Analysis of Fraud Attacks Using Android Package Kit in Indonesia

1st Sopian Amir
Research Center for Data and Information Science
National Research and Innovation Agency
Jakarta, Indonesia
sopian.amir@brin.go.id

2nd Dimas Febriyan Priambodo
Cybersecurity Engineering Departement
National Cyber and Crypto Polytechnic
Bogor, Indonesia
dimas.febriyan@poltekssn.ac.id

3rd Abdul Azzam Ajhari
Department of Informatics
Universitas Siber Asia
Jakarta, 12550, Indonesia
abdulazzam@lecturer.unsia.ac.id

4th Armita Widyasuri
Research Center for Data and Information Science
National Research and Innovation Agency
Jakarta, Indonesia
armita.widyasuri@brin.go.id

2024 International Conference on Computer, Control, Informatics and its Applications (IC3INA) | 979-8-3315-4231-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/IC3INA64086.2024.10732435

Abstract*— The increasing prevalence of new phishing and scamming attack methodologies in Indonesia, orchestrated by threat actors, highlights significant concerns for Android users. The dynamic frequency and sophistication of cyberattacks in Indonesia, particularly through Android Package Kit (APK), presents a challenge for cybersecurity researchers and experts to protect the Indonesian public. This research carefully dissects the patterns and tactics used in these fraudulent attacks, explaining the common traits of malicious APKs and the strategies used by threat actors to exploit vulnerabilities in Android devices. A comprehensive examination of APK phishing incidents reported in Indonesia over the past few years forms the basis of this research, drawing insights from various cybersecurity reports, case studies, and digital forensic analyses. The research studied vulnerabilities inherent to the Android system, including behavioral analysis and security lapses on user devices. In addition, an in-depth review was conducted to assess the efficacy of existing cybersecurity measures and policies in Indonesia, measuring their ability to thwart fraudulent APK attacks. This research underscores the importance of more robust security protocols, better user education, and strict regulatory frameworks to mitigate the risks associated with phishing APK attacks. The findings aim to provide cybersecurity professionals, policymakers, and the general public with a deeper understanding of security awareness of the nature and implications of fraudulent APK attacks in improving digital security in Indonesia.

Keywords*— android package kit, cyber security, cybersecurity awareness, phishing, scamming.

I. INTRODUCTION

Rapid technological advancements and an escalating reliance on mobile applications, coupled with the popularity of smartphones and mobile devices, mobile application (a.k.a. "app") markets have been growing exponentially in terms of the number of users and downloads [1]. In an era where digital transactions and mobile internet usage are on the rise [2]–[4], The various means of cybercrime are increasingly troubling. This unrest triggered a lot of research related to phishing, which was developed by several researchers [5]–[8]. A report from the Headquarters of the National Police of the Republic of Indonesia (MABES POLRI) submitted through the Kompas.com news media on 19 January 2023 [9], revealed that at least 493 people had become victims of illegal APK link fraud cases, with losses reaching IDR 12 billion. Looking at the report, it becomes clear that an adequate investigation is needed to prevent and minimize similar losses in the future.

APK files, the primary packaging format for Android applications, have become the preferred means for criminals to perpetrate scams. As a burgeoning hub for digital innovation, Indonesia has witnessed a surge in the adoption of mobile technologies, with a substantial 88.23% of smartphone users favoring the Android operating system. StatCounter data for February 2023 - February 2024 shows that the majority of smartphone users in Indonesia, at 89.04%, use Android systems [10]. The urgency to address this issue is further reinforced by the Anti-Phishing Working Group's report for Q1 and Q2 of 2023, which recorded a total of 2,910,352 phishing cases that occurred in Indonesia [11], [12].

In addition, a noteworthy development is the creation of increasingly sophisticated spyware systems on the Android platform, which use APK files to surreptitiously collect information about victims, as described in [12]–[14]. This has resulted in concerns over the insecurity of data and information held by users. This alarming trend highlights the urgent need for a thorough investigation into the patterns, tactics, and vulnerabilities associated with APK-based phishing attacks [13], [14]. Such vetting is crucial to strengthening Indonesia's cybersecurity system [15] and ensuring the protection of mobile device users in the face of evolving cyber threats.

