/10.54066/jpsi-itb.v1i1.600

Banking Malware Attacks and Security Solutions Review

Kaira Milani Fitria
[1]Faculty of Computer Science, Informatics & Business, Institute Darmajaya Nama
kairaamilanii@gmail.com

Abstract. *This research explores the growing threat of banking malware attacks and the security solutions that can be implemented to mitigate the risks. The paper begins by providing an overview of the different banking malware attacks, including their propagation methods and the damage they can cause. It then delves into the various security measures that can be taken to prevent and detect these attacks, such as endpoint protection, network segmentation, and user education. The paper also examines the challenges and limitations of these security solutions and the potential for future developments in the field. Overall, this paper provides a comprehensive analysis of the current banking malware attacks and the security solutions that can be employed to safeguard against them. This research aims to comprehensively analyse the different types of banking malware attacks and the security solutions that can mitigate the risks. By understanding the nature of these attacks and the effectiveness of various security measures, this research can help financial institutions develop more effective strategies for protecting themselves and their customers from cyber threats.*

Keywords: *Malware Attacks, Security, Network, Banking Threat*

Abstrak. Penelitian ini mengeksplorasi ancaman serangan malware perbankan yang terus meningkat dan solusi keamanan yang dapat diterapkan untuk mengurangi risikonya. Makalah ini dimulai dengan memberikan gambaran umum tentang berbagai serangan malware perbankan, termasuk metode penyebaran dan kerusakan yang dapat ditimbulkannya. Kemudian membahas berbagai langkah keamanan yang dapat diambil untuk mencegah dan mendeteksi serangan ini, seperti perlindungan titik akhir, segmentasi jaringan, dan edukasi pengguna. Makalah ini juga membahas tantangan dan keterbatasan dari solusi keamanan ini dan potensi perkembangan di masa depan di lapangan. Secara keseluruhan, makalah ini memberikan analisis komprehensif tentang serangan malware perbankan saat ini dan solusi keamanan yang dapat digunakan untuk melindungi dari serangan tersebut. Penelitian ini bertujuan untuk menganalisis secara komprehensif berbagai jenis serangan malware perbankan dan solusi keamanan yang dapat mengurangi risikonya. Dengan memahami sifat serangan ini dan efektivitas berbagai langkah keamanan, penelitian ini dapat membantu lembaga keuangan mengembangkan strategi yang lebih efektif untuk melindungi diri mereka sendiri dan pelanggan mereka dari ancaman dunia maya.

Kata kunci: Serangan Malware, Keamanan, Jaringan, Ancaman Perbankan

Received Maret 28, 2023; Revised April 25, 2023; Accepted Mei 30, 2023
**Kaira Milani Fitria, kairaamilanii@gmail.com*

BACKGROUND

The background of this research is rooted in the increasing prevalence and sophistication of cyber attacks targeting the banking industry. In recent years, there has been a significant rise in malware attacks aimed at financial institutions, with cyber criminals using various techniques to steal sensitive data, compromise systems, and conduct fraudulent transactions. These attacks can have severe consequences, including financial losses, reputational damage, and legal liabilities. As a result, banks and other financial organizations are under increasing pressure to implement robust security measures to protect their systems and customers from these threats. The banking industry has become a prime target for cybercriminals, with malware attacks posing a significant threat to financial institutions and their customers. These attacks can result in the theft of sensitive data, financial losses, and reputational damage, among other consequences. As a result, banks and other financial organizations are under increasing pressure to implement robust security measures to protect their systems and customers from these threats.

Banking malware attacks have recently been a growing concern for financial institutions and their customers. The increasing use of online banking services has made it easier for attackers to steal sensitive information and credentials through attack vectors such as phishing emails, malware, and social engineering. The underground malware economy has fueled the significant growth of banking fraud, and banks have upgraded their security to protect transactions from fraud (Carminati et al., 2018). Having adequate security solutions to prevent and detect banking malware attacks is crucial. State-of-the-art solutions see fraud as deviations from customers' spending habits, but they do not provide an in-depth model's granularity and security analysis against elusive attacks (Carminati et al., 2018). A multi-layer approach to network security is necessary for network-based intrusion response systems to secure modern networks of heterogeneous devices (Grammatikakis et al., 2021).

