ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)

Volume 3, Issue 6, June 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Special Issue: 4th International Conference on Quality Up-gradation in Engineering, Science & Technology "IC-QUEST 2015"

Organized By: Bapurao Deshmukh College of Engineering, Sevagram, Wardha-442102, Maharashtra, India

A Survey on Intrusion Detection System for Android Smartphone in Cloud Environment

Anirudha A. Kolpyakwar[1]
Department of Computer Science & Engg.
M.Tech (IV SEM), Abha Gaikwad Patil College of Engineering,
Nagpur, India

Prof. Yogesh Bhute[2]
Department of Computer Science & Engg.
Abha Gaikwad Patil College of Engineering,
Nagpur, India

***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 misbehaviour 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. The responses are instructs to mobile agent installed on the device to take essential actions and perform recovery of device if needed.*

***Keywords:** Android Smartphone, Cloud Computing, Intrusion Detection.*

I. Introduction

1.1. Cloud Computing

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data centre from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption." Cloud Providers offer services that can be grouped into three categories. [13]

1.1.1. Software as a Service (SaaS):

In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Sales force, Microsoft, Zoho, etc. [13]

1.1.2. Platform as a Service (Paas):

Here, a layer of software or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc are some of the popular PaaS examples. [13]

1.1.3. Infrastructure as a Service (Iaas):

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc. [13]

1.2 Android Smartphone

Android smart phones are extremely popular fast growing communication devices in recent years [13]. With the advent of internet, the mobile network infrastructure quality and affordability consistently enhanced. 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 which also cause several security issues [1], [13]. 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 [2], [13]. 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 cannot be execute 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 [13].

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. To overcome such limitations of smart mobile phone, Cloud Computing provides plenty of services, software and processing power over an internet. In relation of mobile phones it reduces bandwidth usage, power consumption (battery life) and processing power [3], [4], [13]. Cloud computing, and specifically Security as a Service (SECaaS), changes the dynamics of protecting smart phones over a network [13].

Using such cloud services we can detect misbehaviour in network and send back the response signal which initiates recovery on the smart phone device [5], [13]. In Android smart phones recovery has to be done by putting a device in recovery mode. In the recovery process any damage to mobile phone is recovered and device being restore. The recovery is done by using mobile host agent which is nothing but the android application that been installed in device. This application receives signal from cloud and manages traffic between internet and device [13].

1.3 Available Security Mechanism in Android Smartphone

In existing system of protection against malware attacks, Android smart phones are protected by antivirus software (such as Avast, Kaspersky, McAfee) 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 will not provide coverage to most recent signatures. In this paper, we are suggesting the mechanism that uses the cloud environment and virtualization of mobile device as a mobile host agent that protects device with conservation of vital resources battery, bandwidth and computational power [13].

1.4 Mechanism of Mobile Host Agent

Same as an existing antivirus software, the mobile host agent is also a lightweight process that runs on device and inspects the file activity. The only basic difference is that the mobile host is deals with the cloud services and as mentioned earlier existing antivirus software is signature based having very limited signature database size [6], [13]. The signature database size is keep varying in accordance of different antivirus software but as mobile agent works in collusion with cloud environment, it have advantage over antivirus software in terms of database size, as shown in Table 1.

TABLE-I
The Number of Threats Addressed in the Signature Database of Various Detection Engines

Detection Engine	Top
Kaspersky Mobile	284 signature
Clam AV	262289 signature
Mobile Agent	> 5 million + behavior

The second 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. The mobile host can use cloud services and run multiple detection engine in parallel by hosting them on emulated device. The use of virtualization to run multiple detection engines increases the coverage malware detection. This also helps to scale a system to large number of users and engines. This allows analyse any single file by various different detection engines [6], [13]. The increased detection coverage against a dataset of malware samples when using multiple engines in parallel Clam AV (CM), Symantec (SM), McAfee (MA), Bit-Defender (BD), and F-Secure (FS), the coverage also increases as illustrated in Table 2.

TABLE-III
The Increased Coverage using Multiple Detection Engines in Parallel

Engine Combination	Detected	Coverage
CM	229/469	48.82%
CM, SM	290/469	61.83%
CM, SM, MA	358/469	76.33%
CM, SM, MA, BD	417/469	88.91%
CM, SM, MA, BD, FS	430/469	91.68%

1.5 A Mobile System Architecture with Cloud Proxy

The proxy server acts as a intermediary which mirrors the ongoing traffic between mobile devices and internet then sends it to the cloud computing services where further in detail analysis has been performed on the basis of behaviour pattern and code signature [10]. Using various security procedures provided by cloud computing services for Android Smartphone, cloud services ensures the security of device [10].

