Analyzing User Awareness on Security in Android Smartphone Devices

Aedunuri Sambaraju, Muralidhar Pantula, and K. S. Kuppusamy(✉)

Department of Computer Science, Pondicherry University, Pondicherry, India
sambaraju.aedunuri@gmail.com, vijayamuralisarma@gmail.com, kskuppu@gmail.com

Abstract. Today's Digital World is evolving rapidly and the smartphone usage has became mandatory. People use smartphones to get services like email, education, business, social communication, etc. For each service category, there are plenty of applications (Apps) available in the market. Along with Apps usage, it is obvious that a user need knowledge on securing devices and private data. We analyzed Naive Android Smartphone Users (ASUs) on different Security Areas where awareness is in need to secure the device as well as the data. The responses indicates that majority of the participants have a fear of Malicious Attacks on their private data, business information and financial transactions.

Keywords: Smartphone security · Android security features · Vulnerabilities · Security awareness

1 Introduction

Smartphones comes with features that are equivalent to a PC with high speed processing, large storage, HD screens, cameras, etc. The usage of smartphone growing rapidly as the number of smartphone users expected to increase to more than 2.8 billion in 2020 (Fig. 1). Smartphones provide services to user with built-in Apps such as browser, text messenger, Apps stores, e-mail termed as system apps. And it can run a variety of third party Apps installed from online markets for different services such as mailing, chatting, social networking, entertainment, etc. The expected number of Apps to be downloaded for the year 2022 is more than 250 billion (Fig. 2).

There are a few operating systems(OSs) available for Smartphones. The popular among them are Google's Android and Apple's iOS. As per the statsta around 1.5 billion smartphones with either Android OS or iOS were sold out. Among Android, iOS and other smartphone OSs Android leads the smartphone market with 74.45% of the share and iOS with 22.85% [3]. Popularity of Android attracted App developers to target Android Smartphones by developing malicious Apps, which makes the device vulnerable to attacks such as hacking, hijacking, phishing, Malfunctioning, etc. It would be a serious problem if the ASUs unaware of these attacks and the counter measures.

S. Smys et al. (Eds.): ICCNCT 2019, LNDECT 44, pp. 213–221, 2020.
https://doi.org/10.1007/978-3-030-37051-0_24

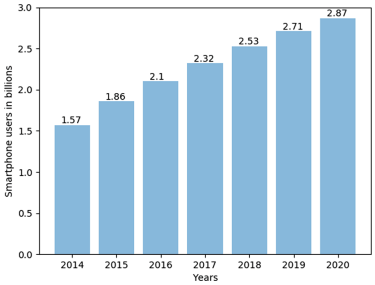

Fig. 1. Expected Smartphone Users Worldwide [5]

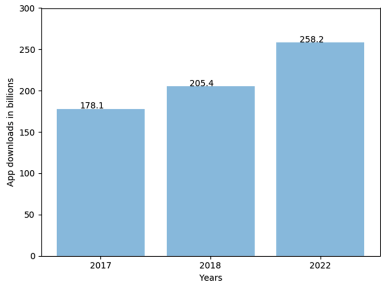

Fig. 2. Expected Apps download Worldwide [4]

ASUs must aware of security features which protect the device and the sensitive (private) data to reduce the risk of attacks. The inability of ASUs in recognizing vulnerable applications and malicious content is due to lack of awareness on types of vulnerabilities and precautions to take against them. So, it is important to the ASUs to possess the knowledge in security areas and confronting behavior with regard to information security. In this paper, we analyzed the ASUs of Pondicherry University who belong to different age groups.

2 Android Operating System

Every Smartphone needs an OS to control the functionalities of the hardware technologies (like Sensors, Camera, Fingerprint, NFC) [12]. OS is responsible in providing security, running other apps to fullfill user needs. As the Android leads the Smartphone market we presented introduction on its Architecture, App Structure and security features that Android OS provide to ASUs.

2.1 Android Platform Architecture

Android is an open source Operating System having a layered Architecture consisting of various components - Linux kernel, Hardware Abstraction Layer, Android Run Time, Android Libraries, Java API Framework, System Apps (Fig. 3).

