Borneo International Journal eISSN 2636-9826; Vol. 4 (2); 2018; 17-24
Published by *Majmuah Enterprise*
www.majmuah.com

Review on Current Target of Mobile Attacks

AHMAD MUSTAQIM BAHARIN and MOHAMAD FADLI ZOLKIPLI
School of Computing, College of Art & Sciences, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: ahmad_mustaqim_ba@soc.uum.edu.my, m.fadli.zolkipli@uum.edu.my | Tel: +60194961164 |

Received: June 01, 2021
Accepted: June 08, 2021
Online Published: June 16, 2021

Abstract

Nowadays, the world is in the digital era. The use of the internet, computers, smartphones and other electronic gadgets is increasingly becoming a necessity for all human beings. Various advantages can be used with electronic devices. Smartphones have also established themselves as a common substitute for computers due to their portability, small screen size, and low manufacturing costs. The use of smartphones is greatly increasing among the people day by day. It doesn't matter age or gender. As a result, smartphones have become a target by hackers who want to attack smartphones. In the smartphone market, the most famous operating system for smartphone is Android. This popularity makes it primary target for hackers and hackers. In this review paper, we have studied the current trend of mobile attacks. We also investigated about malicious and types of malwares for mobile attacks and also malware detection techniques of mobile attacks. We also organized a proper table which help to visualized and easy comparison information.

Keywords: Smartphone, Android, Malware, Hacker and Attacks.

1. Introduction

In our daily life nowadays, smartphones seem to be a part of our lives to simplify the task and job. We will use smartphone to make a call, check emails, send a personal message, take a photo, record a video, voice, surf the internet service to socialize and also sometime playing a game for teenagers. From year 2007 until 2018, the end users were purchase the smartphone in total of 7015 million in the world, among which 84.2% of smartphones is powered by Android operating system (MA Rahim Khan, RC Tripathi & Ajit Kumar, 2019). Android have been different version of operating system such as Nougat, Lollipop, Marshmallow and the latest one is Android 11 of called Android “R” that was released on September 8, 2020. Android have their competitor it is iOS. Just 11% of Android users have the newest Android operating system, compared to 86 percent of iOS users (Nagarjun & Ahamad, 2018). However, Android operating system still become the choice of many people in the world. Popularity of Android made them be a most targeted of mobile attacks between another OS.

Smartphone nowadays also have many applications that can allow user to more interactivity and its aim to make easier for human life. Smartphone can perform the bank transactions, store the sensitive, privacy data, transfer the sensitive, privacy data, privacy email, store the note that contain privacy information such as password and more. The most popular functions of smartphone are allowing the user to use internet service such as surfing web and downloading the applications. Mishra and Thakur (2019) noted mobile operating system can be vulnerable to malicious attacks and suffer as a result because their working a lot of application at the time surfing web and the applications are downloaded from the internet. According to Nagarjun and Ahamad (2018) found data from GSMA Intelligence shows around the word, there are 5 billion unique smartphone subscribers and also for mobile internet users in 2017 are 3.3 billion. People are more knowledgeable about different smartphones, their features, and brands but yet they are less knowledgeable about mobile attacks (Nagarjun & Ahamad, 2018).

While these devices offer many functionalities and internet service, they also have a security risk. If more and more data is generated day by day. More amount of data will be more danger with mobile devices. Mobile attacks on smartphones now become a more common (Yadav & Reddy, 2019). There are many different types and malware of mobile attacks which are targeted towards Android. This paper is organized as follows, Section 1, deal with the literature review. In Section 2, we study the current trend of mobile attacks, Section 3 defines malicious and types of malware mobile attacks, section 4 defines the malware detection techniques of mobile attack and section 5 we give conclusion.

2. Literature Review

The number of new malware variants for mobile devices has risen from 17,000 in 2016 to 27,000 in 2017 shows there has been 45% increase in smartphone malware variants for just last one yar. On every day the average 24,000 malicious smartphone was blocked. The endpoint mobile risk is recorded 34% of mobile is rated as a medium for high risk. Update from hopes controlling this risk also shows only 20% of android smartphone are working with new major version and only just 2.3% are working with the recent minor version (Thiruvaazhi & Arthi, 2018). In general, users have certain restrictions when it comes to updating their Android app, such as their upgrade being disabled in a variety of ways. By manufactures itself they consider only the most recent model to receives update. By Google, which update improves error and security. By network provider, they did not increase bandwidth to accommodate the upgrade. As result, almost all operating smartphone have a bug and also the errors, if without the ability to update, they a give a vulnerable to hacker for attack (Mohamed, 2015). In order to access or receive the latest patches of update, the user must always check the update.

