International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-4 Issue-13 December-2013

Exploring Security Mechanisms to Android Device

Chetan C.Kotkar[1], Pravin Game[2]

Abstract

Android Smartphone devices have gained much popularity in recent years. People are moving from PC/laptop to Smartphone devices. Now a days Smartphone/ tablets are important part of our daily lives since they provide us significant amount of services. Now a days the use of Smartphone services increased significantly because of the connectivity provided by Smartphone like WiFi,GPRS,Blutooth,3G,4G etc. people are using Smartphone devices like PC's to store personal or confidential data, sending mail , web browsing , social networking , net banking etc. Therefore Smartphone become main attraction of attackers/hackers. In particular android operating system for Smartphone devices. In the following survey paper we survey about security threats to android devices, various types of vulnerabilities and related attacks and security mechanisms or solutions proposed/implemented for android threats.

Keywords

Operating system, Security, GPRS, Smartphone.

1. Introduction

Android is an open source operating system and software infrastructure that is implemented on mobile device/Smartphone /tablets. The next generation will use mobile Smartphone's or tablets instead of pc's and laptop. Smartphone device can provide various Computers like services such as gaming/online gaming, web browsing, email, chatting, downloading files, computation, storing personal data etc. it is an programmable network device. Our daily activities/schedule is becoming highly dependent on Smartphone because of their increased capabilities. Security of Smartphone/tabs becomes very important issue.

Chetan C. Kotkar, Department of Computer Engineering, Pune Institute of Computer Technology, University of Pune ,Dhankawdi, Pune-411046,INDIA.

Pravin Game, Department of Computer Engineering, Pune Institute of Computer Technology, University of Pune ,Dhankawdi,Pune-411046,INDIA.

Like our personal computer there are various security mechanisms to protect Smartphone devices from various attacks. To ensure availability, integrity and confidentiality we have to incorporate strong security mechanisms. Android is an open source operating system that is source code of android is available to all. Therefore it allows modification at kernel level. There are various antivirus software, intrusion detection system, malware detection, firewalls available as an application for android devices. Some security enhanced Linux (SELinux) are implemented to improve android security. According to previous work done tightening access control could lead to unsuccessful attack or prevent a successful attack and even prevent some attack entirely.

Today everyone is using Smartphone for various important functions or purposes such as net banking, payments, keeping personal information like bank passwords, ATM passwords, credit card numbers and various confidential data. Therefore Smartphone has become targets of attackers like pc's and laptops in previous days. Malware break into Smartphone's through Wi-Fi, GPRS, Bluetooth, 3G network access. Attacker finds out the vulnerability and can access to the Smartphone data or can gain full access over the Smartphone. Therefore it is essential to provide or construct the strong comprehensive and useful security infrastructure to provide confidentiality, integrity and availability of services to the user of Smartphone. Since Smartphone contain personal and confidential data, it has become more attractive for attackers.

2. Android Structure[1][2][3]:

Android is Linux based operating system associated with software's. Linux kernel provides core system services to android software structure or stack such as memory management, networking, process management, device drivers, file system and power management. Software system contains android native libraries which are written in C/C++. Dalvik Virtual Machine is the heart of android, is and core libraries provide runtime environment for android. DVM runs .dex files which are compact and efficient. Android applications are fully written in java and are packaged in .apk archive which holds all code of app.

Uppermost layer is the application layer provides web browsing, phone, SMS/MMS, email. User ID is assigned to each application at the time of installation and application run in its own dalvik virtual machine that is in its own Linux process. "yaffs2" is default file system in android, it does not support extended attributes i.e. "xattrs." By default only one dalvik based process called zygote can execute within android OS and all other processes are forked from main zygote process to share resources like memory, CPU, disk space etc. core libraries of android are fully written in C/C++ and application can developed in java.Google's android is open source operating system. It allows modification at kernel level therefore any third party software developer can create system level tools for android which can't be trustworthy. Software developer put their apps at android market directly. There is no certification or review process for the apps. People can rate and comment on apps and accordingly if they face any problem or malicious activities of application then they report this to Google. Then according to people review Google remove it from play store and can remove it from device remotely. Therefore download that application with much more downloads and positive comments. For malware it is easy to enter into android Smartphone through various paths. Therefore android devices are vulnerable to attacks that can compromise the confidentiality, integrity and availability.