- *Linux Kernel*: Linux Kernel make the device manufacturers easy to develop drivers for the device and allows to take advantage of key security features.
- *Hardware Abstraction Layer (HAL)*: HAL provides standard Android system interfaces (for hardware components such as Camera/Bluetooth) that allows developer to access the device hardware from Android OS feature-set [1].
- *Android Run Time (ART)*: Android RunTime (ART) used by Apps for system services that executes Dalvik executables and Dex bytecode specifications. It provides features like Ahead-of-time (AOT) compilation for tighter install time verification to improve app performance.

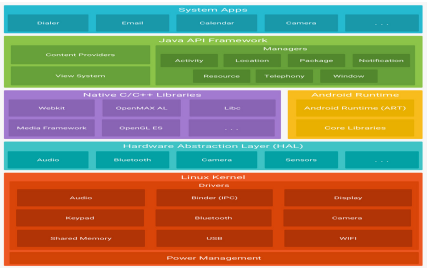

Fig. 3. Android Architecture [1]

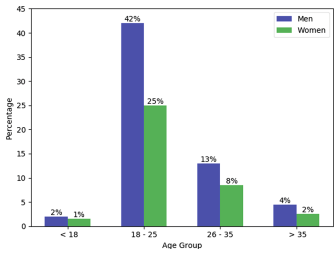

Fig. 4. Participants age groups

- *Android Libraries (AL)*: ALs consists of Android system components (ASCs) and services for ART and HAL. These are of two types: Core Libraries that support ART to write apps in Java and Native Libraries that allows Android Apps to get access to the Open Graphics Libraries (OpenGL)[6].
- *Java APIs framework Layer*: Java API Layer acts as an interface between Apps and the core of the Android Platform. It offers different services to the apps with different managers, System Views, and Content Providers [1].
- *System Apps Layer*: It consists of the basic apps that provide services such as Browsing, Calendar, mailing, SMS service, Keyboard, etc. There can be third party apps which replaces system apps for specific service.

2.2 Android App Structure

The developed Application contains the compiled code, with data and resource files archived as an Android Package (called as apk/APK) consists of the core framework components, a manifest file and resources applied to the device configurations [1].

- *App Components*: App components defines the life cycle of Android App. They are Activities, Services, Broadcast receivers, and Content providers [20].
- *The manifest file*: Components used by App can be declared in the manifest file. In Addition, it contain required permissions, the API level, features (hardware/software), and API libraries to be linked by the app.
- *App Resources*: These require to visually present App that define alternative images for different screen sizes, optimization of app for variety of device configurations, etc.

2.3 Security Features for Android Smartphone

To make Android as the safest Smartphone Platform, Google trying to develop different technologies that brace it's security and over 50 billion apps are checked daily to confirm their proper behavior [7].

- *Google Play Protect*: Google Play Protect acts as a built in malware protection with Google's machine learning algorithms as backbone to improve protection real-time [2].
- *Application Sandboxing*: Apps Sandboxing insulates and defends the installed Apps in Smartphone by stopping them to access ASU's sensitive information in between them [20].
- *Defending with designed Hardware*: For Android Platform, the hardware protects the access to device in the form of securing lock screen, verifying boot, encryption at device level [7].
- *Trusted Execution Environment (TEE)*: The TEE is a technique used for Android which provided by secure OS called Trusty. Trusty OS provides an isolated execution environment to secure App's sensitive information by executing them in TEE which is a highly secured area [8].
- *Security Updates*: For every layer in Android Platform Google reinforces security updates to all device manufacturers, in regular intervals [7].
- *User Access control*: Android Platform allows ASUs (as the Administrators) to customize App permissions in accessing App's data or hardware components [17].

3 Vulnerabilities in Android Smartphones

Android Smartphones vulnerable to attack when they are exposed to public networks to access services by always-on and always connected. There are different types of vulnerabilities with which Android Smartphones can be exploited [16] as follows.

