Threat Analysis of Smart Mobile Device

Shi Pu[1], Zhouguo Chen[2], Chen Huang[3], Yiming Liu[4] and Bing Zen[5]
[1,2,3]Science and Technology on Communication Security Laboratory, 610041, China
[1,2]Email: 271193918@qq.com, czgexcel@163.com

Abstract

With the development of telecommunication and network bands, there is a great increase in the number of services and applications available for smart mobile devices while the population of malicious mobile software is growing rapidly. Most smart mobile devices do not run anti-malware programs to protect against threats, such as virus, trojan, ddos, malware and botnet, which give the chance for hackers to control the system. The paper mainly analyses the typical threats which smart mobile devices face.

1. Introduction

Smart Mobile Device is an electronic device, mainly referred to smart-phone or tablets, which has combined the portability of cell-phones with the computing and networking power similar to PCs. These devices often have an independent operating system, which are generally connected to other devices or networks via different protocols such as WiFi, 3G, 4G, Bluetooth, NFC and so on.

In 2007, iPhone came to the world and redefined the usage of smart-phone. In 2009, smart-phone with Android system became a milestone in the history of mobile Internet. Mobile devices and apps are becoming ubiquitous to both personal and professional lives, allowing for near anytime access to share information. But over recent years, researchers found rapid growth of mobile malware and increased sophistication of cyber criminals. The smart mobile devices has proven to be an irresistible target for attackers as the trend suggests that more attackers are shifting part of their efforts to mobile.[1]

2. Analysis of Threat

Juniper Networks company's research report "Securing your mobile device" shows the current security trend and the evolving threat vectors: Viruses, Worms, Trojans, DOS, Malware, Botnets and APT, shown in Figure 1. [2]

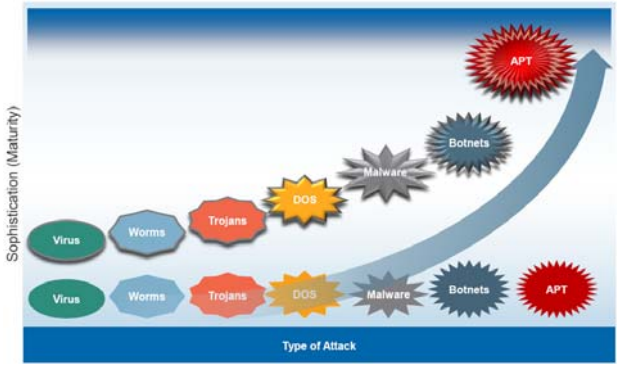

Figure 1 Security Threat Trends

Generally speaking, the threats of Smart mobile devices face are mainly as follows:

- Sensitive data leak (Password, Contact information of your phone)
- Phishing attack (Fake authentication from website, Public WiFi)
- Vulnerability (Bluetooth, jailbreak or browser vulnerability)
- Malware attack (Malicious Apps form app store or third-party)

Here we mainly take the vulnerability and malware attack for analysis.

978-1-4673-5225-3/14/$31.00 ©2014 IEEE

1. Vulnerability

Vulnerability is also called security flaw, which means failure of security policies, procedures, and controls that allow a subject (attacker) to commit an action that violates the security policy including hardware, software, protocols and etc.

Typically, Vulnerability is a great risk to the system, for the hackers can exploit the vulnerabilities to attack the target system and access or root the system. For experiment, we simulate the vulnerability of Andriod Webkit browser (CVE-2010-1807) and use the browser in the emulator to surf the exploit web page in the local web server. The emulator is ideal for studying the network behavior because it provides a controlled environment for managing phone calls, SMS messages and monitoring network traffic. Figure 2 shows the result, in which attackers can view the information of system.

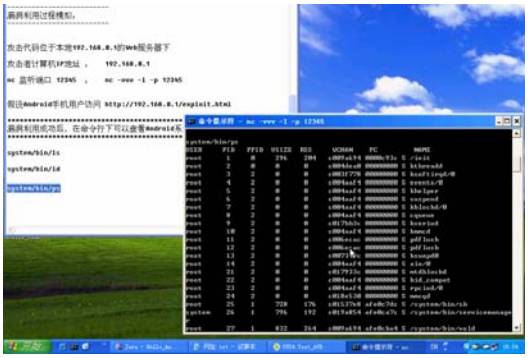

Figure 2 Vulnerability of Andriod Webkit Browser (CVE-2010-1807)

2. Malware

Overall, Mobile malware continues to grow at an exponential pace and remains the most popular hacking technique for devices. Mobile malware has the ability to obtain highly complex control over the devices and the data it transmits and receives.