Using a proxy server permits us to take the advantages of cloud computing which have almost unlimited computing power for analysing the security of the mobile system. The mobile security of the entire system depends basically on the security and trust level of the user, the mobile device, the communication channel, and the backend, the cloud as shown in Figure 1. The proxy, which is under company control, is used to collect as much security related information about the precedent components as possible (for example by analysing network traffic, querying company databases for organizational information et cetera). Additionally, the proxy requests information directly from the mobile device [10].

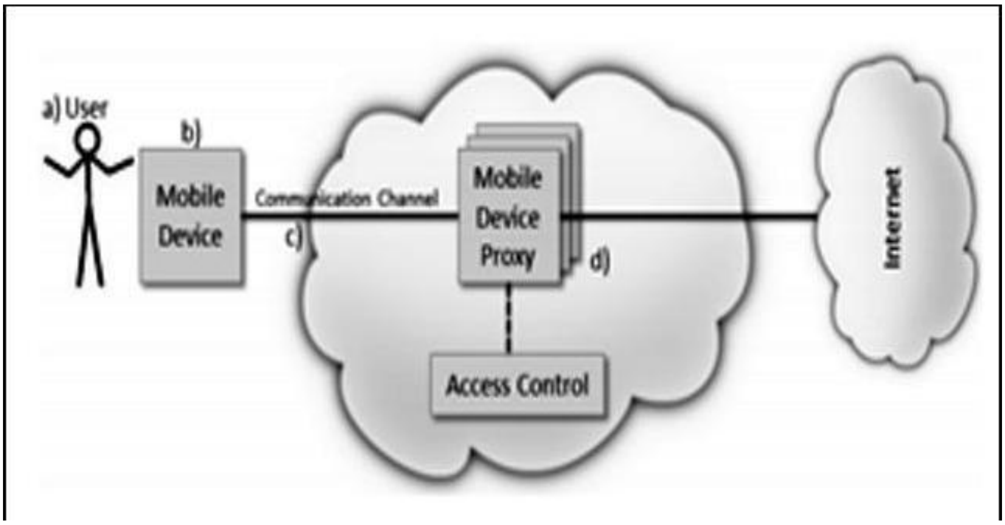

Fig 1: Mobile System Architecture with Cloud Proxy

II. Related Work

Paranoid Android which is an intrusion detection mechanism for Android based smart phones was developed. This system was based on the cloud where intrusion detection used as a service [9]. This mechanism used to mirror the traffic between Smartphone device and internet using proxy server and then analysis was done by replay and record method [9].

A very similar approach Response System for Mobile Phones exists in available Android architecture [5]. In this architecture, to provide intrusion detection through cloud computing where a lightweight mobile host was used to recover the device as well as achieve the input or files from the device and send it to the network. There are many different intrusion detection techniques are used in this system such as game theoretic intrusion and recovery engine that used to plot graph based on the behaviour of network or some particular entity [5]

III. Hi Level Architecture for Android Smart Phone Security

The Android Smartphone's are having limitations in computational resources such as processing power, battery longevity and storage capacity which results in poor protection against various security threats. These threats include zero day attacks, memory resident attacks, viruses, Trojans and many other threats. To protect the Smartphone against these threats we need high level intrusion detection algorithms, antivirus software and scanners. Due to limitations of resources Android smart phones cannot protect themselves powerfully against these attacks. The existing antivirus software provides signature based attack detection which again has limitation for signature database size. To overcome such computational limitation the cloud services present in High Level Architectures are very useful key. The cloud computing provides vast set of services which could be access anywhere from the network. The cloud provides security services which could be used for protecting the Smartphone device [13].

