An Extensive Survey on Mobile Security and Issues

[1]R.Surendiran, [2]Dr.K.Alagarsamy,
[1]Research Scholar, [2]Associate Professor,
Dept of MCA, Computer Center, Madurai Kamaraj University, Madurai.

***Abstract*:**

As wireless communication has been rapidly developed, mobile applications, services are growing much and more popular, like instant messaging, downloading of a variety of contents, mobile commerce, mobile banking, Internet access, etc. Technology advancement has simplified business, enriched the entertainment and made personal transactions more convenient for mobile device customers.

Mobile devices such as cellular phone, PDA and smart phone are opened the door to a lot of security threats like malicious code, vulnerabilities of mobile phone, attacks on communication, data robbery and damage, intruders, hackers, virus, spam, eves drooping, tracing, Jung mails, etc. information security will become a critical issue to mobile devices and be of great concern to mobile devices users, just like what computer users do today. This paper wills analysis the various mobile threats and security issues.

Keywords: S*mart phone, malicious code, intruders, hackers, virus, spam.*

I. INTRODUCTION:

This introduction part provides an extensive overview of mobile malware, threats and some assumption on future threats. Moreover, it explains the differences among security solutions towards smartphones and personnel computers.

A. Mobile Malware:

Malware: Malware is a kind of malicious code that contains worms, viruses and Trojan horses. Destructive malware will make use of familiarcommunication tools to spread, including worms sent through email and instant messages, Trojan horses get install from the web pages and virus infected files downloaded from internet connections. Malware will also search to exploit existing loopholes on systems to make their entry quiet and easy.

- virus
- worm
- Trojan
- rootkits
- botnet

A *virus* is a small code that can fold itself. Different reproduce of a virus can affect other boot sector,programs or files by inserting or attaching itself to them.

A *worm* is a program that makes copies of itself, typically from one device to another one, using different transport mechanisms through an existing network without any user interrupt. Usually, a worm does not attach to existing programs of theinfected host but it may damage and compromise the security of the device or consume network bandwidth.

Trojans are malicious programs that perform actions that have not been authorized by the user. These actions can include:

- Deleting data
- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of computers or computer networks

Unlike computer viruses and worms, Trojans are not able to self-replicate.

A rootkit is a program that, once installed, tries to hide itself from detection. It does not grant administrative-user privileges. Rootkits can operate stealthily since they directly apply changes to the OS .It has to be installed by someone with the rights to modify the file system.

Finally, a *botnet* is a concept of advanced malicious software that incorporates usually one or more aspects. Botnets represent a serious security threat on the Internet and most of them are developed for well-trained professional for gain of money.

II. REVIEW OF LITERATURE

Various Research papers discuss the evolution of mobile malware:for instance, [15] describes the evolution of malware onsmartphones from 2004 to 2006. For an overview and introduction of mobiles viruses and worms up to 2006 refer [3].The first virus for mobile phones, developed for Palm devices [2], was discovered

in 2000 by F-Secure [8]. In the period 2004-2010, 517 families of mobile viruses, worms and Trojans have been categorized [4]. For a complete list of mobile malware in the period 2000-2008 refer [1]; refer [10] for mobile malware that spread from January 2009 to June 2011. In the period 2004-2008, many types of mobile malware has increased significantly: as of March 2008, F-Secure has categorized 401 distinct types of mobile malware worldwide, whereas McAfee has counted 457 kinds of mobile malware [5]. In June 2004, the first worm that could spread through mobile phones with Symbian OS appeared: this worm, calledCabir [7], was only a prototype developed by the 29AEastern European hacker group. Cabir is considered the first example of malicious code that can spread itself exploiting the networking technologies on mobile devices to infect other devices.

Recently, a growing number of viruses, worms, and Trojans that target smartphones have been discovered. As we have already pointed out, the reason of the growing number of mobile virus is due to the maximum use of smartphones. Even more, we have to consider that most of the smartphones lack any kind of security mechanisms and are not well designed against new threats. Within the 2006-2008 periods, security issues exploiting several attack vectors have increased [19], and there has been a dramatic escalation of complex attackstargeting lower-level device functionality: early securitythreats have turned into sophisticated, profit-oriented, attacks driven by experienced criminals.

III. ANDROID

Android is a new mobile platform which is purely open source. Android applications can use trendy level of hardware and software, as well as local and server data. Android should have security mechanism to ensure security of user contacts, data, information, application and network[14]. Open source platform needs strong and high security architecture to secure all information. It was designed with multilayered security that provides flexibleness needed for an open source, whereas providing protection for all users of the platform designed to a software stack, android includes an operating system, middleware and core application as aComplete [16].