This investigation will closely examine various aspects of fraudulent APK attacks, including the social engineering techniques used, the types of data targeted, as well as the impact caused by such attacks. In addition, the investigation will also evaluate the level of effectiveness of the current cybersecurity infrastructure in Indonesia, focusing on its ability to mitigate the risks resulting from such attacks.

II. RELATED WORKS

A. OWASP Mobile Application Security Testing Guide

In conducting this research, we adopted a penetration testing (pentesting) approach in five distinct stages, in line with the OWASP Mobile Application Security Testing Guide (MASTG) guidelines: Preparation, Intelligence Gathering, Mapping the Application, Exploitation, and Reporting [16]. This approach allows us to effectively identify and address security vulnerabilities in applications to find out the medium that criminals are using. The OWASP MASTG was used specifically to test eight malicious applications that have been discovered and utilized by criminals to commit fraud in Indonesia.

TABLE I. DETAIL LIST APK

ID	Ref.	APK Phishing	Description	Attack date
1	https://www.kominfo.go.id/content/detail/53363/hoaks-pesan-whatsapp-aplikasi-pps-pemilu-2024/0/laporan_isu_hoaks	PPS Pemilu 2024	As the 2024 election approaches, many are taking advantage of the situation. Currently, the fraudulent mode of sending the 2024 PPS Election APK is starting to circulate via WhatsApp (WA) messages.	4 December 2023
2	https://www.liputan6.com/tekno/read/5289643/ramai-modus-penipuan-pdf-pesanan-palsu-incar-penjual-online-pengamat-lebih-bahaya-dari-phishing	List Order PDF	The online shop admin sends a file which they call a PDF of the order list in APK format.	15 May 2023
3	https://otomotif.kompas.com/read/2023/03/19/072100815/waspada-marak-modus-penipuan-surat-tilang-pakai-file-apk-dikirim-lewat?page=all	Surat Tilang Elektronik	The perpetrator, who claimed to be a police officer, informed that the recipient of the message had committed a traffic violation. The perpetrator sends an APK file called "Surat Tilang-1.0" and asks the victim to open the application.	19 March 2023
4	https://www.kompas.com/tren/read/2023/02/19/211000565/penipuan-berkedok-ditjen-pajak-kirim-file-apk-melalui-whatsapp-pakar--djp?page=all	Dirjen Pajak Keuangan	The perpetrator wrote a message that there were tax documents in softcopy and hardcopy form for the recipient of the message. The perpetrator also sent an APK file called "Dirjen Pajak Keuangan" which was said to be a softcopy document to the recipient.	12 February 2023
5	https://www.kompas.com/cekfakta/read/2023/01/31/153000182/penipuan-apk-mengatasnamakan-bpjs-kesehatan-pahami-risiko-dan-cara?page=all	Tagihan BPJS Kesehatan	Via WhatsApp, an unknown number sent a BPJS Health bill to the victim. Victims are asked to immediately make payments at the nearest bank or channel. Then, attach an APK file with the title "LEMBAR TAGIHAN" which is forwarded by that number.	30 January 2023
6	https://kumparan.com/kumparantech/waspada-penipuan-berkedok-undangan-nikah-di-wa-bisa-bobol-m-banking-1ziYeSf6tx4/1	Undangan Pernikahan Digital	The mode of fraud is by sending fake wedding invitations on WhatsApp which contains an m-banking hacking application which can also steal WhatsApp accounts.	27 January 2023
7	https://www.kominfo.go.id/content/detail/46185/hoaks-pesan-whatsapp-pengiriman-paket-mengatasnamakan-jt-express/0/laporan_isu_hoaks	Pengiriman Paket J&T Express	A WhatsApp message has been circulating containing package delivery information on behalf of J&T Express. The message sends a document file with the title “VIEW Package Photos” in the Android Package Kit (APK) extension.	7 December 2022

OWASP MASTG is a security standard applied to mobile applications, accompanied by a comprehensive testing guide. This guide encompasses various processes, techniques, tools, and case studies related to the implementation of mobile application security testing. The purpose of using this security standard is to verify the MASVS requirements, consisting of test cases, where each case illustrates the requirements of MASVS.

