(Online) ISSN 2744-1741
Defense and Security Studies *Original Research*
Vol. 5, No. 2, 2024, pp. 108-114
https://doi.org/10.37868/dss.v5.id274

Security considerations for smartphone devices

Almina Musinbegovic[1], Harun Alijagic[1], Amer Hrnjic[1], Ali Abd Almisreb[1*]
[1] Computer Sciences, Faculty of Engineering and Natural Sciences, International University of Sarajevo, Bosnia and Herzegovina

*Corresponding author E-mail: aalmisreb@ius.edu.ba

Received: Nov. 6, 2024
Revised: Dec. 8, 2024
Accepted: Dec. 10, 2024
Online: Dec 15, 2024

Abstract
In the paper, the ways in which smartphone devices are designed to be secure are investigated. Different approaches were examined for Windows, Android, and alike, as well as diving into the three security layers or areas of security. The first layer investigated was a "physical" device protection which involves the protection of the device and the data on it in case the device was stolen by not allowing anyone to gain access to the device, and locking its content. The second protection of the data examined was not allowing applications on the device access to corporate and personal data. The last layer of the protection investigated was in-app information being leaked and otherwise used. Security objectives and mechanisms were also visited in the paper. A literature review on the subject is provided.

Keywords: Computer network reliability surveillance, Communication system security, smartphone protection

1. Introduction

It is important to point out why smartphone security is so important. We take for granted the technology we have and rarely worry about its communication system security. The pictures we have stored on our devices as well as various passwords or bank card details are all vulnerable to all kinds of hacks. Not to mention the soft version of hacks which would be the constant attempts by our apps and companies to gather as much information about us as possible. Be that directly or indirectly our personal information is always under surveillance. Although we might not experience being hacked ourselves one can see the liability carried by companies if they are ever undermined by hackers or thieves, as this would reflect poorly on their computer network reliability. In essence, companies have a vested interest in protecting their users and invest a lot of resources to build their devices/software to be secure. In order for us to know what exact problems should be considered we must first look at how users use their mobile devices. Which tasks do they want to perform and how they perceive the security and privacy of these devices? Are they comfortable using them for sensitive tasks? How do mobile devices compare with laptop and desktop devices in terms of privacy and security? Knowing what users consider useful and necessary in mobile devices allows us to better understand and prevent mistakes from happening.

A smartphone is a mobile phone that is created to offer new advanced features that are useful for its users. In a short time, it became the most useful phone in the world because of its advanced computing ability and

connectivity. One of the best features of a smartphone is installing and running more advanced applications based on a specific platform by using a Wi-Fi internet connection [1][2]. The usage of smartphones requires some of information about the user that be stored to check the user's identity [2]. It looks like secured, but how the security of smartphones is managed? Is the user's information as safe as it looks?

Today, malware and data leakage are the most worrying harms of smartphone users. Because of these kinds of problems, the users' laxity appears and puts security organizations at risk.[3] The centralized application delivery architecture is a good and available way for attackers to attack the security and privacy of smartphones. The security sometimes is weak because application checking mechanisms are often not in place and users may choose which protected resources are accessible by third-party applications created by developers [4][5]. Most webpages like social networks (Facebook, Instagram, etc.) store user's ID and password to verify the right user.

1.1. Security objectives

To keep a system secured, the types of vulnerabilities, that may damage the security of a system, need to be considered. They may be considered by security objectives: confidentiality, integrity, and availability. Confidentiality determines who may access or not to what. Integrity orders who are allowed to manage or use certain resources. Availability describes the request from a legitimate owner to use some resource [1][6]. Many companies use antivirus software to prevent the appearance of viruses and other threats [7].

1.2. Security mechanisms

Three mechanisms are realized:

- System Modification: requires changing the platform's core source code including the kernel.
- System add-on: requires managing of platform's core configuration file. Add-on means to install appropriate applications for smartphones.
- Add-on Applications: mostly applied by the user by installing and updating (add-on) applications.