Banking malware attacks have become increasingly common in recent years, posing a significant threat to financial institutions and their customers. These attacks can result in the theft of sensitive information, financial loss, and reputational damage. Various security solutions have been developed to mitigate the risks associated with banking malware. This paper reviews these security solutions and their effectiveness in preventing and detecting banking malware attacks. By analyzing the strengths and weaknesses of these solutions, this paper seeks to provide insights into the best practices for securing financial institutions against these types of attacks. This research paper aims to comprehensively analyse the different types of banking malware attacks and the security solutions that can be employed to mitigate the risks. The paper will begin by providing an overview of the other banking malware attacks, including their propagation methods and the damage they can cause. It will then delve into the various security measures that can be taken to prevent and detect these attacks, such as endpoint protection, network segmentation, and user education.

Banking malware attacks have been on the rise in recent years, and several notable incidents have occurred. Some examples of recent banking malware attacks is Emotet, this malware was active from 2014 to 2021 and was responsible for stealing banking credentials and other sensitive information from victims. It was spread through phishing emails and malicious attachments (Grammatikakis et al., 2021). Ransomware, this type of malware is designed to encrypt a victim's files and demand payment in exchange for the decryption key. In some cases, ransomware has targeted financial institutions and their customers (Carminati et al., 2018). Adversarial attacks, these attacks use machine learning algorithms to generate malware that can evade detection by security systems. Malware authors use these attacks to bypass security measures and steal sensitive information (Hu & Tan, 2017; Qi et al., 2022). Memory-based attacks: These attacks use memory forensics to identify and track malware that may be hiding in a victim's system. They can be used to discover indicators of compromise and prevent further damage (Proffitt, 2013). These are just a few examples of banking malware attacks in recent years. As the threat landscape continues to evolve, financial institutions and their customers must remain vigilant and take steps to protect themselves against these attacks.

The paper will also examine the challenges and limitations of these security solutions and the potential for future developments in the field. By understanding the nature of these attacks and the effectiveness of various security measures, this research can help financial institutions develop more effective strategies for protecting themselves and their customers from cyber threats. Overall, this research paper aims to contribute to the growing knowledge on banking malware attacks and security solutions, providing insights and recommendations to help financial institutions stay ahead of the evolving threat landscape.

LITERATURE REVIEW

Malware is a collective term used for various malicious software variants such as viruses, trojans, ransomware, and spyware (J. Zhao et al., 2021). It encompasses code created by attackers with the intent to disrupt data, systems, or gain unauthorized network access. Various propagation methods are employed by different types of malware to extend their impact. For instance, certain malware is distributed via email as clickable links, relying on users to click on them, while others are self-activated through malicious file downloads onto a system.

Banking threats are a type of cyber threat that target financial institutions and their customers (Perwej et al., 2021). Banking threats refer to various risks and malicious activities that target the banking industry and its customers. These threats are specifically designed to exploit vulnerabilities in banking systems, compromise sensitive financial information, and carry out fraudulent activities.

A security solution can be defined as the measures taken to ensure the protection of systems, data, and networks against unauthorized access, theft, espionage, and other security threats. Security solution as the key design, architectural, and implementation choices made by organizations to satisfy specified security requirements for systems or system components(Ross et al., 2022). Security solutions refer to a wide range of tools, technologies, and strategies implemented to protect systems, networks, data, and individuals from various security threats and risks. These solutions aim to safeguard against unauthorized access, data breaches, malware attacks, and other malicious activities.

METHOD

The methodology for this paper involves a comprehensive review of the security solutions available to mitigate the risks associated with banking malware attacks. The study will be based on analysing the strengths and weaknesses of these solutions and their effectiveness in preventing and detecting banking malware attacks. This paper will examine the impact of cybercrime and security in online banking transactions.

In the money transfer activities, check account balances, make bill payments, and do other online banking tasks when away from the home computer. This practice is known as mobile banking. Bank consumers like the ease it offers, but the infrastructure for mobile banking is vulnerable to various threats. We outline the development of mobile banking, the many risks that come with it, and some of the most recent malware assaults. To enable safe mobile banking, we also analyze several contemporary security solutions.

