Intrusion Detection for Smart phone using Cloud

[1]G.Hemaprabha, [2]Visalatchi.R
[1, 2]PG Student (CSE), Aarupadai Veedu Intitute of Technology
Chennai, India

Abstract
Smart phones have recently become increasingly popular because they provide “all-in-one” convenience by integrating traditional mobile phones with handled computing devices. Unfortunately these mobile devices are beginning to face many of the same security threats as desktops. Since smart phones software architecture is similar to the PCs software architecture, they are vulnerable to similar type of security risks such as worms, Trojans and viruses. So, this system proposes a cloud based smart phone specific intrusion detection and response engine. If any unsecured file or misbehaviour is detected, the system will take the corresponding response actions to handle the threat. This system will produce accurate intrusion detection and response with light resource requirement.

Keywords— IDS (Intrusion Detection System), PDA (Personal digital Assistant), IP (Internet Protocol),

I. Introduction

A. Smart phone:

Modern mobile devices continue to approach the capabilities and extensibility of standard desktop PCs.One among is the smart phone. Smart phones have recently become increasingly popular be-cause they provide “all-in-one" convenience by integrating traditional mobile phones with handheld computing devices. In short we can say Smart phones integrate the functions of a Cell phone and a PDA or a Handheld PC. Smart phones now face new security problems not found elsewhere. These problems originate directly from the integration process and are often related to the inclusion of multiple wireless technologies into a single device. Hundreds of smart phone viruses have emerged in the past two years, which can quickly spread through various means such as SMS/MMS, Bluetooth and traditional IP-based applications. Currently, mobile security solutions mirror the traditional desktop model in which they run detection services on the device. This approach is complex and resource intensive in both computation and power.

As a case in point, the smart phone virus Cabir [7] spreads and populates through the Bluetooth interface of smartphones.Another recent smart phone security study shows that trojans,using voice-recognition algorithms, can steal sensitive information that are talked through smart phones [2].Such threats not only invade privacy and security of the smart phone users, but also manage to generate coordinated large-scale attacks on the communication infrastructures by forming botnets.Previously the solutions are provided where such security services encounter a lot of limitations in practice. Many of the schemes fail because of the limited memory, storage, computational resources and battery power of the smart phone. Most of such approaches require some data or signatures to be downloaded from the database where it needs large storage and heavy resources.Another class of security services provide light resources but fails in performance and accuracy. And previously there is no automated response and recovery.

B. Cloud Computing:

Cloud computing is the delivery of computing as service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).

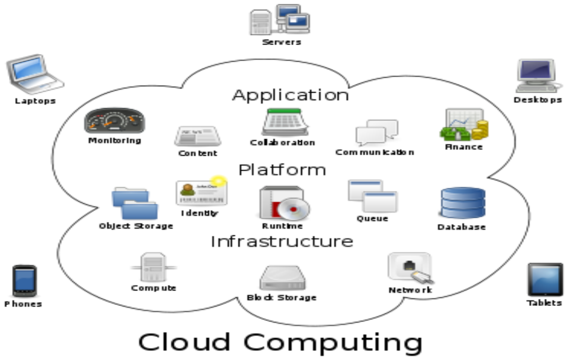

Fig 1 Architecture of Cloud Computing

C. Cloud Services:

Cloud computing providers offer their services according to three fundamental models: Infrastructure as a Service (IaaS), platform as a Service (PaaS), and Software as a Service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models.

(i).Infrastructure as a Service (IaaS)

In this most basic cloud service model, cloud providers offer computers – as physical or more often as virtual machines –, raw (block) storage, firewalls, load balancers, and networks. IaaS providers supply these resources on demand from their large pools installed in data centers. Local area networks including IP addresses are part of the offer. For the wide area connectivity, the Internet can be used or - in carrier clouds - dedicated virtual private networks can be configured.

To deploy their applications, cloud users then install operating system images on the machines as well as their application software. In this model, it is the cloud user who is responsible for patching and maintaining the operating systems and application software. Cloud providers typically bill IaaS services on a utility computing basis, that is, cost will reflect the amount of resources allocated and consumed.

(ii).Platform as a Service (PaaS)

In the PaaS model, cloud providers deliver a computing platform and/or solution stack typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying compute and storage resources scale automatically to match application demand such that the cloud user does not have to allocate resources manually.