B. Mobile Security Frameworks

Mobile Security Framework (MobSF) is an open-source automated testing framework capable of conducting penetration tests, malware analysis, and security assessments of mobile applications through static and dynamic analysis. The analysis process produces reports on the tested Android applications. MobSF can be used for quick and effective security analysis of Android, iOS, and Windows mobile applications, and it supports binaries (APK, IPA, and APPX) as well as source code in zip format. MobSF can perform dynamic application testing at runtime for Android applications and has web API fuzzing capabilities supported by CapFuzz, a web API security scanner. MobSF has a graphical user interface in the form of a web service, which includes a dashboard presenting analysis results, its documentation site, an integrated emulator, and an API that allows users to trigger analysis automatically. MobSF is hosted on a local server, ensuring that sensitive data never interacts with the APK cloud [17].

C. Object

The recent incidents of APK phishing in Indonesia demonstrate a diverse range of approaches adopted by cybercriminals listed in Table I.

III. METHODOLOGY

To achieve Android application security, we refer to the research that has been conducted [18]–[20] which presents a methodology for securing applications based on OWASP guidelines. The methodology consists of a series of steps, including checklists and penetration testing techniques, designed to identify vulnerabilities such as insecure data storage and communications. To expand the scope of the research, Thomas Borja [21] has conducted comprehensive security penetration testing on Android applications, providing in-depth risk analysis and relevant security recommendations.

Provides a comprehensive overview of fraudulent cyber-attacks (phishing and scamming) through Android-based applications in line with Alkhalil's research [14], we analyzed the latest trending APKs being distributed to users in Indonesia, in line with findings from previous research on fraudulent APKs on Android [22], [23]. In addressing this challenge, we propose a different approach by extending the use of traditional reverse engineering methods using APK Editor Studio. That method is commonly used for general application testing as done in previous studies [19], [21], [24]. We propose a more advanced approach by decompiling APKs using Mobile Security Frameworks (MobSF) which is based on the OWASP Mobile Application Security Testing Guide (MASTG) standard. MobSF performs penetration tests, malware analyses, and security assessments of APKs, and presents them in a dashboard as results. The displayed dashboard is then subjected to further analysis.

The key difference in our approach is the use of MobSF, which provides an edge in detecting cyber-attacks and security loopholes that may be missed by traditional methods. By implementing MobSF, we can provide a more in-depth

understanding of cyber threats specific to Android applications, particularly in the Indonesian user environment. In addition, we also provide appropriate remediation steps and solutions that correspond to each weakness we identify.

Another advantage of our approach is the novelty of integrating the OWASP MASTG standard in the analysis process. Using these standards, we can ensure that every aspect of Android application security is comprehensively evaluated according to the latest guidelines in the mobile application security industry. Thus, our approach not only improves the accuracy in detecting fraudulent APK attacks, but also provides a clear direction for developers to increase security awareness in using their smartphones.

Overall, our approach offers a more holistic and innovative solution for combating fraudulent APK attacks in the Android application environment, utilizing the latest technologies and standards in the information security industry.

From Fig. 1, it can be explained that the blue box is the stage that will be carried out during the research, briefly related to tactics, techniques, and procedures (TTP) carried out on OWASP MASTG using the Cross Industry Standard Process for Data Mining (CRISP-DM) method.

A. Reverse Engineering

The process of obtaining the source code of a compiled application. This process involves using special tools called decompilers to analyze the application's binary files and produce human-understandable source code.

B. Static Analysis

Static black box analysis performs analyses without having access to the source code, focusing on the features and functions of the application that are visible from the outside. Both help in finding security issues such as user input vulnerabilities, insecure API usage, and authorization and authentication issues, thus helping in improving the security of mobile applications.

C. Dynamic Analysis

Dynamic analysis is used to identify various security vulnerabilities in mobile applications.

1) Business Logic Flaws, at this stage focus on simulating various application usage scenarios to identify flaws in the business logic. This is done by sending different types of inputs and monitoring the application's responses, as well as analyzing the underlying business logic. For example, dynamic analysis can reveal weaknesses in authentication, authorization, or validation processes that can be exploited by attackers to achieve unauthorized goals.
2) The Vulnerabilities Test, at this stage, explores vulnerabilities and security threats that may exist. This includes performing attacks on the application by attempting to exploit existing vulnerabilities by sending invalid or malicious inputs. Dynamic analysis helps in identifying security holes that can be exploited by attackers to access or manipulate data unauthorisedly.