- Increase of Mobile Banking Users

Online banking was made possible by utilizing specific tools (such as keyboards, terminals, and monitors) to access bank accounts through a telephone connection in the late 1980s. Today, online banking includes any electronic payment system that enables clients (holders of bank accounts) of a financial institution (bank) to carry out financial transactions through the bank's website. Online banking services have recently implemented mobile Internet banking technologies, such as person-to-person payments made possible by some smartphone applications. The following problems are among the leading causes of the sharp rise in the number of people using mobile banking (Kiljan et al., 2016).

1. The factor of age: The growth in mobile banking use is driven by those between 18 and 32.
2. Usability: People utilize a variety of user-friendly mobile banking programs nowadays. Additionally, these applications provide banking consumers with a comprehensive and smooth experience.
3. Accessibility: Mobile banking users get access to several services, including the ability to add beneficiaries, move money between accounts, and receive

notifications when their balance changes, all at the press of a button, whenever they want, from any location.

4. Mobile-only banks Nowadays, traditional banking has changed to utilize mobile applications. For a variety of financial functions, the majority of the significant banks employ mobile apps.
5. Switch to paperless transactions: Many banks provide cash rewards for using mobile banking instead of paper-based transactions. In the near field of communication technology-based contactless payment mechanisms, two cards may speak to one another and digitally transfer funds (Ghosh et al., 2017).
6. Fraudulent activity may be readily identified online by mobile banking users, who can also monitor their bank accounts. Using a one-time password can help prevent unwanted and unlawful online money transfers in this situation.

- The Evolution of Mobile Banking

The development of Internet banking since the 1980s has made it simpler for users to handle the money in their accounts. Customers of the Nottingham Building Society were first made aware of the UK's "Homelink" Internet banking service by the Bank of Scotland in 1983. Early examples of internet banking may be seen in the Homelink service. Online banking was first offered by the personal financial program Microsoft Money in 1994, and it quickly gained popularity. The Stanford Credit Union launched the first online banking website during the same decade. Eight American banks each had at least one million internet customers in 2001. 19 million American homes were utilizing internet banking at the time. The Federal Financial Institute Examination Council published the guidelines and norms in 2005 to help financial institutions conduct risk-based analyses. Online banking was first offered by direct banks, like ING Direct, that don't have physical branches. Financial transactions were moved away from personal computers and onto mobile devices like smartphones after Apple introduced the iPhone in 2007. 54 million American households began using computers and mobile devices to access their online bank accounts 2009. Online banking became widely used in 2011. Social networking, internet banking, personal financial management, payments, and rewards came together in 2012 to usher in the social banking era.

- Attack Trends on Mobile Banking

The financial services sector has acknowledged the promise of mobile banking. For clients to use all the benefits these apps give, the industry has implemented mobile banking applications. However, the security risks associated with mobile banking have discouraged many users from using it. The following are the current mobile banking worries that prospective users of mobile banking have:

1. Mobile malware: Attacks from malware are moving from conventional systems to online financial schemes. Attackers have created malware that targets mobile banking apps, and more malware will likely target mobile banking applications.
2. Usage of third-party applications: Applications from third parties are only partially trusted. Nefarious attackers and fraudsters created some of the applications.
3. Usage of unsecured Wi-Fi: Wi-Fi is available in most public places, such as shopping malls and airports, and hackers and cyber criminals may gain access to smartphones and launch man-in-the-middle and relay attacks.
4. User behaviour: Since users are inclined to download third-party software, utilize unprotected Wi-Fi, and open and click links in emails and short messaging services, they can also help attackers achieve their nefarious intentions. Attackers can also access the system when users' devices are misplaced or stolen.