(iii).Software as a Service (SaaS)

In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its elasticity. This can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be multitenant, that is, any machine serves more than one cloud user organization. It is common to refer to special types of cloud based application software with a similar naming convention: desktop as a service, business process as a service, Test Environment as a Service, service. The pricing model for SaaS applications is typically a monthly or yearly flat fee per user

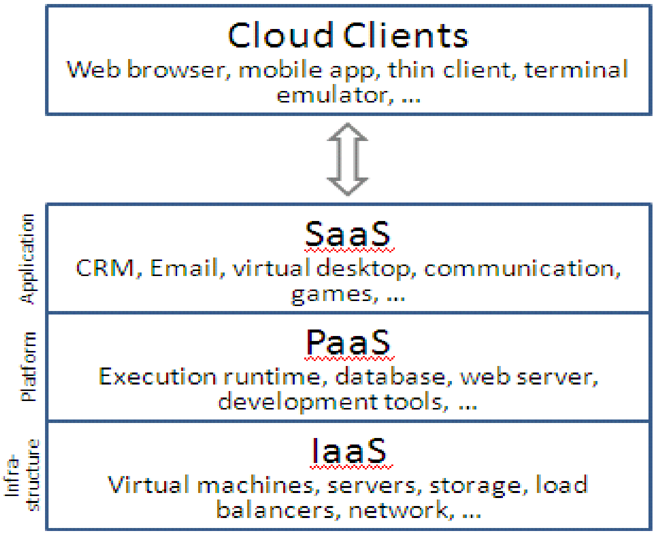
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig 2 Cloud Computing Services

II. Literature Survey

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 on the smart phone to detect any misbehaviour. In case misbehaviour is detected, the proposed engine decides upon and takes optimal response actions to thwart the ongoing attacks. Despite the computational and storage resource limitations in smart phone devices, the engine can perform a complete and in-depth analysis on the smart phone, since all the investigations are carried out on an emulated device in a cloud environment [1].

An approach which analyze the Android applications, providing a framework to distinguish between applications that, having the same name and version, behave differently. The aim is to detect behaviour anomalously behaving applications, thus detecting malware in the form of Trojan horses [3]. Another approach consists of a large set of smart phones that want to be protected from potential virus outbreak and a proxy that interacts with the smart phones through either cellular networks or IP-based Internet connections. Each smart phone runs a light-weight agent that logs the device activities, e.g., the usage of cellular SMS service and Bluetooth interface. These logs are periodically reported to the proxy. Upon receiving such reports from the smart phones, the proxy performs per-device viral behaviour analysis as well as aggregated system-wide viral behaviour analysis, and identifies each smart phone as either healthy or infected. When the viral activity has been verified, the proxy alerts the infected -smart phone users about the suspicious activities. In addition, the proxy also alerts other smart phone users that may immediately be vulnerable to infection attempts from those already infected devices [4].

In an architecture that consists of two primary components: a lightweight host agent that runs on mobile devices, acquires files, and sends them into the network for analysis; and a network service that receives files from the agent and identifies malicious or unwanted content. The proposed architecture could be deployed by a mobile service provider or third-party vendor. This approach is an extension of the existing CloudAV platform. In this they first provide background material on the fundamental CloudAV architecture and then discuss the extensions required to facilitate the approach in a mobile environment [5]. This hierarchical structure of Response and recovery Engine architecture (discussed later) makes it capable of handling very frequent IDS alerts, and choosing optimal response actions. Moreover, the two-layer architecture improves its scalability for large-scale computer networks, in which RRE is supposed to protect a large number of host computers against malicious attackers. Finally, separation of high- and low-level security issues significantly simplifies the accurate design of response engines [6].

III. SYSTEM DESIGN

To make a smart phone secure, a synchronized cloud-based intrusion detection and response framework for Smartphone devices was built. The main objectives are transparent operation to the users who are mostly technically unskilled, light resource requirement, and real-time and accurate intrusion detection and response. The framework involves the cloud environment which detects the intrusting and responses for the registered smart phones. It emulates the actual smart phone 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 Fig 3 shows the architecture of the framework and the connection between different components. In order to use the service, the smart phone has to be registered. The owner of the smart should register his/her mobile by giving the details such as the version of operating system, model number, and list of applications of the smart phone. This is necessary because it emulates the image of the smart phone at the cloud environment.

