Power of Smartphone Security: A Case Study

Mr. Ashish Rajput
MCA Student
Deptt: Computer Application
UIM, Uttaranchal University

Mr. Amit Singh Rawat
MCA Student
Deptt: Computer Application
UIM, Uttaranchal University

Ms. Pooja Gupta
Assistant. Professor
Deptt: Computer Application
UIM, Uttaranchal University

Abstract

Smartphone offers the usage of both mobile phones and PDAs. At present, there is not much difference between Smartphone, PC and other advanced devices like tabs, mobile application. Unfortunately, there are new developments in both mobile phone devices and their services. Market demand forces to focus on new features but at the cost of security. Thus, the most important security feature is neglected. In this paper, authors provide a simple and concise analysis of different attacks with the possible solutions available to improve Smartphone security.

Keywords: Smartphone, Privacy, Security, Threats

1. INTRODUCTION

Mobile devices are divided into eight classes: Notebooks, Tablets, Mobile Media Players, Mobile Gaming Devices, Mobile phones, Smart phones, PDAs, and Industrial Mobile Devices. Smaller size, Notebooks, is portable computer; it has some additional features, like a touch screen but it lacks a full keyboard. Most of the Tablets are without keyboard but have touch screens with wireless connectivity for viewing online and/or multimedia content.

Mobile Media Players also known as "Music Players" are mobile devices especially designed for accessing multimedia content. There are Mobile Gaming Devices that are mostly designed for playing computer games. From the invention of first mobile phone in the year 1973 till today's smart phones, mobile phones evolved in many diverse types and shapes, and provide a range of features. **Smartphone** is a mobile phone with multi-purpose computing facility [1]. However, the main functions of simplest mobile phones are to make phone calls and to send SMSs. On the other hand, very high-end Smartphones are multi-purpose and provide wireless local area or personal area networking capabilities. Industrial Mobile Devices are explicitly used for business, medical, or military applications.

2. IMPORTANCE OF SMARTPHONE SECURITY

Smartphone security has been subjected to intensive research work in the past years. Existing review papers presents the state of the art of popular Smartphone operating systems. [2, 3, 4] showed that mobile malware, similar to Personal Computer (PC) malware, can cause system corruption or reveal private user information [2].

Mobile phone security is also known as wireless security. In this time, mobile security has faced the many problem like hacking problem and virus. Mobile devices have emerged as a necessary part of our life; we depend on the mobile phone devices more than any other gadgets. However, mobile phone is just a mean of providing communication with the people. To understand the impact of a lack of Smartphone security, we need to understand how smartphones are being used. Smartphone usage has become so vast and diverse that it would be almost impossible to record every available usage. There are more than 5 billion mobile devices in use in the world amongst 7 billion people.

As described in [4], five major parameters i.e. Mobility, Strong Personalization, Strong Connectivity, Technology Convergence, and Reduced Capabilities differentiate Mobile device security from conventional computer security are.

2.1 Mobility. Mobile devices are not kept in one place for longer time, they are mobile and hence there is a probability that they might be stolen or physically tampered with.

2.2 Strong Personalization. A computer could be shared among various users and each user can have his/her own profile account on the computer. However, mobile devices are mutually exclusive as they are not shared among multiple users. A user keeps his mobile device close and it is for personal use only.

2.3 Strong Connectivity. There are multiple ways to connect a mobile device to a network or the Internet through hot spots, Wi-Fi or ISP, Bluetooth.

2.4 Technology Convergence. Many diverse technologies like a PDA, a music player, a mobile phone, and a digital camera are merged into one single contemporary mobile device,

2.5 Reduced Capabilities. Mobile devices are just like computers but lack many functionalities that conventional computers have such as, a mobile phone does not have a full keyboard and lacks in processing capabilities.