The wireless mobile networking world has been rapidly evolving. This evolution is toward to the next generation wireless that follow flow from the wireless being the simply mode of access to be wired network, to all the network that build to supply wireless communications. For this reason, new technology advance can provide new and powerful tools for hackers that can intend to attacks on critical information data. As increasing rely on information systems, network, computer, devices to support critical function in telecommunications, e-commerce, banking. The hacker develops the present substantial barriers and threats on the several systems of the devices (Ahmed & Sallow, 2017). When user surf the internet, the security challenge is screen size such as the web browser that contain address bar has disappear after few second. That’s mean, user can’t check the verified Resource Locator (URL). The secure URL is commonly having an SSL certificate. This case can make attacker to creates an attractive content like ads in which that contain the malicious link (Wright, Dawson Jr, & Omar, 2012).

Operating system for smartphone is designed as a permission-based mechanism to manages the approval and admission from third-party applications to reach critical data. If, all the permission setting request from an app can either be allow by user to install or not. This is the big issue security threats will make the user data vulnerable to leak (Ahmed & Sallow, 2017). To steal the user privacy frequently, one of the common methods for attacker is acquire the elevated privilege of the user smartphone and put the eavesdropping modules to other third-party applications. In this process, the users are interesting to install the malware from attackers and give a sensitive permission setting to attacker. In this case, the attacker was getting the permission can directly obtain the elevated privilege by exploiting the system vulnerabilities (Zhang, Yuanfang, Dianjie & Guangming, 2017). When a user installs an app on a smartphone, the user is presented with a comprehensive list of all the credentials that the app needs in order to run. All of these permission requests are specified in the AndroidManifest.xml manifest file (Chatterjee, Paul, Roy & AsokeNath, 2016).

3. Results and discussion

Current Trend of Mobile Attacks

Using a various of vulnerabilities from outside is made for interferences of attacks. All of this interfering is considered an attack, regardless of whether it is done with software have malware or by exploiting vulnerabilities in smartphone or operating system for mobile. The word "attack" is commonly described the hacker's attempt to gain access to a user's personal information without their knowledge. The first real smartphone attack was started on March of 2010, dual researchers named Vincenzo and Ralf launched the first real smartphone attack, stealing a database from via SMS from smartphone. This attack was carried out by exploiting an error on the Safari Browser on iPhone 3GS phones, with the goal of uploading a file sent via SMS to the server (Yesilyurt & Yalman, 2016).

According to Priyanka and Piyal (2013) noted nowadays, there are various classification in terms of attacks. Becher was one of them classification group attacks towards smartphone in four categories. As an example, Hardware Based Attacks, Device Independent Attacks, Software Based Attacks and User Based Attacks (Priyanka & Piyal, 2013). Hardware Based Attacks are a component of mobile security from a broad perspective. So, if the Mobile Device is vulnerable, it cannot easily access user information; however, the device can be accessed. Second, Device Independent Attacks is that are not reliant on the device and directly target the user of the mobile device. They want to use wireless connections or wiretapping to breach the privacy data. Software Based Attacks are there has been a growth in the number of mobile web browsers has resulted in a rise in the number of vulnerabilities in this sector. User Based Attacks are direct assault on mobile device users carried out by hacking without the use of malicious software (Yesilyurt & Yalman, 2016).

By using encryption by malware. That is ransomware aims to hold a victim's details information at ransom. Ransomware can examine as a serious threat when them arrive to protecting of information data (Muslim, Dzulkifli, Nadhim & Abdellah, 2019).

