International Conference on Recent Trends in Engineering Science and Technology (ICRTEST 2017) ISSN: 2321-8169
Volume: 5 Issue: 1(Special Issue 21-22 January 2017) 553 – 556

Enhancing Security of Android Phones

Tejaswini Bhandarkar
TGPCET, RTMNU, Nagpur, India
tejaswinibhandarkar@gmail.com

Prof. G. Rajesh Babu
Coguide,TGPCET,RTMNU,Nagpur,India.

Abstract— Use of mobile commerce for commerce for conducting commercial transactions online is increasing rapidly. A wide range of wireless devices which includes mobile phones, tablets provide an easier way for mobile payments and M-commerce. Risk associated with such devices such as loss of private information is also increasing. The basic requirement for using secure M-Commerce application is a secure mobile operating system. Without a security feature or secure application on the device, it is not possible to have secure Mobile-transaction. Among many operating system used for mobile devices, android operating systems are widely used. Though Android Systems are good in memory management they are also vulnerable to security attacks. Such security attacks make the phone unusable, cause unwanted SMS/MMS (short message service/ multimedia messaging service) billing, or expose private information. There are two doors for attacker to attack a smart phone. The first is to get users to download, install, and run software that contain unethical codes such as virus, worms etc. and the other is to attack device directly by using software vulnerabillties. This paper presents security assessment for Android with an overview of security architecture for android. The Paper also list various threats to android devices and there countermeasures.

Keywords- *Android Systems, mobile payments, software vulnerabilities.*

*****

I. Introduction

In earlier days phones were only used to call other person and to talk to them. As mobile computing technology is growing things have changed. Today's mobile phones have features in common to that of a computer. In fact it could be seen that today's smartphones are simply computers with extra hardware. In this mobile computing world androids are gaining popularity. International data corporation believes that android will maintain its overall leadership position in mobile device market throughout 2016.

Android provides an environment for application to execute in mobile devices. The package of android includes operating system, application framework and core application. Android kernel is similar with UNIX operating system kernel that is the base of the stack, and that is employed for its device drivers working, memory management tasks, method management and networking tasks. Next level contain android native libraries which are incorporated via java native interface. The next level or layer of this architecture is the Android runtime, containing the DV machine and the libraries. And last is application layer which provides various applications such as web browsers, email client etc. Android applications are written in java.

Such architecture helps the developers to develop various android applications. In case of android, any developer can create an android application and place it in Android Public Market. These applications are merely self signed and no review is conducted to verify safety of that application. Because of such a procedure users can be trapped in downloading malware. So android users should check comments and how many times a application is downloaded before downloading that application in their phones. In contrast iOS operating system which is

also an evolving operating system for Apple products support applications only from App Store. Thus iPhone users can never install

and run application unless it is signed by Apple's private encryption key .Another security feature which is better in iOS than in android is Application Sandboxing. Application Sandboxing is a boundary for applications which limit application's access area that is it prevent applications from accessing system or other applications. In case of android each application has its own sandbox and it can be customized by users, thus users can be trapped by attacker and attacker can access their private information. But in case of iOS all applications share same sandbox which can not be customized thus apple limits action of applications.

II. Android Security Architecture

As a historical fact the founders of famous Android were four men namely Andy Rubin, Rich Miner, Chris White and Nick Sears .The formal launch of first version that is 1.0 of android took place on September 23, 2008 and first device to run it was the HTC dream [4]. Android runs on top of Linux 2.6 kernal, following is android security architecture as given by A. Gunasekera in book Android Apps Security [4].

A. Privilege separation

With privilege separation, android can deny one of more common types of attack. Like UNIX, android operating system requires that every application should have its own user identifier (uid) and group identifier (gid). This ensures that one application does not have permission to access other applications. Thus with this an application might not be able to use device's resources to connect to remote server or an application can not read private information directly from device memory. This feature is called sandboxing [4].

B. Permissions

Various applications requires various types of permissions to use system component. But who decides whether to grant or deny access? Android allows end user to perform this final approval process. Note that permission need to be granted at time of installation [4].