3. Analysing Threats to Android:

A. Resource Draining [3][7]:
Android applications are not having either RAM (memory) or storage (disk). Applications are using devices disk space or memory. Any malicious application can use more memory, disk and CPU hogging is also possible.

Solution:

1) Resource management:
This mechanism contains allocation of resource fairly to the applications according to needs of application. It maintains the disk allocation, memory allocation and allocation of other resources to the application. But implementation of such requires kernel level modification. Implementation efforts are high that is configuring kernel to support such system. By doing DOS attack on Smartphone like sending huge amount of SMS/MMS etc. attacker can force device to shut down or drain battery by consuming more CPU usage, deny users to perform regular tasks or deny from using services of the phone. Like this there are various attacks to drain resources. Ex: The battery exhaustion attack, water torture attack (drain battery or consume compacting resources by sending bogus frames)

2) Intrusion Detection System:
Undetected malware can drain the resource by remaining hidden. By using host based IDS we can detect the malwares that are using more disk space or memory.

B. Reading Contents [3]:
Applications in android can read the data or contents of Smartphone by implicitly or explicitly gaining the permission and on wireless communication eavesdropping can be done by attackers remotely.

Solution:

1) Encryption of data:
By encrypting data on Smartphone user can protect the important or sensitive data. The data is secure if anyone stele the device then also he or she cannot read the information because only owner knows the key to decrypt the data.

2) Login:
By setting login password user can protect the private information from exposing. If attacker stele device he can't do anything without password.

3) Firewall:
By implementing firewall we can inspect the network traffic to and from android Smartphone. Configure firewall such that it can examine all packets that is whether android application is sending private contents outside and accordingly it can block such traffic. If firewall operates at kernel level malicious applications can't bypass it. Only drawback of firewall is that it can't block the sending data from phone through SMS/MMS. Malicious apps can send data through SMS/MMS.

4) Access control:
By implementing strong access control mechanisms such as context aware access control (CAAC) we can limit the access to device. Implementation of this solution requires high efforts. We can limit access to the contents while device is connected to cellular network or Wi-Fi.

5) Remotely managing data:
If the device is stolen one can retrieve the data remotely from the device by implementing such solution. For that device must be connected to the network.

C. Attack Through Installed Application [3][7]:
Android application ask for permission to data , phone , message , contacts, network etc. to use it at the time

of installation. These types of attack have high impact on device.

Solution:

1) Selected permission to android application:

By providing user to give certain permissions or to choose such permission by which application can't perform malicious activities. Current scenario is that android apps are asking for the whole permissions it is requesting or none that is user cannot install application on device before he grant all the permission requested by the application. To implement such selective

D. Compromised private network [3][7]:

Hacker use the android device to compromise another network device by running port scanner, email, warms, SMS, worms, mms worms etc.

Solution:

1) Managing network remotely:

A centralized remote management system can be used to solve this problem. We can apply certain security policies when operating within the private network. Remote administrator of private network can control all the activities or forcing security policies.

2) Virtual private network:

By implementing L2TP (layer 2 tunneling protocol), PPTP (point to point tunneling protocol) and IPSec in VPN will gives us the solution to above problem. We can also apply encryption, authentication, and authorization policies for protection of communication.

3) Access control mechanism:

In VPN dynamic remote management mechanism as context aware access control (CAAC) can be used. This mechanism can activate security mechanism permission mechanism we have to do certain modification in application installer of android.

