International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 12 (2018) pp. 10256-10259

Review of Mobile Security Problems and Defensive Methods

PMD Nagarjun[1] and Shaik Shakeel Ahamad[2]

[1&2]Department of Computer Science & Engineering, K L University, Vijayawada, India.
[1]Nagabot Software Development Pvt. Ltd., Nellore, India.
[2]CCIS, Majmaah University, Majmaah, Kingdom of Saudi Arabia.
[1]Orcid: 0000-0003-0386-9556, [2]Orcid: 0000-0002-9619-0907

Abstract

Mobile devices integrated into daily activities of people's life. Compared to desktop computers the growth of mobile devices is tremendous in recent years. The growth of mobile devices opens vast scope for attackers to steal sensitive data or to perform other types of attacks on these devices. In this paper, we studied different types of security risks involved in mobile devices and mobile applications. We discussed various defensive mechanisms to prevent these security risks in mobile devices.

Keywords: Mobile Attacks, Mobile Security, Data Privacy, Mobile Applications, Malware Attacks.

INTRODUCTION

Mobile devices are having applications for every activity of human life. Mobiles are used to perform bank transactions, and sensitive data transfer in the form of E-mails, messages, etc. Mobile devices are used to connect with family and friends through social networks. According to GSMA Intelligence, in 2017 there are 5 billion unique mobile subscribers around the world, and 3.3 billion mobile internet users.

Most popular operating systems used in mobile devices are Android and iOS. There are different versions of Android operating systems like Nougat, Lollipop, Marshmallow, etc., similarly different versions of iOS are iOS 10, iOS 9, iOS 8, etc. Compared to iOS 86% only 11% of Android mobile users having the latest Android operating system.

Open Web Application Security Project (OWASP) [1] analyses mobile risks, according to their top risks list, insecure data storage and insecure communication risks are most severe problems in mobile security.

In this paper, described some significant security problems in mobile devices along with some defensive methods. This paper is structured as follows. Section 2 contains related work. Section 3 describes security problems. Section 4 discusses defensive methods, and Section 5 gives the conclusion.

LITERATURE WORK

Khana et al. [2] studied different security-related challenges for mobile users, mobile threats, mobile vulnerabilities. Different types of mobile risks involved in their study are physical based threats, application-based threats, network-based threats and Web-based threats. A botnet is one of earnest money related threat in all mobile vulnerabilities. According to them one of important security defense mechanism for data privacy and mobile security is Biometric authentication. Security mechanisms need to be involved in every stage of mobile application development.

Cifuentes et al. [3] analyzed the vulnerabilities found in mobile applications related to health care. They categorized mobile health apps into six groups based on apps functionalities and downloaded ten android apps related to each group from Google play store to analyze vulnerabilities. Total 157 vulnerabilities detected in 60 mHealth apps. Their results show that apps with remote monitoring functionalities have the most number of vulnerabilities and also vulnerabilities in these apps contain high-risk levels. Their results show that 64% of vulnerabilities in mHealth apps related to untrusted input.

Chatzikonstantinou et al. [4] classified cryptographic weakness in mobile applications into weak cryptographic algorithms, weak cryptographic keys, weak implementation of cryptographic algorithms and weak parameters. They downloaded 49 random android apps from Google play store, and they performed manual static analysis and dynamic analysis of those applications. Their results show that almost 87.8% of Android apps are using weak cryptographic algorithms and 12.2% of android apps not implemented any cryptographic algorithm at all.

Shukla et al. [5] implemented a new key agreement and authentication protocol for Electronic Health Record systems. EHR system has different types of users like doctors, lab staff, patients, and insurance agency so in this system authentication and proper key agreements are critical. The proposed protocol based on commitment scheme and it will stop communications if it encounters authentication failure. They stated that because of binding/hiding nature of protocol it is very effective to prevent Man in the middle attacks in wireless communications.

