IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Intrusion Detection in Cloud for Smart Phones

Namitha Jacob

Department of Information Technology,
SRM University, Chennai, India

Abstract

The popularity of smart phone is increasing day to day and the security is a great concern for the smart phone since it contains much relevant information. We download a large amount of contents from internet like image, music, video file, text file etc to our mobile phones. There is no mechanism to detect whether the contents are corrupted or not. In this paper I am proposing a methodology where an intrusion and detection process is defined in the cloud and it detects the corrupted files in web server. It checks the properties of content in server based on algorithm and an alert message will be given to the smart phone users. Since the application is build in cloud any number of users can download this application from cloud. Call blocking and sms blocking is provided through this application. To validate our methodology, I injected malicious programs into our mobile cloud test bed and used a machine learning algorithm to detect the abnormal behaviour that arose from these programs.

Keywords: Monitoring and detecting process, string matching algorithm, call and sms blocking

1. Introduction

Smartphones, as extremely fast-growing type of communication devices, offer more advanced computing and connectivity functionalities than contemporary mobile phones by conceptually integrating handheld computers' capabilities with phone devices. While most traditional mobile phones are able to run applications based on specific platforms such as Java ME, a smartphone usually allows the user to install and run more advanced third-party software applications. Being an "all-in-one" device, smartphones are increasingly getting attractive to a wide range of users. A recent study by ComScore Inc. indicates that over 45.5 million people in the United States owned smartphones in 2010, a 20% share of the total devices sold, and a continuous annual growth rate of 156% [1] is estimated.Following smartphones' increasing popularity, attackers have also been interested in attacking to such platforms. In fact, a large number of smartphone malware have attempted to exploit unique vulnerabilities of smartphones. As a case in point, the smartphone virus Cabir spreads and populates through the Bluetooth interface of smartphone. Another recent smartphone security study shows that trojans, using voice-recognition algorithms, can steal sensitive information that is talked through smartphones. Such threats not only invade privacy and security of the smartphone users, but also manage to generate coordinated large-scale attacks on the communication infrastructures by forming botnets consumption because packets are transmitted over shorter distances, and improve the area spectral efficiency and the network throughput and capacity.

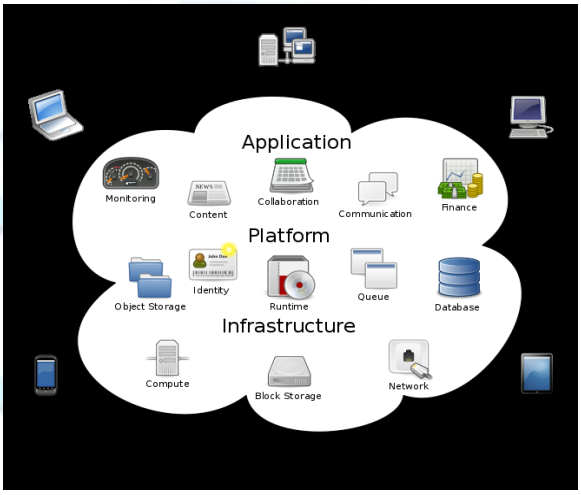

Fig 1.a Cloud Computing

There are three types of cloud computing:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS).

Using Software as a Service, users also rent application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run. End users access cloud based applications through a web browser or a light weight desktop or mobile app while the business software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.

For companies that only have to process large amounts of data occasionally running their own data center is obviously not an option. Instead, Cloud computing has emerged as a promising approach to rent a large IT infrastructure on a short-term pay-per-usage basis. Operators of so-called IaaS clouds, like Amazon EC2, let their customers allocate, access and control a set of Virtual Machines (VMs) which run inside their data centers and only charge them for the period of time the machines are allocated. The VMs are typically offered in different types, each type with its own characteristics (number of CPU cores, amount of main memory) and cost.

