Sanjatul Hasan Siam

by Iftekhar Efat

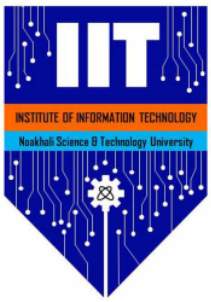
Submission date: 13-Mar-2022 12:32AM (UTC-0500)
Submission ID: 1782966613
File name: ASH1825023M.pdf (186.96K)
Word count: 2724
Character count: 14778

Mobile Cybersecurity Best Practices in 2022

Sanjatul Hasan Siam
STUDENT ID

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University



Project Area: **Information Security Lab**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

In recent years, more and more users and businesses use smart phone as communication tools, but also use in our private life. In the meantime, hackers use the network exploits to attack users' smart phone. These attacks exploit weaknesses come from different kinds of access just like SMS, Wi-Fi networks and MMS.Due to the continual discovery of new mobile device vulnerabilities, communicating mobile security dangers and best practices has become a top priority. The purpose of this article is to identify and assess existing dangers and best practices in the domain of mobile security in order to deal with this overarching issue.

1 Introduction

The popularity and ubiquity of mobile devices has increased dramatically in recent years among consumers all around the world. These devices, which run on a specific operating system, let users to download a wide range of software, known as "apps," from online markets such as the Apple App Store and Google Play. The aforementioned applications are the lifeblood of smartphones, strengthening their performance and improving their users' daily lives. The app stores let users to quickly find and install new programs, but they are also a source of spyware disguised as legitimate software. Mobile devices are now vulnerable to a wide range of security risks and malicious attacks.[2]

Users have been enabled and encouraged by the mobile revolution to migrate practically all of their daily activities into the mobile environment via so-called mobile applications. As a result, both mobile developers and consumers are seeing significant development. Users regard mobile devices as highly personal tools that are primarily used to assist day-to-day operations but also serve to store very sensitive personal data.Modern mobile applications are widely available and simple to install on practically any mobile operating system, including iOS, Android, and Windows Phone. We may see more and more powerful and customized apps arriving on the market as a consequence of fierce rivalry among application suppliers, tackling challenging challenges. These programs have a significant impact on a user's behavior by making day-to-day transactions easier.[4]

2 Background

Mobile technology is a phenomenon which is strongly rooted in our everyday activity. More often than not, we are dependent on different kinds of applications, both for leisure (instant messaging, booking, maps, etc.) and for business (online banking, e-mail management, business functions,etc.). Users install mobile apps and provide their personal information while rarely thinking about security issues. According to Landmann [3], the unprecedented growth in the number of smartphones and mobile workers has a direct impact on the number of attacks deployed on mobile devices. Smartphones today store hefty amounts of data and operate over international cellular networks, WLANs, and Bluetooth PANs. they run a diverse set of complex operating systems such as Symbian, iOS, BlackBerry OS, Android, and Windows Mobile. Most smartphones also support the Java platform for mobile devices, J2ME, with a variety of extensions. All this network connectivity and diverse rich code makes these devices more vulnerable than traditional PCs, which typically run standard operating systems for which many security products are readily available [5].

3 Mobile Security Threats

Users of mobile devices or so-called mobile users are increasingly subject to malicious activity, mainly concerning pushing malware apps to smartphones, tablets, or other devices using a mobile OS. these handheld devices, carried in our pockets, are used to store and protect sensitive information. Even though Google and Apple offer distribution environments that are closed and controlled, users are still exposed to different kinds of attacks.A few of them are given in the following [1]

1. Phishing in an app: we observed that one way criminals can bypass the app market source code checks was not by including anything malicious in the app itself, but rather by making an app that, in essence, is a browser window to a phishing site. Such apps, in this case, are designed in tandem with the phishing site so that the user has a seamless experience.

2. Supply chain compromise: it was observed that a trojanized version of a legitimate app had been included in the factory firmware from a small mobile phone manufacturer and shipped to customers on brand new phones. -e original app, called Sound Recorder, was found to have been modified to include code that was not part of its stated purpose: it could intercept and send SMS messages secretly. -e malicious version of the app could have been inserted into the supply chain in a number of different places. It was never made available through any app store, but only in a specific firmware image on a specific model of an inexpensive Android phone.

3. Cryptominer code in games or utilities: we encountered a significant jump in the number of apps that, without notification to the user, included cryptominer code in the app. -e code would run whether or not the app itself was running and functioned as a constant drain on the phone's (or other device's) battery.

4. Click-fraud advertising embedded in apps: advertisement fraud is, surprisingly, one of the most profitable criminal enterprises nowadays, and mobile apps appear to be a key part of this subtle crime. -e advertising industry estimates that, today, the cost to advertisers of fraudulently "clicked" ads, according to data published by the World Federation of Advertisers, tops US 19 billion US dollar each year.

