IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VI (May – Jun. 2015), PP 01-04
www.iosrjournals.org

Comparative Study on Intrusion Detection Systems for Smartphones

Supriya Kamble [1], Leena Ragha [2], Puja Padiya[3]
[1,2,3] *(Department of Computer Engineering, Ramrao Adik Institute of Technology, Navi Mumbai, India)*

Abstract: *Now-a-days the usage of Smartphone has been increasing greatly in recent years. Most of the people are de-pendent on Smartphone for all sort of activities such as checking mails, browsing internet, performing online transactions, surfing social networks, shopping online, paying bills etc. With so many advantages in Smartphone for users, the threats to user are also increasing. The threats are caused by creating malicious applications and game of which most of them are freely available to users on Google play. As the Smartphone have limited processing and computational power to execute highly complex algorithms for intrusion detection, virtual Smartphone images are created in cloud to prevent user from threats and vulnerabilities. In this paper we perform a comparative study on existing methods on intrusion detection system on cloud and on host devices for securing Smartphone. Cloud intrusion detection system is a better solution to achieve higher level of security. The paper discusses architectures of existing Intrusion detection system for Smartphone and their techniques*

Keywords: *Intrusion Detection System, Cloud Computing, Smartphones, Android Security.*

I. Introduction

Smartphones usage have been continuously growing in recent times with the advent of internet. Smartphones offer Personal Computer functionality to the end user and are vulnerable to the same sorts of security threats. Smartphone are extremely fast growing type of communication devices offering more advanced computing and connectivity functionalities than contemporary mobile phones [2]. With rapidly growing popularity more and more people and companies are using these devices making it more integrated and prevalent part of people daily lives [3].

People use their smartphone to keep their data, to browse the internet, to exchange messages, to check emails, to play games, to keep notes, online shopping, online banking, bill paying, to carry their personal files and documents, etc. Various models of smartphones have been released catering to the various demands of mobile users. A smartphone user needs to install and run third-party software applications. There are, lot of third party applications available in free of cost on Google Play and various other store website. Its easy availability encourages attackers to build malicious applications for such devices [1]. Being all-in-one device, the smartphones are increasingly getting attractive to a wide range of users [2]. With the advent of internet, the mobile network infrastructure quality and affordability consistently improved, thus usage of smart mobile phones for financial transactions, mobile learning and web browsing is becoming popular among users which causes several security issues [1].

With such an increasing popularity of the smartphones attacks threats are also increasing. Also as the device is coupled with the always on connectivity to the Internet that wireless networks allow, mobile technology is potentially vulnerable to increasing number of malicious threats Smartphones are more vulnerable to malware attacks, Trojans and viruses [10].

Distribution of applications is made easy for the developer by offering a central distribution market, where every developer can upload own applications, and the user simply downloads it in very few steps. Malicious application scan also get distributed in this manner, because only little security scanning, whether an application behaves malicious or benign, is applied. These facts show, that there is a high demand for solutions which increase the security of the devices. One approach to mitigate the limited capabilities of smartphones (e.g. processing power and battery capacity), is to off-load workload into the cloud. Taking advantage of the cloud is a very promising approach, since a service in the cloud can be modified as needed, whereas modifications to the smartphones are more difficult.

The rest of the paper is organized as follows. Section II presents the related work. Section III presents existing IDS framework for Smartphone. Section IV gives the detailed comparison and analysis of different IDS methods described in Section III by considering different parameters. Finally, Section V concludes the paper.

II. Literature Review

Khune and Thangakumar [1] proposed a cloud based intrusion detection and recovery system for Android smartphones. The framework performs in-depth forensics analysis and detect any malicious activity in network. The users of smartphone gets register to cloud-based services specifying relevant in-formation about the operating system, device, applications. A light-weight mobile agent on the user's smartphone. In the cloud environment intrusion detection and in-depth analysis is performed. The result of detail analysis and recovery methods are sent to the mobile host on the device to take necessary actions. An optimal protection and recovery is provided by the framework.

Halilovic et. al. [4] has proposed and developed a conceptual AmoxID model for android devices. The proposed model is generally useful for companies who needs to protect their company data. The proposed model enforces certain policy levels depending upon employees network locations i.e. Office Network, Home Network or Outdoor Networks. The employees smartphone is configured with pre-built IDS enforcing policies protecting access to company data on the phone. The model uses SVM classifications enforcing policies based on type of network the user is connect to categorizing threats on the devices.

Ghorbanian et. al. [5] proposed a host-based intrusion detection model. The model analyzes security of smartphone for android devices providing an active defense system for android security user. The application is developed in the area of smartphone security and analyzes the log file generating a response for intrusion. The proposed system detects attacks using pattern matching algorithm.

Shabtai A and Elovici Y [6] has proposed a light-weight, behavioral-based detection framework called Andromaly for Android smartphones based on Host-based Intrusion Detection System (HIDS). The detection system runs directly on the device, monitoring various features and events on the smartphone and classifies them as benign or malicious. Several combinations of classification algorithms and feature selections for evaluation and conclude that the proposed anomaly detection is feasible on Android devices.

Jacob [7] proposed cloud based intrusion detection and response engine, which performs an in-depth forensics analysis. An intrusion is detected using cloud service and if any corrupted file or misbehavior is detected, corresponding response actions are taken by the system to handle the threat. The system produces accurate intrusion detection and response.