3. CHALLENGE OF SMARTPHONE SECURITY

- Data
- Identity
- Availability

Three most hacked assets of Smartphone are Data, Identity, and Availability. These smart devices manage user's data. Smartphone stores sensitive and confidential information of users like user's login credentials, personal or businesses related data, and activity logs (e.g., pictures or audio-memos). Mobile devices in particular with wireless connectivity, are tailored according to user's needs. That is, a device or its data is directly attached with a particular person. Availability of services in a mobile phone cannot be stolen or misused but it is something that can be denied to its genuine user.

4. THREATS ON SECURITY

4.1 Physical Security

Confidentiality is broken when a device is lost or stolen. In the 2011, Lookout Labs estimated that every 3.5 seconds a mobile phone was lost in the USA and almost every person who found missing devices tried to access the information stored in the phone [5]. This “access” may be an effort to find out the owner, but who knows? Even temporarily misplacing a phone can put sensitive data at risk. A device without a strong PIN or password and full data encryption is at the higher risk if lost or unattended [6].

4.2 Multiple User Logging

Multiple user login on a mobile device is still not recommendable, as these devices are not that versatile like computers. Multiple user logins on mobile devices still have difficulty in when it comes to protection and privacy of the accounts. Customizable third-party solutions are available, sharing of mobile phones is not recommended for security purpose.

4.3 Secure Data Storage

Proper file encryption techniques are required for the security of stored data on the mobile phone. The best possible and simplest way to avoid any data compromise is not to store any confidential data on mobile phones [7]**.** As stated by ‘‘Mobile Security Project” under ‘‘The Open Web Application Security Project (OWASP)”[8],the leading top 10 security issues in smart phones is insecure data storage as improper encryption techniques can be easily hacked and confidential data can be revealed.

4.4 Mobile Browsing

More number of users is switching to mobile browsers for its umpteen advantages such as speed, convenience, portability, ease in sharing content and improved user experience [9] but this also opens the doors for security risks. Due to small screen, the complete URL is not visible to users and hence cannot be verified whether the link or URL is safe. User while browsing the web may click onto malicious links, phishing links or compromised links.

4.5 Application Isolation

Smartphone is used for a variety of services ranging from social networking to banking. User must read the application access request for permission agreement before installing any mobile app. This often-overlooked agreement contains valuable information regarding specific permissions on how the app is to access your device.

According to a study done by [10], there are many vulnerabilities of using device public information in apps for user authentication. Identity-transfer attack can be performed, as all the sensitive information required authenticating the user was accessible and can be used by the any app. The two top-rated messaging apps, WhatsApp and Viber which are categorized as vulnerable.

5. ATTACKS ON SMARTPHONE

5.1 Wireless Attacks

Smartphone is most vulnerable to wireless attacks, these attacks intent to target personal and sensitive data. Eavesdropping on wireless transmission is most common attack. Eavesdropping is usually done to steal user credentials, such as usernames and passwords. Not only eavesdropping, wireless attacks can hack the unique hardware identification (e.g., wireless LAN MAC address). LAN MAC address reveals the traces of mobile owner. Bluetooth can be used as a medium for malware propagation [11]. Authors provided a review study of Bluetooth attacks affecting smart phones [12]. A number of studies proposed solution for this class of attacks [11, 13, 14, 15].

5.2 Bluetooth Attacks

Bluetooth is most handy technology and can be used to connect to headsets, synchronize up with cars or computers, and much more but it can be a medium for attackers to access one’s phone and data stored within. Bluejacking , Bluesnarfing and Bluebugging are three basic attacks based on Bluetooth technology [17] . Bluejacking attack allows the hacker to send unsolicited messages to discoverable devices within the area. By Bluesnarfing attack, a hacker using special software can send a request and gain sensitive information stored in a device through the Bluetooth OBEX push profile. This attack can access the invisible devices. Bluebugging attack also allows the attacker to take the control of one’s phone.

5.3 Break-in Attacks: break-in attack allows the hacker to get the full access of the targeted device by means of programming errors, for example, to cause buffer overflows, or format string vulnerabilities.

These attacks can be seen as a stepping-stone for targeting further attacks, for example overbilling attacks or data/identity theft. A number of studies for preventing this class of attacks are discussed in [16, 17].