III. Threats to the Android Framework

As mentioned earlier there are two doors for attacker to attack a smart phone, following are threats which comes in user smart phone when user download, install, and run software that contain unethical codes. These attacks are possible because android applications are not reviewed before they are available for download by user. With following attacks attacker can collect user's private information, send some fake service messages, delete user's important data, make some function of system or some popular software useless, install other malicious applications like worms or botnets, these can also serve as method for committing various cyber crimes including phising etc.

A. Malwares(virus, worms,Trojan horse)

Virus are malicious code that attach themselves to a file and execute when that file execute. Also while executing they may replicate themselves and infect other files. Worms like virus are also self replication malicious code but unlike virus they do not require executing a file to spread their action. This malware was ported to mobile platforms after introduction of Caiber [5], which is a worm that spreads through Bluetooth links. Trojan horse unlike virus and worms do not self replicate instead they gain control over device while pretending to do some useful function. The very first android Trojan horse was Fake Player and was discovered in August 2010 [6]. This malware was fake Microsoft window media player icon and was responsible for sending SMS without user's permission [6]. With this a GPS malware was also reported by Symantec. This malware could connect to a remote server to transfer all mobile data [6] [7]. In 2011 a new generation of malware called Droid dream malware was discovered [6]. The Trojan gained root access to Google Android mobile devices in order to access unique identification information for the phone. Once compromised, the infected phone could also download additional malicious programs without the user's knowledge as well as open the phone up to control by hackers.

B. Advanced persistent threat (APT)

APT is a cyber attack launched by a group of sophisticated attackers, determined attackers and coordinated attackers who systematically compromise the network of specific target or entity for prolonged period [10]. APT also known as targeted threats are targeted on enterprises and commercial organizations. Such attacks mostly aims at accessing internal system to steal valuable data and trade secrets. Traditional security measures like firewalls, gateways etc can stop malware but not such attacks. Significant breaches at national banks and international banks like RSA and worldwide Payments have created headlines, and consistent with a recent ISACA survey, twenty first of respondents reported that their enterprise has already been been by associate APT, and sixty three suppose it's solely a matter of your time before their enterprise is targeted [15]. About two- thirds of the respondents said the mobile endpoints used in their organizations had been hit by malware and 40% also said these endpoints were the entry point for an APT-style attack aimed at specific individuals to gain access to corporate information.

C. Privilege escalation vulnerability

Because android is based on linux kernel and thus it applies the discretionary access control (DAC) on the file system level, this means user get root-level privilege, which is the goal of exploiting privilege escalation vulnerability .

D. RootKit

Rootkit is a malicious or harmful application which gains authority to run in a privileged mode. Such harmful applications usually hide their existence from the user by modifying standard operating system functionalities. Recent research efforts indicate the potential of this attack strategy and classify it as an emerging threat to mobile security. Droid Dream is one of malware which utilizes this root privileges. The two security issues that fail due to these attacks are permission system and priority associated

activity. But developers could easily manage to prevent such attacks [14].

IV. Security Mechanisms Improvement Solutions:

I.Permission Mechanism

After the comparison of Android and IOS, we found that users with Android system should be smarter than users with ISO system. The security mechanics of Android application markets relied on its users to find stealthy malwares and report them. Even the Official Application Market only provides an automatically scanning mechanic (Bouncer) to help user detect malwares. In addition, compared with IOS which only have one official Application markets, there are so many third-party applications markets and no unified supervision. Most of them allow developers to upload their application without any inspection. Some of them are even the beneficiary of malwares or adwares. Such mechanism is not reliable. As a service industry, Android is responsible for providing the best services for users. It should not rely so heavily on users to solve the problems. In addition, the backgrounds of users are wide, and most of them lack professional knowledge, and the developers of malwares are always expertise of information technology. Even though users have high awareness of Android security, they also have difficulty to defeat with the expertise all by themselves. Therefore, we attempt to propose two solutions to help users protect themselves.