Other applicable mechanisms are an anti-virus solution, Firewall, Secure API, Access Control, Authentication, Spam Filter, Pre-Testing, Regular Update, and Remote Access Control [1][8].

1.3. Keeping smartphone safety

User may keep his/her smartphone safe by using the following steps:

- Guard his/her phone, and set PINs and passwords,
- Take safety in case his/her phone is lost or stolen,
- The user should not override his/her smartphone's security settings,
- Backing up and securing his/her data,
- Installing applications from trusted and safe sources,
- Using of antivirus software,
- Using software to find or erase his/her phone data if he/she loses a phone,
- Clearing his/her phone before dispensing with it,
- Accepting updates and patches [9],
- The benefits of smartphones attract hackers to try to hack and take information from users. Because of that, smartphone security and privacy always need to be updated to provide better security for users [10].

2. Literature review

With the sudden advance in hardware and software capabilities of smartphones, came the seemingly same set of security issues as with desktop computers, especially considering that smartphones have access to the internet where viruses and various other forms of attack can be performed [11][12].
Smartphone security problems can, arbitrarily, be classified into several categories: Authentication, Data Protection and Privacy, Vulnerabilities, and Attacks. These will be discussed in separate sections in the following.

2.1. Authentication problem

The authentication method is one in which the owner is confirmed using one of several methods. Using a password that one inputs when accessing the device, a token password like a set of nodes pressed a specific way or biometrics such as a fingerprint or iris.

Wei-Han in his research proposed a system where the authentication is implicit. The system learns the user's behavior pattern in the background continuously updating itself without disturbing the user. This method has been shown to be very effective, being able to detect abnormal behavior within 20 seconds of use with 90-95% accuracy [13].

Zahid et al. [14] proposed a user identification system to monitor mobile phone key users to distinguish authentic customers from quacks dynamically. The authors used a 25-user data set that only gave a fault of a rate of less than 2%.

Chine-Cheng et al. suggested also a non-intrusive authentication method that collects user data in the background using the device's sensors. The method uses stepwise linear regression to select features of each user the data is then classified using the k-nearest neighbor algorithm. The results show an error rate of 6.85%. The authors concluded that this method can be combined with intrusive methods like PIN or password to maximize smartphone security [15].

Morris in his research worked on combining multiple authentication methods [16]. There could be implemented SIMs that allow the user access to the network, without which no traffic can pass to the mobile device which would stop most if not all web-based attacks.

2.1.1. Data protection and privacy

Boshmaf et al. [17] in their studies addressed the problem of data protection. In his analysis, he found that indeed users want to protect their data but often find it inconvenient to do so practically using solutions available today.

Muslokhlove analyzed the problems of data protection against physical threats and what can be done to combat them. He found that there exist several vulnerabilities in detecting malicious data and when the device falls into the wrong hands. He concluded these issues might for the most part be fixed by updating the lock screen and authentication methods [18].

2.2. Vulnerabilities

There exist several types of vulnerabilities that have been described in smartphone devices [19]. These vulnerabilities can be exploited by malicious attackers to gain access to or destroy smartphone devices. Smartphone vulnerabilities can be split into: System faults, bad application management, insecure networks, and user unawareness.

2.2.1. System fault

When designing any device it is very likely that some hardware and software defects will be left unchecked as it can sometimes be very difficult to find them without extensive use, which is why they are often found only when something has already gone wrong. Software faults can, generally, be easily fixed when found but hardware ones often cost a lot more to fix. These defects when found by the wrong may obviously be exploited.

2.2.2. Bad app managemanet

Smartphone devices have very flexible APIs which allow for application development, however, this also means that they can be infected with malicious code from said applications. When installing third-party applications these apps might demand high privileges that might update or change system files. Attackers might exploit the control and privileges that they might gain.