Choo [6] stated that improvements in new technologies and developments in security measures needed to be parallel. According to Routine activity theory crime occurs when there a weak guardianship, targeted device and motivated attacker. Cloud storage apps like DropBox, Google Drive, One Drive,

etc., are favorite targets for attackers because of their functionality to store a significant amount of user data. They investigated on compromised celebrities iCloud accounts and stated that most of the attacks are targeted attacks on security questions, usernames, and passwords.

Agasi [7] stated that there is no complete solution to prevent mobile security problems. The main issues with the mobile security are implementing proper security policies, integrating current security and protecting data in mobile devices. To secure business documents and data, corporates need to implement a secure environment for mobile devices, threat management and security policies need to be independent of devices and operating system used in them.

MOBILE ATTACKS

According to OWSAP some of the top mobile risks are insecure data storage and insecure communications.

A. Securing Data Storage

A lot of mobile applications store information in plain text format, and 87.7% of mobile apps use weak cryptographic algorithms [4]. If a mobile device is stolen/lost from its user, then whoever found that device can access all personal and sensitive information of that device. Another way of stealing data from mobile devices is by encouraging the user to install malware infected mobile application [8].

B. Securing Communications

Most of the communications happened in mobile devices in a client-server model. Applications in mobile devices act as a client, and they communicate with their servers to store different types of data belong to the user. The developer needs to implement secure communication between their mobile application and their server. With the development of sniffing tools it easy for an attacker to sniff communications between the mobile device and public Wi-Fi hotspot. If the connections are not secure, then the attacker can steal sensitive data from the user. If developer setup weak SSL for their app server communications then the attacker can perform Man-In-The-Middle (MITM) attacks and phishing attacks fig. 1.

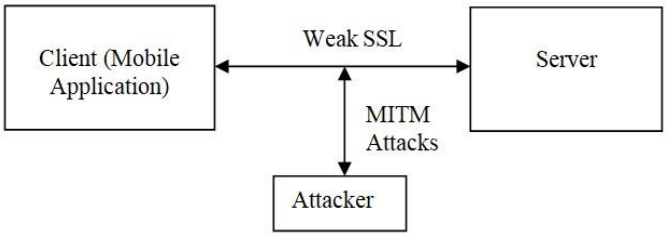

Figure 1: Weak SSL Communication

Fig. 2 shows different communication technologies used by a mobile device.

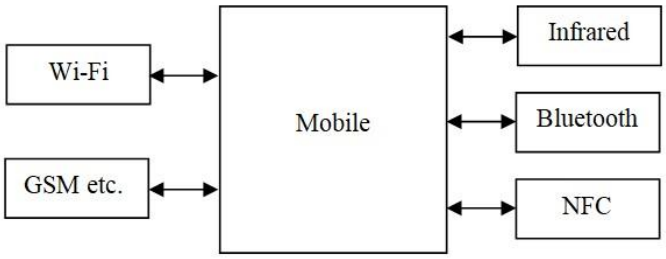

Figure 2: Different communication technologies

C. Cross-Site Scripting Attacks

Cross-site scripting (XSS) attacks are one of severe web application attack. A lot of developers uses HTML and JavaScript to create hybrid mobile applications, insecure coding of these hybrid mobile applications causes XSS attacks in mobile devices. Through these vulnerabilities, an attacker can affect the behavior of the mobile device. Sharing is one of favorite activity on mobile devices, and an attacker can share malware app link from the trusted website by exploiting XSS vulnerability on that website.

D. Malware Attacks

Malware or malicious software installs on user's mobile device without user's knowledge [9]. Malware can spread through the internet or unsecured applications. Malware can send messages to the full contact list or unwanted numbers, and it can steal and send sensitive information to attackers and attackers can gain full control of the mobile device through that malware [10]. Different categories of most common mobile malware are listed below.

