IJETCR Open Access

ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 6; Page No. 96-100

Review on Securing Android Mobile Devices and Improving Integrity Protection against Cellphone Malware

Amruta H. Jagtap[1], Archana C. Lomte[2],

[1]JSPM's Bhivarabai Sawant Institute of Technology and Research, Wagholi Pune 412 207, India

amrutajagtap14@gmail.com

[2] JSPM's Bhivarabai Sawant Institute of Technology and Research, Wagholi Pune 412 207, India

archanalomte@gmail.com

ABSTRACT

In this paper we have reviewed the different integrity protection against different smartphones. Now a days mobile phones, smartphones are essential for daily life but the smartphones based on different operating systems like Symbian, Android contain various infected malwares .The malware is a big issue of user mobile security and the downloaded contain through the internet. The integrity must be provided to smartphone because in advanced the malware after they've been infected they may lose the integrity of our mobile phone. This paper investigates the evaluation of trust based routing in the network. The trusted and untrusted domains are based on smartphone content. This is mandatory provide the efficacy related to security antivirus and other solutions.

Key Words: Smartphones Security, Integrity Protection, Malware Detection.

INTRODUCTION:

The various malware are found due to downloaded application in the smartphones the different viruses, Trojans and spyware also present in the sharing of application via Bluetooth or multimedia message service (MMS).[1] The integrity protection based upon different control mechanism like trusted and untrusted domains .The service provider, user, devices, are the various trusted party whereas the untrusted domain include the downloaded contain via browser, application store in smartphone. Linux based smartphone provides access control mechanisms. The element of these mechanisms is user, User is represented by any integer number or user id and own objects a process or a file, or directory. They are further link to groups. In the Linux Smartphone based file permissions operations each contain of file is divided within an owner user and group IDs and three major contain of read, write, and execute permissions.[2]

Mobile device like smartphone, Linux Based, Cellular Phones have been evolved to be in variety of ways. As it is open source available at anywhere so it is instantly used. It became essential and necessary thing for now a day .The smartphone are user-friendly so security issue arises for manufacturer, provider and user also. The F-secure report [3] Show that different malware are infected to smartphones and also threat and virus loss the data in smartphone. So that Security functionality is major issue. The mechanism for detection of malware in smartphone having curtain issue as follows:

1. Analyse the integrity of threats on different mobile platform based also find the the infected threat, virus, Trojans based on various contribution or related mechanism. It also helps to find out the requirements of mobile phone security.
2. The different functionality provided to smartphone i.e. it contain the integrity based rules to provide the protection of smartphone against untrusted domains

1. REVIEW PROCESS:

A.SMARTPHONE SECURITY TECHNIQUES

The smartphone based security techniques come under the hierarchy of security mechanism which helps to detect the unauthorized use of mobile applications [4],save the contain of data. It provide user authentication and variety of security actions.

a) Server-based Tiered Security

The Security related level, events, action are captured by the authorized user .the action or event are stored in client server based techniques. This mechanism helps to setup the security level in smartphone.