2.2.3. Insecure network

When using Wi-Fi, Bluetooth, or GPS to connect with any network, a hacker might attempt to retrieve data packets from our device if on the same network. These vulnerabilities can be overcome with various encryption/decryption methods.

2.2.4. Lack of user awareness

No matter how much security methods become well there will always be a looming threat of users being jinxed into doing something they shouldn't. Although it's not easy to think up ways to trick someone these days it still can be done. There are many emails we receive that say they do one thing but pressing a link they provide might in fact do something entirely different that might be malicious. Many unacquainted with malicious code have been tricked and will continuously be tricked until awareness is raised.

2.3. Attacks

There are various ways in which a device could be attacked but they can be subdivided into groups according to their implementation and methodology, although most of them are similar if not the same as those used on desktop and laptop devices.

- **Physical attacks:** Smartphone devices can be stolen in which case this is considered a physical attack and for the most part responsibility for this does not fall on the manufacturer and there is little they can do to prevent it, but there are ways to find lost or stolen devices.
- **Rebooting attack:** When stolen a smartphone device may be accessed with a cold boot, if the information and passwords etc. of the previous user are lost the device can be made to act as if it were newly bought, there exist ways to prevent this but exploits still exist.

The following attacks can be classified into malware, or software designed to do something malicious to the device:

- **Backdoor attack:** This attack is when a hacker tries to establish a connection with the device whilst not being detected. Once the attacker gains access to the system he/she may for the most part do anything the regular user might do including extracting data. These attacks happen most often due to an unhandled exploit in the hardware/software with which the authentication process can be bypassed [20].
- **Virus attacks:** These are scripts designed to infect files, what they do exactly may vary but for the most part they simply make replicates of themselves thus bogging the system down to a crawl [21]. There are ways to detect viruses by continuously analyzing computer activity and network communications for abnormal behavior.
- **Worm attacks:** Worms are software that tries to send copies of itself from one device to another and much like viruses may also have another purpose to execute when it gets to a device [21].
- **Trojan:** This is a program most famously associated with malware, it is on the surface some sort of useful program or has an otherwise uneventful function but hidden in its code are malicious abilities. For the same reason, they remain very hard to detect as other malware's activity may immediately be spotted as unusual, a Trojan may remain dormant for some time thus evading detection. Houmansadr et al. [22] suggested that a cloud-based engine should be made that does a detailed detection on a smartphone device, finding and erasing any threat.
- **Spam attack:** Spam is a very common form of attack that sends a massive amount of requests or emails that have attached some other malware program. In essence, it is a method of transporting viruses or worms and is often used in hand in hand with other attacks [23].

Whereas previous malware was somewhat passive, that being a program already made and then spread the following are active attacks where the attacker is presently attempting to gain access:

- **Brute force attack:** The attacker tries to gain access to the device by literally finding out the authentication information. The brute force attack can be further split into an informed and uninformed where an informed attack might use various sets of words from a dictionary or personal information about the user, an uninformed attack tries random combinations until it succeeds. Naturally, this takes a very long time and lots of processing power.
- **Denial of service attack:** This attack attempts to stop the user from using Wi-Fi by replacing the original connection with one that just occupies the bandwidth but does nothing essentially. It was proposed by Dondyk and Zou [24] and they have shown that most iPhone and Android devices

were susceptible to this attack. A solution that was also proposed by them was to create an extra protocol where in order to authenticate the network the smartphone device sends a key password using cellular connection to the internet after which it tries to recover the same key using the Wi-Fi network. The protocol has already been tested on Android devices.

- **SMS attack:** Much like spam attacks SMS messages can be used to send links that might contain malware many operators allow sending credit using SMS messages which present a vulnerability that might be exploited.
- **USB connection attack:** USB connections can house various malware which might transfer itself onto a smartphone device there are ways already implemented to prevent USB root access and also to detect if the particular USB connection has risks [25].
- **Camera vulnerabilities:** Since almost all smartphone devices have cameras, they have opened a new sphere of possible attacks. There are many applications that demand access to the smartphone camera and some of these might execute malicious operations by running the camera or extracting photos. Much of the same issues are shared with sound applications that might take access to the device's microphone.
- **Control flow attacks:** Attacks that attempt to control which code is executed and have become common. A framework was provided to counteract this attack by monitoring contradicting flow control attempts [8][26].