Weak/Bad Input Validation, at this stage aims to test the strength of the application's input validation. By sending invalid or suspicious input, dynamic analysis can identify whether the application can handle the input correctly or is vulnerable to attack. For example, sending input containing special characters or unexpected data to see if the application can filter and validate the input correctly, or if the input can trigger a vulnerability or threat.

D. Binary Analysis

At this stage, the binary code of the mobile application is analyzed by translating the behavior of the program into logical formulas. This process aims to understand how the application interacts with the operating system, hardware, and other resources. The translation into logical formulas makes it possible to detect and analyze potential security issues, such as security holes or vulnerabilities in the application. This helps in deeply understanding how the application behaves at the binary level, which is important in identifying and fixing security issues.

E. Tampering and Runtime Instrumentation

The runtime manipulation stage in OWASP MASTG includes tampering and runtime instrumentation.

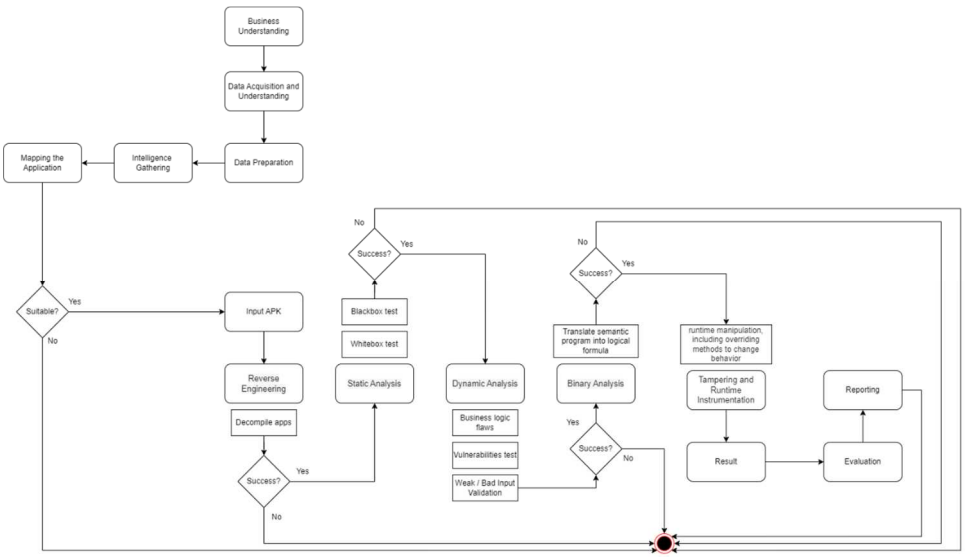

Fig. 1. Data Mining Mobile Security Testing Techniques

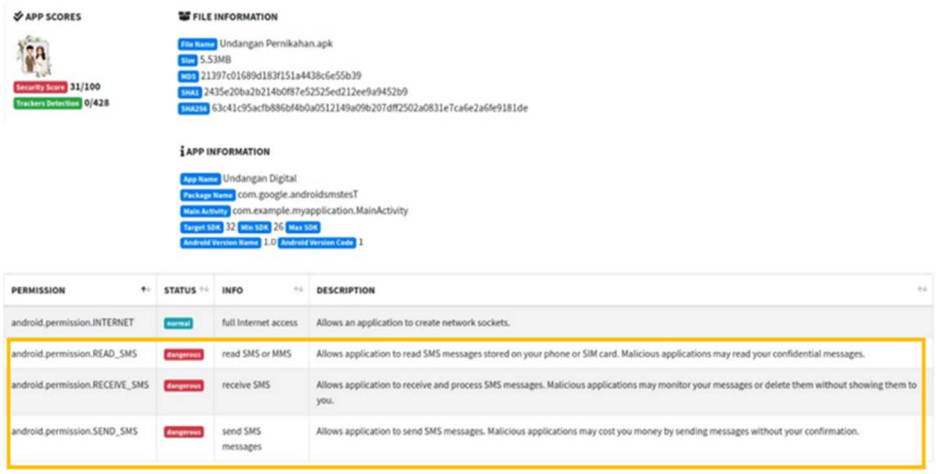

Fig. 2. MobSF report dashboard

1) Tampering involves modifying an application at runtime to manipulate behavior or data. This includes modifying data stored locally on the device, such as changing variable values, changing HTTP parameters, or even changing the flow of program execution. Examples are manipulating variable values that affect user authorization or changing the results of critical calculations in the application.

