IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Intrusion Detection System for Android Smartphone in Cloud Environment

Anirudha A. Kolpyakwar[1], Prof. Pragati Patil[2]

Department of Computer Science & Engineering, A.G.P.C.E. Nagpur, India [1]

Professor, Department of Computer Science & Engineering, A.G.P.C.E. Nagpur, India [2]

Abstract: Cloud computing is primarily being use for eliminating the need of local information resources. The ability of cloud offers vast variety of services on web. As Smartphone usage has been continuously increasing in recent years, but due to its complexity and functionality, they are also susceptible to the attacks such as virus, Trojans and worms. The smart phones have inadequate storage, processing and computational power to execute highly complex algorithms for intrusion detection and implementing signature based attack detection. In this paper, different system architecture for a cloud based intrusion detection. This architectures offers security against any misbehavior in network. This analysis on the emulated device includes running multiple detection engines in parallel, memory scanners and system call inconsistency detection that generate responses in event of attack.

Keywords: Android Smartphone, Cloud Computing, Intrusion Detection.

1. INTRODUCTION

Android smart phones are extremely popular fast growing communication devices in recent years [4]. With the advent of internet, the mobile network infrastructure quality and affordability consistently improved. As their data transmission become affordable and available, usage of smart mobile phones for online financial transactions, mobile learning and web browsing become widely popular among users [13] which also cause several security issues. For Android based smart phones, there are lot of third party application are available in free of cost on Google Play and various other application store websites. Its easy availability of application encourages attackers to build malicious applications for such devices. As architecture of such devices are much similar to classic personal computers in terms of functionality as well as performance, common security threats like worms, Trojans and viruses are also affecting smart phones [9, 10]. To protect from such threats same security algorithms required that used to secure desktop-PC. But these algorithms are highly complex and resource consuming, it can not beexecute on such smart mobile phone devices as they have power, computational and storage limitations.

Another problem is inconsistency in software support and security fixes by the manufacturer of smartphone device. If bug fixes and patches are does not provide by manufacturers to customers then security of smartphone would be highly compromised and make them vulnerable to attack. This is for example shown by the apparent version fragmentation which can be observed in the Android environment [5]. The consistent updating of software version and fixes makes devices more secure but it lacks in mobile devices. Using firewalls, antivirus scanners, spyware scanners and root kit detectors on smart mobile devices is proves to be difficult, mainly because of lack of resources like battery longevity, computing power and storage.

2. PROPOSED TECHNIQUE

To enhance mobile device security, cloud-based intrusion detection has been proposed. A synchronized cloud-based intrusion detection and response framework for Android smart phone devices is achieved by introducing security level integration in a cloud proxy. These security levels classify the security level at the user level, communication channel and device itself. The cloud provides bandwidth usage, power consumption (battery life) and processing power required to execute highly complex intrusion detection algorithms, a Security as a Service (SECaaS) of cloud computing is used.To recover and restore device from attack situation and interact with cloud, use of proxy server is proposed which communicate to device through mobile host installed on device.

In this project, the proposed architecture consists of a cloud computing services that receives input from the device and performs intrusion detection to identify malicious behavior or content over a network and a lightweight mobile host agent installed on mobile device.

The proposed architecture consists of computing services that receives input from the device and performs intrusion detection to identify malicious behavior.

- Mobile Host Agent
- Proxy Server
- Web Service
- Intrusion Detection System Engine

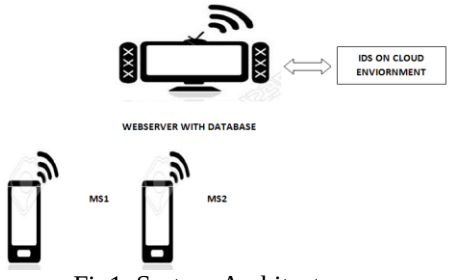


Fig1. System Architecture

DOI 10.17148/IJARCCE.2015.412158

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

3. CLOUD COMPUTING SERVICES

The major component of the architecture is cloud computing services. In this architecture platform as a service and security as a service for intrusion detection and taking proper action against it. Firstly, the target device is communicated with the cloud server application that monitors the traffic between device and internet and detects malicious activities.

4. MOBILE HOST AGENT

The mobile host agent is a lightweight process that installed in the form of application on the Android device. It inspects file activity on the system and receives a signal from a cloud. It is also provides the access control where each file is trapped and send to a handling routine which begins by generating a unique identifier (such as a hash) of the file, which is compared against a cache of files those are previously analyzed. If a file identifier is not present in the cache, then the file is sent to the in-cloud network service for analysis.

After the analysis of file, the results are stored in both a local cache on the mobile host agent and in a shared remote cache in the cloud computing service. Then the files can be accesses by mobile device simply look up the result in the local cache without requiring network access. In addition, access of the same file by other devices can be mediated using a shared remote cache located in the cloud service, without having to send the file for analysis.

Cached reports stored in the network service may also opportunistically be pushed to the agent to speed up future accesses.

5. TECHNIQUE

Intrusion Detection System Engines are used

- Symantec Protection Engine
- ClamAV
- Microsoft Anti-Virus API

In this module an ongoing mirrored traffic is monitored for any malicious activity and intrusion. The intrusion detection is done on the basis of behavior, signature-based and anomaly-based analysis. The latest antiviruses are also deployed on cloud to detect malware specific for android smart phones.

5.1 Behavioral Analysis

Another approach is described by Bose et al. [1]. They are relying on behavioral analysis for detecting malware on mobile devices. Their idea is based on the assumption that a single action performed by an application can be classified as harmless, but in relation to other actions, which are performed in the same context, malware behavior can be exposed.

Based on this assumption Bose et al. developed a database of behavioral signatures for malware. By training a support vector machine with normal behavior of applications, anomalies such as malware can be detected.

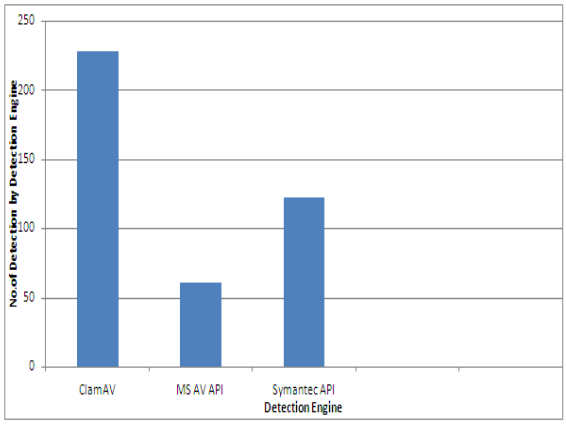
6. RESULT ANALYSIS

In existing system of protection against malware attacks, Android smart phones are protected by antivirus software (such as Avast, Kaspersky, McAfhee) which consumes substantial battery power of a device even in standby mode.

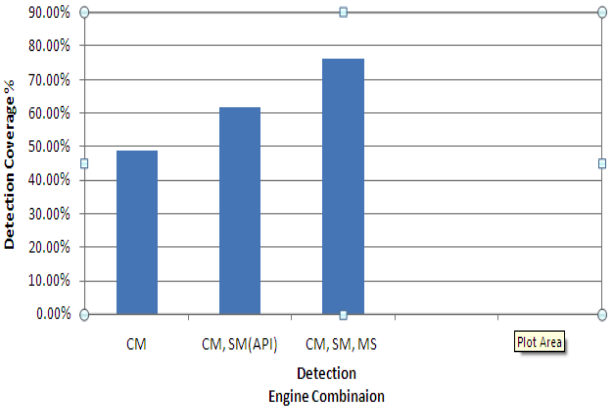
In addition to this, antivirus software is based on signature based detection which limits the detection range up to dataset available to that particular software. This dataset set again need to update consistently which affects bandwidth efficiency. Many times such software won't provide coverage to most recent signatures.

6.1 Performance Analysis

The major advantage of mobile host agent over antivirus software is ability to run multiple detection engines in parallel. The existing antivirus software cannot run multiple detection engines on a single device due to technical conflicts and resource constraints. Because of that the coverage of detection threats is very limited as illustrated in Graph 1.



Graph 1. Detection by using Detection Engine Individually



Graph 2: The increased coverage using multiple detection engines in parallel

7. CONCLUSION

Cloud based an intrusion detection service that provides optimal protection to Android Smartphone and mobile host provides efficient detection It provides desired configuration by installing several application at once.

This eases the conformability with the system even for technically unsound users.

In this system, proxy server is responsible for duplicating the communication between the Smartphone and the Internet and sending it to the emulator in cloud environment where the intrusion detection and in-depth forensics analyses are performed. This process won't interrupt the regular communication between the Smartphone and the Internet. the lightweight mobile host agent on the Smartphone performs three main tasks. It collects all user and sensor inputs to the device, it sends them to the emulation environment, and it waits for potential response and recovery commands, e.g., neutralizing the malicious application, from the emulation environment in order to take the required actions**.**

8. FUTURE ENHANCEMENT

To counter limitation mentioned above the mobile host will be enhanced with new feature of ability to generate update.zip file. The update.zip is .zip file that contains all apps information of user and can be used for flash an Android Smartphone device at the root level. As the further enhancement providing update.zip generation capabilities, even a technically unsound user can customize the update.zip file as per his convenience. So when recovery of the Android Smartphone device will takes place, the device would be flash through update.zip file that would be generated and stored before initiation of the recovery process. Due to this feature user will not need to restore all the lost application manually.

As the flashing of Android Smartphone device would be done on root level, it requires executing command on terminal of Android Smartphone. The future enhancement will also include patch to mobile host to run those commands on terminal level.

REFERENCES

[1] Android tops iosas most popular platform on global ad network [online], http:// techcrunch. com/2012/07/18/adfonic -android- tops-ios- as-most-popular-platform-onglobal-ad-network-iphone-ipad-still-top-devices/

[2] Stojankitanov, dancodavcev "Mobile Cloud Computing Environment as a Support for Mobile Learning". In CLOUD COMPUTING: The Third International Conference on Cloud Computing, grids, and Virtualization, 2012, pages 99-105.

[3] The 10 most common mobile security problems [Online] http:// www.networkworld.com /news/ 2012 /091912-mobile-security-262581.html.

[4] J. Jamaluddin, N. Zotou, and P. Coulton. "Mobile phone vulnerabilities: a new generation of malware". In Consumer Electronics, IEEE International Symposium, 2004, pages 199 – 202.

[5] IBM Corporation, "IBM X-Force 2011 Mid-year Trend and Risk Report"https://www 14. software.ibm.com/webapp/iwm/web/signup.do?Source=swg-spsm-tiv-sec-wp&SPKG=IBM-X-Force -2011-Mid-year, 2011, [retrieved: May, 2012].

[6] Thomas Ruebsamen, Christoph Reich, "Enhancing Mobile Device Security by Security Level Integration in a Cloud Proxy". In CLOUD COMPUTING : The Third International Conference on Cloud Computing, grids, and Virtualization , 2012, pages 159-168

[7] Hamethamad, Mahmoud Al-Hoby, "Managing Intrusion Detection as a Service in Cloud Networks". In International Journal of Computer Applications, 2012, pages 35-40.

[8] Cloud Computing [Online] http://en. wikipedia. org/ wiki/Cloud_computing

[9] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier, "A Cloud-based Intrusion Detection and Response System for Mobile Phones". In DSN-W, 2012, pages 31-32

[10] Jon Oberheide, kaushikveeraraghavan, Evan Cooke, Jason Flinn, farnamjahanian, "Virtualized In-Cloud Security Services for Mobile Devices". In Proceedings of the First Workshop on Virtualization in Mobile Computing, 2008, pages 31–35.

[11] Piromsopa, K.; Enbody, R.J. "Buffer Overflow Protection: The Theory". In Electro/information Technology, IEEE International Conference, 2006, pages 454-458.

[12] Zhichun Li; Lanjia Wang; Yan Chen; Zhi Fu, "Network-based and Attack-resilient Length Signature Generation for Zero-day Polymorphic Worms". In Network Protocols, 2007, Pages 164 – 173.

[13] Georgiosportokalidis Philip Homburg Kostas Anagnostakis, "Paranoid Android: Versatile Protection For Smartphones". In Proceedings of the 26th Annual Computer Security Applications Conference, 2010, pages 347–356.

[14] Yajin Zhou, Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution". In DSN Oakland, 2012

[15] A.D. Schmidt, R. Bye, H.-G. Schmidt, J. Clausen, O. Kiraz, K. Yuksel, S. Camtepe, and S. Albayrak, "Static analysis of executables for collaborative malware detection on android," in Communications, 2009. ICC '09. IEEE International Conference on, june2009, pages1–5.

[16] Bose, X. Hu, K. G. Shin, and T. Park, "Behavioral detection of malware on mobile handsets," in Proceeding of the 6th international conference on Mobile systems, applications,and services, ser. Mobisys '08. New York, NY, USA:ACM, 2008, pages 225–238.

[17] Android Developers, "Android Platform Versions –Current Distribution,"http:// developer.android. com/resources/dashboard/platform-versions.html, 2012,[retrieved:October,2012].