1. Selective App Permission Controls

Android's most attractive points are freedom of choice and controls over your phone. User should be able to customize their phone to tailor their needs. But until now, Android is currently unable to/does not give control to the user regarding about security control. In contrary, iOS will ask the user explicitly for features that an app wants to access such as location, contacts. It works flawlessly, and the app still works even though full permission is not given. Granted not every access can be controlled in iOS, it is still more control than what Android gives. When an app is installed from Google Play, a pop up will show the summary of permissions that are required by the app. There are not so many things you could do except accepting everything that has been offered. A better cautionary message would be a special warning popup for sensitive application permission. The solution we proposed is selective android permissions, which was actually a secret feature in android 4.3 (Freml 2013). Unfortunately it seems that the feature is far from ready since it has been removed from new android 4.4. Another thing that could be integrated to the android stock OS regarding app permission is the detailed information and warning, one by one breakdown of the permission. This is a feature that can be found from some custom ROM (custom android OS) such as Cyanogenmod.

2. Point System and Technical User Review

Users' feedbacks are very valuable information for everyone. Google is using it to track applications, for developers it can be used to improve their application and in a survey done by us, 70% of users stated that they use app reviews to assess the quality of the app. In this discussion, we want to propose a point system for every useful user review and a special section for technical review. A useful review can be easily classified as having 75% or more people agree that your review is useful. Special section for technical reviews will allow only users with developer's account meaning they have the tools to monitor the

app they are review. They can see what the data the app is using or what data the app is sending, etc. Our suggestion can be backed by a recent controversy (Savov 2013), an iMessage app for android that takes your apple email and password through a third party unknown server in China. The app has since then been pulled from the play store and people have been informed to change their passwords. This incident could have cause less damage if there's a dedicated review section where user can read technical review before installing the app. The point system will act as an incentive for a more well thought out and in depth review. A good review takes time and reviews could be rewarded with gift cards or Google play credit.

2.Root Exploit Mechanism

Rooting is always the first step for attackers. When they got the root permission, they could do a lot of harmful works, such as information thefts and DDoS attacks. Nowadays, mobile devices are gradually replacing PC to achieve many important, such as payment, website browsing and files transmit. This change is good for both vendors and users. The key issue of the rooting problem is that both users and attackers have the incentive to root Android systems. The expected security situation is shown in Figure 2, but the realistic situation is Figure 3. To solve this problem, we suggest two solutions.

Technical Data Screenshot/report Review content

1. Root Access Authorization

This solution is expected to change users' desire of rooting exploits. For Android system designer, it is extremely hard and expensive to design an Android operation system which could defend the attack from both users and attackers. In other choice, vendors could allow users to access root. In most of situation, amateurs who attempt to find a root exploit only want

to show off their talents. If vendors provide an official channel for users to gain root permission, the

incentive will disappear. In fact, there are many vendors, such as HTC, Asus, Google and Sony allow users to unlock their devices or change their operating system entirely.

2. Rooting and Custom ROM

Rooting is the process of unlocking full access to your phone's system files, which will result in even more control over your phone. You can alter the Linux system to perform better or add binaries but the main purpose for rooting is to install a custom ROM. Custom ROM is a custom operating, community made, and it's based on Android OS. The purpose is to improve performance and experience of users' android device. The process of rooting your phone and installing a custom rom is not a simple task and is seen as a dangerous activity to the average android user and a big percentage of them do not realize that it exists. While the risk of problem such as bricking your phone is there, the chance is very low and the process is reversible.

V. Conclusion

Android operating system is widely being used in mobile phones .In this paper we presented an Android Security Architecture with briefly explaining security threats to android phones and proposing secured solutions of Root Access Authorization and Permission Mechanisms for enhancing security of Android Phones.

References

[1] An Insight into the Security Issues and Their Solutions for Android Phones.[2015]

[2] "Mobile Attacks and Defense", white paper copublished by the IEEE computer and Reliabilty Societies, 2014.

[3] Countering the Advance Persistent Threat challenge with deep discovery, white paper, copublished by Trend Micro white paper April 2013.

[4] Sheran A.Gunasekera, "Android Architecture", in Android Apps Security, Ed.New York: Apress, 2012.

[5] Mobile Aattacks and Defense , white paper copublished by the IEEE computer and Reliability Societies,July/August 2011.

[6] Google Android: A Comprehensive Security Assessment, copublished by the IEEE computer And Reliabilty Societies, March/April 2010.