- Mobile Banking Malware Attacks

Several malware varieties might harm mobile banking systems. Different types of potential malware attacks on mobile banking is explained :

1. Keyloggers: A malicious application known as a keylogger captures all keystrokes on a computer system. It may be used to steal the user's credentials (such as those for online banking accounts) and other sensitive data about a business.
2. Spyware: Spyware is a program that tracks essential information from a system (i.e., a smartphone). The stolen data might be utilized improperly, such as selling email addresses to spammers.
3. Virus : A virus is an infectious program that connects to another piece of software (or program) and then replicates once that software begins to run.

4. Worm: A worm is a computer software that spreads itself throughout a system and deletes files and data. It can propagate across computer networks by taking advantage of flaws in the operating system.
5. Trojan: Trojan programs are written to obtain a user's financial data and gain control of the system's resources. A connected smartphone can execute further assaults against a router using an Android-infected trojan virus.
6. Rootkit: A rootkit is a form of malware that uses aspects of the operating system, such as application programming interface function redirection, to conceal its presence or the presence of another program (for example, spyware in a smartphone).
7. Hijacker: A malicious software that primarily impacts the browser is a hijacker or browser hijacker. It reroutes typical search activity and displays the outcomes that its creators intended for users to view.
8. Ransomware: This malware locks users' data or locks the system's screen until or unless a certain amount (called a "ransom") is paid. This software prohibits users from using their design (i.e., smartphone).

On mobile/Internet banking systems, several virus assaults can be deployed. The details of these assaults, including the name, kind, traits, and impact of the malware, are summarized in Table 1.

Table 1. Mobile banking malware attacks

Name	Type	Characteristics
Zbot	Trojan with Ransomware	Zbot, or Zeus, was first identified in July 2007. Attackers use this malware to steal banking data by the man-in-the-browser keystroke logging method
Faketoken	Trojan	It creates fake login screens so that an attacker can steal login credentials through some financial applications.
Tordow	Trojan	It piggybacks on popular applications (e.g., Pokemon GO) and steals sensitive information from a mobile device by gaining root access.
Black Jack Free	Trojan	It is based on the vicious malware that steals users' personal and banking information and login credentials of popular online websites.
HijackRAT	Trojan	HijackRAT behaves like a mobile banking trojan. It comes loaded with a malicious Android application that camouflages itself as "Google Service Framework."
Tinba	Trojan	Tinba first infects a system when a user tries to log in to one of the targeted banks' websites. Then, the victim

		(customer) receives fake messages and web forms asking for login credentials.
TrickBot (Dyre)	Trojan	In 2014–2015, it did a lot of damage via malicious activities (i.e., spamming and phishing). It succeeded in stealing roughly US$5.5 million by performing unauthorized wire transfers.
SpyEye	Trojan	It is a data-stealing malware that was created for stealing money from online bank accounts.
Shylock	Trojan	This banking malware can steal a user's banking credentials for illegal money transfer.

HASIL DAN PEMBAHASAN

Security Requirements For Mobile Banking

A certain level of security must be maintained to keep mobile banking customers secure.

1. Confidentiality: Only those with the proper authorization should have access to the financial information of the different bank clients.
2. Integrity: Under no circumstances should any unauthorized entity (i.e., an attacker) modify or otherwise alter a bank's financial data.
3. Availability: Any denial-of-service attack against financial information systems, including various banking servers, should be prevented.
4. Authentication: The process of confirming a user's (i.e., the owner of a bank account's) identity is known as authentication. Two-factor authentication and three-factor authentication are the two different kinds of multifactor authentication techniques that are covered in this article. A user uses two types of credentials a password and a mobile device (smart card) in two-factor authentication. When a user registers with the server, the smart card or mobile device can save the necessary data. In three-factor authentication, a user authenticates with the system using three different credentials, including a password, a smart card or mobile device, and biometrics (fingerprint and face recognition).
5. Authorization: Authentication allows someone to do an approved operation. It prevents a mobile banking user from accessing information kept on the banking

server(s) to which they are authorized (for example, depending on their stated position in the system).

