International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(2), pp.448-454
DOI: http://dx.doi.org/10.21172/1.82.060
e-ISSN: 2278-621X

A SURVEY ON VARIOUS MOBILE MALWARE ATTACKS AND SECURITY CHARACTERISTICS

Bala Ganesh[1], Dr. Amlan Chakrabarti[2] and Dr. Divya[3]

Abstract- The increase of the smart devices is quickly expanding and is progressively turning out to be more modern device in the recent smart world. This expanding prominence is making the attackers have a flawless focus on it. The smart devices prepared with the advanced complicated software and hardware systems are paying way for the profit of the malware attackers. The malware authors targets the mobile devices and destruct the information in the devices like privacy theft, information theft, denial of service, distributed denial of service and so on. There should be an effective mechanism implemented to overcome these threats and protect the devices from these severe implications malwares. To provide the cost-effective output solution for the smart devices malware detection, the optimization techniques to be improved for the end users control during run-time.

Keywords – Mobile, Malware, Hardware, Software, Attack.

I. INTRODUCTION

Android Devices have fundamentally changed into an inescapable figuring and stage for limit, with these gadgets; Android gets a handle on an enormous in turn off rate in the share advertise [1]. In 2013 more than 967 million units of cell phones were sold to purchasers around the world, of these PDAs sold to end clients in the last quarter of 2013, essentially 78 percent kept running on the Android position [2] this demonstrate offers of practically 220 million units. The hardware and the software characteristics of the mobile devices are explained. Utilizing the different methods and interfaces used for communication, the malwares utilizes the social building and exploits its range and is discussed in mobile malware and its categories. Mobile devices cannot execute some of the software applications those programs that utilizes large resources as the computer systems do. The malwares infecting these mobile devices will target and destroy the resources through the denial-of service attack. The most difficult and challenging limitation for the defense and detection of data is the resource constraints. Attackers utilizes the trustful channels for the process of authorization using the network services such as messages, calls, payment modes to create loss for the end user of the devices. Various security characteristics related to mobile devices are discussed in this article.

II. CHARACTERISTICS OF SMARTDEVICES The characteristics of the smart devices are classified into two as shown below:

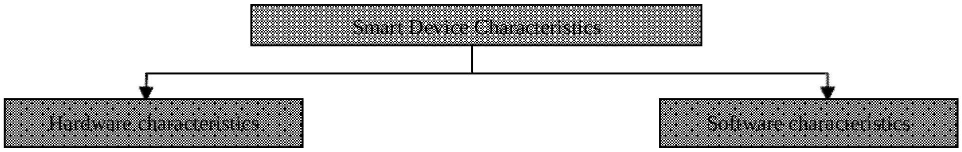

Figure 1. Characteristics of Smart Devices

[1] *Faculty of Computer Science and Multimedia Lincoln University College, Petaling Jaya,Selangor,Malaysia*
[2] *Faculty of Computer Science and Multimedia Lincoln University College, Petaling Jaya, Selangor,Malaysia*
[3] *Faculty of Computer Science and Multimedia Lincoln University College, Petaling Jaya, Selangor,Malaysia*

A. Hardware Characteristics

Based on the [3], the architecture of the smart devices is figured and its general depiction has been shown in the figure below. Different functionalities are combined and found in the integrated circuits as the majority of highlighted segments. To depict the characteristics of the mobile devices, the subcomponent of the heighted segments is presented.