The number of mobile Ransomware attack from Q1 2018 until Q1 2019 by Humayun, Jhanjhi, Alsayat & Ponnusamy (2020) that found in Q1 2018 the number of Ransomware attack is the only around 9000 attacks and increase slowly to 14,000 attacks for Q2 2018. But, from Q2 2018 to Q3 2018 the data shows number of Ransomware attacks was a little bit decreased in around 1,000 attacks that means from 14,000 to 13,000 attacks. Start from Q3 2018 the data was spike with a lot that to around 2,300 attacks in Q4 2018. The data also shows in Q1 2019 is the highest recorded case for Q1 2018 until Q1 2019 data. Around 2,800 attacks were recorded in Q1 2019 (Humayun et al., 2020). **Figure 1** shows a graph Number of mobile Ransomware Attacks from Q1 2018 until Q1 2019 (Humayun, Jhanjhi, Alsayat & Ponnusamy, 2020).

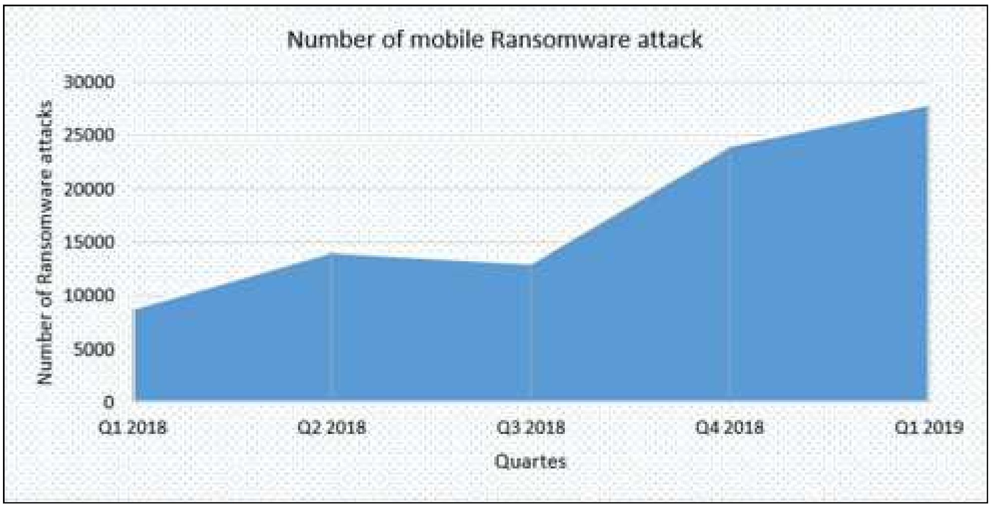

Figure 1 : Number of mobile Ransomware Attacks from Q1 2018 until Q1 2019.

Malicious and Types of Malwares for Mobile Attacks

People nowadays, very excited to download the app that have function for different function including mobile game, social networking, photography and more. In, general user does not take care about the malicious app whether they download apps are either contain malware or not and then user install the app on their smartphone and use the applications. The report form Kaspersky Lap also shows the number of malicious code installation package was increased very extreme in year 2016, a total of 8,526,221 up three times over the last year. For differentiation, from 2004 until 2013, was over ten million malware installation packets is discovered, in 2014 and 2015 each with 2.4 million and 2.96 million (Ahvanooey, Li, Rabbani & Rajput, 2017).

The software security issues on the smartphone OSes are divide to three sections with Malicious Applications, Vulnerabilities and Attack or Threat (Ahvanooey et al., 2017). **Figure 2** shows the Software Security Issues on the Smartphone OSes (Ahvanooey, Li, Rabbani & Rajput, 2017).