Worm: Mobile Worm [11] functions as typical computer worm, it will replicate itself and spread to other mobile devices. Mobile Worms can spread through SMS or other communication sources without user interaction.

Trojan: These malicious codes (Trojan) inserted into trusted executable files whenever the user executes these files that Trojan will be activated. Trojan can steal information, disable some functionality of mobile devices and can open the door to the attacker to install other types of malware [12].

Spyware: The primary purpose of Spyware [13] is to steal user's sensitive or personal information and to spread that information without user's knowledge.

Ghost Push: This malware gets root access to the mobile device then installs malicious applications, convert it to system application and losses root access permissions. Sometimes users need to factory reset their mobile devices to remove these infections. This type of malware can steal user information [14].

DEFENSIVE METHODS

Mobile security measures need to be followed by different entities at different stages to protect sensitive data of the user

in mobile devices storage or while communicating over different channels. We consider Android mobile devices for our examples, but same methodologies are also applicable to iOS mobile devices. Fig. 3 shows how .apk files of Android applications reach the end user. Those mobile applications .apk files can be decompiled by anyone to get the source code, so it is possible for mobile application hosting providers or users to read or modify the source code.

To protect mobile devices from security attacks there need to be a correlation between developers, mobile application hosting providers like Google play store, mobile device OS manufactures and mobile device users [2].

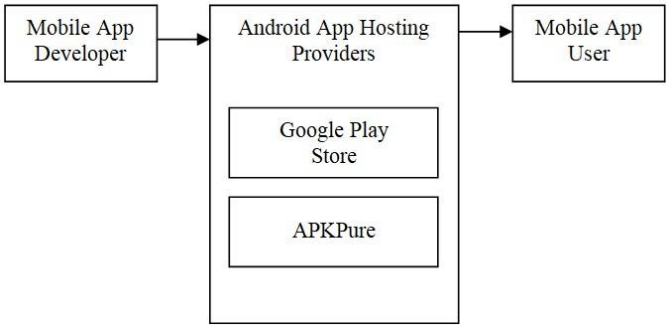

Figure 3: APK file flow from Developer to User

A. Security Measures by Developer

Secure Coding: Developers need to consider security as a major requirement and need to implement security steps at every stage of mobile application development. Some of the security practices are like using strong cryptographic algorithms with long keys and implementing proper TLS/SSL for secure communication between mobile app and server.

Proper Updates: Developers need to release updates to their mobile applications whenever there is a security issue in their mobile app. Update apps if libraries used in their apps had a security update.

B. Security Measures by User

Update Apps and Operating System: Mobile app users need to update their app whenever developer releases a new update. Sometimes developers release an update to patch a security issue in their apps. Compared to application updates Operating System updates are most important [15].

Stop Rooting Devices: Rooting means getting full access to different subsystems in Android mobile devices. Rooting breaks security model of the mobile device and may cause installation of malicious apps. These malicious apps can access data from other apps.

Installing Unknown Applications: Trusted app hosting providers like Google Play Store or Apple App store [16] checks apps thoroughly for malicious codes before making them public. So there will be very few security issues when apps downloaded from these stores. Third-party app stores like APKPure, APKMirror may contain apps with malicious code, so downloading .apk files from these stores or some other places over the internet and installing them on mobile devices may cause a lot of security issues [17].

C. Security Measures by App Hosting Providers

By default, Android developers consider Google Play Store [18] as a trusted hosting provider for their Android apps and for iOS applications Apple App Store is trusted hosting provider. These mobile app stores need to monitor apps on mobile devices, and if there are any security issues in those apps, these stores need to disable those apps immediately. Currently, Google Play Store and Apple App Store perform malware checks [19] on mobile apps before making them public.

We suggest that app stores can provide security scores to mobile apps based on their security measures. They can calculate security scores by performing static analysis and partial dynamic analysis on mobile apps. Table. 1 shows example security problems and corresponding security scores. If mobile app stores provide security scores to mobile apps and give more value to these apps in searches and recommendations, then it may force developers to follow proper security measures in their mobile applications.