Android architecture is designed for ease of development for developers. Security modules have designed to minimize the load for developers. Developers have to simply work on additional security enhancement aspect level controls. Developers are not aware with securities that apply by defaults on application. It is also designed with focused on user's perspective. Developers can view how applications work and manage the built-in applications.

Researchers are working to create a novel security application to prevent these threats and issues. Android is the one of the popular mobile OS in smartphone sectors.

A. Android Platform Security Architecture:

Android expecting the most secure and usable operating system for mobiles by modifying classical operating system security controls to protect user data, system resources and provide application isolation. Android provides following security features to achieve these objectives are first robust security at the operating system level through the Linux kernel, second compulsory application sandbox for all applications, third secure interposes communication (IPC), fourth application signing and sixth application defined permission and user have to grant permissions.

B. Security in Android:

1) ***Design Review:***
Each major feature of the platform is reviewed by engineering and security resources, with appropriate security controls integrated into the architecture of the system.

2) ***Penetration Testing and Code Review:***
During the development of the platform, Android-created and open-source components are subject to vigorous security reviews.

3) ***Open Source and Community Review:***
The Android Open Source Project enables broad security review by any interested party. Android also uses open source technologies that have undergone significant external security review, such as the Linux kernel.

- ***Incident Response:***
Even with all of these precautions, security issues may occur after shipping, which is why the Android project has created a comprehensive security response process.

C. Security Issues faced by Android:

Mobile hand-held devices which are popularly called smart phones, tablets. For many it's essential to everyday social activities. These emerging developed technologies make easier and cheaper the access, the processing, the storing and the transmitting of information. In this ever changing and evolving environment, establishing secure communication is an

important target for researchers as well as users and clients.

Cryptography and steganography are two techniques used to ensure information confidentiality, integrity and authenticity. Cryptography uses encryption to scramble the secret information in such a way that only the sender and the recipient are able to understand or decrypt it. Steganography hides the secret information in different medium like image, audio, video, etc. other supports like communications protocols. Due to that it becomes difficult to detect.

Both techniques have their certain limitations and this is why most of the researchers sustain that a good solution for securing the digital information is to combine the two techniques [21].

D. Security Threats &Example Attacks:

There are numerous threats available in mobile phone. Here we will listout some of these

- Victimmay receive some spam messages on mobile devices
- User may receive virus from SMS, Bluetooth.
- Victim mobile devices may be eaves dropped by unauthorized persons.
- Victimmobile devices get lost.
- Victimcan get the virus while accessing network through mobile device
-

E. DroidKungFu:

A trojan content in Android applications, which when executed, obtains root privileges and installs the file com. google. search. apk, which contains a back door that allows files to be removed, open home pages to be supplied, and 'open web and download and install' application packages. This virus collects and sends to a remote server all available data on the terminal.

1) Description:

Android/DroidKungFu.A is a trojan that sends sensitive information to an attacker and includes backdoor functionality. It also exploits vulnerabilities to gain root access.

2) Indication of Infection:

Sends sensitive information Exploits known vulnerabilities to gain rootInstalls an Android application into system director has backdoor functions.

3) Methods of Infection:

This malware requires that the user intentionally install it upon the device. As always, users should never install unknown or un-trusted software. This is especially true for illegal software, such as cracked applications - they are a favorite vector for malware infection.

4) Virus Characteristics:

Android/DroidKungFu.A is a cracked version of a legitimate application. It includes functionality to execute backdoor commands and exploits vulnerabilities in order to gain root access. Installation of the trojan is shown in

Fig 1 - The permissions requested by Android/DroidKungFu.A.

When the infected device starts up, the malicious service "SearchService" will be activated.

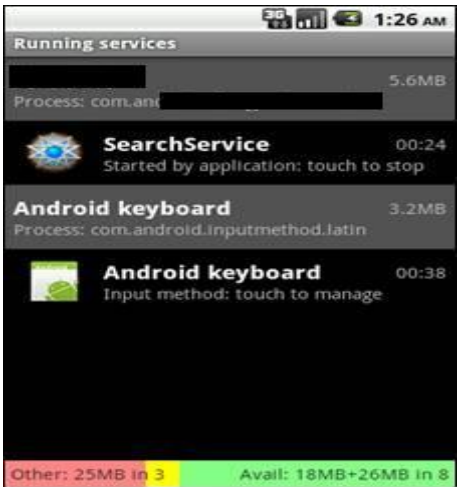

Fig 2 - Running service "SearchService"

Android/DroidKungFu.A repeatedly launches two Android native executables "assets/ratc" and "assets/gjsvro". The exploits are stored in the APK file and are detected as Exploit/DiutesEx.B and Exploit/LVedu.B respectively.
If an exploit is successful, Android/DroidKungFu.A remounts /system in order to copy a malicious APK into the "/system/app" directory. Otherwise, it shows dialog to explain that the exploit has failed.