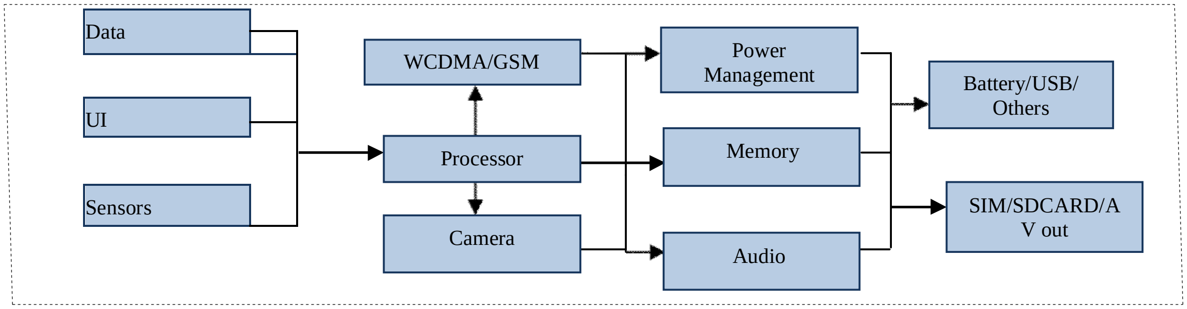

Figure 2. Overview of Smart Device Architecture

For the purpose of wireless connections, mobile devices go with various methods for their communication needs:

- Services like SMS and video calls are basically utilized and used with Second generation mobile devices represented as GSM for their end-to-end connections
- Services like voice and packet data transmission are performed with the combination of GPRS.
- For the faster transmission of data than GSM, FOMA and UMTS was used for the design and structure of W-CDMA.

B. Software characteristics

Along with the mobile device operating system, the additionally relating improvised application developments are explained in this section. The awareness for the threatened stages, phases and devices are brought into and listed below in the figure.

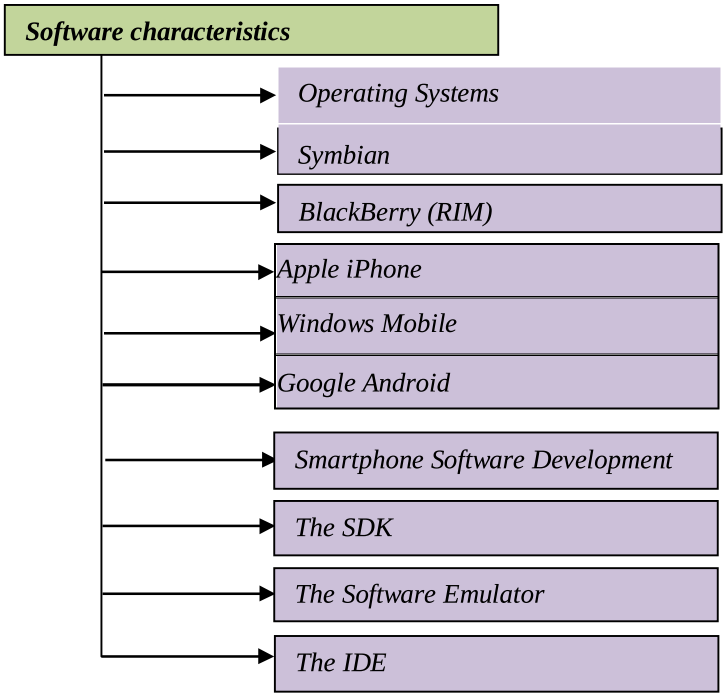

Figure 3. Software Characteristics of Android Devices

Operating Systems - Mobile devices using the proprietary Operating systems has the limitation that few and sometimes extra programming softwares are also not accessible.

Symbian - Symbian Foundation goal is that[4], "To enliven a mutual vision to make the most demonstrated, open and finish versatile programming stage - and to make it accessible for nothing." [4]. Three security strategies that are utilized by the Symbian OS are file signing installation, data-caging and capabilities. Symbian Operating Sytem (.SIS) file is the installation system which is to be signed and this is defined based on the levels limitation by the certificates.

BlackBerry (RIM) - For the BlackBerry systems the operating system was exclusively given by the Research In Motion(RIM). Mainly, the communication through email messages performed by the managers of business and various different people are highly attracted by these BlackBerry devices to send and receive the email messages. The customer expectations regarding the security components are consequently done based on Java-level permission. For the faster writing of email, the QWERTY- based keyboard mechanism is utilized by most of the BlackBerry mobile devices. The transmission of instant emailing through the smart device permitted by the BlackBerry platform is the best pros email technology. The limitation of the Blackberry device is that the programmer cannot access directly the basic applications installed in the device with the system.