6. Physical theft of devices: Devices such as smart cards and mobile instruments (e.g., smartphones) hold valuable information required for safe and effective authentication. Following the theft of these devices, various attacks, including privileged insider and offline/online password-guessing attacks, can be conducted.
7. Nonrepudiation: Nonrepudiation refers to the user's incapacity to refute the legitimacy of their signature on a document or message submitted by them.
8. Freshness: In the mobile banking payment system, freshness guarantees that the data are current and prevents adversaries from replaying previous messages.
9. Forward secrecy: Suppose an entity leaves the network. Any messages sent after the departing entity must be inaccessible to it.
10. Backward secrecy: requires that a new entity joining the network not have access to any communications that have already been sent.

Security Solutions For Mobile Banking Threats

Several security measures should be in place to limit potential risks to mobile banking networks.

1. Awareness: It is essential to create programs that inform bank employees and mobile banking users about various threats, including malware, phishing, and malicious file downloads.
2. Malicious email attachments: Mobile banking users should be careful not to click, download, or open a file received in an email attachment since it can contain malware.
3. Operating system updates: The ability to automatically download software updates is one of the most significant features of modern techniques (including desktop, smartphone, and tablet computers).
4. Protection: Mobile banking users should protect themselves by installing antivirus software on their computers.
5. Use of solid authentication schemes: To safeguard the mobile banking system, a secure authentication technique is required.

Limitations Of Mobile Banking Security Solutions

There are restrictions to the security applications in mobile banking, even with awareness and prudence.

1. Several institutions provide security awareness courses to online or mobile banking customers. However, to adequately inform consumers about the risks associated with mobile banking, we need to perform security awareness programs more regularly in both the online and offline modes.
2. A smart card or a mobile device can be used to launch several types of assaults. A secure authentication strategy must be created to withstand assaults against smart cards or mobile devices.
3. Unknown abnormalities, such as a zero-day assault, may impact security measures. Therefore, unidentified anomalies should have a minimal impact on the mobile banking infrastructure.

Comparison Of Security And Functionality Features Of Authentication Schemes

We outline several security requirements that two-factor and three-factor authentication should meet to defend against threats already known to exist.

1. Replay attack: In this scenario, attacker A attempts to trick another trustworthy user by reusing knowledge gained by listening in on transmitted data.
2. Man-in-the-middle assault: In this type of attack, A places themself in the centre of two communicating parties, pretend to be both of them and accesses the information they share.
3. Attack by impersonation: In this type of attack, A uses the identity of a legitimate user on a network to trick other users. A goal is to persuade the recipient by modifying a legal message or inserting fake news into the communication.
4. Attack on password guessing: In the password guessing attack, A either intercepts some messages during a communication exchange and uses the password dictionary attack method to try to guess the user's password, or A uses the user's lost or stolen smart card, mobile device, and the data gathered during the registration time to try to guess the user's password.

5. Smart card/mobile device stolen attack: In the smart card/mobile device stolen assault, A uses information acquired from a lost/stolen smart card/mobile device, together with strategies like the power analysis attack (Messerges et al., 2002), to try to guess the password of an authorized user.
6. Privileged insider attack: In a privileged insider attack, a lousy insider (attacker A, for example) can access the user's registration information. A then tries to calculate the secret credentials, such as the user's password.
7. User anonymity and untraceability: To protect user privacy, A should be unable to determine the user's true identity from the intercepted messages. A, however, should be unable to decide on the user's activity from the intercepted communications thanks to the untraceability attribute.

Comparison Of Two-Factor And Three-Factor Authentication Techniques

We examine the security and functional aspects of a few recently suggested two-factor authentication methods (Memon et al., 2015; Mun et al., 2012; Xie et al., 2014; D. Zhao et al., 2014) in Table 2. The different security and functional aspects of newly suggested three-factor authentication methods (He & Wang, 2015; Lin et al., 2015; Lu Yanrong AND Li, 2015; Wang Chengqi AND Zhang, 2016) are displayed in Table 3.