2) Runtime Instrumentation involves the use of tools or techniques to insert instrumented code into an application at runtime. These techniques allow monitoring and analysis of the application's behavior while it is running. One of the actions often performed in runtime instrumentation is to replace or switch methods to dynamically change the behavior of the application. For example, by switching or replacing authentication or encryption methods, an attacker can infiltrate malicious functionality or gain unauthorized access.

The output of the entire TTP process can be seen in the green box which will include a comprehensive report that identifies, analyses, and describes the security findings in the tested mobile application. This report includes a detailed description of the vulnerabilities found, such as unvalidated user input vulnerabilities, weak authorization issues, or security holes in the code. In addition, the report also includes specific corrective action recommendations, as well as mitigation measures to address each identified vulnerability. The purpose of this report is to provide clear insights to the public who receive phishing APKs regarding the potential threats of such APKs and how they can be prevented.

IV. RESULT AND DISCUSSION

A. APK Analysis

The examination of malicious APKs through MobSF unveiled various critical vulnerabilities. First, many of these APKs were found to be in a debuggable state, making them easy targets for reverse engineering. Attackers could exploit this to modify the app's code and behavior. Furthermore, the identification of exported activities and broadcast receivers within these APKs signifies a deficiency in proper isolation, exposing these applications to external access. This weakness can allow unauthorized apps to access sensitive parts of the APK. And last, the recurrent solicitation of dangerous permissions, such as Android. Permission.RECEIVE_SMS indicates an apparent intent to intercept or manipulate SMS messages. This includes the interception of One-Time Passwords (OTPs) and other sensitive information, posing a substantial threat to user security.

Fig. 2 shows one example of the output from MobSF. By conducting further analysis, these vulnerabilities can be mapped against several standards such as CWE, OWASP Top 10, and OWASP MASVS. All APK has been joined and analyzed with other standards compiled in Table II.

TABLE II. PERMISSION, RATING, AND STANDARD ANALYSIS

APK	Permission	Status	Detail
1	-	Medium	**CWE:** CWE-919: Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2
2	-	Low	**CWE:** CWE-312: Cleartext Storage of Sensitive Information CWE-327: Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10**: M9: Reverse Engineering M5: Insufficient Cryptography **OWASP MASVS:** MSTG-STORAGE-14 MSTG-CRYPTO-4
3	android. Permission.RECEIVE_SMS android. Permission.INTERNET android. Permission.SEND_SMS DYNAMIC_REC EIVER_NOT_EX	Medium	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS**: MSTG-STORAGE-2"

APK	Permission	Status	Detail
	PORTED_PERMI SSION0wleumc		
4	android.Permission.RECEIVE_SMS	Medium	**CWE:** CWE-532: Insertion of Sensitive Information into Log File CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG STORAGE-3 MSTG-STORAGE-2
5	Unknown permission from Android reference	Medium	**CWE:** CWE-532: Insertion of Sensitive Information into Log File CWE-919: Weaknesses in Mobile Applications CWE-276: Incorrect Default Permissions CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-312: Cleartext Storage of Sensitive Information **OWASP Top 10:** M1: Improper Platform Usage M2: Insecure Data Storage M7: Client Code Quality M9: Reverse Engineering **MASVS:** MSTG-STORAGE-3 MSTG-RESILIENCE-2 MSTG-STORAGE-2 MSTG-STORAGE-14
6	android.permission.RECEIVE_SMS android.permission.INTERNET Android.permission.SEND_SMS org.traccar.gateway.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSIONpyyynfz ffsrrchepvk	High	-
7	-	Medium	**CWE:** CWE-532: Insertion of Sensitive Information into Log File CWE-276: Incorrect Default Permissions CWE-919: Weaknesses in Mobile Applications **OWASP Top 10:** M2: Insecure Data Storage M1: Improper Platform Usage **OWASP MASVS**: MSTG-STORAGE-3 MSTG-STORAGE-2 MSTG-RESILIENCE-2