Apple iPhone - Apple is incorporated with many applications in it such as, a music player, digital camera and safari browser and this system is call as iOS an advanced modified version of Mac OSX. Apple iPhone has its limitation to non-critical libraries regardless of this driving part, making it difficult to make applications to device-level, as similar to that of the security applications.

Windows Mobile- Smart phone devices such as PDAs, embedded system, PocketPCs and so on was structured and developed using the Windows Mobile working OS and they depend on Windows CE [5]. Three main security methodologies utilized by Windows Mobile are: Security Policies, Application signing and Security Roles.. The uncertainly and insecurity are the windows mobile devices limitations and it is also stated by Communications-Electronics Security Group (CESG), UK [6] that, "*The current CESG policy/ guidance states that Windows Mobile version 6.1 is not deemed suitable to access, store or process RESTRICTED (IL3) data.*"

Google Android - Basic applications, middleware and Operating system are the software package stack included in the Google Android. Based on the Linux system, the security mechanism for Google Android was developed. For establishing and installing each and every application in the program, the accessability right is provided by the user or group IDs. Own user ID is controlled wherein each established application gets its personal person id with its specific permissions. Android is open platform on the large market and it is more feasible and recognized by most of the malware attackers.

Smartphone Software Development- Integrated Development Environment (IDE) or Software Development Kit(SDK) are the essential tools to be included for the process of developing, building, implementation and testing out mobile device software.

The SDK - For the development and deployment of software program development with certain platform, OS, framework, hardware or the programming language, SDK contains a set of software. Software emulators are also found with most of the SDKs.

The Software Emulator - Software Emulator like Symbian Operating System devices provides the programmer the capacity to execute and test the software on the users system even though that was developed for some other platforms or systems. Not all the functionalities of the original device frequently supported by the emulators. Some critical troubles may be led; the programs stability will have a excessive impact if no longer they are supported. Emulation tries to enter through corresponding points to produce a copy of the same existing state which is not like a simulator that produces a copy of program behavior. Through mapping process maximum of the so referred software emulators, SDKs simulates the interface, functionalities and connections such as Bluetooth port of simulator to serial port desktop systems.

The IDE - Similar to that of SDK, the Integrated Development Environment performs the functionality of combining the tools to write, compile, construct and debug the software program. Most of the tools used are combined together as a single tool with Graphical User Interface(GUI) and this difference is done. To often improve the speed of the developed device, the relevant improvisations are implemented through the user interface. Some of the example Mobile devices with IDEs are Metroworks, Nokia Carbide, Eclipse, MS Visual Studio and Codewarrior.

III. MALWARE EVOLUTION

In the year 2004, the malicious softwares for infecting the mobile devices came into existence. 29A is the group that infected the mobile devices through their mentioned virus in June,2004. Cabir [17] is the first infection virus and that is composed for Symbian OS. Mobile devices constrained resources are abused using the Bluetooth, here the Bluetooth is used to spread Cabir virus. The mobile devices are attacked through a wide range of malwares such Trojans, worms, file infectors and backdoor. Messaging services through Short Message Service (SMS), Multimedia Messaging Service (MMS) and Bluetooth are the vulnerabilities used for the malware propagation mainly. Gostev's [7] in 2012 stated that, there will be the financially infecting malware in the Android devices and they will be encouraged to expand its infection. Moreover Thomas et al. [8] predicted the similar Financial infection malware pattern trend.