Table 2. Comparison of two-factor schemes

Feature	(Mun et al., 2012)	(Xie et al., 2014)	(D. Zhao et al., 2014)	(Memon et al., 2015)
User anonymity & untraceability	No	Yes	Yes	Yes
Mutual authentication	No	Yes	Yes	No
Authentication & key agreement	No	No	Yes	No
Session-key agreement	No	Yes	No	No
Privileged insider attack	No	Yes	No	No
Replay attack	No	Yes	No	Yes
Password guessing attack	No	No	No	Yes
User impersonation attack	No	Yes	Yes	No
Smart card stolen attack	N/A	Yes	No	Yes
Secure password changing facility	N/A	No	Yes	No
Man-in-the-middle attack	No	No	Yes	Yes
Perfect forward secrecy	Yes	Yes	Yes	Yes
"Yes" means a scheme is secure against a particular attack or it supports a particular feature, and "No" means otherwise				

Two-factor authentication (2FA) in mobile banking is a security measure that adds an extra layer of protection by requiring users to provide two different types of authentication factors when accessing their mobile banking accounts. This method enhances the security beyond the traditional username and password combination. The two factors typically used in 2FA are:

1. Knowledge Factor: This involves something the user knows, such as a password, PIN, or pattern. It is the most common form of authentication and is the first step in the verification process.
2. Possession Factor: This factor involves something the user possesses, usually a physical device like a smartphone, tablet, or hardware token. The possession factor adds a layer of security by requiring the user to access a specific device to complete the authentication process.

Users who enable 2FA for their mobile banking account typically need to enter their username and password (knowledge factor) as the first step. Once this information is verified, the system prompts the user to provide the second factor, a one-time passcode (OTP) generated by an authentication app on their mobile device, received via SMS or push notification. By entering this second factor, the user demonstrates possession of the registered device, confirming their identity.

Table 3. Comparison of three-factor schemes

Feature	(Lu Yanrong AND Li, 2015)	(Lin et al., 2015)	(He & Wang, 2015)	(Wang Chengqi AND Zhang, 2016)
User anonymity & untraceability	No	No	Yes	No
Mutual authentication	Yes	Yes	No	Yes
Replay attack	Yes	Yes	Yes	Yes
Man-in-the-middle attack	No	No	Yes	Yes
Stolen smart card attack	Yes	Yes	Yes	Yes
User impersonation attack	No	No	No	No
Server impersonation attack	No	No	Yes	No
Insider attack	Yes	Yes	No	No
Password guessing attack	Yes	Yes	Yes	Yes
Perfect forward secrecy	No	Yes	Yes	Yes
"Yes" means a scheme is secure against a particular attack or it supports a particular feature, and "No" means otherwise				

Three-factor authentication (3FA) in mobile banking refers to a security measure that adds a layer of authentication beyond the traditional username-password combination and the commonly used two-factor authentication (2FA). It involves using three factors to verify the user's identity attempting to access their mobile banking account. The three factors typically include:

1. Knowledge Factor: involves something the user knows, such as a password or PIN. It is the most common and essential form of authentication.
2. Possession Factor: This factor involves something the user possesses, typically a physical device or token. In the context of mobile banking, this can be a mobile device, a smart card, a hardware token, or a security key.
3. Inherence Factor: involves something inherent to the user, often called biometrics. It includes unique physiological or behavioural characteristics, such as fingerprints, facial recognition, voice recognition, or even iris scanning.

By combining these three factors, three-factor authentication provides an additional layer of security, making it harder for unauthorized individuals to access a user's mobile banking account. Even if one aspect is compromised, the other factors protect. To implement three-factor authentication in mobile banking, users may be required to provide their username and password (knowledge factor), use a mobile device or security token (possession factor), and provide biometric data like fingerprint or facial scan (inherence factor) to complete the authentication process.

CONCLUSION

During our comprehensive discussion on mobile banking, we delved into many topics, including the fundamental driving forces behind its adoption, the inherent risks it encounters, and the essential security requisites it demands. Moreover, we explored various security solutions devised to combat the threats targeting mobile banking, meticulously analyzing their limitations and exploring potential avenues for enhancement. While these security solutions provide a solid foundation for combating malware threats in mobile banking, it is essential to acknowledge that the threat landscape is constantly evolving. Continuous research, adaptation of new technologies, and proactive security measures are crucial to stay one step ahead of cybercriminals and protect the integrity of mobile banking systems.

UCAPAN TERIMA KASIH

I would like to express my gratitude to Mr Sriyanto, PhD for his contributions as specialists to this study.

