Mobile Security Problems and Defensive Methods

Balaji Sarvepalli
Northwest Missouri State University,
Maryville MO 64468, USA

Abstract:- Mobile gadgets has became an integral part of daily lives. In comparison to desktop computers, mobile devices have grown exponentially in recent years. As mobile devices become more common, attackers have more opportunities to steal sensitive data or carry out various forms of assaults on them. We investigated many sorts of security concerns associated with mobile devices and mobile applications. In this research paper, various defensive measures for preventing these security threats in mobile devices were discussed.

I. INTRODUCTION

Every aspect of human existence has an application for mobile devices. Mobile phones can be used for the online bankings and sending files via e-mail, text messages, etc. Through social media, we can communicate with long distance people. Generally, the GSM surveillance has the 6 billion different mobile connections and 3.8 billion internet users worldwide in 2018.

The various different operating systems are Android and iOS. Android operating systems come in a variety of favors, including Nougat, Lollipop, and Marshmallow. In the meantime, there are several iOS versions and only 11 percent of Android users have the most recent version of Android, compared to 86 percent of iOS users.

According to the Open Web Application Security, secure data storing and secure communication threats are serious challenges in the devices, according to their top risks list. In this research paper, described the various important security problems and with the protective methods.

II. RELATED WORK

Khana et al. learn various challenges related to mobile user safety, cell phone threats, mobile risk. The various types of cell phone problems, the application problems and internet searching problems. The Trojan is most important financial-related threats to the cell phone problems. The main security measures for data secure is fingerprint security. The most measures require involvement in all stages in different mobile devices.

Agassi told that checking device problem issues does not have a perfect solution. It is the biggest problem in mobile device security are applying appropriate safety plans, including present security and securing data on devices. To secure important documents and stored files, companies required to use a safe location for devices and to secure application, secure policies must be separate of the devices and applications used on them.

III. MOBILE ATTACKS

According to the Open Web Application Security, insecure data storage and communications are two of the most significant mobile risks.

A. *Secure Storage Data*

Many applications save data in text format, while 89.4 percentage of mobile applications employ weak techniques. A user’s mobile phone is stolen or misplaced, the person who finds it has access to all of the device’s personal and sensitive information another method of obtaining. The purpose of using data from mobile devices is to convince the user to download a malware-infected app.

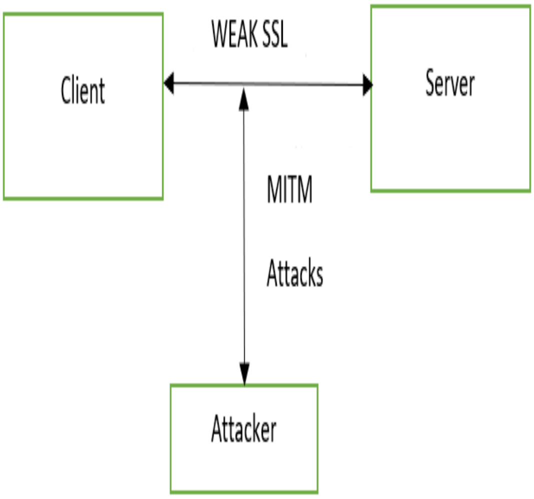

Fig. 1: SSL Weak Communication

B. *Protective Communications*

The majority of communication in a client-server approach takes place in the devices. Mobile apps act the clients, communicate with the server to store various types of the user information. Developer must set up encrypted connectionbetween the mobile app and the server. Due to the implementation of sniffing software, an attackers can now easily sniff communication in between the device and the public WiFi hotspot. If connections are not secure, the attackers steal sensitive information from the users. If the developer uses a bad SSL (Secure socket layer) for their app server communications, an attackers use MITM and phishing attacks.