There are other important research regarding this topic, for example papers [30][31][32][33][34][35], with valuable insights.

3. Discussions

The first question that appears in our work is:" What does smartphone security mean?". Mobile security refers to the effort to secure data on mobile devices such as smartphones and tablets [27].

The next question is:" Do we have a need for smartphone security in our devices?". The answer is very obvious. Yes, the security of our mobile devices has priority over all other needs nowadays. Nowadays most of our personal information and data (photos, videos, contacts, etc.) are stored on our smartphones, or through our smartphones we can access them.

According to the FBI, more than 4,000 ransomware attack occurred on daily base in 2016. That was a 300 percent increase compared to 2015. If we consider technological improvement and expansion of the smartphone market, we can assume that today we have 15,000 to 20,000 attacks daily [28]. Also, according to Kaspersky Lab Android is the most frequently OS for malware attacks in the mobile world and the second most targeted platform, right after Windows [29]. This information is very worrying because now we see how easily we may be finished as the target of a potential attack.

If you ask if is there any solution to this problem, yes there is. Actually, there are a lot of solutions for improving the security of your phone and your data, as we already mentioned before [1][8].

Some journalists conducted research about reasons why hackers make malware. According to Kayla Matthews, top five reasons are:

- Eavesdrop on calls
- Steal money
- Blackmail people
- Damage your phone
- Threaten national security.

4. Conclusions

We can conclude that mobile security is very important nowadays. We use mobiles on a daily base, hold our information and data, and communicate over them. Malware and ransomware may cause problems in usage or even worse, they may cause leaking of information and data. We may finish as victims of blackmail or theft. We need to be aware of the danger that smartphones bring with their advantages. People need to understand

all potential threats and act at the right time. We need to educate ourselves and others about the mechanism for dealing with viruses, malware, etc. It is not enough just to install antiviruses on smartphones and think that we are safe. It is also important to take care about which sites we visit, which apps we install, and to whom we give our phones. Right-time action is best to prevent any unwanted attacks and data leaking.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] W. Jeon, J. Kim, Y. Lee, D. Won, "A practical analysis of smartphone security," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011.

[2] S. Haug, R. P. Castro, M. Kwon, A. Filler, T. Kowatsch, M. P. Schaub, "Smartphone use and smartphone addiction among young people in Switzerland," *J. Behav. Addict.*, 2015.

[3] A. Das and H. U. Khan, "Security behaviors of smartphone users," *Inf. Comput. Secur.*, 2016.

[4] A. Mylonas, A. Kastania, D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Comput. Secur.*, 2013.

[5] W. Enck, D. Octeau, P. McDaniel, S. Chaudhuri, "A Study of Android Application Security," in *SEC (USENIX Security Symposium)*, 2011.

[6] "Ten Steps to Smartphone Security (Android)", https://www.fcc.gov/sites/default/files/12.14%20Mobile%20Security%20Tips%20%28Android%20-%20Links%29_0.pdf

[7] "Mobile device security Understanding vulnerabilities", https://www.shadowdetect.com/mobile-device-vulnerabilities/.

[8] S. Farhan, M. Ali, M. Kamran, Q. Javaid, S. Zhang, "A Survey on Security for Smartphone Device," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, No. 4, 2016.

[9] "Safer smartphones - a guide to keeping your device secure", https://ico.org.uk/media2/migrated/1446/smartphone-securityv5.pdf

[10] M. Alsaleh, N. Alomar, A. Alarifi, "Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods", *PLOS ONE*, Vol. 12, No. 3. 2017.

