The study found that the intelligent mobile phone technology of malicious code

FAN Ya-qin [1,a,] ZHANG Ge [1,b] LIU Miao [2,c], , ZHANG Xin[1,d]

1.College of Communication Engineering,Jilin University Changchun 130012 china

2. Jinzhou Branch Company of China United Network Communications Co., Ltd.121010 china

a.fanyaqin_joy@163.com， b.404360310 @qq.com，

c.18604690683@wo.com.cn d.940614745@qq.com

Keywords: intelligent mobile phone; malicious code; eigenvalue; data stream

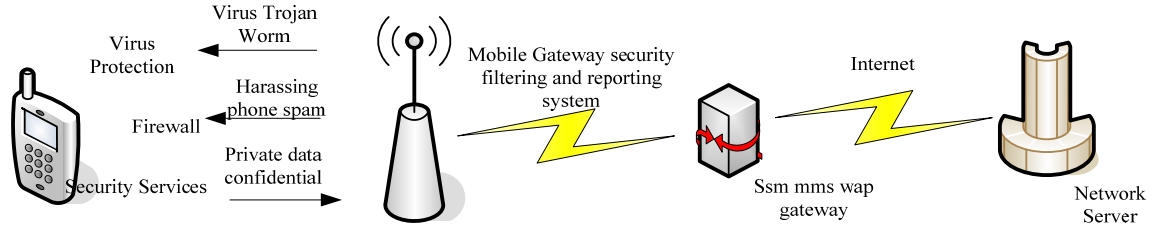
Abstract: This paper studies the development trend of intelligent mobile phone, confirmed the necessity of research on intelligent mobile phone malicious code. Study on the detection technology, proposed intelligent mobile phone regular networks and random networks based on malicious code propagation model, propagation mechanism is studied. Set up a perfect malicious code discovery and defense system model, at different levels is put forward that different, prove the necessity of scanning algorithm and Semantic Detection Algorithm for eigenvalue. To improve the security of the whole communication network.

Overview

Although the harm of intelligent mobile phone malware is not very serious, but relates to personal data and the issues of cost, but with the increasing proportion of data services, intelligent mobile phone platform to the operation of the PC machine platform, if we do not timely malicious code found and defense method, intelligent mobile phone malware will affect the whole communication network security. Therefore, we need to come up with the perfect solution to the problem of intelligent mobile phone malicious code.

Discovery technology

At present, the intelligent mobile phone common malicious code found methods mainly refer to PC malicious code analysis techniques. On the current situation, modern intelligent mobile phone antivirus product basically can achieve efficient real-time scanning monitor, killing the virus, update the virus database, its basic communication equipment related to the increasingly approaching perfection. But previous antivirus means basically is based on signature scanning technology, this technology has many advantages, but for unknown malicious code is incapable of action, and that means more passive defense[1-2]. Therefore, we need to establish a malicious code detection system, the traditional passive defense style and active monitoring defense together, try to find all the malicious code.



The way of finding Smart phone virus

Figure1 the discovery of Communication network and mobile phone ' s viruses

Figure 1 is the propagation path of mobile phone virus and found the technology principle, according to the pie chart shows: prevention we can achieve different malicious code in different

ways [3-4]. Such as the short message of malicious code can use the firewall technology, the Trojan can use antivirus software, in addition, the intelligent mobile phone and Internet are connected, we propose immune solutions on the part of malicious code.

Discovery model

We can put the intelligent mobile phone malicious code detection technology is divided into five levels, as shown in Figure 2, propose corresponding at every level. The proposed model is terminal, gateway, network integration defense.