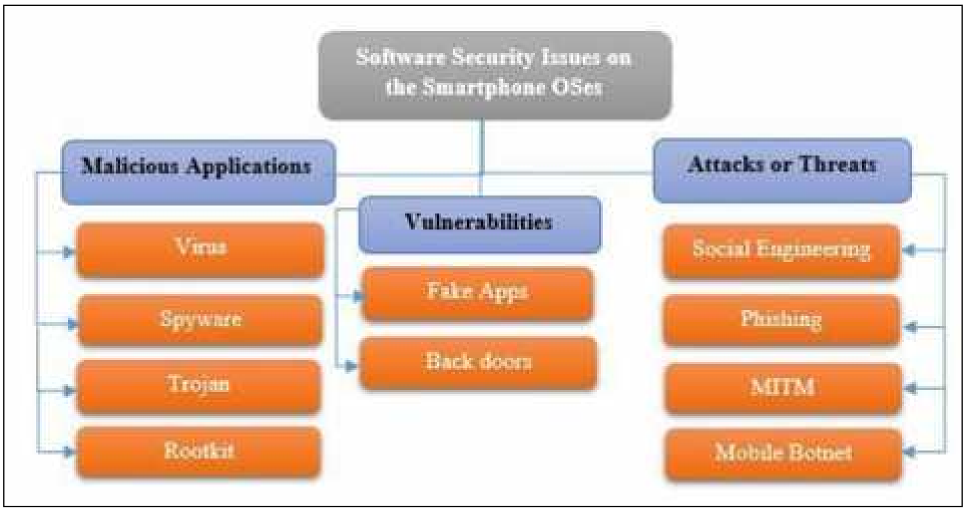

Figure 2 : Software Security Issues on the Smartphone OSes.

Malicious Applications

As we know Malware is a term used to describe malicious malware that focus to steal user data from smartphone user. Basically, Malware have four types which details in following.

Virus

Virus is a malicious app that can imitate or resembles themselves, and their various imitations are capable of infecting other application, by binding (or adding) themselves to boot sectors or files to them (Ahvanooey, Li, Rabbani & Rajput, 2017). In order to be clone the virus in targeted smartphone, the infected application must be sent first to the targeted smartphone and user will performed by itself (Polla, Martinelli & Sgandura, 2013).

Spyware

Spyware also is a malware which control and tracking the targeted smartphone to control user activities like contacts, call, location, voice, email and more. It has ability to deliver data to another place via network or email and can gain control of a user smartphone without realised. The spyware was extremely powerful and reliable allowing hacker to control of victim’s smartphone (Ahvanooey, Li, Rabbani & Rajput, 2017).

Trojan

Trojan is type from malware can allows unauthorised access to confidential information actions form user like pay the transaction, premium call rate at the background targeted smartphone. Therefore, the aim of this malicious app is transmitting the front of original application, file (Marforio, Masti, Sorentio, Kostianen & Capkun 2016). For example, on February 2017, was reported Trojan which name ‘Swearing” was widely distributed of Android user and thief the credentials from bank.

In 2018 the total of mobile ransomware trojans is 60, 176 with 20%. Next, in 2019 was recorded the highest mobile ransomware trojans in among of three years with 68,362 or 30%. Next, in 2020, the data show recorded the lowest mobile ransomware trojans in among of three years with only 20,708 or 10% (Securelist, 2020). **Table 1** show the table Mobile Ransomware Trojans in 2018 until 2020 (Securelist, 2020).

Table 1: Mobile Ransomware Trojans 2018-2020.

Year	Total	Percentage (%)
2018	60, 176	40.32
2019	68, 362	45.80
2020	20, 708	13.88

Rootkit

Rootkit work by hidden process that running at the background of targeted smartphone and develop some malicious flaws by contaminating the operating system. Basically, this malware keep tries to make firewall and also anti-malware not working by keep tries to disable it (Polla, Martinelli & Sgandura, 2013).

Vulnerabilities

In term of mobile attacks, weakness of flaw for vulnerability that allows a hacker to compromise the protection of a smartphone. Vulnerability was defined as the intersection of three factors, it is system susceptibility or flaw, hacker's capability to invoke the flaw, and attacker obtainability to the flaw. For technical term, that have three bases for vulnerability such as a smartphone susceptibility or flaw, hacker ability to extract the flaw, and obtain of hacker to the flaw. Two reasons why vulnerability increase on Android smartphone. First, Android OS is a famous OS that is open-source programme that has a number of security weakliness. User also not care to update their latest patch. Second, not only from official store but user also can download the app from third-party. But these two places also have a certain malware application (Chaudhry, Shafique & Rittenhouse, 2016). User must have knowledge and take time to research about application before they install it.

Attacks or Threats

Intrusions or threats are examples of attack that carried out by malicious programmers who use various insecure vectors in the target OS or apps to gain command of the infected smartphones. Both of these intrusions became known as threats or threats, and they used ransomware apps or bugs in the context of victims' smartphones to gain control of the compromised computer.