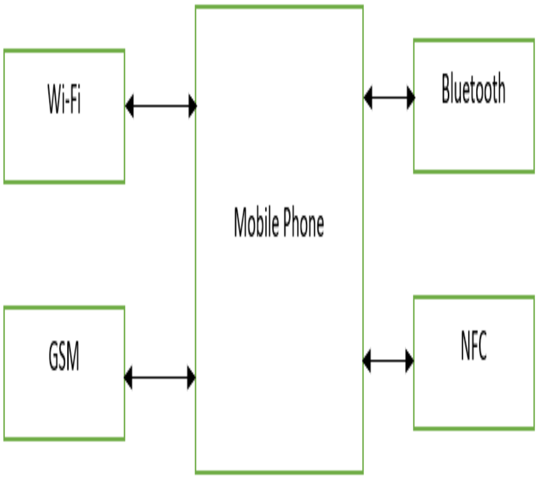

Fig. 2: Communication Technologies

C. *Malware Attack*

Malware software installs without the user understanding in the mobile device. Attacks can be spread via internet insecure applications. Malware has the ability to broadcast text to contact list are to unauthorized users, as well as transfer sensitive information to attackers. Attackers can give complete control of the mobile device.

Spyware attacks Spyware's primary goal is to steal a user's sensitive or personal information and spread it without the user's knowledge.

Trojan These dangerous programs are put into trustworthy executable files, and the Trojan is activated when the user runs them. Trojans can steal data, disable various functions of mobile devices, and allow an attacker to install more software.

WormMobile Worm works similar to a computer worm in that it duplicates and spreads the additional devices.The Worm can despise by messages and other forms of applications requiring user's interaction.

D. *Cross Siti Attacks*

Crosssite scripting attacks are the most dangerous types of online application threats. Many developers use HTML and JavaScript to create hybrid mobile apps, but insecure coding can result in CSS attacks on mobile devices.These defects can be used by attackers to manipulate behavior mobile devices. Share is a popular activity on the devices, and the attackers can reputable website liable to share malicious program links.

IV. DEFENSIVE METHODS

Different entities must implement different mobile security procedures at different phases to protect sensitive data of users. when over various channels for our examples, we'll use Android mobile devices, but the same approaches apply to iOS devices as well. Figure 3 depicts how Android application.apk files reach the end user. Those applications for mobile devices. Because apk files may be decompiled by anyone to obtain the source code, mobile application hosting providers and users can access and edit the source code.

Developers will have the mobile application hosting providers like mobile device operating system manufacturers, and mobile phone must all work together to protect mobile devices from security attacks.

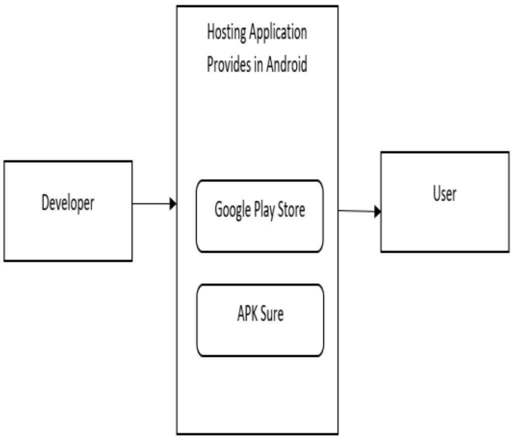

Fig. 3: Developer and user APK Files

A. *Security Measures by Developer*

Secure Coding Security should be a top priority for developers, and security measures should be implemented at every level of the mobile app developmentprocess. Using strong cryptographic methods with long keys and values are updated Secure socket layer safe interaction between the mobile app and some of the security practices.

B. *Security Measures by User*

Installing Unknown Applications In trying to make programs public, trusted app hosting companies such as Google Play Store or Apple App Store extensively scan them for dangerous malware. As a result, there will be relatively few security concerns when downloading programs from these marketplaces.

Application update and OS Mobile Phone application must update their apps whenever a new version of the software is released by the developer. Occasionally, developers will provide to fix a security flaw in their application. Operating system are more crucial than application updates.