Since the VM abstraction of IaaS clouds fits the architectural paradigm assumed by the data processing frameworks like Hadoop. The Apache Software Foundation, a popular open source implementation of Google's Map Reduce framework, already have begun to promote using their frameworks in the cloud. Only recently, Amazon has integrated Hadoop as one of its core infrastructure services. However, instead of embracing its dynamic resource allocation, current data processing frameworks rather expect the cloud to imitate the static nature of the cluster environments they were originally designed for, e.g., at the moment the types and number of VMs allocated at the beginning of a compute job cannot be changed in the course of processing, although the tasks the job consists of completely different demands on the environment. As a result, rented resources may be inadequate for big parts of the processing job, which may lower the overall processing performance and increase the cost.

In this project a proactive defense mechanism is developed in cloud for the smart phones. When the user gives request to download the content from the web server, the IDS system in cloud checks whether the file is corrupted or not based on an algorithim I am designing.

2. Related Works

The proposed framework targets a practical scenario in which most smartphones cannot be equipped with heavyweight anti-malware software, but need to be protected against attacks. The proposed framework is in fact a cloud service which provides intrusion detection and response capabilities to the registered smartphones. It emulates the actual smartphone device in a virtual machine in cloud using a proxy which duplicates the in-coming traffic to the devices and forwards the traffic to the emulation platform. The real-time emulation on powerful servers allows the framework to instrument the emulated environment with a rich set of (possibly resource intensive) off-the-shelf intrusion forensics and detection systems, which do not necessarily have to be lightweight, and perform a run-time in-depth detection analysis. The key difference with previous attempts is to replicate user input in real time. This enables our solution to have very limited bandwidth requirements while keeping the replica always synchronized. In case a misbehaviour is detected, the intrusion response decides upon the best countermeasure actions and sends it to a non-intrusive software agent in the device, which is in charge of only carrying out the received actions.

3. Existing Systems

In the existing security systems the intrusion detection software should be downloaded in the

mobile phones. And once the detection occurs the software detects and informs the user.

3.1 Disadvantages of existing system

In the existing the intrusion software that is downloaded consumes memory and power. It is not a proactive defence mechanism since once the threat get affected in the mobile it informs the user.

4. Proposed System

In the proposed system a proactive defence mechanism is developing where the smart phone user is given the alert that the file is corrupted before it is downloaded. The system is developed in cloud so all the registered user can use the system at a single time.

In this project the user can view and download the contents from the web server. The different contents provided by the web server include the images, videos and text files. The user is registered in the cloud initially. The device type, operating system and application are entered of the user and an instance of the user mobile is generated in cloud. After the successful registration the user can use IDS as a software as a service.

A string matching algorithm is developed here for detecting the corruption in the file. The properties of the files are entered in the cloud server. Once the file is corrupted the cloud server compares properties of file that are not changed in cloud server with that of the changed contents in the web server. And detecting that the contents are altered an error message will be send to user. In this project I am developing an application for smart phone users. This is provided as the SaaS in the cloud .The user can get the service when the user is registered in the cloud. Once the user is successfully registered he can get access of the service. When the user is intended to download a particular file from the server the system uses a string matching algorithm for determining whether the file is corrupted or not. If the file is corrupted then an error message will be send to the user then the user can cancel the downloading. If the content is not corrupted then the required file is downloaded.

The different services the user can provide is to view and download a file. Images, videos and text files are provided to the user for viewed and downloaded from internet. Once the user click the download button the proxy server will be redirecting the connection to the cloud server and local server. The cloud server then checks the file to identify whether the contents are corrupted or not. The cloud server uses a string matching algorithm for checking it

As smart mobile phones, so called smart phones, are getting more complex and more powerful to efficiently provide more functionality, concerns are increasing regarding security threats against the smart phone users. Since smart phones use the same software architecture as in PCs, they are vulnerable to similar classes of security risks such as viruses, Trojans, and worms. In this paper, they propose a cloud based smart phone-specific intrusion detection and response engine, which continuously performs an in-depth forensics analysis. In case misbehavior is detected, the proposed engine decides upon and takes optimal response actions. Despite the computational and storage resource limitations in smart phone devices, the intrusion detection is done in cloud.