5.3 Infrastructure-based Attacks: Infrastructure is the base of all services provided by any Smartphone, like placing or receiving calls/SMS/e-mails services, hence the economic and social impact of these attacks are serious, as discussed in [18].

5.5 Attacks against GPRS can be active and passive: An active attack requires attacker’s direct interference to listen, modify, and inject data into the transmission channel, if the attacker is not inside the GPRS, this attack is called an external attack; otherwise, it is an internal attack.

If an attacker taps a communication channel without disturbing the communication to steal some sensitive information, then this type of attack is known as passive attack.

6. GOALS OF THE ATTACKS

6.1 Privacy: the goal of privacy attacks is to corrupt the integrity and confidentiality of data. Privacy can be breached when a smart phone is misplaced or stolen. Due to small size of smart phones, there are more chances of getting them stolen or lost. One the phone is stolen it is much easier for someone to install a spyware on the phone or to read personal data.

6.2 Sniffing: Sensors are used for sniffing attacks on smart phones. e.g. camera, microphone, GPS receiver. To compromise the user's privacy these sensors facilitate a range of new applications. Sniffing allows an attacker to gain access of the information stored in the device and to use the sensors to record all of the user's actions. A preventing scheme against sniffing is proposed in [19].

6.3 Overbilling: An additional fee is imposed on the victim's account and this attack may transfer these extra fees from the victims to the attackers. These attacks are particularly used for wireless smart phones.

7. SUMMARY OF SECURITY SOLUTIONS FOR SMARTPHONE

Attack type	Vulnerabilities	Effect of attack	solution
Physical attack	Stolen/lost System	Privacy is breached	
	manufacturing defects	Weak the security of mobile phone Some of the options are not functional	Re-manufacturing whether it is software or hardware.
	Insufficient APIs management	Malicious code can infect user's data or files	Use only trusted application
Wireless attack	Sniffing / Eavesdropping and spoof computing blocking.	Intrusion to privacy and confidential data can be hacked easily.	disconnect abruptly from the wireless network is suggested
	Insecure Wireless Network.	Sensitive information can be abused w/o disturbing the communication	Use of only trusted network is recommended. Additional encryption / decryption methods to secure communication

Backdoor attack	System bugs and disclosure.	Security of smart phone can be compromised. A backdoor for viruses can be opened	Regularly update device and install strong antivirus software's.
Virus	Finding the Target and replicating file with unidentified source	Unusual behavior of application. Information may be corrupted	Install and timely update Antivirus in your system.
Worms	Transferring information to some unknown source. Transfer malicious program.	Backdoor for hacker can be created.	Use updated Antivirus.
Malware	Downloading of files from fascinated resources.	corrupt computer operations. Gather sensitive information.	update anti-virus regularly, install malware prevent software..
Trojan	Apps download from untrusted resources and hidden malicious functionality	Corrupt computer functionality and intend to gather sensitive information.	Install intrusion detection system designed for smart phones and use anti-virus.
Spam	Malicious code transferred though email. And phishing links	Overflow mailbox with unwanted emails. Consume Internet speed largely. Steals information from email account like Contact list.	Do not open these types of emails. Do not respond to any emails that you never asked for.
Threat	Spoofing, Information disclosure.	Corrupt data. Decline computer security.	Use Cyber threat management system.
Relay Attack	Unsafe network environment.	Information hacked during communication.	Use secure network.

