Borneo International Journal eISSN 2636-9826; Vol. 4 (2); 2021; 8-16
Published by *Majmuah Enterprise*
www.majmuah.com

Review on Mobile Attacks: Operating System, Threats, and Solution

[1]SITI NURAISYAH ZAKARIA and [2]MOHAMAD FADLI ZOLKIPLI
[1,2]School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA
Email: [1]siti_nuraisyah_za@uum.edu.my,[2]m.fadli.zolkipli@uum.edu.my | Tel: +60177247779 | Fax: +608123456 |

Received: May 10, 2021
Accepted: May 27, 2021
Online Published: June 16, 2021

Abstract

Obviously, smartphones and other mobile devices have replaced personal computers (PCs). They have become part of users' personal and business lives. Therefore, they involve with security issues as well as mobile attacks issues have arisen nowadays. Not only to individuals but government agencies and many companies become the victim of these malicious attacks. As these devices are widely used to access and stored sensitive personal information, this would be a big concern. Other that that, during this pandemic user always use smartphone for important transaction such as online banking and online purchases. The vulnerability of the attacks is high, especially when unsuspecting users being the targets. Companies could lead to huge loss, when it is due to data leakage or losing data resources that use to protect the organization. In fact, malicious attacks on mobile devices are considered high rather than PCs. However, these attacks have been severed due to the ignorance of users who fail to enable the security setting in their phone. This paper discusses mobile security on operating system followed by some discussion on various attack on mobile devices. The discussion intended to give solutions by reduce the mobile attacks.

Keywords: Mobile security, malicious target, threats

1. Introduction

Smartphone is one of technology that the most important thing we should have, and it provided a plethora of capabilities like personal computer (PCs). As the growth of technology, there are many smartphone companies competing in offering the best network connection. This abundance of properties has become the new ideal target for the malicious attacks on the devices (Shaik et al., 2015). Fundamentally, mobile operating system can be the top target of malicious attacks. It is because running a lot of application in the background while surfing the internet. Besides, downloading any apps or source form the internet also can be the reason of malware attacks. Because of that, mobile security very important as protection of mobile devices from threats of wireless computing. These days, businesses and smartphone's user like to save their personal and business information in their phone. For companies, these growths of technologies are causing problem in the organization and become the new target of attacks. All type of mobile devices are preferred targets of attacks because anything could be in the devices such as photos, login credentials, and more (Mavoungou et al., 2016). For attackers, this would such a good opportunity to access everything they want to know. This is the reason mobile devices need to be secured before becoming the new target of malicious attacks.

According to Kaspersky's report in December 2016, Attacks on Android devices accounted for 36% of all Internet banking attacks in 2016, up 8% from 2015. In 2016, all Internet banking attacks exceeded US$100 million. Stolen all over the world. Although the Android operating system has become more and more popular recently, the availability of open-source software makes it more vulnerable to attacks because everyone can develop applications freely. Malware authors (or developers) can use these features to develop malicious applications. Due to malicious applications, smart phones are vulnerable to phishing, hijacking, hackers, and other malicious activities without the user's knowledge (Melicher et al., 2016). Since mobile operating systems can be installed on other mobile devices such as tablets and phablet phones, there are repeatedly alike security issues. For instance, mostly users have downloaded and installed third-party applications such as games and photo applications. Therefore, the possibility of installing malicious and adware applications has also increased. Generally, for bank transfers, such as online banking and online shopping, cell phones are used. Furthermore, great writers may use more fake apps, for example, malicious apps that target real apps to make huge profits.

This paper will organize into 5 section as follow. **Section 2** is a literature review of mobile operating system. **Section 3** describes different types of mobile devices threats. **Section 4** discusses solution to mobile devices attacks or threats. Finally, in **section 5**, the conclusions are drawn.