[11] K. Bala, S. Sharma, G. Kaur, "A Study on Smartphone based Operating System," *Int. J. Comput. Appl.*, 2015.

[12] J. H. Choi, H. J. Lee, "Facets of simplicity for the smartphone interface: A structural model," *Int. J. Hum. Comput. Stud.*, 2012.

[13] C. Shen, Y. Li, Y. Chen, X. Guan, R. A. Maxion, "Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication," *IEEE Trans. Inf. Forensics Secur.*, 2018.

[14] S. Zahid, M. Shahzad, S. A. Khayam, M. Farooq, "Keystroke-based user identification on smart phones," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009.

[15] C. C. Lin, C. C. Chang, D. Liang, C. H. Yang, "A new non-intrusive authentication method based on the orientation sensor for smartphone users," in *Proceedings of the 2012 IEEE 6th International Conference on Software Security and Reliability - SERE*, 2012.

[16] Venkatesh, Morris, Davis, Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Q.*, 2003.

[17] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, K. Beznosov, "Understanding users' requirements for data protection in smartphones," in *Proceedings - 2012 IEEE 28th International Conference on Data Engineering Workshops - ICDEW*, 2012.

[18] I. Muslukhov, "Survey: Data Protection in Smartphones Against Physical Threats," Term Project Papers on Mobile Security, University of British Columbia, 2012.

[19] Y. Zou, J. Zhu, X. Wang, L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, 2016.

[20] O. Ugus, D. Westhoff, H. Rajasekaran, "A leaky bucket called smartphone," in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops*, 2012.

[21] M. La Polla, F. Martinelli, D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surv. Tutorials*, 2013.

[22] A. Houmansadr, S. A. Zonouz, R. Berthier, "A cloud-based intrusion detection and response system for mobile phones," in *Proceedings of the International Conference on Dependable Systems and Networks*, 2011.

[23] C. Guo,H. J. Wang, "Smart-Phone Attacks and Defenses," *Microsoft Res*., 2007.

[24] E. Dondyk, C. C. Zou, "Denial of convenience attack to smartphones using a fake Wi-Fi access point," in *2013 IEEE 10th Consumer Communications and Networking Conference*, 2013.

[25] A. Pereira, M. Correia, P. Brandão, "USB connection vulnerabilities on android smartphones: Default and vendors' customizations," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

[26] J. Khan, H. Abbas, J. Al-Muhtadi, "Survey on mobile user's data privacy threats and defense mechanisms," in *Procedia Computer Science*, 2015.

[27] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," in *Proceedings - IEEE Symposium on Security and Privacy*, 2011.

[28] A. Apvrille, "The evolution of mobile malware," *Computer Fraud and Security*, 2014.

[29] Kaspersky Lab, "Kaspersky Lab discovers ZooPark, an Android-based malware campaign, Kaspersky Lab US," KAspersky Lab, 2018.

[30] M. Ibrahim, G. Supayah, J. Bin Ibrahim, "Mobile Security And Privacy In Smartphone Technology", *International Journal of Computer Science and Information Technology Research*, Vol. 3, No. 4, 2015.

[31] M. A. Bari, S. Ahamad, M. R. Ali , "Smartphone Security and Protection Practices", *International Journal of Engineering and Applied Computer Science (IJEACS)*, Vol. 3, No. 1, December 2021.

[32] Z. Muhammad, Z. Anwar, A.R. Javed, B. Saleem, S. Abbas, T.R. Gadekallu, "Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses", *Technologies*, Vol. 11, No. 3, 2023.

[33] N. J. Siddiqui, "The Study of Smartphones Security and Privacy", *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, Vol. 2, No. 6, 2022.

[34] "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", *European Union Agency For Network and Information Security*, 2017.

[35] R. Mueller, S. Schrittwieser, P. Fruehwirt, P. Kieseberg, E. Weippl, "Security and privacy of smartphone messaging applications", *International Journal of Pervasive Computing and Communications*, Vol. 11, No. 2, 2015.