4) Firewall:

By implementing firewall application on android we can analyze the application or malware behavior. We can analyze the outgoing traffic that is weather application already installed on device is sending content or data over network.

5) Certification:

Certification of application is one of the solution to application with malicious behavior. For certification every application is verified and checked before installation. But the cost requires verifying all applications is more.

6) Intrusion Detection system:

By implementing IDS we can detect the malicious activities of application. Various intrusion detecting systems proposed earlier for ex: enhancing security with a self-built intrusion detection system.
such as connection encryption , message authentication etc.

E. Exploring vulnerabilities of kernel [3][6]:

Application on android can exploit the vulnerabilities in Linux kernel.

Solution:

Security enhanced Linux is the solution to the above problem.

We have discussed threats to android Smartphone and possible solutions to threats broadly. The above discussed threats can lead to compromising availability, confidentiality and integrity of android device.

F. summarized List of threats to android device [3][6][7]:

1) By using permission approved by user at the time of installation application can do malicious activities from the device such as infecting other device, scanning, sending spam or sniffing etc. Application can do these activities by exploiting vulnerabilities of core component of android.
2) Hardware malfunctioning can occur.
3) Entering into device by receiving email, spam, MMS/SMS.
4) By remotely exploiting vulnerabilities of core component of android attacker can eavesdrops on communication, delete/alter/modify/corrupt the contents on device.
5) Attacker can disable the functionalities of device by using permissions granted by user or do the same by exploiting vulnerabilities of core components.
6) Attacker can misuse the services that costs the user such as making phone calls , sending SMS/MMS or diverting calls to high rate numbers by using permission granted or by exploiting vulnerabilities of core components exposed on network.
7) Pushing adds while using the internet will interrupt while doing important work.
8) Attacker can full control of device.

4. Methods To Attack On Android Device [3][7]

1) Wireless:

Various types of wireless attacks are there compromising the sensitive data of Smartphone. The most popular attack is eavesdropping on transmission media to get the password like sensitive information. Wireless attack can misuse the MAC address of device.

2) User based:

User should know the fundamental of basic security mechanisms. Attacker can use different tricks to trap users device. User should keep the confidential data in encrypted form. User should identify malicious links and trusted links to click and should know to keep their password secret

3) Worm based:

Smartphones have facilities with various connectivity tools. Worm based attack can be done through Bluetooth , downloading infected files , inserting infected memory card , email , SMS/MMS etc.Well known way to spread the worms is Bluetooth connection. Worms can also attack on networks and compromise the phone to use the network services.

4) Break in:

In this attack the attacker find out the vulnerabilities in kernels core libraries, applications and break in. attacker can gain full control of device. For ex: Doom boot-this Trojan installs corrupted system libraries into C: drive of device.

5) Infrastructure based attack:

In this type of attack the attacker attacks on services like making/receiving calls or SMS. This type of attack can happen in GSM, GPRS,UMTS,EDGE networks.

6) Botnet:

Android Smartphone can be part of botnets. Attacker can use Smartphone device as client/bots to attack other device or networks.

5. Linux Tools

Some Linux tools that can be applied to android to improve security are listed below [5][6].

1) Firewall:

Firewall tool called netfilter is present in Linux kernel. Registered callback function used by this firewall to check every packet that traverses the network stack. Netfilter is not as it is compatible to android but by modifying source code it can be implemented on android. Iptable does not work with android because of its page alignment issues that need static compilation of libc.

2) Antivirus:

The open source antivirus calm antivirus is available in Linux system. It is purposely implemented to scan email and email gateway. It is compatible with android with most of the parameter. Static compilations require implementing. Size of this antivirus is approximately 28 MB. But checking every file and maintaining the virus database consumes more memory and disk space.

3) Intrusion detection system:

The intrusion detection system called Snort is available on Linux system. It is useful for packet logging and traffic analysis on ip networks. It can detect various kinds of worms, port scans and exploitation of vulnerabilities and other suspicious behavior by securing contents, analysis of protocol and some preprocessing. Static compilation is not there for snort due to static libc requirement and requires statically compiled libc parts that are not available on android.