C. Security Measures

Android developers regard Play Store to be a reliable hosting source for Android application, while Apple App Store is a rusted hosting service for iOS apps. The application stores must monitor application on the devices and, if any security issues arise, must ban programs quickly. Currently, virus checks are performed on mobile apps before they are made public on the Google Play Store and the Apple App Store.

They recommend applications to assign security scores to mobile apps based on the security measures they implement.Table.1 shows the example,the mobile application stores assigns the scores to application and have the higher value in these application in search and recommend, developers be compelled and to be includes perfect security features in the application.

Secure Problems	**Conditions**	**Scores**
Secure the Data Storage	There will be no Security, Strong and weak	0.1
Secure communication	No Security, Strong and weak	0,1
Malware	No	1
Other problems	No	1

Table 1: Secure problems and score tables

V. CONCLUSION

Mobile device applications are developing at an unsustainable rate, managing security in these devices is becoming increasingly difficult. We looked at common mobile security issues like data storage security, communication security,cross-site scripting, and malware problem. This research paper we analyzed and presented a few defensive strategies that developers, mobile users, and app hosting providers should use to prevent issues in the mobile phones. It recommended scoring system for the applications in the devices.It upgrades applications to secure required in their applications, because it compares applications. They have the option of selecting an application with a more security rating, so that we can secure the mobiles phones.

REFERENCES

[1.] Al-Qurishi, M., Al-Rakhami, M., Alamri, A., Alrubaian, M., Rahman, S.M.M., Hossain, M.S.: Sybil defense techniques in online social networks: a survey. IEEE Access 5, 1200–1219 (2017)

[2.] Bagga, P., Hans, R.: Mobile agents system security: A systematic survey. ACM Comput. Surv. 50(5) (Sep 2017). https://doi.org/10.1145/3095797, https://doiorg.ezproxy.nwmissouri.edu/10.1145/3095797

[3.] Balaji, S., Julie, E.G., Robinson, Y.H., Kumar, R., Thong, P.H., et al.: Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. Computer Standards & Interfaces 66, 103358 (2019).

[4.] Garba, A.B., Armarego, J., Murray, D., Kenworthy, W.: Review of the information security and privacy challenges in bring your own device (byod) environments. Journal of Information privacy and security 11(1), 38–54 (2015)

[5.] Lee, S., Lee, S., Kang, T., Kwon, M., Lee, N., Kim, H.: Resiliency of mobile os security for secure personal ubiquitous computing. Personal Ubiquitous Comput. 22(1), 23–34 (Feb 2018). https://doi.org/10.1007/s00779-017-1098-x, https://doiorg.ezproxy.nwmissouri.edu/10.1007/s00779-017-1098-x

[6.] Olalere, M., Abdullah, M.T., Mahmod, R., Abdullah, A.: A review of bring your own device on security issues. Sage Open 5(2), 2158244015580372 (2015)

[7.] Pawlick, J., Colbert, E., Zhu, Q.: A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. ACM Comput. Surv. 52(4) (Aug 2019). https://doi.org/10.1145/3337772, https://doiorg.ezproxy.nwmissouri.edu/10.1145/3337772

[8.] Shrestha, P., Saxena, N.: An offensive and defensive exposition of wearable computing. ACM Comput. Surv. 50(6) (Nov 2017). https://doi.org/10.1145/3133837, https://doi-org.ezproxy.nwmissouri.edu/10.1145/3133837

[9.] Singh, V.V., Wang, J.: Nano/micromotors for security/defense applications. a review. Nanoscale 7(46), 19377–19389 (2015)

[10.] Sun, L., Dou, Y., Yang, C., Wang, J., Yu, P.S., He, L., Li, B.: Adversarial attack and defense on graph data: A survey. arXiv preprint arXiv:1812.10528 (2018)