Social Engineering

That is a kind of secret trick for revealing personal data information, theft, or the password to a device, and more. This is a type of hacking that entails abusing sensitive information in order to extract sensitive personal details that can be used for malicious purposes (Chaudhry, Shafique & Rittenhouse, 2016).

Phishing Application

Basically, this is a fake application that can imitate like actual apps by posing as trusted client on the targeted smartphone. Phishing apps will compromise user input security in order to steal login credentials. A phishing software, for example, displays a phone mobile banking authentication screen in order to get the user's account credentials like id and password (Chaudhry, Shafique & Rittenhouse, 2016).

Man in The Middle (MITM)

Man in The Middle is a type of stealthy fraud that aims to obtain data by listening on data communication between two smartphones as they speak. The hacker uses various methods to break the direct link into two new lines. First is the hacker and the server have a connectivity. Second is between the targeted smartphone and the hacker. Because of the TCP and HTTP protocols properties, this attack is one of the most powerful attacks (Bicakci, Unal, Ascioglu & Adalier, 2014).

Mobile Botnet

Mobile Botnet deal with group of infected devices that are managed by botmaster through remotely like the normal traffic flow that want prevent by a person without information. It creates a loophole in the planned app that allows attackers to gain full control of the targeted smartphone, and then it starts communicating with it and receiving latest commands from the particular servers. Botnet was thought to be one of the most aggressive types of malware attacks because it can control and utilized any malicious purpose most often is Distributed Denial of Service or (DDoS). For example, the malware known "FalseGuide" was hidden in over 40 applications for guiding mobile games. But this malware ha generates the quiet botnet (Chaudhry, Shafique & Rittenhouse, 2016).

Mobile threat vectors by McAfee found for click fraud have recorded a highest mobile threat vector with 36%. Number 2 from Spyware with 23%. Next, Botnet C&C Activity recorded 22%. Banking Trojans show 12%. Cryptomining 5%. Drop in Root recorded is the lowest in Q1 2018, only 2% (McAfee, 2018). **Figure 3** shows the chart Mobile Threat Vectors according to McAfee Mobile Threat Report Q1 2018 (McAfee, 2018).

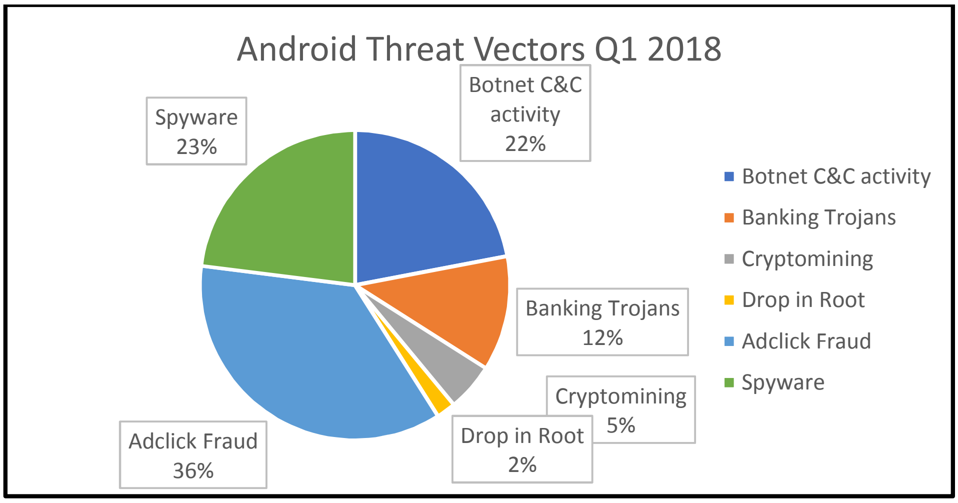

Figure 3 : Mobile Threat Vectors.

Malware Detections Techniques of Mobile Attacks

Detection techniques can be used to investigate malware. Malware analysis is the method of examining malware's code, actions, and features in order to assess the seriousness of an attack. **Figure 4** shows the Malware Detection Techniques by Dua & Bansal (2014) proposed the malware detection techniques basically are grouped to three types such as, Static Analysis, Dynamic Analysis and Permission-Based Analysis (Dua & Bansal, 2014).