2. Literature Review

Mobile Operating Systems

Smartphone operating system (or mobile operating system) is the system software that can be run on devices such as smartphones, tablets, phablets, and other supporting devices (Yesilyurt et al., 2016), so that you can run other applications designed for the platform. The operating system of a smartphone controls which features are available on the device, such as the keyboard, role, WAP, application synchronisation, and so on. Technically, it adds a layer to the system that allows users to start apps, schedule tasks, and monitor things like network connections and output peripherals. The common smartphone operating systems is Android, iOS, Samsung, Symbian, BlackBerry, and Microsoft's Windows Phone. Now, there are variety of third-party apps on market store (Aron et al., 2015). Other than that, some default apps have been installed into OS such as email, web Browser, etc. Mostly, malware applications are disguised as fake apps under the real applications in devices, but users do not know whether it is real apps or malware apps. Google Play store is the market store for Android, Microsoft Store for Windows phone, and Apple Store for iOS. Basically, the online markets (app store) will check the apps by some anti-malware before sharing it in the app store. As we know, in many of mobile operating system there are two OSes that widely used, which is iOS (formerly iPhone OS) and Android.

Android and IOS

Android is a mobile operating system built on a changes version of the Linux kernel and other open-source applications, designed sepecially for touch-screen mobile devices (Yewale et al., 2016). Android was developed by Open Handset Alliance and sponsored by Google. As shown in Figure 1, Android architecture has four main layer which is System Applications, Application Framework (JAVA API), and Libraries.