IV. MOBILE MALWARE

The malware works with two words software and the malicious that shows plainly that the programs in the system containing vindictive expectations of Malware [9]. The en goal of these malicious expectations are represented with terms namely infection payload and infection vector. The infection to be caused to the original data or the content existing in the vulnerable machines is represented as information payload. The methods utilized for conveying the application with malicious contents and methodologies are described as infection vector. Some known methodologies existing are file transport, file injection, boot sector corruption, exploit2, etc.
The potential outcomes for the few known payloads are:

- Denying service
- Logging keystrokes
- Denying services

The communication mediums utilized for the contaminations are MMS, Bluetooth, USB, Internet Wi-Fi and Memory C are they are shown in the figure below.

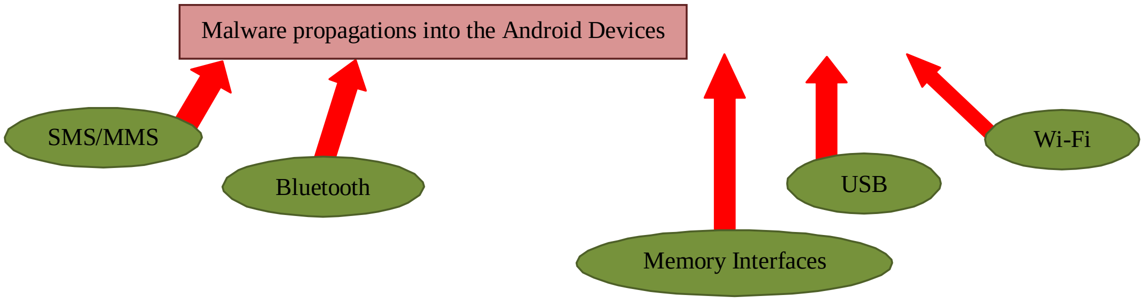

Figure 4. Malware propagation in the Smart Devices

The malicious exercise performed by the Smart device malwares are the credentials sending to the vulnerable devices, data stealing and valuable SMS transformation are some examples.

Categories of Mobile Attacks
Unauthorized access performed by the malware authors on the devices are referred to as the Attack Vector.
Figure below describes the classification of attacks on the mobile devices [10].

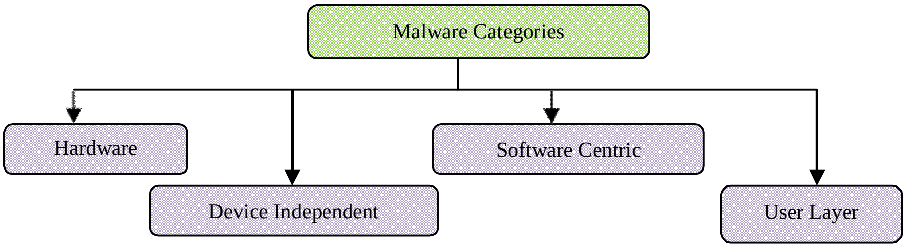

Figure 5. Attack Categories in Smart Devices

Hardware Based-
Interception of corresponding communication in the Mobile Network Operator causes the damage for physical access and they are identified as the hardware attacks. Some of the examples of the hardware centric attacks are man-in-the-middle attack and SIM lock evacuating of the iPhone. Debugging done on the device is additionally a type of attack based on hardware.

A. Device independent attack-

The attack that is made on separately out of the smart devices, for example, on protocols, infrastructure and so on go under this class of attack. The protocol produced 25 years ago is the Global System for Mobile (GSM) protocols has much vulnerability for the attacks such as unauthenticated network, immature croto system and so on. So as that, SMS framework has considerable number of defects like the overload limitation found in the network by paging channel.

C.S oftware centric-

Infecting the software execution on the smart devices are referred as the software based attacks. In 2004, Symbian Operating System was repeatedly affected by the malware named Cabir. These software centric attacks are utilizing the below

- MMS correspondence channels
- Rootkit assaults
- SMS correspondence channels
- Attacks by means of portable web programs

D. User Layer –

Attacks that are related to trick the user and not exploiting any technical vulnerability come under this category. Social engineering is a category to lure customers and perform attacks. Assaults that are identified with trap the client and not misusing any specialized weakness goes under this classification. Social building is a classification to bait clients and perform attacks.