Cold Boot Attack	Unauthorized user can access system RAM and encryption / decryption key.	Weaken data security.	Use powerful encryption decryption method
Brute Force Attack	Attempt repetitively to unlock phone using different passwords combinations and no limit to prevent from hacking.	Password hacked. Slow down the CPU speed.	Setting a limit for password trial to unlock Smartphone.
Denial of Service Attack	Dismiss the mobile broadband connection. Link to bogus Wi-Fi connection	Busy the network. Busy smart phone and block other services.	Use Internet Access Authentication protocol.
SMS based Attack	Phishing links sent by attacker.	Confidential information can be hacked.	Device can be protected by changing the Message settings, and to disallow auto receiving MMS or text.
USB Attack	Access to Root login, enable ADB(open command tool and avail both developer and attacker)	Access to sensitive information stored in phone. Easy Malware injection.	Use apparently inoffensive smart phone charging station
Camera based attacks	Using Camera of Smartphone as spy through Malicious program	Weak the smart phone security. Easy access to data and information stored in Smartphone.	Spy camera could support. Implement effective fine Grained access

8. CONCLUSION

Smartphone are multipurpose device, where security is an important issue. This paper discusses the importance, challenges and threats of Smartphone security. In this paper, authors also investigated the vulnerabilities in Smartphone and different types of attacks that can abuse Smartphone.

REFERENCES

1. https://en.wikipedia.org/wiki/Smartphone, last accessed on 3 March 2019.
2. Khan, Jalaluddin, Haider Abbas, and Jalal Al-Muhtadi. "Survey on mobile user's data privacy threats and defense mechanisms." Procedia Computer Science 56 (2015): 376-383.
3. Ahvanooey, Milad Taleby, Qianmu Li, Mahdi Rabbani, and Ahmed Raza Rajput. "A survey on smartphones security: software vulnerabilities, malware, and attacks." Int. J. Adv. Comput. Sci. Appl. 8, no. 10 (2017): 30-45.
4. La Polla, Mariantonietta, Fabio Martinelli, and Daniele Sgandurra. "A survey on security for mobile devices." IEEE communications surveys & tutorials 15, no. 1 (2013): 446-471
5. https://www.checkmarx.com/2013/11/29/10-challenges-of-mobile-security/ , last accessed on 3 March 2019
6. (https://www.bullguard.com/bullguard-security-center/mobile-security/mobile-protection-resources/8-ways-to-keep-your-smartphone-safe.aspx, last accessed on 8 March 2019
7. https://heimdalsecurity.com/blog/smartphone-security-guide-keep-your-phone-data-safe/, last accessed on 11 March 2019
8. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project, last accessed on 25 March 2019
9. Punchoojit, Lumpapun, and Nuttanont Hongwarittorrn. "Usability Studies on Mobile User Interface Design Patterns: A Systematic Literature Review." Advances in Human-Computer Interaction 2017 (2017).
10. Altuwaijri, Haya, and Sanaa Ghouzali. "Android data storage security: A review." Journal of King Saud University-Computer and Information Sciences (2018).
11. S. C. Peng, “A Survey on Malware Containment Models in Smartphones,” Appl. Mech. Mater., vol. 263–266, pp. 3005–3011, Dec. 2012.
12. I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, “Crowdroid: behaviorbased malware detection system for Android,” in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices - SPSM ’11, 2011, p. 15
13. A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, “‘Andromaly’: a behavioral malware detection framework for android devices,” J. Intell. Inf. Syst., vol. 38, no. 1, pp. 161–190, Jan. 2011.
14. A. Mylonas, S. Dritsas, B. Tsoumas, and D. Gritzalis, “Smartphone security evaluation The malware attack case,” in Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on, 2011, pp. 25–36
15. E. Gelenbe and R. Lent, Eds., Information Sciences and Systems 2013, vol. 264. Cham: Springer International Publishing, 2013
16. A. Mylonas and S. Dritsas, “Smartphone security evaluation The malware attack case,” in Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on. IEEE, 2011, pp. 25–36.

17. Z. Xu, K. Bai, and S. Zhu, “inferring user inputs on smartphone touchscreens using on-board motion sensors,” in Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks - WISEC ’12, 2012, p. 113.
18. A. Houmansadr, S. A. Zonouz, and R. Berthier, “A cloud-based intrusion detection and response system for mobile phones,” in 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), 2011, pp. 31–32
19. Cai, Liang, Sridhar Machiraju, and Hao Chen. "Defending against sensor-sniffing attacks on mobile phones." In Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds, pp. 31-36. ACM, 2009.