It is also crucial to mention top 10 web application security risks according to the most prominent security community worldwide named OWASP Foundation. Mitigation of these threats would be the first step in the production of secure code of mobile apps[6]

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Using Components with Known Vulnerabilities
8. Cross-Site Scripting XSS
9. Insufficient Logging and Monitoring
10. Insecure Deserialization

4 Mobile Security Best Practices

Mobile security best practices are recommended guidelines and safeguards for protecting mobile devices and users' data [6]

1. Make user authentication the highest priority: most mobile devices can be locked with a screen lock and unlocked with a password, biometric (e.g., fingerprint and face recognition) or personal identification number (PIN) [56]. Nowadays, multifactor authentication is considered as the best practice to protect user's data [57]. On the contrary, security is entirely based on password complexity and the user's attention to its confidentiality.

2. Update mobile operating systems and on-board applications with security patches: keeping the operating system (Android and iOS) and the installed applications up to date is a must. Both Google and Apple provide regular updates to users, which resolve recent vulnerabilities or other threats, as well as sharing additional performance and security features. However, updating

an app is a two-edged sword since a new release can decrease its overall performance and the user's productivity. From a security perspective, updates can trigger the revetting process to confirm security clearance. In order to ensure that a mobile application conforms to an organization's security requirements and is free from vulnerabilities, a series of rigorous and comprehensive analyses take place. One has to keep in mind that app vetting might also include updated external components (e.g., third-party libraries) and new mandatory versions of the operating systems.

3. Back up user data on a regular basis: backing up is a basic method of preventing data loss or deletion. A backup schedule should be adapted to an increase in data over time. Examples of user data include individual user files (documents and spreadsheets), media files (e.g., pictures and videos), contacts, and other sensitive data. In case of mobile devices, the obvious choice is a remote backup, which means copying and storing files in a private or public cloud. However, the main concern in this case is the transfer speed. Even if a high-speed connection is used to send the data, the upload limitations, antivirus scanners, and firewalls can slow down the speed considerably. Another limitation concerns the cost of data uploading set by mobile internet providers. On the contrary, there is no guarantee that data stored in the cloud will be kept private. However, this can be easily overcome and most recommends that data files be encrypted which in turn might extend the overall backup task duration, if performed on the fly.

4. Utilize encryption: data encryption translates data into another form, or code, so that only authorized parties can decrypt and read these data. -e encryption feature is used for data stored on the mobile device as well as for data transmission over the network. Nevertheless, by default, encryption requires a password to encrypt and decrypt data files. If one forgets the password, the data recovery is usually problematic and not always successful. On the contrary, relying on the publicly available solutions could simply lull a user into a false sense of irrefutable security. Moreover, it is also strongly advised not to connect to and use a public and insecure Wi-Fi spot without using a secure transmission option such as a virtual private network (VPN). In this case, compared to regular internet connections, VPNs are still almost invariably slower, depending on the distance between the server and the client, the current server load, and the encryption level applied.

5. Enable remote data wipe: in case a user has their device with sensitive data stolen and there is little chance of retrieving them in a relatively short period of time, one should consider turning on the device capability which allows a factory reset message to be remotely executed [59, 61]. Furthermore, remote data wipe is imperative in case of termination of employment or contracting a malware infection which cannot be uninstalled or deleted. While the existing solutions have clear advantages, they are not cure-all for mobile security. For instance, while some tools erase only part of the data, others erase the entire content, including applications and personal data. -erefore, one should

consider deploying a secure container which, by design, separates the applications from personal data, enabling selective erasure in case of a security incident. Moreover, a proactive approach that tracks the use of sensitive data will improve security by early detection and prevention of its misuse or theft.

6. Disable Bluetooth and Wi-Fi when not needed: minimizing both Bluetooth and Wi-Fi usage reduces exposure to having vulnerabilities exploited, although the flaws are not in these standards, but in their implementations [62]. Here, it should be noticed that the disabling action requires an intentional interaction from a user. However, there are tools (e.g., Auto- Bluetooth) that turn Bluetooth on or off without any user interaction, based on the rules defined by a user.

Figure 1: Types of theft and loss by frequency

Type of theft or loss	Frequency (%)
Misplaced	69.12
Pickpocketed	10.98
Home invasion	7.60
Robbery	6.76
Car break-in	2.77
Business break-in	2.77

7. Be aware of social engineering techniques: social engineering is a term that encompasses a broad spectrum of malicious activity such as phishing, pretexting, baiting, quid pro quo, and tailgating ("piggybacking"). With this human-centric focus in mind, it is up to a user to be aware of malicious "actors" who engage in social engineering attacks hunting for human greed and ignorance. Organizations, in particular security analysts, might also consider conducting social engineering penetration tests (also known as social pen testing) among employees. By design, social pen testing is the practice of applying social engineering scams on an organization's employees to evaluate their capability to provide sensitive information. Such an assessment is beneficial by providing a real attestation on the level of adherence to the company's security policies by particular individuals.