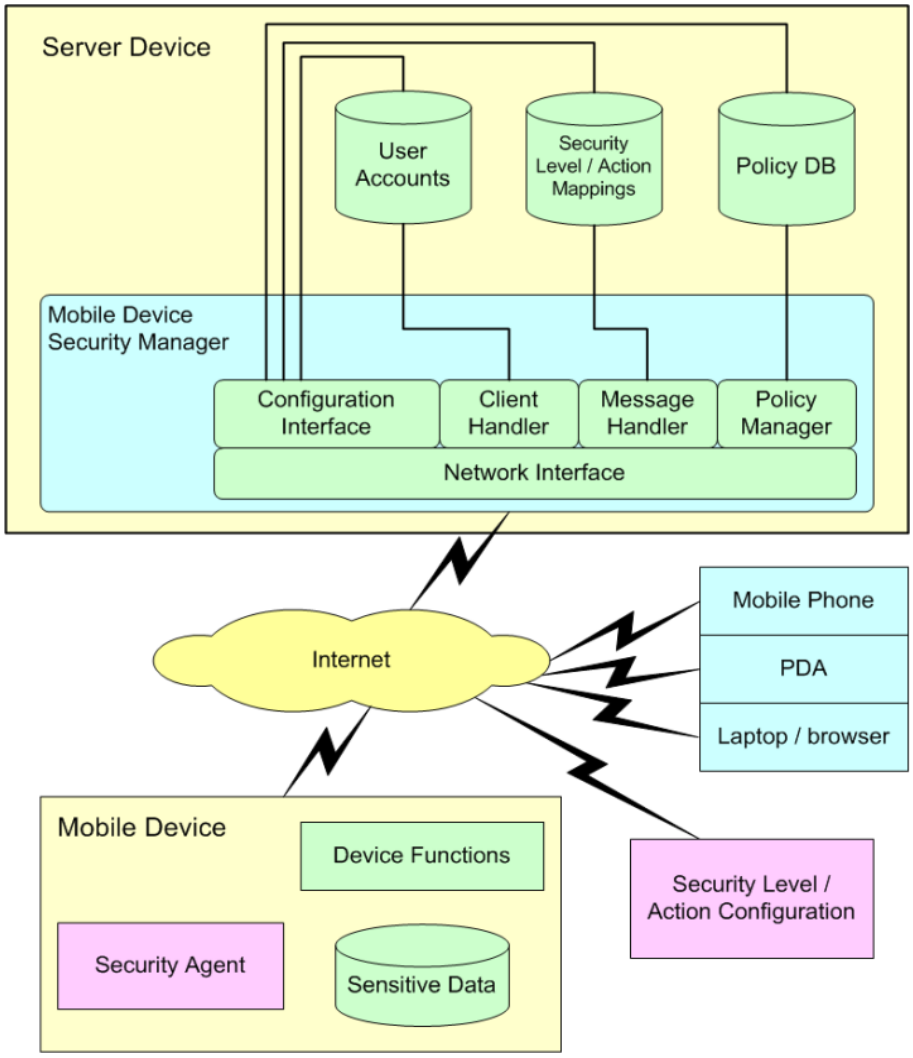

Figure 1: The network-based tiered security system for mobile devices.

- The security based smartphone contain different configuration and mechanism to give the action to handle the security levels present in the smartphones. From the figure 1 it contain the security manager which provide the interface between the network like TCP/IP .The client and server architecture in which the client handles the user specific information to its database
- The security manager handles the security policies like acceptance policy or user policy or any acceptance policy. A message handler is for communicating between the secured mobile device and the Security Manager.
- The security Action based on the smartphone, laptop or any device which user or security manager is provided. For detection of security level in the smartphone user or security manager has to check the setting related to the system .once the setup done the user receive message i.e. it is being secured .

b) Device-based Tiered Security

The device based smartphone designed so that it can configure to remote browser and the user interface .The device based smartphone uses the wireless network area so that it can easily move in the internet area, download the data, share the data .The security issue related to device based smartphone is easily solved, the security manager and its database very effectively handled in the device based area.

© 2013 IJETCR. All Rights Reserved.