V. SMARTPHONE SECURITY CHARACTERISTICS

Mobile computer hand-helds in the minimized forms are represented as Smartphones. Security term refers to the protection ensured against any misfortune or loss or danger. USA Defense Department characterized security as "*a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences" [11].*

Security goal is expressed by Bishop [13] that network or the computer system should be kept secured as because this should be the specific or primary goal to be attained. The outlines of the process of achieving this are confidentiality, integrity and availability.

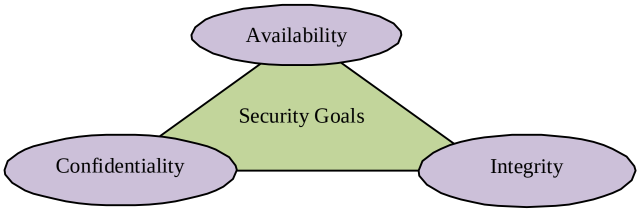

Figure 6. Security Goals

A. *Confidentiality* - United States Code (U.S.C.) indicated that, confidentiality is referred as the process of preserving the data from the unauthorized confinements and also implies to the proprietary information and personal privacy security.

B. *Integrity- According* to U.S.C.[12], the term integrity refers to the process of safeguarding the information from the unauthorized attackers process of destruction or modification and further the guarantee for the authenticity and non-reputation of information.

C. *Availability* - Following the U.S.C. [12], Availability is characterized as guaranteed access and utilization of data within the assured time. The term availability ensures that the information and data used are utilized in timely forms. Once if the data is lost of availability portrays that the utilization of access data or information system is disrupted [14].

The mobile Security characteristics are specified and classified by Becher et al. [10] is shown in the figure and explained below.

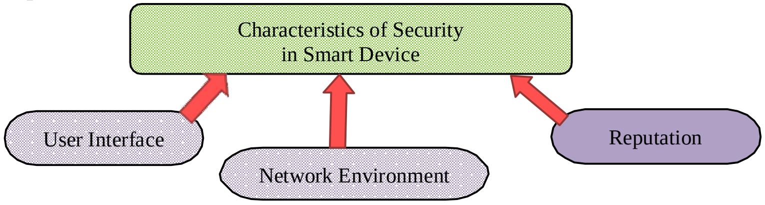

Figure 7. Security Characteristics of Smart devices

User interface: Based on the size, desktop Personal Computer and the mobile devices are not the same. Thus, the security techniques applied such as URL bars, browsers visual indicators, CAPTCHA for the desktop systems cannot be straightforwardly applied for the mobile devices. Therefore for the mobile devices, there is the need for smaller screen redesigning. For the user's security, this is more noteworthy. Phishing attack can be easily applied on the mobile devices through the interfaces limitations compared to that of the desktop programs [16].

Network Environment: Mobile Network Environment (MNE) is found in between the Mobile Network Operator (MNO). In the Android devices Network Environment assumes to play the primary role. Management Network Environment (MNE) controls and manages the basic remote and the update processes. End users on both the end permits the malware attacker to enter the device through this strong impact of MNO. For updating the recent firmware in the mobile devices, they are in need of MNO. If the devices are stolen, MNO has to carry out functionality like remote wiping and management.

Reputation: Reputation of MNO is playing an important role, in the event of mobile devices. The exploration of malicious exercises takes place in the mobile devices through the malwares. Unauthorized sniffing attack on the smart devices sensors are the more vulnerable states in the Mobile devices. To provide protection against the privacy attacks is one of the challenges upon the context of sensors access control, on the account of smart devices. In August 2009, it was found that Denial of Service (DOS) attacks are one of the typical cases that are disturbing the online services [18]. Unintended activities in the devices create the unavailability of data other than the DOS attacks.