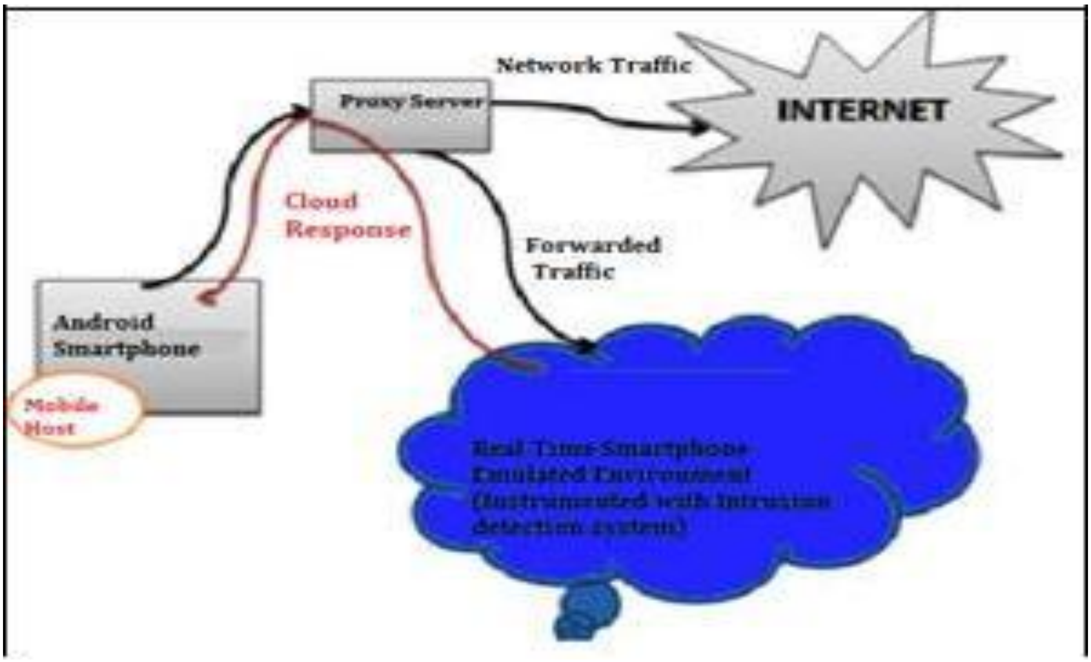

Fig 2: System Architecture

High Level architecture consists of a cloud computing services that receives input from the gadget and performs intrusion detection to recognize malicious behaviour or content over a network and a lightweight mobile host agent installed on mobile device that performs recovery process in event of failure [13]. High level system architecture is shown in Figure 3. It consists of two major services cloud computing and mobile host agent. The function and sub functions of these two services explained below.

3.1 Cloud Computing Services

The major component of this architecture is cloud computing services. In this architecture, emulated device platform as a service and security as a service for intrusion detection and taking proper action against it. Firstly, the target device is registered on the cloud server application that monitors the traffic between device and internet and detects malicious behaviour [13]. This application set up following security methods.

Antivirus Software: The various effective, efficient and popular open source ant viruses being used to run in the emulator to detect various malicious scripts, signature and definition of viruses, worms, and Trojans [13]. The heading for sub subsections should be in Times New Roman 11-point italic with initial letters capitalized and 6-points of white space above the sub subsection head.

3.2 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 analysed. If a file identifier is not present in the cache, then the file is sent to the in-cloud network service for analysis [13].

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 [13]. Cached reports stored in the network service may also opportunistically be pushed to the agent to speed up future accesses. It is also responsible for executing commands required to flash Android Smartphone device into recovery mode [13].

IV. Conclusion

This paper explains various cloud based intrusion detection services that provides favourable shield to Android Smartphone and mobile host provides optimal recovery procedure. It gives desired configuration by installing several applications at one time. 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.

The evaluation of a user space implementation of Paranoid Android architecture, shows that transmission overhead can be kept well below 2.5 Kbps even during periods of high activity (browsing, audio playback), and to virtually nothing during idle periods. Battery life is reduced by about 30%, but it can be significantly improved by implementing the tracer within the kernel. It offers more comprehensive security than possible with alternative models.

To address the growing concern of mobile device threats, Record and Replay approach can be used in mobile device for malware detection. By moving the detection capabilities to a network service, it increases the detection coverage, less complex mobile software, and reduced resource consumption. This approach shows that it is feasible and effective for the current generation of mobile devices, but will become even more consequential and valuable in the future as the scale and sophistication of mobile threats increases.

References

1. Stojan Kitanov, Danco Davcev “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.
2. 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.
3. 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
4. Hamet Hamad, Mahmoud Al-Hoby, “Managing Intrusion Detection as a Service in Cloud Networks”. In International Journal of Computer Applications, 2012, pages 35-40.
5. 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
6. Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, Farnam Jahanian, “Virtualized In-Cloud Security Services for Mobile Devices”. In Proceedings of the First Workshop on Virtualization in Mobile Computing, 2008, pages 31–35.
7. Piromsopa, K.; Enbody, R.J. “Buffer Overflow Protection: The Theory”. In Electro/information Technology, IEEE International Conference, 2006, pages 454-458.
8. 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.
9. Georgios Portokalidis Philip Homburg Kostas Anagnostakis, “Paranoid Android: Versatile Protection For Smartphones”. In Proceedings of the 26th Annual Computer Security Applications Conference, 2010, pages 347–356.
10. Yajin Zhou, Xuxian Jiang, “Dissecting Android Malware: Characterization and Evolution”. In DSN Oakland, 2012\
11. 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, june 2009, pages 1 –5.
12. 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.
13. CLOUD COMPUTING – An Overview by Torry Harris