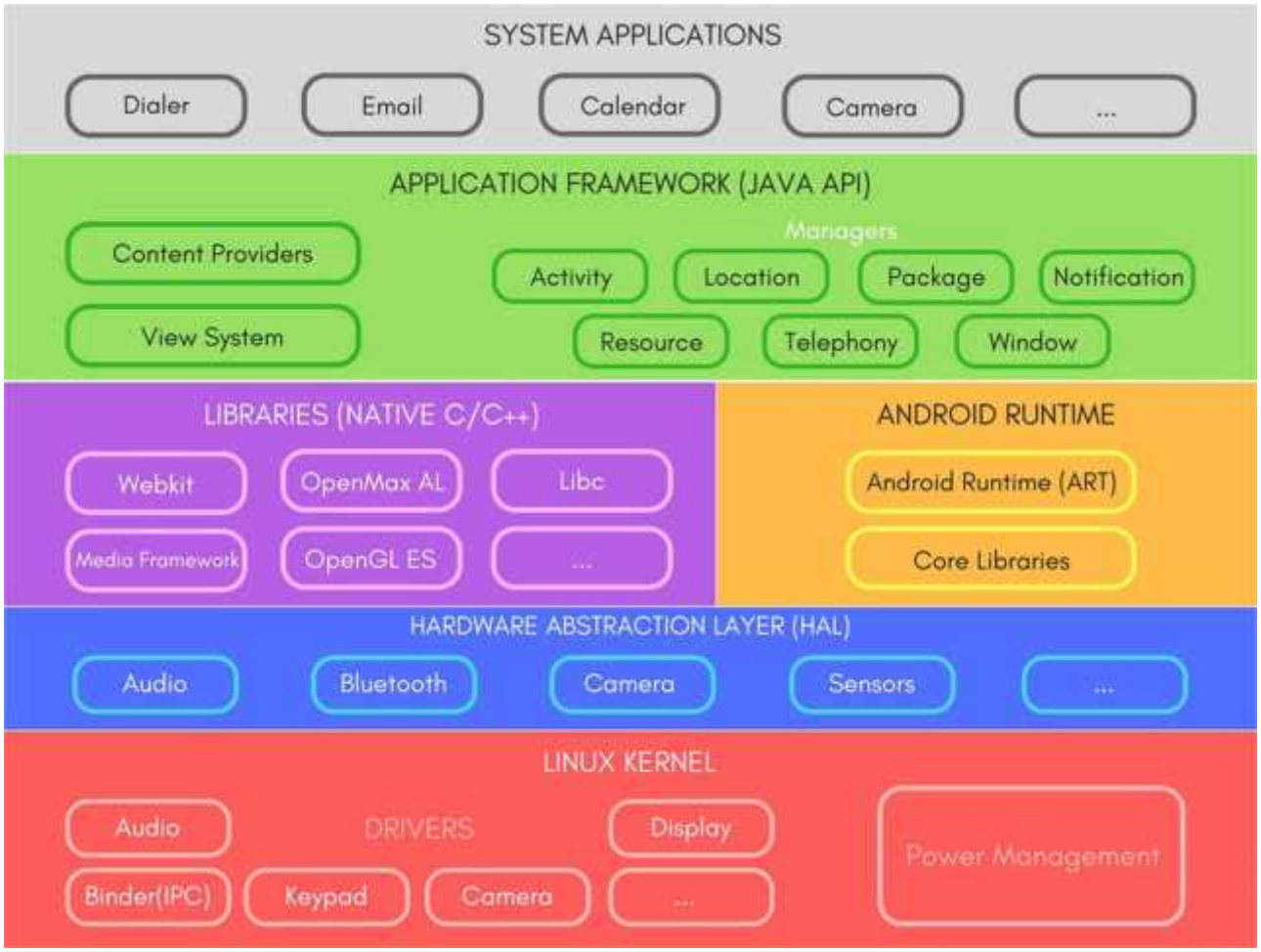

Figure 1: Android architecture

Android's architecture is built around the Linux kernel. It oversees managing all of Android's drivers, including memory, camera, and display drivers, Bluetooth, and audio drivers, among others, that are required during runtime. Platform layers include C/C++ core libraries and java-based libraries like SQLite, Media, and Webkit, among others. The Android runtime, which contains the core library and the Dalvik virtual machine, is an integral part of Android rather than an internal computer. The Android Runtime is the engine that underpins the application system and supports the application libraries. The Dalvik Virtual Machine (DVM), like the Java Virtual Machine, is a registry-based virtual machine (JVM). It is designed and optimised for Android to ensure that multiple instances will run smoothly on the system. The standard programming language JAVA was used to implement Android applications with the most important Android runtime library. Furthermore, to write Android applications using the standard Java language, developers need several core libraries provided by the Android Runtime.

Many resources are obtained by the layers in the Java API Framework for applications that use Java classes. These resources are available to developers to use in their applications. The framework structure also includes main resources such as an operations manager, a content provider, a resource manager, a notification manager, a display system, and so on. Furthermore, Android has a number of System Applications for contacts, messages, emails, calendars, web browser, and so on. The platform's apps have no special status in comparison to the applications that the user wishes to install. A web server, a regular keyboard, and so on. System systems serve as end-user applications, providing key features that developers can call from their own programmes. For the security of Android users, in Android 6.x, Google includes a device access control form that enables users to activate or disable application permissions. This access can also be used to handle tedious adware applications. This is a good way to keep malicious apps from getting unauthorised permissions, but most users do not know how to get permissions (Divya et al., 2016). according to the (Kaspersky, 2019) Kaspersky's web antivirus have detected malicious object that reach 24, 610,126 compare to last year. Over the reporting period, in 2019 malware variety grows by 13.7%.

Apple iOS was developed by Apple and was first released in 2007 (Lee et al., 2015). iOS was written in C++, Objective-C, and swift assembly language. iPhone OS was very tightly guarded. Therefore, only some apps that approve by Apple can be downloaded into iPhones. This helps to ensure the security of the devices while Android is more open to mobile attacks, thus everybody can develop apps freely. As shown in Figure 2, iOS contains four layers. In iOS, the lower layers provide basic services, while the higher layers provide a more complex GUI (Ahvanooey et al., 2020).

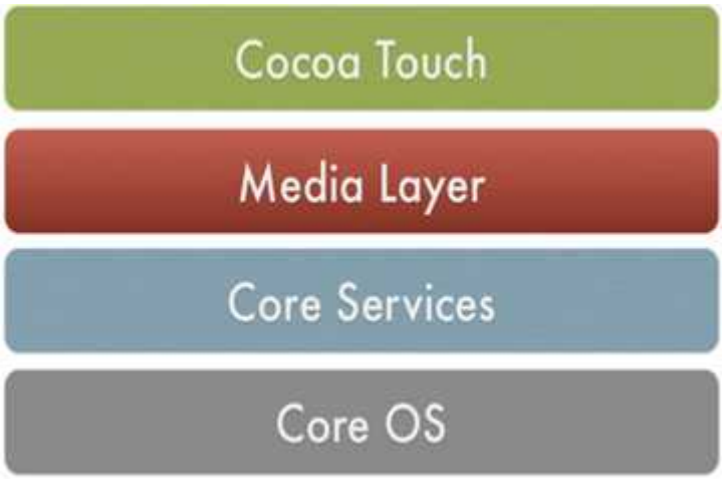

Figure 2: iOS layer architecture (Ahvanooey et al., 2020)