- *Denial of Service (DoS)*: DoS vulnerability can effect the Android Smartphone by a malicious app installation or through a website. It makes the attackers service executed continuously even the malicious app is terminated [13].
- *Overflow*: This vulnerability in Android make the phone dead where ASUs can't make calls, and can't access screen [14].
- *Cross-site Scripting (XSS)*: XSS vulnerability steals credentials of the ASUs by injecting malicious scripts into trusted web pages loaded in browser.
- *Web view Vulnerability*: It is a customized web view of the web browser displaying the contents of the attacker by running customized functionalities. There are two web view vulnerabilities namely authorization and cross-zone scripting based on file [11].
- *Repackaging*: Android applications can be decompiled, modified and repacked with Attacker's code, finally published in official/unofficial market [14].
- *Android NFC*: Attacker can take full control of NFC (Near Field Communication) in Android Smartphone by using another hardware or device within distance to attack any operation can be done [9].
- *Social/Sharing Authentication Flaws*: The social Apps saving authentication details in unencrypted form can be vulnerable to that Smartphone device [14].

4 Awareness for ASUs to Secure Android Smartphones

The ASUs must focus on distinct areas relevant to information security in Android Smartphones. It is obvious that ASUs must have knowledge over security areas, and confronting behavior with regard to information security. From [19], the main security areas broadly categorized as Applications, Browsing and Accounts, Connecting Mediums, and Device. These security areas elaborated in the following sections.

4.1 Security Areas

- Application: The careless behavior of ASUs with rooted or jailbroken devices permits Apps to bypass the application sandboxing mechanism. With respect to Apps the two sub areas that ASUs must aware of are App installations and handling, discussed below.
  - Installation: In this, ASUs make sure of the App's source of installation, and permissions required by it before installing.
  - Handling: After installation, While handling the app, ASUs asked for granting required permissions, changing privacy settings and access control, and updating the app.
- Browsing and Accounts: ASUs communicate each other by surfing the Internet which in turn expose ASUs to different attacks like phishing, spam links, account hijacking, etc [13]. This area related to the browsing and device/social accounts management.
  - Browsing: While browsing, ASUs must take safety actions like avoiding unsecured websites, blocking pop-ups and spam, validating site certificates, and avoid giving personal details to distrusted web services.
  - Device/Social Accounts: Smartphones contain accounts which include customized privacy and security settings which can be hijacked by attackers to access the multimedia data, payment details and other business corresponding information. ASUs can avoid this by using strong passwords, service specific passwords, updating passwords in a regular interval, and securing those passwords appropriately [10].
- Connecting Mediums/Channels: Smartphones have connectivity technologies for information sharing through connecting Mediums (such as Wi-Fi, Bluetooth, etc) with distinct properties. Some of them have limited or no security/privacy features. To avoid ASUs falling in to these distrusted channels they can use VPNs, external security tools, and predefined settings.
  - Physical channels: Smartphones can connect to physical channels such as Wired headphones, PCs, memory cards, USB charging ports, different gadgets and accessories. These are also prone to attacks (like malicious chargers, replacement screens, etc.) [19]. So, ASUs must aware of risk in connecting to the physical channels and distrusted components.
- Device: To protect Smartphone device ASUs must have security concerns on Device OS, Data privacy, and Security systems.

- Device OS: ASUs must be careful in 'rooting' or 'jailbreaking' the smartphone to get the super user privileges. It may leads to the unofficial or unsupported OS updation used by malicious entities [18].
- Data privacy: The sensitive information abides in Android Smartphone need to be protected with privacy settings provided by the device. ASUs should use SIM card lock, setting Location on or off, encryption of data and account credentials to avoid privacy related issues [15].
- Security systems: Using security systems (system or user defined) on top of Android OS helps in scanning malware and preventing attacks in Android Smartphones [15].

5 User Awareness Survey

Participants were asked to answer the Questionnaire to analyze the knowledge on Security of Android Smartphone. The details of their responses are illustrated in this section.