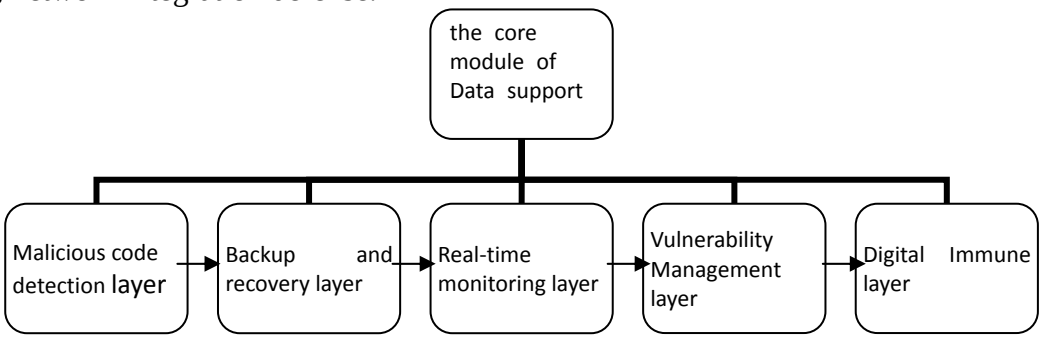


Figure 2 Model of malicious code found in smart phones

Malicious code detection layer

Malicious code detection layer the main detection has invaded the malicious code inside the mobile phone [5]. Emphasis is on the detection of malicious code, clear.

Scan code feature. Scan code feature is the detection of malicious code found most commonly in detection technology, it has been widely used in various anti-virus software provider, is now the main way of application of anti-virus software. It mainly includes two parts : the construction of characteristic database, scanning algorithm [6-7].

The advantages of this detection method can be used as antivirus tools; don't need specialized software, use the edit software can also killing malicious code, provides convenience for not understanding the malicious code; the name can identify virus; low false detection rate. Another comparison method, experimental infection and detection method based on behavior semantic.

Method based on semantics. To test for the virus to take advantage of the unique behavior of the virus. When malicious code with the normal data flow to the mobile phone, the behavioral semantics can extract the monitoring objectives. These semantic extraction. In the array, and the semantic value and weighted to preserve the original, and then compared with the previous situation according to the established threshold, if more than a threshold value, it is judged to be malicious code behavior. Scan code and characteristics of this method have different approaches but equally satisfactory results of the wonderful, but they are different in essence. Signature scanning is malicious code feature library based behavior, and behavior detection is based on the semantic rules of the extracted. Each feature corresponds to a virus, and a semantic rule is corresponding to a kind of virus. So compared with the signature scanning, the behavioral semantics test can detect unknown virus, detection and protection against malicious code plays a profound role. Figure 3 is the behavior semantic technology structure graph. The client agent belonging to the core part, responsible for the comparison of the information received and threshold. If malicious code, database for storing semantic features [8-9]. Console receives client proxy to the information, to upgrade the database.

Backup and recovery layer

The proposed some methods and ideas of some malicious code detection, but for mobile phone users, the most important is how to find the malicious code, but how to restore the function of

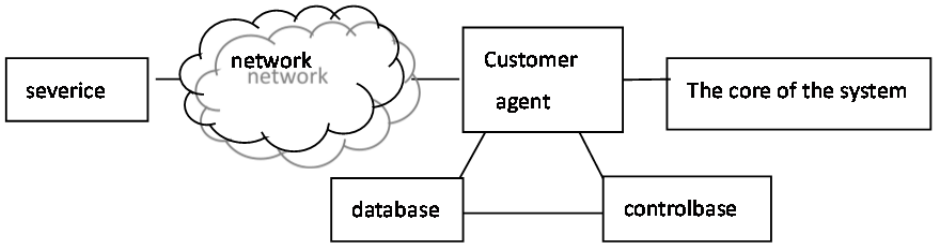


Figure 3 Behavior Detection Architecturesemantic

mobile phone and related documents. Because the application of intelligent mobile phone is poor, so we can according to different devices and operating system, some important program backup in the public platform. The user can download according to need. The SMS, contacts and other related to the data part, only need and PC directory manager business as synchronization can be [10].

Real-time monitoring layer

This layer is a preventive function, is the main entrance, the intelligent mobile phone data. Compared with the detection layer mentioned earlier, real-time monitoring layer belongs to the active defense [11]. In real life, way of malicious code intelligent mobile phone mainly have Internet access, short color information service, Email service, information sharing (USB and Bluetooth), this layer of focus can monitor these ports, in order to reduce the intrusion of malicious code, and the malicious code to intercept, recording its behavior. Provide material for feature database updates. Monitoring of harmful information flow including the inflow and outflow of invasion and illegal behavior. Intrusion detection system is shown in figure 4.