Low-level functions such as acceleration framework, external accessory framework, Bluetooth framework, and so on are all included in the Core Operating System. The accelerate platform, for example, includes interfaces for computing DSP, linear algebra, and image processing (Squires et al., 2016). Cloud Kit architecture, address book structure, kernel location structure, and other general functions that can be used by all applications make up the Core Services. Cloud Kit, for example, offers a way to share data between user devices and iCloud. Unique interfaces for low-level data forms, network links, start-up, and access services are also included. These interfaces are typically C-based and kernel-oriented, and they support SQLite, POSIX streams, and UNIX sockets, among other technologies.
A play collection, a card set, IAD, UIKit, and view controllers are all included in the Media Layer. It also has a data area that can be used to store audio, animation, video, text, and images in PNG and JPEG formats. Finally, Cocoa Touch is made up of many important frameworks for developing iOS applications. Contact, multitasking, and

augmented reality are only a few of the core innovations supported by these networks. Many conventional system services are still available, such as push alerts. When developers want to make apps, for example, they must do more research into the technologies of this layer.

IOS architecture is based on the bottom layer functions of the core operating system (Mohamed et al., 2015). It includes Frameworks for Bluetooth, remote accessories, acceleration, monitoring services, local permission, and so on (Demetriou et al., 2017). For core services, there are several platforms available, such as Cloud toolkit architecture, master data platform, central location framework, and so on. At the media level, the middle structure offers placement and support; it includes Core Graphics platform, Core animation, and AV Kit are all included in the AV Kit package. It contains data areas for audio, text, animation, and image formats such as PNG and JPEG, in other words.

Although Apple's security is solid, iOS offers a number of APIs for developers to use to perform security functions. The Popular Data Protection Architecture (CDSA) is used by IOS to perform security functions such as Desktop copy and file permissions for low-level attributes, which are handled by UNIX-based kernel (BSD). Furthermore, CDSA offers higher-level features, such as, encryption, secure data storage, and authentication are all important features. Users of iOS devices have no control over the access permissions that apps need to access their data. In reality, iOS only allows a limited number of third-party device permissions, which is necessary for an application sandbox, which allows each app to operate independently of other iOS applications. Furthermore, iOS has the ability to restrict access to device subsystems (Mohamed et al., 2015). Basically, iOS policy is in charge of managing the application's permissions without prompting the user. In certain instances, iOS often allows the computer user to accept access to those services. Receiving Internet alerts, accessing location data (GPS), sending messages or email, and initiating extroverted calls are all examples of these permissions. Despite the fact that Apple iOS has the following features like security mechanisms, defence against malicious software, on the other hand, continues to develop as new methods of overwriting actual applications are adopted.

Windows Phone

Windows Phone is a mobile operating system developed by Microsoft for wide-screen smartphones. The most recent updates for WP 8 and Windows 10 are now available. Windows Phone 7 was first introduced in 2010, and the most recent updates for WP 8 and Windows 10 are now available. It also allows multitasking and the downloading of third-party applications and devices, and it deals with big-screen computers, phablets, and X-Box (Yesilyurt et al., 2016). The Microsoft Lumia, which received the Windows 10 beta edition which is updated in February 2015, is the first of this series of Microsoft smartphones. Only smartphones and tablet phones with ARM processors or architectures will run Windows 10 Mobile. Developer tools were introduced by Microsoft. Some iOS devices are simple to port. Microsoft Visual Studio can be used to build WP applications in Visual Basic.NET and C# (Zaidi et al., 2016). Windows 10 Mobile uses the identical authentication measures as the Windows 10 operating system to guard from new security attacks (PC). These programmes provide Windows Hello for business, Windows Information Protection, and anti-malware software.

a) *Windows Hello:* Allows only approved users to access data and services by providing identification and access control functions. It also uses supporting devices that include PIN and biometric authentication methods, as well as a stable implementation of multi-factor authentication (MFA).
b) *Windows Information Protection:* When sharing with apps and personal data, this technology will be enabling automatic data isolation to preserve company information.
c) *Anti-Malware Software:* This useful technology applies layered protection, such as the boot process, hardware devices, and application platform to minimize malicious threats.