1. Demographic data of the Participants: Majority of the participants (of different age groups) are 18 to 25 years of age having education as either graduation or post graduation (Fig. 4).
2. Different category of apps that participants using frequently: Majority of the participants are using Chat/Instant Messaging apps (with 92%) and Social Networking (76.5%), Browser (71%), Education (63.5%), and Entertainment (56.5%) Apps falls next in the most used apps categories (Fig. 5).

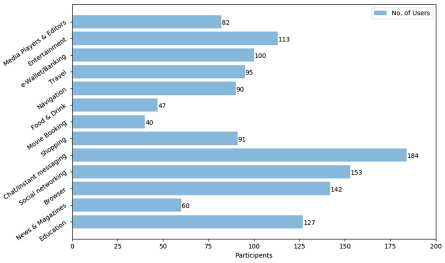

Fig. 5. Category of Apps frequently used

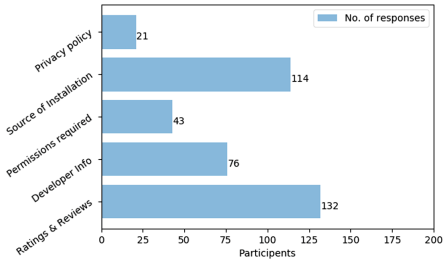

Fig. 6. Awareness on App installation

3. App Installation Concerns by ASUs: Related to App installations, from given options (Ratings & Reviews, Developer information, permission required, source of installation, and privacy policies), participants ignoring the privacy policies and permissions required (Fig. 6).
4. App Updation Awareness by ASUs: Regarding App/OS updations, the participants (51%) are thinking its only for the Feature Updation. Most of them are unaware of the fact that the updations meant for security patches and boosting efficiency (Fig. 7).

5. Type of data User thinks private: The responses reveal that multimedia data (like pics, videos, and voice notes) and chat history are considered as more private to them (Fig. 8).

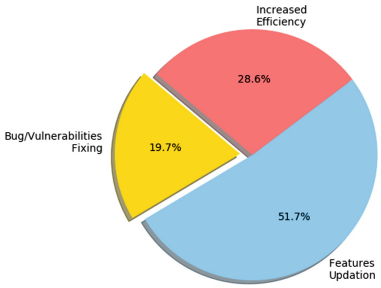

Fig. 7. Awareness on App updations

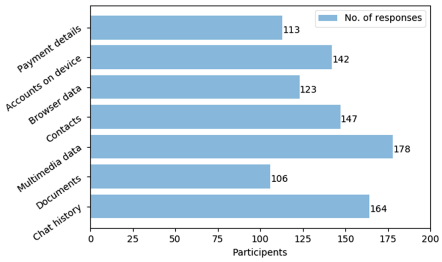

Fig. 8. Type of data considered Private

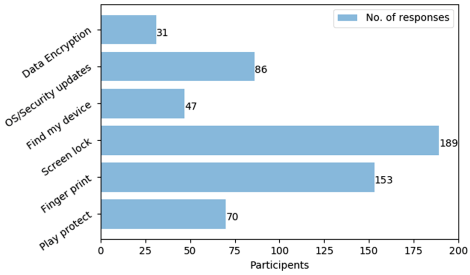

Fig. 9. Awareness on Android Security Features

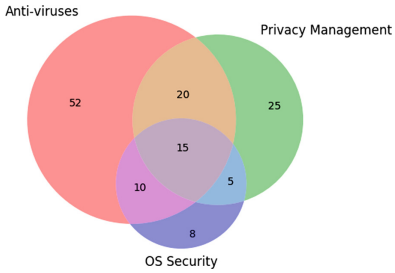

Fig. 10. Awareness on different security systems

6. Android Security Features awareness: Majority of the participants are unaware of the major security and privacy protection features (like Find my device, and Data Encryption) provided by the Android OS (Fig. 9).
7. Awareness on Security Systems Usage: Participants aware of additional security systems and Android OS Security usage. But, majority of respondents are aware of Antivirus systems (52) and Privacy Management Applications (25) and few (15) are using combination of all (Fig. 10).