Fig 3 - Dialog explaining that the exploit has failed.

Android/DroidKungFu.A performs the following backdoor functions in response to commands from an external server:

- Delete file
- Install APK
- Uninstall APK
- Launch Web browser with URL
- Launch application

It also posts the IMEI and whether the trojan gained root access to the external server. The malicious APK installed by the trojan will run as a service at device start up, even if Android/DroidKungFu.A is removed.

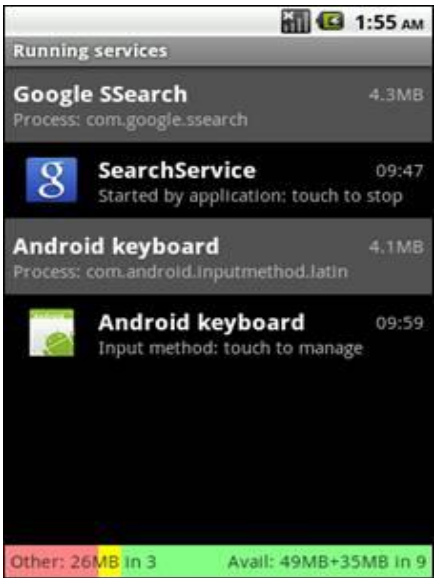

Fig 4 - Maliicous APK running in the /system/app directory

F. Ginger Master:

A trojan developedfor an Android platform that propagates by installing applications that incorporate a hidden malwarefor installation in the background. It exploits the frailty in the version Gingerbread (2.3) of the operating system to use super-user permissions by privileged escalation. Then it creates a service that steals information from infected terminals user ID, number SIM, phone number, IMEI, IMSI, screen resolution and local time by sending it to a remote server through petitions HTTP.

Installation:
Trojan: Android OS/Ginger Master. A may be downloaded from the Internet from third-party Androidmarkets.
Upon installation, it displays the following information on the device, outlining its capabilities:

Payload Steals information:

Trojan Spy: Android OS/Ginger Master. A is capable of doing the following:

- Gaining the Internet Access
- Accessing your device's SD card which including modifying and deleting the card contents.
- Modifying your device's settings and system files
- Gaining highest privilege on your device's operating system
- Downloading other potentially arbitrary, possibly malicious files onto the device

Trojan: Android OS/Ginger Master. A contains an exploit code masquerading as an image file named '*gbfm.png*', and might allow a remote attacker to gain administrator privilege to the underlying operating system of the mobile device.

The malware can steal the following information stored on the device, and save it to a file named '*game_service_package.db*', before sending the information to the remote address '*client.mustmobile.com*' via HTTPPOST:

Device ID (IMEI)
Subscriber ID (IMSI)
Model
Manufacturer
SIM Serial number
Line number
CPU
Network Type
UserId

It is also capable of downloading and installing other potentially malicious files onto the compromised device; in the wild, we have observed it downloading a file named '*19225910801.apk*' from the above mentioned remote server.

System changes:
The following system changes may indicate the presence of this malware:

The presence of the following files:

'*gbfm.png*'
'*game_service_package.db*'
'*19225910801.apk*'

G. Trojan. FakeInst.

This Malware tricks [9] uses into believing that they're installing a perfectly legitimate app, while in fact it sends SMS messages to premium rate numbers. The Trojan is particularly deceitful and tricky to pin down in case of infestation. The main infection vector was through highly popular games such as Asphalt6, Bekeweled, Doodle Jump and others. This Malware can display advertisements and collect personal information at the same time.

H. IRC Bot

Once installed, the malware [9]disguises itself as Madden NFL 12 – a seemingly trustworthy app. Unlike this guise may suggest, though, the application actually consists of three malicious components: a root exploit, an SMS Trojan, and the IRC bot. The files are extracted and stored in /data/data/com.android.bot/files as "header01.png," "footer01.png," and "border01.png" respectively.

I. MarketPay.A

Money stealing virus [9]it sits in the background and has the capability to purchase app on its own, withoutuserknowledge.A is a virus found in trojanized applications that automatically place orders to buy apps from a Chinese mobile market without user's consent.This virusrequires that the user intentionally install it upon the device. As always, users should never install applications from unknown or un-trusted android markets.

J. Android/Funsbot.A

It can turn your [9] device into a Zombie machine. Like any botnet client, it talks to the command

and control server to take instruction, through which files can be downloaded or uploaded to and from the device.

K. Android/ Plankton.A

Discovered in June2011 and able to collect [9] information about application installed in the device,its security settingsetc. and send this to a server over HTTP. This server returns the URL of a JAR file, which is downloaded and executed.

L. Android/ BackScript.A

Being a Botnet client, it talks to the command[9]and control server to get updated commands and functionality. At the core of it is Java Script to provide the self-updating facility.