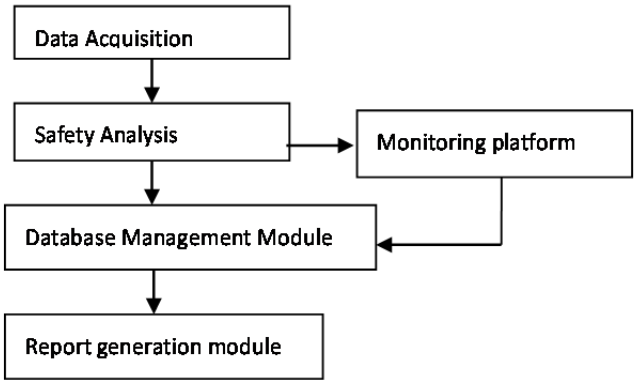


Figure 4 Intrusion Detection System

Vulnerability Management layer

Vulnerability, as the name suggests, is a kind of defect. This defect is like a system error, accompanied by the operating system or install the system to produce, can not be completely eliminated, can only minimize. In addition to software, mobile phone will also have their own vulnerability, vulnerability prevention mainly patch repair by the supplier updates, and operating system in the updated revision. As the PC machine, with the intelligent mobile phone operating system updates, bug form also change rapidly. Therefore, our study on vulnerability to operating system, different release [12].

Digital Immune layer

The main function of Digital Immune layer is to prevent malicious code from the network. Because of all kinds of malicious code from the network, if we all of its eigenvalues, then there will

be a large amount of data needs to be calculated, so we adopt direct immune, nip in the bud. We first collect the digital signature immune information, stored in the immune information database, when users need to download and install the software, immune verification platform according to the database information to verify the download software is embedded in the malicious code. If it is found that the known malicious code, can be directly processed in immune verification platform; if found the unknown malicious code, sending the query to the malicious code into the superior processing mechanism, the combination of heuristic scanning technologies, according to the current database and past experience, produce new defensive measures, then return to update the database.

Summary

This paper established a perfect malicious code discovery and defense system model. This model is of the intelligent mobile phone, communication network, prevent gateway integration. It relates to the mobile phone equipment manufacturers, network operators, antivirus software vendors. For each layer, we present a different approach. In practical applications, we put these methods, combined with active protection and passive protection, combined with the unknown and known detection, basically can be completely protection.

Reference

[1] Melissa Chau, Kiranjeet Kaur, Wong Teck Zhung. Asia\/Pacific (Excluding Japan) Mobile Phone 2011-2015 Forecast and Analysis[R].IDC:IDC, 2011:5-9.

[2] temperature Rashomon, clock. The propagation model of mobile phone virus [J]. Application Research of computers, 2008,28 (11): 2814-2815.

[3] Ding Xuefeng, Ma Liang, Ding Xuesong. The spreading of mobile phone virus complex network theory model study based on [J]. science technology and engineering, 2009,9 (11) .2934-2935.

[4] Hao Xiangdong, Wang Kai-yun. Computer engineering and design of typical malicious code and its detection technology of [J]., 2007,28 (19): 4639-4661.

[5] Qin Jia. Intelligent mobile terminal on [D]. Wuhan: Wuhan University of Technology Computer Institute.2010:27-34.

[6] Tan Qing. A method of active defense executable malicious code and its realization [D]. Beijing: Beijing Jiaotong University, .2007:7-17

[7] Chen Zemao, Shen Changxiang. The malicious code mechanism and model of [J]. computer engineering and design, 2008,

29 (22): 5709-5711.

[8] Wang Xiaojie, Wang Haifeng. Application of malicious code detection algorithm based on semantic [J]. based on computer system, 2009 (8): 103-105.

[9] Jing Rui. Research and implementation of [D]. Chengdu malicious code detection system: University of Electronic Science and technology.2010:12-15.

[10] Gui Jiaping, Zhou Yongkai, Shen Jun et al. Prevention of malicious code intelligent mobile phone [J]. information technology, 2009 (12): 9-12.

[11] fresh permanent chrysanthemum. Intrusion detection [M]. Xi'an. Xi'an Electronic and Science University press, 2009:23-27.

[12] Jungsuk SONG etc.Cooperation of Intelligent Honeypots to Detect Unknown Malicious Codes[R]. WOMBAT Workshop on Information Security Threats Data Collection and Sharing.2008:31-33.

Published by Atlantis Press, Paris, France.