A brief review of attacks and mitigations on smartphone infrastructure

Rico Setyawan, Allicia A. Rahayu, Nur Annisa K. F., Amiruddin Amiruddin *
Sekolah Tinggi Sandi Negara, Bogor, Indonesia

* amir@stsn-nci.ac.id

Abstract. The increasing number of smartphone users will encourage competition among smartphone manufacturers in innovating and marketing their products. Such competition can create open space for attackers to understand how smartphones work and then spread threats through malicious programs. In this study, a brief review of various threats and mitigations is carried out on smartphones infrastructure, especially on several well-known brand smartphones.

1. Introduction
Smartphone users in the world have reached more than 5 billion in 2017 and it is estimated that this number will reach 5.9 billion in 2025, equivalent to 71% of the world total population [1]. This is in line with the large percentage of total digital time on smartphone use. The top five countries that have the highest percentage of total digital time using mobile phones are Indonesia (90%), India (86%), Mexico (75%), Brazil (73%), and Argentina (73%) [2]. The large use of smartphones supports trade competition among smartphone manufacturers in the world. There are 5 big brands of smartphones that are most in demand by users. In sequence, the list of top well-known smartphone brands are Samsung, iOS, Lenovo, Xiaomi, and LG [3]. In line with the development of the smartphone, various types of attacks have emerged that can threaten smartphone users including malware attacks [6], DDoS [10], injection [7], information leakage [8], phishing [9], man in the middle attack [5], and many more. There has been a lot of literature that discusses attacks on smartphones in general, but there is still little literature that discusses specifically on a certain smartphone brand. This paper describes the result of a review of any attacks that have occurred on the infrastructure of top 5 (five) smartphone brands and also explains the mitigation of such attacks.

2. Method and materials
2.1. Sample preparation
This research is a concise review conducted by reading some of the latest literature on attacks and mitigation on smartphones infrastructure. Data was collected through a simple search using the Google search engine with the keywords such as: attacks, mitigation, smartphone, and well-known brand smartphone.

2.2. Method
From the literature that has been collected, data extraction related to attacks and mitigations that occur on the smartphone infrastructure was conducted. Attacks were grouped by assets that consist of network infrastructure, data center, main infrastructure, virtualization infrastructure, and user devices. Mitigation is explained based on four major group of attacks i.e. malicious software, phishing, SQL injection, and ransomware.

3. Results and discussion
3.1. Attacks on smartphones
Researchers have described various types of attacks that have been carried out on smartphones, both technical and related to the policy contexts [7]. Technical attacks target devices and services that are available on a smartphone while attacks in the context of policies target the rules or procedures adopted in the smartphone work process. Common attacks on smartphones are summarized in Table 1. Attacks are grouped according to the asset or infrastructure being attacked.

| Assets                      | Attacks                                                                 |
|-----------------------------|-------------------------------------------------------------------------|
| Network infrastructure      | Denial of Service [10], main in the middle attack [5], malware [6]     |
| Data center                 | Physical attack [11], privacy breach [8], privilege escalation [12], service manipulation |
| Main infrastructure         | Privacy breach [8], service manipulation                               |
| Virtualization infrastructure| Denial of Service [10], resources misuse, privacy breach [8], privilege escalation [12], virtual machine manipulation |
| User device                 | Injection, service manipulation, device port attack [4]                |

In the following, various attacks that occurred on several well-known brand smartphone i.e. Samsung, iOS, Lenovo, Xiaomi, and LG are explained and are summarized in Table 2.

**Samsung.** Samsung ranks first in the smartphone brand in the world [3]. This brand has various types of products in the smartphone industry and other electronic products. Samsung was founded in South Korea in 1938 by Byung-Chull Lee [13]. Apart from the sophisticated technology offered by this brand, there are several threats that have occurred on Samsung smartphone which are remote code execution [25][26], ransomware [16], privilege escalation [19], data leakage [16], heap overlow [20], human error [21], privilege escalation [22], rooting vulnerability [23], network traffic snooping [14], meltdown exploit [15][17][18], keyboard cracking attack [24]. The asset category most often targeted by attackers are the core infrastructure which includes data leakage, heap overflow, human error, privilege escalation, and rooting vulnerability.

**iOS.** Developed by Apple Inc. and introduced to the market in 2007 with the iPhone product, iOS puts forward technological innovations, which helped it begin to achieve success in 2008. Having several types of smartphone, iOS is certainly facing security vulnerabilities. Several types of vulnerabilities and attacks that have occurred on iOS smartphones are malware [28], cross-site scripting [29], trustjacking [30], information leakage [28][29], insufficient authorization [28], memory corruption [52], privilege escalation [29], malicious application [29], jailbreaking [27], unauthorized USB connection [30]. According to obtained data, on iOS smartphones, not all asset categories have been affected. No attack has ever attacked the asset category of virtualization infrastructure. While most attacks are in the category of assets, the core infrastructure includes insufficient authorization, memory corruption, privilege escalation, and malicious applications.

**Lenovo.** Lenovo, a company that was founded in 1984, began to expand its wings to the smartphone industry in 2015. Holding a company that is well known in the personal computer industry does not make Lenovo avoidable from attacks on its assets. Several
attacks that have threatened their assets are Bluetooth BlueBorne [31], man in the middle attack [34], SQL injection [32], remote Attack [42], improper access control [34], and privilege escalation [35][36][37]. Three asset categories being the target of attacks are network infrastructure, core infrastructure, and virtualization infrastructure. So far, no attacks have been reported on two other asset categories i.e. data center and user device. Most attacks are in the asset category of core infrastructure including SQL injection, remote attack, and improper access control.

**Xiaomi.** Founded by Lei Jun in 2010, Xiaomi puts forward technological innovations that are supported by consumer-friendly prices. Good innovation does not guarantee Xiaomi avoidable from attacks. This is indicated by several attacks that have occurred on Xiaomi smartphones which are man in the middle attack [38][39][41], malware, and backdoor [40]. Network infrastructure is the asset that is often reported attacked by man in the middle and malware. In addition to network infrastructure, core infrastructure is also the target of backdoor attack. No findings of attacks targeting data center, virtualization infrastructure, and user devices.

| Table 2. Common attacks on top 5 brands of smartphones |
|-----------------------------------------------|
| **Asset**                                      |
| Samsung | iOS | Lenovo | Xiaomi | LG |
| Network infrastructure                        | Remote code execution | malware, cross-site scripting, trustjacking | Bluetooth BlueBorne, Man in the middle attack | Man in the middle attack, Malware | Denial of Service, Man in the middle attack |
| Data center                                   | Ransomware, privilege escalation | Information leakage | - | - | Data theft, Phising |
| Main infrastructure                            | Data leakage, heap overflow, human error, privilege escalation, rooting vulnerability | Insufficient authorization, memory corruption, privilege escalation, malicious application | SQL Injection, Remote Attack, Improper access control | Backdoor | Location Manipulation, SQL Injection |
| Virtualization infrastructure                 | Network traffic snooping | Privilege escalation | - | Privilege escalation |
| User device                                   | Meltdown exploit, keyboard cracking | Jailbreaking, unauthorized USB connection | - | - | - |

**LG.** As a large electronic company from South Korea, LG started manufacturing smart devices in 2013 under the Mobile Communication unit. Some attacks on LG devices are Denial of Service (DoS) [44], man in the middle attack [45], data theft [44], phishing [44], location manipulation [45], SQL injection [46], and privilege escalation [46]. It can be seen that almost all aspects of assets have been attacked. The most common types of attacks
are man in the middle of and Denial of Service (DoS) targeting network infrastructure assets. Aside from network infrastructure assets, virtualization infrastructure is an asset that has the most types of attacks when compared to other types of attacks that occur on other assets.

3.2. Attack mitigation on smartphones
In this section, mitigation can be carried out on some of the attack types that have occurred on smartphones are described. These types of attacks are malicious software, phishing, SQL injection, and ransomware.

3.2.1 Malicious Software
Malware is software that is designed with the aim to harm, infiltrate, or damage computer. Malware can interfere or even cripple the operation of a system, allowing hackers to gain access to confidential and sensitive information and spy on computers or even the computer owners. The following are attack mitigations that can be done against malware on smartphones:

- Only allowed to install applications from trusted stores, such as Apple Store and Google Play Store.
- Choose applications that do have good ratings and good reviews.
- Always back up data regularly and arrange smartphones to back up data.
- Use data security applications.
- Periodically update the operating system of the device.

3.2.2 Phishing
Phishing is a method used by hackers to steal passwords by tricking targets, for example, using fake login forms on fake sites that resemble the original site. Mitigation that can be done against Phishing attacks is as follows:

- Make sure the website that is accessed is the correct website
- Use a secure cloud system
- Using antivirus
- Perform regular data backups and arrange smartphones to back up data when synchronizing the phone.

3.2.3 SQL Injection
SQL injection is a technique that misuses a security hole that occurs in the database layer. This loophole occurs when user input is not filtered correctly from the escape string formatting characters added in the SQL statement. Mitigation that can be done to prevent SQL Injection attacks is as follows:

- User input validation, you should filter input SQL comments and special characters.
- Limit the length of the input box, by limiting it in the program code so that the input box cannot be injected with a long command.
- Restrict database access on the website.
- Disable or hide SQL server error messages on the web.
- Add a get variable containing md5 encryption which is varied by url. Encrypt the password or change the login authentication algorithm specifically for the login form.
Filter user input.

3.2.4 Ransomware
Ransomware is malware designed to prevent access to a system until ransom is paid. Ransomware is called malware because it causes interference and loss to the user. A special feature of ransomware is ransom requests for victims to be able to decrypt their files or data. Mitigation that can be done to attack ransomware is as follows:

- Watch out for suspicious fraud. Only a few of these cases occurred and there may be many other events which have more severe consequences.
- Use reliable anti-malware tools to detect and block ransomware.
- Using firewall that performs whitelisting and blacklisting of data traffic is often a success factor for the system to be prevented from malware in general.
- Filtering spams and emails that are likely to carry malware by implementing email filtering.
- Blocking attachments.

4. Conclusion
In this study, a brief review of attacks and mitigation has been carried out on special pintra phones on five well-known smartphone brands based on its infrastructure. Common attacks on smartphones are Denial of Service (DoS), man in the middle attack, malware, physical attacks, privacy breaches, privilege escalation, service manipulation, resource misuse, virtual machine manipulation, injection, and device ports attack. Some identified mitigations for attacks on smartphone are only allowed to install applications from trusted stores, periodically update the operating system of the device, filter input SQL comments and special characters, and encrypt the password or change the login authentication algorithm specifically for the login form.

References
[1] GSM Association, “The Mobile Economy 2018”, 2018.
[2] Martin, Ben, “The Global Mobile Report”, comScore Mobile Metrix, 2017.
[3] Anh, Ha Ngoc, “Smartphone Industry: The New Era of Competition and Strategy”, Centria University of Applied Sciences, 2016.
[4] Amarante, J. and Barros, J., “Exploring USB Connection Vulnerabilities on Android Devices: Breaches using the Android Debug Bridge”, Polytechnic Institute of Beja, Portugal, 2017.
[5] Ferrag, Mohamed A., Maglaras, Leandros, “Authentication schemes for Smart Mobile Devices: Threat Models, Countermeasures, and Open Research Issues”, 2018.
[6] Grisham, J., Samtani, S. Patton, M., Chen, Hsinchunn, “Identifying Mobile Malware and Key Threat Actors in Online Hacker Forums for Proactive Cyber Threat Intelligence“, IEEE International Conf. on Intelligence and Security Informatics (ISI) pp.13-18, 2017.
[7] Park, Won H., Kim, Dae H., Kim, Myung S., Park, N., “A Study on Trend & Detection Technology for Cyber Threats in Mobile Environment”, 2013 International Conference on IT Convergence and Security (ICITCS), 2013.
[8] Park, Seon G., Kim, S., On, Joohyun, Noh, Myoungsun, Im, Chaetae, “Threats and countermeasures on a 4G Mobile Network”, Eighth International Conf. in Innovate Mobile and Internet Service in Ubiquitous Computing, 2014.
[9] Qamar, A., Karim, A., Chang, V., “Mobile malware attacks: Review, taxonomy & future directions”, Future Generation Computer Systems, Vol. 97, 2019, pp. 887-909.
[10] Roman, R., Lopez, J., Mambro, M., “Mobile edge computing, Fog et al: A survey and analysis of security threats and challenges”, Future Generation Computer Systems, Vol.78, Part 2, 2018, pp. 680-698.

[11] Khan, J., Abbas, H., Al-Muhtadi, J., “Survey on Mobile User’s Data Privacy Threats and Defense Mechanisms”, International Workshop on Cyber Security and Digital Investigation, 2015.

[12] Abawajy, J., Huda, S., Sharmeen, S., Hassan, M. M., Almogren, A., “Identifying cyber threats to mobile-IoT applications in edge computing paradigm”, Future Generation Computer System, pp. 525-538, 2018.

[13] Wolters, P. T. J., “The Obligation to update insecure software in the light of Consumentenbond/Samsung”, Computer Law & Security Review, Vol. 35, Issue 3, 2019, pp. 295-305.
[14] Back to College, “All Samsung phones vulnerable to network traffic snooping, unwarranted screen recording: Security Researcher Elliot Alderson”, 2019.
[15] TechRepublic, “Despite patches, Samsung Galaxy S7 open to Meltdown exploit and millions are affected”, 2018.
[16] Insights, “Mobile Security Risks Threaten Even the Most Secure Phone”, 2017.
[17] Cnet, “Samsung Galaxy 7 vulnerable to hacking due to flaw, researchers say”, 2018.
[18] Reuters, “Samsung Galaxy S7 smartphones vulnerable to hacking: researchers”, 2018.
[19] Threatpost, “Samsung, Crucial’s Flawed Storage Drive Encryption Leaves Data Exposed”, 2018.
[20] Hacker News, “Serious vulnerabilities discovered in Samsung Galaxy S9 and Xiaomi Mi6”, 2018.
[21] Insights, “Top Three Mobile Security Threats”, 2016.
[22] Information Security Newspaper, “Vulnerability in Samsung exposed user accounts”, 2018.
[23] Insights, “What Are the Security Risks of Rooting Your Smartphone”, 2019.
[24] Forbes, “600 Million Samsung Mobiles Vulnerable To Keyboard Cracking Attack”, 2015.
[25] Ars Technica, “New exploit turns Samsung Galaxy phones into remote bugging devices”, 2015.
[26] NowSecure, “Remote Code Execution as System User on Samsung Phones”, 2015.
[27] TrendMicro, “2018 Mobile Threat Landscape”, 2019.
[28] Forbes, “Critical Security Warning For iPhone Users”, 2019.
[29] Bleeping Computer, “iOS 12.2 Patches over 50 Security Vulnerabilities”, 2019.
[30] Symantec Blogs, “iOS Trustjacking – A Dangerous New iOS Vulnerability”, 2018.
[31] Intego, “What is BlueBorne? An Apple Device FAQ”, 2017.
[32] Hacked, “Lenovo & Infinix SQL Injection to Mobile SMS Leakage”, 2018.
[33] Security Week, “Lenovo Patches Critical Wi-Fi Vulnerabilities”, 2018.
[34] Tech Genix, “Lenovo patches fix high-risk vulnerabilities on ‘tens of millions’ of devices”, 2017.
[35] Threat Post, “Lenovo Patches Intel Firmware Flaws in Multiple Product Lines”, 2019.
[36] Network World, “Lenovo software has a major security risk”, 2016.
[37] Gadgets 360, “Lenovo Vibe Phones Affected by Critical Vulnerability Spotted by FireEye’s Mandiant”, 2017.
[38] Forbes, “Pre-Installed Security App Puts 150 Million Xiaomi Smartphone Users At Risk -- What You Need To Know”, 2019.
[39] Help Net Security, “Vulnerability found in Guard Provider, Xiaomi’s pre-installed security app”, 2019.
[40] Cnet, “Xiaomi phones came with security flaw preinstalled”, 2019.
[41] Threat Post, “Preinstalled Mobile Security App on Xiaomi Handsets Delivered Vulnerabilities, Not Protection”, 2019.
[42] Security Week, “Lenovo Patches Critical Wi-Fi Vulnerabilities”, 2018
[43] Cynet, “‘SNAP’ – Millions of LG Smartphone Devices are Vulnerable to Phone Hijack”, 2016.
[44] SC 30th Anniversary, “LG G3 vulnerability allows arbitrary JavaScript code”, 2016
[45] Check Point Research, “Remote Code Execution Vulnerability on LG Smartphones”, 2018
[46] Trend Micro, “Vulnerabilities Found in LG Mobile Devices”, 2016.