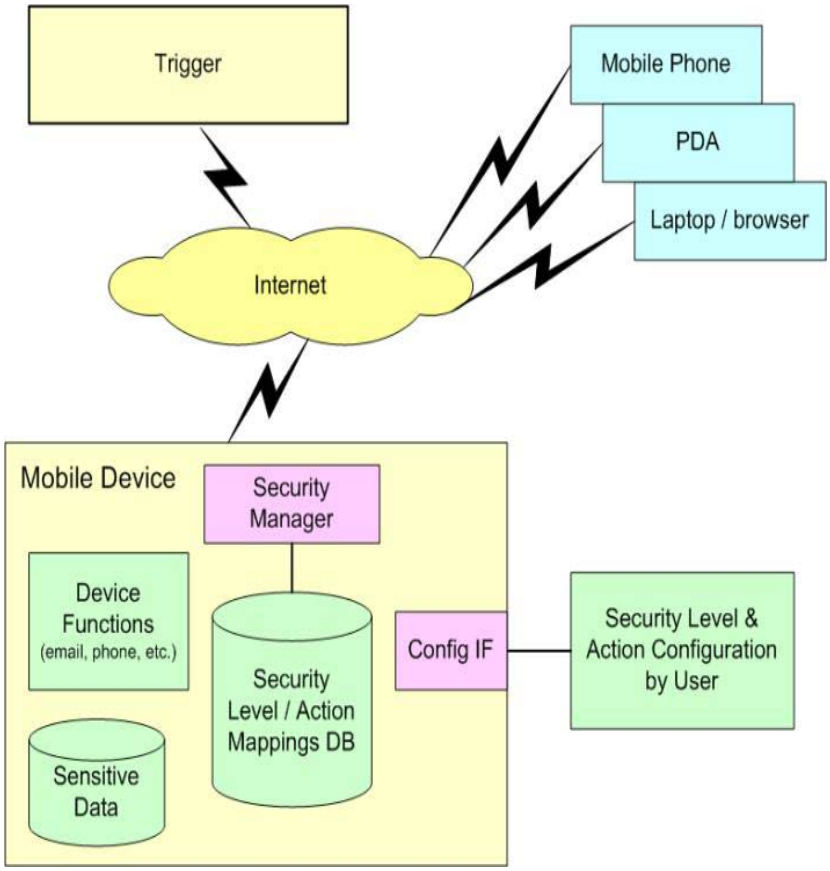

Figure 2 Device-based Tiered Security

- The security manager provides the device based smartphone security in acknowledgement of variety of security. The Security manager helps to ask user the password and security mechanism like digital signature .Based on the received password or keyword to the manager at the current time, then only the security of system or device like smartphone get started otherwise it remain the same.
- The design of security for mobile phone where security holds the user friendly and user define actions,events.The system can be set up and activated from any user defined browser or directly access through the mobile device .
- The trigger information is stored in the database which is defined by the security manager. Mobile device contain different devices like smartphone based application, secure data. The Mobile device is configure due to user define security level. This device security is used in banking, credit card based system.

B.INTEGRITY PROTECTION

The integrity is defined as protection from the untrusted party [5]. This can be said that it is avoided from the modified data. The integrity in other words is nothing but confidentiality of data i.e. it remain secure in the user authentication only. The integrity is defined as protection from the untrusted party. This can be said that it is avoided from the modified data. The integrity in other words is nothing but confidentiality of data i.e. it remain secure in the user authentication only. With the help of antivirus tools data integrity is maintain .the protection is done by using many programs and tools used in integrity usage. They protect the damage caused from virus, Trojans and worms and different malwares.

a) Integrity Rule

The integrity based rules define the flow control based integrity from the high and low attribute or entities. The set of information defined in the attributes it contain types of subjects. These subject mainly consumed with create, read and write operation. The integrity rules are defined under the different subjects or object suppose 'x' and integrity level is defined under L(x).Table 1 shows the integrity rules

© 2013 IJETCR. All Rights Reserved.

Create Object: Rule 1: $create(s, o) \leftarrow L(o) = L(s)$: when object o is created by a process s, o inherits s's integrity level. Rule 2: $create(s_1, s_2, o) \leftarrow L(o) = MIN((L(s_1), L(s_2))$: when o is an object created by process s_1 with input from another process s_2, o inherits the lower bound of integrity levels of s_1 and s_2.
Read/Write: Rule 3: $can\_read(s, o) \leftarrow L(s) \leq L(o)$: a low integrity process s can read from a low or high integrity process or object o. Rule 4: $can\_write(s, o) \leftarrow L(s) \geq L(o)$: a high integrity process s can write to a low or high integrity process or object o. Rule 5: $can\_read(s, o_1) \leftarrow L(s) \geq L(o_1) \wedge can\_write(s, o_2) \wedge L(o_1) \geq L(o_2)$: a high integrity process s can receive information from low integrity subject or object o_1, provided that the information will be written to low integrity subject or object o_2 by the high integrity process s. Rule 6: $change\_level : L'(s) = L(o) \leftarrow read(s, o) \wedge L(s) > L(o)$: when a high integrity process s reads low integrity object o, its integrity level is changed to $L(o)$.

Table 1 Integrity Rule

- Process is created by using Rule 1.When Process is created its integrity level is checked by using Rule 2 with comparing two attributes or subjects. Rule 3 defines the read process of different attribute with lower and upper bound at the same level i.e. reading process is done by using read command .Rule 4 defines for the write operation on different attributes, the low integrity process is applicable for the write process. Rule 5 both read and write operation is done by using this rule which is applicable for the subjects in the process. The last rule i.e Rule 6 defines the change of level i.e. the high integrity process can be change to low integrity process.

- **C.MALWARE DETCTION TECHNIQUES**

The malware found in smartphones have become issue in cellular network it may damage the data [6], leakage the data, infect to the battery and also may cause the malware traffic in the network. The attacker main target is smartphone and different cellular devices and laptops. The malware detection is through the network devices and also the mobile users.