- Rootkit

Rootkit is malicious program that can secretly modify the operating system code and data, which has been a big problem also faced by desktop computers for a long time. The increasing complexity of smart mobile device operating system, which contains tens of millions of code, makes them as vulnerable to rootkits as desktop operating systems are.

For smart mobile device, its unique interfaces, such as Voice, Short message, GPS, Bluetooth and Batteries, has become a new direction to be attacked.

The GSM rootkit intercepts an alarm signal, e.g., a meeting notification, and stealthily dials the attacker, therefore allowing him to snoop on confidential session, the process is shown in Figure 3. [3]

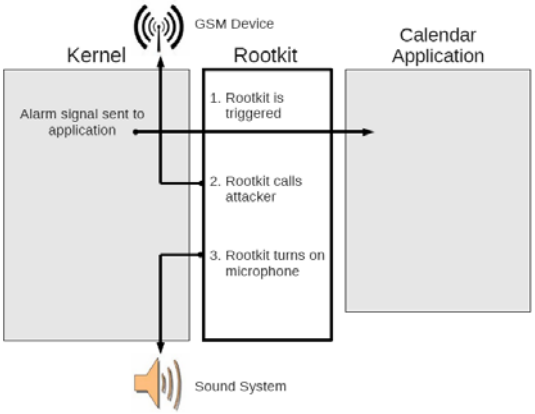

Figure 3 Rootkit intercepts an alarm signal

- Botnet

Botnet may be one of the most famous representatives of malware. These malware has been a big threat to the privacy and property safety of users. Zeus-based Botnet is perhaps the most commonly encountered and easily accessible

botnet DIY construction kit. It is used for a broad range of crimes – ranging from bank credential theft to industrial system backdoor.

Bot detection is still a challenging task since bot developers are continuously adopting advanced techniques to make bots stealthier.

Similar to the botnet in computer area, attacker can send spam, flooding, steal information through mobile botnet.

Security research shows a clear trend that is the malware evolving from computer platform to mobile platform, such as mobile smart devices. For example, ZitMo, is an Android version of the Zeus in the Mobile Trojan, which works in conjunction with the Zeus banking Trojan to steal login information or money from your bank account, packaged to look like Trusteer Rapport, a legitimate security application for online verification of transactions for customers of banks and financial institutions. The packaging as a security application is the key to the success of the phishing attack that gets users to install the malware on their phone. [4]

To accomplish this goal, it uses a number of hacking techniques including phishing, pretending to be a security application, intercepting SMS messages and sending authentication credentials to a remote server.

Once the ZitMo application is successfully installed on the mobile device by user it starts the service called "com.systemsecurity6.gms". This service starts monitoring all SMS. And the intercepted messages are sent to the Command & Control (C&C) servers the attacker can control the victim's smart mobile device.

3. Summary

According to the mobile security study, a lot of malicious software comes from the Official or Third-party App Stores. Users often download and install apps from them and tend to believe in the legitimacy of the App Stores by default, which gives the attackers the opportunity to hack the system.

With the development of mobile Internet and complex applications, the analysis above shows that the smart mobile devices are the same as the desktop operating system, in which there are a variety of security flaws, vulnerable to malicious attack.

Nowadays, smart mobile devices have been an essential tool for information exchange in people's social life. In the face of all kinds of threats, studying the threats they facing will gradually attract people's attention and be helpful to protect your personal information and maintain the development of mobile Internet.

4. References

1. Juniper Networks Third Annual Mobile Threats Report, 2013, pp3.

2. Leslie K. Lambert. "Securing your mobile device", 2011, pp7.

3.Jeffrey Bickford, Ryan O'Hare, Arati Baliga, Vinod Ganapathy, Liviu Iftode. "Rootkits on Smart Phones: Attacks, Implications and Opportunities",2010, pp3-5.

4. Dhawal Desai, "Malware Analysis Report: AndroidOS/Zitmo", 2011, pp7.