Symbian

It is a discontinued mobile operating system originally released by Symbian Ltd. in 1998. As of the end of 2010, Nokia, Sony Ericsson, and Motorola mainly used the operating system through their UIQ user interface. The Symbian Foundation was disbanded at this stage, and Nokia regained control of the operating system's growth. Nokia is the only organisation outside of Japan that still supports Symbian as of February 2011. Furthermore, Japan has confirmed that Its preferred mobile platform is Microsoft Windows Phone 7. Todays, some Japanese mobile phone manufacturers also use Symbian OS on their phones and sell them in Japan.

3. Threats

Smartphone user is exposed to different types of threats when related to their phone. These attacks can disturb the system of the smartphone and filter out the data. Malicious programmes are undetectable malware that runs in the context of the victim's smartphone (Spreitzer et al., 2017). They may also be used to receive new instructions by launching them or connecting them to other networks. It may also tamper with the user's device and create such outcomes, such as data theft and account control.

In addition, since user cannot guess whether the apps could be malware because they were hidden under the normal apps, permissions and accessibility should be limit. For example, close location information in the background, prevent the transmission of data on the network connection, etc. The common attacks were known malware (Chen et al., 2018). Malware is a malicious software that attack mobile OS and steal user information data. It can perform numerous of harmful operations, which might damage system's operation, steal sensitive information, provide unauthorized access, etc. In this case, malware apps categorized into four types which is viruses, worms, Trojan, and spyware.

a) *Virus* is a program designed to enter the computer and change the data. It may damage or delete the data and virus can imitate themselves. Viruses are more dangerous than worms because worms can simply copy but do not make any changes to the data. It can enter to mobile devices in the form of greetings, video or audio files and attached pictures. Besides, virus can also occur via internet downloads.
b) *Spyware* is a software with malicious behavior that gather all user or companies' information and send it to other agencies in a way that could be harm for user. For example, invading the user privacy or harm the system's security.
c) *Worm* is a malicious software that can spread through the network. Worm can cause damage, for example, using viruses, vulnerabilities in security software, stealing confidential information, damaging files, and creating gaps in remote system access. Storage and bandwidth often lead to overloading and overloading of affected servers, networks, and individual systems. Worms are not viruses. The virus requires a host or operating system. Work independently, including network sharing, communication functions, email attachments or links to malicious websites. Internet worms are usually developed to take advantage of new security issues and find systems that do not have the latest operating system or software security updates installed.
d) *Trojan* is a kind of malware that usually disguised as legitimate software. Attacker or hacker can use Trojan to gain access of user's system. They often force users to download and execute Trojan on their system devices. Once Trojan has been activated, it can allow hacker to spy on user, steal sensitive data and access the system through backdoor.

An attack is an intruder or threat from an intruder. Furthermore, various vulnerable vectors are used in the target operating system to control the afflicted device. Any one of these interventions are often referred to as attacks or threats. Malicious applications or vulnerabilities in the background of the user's smartphone. Usually, they are created by malicious writers to be able to access them and provide information without the user's concerns.

a) *Phishing* applications may intercept information about the victim's account and information stored on the device. It is similar like real applications such as online banking applications which designed to steal information like usernames, password, credit cards, etc. For example, phishing applications may disguise as fake online banking login screens to steal user's account and password. According to (Shahriar et. al, 2015) this kind of techniques was the common one which have become a constant threat. As a result of spam and phishing in 2020 by Kaspersky, the Kaspersky anti-phishing has blocked 434,898,635 attempts at scam sites. The most common target of phishing attacks was online store which is 18.12%.
b) *Man-In-The-Middle (MITM*) is the general term for an attacker, through eavesdropping or claiming to be one of the participants, it inserts itself into the interaction between the recipient and the programme, emulating an interchange. This is common knowledge. The attack's aim is to capture personal data including user credentials, account details, and credit card numbers (Mirza Abdullah et al., 2018). Financial device consumers, SaaS businesses, e-commerce websites, and other websites that need logging in are usually the targets. Identity fraud, fraudulent fund withdrawals, and illicit password changes are also possible uses for the details gained during the attack. Advanced Persistent Threats (APT) may also be used to establish a foothold during the penetration process. Generally, a MITM attack is equivalent to the postman opening your bank statement and entering your details. Keep the account, then seal the envelope and deliver it to the door. As shown in Figure 3, hacker creates new connection between the victim's devices and the server in online banking transactions (Ahvanooey et al., 2020).