DAFTAR REFERENSI

Carminati, M., Polino, M., Continella, A., Lanzi, A., Maggi, F., & Zanero, S. (2018). Security Evaluation of a Banking Fraud Analysis System. ACM Transactions on Privacy and Security (TOPS), 21, 1–31.

Ghosh, S., Majumder, A., Goswami, J., Kumar, A., Mohanty, S. P., & Bhattacharyya, B. K. (2017). Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment. IEEE Consumer Electronics Magazine, 6(1), 82–93. https://doi.org/10.1109/MCE.2016.2614522

Grammatikakis, K.-P., Koufos, I., Kolokotronis, N., Vassilakis, C., & Shiaeles, S. (2021). Understanding and Mitigating Banking Trojans: From Zeus to Emotet. CoRR, abs/2109.01610. https://arxiv.org/abs/2109.01610

He, D., & Wang, D. (2015). Robust Biometrics-Based Authentication Scheme for Multiserver Environment. IEEE Systems Journal, 9(3), 816–823. https://doi.org/10.1109/JSYST.2014.2301517

Hu, W., & Tan, Y. (2017). Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN. CoRR, abs/1702.05983. http://arxiv.org/abs/1702.05983

Kiljan, S., Simoens, K., Cock, D. De, van Eekelen, M. C. J. D., & Vranken, H. P. E. (2016). A Survey of Authentication and Communications Security in Online Banking. ACM Computing Surveys (CSUR), 49, 1–35.

Lin, H., Wen, F., & Du, C. (2015). An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics. Wireless Personal Communications, 84(4), 2351–2362. https://doi.org/10.1007/s11277-015-2708-4

Lu Yanrong AND Li, L. A. N. D. Y. X. A. N. D. Y. Y. (2015). Robust Biometrics Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. PLOS ONE, 10(5), 1–13. https://doi.org/10.1371/journal.pone.0126323

Memon, I., Hussain, I., Akhtar, R., & Chen, G. (2015). Enhanced Privacy and Authentication: An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme. Wireless Personal Communications, 84(2), 1487–1508. https://doi.org/10.1007/s11277-015-2699-1

Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers, 51(5), 541–552. https://doi.org/10.1109/TC.2002.1004593

Mun, H., Han, K., Lee, Y. S., Yeun, C. Y., & Choi, H. H. (2012). Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Mathematical and Computer Modelling, 55(1), 214–222. https://doi.org/https://doi.org/10.1016/j.mcm.2011.04.036

Perwej, Dr. Y., Abbas, Q., Dixit, J., Akhtar, N., & Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, Volume 9, Pages 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Proffitt, T. (2013). Indicators of compromise in memory forensics GIAC (GCFA) Gold Certification.

Qi, X., Tang, Y., Wang, H., Liu, T., & Jing, J. (2022). Adversarial Example Attacks Against Intelligent Malware Detection: A Survey. 2022 4th International Conference on Applied Machine Learning (ICAML), 1–7.

Ross, R., Pillitteri, V., & Dempsey, K. (2022). SP 800-172A, Assessing Enhanced Security Requirements for CUI CSRC.

Wang Chengqi AND Zhang, X. A. N. D. Z. Z. (2016). Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme. PLOS ONE, 11(2), 1–25. https://doi.org/10.1371/journal.pone.0149173

Xie, Q., Hu, B., Tan, X., Bao, M., & Yu, X. (2014). Robust Anonymous Two-Factor Authentication Scheme for Roaming Service in Global Mobility Network. Wireless Personal Communications, 74(2), 601–614. https://doi.org/10.1007/s11277-013-1309-3

Zhao, D., Peng, H., Li, L., & Yang, Y. (2014). A Secure and Effective Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks. Wireless Personal Communications, 78(1), 247–269. https://doi.org/10.1007/s11277-014-1750-y

Zhao, J., Masood, R., & Seneviratne, S. (2021). A Review of Computer Vision Methods in Network Security. IEEE Communications Surveys & Tutorials, 23(3), 1838–1878. https://doi.org/10.1109/COMST.2021.3086475