Table 1: Security Problem and Corresponding Score

Security Problems	Condition	Score
Securing Data Storage	No Security Weak Security Strong Security	0 0.5 1
Securing Communications	No Security Weak Security Strong Security	0 0.5 1
Malware or Malicious Code	No Yes	1 0
Unpredictable Behavior at Runtime	No Yes	1 0
Other Security Problems	No Yes	1 0

Users can install apps based on security score. But this scoring method involves a lot of false negative and false positive cases and requires a lot of recourses to analyze security issues of every mobile app.

CONCLUSION

Mobile devices and their applications are growing too rapidly, so it is challenging to handle security in these mobile devices. We reviewed popular mobile security problems like securing data storage, securing communications, cross-site scripting

attacks and malware attacks. This paper analyzed and presented some of the defensive methods needs to be followed by the developer, mobile user, and app hosting provider to prevent security issues on mobile devices. We suggested security scoring system for mobile apps at app stores. Which may improve mobile apps security by forcing developers to consider security as a requirement in their apps because compared to other similar apps the user may choose app with higher security scores.

REFERENCES

[1] OWASP. (2016). Owasp Mobile top ten project. https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

[2] Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. Procedia Computer Science, 56, 376-383.

[3] Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015, August). Analysis of Security Vulnerabilities for Mobile Health Applications. In 2015 Seventh International Conference on Mobile Computing and Networking (ICMCN 2015).

[4] Chatzikonstantinou, A., Ntantogian, C., Karopoulos, G., & Xenakis, C. (2016, May). Evaluation of Cryptography Usage in Android Applications. In proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, pp. 83-90.

[5] Shukla, V., Chaturvedi, A., & Srivastava, N. (2015). A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography. Communication on applied electronics (CAE), 3(3), 16-21.

[6] Choo, K. K. R. (2014). Mobile cloud storage users. IEEE Cloud Computing, 1(3), 20-23.

[7] Agasi, O. (2015). Encapsulating mobile security. Computer Fraud & Security, 2015(6), 10-12.

[8] Mobile malware. (2017, March 28). In Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Mobile_malware&oldid=772698711

[9] Malware. (2017, July 6). In Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Malware&oldid=789247319

[10] Mercaldo, F., Visaggio, C. A., Canfora, G., & Cimitile, A. (2016, May). Mobile malware detection in the real world. In Software Engineering Companion (ICSE-C), IEEE/ACM International Conference on (pp. 744-746). IEEE.

[11] Tiwari, S., & Tiwari, V. (2016, September). Bluetooth Worm Propagation in Mobile Networks. In Micro-Electronics and Telecommunication Engineering (ICMETE), 2016 International Conference on (pp. 235-239). IEEE.

[12] Otrok, H., Mizouni, R., & Bentahar, J. (2014, November). Mobile phishing attack for android platform. In Innovations in Information Technology (INNOVATIONS), 2014 10th International Conference on (pp. 18-23). IEEE.

[13] Spyware. (2017, July 2). In Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Spyware&oldid=788660061

[14] New "Ghost Push" Variants Sport Guard Code; Malware Creator Published Over 600 Bad Android Apps (2015, September). Trendlabs Security Intelligence Blog. http://blog.trendmicro.com/trendlabs-security-intelligence/new-ghost-push-variants-sport-guard-code-malware-creator-published-over-600-bad-android-apps/

[15] Platform Versions (2017, July). Android Developer. https://developer.android.com/about/dashboards/index.html

[16] App Store (2017, July). Apple Developer. https://developer.apple.com/support/app-store/

[17] When Malware Goes Mobile. (2017) Sophos Security News and Trends. https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx

[18] Google Play. (2017, July). Google Inc. https://play.google.com/store?hl=en

[19] Mobile Threat Report. (2016). McAfee. https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf