International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 3, Issue 12 [July. 2014] PP: 91-94

Malware vulnerabilities in Mobile OS: Risk and Exploitation

V. Krishna[1], K. Srinivas[2], J S V R S Sastry[3]
[1]*Working as Professor in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU-Hyderabad, T.S, India*
[2,3]*Working as Assistant Professor in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, T.S, India*

Abstract: In this research paper, we are presenting the malware practices in Mobile OS. Discussing the related work to find the risk and attack threats available for Mobile Operating System. A framework has been discussed which help in Malware Detection through rule based, Knowledge based system.

Keywords: Malware, Security, Risk, Operating System.

I. INTRODUCTION

As the scenario has changed, Mobile users have been increased to large extent. There are many mobile operating systems which are available in the market. As the user increases the mobile OS is also increases. Now most of the companies are working to give the best MOS (Mobile Operating System) to attract the users towards their mobile handsets. With the availability of good handsets like Smartphone's which uses online access, keyboard and all the functions of the computer made the communication very fast. Data storage capacity of the handsets also increases. So slowly the mobile is replacing desktop computer, laptops etc.

So as there are security issues in the computer system same way the Mobile is also prone to malware practices. There are malicious code and viruses such as Trozen horse, Logic bombs, worms and social engineering affecting the computer system is also having the possibility of vulnerability for the mobile handsets. The adhoc network created to data transfer is also very much prone to malicious code transfer without the intimation to the user. In this research paper, we tried to find out the malware vulnerability possible with the MOS like symbian, android and iOS.

At present, in response to this increasing threat, security vendors such as F-secure, Kaspersky Lab, McAfee, and Symantec have released mobile anti-virus, firewall, and encryption products. As desktop environments, antimalware solutions are the major mechanism against mobile malware. Such a mechanism relies on an up-to- date malware signature database and scanning engine to detect them. However, several important differences exist between mobile and traditional desktop environments. First, a mobile device typically has only limited processing power, storage capacity and battery power. Although mobile devices' CPU speed and memory capacity have been increasing rapidly at low cost in recent years, they are still much less than their desktop counterpart. In particular, energy-efficiency is the most critical requirement that limits the effectiveness of complex anti-malware solutions in battery-powered mobile devices. Second, mobile malware can spread without the reliance on the network infrastructure, e.g., through Bluetooth interfaces. This may happen when a new malware emerges and the anti- malware researchers have not yet identified its signature. As a result, even when the malware signature is available, the mobile device may not be able to obtain it in a timely manner. If the signature of a malware is outdated, its effectiveness will diminish. Lastly, a mobile device is highly mobile and always has a greater degree of difficulty in quarantining the malware in a local region.

More popularity and capabilities

Smart phones' growing popularity has made mobile devices a more attractive target for hackers. Worldwide, Canalys estimates that the number of smart phones grew from 9 million in 2003 to 115 million in 2007. There are many more phones without all the features of smart phones but
that still have browsers, which makes them vulnerable to malware, noted Jan Volzke, global marketing head at McAfee's Mobile Security Unit.

Bluetooth

Hackers have written some types of mobile worms, such as Cabir, to take advantage of many phones' Bluetooth capabilities. These worms spread to phones in which the Bluetooth function is activated and that are within the technology's transmission range of 10 meters. In these attacks, F-Secure's Runald noted, the potential victims get continuous messages about downloading a file from another Bluetooth enabled device,

even if they click "no" in response each time. Some accept the file just to stop the messages, unaware that they are downloading malware, he said. Volzke noted that Bluetooth-hacking software is one of the Internet's five best-selling types of malware toolkits.

Wi-Fi

Some service providers use malware firewalls to screen content coming over their cellular networks for mobile viruses, Runald said. However, he added, content coming to phones over Wi-Fi systems runs over Wi-Fi networks and thereby avoids providers' checks.

Messaging

Text and media messages can come with links to virus- hosting sites. Once installed, malware could make compromised phones send messages to phone numbers in contact lists, fooling future recipients into believing the information is safe because it was sent by a trusted friend.

Open platforms

Companies such as Google and Verizon Wireless have promised to create open mobile-phone platforms on which customers can use any handset they want and for which anyone can write applications. The systems would be more vulnerable to malware because they would allow applications and devices that have not had the same scrutiny and control by service providers as in the past, noted David Wood, Symbian's executive vice president of research.

II. RELATED WORK

Internet worms and computer viruses have been plaguing computer environment for many years and led to the widespread investigation of malware propagation on the Internet. Traditionally, the detection of malware is handled by anti-malware software. The most commonly-used technique for malware mitigation is signature-based methods. Typically, a signature-based method is picked to illustrate the distinct properties of a specific malicious executable. A unique detection signature is extracted by an expert in the field or using static information and a code value for each malware program so that future examples of it can be correctly classified with a small error rate. Therefore, this type of detected method must rely on a signature database to analyze each malware. In other words, signature-based detection cannot detect an attack from unknown malware or its variant [2], [3]. Protection from unknown malware is the major issue of the day in computer virology. The antimalware community relies heavily on known signatures to detect malicious programs but all efforts still have not solved the key problem until behavior based method appeared. The behavioral detection method is based on an in-depth understanding of malware' nature, characteristics, and dynamic behavior. The runtime behavior of an application is monitored and compared against malicious and normal behavior profiles. Behavioral detection is more resilient to polymorphic worms and code obfuscation, because it assesses the effects of an application based on more than just specific payload signatures. Moreover, behavioral detection has potential for detecting new virus and zero-day worms [4], because new virus are often constructed by adding new behaviors to existing malware or replacing the obsolete modules with fresh ones, indicating that they share similar behavior patterns with existing malware [2]. In addition, Signature-based detection methods are not efficient for resource-limited mobile devices because they must check if each derived signature of an application matches in the virus database. Moreover, due to the high mobility of devices and the relatively closed nature of cellular networks, constructing network signature of mobile malware is very difficult. Thus a lightweight and novel detection method is required. There have been recent studies to model propagation of such malware in cellular and ad- hoc networks. Most previous works of mobile malware propagation are focused on Bluetooth worms. Generic worm propagation model is based on behavioral signatures that describe aspects of any particular worm's behavior such as sending similar data from one machine to another, the propagation pattern, and the change of a server into a client [5].

Some Researcher proposed a File system Monitoring method that can be monitored by checking file integrity, file attributes, or file access attempts. In checking for file integrity, the agent yields messages digests or cryptographic checksums for critical files, compare them against reference values, and verified their differences. Power-monitoring malware-detection framework that monitors detects and analyzes previously unknown energy-depletion threats. Kim et al. [6] characterize power consumption patterns of events and designed two important system components to perform a comprehensive analysis of the detection accuracy for pinpointing the identify of events, as well as classifying them as malicious or normal. SMS/MMS and Bluetooth vulnerabilities analysis identified the vulnerabilities in Bluetooth and SMS/MMS messaging systems that may be exploited by future mobile malware. By analyzing existing mobile malware to extract a set of their common behavior vector can be used to develop mobile malware detection and containment algorithm. Bose and Shin [7] investigated the propagation of mobile worms and viruses that spread primarily via SMS/MMS messages and Bluetooth. First, they analyze these propagated vulnerabilities in-depth so that appropriate malware behavior models can be developed. Next, they study the propagation of a mobile malware similar to Commwarrior in a cellular network. This result reveal that hybrid worms that

use SMS/MMS and proximity scanning (via Bluetooth) can spread rapidly within a cellular network, making them potential threats in public meeting places such as sports stadiums, train stations, and airports. Ruitenbeek et al. [8] also investigated propagation of MMS/SMS malware and various responses, although within only a small user population with an unconstrained messaging server.

Malware Detection Framework

In an innovative host-based Malware detection system for detecting malware on mobile devices was developed and evaluated. The framework (figure 1) relies on a lightweight agent (in terms of CPU, memory and battery consumption) that continuously samples various features on a device, analyzes collected data using machine learning and temporal reasoning method and inferences the state of the device. Features belonging to groups such as Messaging, Phone Calls and Applications belong to the Application Framework category and were extracted through APIs provided by the framework; features belonging to groups such as Keyboard, Touch Screen, Scheduling and Memory belong to the Linux Kernel category.

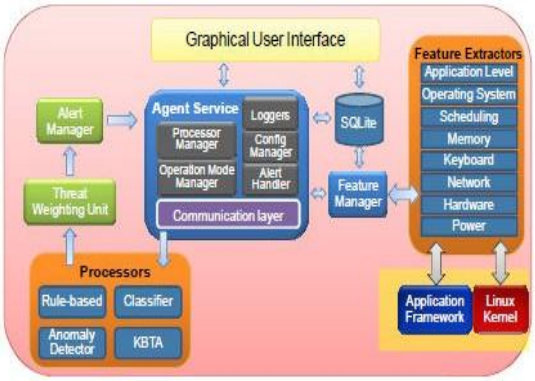

Figure 1: Mobile Malware Detection framework.

The above framework will help to reduce the malware intrusion and detecting to reduce the vulnerability in Mobile OS. KBTA (Knowledge Based Temporal Abstraction) light version is used for depicting the malware practices in the Mobile OS. Classifier is used to classify the behavior pattern. Anomaly Detector used to detect the anomalies in the data is passing in Mobile systems, Rule based processes used to divide the input based on the specified rule. So for communication processing four entities are used to reduce the Malware detection.

Prevention of Mobile Malware Attacks

The best way to protect your mobile device is to keep malware off in the first place. Use the same precautions for your phone as you would for your Windows laptop or desktop computer. Anti-virus and anti-malware tools to prevent infection are more effective solutions than products that only detect or clean viruses. After your mobile has been infected by malware, removal can be complicated. It's best to use a combination of both PC- based anti-virus software (with on-access scanning enabled) and mobile anti-virus software. Mobile users also should follow the same safe browsing practices they observe at their computers. We also recommend that users accept only programs that bear digital signatures—programs that have passed the certificate test and are developed by legitimate commercial software vendors.

As a well said sentence precaution is better than cure, so following are some of the way we can prevent malware attacks:

Install process management

Using process-management software, advanced users can search for suspicious processes on your mobile phone and stop them. Windows Mobile cannot run too many processes because of hardware limitations. So, log all the running processes when you're sure the mobile is not infected. Any time thereafter, it should be easy to spot a malicious process and stop it by following the advice of the mobile anti-virus software.

Be careful with Wi-Fi and Bluetooth

Disable Wi-Fi and Bluetooth when you're outdoors. These functions are easy to exploit for sending malicious code or viruses. It's also possible that sensitive information could be intercepted by a sniffer when these functions are enabled. The safest place to use these functions is at home or at trusted locations.

Back up frequently

Contact lists are vitally important to the company you work for and to you personally. If the list is lost or stolen, the consequences can be disastrous. It's a good practice to make frequent backups of data stored on mobile devices. Then, even if your mobile device has been infected, you can recover the default phone

settings to clean the system.

Install mobile anti-virus software

The majority of large security software vendors now have a mobile version of their anti-virus solutions, and many carriers and handset manufacturers are now including mobile anti-virus software by default. It's time to give your smart phone the same protection you give your desktop system.

Do not save business data on your mobile

Save confidential files or photos on removable disks. Don't save them on a mobile device. Mobile phones and PDAs are simply not very secure. The profit motive is expected to drive malware writers in increasing numbers to create mobile malware.

III. CONCLUSION

As we know that providing full fledged protection, a security method for mobile devices should include a collection of tools blending various capabilities that operate in synergy fashion. This paper discussion the malware practices in Mobile OS, a new frame work for mobile malware detection and the prevention mechanism for the malware as prevention is better than cure. So in this paper only the analysis, framework and prevention part is covered, other technical details have not been included.

REFERENCES

[1]. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, "Google Android: A State-of-the-Art Review of Security Mechanisms", CoRR abs/0912.5101, 2009.

[2]. M. Christodorescu, S. Jha, S.A. Seshia, D. Song, and R.E. Bryant, "Semantics-aware malware detection," in *Proc. the IEEE Symposium on Security and Privacy*, Oakland, California, pp. 32-46, May 2005.

[3]. J. A. Morales, P. J. Clarke, Y. Deng, and B. M. Golam Kibria, "Testing and evaluating virus detectors for handheld devices", *Journal in Computer Virology*, vol. 2, no. 2, pp. 135-147, 2006.

[4]. K. Wang, G. Cretu, and S. J. Stolfo, "Anomalous payload-based worm detection and signature generation," in *Proc. the 8th International Symposium of Recent Advances in Intrusion Detection (RAID 2005)*, pp. 227-246, Sep. 2005.

[5]. D. R. Ellis, J. G. Aiken, K. S. Attwood, and S. D. Tenaglia, "A behavioral approach to worm detection," in *Proc. the 2004 ACM Workshop on Rapid Malcode (WORM)*, pp. 43-53, 2004.

[6]. H. Kim, J. Smith, and K. G. Shin, "Detecting energy-greedy anomalies and mobile malware variants," in *Proc. the 6th ACM International Conference on Mobile Systems, Applications, and Services*, pp. 239-252, 2008.

[7]. Bose and K. G. Shin, "On mobile viruses exploiting messaging and bluetooth services," in *Proc. the 2th IEEE International Conference on Security and Privacy in Communication Networks*, pp. 1-10, 2006.

[8]. E. V. Ruitenbeek, T. Courtney, W. H. Sanders, and F. Stevens, "Quantifying the effectiveness of mobile phone virus response mechanisms," in *Proc. the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 790-800. June 2007.