6 Conclusion

Android has become a prominent smartphone OS used by more than 70% of the users. Android architecture eases the use of Apps and its openness allows attackers to target the Android devices for ASU's sensitive information by developing malicious Apps. We've surveyed the vulnerabilities (affects ASU's information)

and counter measures (exploits vulnerabilities). In this article we imposed set of questionnaire on ASUs targeting awareness of security in Android Smartphones. The analysis revealed that ASUs lack of knowledge on Android OS security features and usage of security systems. In this regard we are about to develop an Android App which provide knowledge on various security aspects and gives count that indicates the Freshness score of Android Smartphone.

7 Compliance with Ethical Standards:

All author states that there is no conflict of interest. We used our own data. Humans/aniamls are not involved in this research work. We used our university students and got approval from the university.

References

1. Android, platform architecture. https://developer.android.com/guide. Accessed 15 Feb 2019
2. Google play protect. https://www.android.com/intl/en_in/play-protect/. Accessed 11 Feb 2019
3. Mobile operating system market share worldwide. https://gs.statcounter.com/os-market-share/mobile/worldwide/2019. Accessed 10 Feb 2019
4. Number of mobile app downloads worldwide in 2017, 2018 and 2022. https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/. Accessed 10 Feb 2019
5. Number of smartphone users worldwide from 2014 to 2020. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. Accessed 10 Feb 2019
6. OpenGL ES. https://developer.android.com/guide/topics/graphics/opengl.html. Accessed 12 Feb 2019
7. Protect every android user,hardware designed to defend and regular security updates keep things in order. https://www.android.com/security-center/. Accessed 15 Feb 2019
8. Tee in android development by varun malhotra. https://dzone.com/articles/overview-tee-in-android. Accessed 09 Feb 2019 (published on 10 Jan 2018)
9. Top mobile vulnerabilities and exploits of 2012, darkreading. https://www.darkreading.com/top-mobile-vulnerabilities-and-exploits-of-2012/d/d-id/1138833. Accessed on 18 Feb 2019 (Published on 12 Dec 2012)
10. Adams, A., Sasse, M.A., Lone, P.: Making passwords secure and usable. In: People and Computers XII, p. 15. Springer (1997)
11. Chin, E., Wagner, D.: Bifocals: analyzing webview vulnerabilities in android applications. In: International Workshop on Information Security Applications, pp. 138–159. Springer (2013)
12. Divya, K., Kumar, S.K.V.: Comparative analysis of smart phone operating systems android, apple ios and windows. Int J Sci Eng Appl Sci (IJSEAS) **2**, 432–438 (2016)
13. Goel, D., Jain, A.K.: Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Comput. Secur. **73**, 519–544 (2018). (Elsevier)
14. Hur, J.B., Shamsi, J.A.: A survey on security issues, vulnerabilities and attacks in android based smartphone. pp. 40–46 (2017). (IEEE 978-1-5386-2186-8/17)

15. Park, J.H., Yi, K.J., Jeong, Y.S.: An enhanced smartphone security model based on information security management system (ISMS). Electron. Commer. Res. **14**, 321–348 (2014). https://doi.org/10.1007/s10660-014-9146-3 (Springer Science and Business Media)
16. Joshi, J., Parekh, C.: Android smartphone vulnerabilities: A survey. 5 (2016). (IEEE 978-1-5090-0673-1/16)
17. Ahvanooey, M.T., Li, Q., Rabban, M., Rajput, A.R.: A survey on smartphones security: software vulnerabilities, malware, and attacks. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **8**(10), 16 (2017)
18. Miller, C.: Mobile attacks and defense. Secur. Priv. IEEE **9**(4), 68–70 (2011)
19. Bitton, R., Finkelshtein, A., et al.: Taxonomy of mobile users' security awareness. Comput. Secur. **73**, 266–293 (2018). (Elsevier Publication)
20. Yadav, S., Apurva, P.R., et al.: Android vulnerabilities and security. In: International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), pp. 204–208 (2017). (IEEE 978-1-5386-0627-8/17)