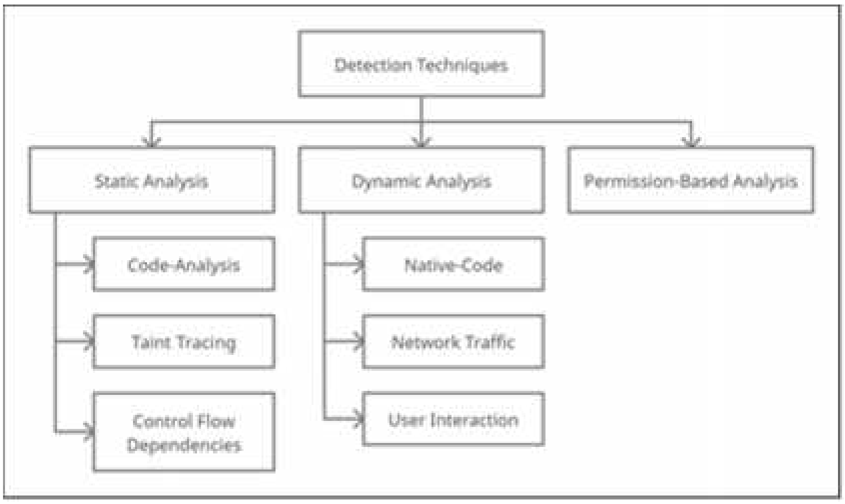

Figure 4 : Malware Detection Techniques.

Static Analysis

Static Analysis is to use to analyze the programs without must run or execute it. The programme is isolated during static analysis by using reverse engineering techniques and systems to recreate the source code and calculations used to create the application. Static examination should be possible through program analyzer, debugger and disassembler (Gyamfi & Owusu, 2018). Static analysis examines the software properties and source code of a downloaded app. Static analysis may employ a variety of techniques, including decryption, decompilation, static system calls analysis and pattern matching. However, obfuscation of apps and encryption methods make static analysis difficult. However, this can be divided into two groups such as Misuse Detection and Anomaly Detection (Dua & Bansal, 2014).

Misuse Detection is based from signature-based approach for tracing malware using security policies and signature matching in a rule collection. The work of each application can be understood by flow of dependency in source code (Dua & Bansal, 2014).

Anomaly Detection can learn malware and predict unknown malware by use machine learning. This step is used to create suspicious application activity, and then observed signatures are compared to a database of standard application behaviour. By training a network with a classifier such as a support vector machine (SVM), it can differentiate between malicious and normal actions (Dual & Bansal, 2014).

Dynamic Analysis

Dynamic Analysis implies running an application in a controlled environment to observe its actions. Dynamic analysis, in comparison to static analysis, allows for the disclosure of malware's normal actions when the code is being examined, making it resistant to obfuscation attempts (Dual & Bansal, 2014). Observing function calls, monitoring the data stream, breaking down function parameters, and tracing path should all be part of a Dynamic Analysis (Gyamfi & Owusu, 2018). Android SDK can be run the android applications; all the features can be done only in emulator run on the computer except generating phone call functions (Dual & Bansal, 2014). For example, Andromly, an Android malware detection system, was proposed. While running, this programme continuously monitors the state of the phone, such as usage of CPU, level of battery and so on, and then uses a machine learning algorithm to tell the difference between malicious and benign apps. For solution will detect continuous attacks and provide a report to the client (Gyamfi & Owusu, 2018).

Permission Based Analysis

Permission is an important role for key to analyzing android applications. While each app is installed, they are specified in the Manifest.xml file. Installing time permissions restricts app activity while maintaining anonymity and reducing glitches and vulnerabilities. Users have the power to approve or disallow the programme installation, but they do not have control of individual permissions. Since the usage of resources in Android phones is focused on these permissions, these permissions are provided in android apps (Dua & Bansal, 2014). On the basis of permissions defined in Manifest.xml, several researchers have been able to detect malicious activity in Android applications.