The user has to install a light weight software agent in to the smart phone which automatically configures the proxy settings.

A proxy server is responsible for duplicating the communication between the smart phone and the Internet and forwarding it to the emulation environment in cloud where the detection and forensics analyses are performed. Note that this does not disrupt the usual communication between the smart phone and the Internet. The light-weight agent on the smart phone performs three main tasks. It gathers 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., killing the malicious application, from the emulation environment in order to take the required actions. The real-time emulation environment is instrumented with several accurate off-the-shelf intrusion detection systems (IDSes), which currently cannot be deployed in smart phone devices due to their high resource requirements. The deployed set of detectors monitor different parts of the smart phone’s software stack and perform an online and in depth analysis to identify any malicious activity. In case misbehaviour is detected, our intrusion response engine [6] in the emulation environment solves a resource intensive game-theoretic optimization, and sends the selected optimal response action to the agent running on the smart phone device. The agent, then, can take the required actions and recover the smart phone back to its normal secure operational mode.

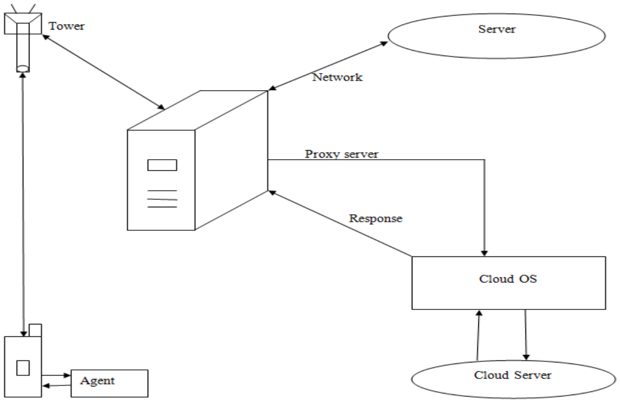

Fig3. High Level Architecture

IV. IMPLEMENTATION

Working prototypes of the intrusion forensics analysis engine for the Linux kernel was implemented, and are
Currently working on the emulation environment. At the user end a software agent is installed which automatically sets the proxy settings. The light-weight agent on the smart phone performs three main tasks. It gathers all user and sensor inputs to the device, it sends them to the emulation environment, and it waits for potential response and recovery commands. The proxy duplicates the traffic to the cloud server. This does not disrupt the usual communication between the smart phone and the Internet The cloud server creates an emulator environment to create the image of the user's smart phone. In order to make it performed the user has to do online registration by specifying the smart phone name and model. Whenever the user try to download a file the traffic will be redirected to the cloud and cloud starts detection for intrusion. If the cloud identifies any intrusion it sends a response to the smart phone.

V. 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.

VI. FUTURE ENHANCEMENT

A cloud based security to be provided the intrusion that affects the smart phone through Bluetooth and SMS/MMS.

The security to be provided to all smart phones. The registration can be made at the cloud end so that smart phone is secured from all services.Light weight resources can be utilized.

VII. REFERENCES

[1] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier A Cloud-based Intrusion Detection and Response System for Mobile Phones. *University of Illinois at Urbana-Champaign fahouman2, saliari2, rgbg@illinois.edu,2011*

[2] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang. Soundminer: A Stealthy and Context-Aware Sound Trojan for Smartphones. In *NDSS*, 2011.

[3] A. Boukerche and M. S. M. A. Notare. Behavior-based intrusion detection in mobile phone systems. *Jour. Paral.& Dist. Comp.*, 62(9):1476 – 1490, 2002.

[4] J. Cheng, S. H. Wong, H. Yang, and S. Lu. Smartsiren: virus detection and alert for smartphones. In *MobiSys*, pages 258–271, New York, NY, USA, 2007. ACM.

[5] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. Virtualized in-cloud security services for mobile devices. In *Proceedings of the First Workshop on Virtualization in Mobile Computing*, pages 31–35. Citeseer, 2008.

[6] S. A. Zonouz, H. Khurana, W. Sanders, and T. Yardley. Rre: A game-theoretic intrusion response and recovery engine. In *DSN*, pages 439 –448, 2009.

[7] 2010. Virus Library: http://www.viruslibrary.com/.