The two main techniques are used in the detection of malware

- Access control–based Protection
- Graphic Turing Test on Smartphones

a) Access control-based Protection

This process defines the access to the key resources [7] only present in the cellular phones and denying the other resources. This technique based on the privileges to the resources if the least privilege key is used then only the aces is provided to resources. The privacy is maintained by using the target resources .These objects are visible to the all subject in the same domain then only the protection is maintained.

b) Graphic Turing Test on Smartphones

GTT technique used to identify virus and malware in mobile device. MMS related malware which is present in smartphone device are detected by using this technique [8]. The malware also found in sharing of data using various Bluetooth and Wi-Fi.

© 2013 IJETCR. All Rights Reserved.

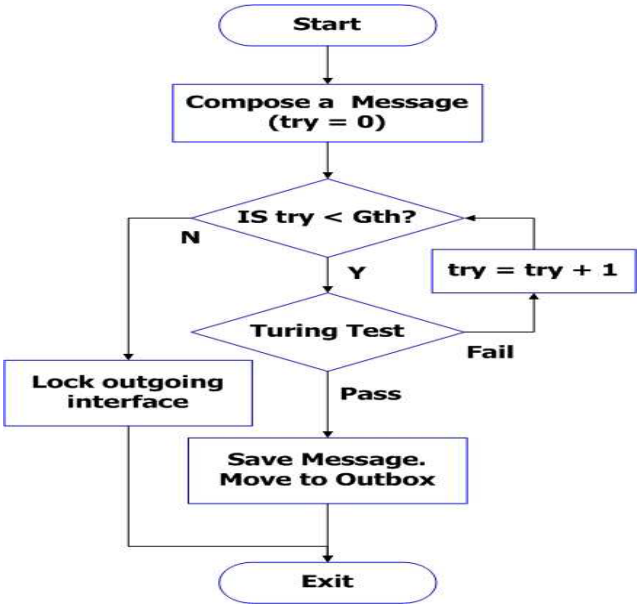

Figure 3 GTT-based protections in a cellphone

This algorithm defines the test between its security and the user convenience. [9] The test demonstrate the composition of message .If the test pass the malwares are broken instantly otherwise the process do the things periodically. The interfaces between the malware and user also identified.

2. IMPORTANCE:

The malware detection technique helps to provide the efficient way to protect smartphones. The cellular phone has gained extensive importance related to integrity. The integrity and security goals of open mobile platform like Android and Linux based smartphones have more and more usage now a day. The different security issue like 'Device based Security' and 'Network based Security' helps user to investigate the different security aspects.

3. CONCLUSION:

In this paper we studied the detection of malware by using different techniques like GTT, Access Control Permission. This technique detects the malware, Trojans, virus from different sharing media like Bluetooth, MMS. The integrity rules defined from the security based smartphone. The smartphone security and providing integrity to mobile phone is big issue it overcome all problem related to the anti-virus program flow.

4. REFERENCES:

1. Xinwen Zhang, Member, IEEE, Jean-Pierre Seifert, Member, IEEE, and Onur Aciic¸mez, Member, IEEE "Design and Implementation of Efficient Integrity Protection for Open Mobile Platforms," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 1, JANUARY 2014
2. McAfee, "Mobile Security Report 2008," http://www.mcafee. com/us/research/mobile_security_report_2008.html, 2008
3. D.D. Clark and D.R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," Proc. IEEE Symp. Security and Privacy, 1987
4. Theodosios Thomas, R. Paul Morris "A Tiered Security System for Mobile Devices", Scenera Research Labs, Cary, NC 27518
5. K.J. Biba, "Integrity Consideration for Secure Computer System, "Technical Report TR-3153, Mitre Corp., 1977.
6. Bose and K. Shin, "Proactive Security for Mobile Messaging Networks," Proc. ACM Workshop Wireless Security, 2006
7. G. Hu and D. Venugopal, "A Malware Signature Extraction and Detection Method Applied to Mobile Networks," Proc. IEEE 26th Int'l Performance, Computing, and Comm. Conf., 2007.
8. Shabtai, Y. Fledel, and Y. Elovici, "Securing Android-Powered Mobile Devices Using SELinux," IEEE Security and Privacy, vol. 8, no. 3, pp. 36-44, May/June 2010.
9. M. Hypponen, "State of Cell Phone Malware in 2007," http://www.usenix.org/events/sec07/tech/hypponen . pdf, 2007

© 2013 IJETCR. All Rights Reserved.