5. Implementation

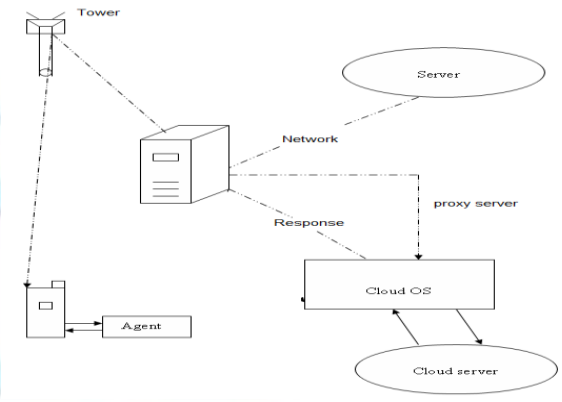

Figure1: High Level Architecture

6. Methodology

6.1. IDS design in cloud

The cloud architecture module is responsible for creating an intrusion detection system in cloud. I am creating a web server where the contents are entered into it. The view and download options are provided to the users. The properties of all the files are entered into the cloud server. A string matching algorithm is entered into the cloud server for comparison.

6.2 Client registration module & proxy process

To register, the client should first specify his or her device, it operating system and the application list, so the frameworks can instantiate an identical image of the smart phone in cloud. A proxy server is responsible for duplicating the communication between the smartphone and the Internet and forwarding it to the emulation environment in cloud where the detection and forensics analyses are performed. The registered client only gets the service from the cloud. A proxy server is responsible for duplicating the communication between the smart phone and the Internet and forwarding it to the intrusion detection environment in cloud where the detection and forensics analyses are performed.

6.3. Monitoring and detecting process

The monitoring and detecting process is developed in cloud for identifying any intrusion in the web server. When the request is send by the client it is forwarded to the cloud where cloud server identifies any change in the contents of the file based on the string matching algorithim. If the intrusion is identified then the cloud provides an alert message to the user else the user can identify them.

The features of CPU, memory, and network usages monitored these using their mobile application, and then detected malware using several machine learning algorithms. *Damopoulos et al.* focused on malware that are related to spamming, but their method cannot detect more general malware. They defined the behaviour of mobile devices as web browsing, SMS, phone calls, and were able to detect abnormal behaviour using machine learning algorithms available with high accuracy. There are other studies that also focus on abnormal behaviour in mobile devices, but those studies defined the behaviour of mobile devices differently. *Enck et al.* related abnormal behaviour of mobile devices to privacy information on mobile devices. Their framework monitors the privacy data by observing event lists in Android devices, and detected that several mobile applications can misuse users' private information. *Burguera et al.* correlated behaviour with the number of each system call counter, and focused on some important system calls that are related to normal applications and malware such as access(), chmod () However, their framework requires root permission in Android devices in order to monitor the number of system calls in mobile devices.

7. Conclusion

A cloud-based service to provide security and tolerance to resource limited mobile phone devices. The system identifies the intrusion in the specific smart phone using cloud. If any unsecured file or misbehaviour is detected, the system will take the corresponding response actions to handle the threat. This system produces accurate intrusion detection and response .The system uses the light weight resources. Any number of users can register and get the benefit of this application. This keep your phone free from viruses and malware.

8. References

[1] IEEE. 2012 :Monitoring and Detecting Abnormal Behaviour in Mobile Cloud Infrastructure" Taehyun Kim, 1Yeongrak Choi, 2Seunghee Han.

[2] A. Boukerche and M. S. M. A. Notare. Behavior-based intrusion detection in mobile phone systems. Jour. Paral. & Dist. Comp

[3] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. Virtualized in-cloud security services for mobile devices.

[4] F. Gens, "IT Cloud Services User Survey, pt.2: TopBenefits&Challenges",IDCeXchange(http://blogs.idc.com/ie/), August 14, 2008.

[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 2010, Vol.34, No.1, July 2010, pp.1-11.

[6] A.Shabtai, U. Kanonov, and Y.Elovici, "Andromaly: a behavioural malware detection framework for android devices", Journal of Intelligent Information Systems, January 2011, pp 1-30.