4) Root kit detectors:

The chkrrootkit rootkit detector detects the worms, Trojans etc. by checking log files for suspicious entries, checking hidden files, scans binaries. It works on android with some minor dependencies. It requires static compilation and also require netstat provided by buqsybox and requires standard dictionaries like /etc,/lib etc.

5. Some other tools that work with android[5]:

- **a.** Bash: command language interrupter, offers functionalities for interaction and programming
- **b.** Nmap: (network mapper) utility used to explore the network and network security tasks.
- **c.** Strace: used for sanity checking, bug isolation and to capture race condition.
- **d.** Busybox: it is small and compact version of utilities that are regularly used.
- **e.** OpenSSH: used for encryption of all the traffic goes over a network to avoid the various types of attack. It also provides various authentication methods, secure tunneling etc. It is not directly compatible with android but works with minor dependences. It requires

the static version of OpenSSL libraries.

6. Security Mechanisms And Existing Tools For Android Device[3][4][2][1][6]

1) Spam filter:
Blocks MMS/SMS, calls and emails from unwanted users. No existing tool such as.

2) Selective android permission:
Provide greater security by granting selected permission to application. The tool called secure application INTearaction is available for this. But by using this applications will not work properly.

3) Login:
It provides screen locking by maintaining secret password by user. It prevents unauthorized use of device. It is inbuilt in android device.

4) Data encryption:
Encryption of content of device. It is available on android device now days. It prevents access to sensitive information.

5) Intrusion detection system:
Detect the malware, virus by abnormal behavior of phone. It prevents malware attacks to Smartphone. Andromaly, droidhunter tools are available for android. Also various intrusion detection/prevention systems were proposed by various researchers over the years like host based IDS, Behavior based IDS etc.

6) Antivirus :
This tool scans memory, files, emails, scripts, sms/mms for virus, worms, root kits, malware etc. to prevent attacks or malicious activities. Droidhunter, mocana, Smobile antivirus etc. tools are available for android.

7) Resource management:
This system allows to manage the resources such as memory, CPU, disk space, networks, I/O etc. by allocating them to various applications on the phone fairly. It can prevent DNS attack. No such tool is available as such.

8) Firewall:
It can check the traffic going or coming to phone. It can check each and every packet. It prevents various types of network attack. Smobile, netfilter/Iptable are available tools for android but they work with certain dependencies.

9) Application certification:
It provides signatures that signs applications by certificate authority. It can prevent damage from untrusted applications. The open mobile terminal platform's application security framework tool is available for android.

7. Related Work

1) Behavioral based intrusion detection system: it works on the principle of anomaly detection. It is based on local architecture and historical data that is behavior of the device after attack. It measures the events in the communication and keystrokes. It was first proposed in 2005 and gradually improvements were proposed in 2009-10.[8][9]

2) How mobile host batteries can improve network security: it based on power consumption. Based on local architecture. Implemented in 2006. It uses all data that is communication events, keystrokes, OS events.[10]

3) Measuring Integrity on mobile phone system: It is based on Integrity verification and is based on local architecture. Implemented in 2008. It uses OS events and works on SELinux [11].

4) Andromoly: a behavioral malware detection framework for android device: it based on principle of machine learning. Implemented in 2011 but first proposed in 2008. Both implementations are available local as well as distributed. It uses all data to detect the intrusion [12].

5) Google's android: a comprehensive security assessment: it is based on principle of run time policy enforcement. It is based on local architecture and implemented in 2010. It uses OS events to detect intrusion or attack [13].

8. Proposed Ideas

1) Dynamic or Runtime resource allocation mechanism:
The efficient runtime resource allocation mechanism can be implemented on android device. This will solve the problem of resource draining occurred by malicious application. Allocate the resource as per the need of application by analyzing it. This can be implemented by extending the kernel of android. Implementation efforts are high because implementations require kernel level modification to support such a resource allocation mechanism.