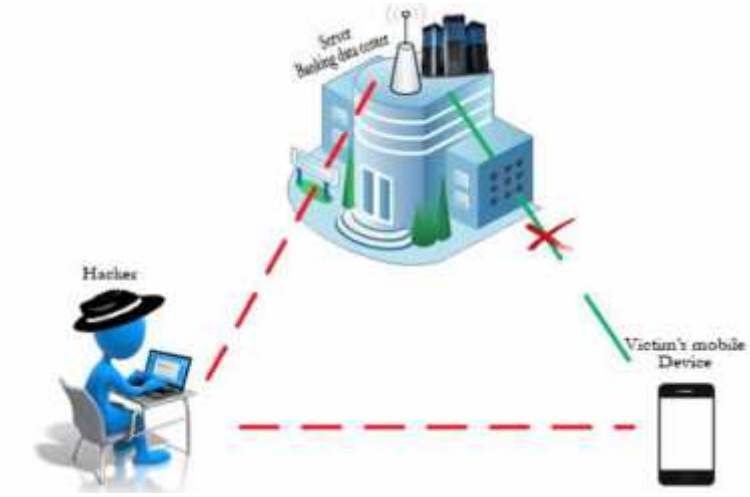

Figure 3: example of MITM attack (Ahvanooey et al., 2020)

c) *Mobile Botnet* is a network of infected mobile devices with malicious software and controlled as a group without the user's knowledge (Cusack et al., 2016). Botnets are one of the most risky forms of threats from the perspective of hackers, since they can be used and run for a range of malicious reasons, for instance Distributed Denial of Service or spam attacks. When a huge number of computers want to connect to a node at the same time, something happens (Bernardeschi et al., 2019). The server's ability to manage all incoming requests will be harmed as a result of this process, thus making it inaccessible to user who wish to use the service. For example, sign of being infected by botnet is system's behaviour become strange, the devices may lag more often and reboot itself, and device's system become slower.

4. Countermeasures

This section will introduce some mechanisms that can be used to prevent different types of smartphone attacks. Besides, existing method for detecting malware will be present, and some countermeasures will be introduced to reduce mobile malicious attacks.

File permissions, sandboxes, and other security features are available on Android and iOS. To strengthen the protection of the user, these safety measures are not appropriate for preventing new malicious attacks as a result of sudden attacks on smartphones (Sivaraman et al., 2016). Clearly, existing mechanisms haven't been able to detect new malware that hasn't been identified before, and further improvements are needed against these attacks. From the perspective malware can be classified into two types in terms of detection, Unknown malware: This is a category of malware that has yet to be located by anti-malware, and malware transformation: Known malware with the following characteristics: produce the same behaviour and a different interface.

The combination of many existing free applications and unknown malicious code makes it difficult to manually detect malicious applications, which is almost impossible for network security analysts. For malware detection applications, a variety of techniques have been implemented. Signature-based methods, machine learning or behavioural detection methods, and anomaly-based methods are the two broad categories of malware detection methods (Alwahedi et al., 2016).

a) *Signature-based methods:* malware detection technique that uses signatures to distinguish specific patterns of known malware. The signature-based approach generates a specific signature for known malware, which can be used to identify malware by comparing the newly discovered malware signature to a signature database previously established. The disadvantage of this method is that if the malware creator makes minor changes to the new version of the malware, the signature will be completely changed or not changed. To solve this problem, cybersecurity researchers have introduced behavioural, or machine learning classifiers based on the functions extracted from the application during trend and constant analysis.

b) *Machine learning methods:* Machine learning algorithms are used in this form of malware detection technology to create learning patterns that can detect unwanted malware (or new malware) as well as existing malware using examples of harmless malware. When compared to methods that rely on signatures for detecting new malware, they are more effective because their accuracy depends on the features used and the training set of templates generated using constant analysis (chen et al., 2018). For dynamic analysis, machine learning use algorithms to extract features, so that many malicious applications in the operating system run on

virtual or real devices, and after the application runs for a set period, the algorithm can generate a log function composed of dynamic behaviours that occur in the application that been tested before. Therefore, these methods can generate training patterns for feature extraction to detect malware at the run apps.