TABLE III. TELEGRAM BOT ANALYSIS

APK	Token Access	Id Bot	Phone Number
1	6459124189:AAEZV3zeVoLencdDfmhkovhhI-TNjEotH8 6459124189:AAEZV3zeVoLencdDfmhkovhhI-TNjEotH8	6459124189 5994350601	08121603xxxx
2	6177934854:AAF4gryDahyBSzq3_sanyma1c09qAj38z5I	5855468189	-
3	7118386657:AAGcgkfR0HsocV0M0YScmJ5-6H1WXPSN_mM	6731508414	08219631xxxx
4	6725776355:AAF8CizUYvoW_Syqhp YbisINexwb20y9p84	6839116973	08217980xxxx
5	6933087498:AAHy2b_ysgD5WvSXQwq8W_IYCY97vj0m9GU	6504219137	08082123xxxx 08041523xxxx 08217622xxxx
6	7176012521:AAFeNW488INs_TQWjPSw2GUai4_6bGSd6vk	1479471246	08521915xxxx
7	6658906647:AAFl7CdoHZSXWjBT 58VnvAwXx-102m8Gi40	6859026490	08237977xxxx

B. External Entities Analysis

External entities are the results of the analysis obtained from mapping the relationship between the APK and the telegram bot. The results of the analysis of these external entities, further tracing can be used as evidence that can refer to the perpetrator of the crime based on the number contacted by the telegram bot. Sample external entities analysis of APK number 7 is depicted in Fig.3 .APK code analysis compilation lists in Table 3.

V. CONCLUSION AND FUTURE WORK

The common vulnerabilities exploited in these attacks include:

1) Malicious Code Injection: Embedding harmful code within seemingly benign APKs to execute unauthorized actions.
2) Abuse of Permissions: Malicious APKs often request excessive permissions that go beyond their functional needs, enabling them to access sensitive data.
3) Old OTP Verification Exploits: Utilizing outdated one-time password (OTP) methods to gain unauthorized access.

The diversity of APK phishing methods in Indonesia underscores the adaptability and ingenuity of cybercriminals. The reliance on social engineering, exploitation of current events, and the use of seemingly legitimate APKs to distribute malware highlight the sophistication of these attacks. This calls for a multi-faceted approach to cybersecurity, involving not only technological solutions but also user education (security awareness) and regulatory measures.

Fig. 3. Code analysis

The findings suggest a need for continuous monitoring and updating of security protocols, increased public awareness of digital threats, and stronger collaboration between the governmental and private sectors in Indonesia to effectively combat these evolving cyber threats. Finally, this research provides valuable insights for forensic analysis to trace cybercriminal actors. These insights underscore the broader role of digital forensics in understanding and mitigating the impact of mobile phishing attacks in Indonesia.

REFERENCES

[1] M. Abbasi et al., "In-Depth Analysis of Mobile Apps Statistics: A Study and Development of a Mobile App," in 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), 2023, pp. 1–7. doi: 10.23919/CISTI58278.2023.10211912.

[2] A. A. Shaikh, R. Glavee-Geo, H. Karjaluoto, and R. E. Hinson, "Mobile money as a driver of digital financial inclusion," Technol. Forecast. Soc. Change, vol. 186, p. 122158, 2023, doi: https://doi.org/10.1016/j.techfore.2022.122158.

[3] F. Liébana-Cabanillas, I. García-Maroto, F. Muñoz-Leiva, and I. Ramos-de-Luna, "Mobile payment adoption in the age of digital transformation: The case of apple pay," Sustain., vol. 12, no. 13, pp. 1–15, 2020, doi: 10.3390/su12135443.

[4] R. Marginingsih, W. Widiyanti, I. H. Susilowati, J. Retnowulan, and I. Soraya, "Mobile Payment As Financial Transactions in the Digital Era: An Empirical Analysis," IOP Conf. Ser. Mater. Sci. Eng., vol. 662, no. 2, 2019, doi: 10.1088/1757- 899X/662/2/022133.

[5] A. A. Ajhari, D. F. Priambodo, R. H. Paradisa, and H. Yulianti, "PROCTOR: A Robust URL Protection System Against Fraudulent, Phishing, and Scam Activities," Int. J. Comput. Digit. Syst., vol. 14, no. 1, pp. 1013–1021, 2023, doi: 10.12785/IJCDS/140179.

