Threats and Vulnerabilities of Mobile Applications

4

Thangavel M.
https://orcid.org/0000-0002-2510-8857
Thiagarajar College of Engineering, India

Divyaprabha M.
Thiagarajar College of Engineering, India

Abinaya C.
Thiagarajar College of Engineering, India

INTRODUCTION

Today's mobile smartphones are very powerful, and many mobile applications use wireless multimedia communication. The attack faced by the mobile phones are increasing day by day. The downloadable mobile application has many types of security issues. Malicious apps look like fine in downloadable sites, but they specially designed to commit an attack. Application-based threats may generally be fit into the following categories: Malware, Spyware, Physical Threats, and Vulnerable Application. Malware is a software that performs a malicious action when it is installed without your knowledge. It can even make changes to your phone bill and also an attacker can gain control over it. Spyware is mainly designed to collect all the private information of the system without your knowledge. It specifically targets the browsing history, contact list, user location, email, etc. Privacy threats are somewhat similar to Spyware, but it gathers sensitive information rather than performing their action. Vulnerable applications allow an attacker to access sensitive information, perform undesirable actions, stop service from functioning correctly, or download apps to your device without your knowledge. As mobile devices are constantly connected to the internet and frequently used to access web-based services, web-based threats will cause persistent issues for mobile devices. Then server-side attacks to mobile devices are also increasing, any communication that happens between the application and the user outside the mobile phones happens through a server. Thus, this becomes a primary target that gets exploited by hackers. Some common reasons for this are small security budgets, lack of security knowledge in a new language, too much dependability on the mobile OS for security updates and responsibility, and vulnerabilities due to cross-platform development and compilation. The easiest way to overcome this server vulnerability is to scan mobile devices. Other vulnerable components of the mobile devices are incorrect permission setting that allows access to controlled functions such as the camera or GPS, and obfuscation where functionality or processing capabilities are hidden or obscured from the used emails, email addresses, and attached data and malformed SMS causing devices to crash. Sometimes untested mobile applications also cause the attack to the device, that is the users tend to download apps from third-party vendors instead of downloading from the app store; many of these apps don't have a clear source and becomes vulnerable due to the coding errors, which are not updated enough to prevent exploitation. The excessive power consumption applications are also vulnerable to the mobile devices that run continuously in the background, that drain the battery thereby reducing the system availability.

DOI: 10.4018/978-1-7998-3479-3.ch034

BACKGROUND

Based on the research, the chapter shows that the major attacks are phishing attacks, attacks based on the use of phone cameras, and a screenshot attack "capture me". By this threat of the mobile application, the user credentials are stolen by an attacker. Several recent works have studied the issue of obtaining private information on smartphones using multimedia devices such as microphones and cameras if the camera is affected by malicious software. Moreover, most of the users have the impression that smartphones are just the phones installed with a variety of software and don't think of them as handheld computers that are more vulnerable to cyber-attacks. A recent survey reported that 267,259 malware-infected apps have been found, among which 254,158 reside on the Android platform (Daojing, 2015). It also suggested that the number of malware in apps has increased by 614% since 2012. The wide use of smart devices (phones and tablets) encourage the financial institution to consider mobile banking applications as a necessary service to their clients. This issue should be addressed by both preventive approaches and effective detection techniques. For preventing, the application developer should ensure this app by policies governing secure coding and privacy, which do not access any unnecessary information. Then the App market administrator should strictly verify every uploaded application and remove the suspicious app. Detecting techniques are based on signature-based or anomaly-based. In signature-based, the malware is identified by comparing the signatures with the known signature, and in anomaly-based, the normal behavior of the system is monitored and it checks for deviations from the normal behavior.

THREATS

In information security, a threat is a danger or a possibility for an attack that might exploit a vulnerability to breach the security system and therefore cause huge damage to the system. It can be either intentional or accidental. As the population of smartphone users is rapidly increased, the hackers are targeting mobile phones, which have a wide variety of applications. There are many types of threats that are classified as application-based, web-based, and server-side threats (Delac, 2017).

APPLICATION-BASED THREATS

The number of malware, spyware has been increased in mobile devices by more than 600% since 2012, with over 250.000 malware in the Android operating system alone (Daojing 2015). The malware is malicious software that refers to viruses, worms, Trojan horses, ransomware, which cause the deviation from the normal behavior of the system. The malware has many types of malicious behaviors which include leaking sensitive data or stealing credentials, restricting device usage, mobile distributed denial of service, etc. The recent malware is the root exploits (jailbreak exploits) by which the attacker gain access privileges. In mobile, the official application stores such as Google Play and Apple App Store will scan the application they offer for traces of malware, spyware, and remove the application is any threat is detected. The main threat lies in application installation and application handling in mobile devices. The security of the mobile users won't end once an application has been installed, then the user is asked to make a decision regarding the security and privacy while handling the application. Moreover, it will ask the user for permission to access the information in the mobile device. The application installed are tends to update automatically, in that time it can even change the permission settings, which become a major threat.