8. Be sure not to jailbreak your device: jailbreaking is a privilege escalation with the aim of removing software restrictions imposed by the device manufacturer. In other words, deploying a series of kernel patches permits a root access which allows software, not available and distributed via the app store, to be installed. Jailbreaking can seriously expose an operating system to additional vulnerabilities, effectively exploited by attackers. One should also keep in mind that, in case of removing manufacturer restrictions, the device's warranty will most likely be voided. Moreover, a decrease of overall system stability might occur since buggy apps tend to utilize substantial amounts of hardware resources.

9. Be sure not to grant unnecessary permissions to applications: app permissions are the privileges an app has—like being able to access peripherals such as the camera, contact list, or location. Current versions of operating systems come in a variety of flavors depending on the manufacturer. -e major tenet is to grant only those permissions that are necessary for the application to work properly. In other words, a user should always employ the principle of least privilege (PoLP) [65]. On the contrary, granted permissions can be described as the keys that unlock the app's functionality. -erefore, a good design pins runtime permissions with specific actions and tasks, which justify the permission requests.

10. Install mobile security and antivirus applications: since there is no additional protection by default, mobile security and antivirus real-time scanners safeguard against malicious applications and viruses, as well as identify theft, ransomware, and cryptominers. Moreover, some tools can also scan URLs and block dangerous sites, monitor links in text messages, and provide parental control. -ere is no doubt that experts highly recommend using such tools, but nothing comes for free. In their case, the side effects refer to additional hardware resource allocation and increased battery drain due to the processes executed in the background.

Notes: Naturally, following these best practices will not 100 percent guarantee mobile device security; however, it will leverage the security level by reducing the attack vector and lowering the risk of system outages and malformed requests. [6]

5 Conclusion

Between attackers and defenders, security is always an arms race. Because the market for mobile applications is expanding, mobile security will continue to provide a slew of challenges. To put it another way, security is frequently a balance of risk and benefit, protection vs convenience. The possible hazards and advantages, as well as their tradeoffs, need additional and deeper examination, according to this school of reasoning. - This study provides a comprehensive picture of the issue, examining the negative events, situations, and circumstances that have the potential to result in asset loss, as well as the remedies that try to eradicate them and offer enough and effective protection for a user.

References

[1] Suraj Gangwar and Vinayak Narang. A survey on emerging cyber crimes and their impact worldwide. In *Encyclopedia of Criminal Activities and the Deep Web*, pages 23–35. IGI Global, 2020.

[2] Bin Guo, Yi Ouyang, Tong Guo, Longbing Cao, and Zhiwen Yu. Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review. *IEEE Access*, 7:68557–68571, 2019.

[3] Max Landman. Managing smart phone security risks. In *2010 Information Security Curriculum Development Conference*, pages 145–155, 2010.

[4] Silvere Mavoungou, Georges Kaddoum, Mostafa Taha, and Georges Matar. Survey on threats and attacks on mobile networks. *IEEE Access*, 4:4543–4572, 2016.

[5] Bruce Potter. Mobile security risks: ever evolving. *Network Security*, 2007(8):19–20, 2007.

[6] Paweł Weichbroth and Łukasz Łysik. Mobile security: Threats and best practices. *Mobile Information Systems*, 2020, 2020.

Sanjatul Hasan Siam

ORIGINALITY REPORT

88%	82%	71%	52%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.hindawi.com Internet Source	66%
2	downloads.hindawi.com Internet Source	6%
3	Submitted to University of Wollongong Student Paper	4%
4	Submitted to University of Adelaide Student Paper	3%
5	www.atlantis-press.com Internet Source	2%
6	Submitted to American Public University System Student Paper	2%
7	Submitted to University of Wales Institute, Cardiff Student Paper	2%
8	Submitted to The University of Fiji Student Paper	1%
9	www.bongos.net.au	

	Internet Source	1%
10	Submitted to Gulf College Oman Student Paper	1%
11	Submitted to Lindenwood University Student Paper	1%
12	www.coursehero.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Sanjatul Hasan Siam

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 3

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sentence Cap. Remember to capitalize the first word of each sentence.

Sentence Cap. Remember to capitalize the first word of each sentence.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Possessive This word may be a plural noun and may not need an apostrophe.

Possessive This word may be a plural noun and may not need an apostrophe.

Article Error You may need to use an article before this word.

PAGE 4

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

PAGE 5

Article Error You may need to remove this article.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to remove this article.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to remove this article.

Missing "," You may need to place a comma after this word.

Word Error Did you type "**the**" instead of "**they**," or have you left out a word?

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 6

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 7

Wrong Form You may have used the wrong form of this word.

Wrong Form You may have used the wrong form of this word.

Wrong Form You may have used the wrong form of this word.

Wrong Form You may have used the wrong form of this word.

Wrong Form You may have used the wrong form of this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word. Consider using the article **the**.

Hyph. You may need to add a hyphen between these two words.