c) *Anomaly-based methods:* This approach involves tracking system behaviours and categorising them as normal or pathological in order to detect interference and harassment on networks and machines. Heuristics or laws, not patterns or signatures, are used to classify objects (Alwahedi et al., 2016). Unlike a signature-based approach, it tries to detect some form of aggression that is beyond the system's usual operating range. The system must learn to understand regular system behaviour in order to correctly distinguish attack traffic. A preparation process (creating a profile displaying normal behaviour) and a monitoring phase are the two stages of most anomaly-based approaches (compare the current traffic with the profile created during the training phase). Anomalies can be found in a number of ways, the majority of which depend on artificial intelligence. Artificial neural network systems have had a lot of popularity. Another approach is to use a detailed mathematical model to decide what standard device use entails, and to mark any deviation as an assault. This is what is referred to as "strict anomaly identification." Other methods for identifying anomalies include data processing, syntax, and artificial immune systems.

Nowadays, users thought malicious apps as a threat only to PCs and laptops. However, since most users have switched to smartphones, cybercriminals are increasingly targeting these devices. Several issues and vulnerabilities related to mobile malware, so how can users tackle these problems by securing their devices. In this part, we introduce solutions to protect mobile device and prevent malware attacks (Ahvanooey et al., 2020).

a) *Install the application from a trusted source.*
Users have to download applications and install from reputable app stores such as Apps Store, Google Play Store, etc. If user want to download an application or game, user can safely choose an application or game with a score (5 stars) and a good feedback.

b) *Update your mobile operating system.*
Since there are several limitations to upgrading the Android operating system, updates may be prevented in a number of ways: by the manufacturer (who might only accept updates for the most recent models); by Google (which is used to update or improve security or operating system errors); or by the network provider (cannot expand its network bandwidth to support updates). As a result, almost all mobile operating systems contain bugs, making them vulnerable to criminal attacks if they are not modified. The best recommendation for consumers is to search for software changes with current patches on a regular basis (such as security patches).

c) *Avoid from Root (Android) and Jailbreaking(iOS)*
Users who jailbreak their iOS devices or gain root access on their Android devices gain access to a variety of useful features that would otherwise be inaccessible, but they often become more vulnerable to malicious attacks. The information you carry on these devices is usually very confidential and if you are not sure about the risk you are taking, please do not do it. The process itself is usually very simple. What is interesting is that jailbreaking an iPhone is much easier than rooting it on thousands of different Android terminals. This is important to some people, but it user have to faces the risks if anything happen to their devices.

5. Conclusions

To secured mobile devices from continues to be threatened by malicious attackers who gain unauthorized access. Devices attacks like malware, phishing, viruses, denial of service attack (DoS), spoofing, etc. These can be tackled by using appropriate software such as anti-virus Kaspersky, firewall or encryption. Although, all the solution has certain shortcoming, other measures need to be taken to overcome this limitation (Alwahedi et al., 2016). However, users also must be knowledgeable in this area, they should be aware of security issues, not just downloading and installing the applications on their devices. An investigation should be made before doing anything to risky, user should take seriously about security warnings issued by the system (Aonzo et al., 2018). In short, there are many countermeasures to prevent mobile devices attacks. However, due to the continuous development of malware world, this is necessary step for user to be aware of this problem so they can protect their own devices.

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

Ahvanooey, M. T., Li, Q., Rabbani, M., & Rajput, A. R. (2020). A survey on smartphones security: software vulnerabilities, malware, and attacks. *arXiv preprint arXiv:2001.09406*.

Alwahedi, S., Al Ali, M., Ishowo-Oloko, F., Woon, W. L., & Aung, Z. (2016, October). Security in mobile computing: attack vectors, solutions, and challenges. In *International Conference on Mobile Networks and Management* (pp. 177-191). Springer, Cham.

Aron, L., & Hanacek, P. (2015, March). Overview of security on mobile devices. In *2015 2nd World Symposium on Web Applications and Networking (WSWAN)* (pp. 1-11). IEEE.

Aonzo, S., Merlo, A., Tavella, G., & Fratantonio, Y. (2018, October). Phishing attacks on modern android. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1788-1801).

Android Architecture, Retrieved May 7, 2021, https://developer.android.com/guide/platform/index.html

Bernardeschi, C., Mercaldo, F., Nardone, V., & Santone, A. (2019). Exploiting Model Checking for Mobile Botnet Detection. *Procedia Computer Science*, *159*, 963-972.