VI. CONCLUSION

The paper discussed the mobile device characteristics and the various the mobile device malwares and the security features required for the smartphones to defend from different malwares. The appearance of smart devices with multiplied storage space and calculating capabilities and the invasive exercise of systems for susceptible applications such as online banking, e-commerce and the storage of susceptible data on the smart instruments have lead to growing risk connected with malware distinguishing at these mechanisms. The setting of malicious code attacks has converted extensively from large-scale internet malicious attack incidents to more straight attacks against company resources. As smart devices become a number for delicate knowledge and appliances, increased malware detection mechanisms not standing on signatures are critical complying with the useful resource constraints of current smart instruments. There are various techniques existing to provide the effective detection mechanism. To perform effective detection mechanism in the mobile devices the data mining techniques are to be improved in terms of accuracy. Moreover, the users also have to educate themselves.

REFERENCES

[1]. Babu R.V., Phaninder R., Himanshu P. & Mahesh U.P., Androinspector: A System for Comprehensive Analysis of Android Applications. International Journal of Network Security & its Applications (IJNSA) Vol.7, No.5, September 2015, pp. 1-21. DOI: 10.5121/ijnsa.2015.75011.

[2]. Statista, Global Smartphone Sales 2009-2014, by OS, 2015. Retrieved from http://www.statista.com

[3]. Nokiaport. Aufbaueines mobiltelefons. http://nokiaport.de/content/de/inside/mobile_architecture.png, July 2009.

[4]. Symbian Ltd. Symbian. http://www.symbian.org/, 2010.

[5]. Microsoft Corporation. Windows mobile. http://www.microsoft.com/germany/windowsmobile/default.mspx, 2007.

[6]. Ian Cuddy. Mobile working: Gov connect pulls the plug, June 2009.

[7]. Y. Bulygin. Epidemics of mobile worms. In Proceedings of the 26th IEEE International Performance Computing and Communications Conference, IPCCC 2007, April 11-13, 2007, New Orleans,Louisiana, USA, pages 475- 478. IEEE Computer Society, 2007.

[8]. Jerry C., Starsky H.Y.W., Hao Y., and Songwu L. (2007). SmartSiren: Virus Detection and Alert for Smartphones. In Proceedings of the 5th International Conference on Mobile Systems, Applications and Services (MobiSys' 07), ACM New York, NY, USA, pp. 258- 271. doi:10.1145/1247660.1247690.

[9]. SlideME (2013) SlideME | android apps market: download free & paid android application. http://slideme.org/.

[10]. Gregory D. Abowd, Liviu Iftode, and Helena Mitchel. The smart phone: A first platform for pervasive computing. IEEE Pervasive Computing, vol. 4, No.2, pp: 18-19, April-June 2005.

[11]. Department of Defense. Dod dictonary of military terms. http://www.dtic.mil/doctrine/jel/doddict/data/s/04767.html, 2001.

[12]. Section 3542: Definitions Title 44, U.S. Code. Information security.

[13]. Matthew A. Bishop. The Art and Science of Computer Security. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

[14]. National Institute of Standards and Computer Security Division Technology (NIST), Information Technology Laboratory. Standards for security categorization of federal information and information systems. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB- 199-final.pdf, February 2004.

[15]. Pocket Computing. Bellsouth ibm simon: Pda cellphone. http://cdecas.free.fr/computers/pocket/simon.php.

[16]. Abhishek Chaturvedi, Eep Bhatkar, and R. Sekar. Improving attack detection in host-based ids by learning properties of system call arguments. In Proceedings of the IEEE Symposium on Security and Privacy, 2006.

[17]. Wired.com. Denial-of-service attack knocks twitter onine. http://www.wired.com/epicenter/2009/08/twitter-apparently-down/, August 2009.

[18]. Abhishek Chaturvedi, Eep Bhatkar, and R. Sekar. Improving attack detection in host-based ids by learning properties of system call arguments. In Proceedings of the IEEE Symposium on Security and Privacy, 2006.