[6] W. Ali, "Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 9, pp. 72–78, 2017, doi: 10.14569/ijacsa.2017.080910.

[7] A. Mughaid, S. AlZu'bi, A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, "An intelligent cyber security phishing detection system using deep learning techniques," Cluster Comput., vol. 25, no. 6, pp. 3819–3828, 2022, doi: 10.1007/s10586-022-03604-4.

[8] S. Alnemari and M. Alshammari, "Detecting Phishing Domains Using Machine Learning," Appl. Sci., vol. 13, no. 8, 2023, doi: 10.3390/app13084649.

[9] "Bareskrim Tangkap 13 Tersangka Kasus Penipuan APK Andorid, Kerugian Capai Rp 12 Miliar." https://nasional.kompas.com/read/2023/01/19/18211941/bareskri m-tangkap-13-tersangka-kasus-penipuan-apk-andorid-kerugian- capai-rp (accessed Jun. 19, 2024).

[10] "Mobile Operating System Market Share Indonesia | Statcounter Global Stats." https://gs.statcounter.com/os-market-share/mobile/indonesia/#monthly-202302-202402 (accessed Jun. 19, 2024).

[11] Anti-Phising Working Group, "Phising Activity Trends Report," vol. Q1, no. March, pp. 1–7, 2023.

[12] Anti-Phising Working Group, "Phising Activity Trends Report," vol. Q2, no. November, p. 8, 2023, [Online]. Available: https://apwg.org/trendsreports/

[13] C. N. Gutierrez et al., "Learning from the ones that got away: Detecting new forms of phishing attacks," IEEE Trans. Dependable Secur. Comput., vol. 15, no. 6, pp. 988–1001, 2018, doi: 10.1109/TDSC.2018.2864993.

[14] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Frontiers in Computer Science, vol. 3. Frontiers Media S.A., 2021. doi: 10.3389/fcomp.2021.563060.

[15] A. Yusuf, T. Ariyanto, and C. D. Amanda, "Keamanan siber indonesia 2022," Badan Siber dan Sandi Negara, 2022.

[16] "OWASP MASTG - OWASP Mobile Application Security." https://mas.owasp.org/MASTG/ (accessed Jan. 18, 2024).

[17] A. S. Rusdi, N. Widiyasono, and H. Sulastri, "Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis," J. Ilm. Inform., vol. 07, no. 02, pp. 99–107, 2019.

[18] S. Acharya, B. Ehrenreich, and J. Marciniak, "OWASP inspired mobile security," in 2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2015, pp. 782–784. doi: 10.1109/BIBM.2015.7359786.

[19] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, "Mobile Application Security Penetration Testing Based on OWASP," IOP Conf. Ser. Mater. Sci. Eng., vol. 846, no. 1, 2020, doi: 10.1088/1757-899X/846/1/012036.

[20] D. F. Priambodo, G. S. Ajie, H. A. Rahman, A. C. F. Nugraha, A. Rachmawati, and M. R. Avianti, "Mobile Health Application Security Assesment Based on OWASP Top 10 Mobile Vulnerabilities," in 2022 International Conference on Information Technology Systems and Innovation (ICITSI), 2022, pp. 25–29. doi: 10.1109/ICITSI56531.2022.9970949.

[21] T. Borja, M. E. Benalcázar, Á. L. Valdivieso Caraguay, and L. I. Barona López, "Risk Analysis and Android Application Penetration Testing Based on OWASP 2016 BT - Information Technology and Systems," 2021, pp. 461–478.

[22] H. M. Salih and M. S. Mohammed, "Spyware Injection in Android using Fake Application," in 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 100–105. doi: 10.1109/CSASE48920.2020.9142101.

[23] N. Abura'ed, H. Otrok, R. Mizouni, and J. Bentahar, "Mobile phishing attack for Android platform," in 2014 10th International Conference on Innovations in Information Technology (IIT), 2014, pp. 18–23. doi: 10.1109/INNOVATIONS.2014.6987555.

[24] D. F. Priambodo, M. Hasbi, and M. S. Malacca, "Security Assessment Aplikasi Mobile E-Kinerja dengan Acuan OWASP Top 10 Mobile Risks," JEPIN (Jurnal Edukasi dan Penelit. Inform., vol. 8, no. 3, pp. 560–571, 2022.