Chen, S., Xue, M., Fan, L., Hao, S., Xu, L., Zhu, H., & Li, B. (2018). Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach. *computers & security*, *73*, 326-344.

Cusack, B., Lutui, R., & Khaleghparast, R. (2016, December). Detecting slow ddos attacks on mobile devices. In *The 27th Australasian Conference on Information Systems*. Australasian Conference on Information Systems (ACIS).

Demetriou, S., Zhang, N., Lee, Y., Wang, X., Gunter, C., Zhou, X., & Grace, M. (2017). Guardian of the HAN: Thwarting mobile attacks on smart-home devices using OS-level situation awareness. *arXiv preprint arXiv:1703.01537*.

Divya, K., & Kumar, V. K. (2016). Comparative analysis of smart phone operating systems Android, Apple IOS and Windows. *International Journal of Scientific Engineering and Applied Science (IJSEAS)*, *2*(2), 432-439.

Kaspersky Lab Threat Review for 2016, Retrieved April 24, 2021, http://usa.kaspersky.com/about-us/press-center/press-releases/2016/Kaspersky_Lab_Threat_Review_for_2016_servers_for_sale_global_botnets_and_a_strong_focus_on_mobile

Lee, Y., Heo, I., Hwang, D., Kim, K., & Paek, Y. (2015, June). Towards a practical solution to detect code reuse attacks on ARM mobile devices. In *Proceedings of the Fourth Workshop on Hardware and Architectural Support for Security and Privacy* (pp. 1-8).

Li, H., Zhu, H., Du, S., Liang, X., & Shen, X. (2016). Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing*, *15*(4), 646-660.

Mavoungou, S., Kaddoum, G., Taha, M., & Matar, G. (2016). Survey on threats and attacks on mobile networks. *IEEE Access*, *4*, 4543-4572.

Mirza Abdullah, S., Ahmed, B., & M Ameen, M. (2018). A new taxonomy of mobile banking threats, attacks and user vulnerabilities. *Eurasian Journal of Science and Engineering*, *3*(3), 12-20.

Mohamed, I., & Patel, D. (2015, April). Android vs iOS security: A comparative study. In *2015 12th International Conference on Information Technology-New Generations* (pp. 725-730). IEEE.

Melicher, W., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., Ur, B., ... & Mazurek, M. L. (2016, May). Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 527-539). Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J. P. (2015). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *arXiv preprint arXiv:1510.07563*.

Noureldien, N. A., Saeed, S. K., Salih, M. A., & Ahmed, A. M. (2015). Survey of mobile ad hoc networks attacks and a new classification scheme.

Rastogi, V., Shao, R., Chen, Y., Pan, X., Zou, S., & Riley, R. (2016, February). Are these Ads Safe: Detecting Hidden Attacks through the Mobile App-Web Interfaces. In *NDSS*.

Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of Information Security*, *6*(03), 206.

Sivaraman, V., Chan, D., Earl, D., & Boreli, R. (2016, July). Smart-phones attacking smart-homes. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (pp. 195-200).

Squires, W., & Centonze, P. (2016, May). Cross-platform access-rights analysis of mobile applications. In *Proceedings of the International Conference on Mobile Software Engineering and Systems* (pp. 295-296).

Securelist by Kaspersky on December 2019, Annual Threats Statistics, Retrieved April 23, 2021, Available: https://www.kaspersky.com/about/press-releases/2019_malware-variety-grows-by-137-in-2019-due-to-web-skimmers

Securelist by Kaspersky on February 2021, Spam and Phishing in 2020, Retrieved April 24, 2021, Available: https://securelist.com/spam-and-phishing-in-2020/100512/

Windows 10 Mobile security guide, Retrieved May 8, 2021, https://docs.microsoft.com/en-us/windows/device-security/windows-10-mobile-security-guide

Yesilyurt, M., & Yalman, Y. (2016). Security threats on mobile devices and their effects: estimations for the future. *International Journal of Security and Its Applications*, *10*(2), 13-26.

Yewale, A., & Singh, M. (2016, May). Malware detection based on opcode frequency. In *2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)* (pp. 646-649). IEEE.

Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A survey on security for smartphone device. *International journal of advanced computer science and applications*, *7*(4), 206-219.