4. Conclusions

With the rapid growth of the smartphone devices and development of application with a lot of features, as connection, several sensors. The number of malware and attacks is increasing day by day. In the other hand, the spread of malware is accelerating due to a lack of consumer awareness. To reduce malware risks, consumers need to be more aware of malware threats. In this review, first of all, we have reviewed the literature for current trend of mobile attacks. Secondly, we have discussed the current trend of mobile attacks. Thirdly, we have classified the malicious and types of malwares for mobile attacks. Finally, we have defined the malware detection techniques of mobile attacks.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

References

Ahmed, O. M., & Sallow, A. B. (2017). Android Security: A Review. *Academic Journal of Nawroz.*

Ahvanooey, M. T., Li, Q., Rabbani, M., & Rajput, A. R. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, Attacks. *(IJACSA) International Journal Advanced Computer Science Applications.*

Bicakci, K., Unal, Ascioglu & Adalier. (2014). Mobile Authentication Secure Against Man-In-The-Middle Attack. *11th International Conference Mobile Systems Pervasive Computing.*Orlando.

Chatterjee, S., Paul, K., Roy, R., & AsokeNath. (2016). A Comprehensive Study on Security issues in Android Mobile Phone - Scope and Challenges. *International Journal of Innovative Research in Advanced Engineering (IJIRAE).*

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. *International Journal of Security and its Applications .*

Dua, L. & Bansal, D. (2014). Taxonomy : Mobile Malware Threats and Detection Techniques. *Computer Science & Information Technology (CS & IT).*

Gyamfi, N., & Owusu, E. (2018). Survey of Mobile Malware Analysis, Detection Techniques and Tool. *IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).* British Columbia: IEMCON.

Humayun, M., Jhanji, N. Z., Alsayat, A., & Ponnusamy, V. (2020). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*.

Khan, M. A. R., Tripathi, R. C., & Kumar, A. (2019). A Malicious Attacks and Defense Techniques Android-Based Smartphone. *Journal Innovative Technology Exploring and Engineering*.

Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., & Capkun, S. (October, 2016). Hardened Setup of Personalized Security Indicators to Counter Phishing Attacks in Mobile Banking. *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices.* New York: SIGSAC.

McAfee. (2018). *McAfee Mobile Threat Report Q1 2018.* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf

Mishra, S., & Thakur, A. (2019). A Survey on Mobile Security Issues. *Proceedings of Recent Advances in Interdisciplinary Trends in Engineering & Applications (RAITEA)* . India.

Mohamed, I. (2015). Android vs. iOS Security: A Comparative Study. *12th International Conference on Information Technology - New Generations (ITNG).* Nevada: ITNG 2015.

Muslim, A. K., Dzulkifli, D. Z., Nadhim, M. H., & Abdellah, R. H. (2019). A Study of Ransomware Attacks: Evolution & Prevention. *Journal of Social Transformation Regional Development.*

Nagarjun, P. M. D., & Ahamad, S. S. (2018). Review of Mobile Security Problems and Defensive Methods. *International Journal of Applied Engineering Research*.

Polla, M. L., Martinelli, F., & Sgandurra, D. (2013). A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials*.

Priyanka, V. K., & Payal, N. I. (2013). Internal structure of iOS and Building tools for iOS apps. *International Journal Of Computer Science And Applications* .

Securelist. (2020). *Mobile Malware Evolution 2020.* https://securelist.com/mobile-malware-evolution-2020/101029/

Thiruvaazhi, U., & Arthi, R. (2018). Threats to Mobile Security and Privacy. *International Journal of Recent Technology and Engineering (IJRTE).*

Wright, J., Dawson, M. E., & Omar, M. (2012). Cyber Security and Mobile Threats: The Need for Antivirus Applications for Smartphones. *Journa Information System Technology & Planning*.

Yadav, A. M., & Reddy, B. I. (2019). Android Device Attacks and Threats. *International Research Journal of Engineering and Technology (IRJET).*

Yesilyurt, M., & Yalman, Y. (2016). Security Threats on Mobile Devices and their Effects : Estimations for the Future. *International Journal of Security and Its Applications.*

Zhang, D., Guo, Y., Guo, D., & Yu, G. (2017). Privacy Leaks through Data Hijacking Attack on Mobile Systems. *ITM Web of Conferences.*