IV. SIMPLE WAYS TO AVOID MOBILE THREATS FOR NON-TECHNICAL USERS:

1) Don't navigate and whatever you do download, materials from malicious Web sites

2) Look carefully at any program before you install it to make sure it's legitimate and it only asks for necessary permissions

3) Don't download programs from third-party Android stores.

4) Ensure thatbefore install an application whether trusted or not and then make sure that, it will askonly proper query.

5) Upgrade your software to the latest version of Android.

6) Use Antivirus software.

Use Anti-virus software from the reputed and popular vendor to protect our valuable data's.

V. CONCLUSION:

There are numerous threats available in the mobile computing era but in our research focusing on mobile devices and related issues. In our survey we have discussed various threats, vulnerability, and various attacks. Whatever we have discussed in our survey are based on our vision and statistical facts. We had found out some of the major issues and problems persist in the mobile device and tablets during our survey. To rectify those issues we are going to produce some effective methodologies in our forthcoming works.

VI. FUTURE WORK:

We believe that our statistical report will be useful for the public and researchers. Researchers can make use of these things and they can develop some application or methods to deny those threats and vulnerabilities.

VII. REFERENCE

[1] A-D Schmidt and S.Albayrak, "Malicious Software for Smartphone," TechnischeUniversitat Berlin - DAI - Labor, Tech. Rep. TUB-DAI 02/08-01,February 2008, http://www.dai-labour.de.

[2] N.Leavitt, "Mobile Phone: The Next Frontier for Hackers?" Computer, vol. 38, pp. 20-23, April 2005.

[3] M. Hypponen, "Malware Goes Mobile," Scientific American, vol. 295,no. 5, pp. 46–53, 2006.

[4] M. Hypponen, "Mobile Security Review September 2010," F-SecureLabs, HelsinkiFinland, Tech. Rep., September 2010.

[5] G. Lawton, "Is It Finally Time to Worry about Mobile Malware?"Computer, vol. 41, pp. 12–14, May 2008.

[6] S.Toyssy and M.Helenius, "About malicious software in smartphones," journal in computer Virology, vol. 2, no 2, pp. 109-119.2006.

[7] "Bluetooth-Worm:SymbOS/Cabir," Jun 2004. [Online].Available: http://www.f-secure.com/v-descs/ cabir.shtml

[8] F-Secure, "Liberty (Palm)," Aug 2000. [Online]. Available: http://www.f-secure.com/v-descs/lib palm.shtml.

[9] http://hackyogi.com/top-10-malware-of-android-operating-system/

[10] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner,"Survey of Mobile Malware in the Wild," 2011. [Online]. Available: http://www.eecs.berkeley.edu/~afelt/malware.html.

[11] TiwariMohini, SrivastavaAshish Kumar and Gupta Nitesh Review on Android and Smartphone Security. Research Journal of Computer and Information Technology Sciences.

[12] http://home.mcafee.com/

[13] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra, A Survey on Security for Mobile Devices, Ieee Communications Surveys & Tutorials, Vol. 15, No. 1, First Quarter 2013.

[14] Android Open Source Project. Android Security Overview.http://source.android.com/devices/tech/security/index.html. (2013) .

[15] A. Gostev, "Mobile malware evolution: An overview," KasperskyLabs Report on Mobile Viruses, 2006.

[16] Kaur S. and Kaur M., Review Paper on Implementing Security on Android Application, Journal of Environmental Sciences, Computer Science and Engineering & Technology, 2(3), (2013)

[17] J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy, and L.Iftode,"Rootkits on smart phones: attacks, implications and opportunities, "in Proceedings of the Eleventh Workshop on Mobile ComputingSystems & Applications, ser. HotMobile '10. New York, NY,USA: ACM, 2010, pp. 49–54.

[18] C. Papathanasiou and N. J. Percoco, "This is not the droid you're looking for..." in DEFCON 18, July 2010.

[19] McAfee Labs, "Mobile Security Report 2009," 2009.[Online]. Available: http://www.mcafee. com/us/resources/reports/rp-mobile-security-2009.pdf

[20] Kasperksy Lab, "Popular Porn Sites Distribute a New TrojanTargeting Android Smartphones," 2010. [Online].Available:http://www.kaspersky.com/news?id=207576175

[21] D. Damopoulos, G. Kambourakis, and S. Gritzalis, "iSAM: AniPhone Stealth Airborne Malware," in Future Challenges in Securityand Privacy for Academia and Industry, ser. IFIP Advances in Information and Communication Technology, J.Camenisch, S.FischerHubner, Y.Murayama, A.Portmann, and C. Rieder, Eds. Springer Boston, 2011 vol. 354, ch. 2, pp. 17-28.