2) Android firewall:

Kernel level firewall can be implemented on android device by modification of source code. A piece of software that provide you filtering capabilities with real time connection monitoring. Providing you greater control over where your data is going and what your apps are doing. It provides the ability to restrict apps from sending out any information at all.

9. Conclusion

In this paper we have discussed threats to android device. And we have explored the possible security mechanism that can be deployed on android device. We have overviewed some of the related work on android security. The available tools to secure the android device and certain limitation of tools available. We have proposed some ideas to improve the security of android device. Android can provide security to users by many implementations but understanding the building blocks of android is necessary. The next generation computing is based on Smartphone devices. Therefore we have to focus on security aspects of android.

References

[1] William Enac, Machigar Ongtang and McDaniel, "Understanding Android security" pennsylvania State university 2009 IEEE.

[2] Asaf Shabtai,Yuval Fledel and Yuval Elovici , "Securing Android-Powered Mobile Devices Using SELinux" Ben-Gurion University, 2010 IEEE.

[3] Asaf Shabtai,Yuval Fledel,Uri Kanonov,Shlomi Dolev, Yuval Elovici and Chanan Glezer, "Google Android: A Comprehencive security Assessment" Ben- Gurion University of the Negav,Israel, 2010 IEEE.

[4] Portokalidis, Georgios, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. "Paranoid Android: versatile protection for smartphones." In Proceedings of the 26th Annual Computer Security Applications Conference, pp. 347-356. ACM, 2010.

[5] Schmidt, Aubrey-Derrick, Hans-Gunther Schmidt, Jan Clausen, Kamer A. Yuksel, Osman Kiraz, Ahmet Camtepe, and Sahin Albayrak. "Enhancing security of linux-based android devices." In in Proceedings of 15th International Linux Kongress. Lehmann. 2008.

[6] Charlie Miller Accuvant Labs, "Mobile Attacks and Defence" , 2011 IEEE.

[7] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra, "A Survey on Security for Mobile Devices" , 2012 IEEE.

[8] T. S. Yap and H. T. Ewe, "A Mobile Phone Malicious Software Detection Model with Behavior Checker," in Web and Communication Technologies and Internet-Related Social Issues – HIS 2005, July 27-29, 2005, Proceedings, ser. Lecture Notes in Computer Science, vol. 3597. Springer, 2005, pp. 57–65.

[9] S. Dai, Y. Liu, T. Wang, T. Wei, and W. Zou, "Behavior-BasedMalware Detection on Mobile Phone," in Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on, Sept 2010, pp. 1–4.

[10] G. A. Jacoby, R. Marchany, and N. J. D. IV, "How Mobile HostBatteries Can Improve Network Security," IEEE Security and Privacy, vol. 4, pp. 40–49, 2006.

[11] D. Muthukumaran, A. Sawani, J. Schiffman, B. M. Jung, andT. Jaeger, "Measuring integrity on mobile phone systems," in SACMAT'08: Proceedings of the 13th ACM symposium on Access control models and technologies. New York, NY, USA: ACM, 2008, pp.155–164.

[12] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly": a behavioral malware detection framework for android devices," Journal of Intelligent Information Systems, pp. 1–30, 2011.

[13] A. Shabtai, Y. Fledel, and Y. Elovici, "Securing Android-Powered Mobile Devices Using SELinux," IEEE Security and Privacy, vol. 8, pp. 36–44, May 2010.

Chetan C. Kotkar born 21 aug,1989 at Hingoli. Graduated BE(computer engineering) from University of Pune in 2011, currently pursuing his masters ME(Computer Engineering) from Pune Institute of Computer Engineering, pune.

Prof. Pravin Game working at Pune Institute of Computer Engineering, Department of Computer Engineering, Pune. Completed ME (Computer Engineering) from University of Pune.