III. Existing Ids For Smartphone

A. Security as a Service Based Anomaly IDS

In the paper [1] the author had proposed a cloud based IDS and recovery system for android. The proposed architecture uses the cloud services i.e., platform as a service and security as a service for performing intrusion detection. A lightweight mobile host is installed on the mobile device which inspects the file activity on the system. Firstly, the target device is registered on the cloud server application. The cloud server application deploys security methods such as emulator, memory scanners, system call anomaly detection and antivirus software. The mobile host generates a unique identifier of the file, which is compared against a cache of previous analyzed files and is sent to the in-cloud network analysis if the file is not present. After the analysis of file, the results are stored in both local cache on the mobile host agent and a shared remote cache in the cloud computing services. The proxy server acts as a mediator which mirrors the ongoing traffic between the mobile device and internet and sends it to cloud services for further analysis. It controls the access of devices to various applications and services.

B. Signature-Based HIDS

In [5] proposed system, the user has to authenticate to the system by creating an account. The log files from the device are fed to the system. The Log File Decoder Module changes the record into a defined format for system analysis and the result is send to the Detection Engine which compares the records with the rule-sets. In case of no matching item, natural action is done and the system goes to this next record to process. With the purpose of adapting the changing Internet and new intrusion behavior, the proposed system has Update Rule-set interface to update rule-set which is enable to detect.

C. AMOXID IDS

In [4] the author proposes a host based IDS named AmoxID for smartphones with a proof of concept. The model proposes categorization of threats into three main categories: 1-Threats to user's experience; 2-Cost generating threats; 3-Privacy in-fringing threats. Each category is analyzed separately and deals with three different subsystems in IDS for smartphones.

The model proposes system of policies depending on the user's current network, different policy levels is applied. To create the proof of concept the model is used in a company where employees are provided with a smartphone which require them to follow certain policy. If company sends confidential emails and give confidential data to employees that are accessed through smartphone, then it is important to protect this

information. Special designing policies are included in pre-built IDS enforcing various policies depending on the users current network. The features such as numbers of outgoing call, outgoing SMS, connection to GPRS are tracked using SVM classification.

D. Andromaly Framework

The paper [6] proposes a andromaly behavioral-based detection framework which realizes on HIDS monitoring various features and events from the device. Machine learning methods are applied to classify the collected data as normal or ab-normal. The framework evaluates games and tool applications effectively detecting application having similar behavior. The feature extractor collects various features from the device and pre-process the raw features. The processor performs analysis and generate output threats assessment which are given to the threat weighting unit. The threat weighting unit applies ensemble algorithms (such as Majority Voting, Distribution Summation etc.) to derive a final coherent decision regarding the infection level in device. The service agent is an important component which synchronizes feature collection, alert process and malware detection. The graphical user interface configures the agent's parameters, activate or deactivate, visual exploration and visual alerting of collected data.

E. Anomaly Based IDS

The paper [7] proposed a proactive defense mechanism in which the smartphone user is given the alert before downloading the file. The author created a web server where contents are entered. The properties of all the files are entered into a cloud server and also a string matching algorithm is entered into the cloud for comparison. The user first registers itself specifying the device OS and application lists, so an emulated image is created in cloud. The communication between the smartphone and the Internet is duplicated and forwarded to the emulator in cloud where the detection, forensics analyses are performed. 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 algorithm. If any unsecured file or misbehavior is detected, system takes the corresponding response actions to handle the threat. This system produces accurate intrusion detection and is scalable to any number of users.

IV. Table 1: Comparison & Analysis

Papers / Parameters	Cloud-Based IDS for Android Smartphone	Signature –Based Hybrid IDS for Android	Intrusion Detection on Smartphone	Applying Behavioral Detection on Android Device	Intrusion Detection on Cloud for Smartphone
Method	Anomaly Based	Signature Based	Rule Based	Anomaly based	Signature Based
Type of Detection	NIDS	HIDS	HIDS	HIDS	NIDS
Positioning	At Cloud	On Host	On Host	On Host	At Cloud
Service Used	SeaaS	-	-	-	SaaS
Analysis	Performs in –depth analysis and provides recovery	Active defense mechanism. Low false positive and negative	Provides optimal protection against threat	High true positive rate	Alerts for abnormal behavior
Scalable	Yes	No	Yes	No	Yes
Pros	-Provides optimal protection. -Parallel multiple detection engines provides good detection of attack	-Higher detection rate and accuracy -Update rule interface allows to detect modified attacks	-Analyzes threats at 3 levels i.e., threats to user experience, threat to generate cost, privacy infringement threats -Provides optimal protection	-Lower false alarm rate	-Proactive defense mechanism -Performs optimal response actions against abnormal behavior
Cons	-More false alarms as user and network behavior are not known beforehand	-Rule set needs to de updated	-Requires different policy rules for different levels of alert	-Requires large matching data set -Detection accuracy based on amount of calculated behavior or features	-Requires large data sets for accurate calculations

V. Conclusion

With the growing use of Smartphone, the number of attacks and threats are also on increase. It is necessary to provide security to end users from threats. In above section we have studied various existing IDS for smartphone each based on single type of IDS (Anomaly based IDS or Signature based IDS) which restricts the detection of attacks.

The main characteristic of signature based IDS is detection of incoming threats against a predefined knowledge base whereas in anomaly based IDS detects unexpected change in the system behavior from a normal behavior. In future, the combination of both anomaly and signature based IDS, the performance of attack detection can be increased thus preventing the smartphone from any malicious attack.

References

[1]. Rohit S. Thune, J. Thangakumar,"A Cloud-Based Intrusion Detection System for Android Smartphones,"
[2]. Radar, Communication and Computing (ICRCC), 2012 International Conference on, vol., no., pp.180-184, 21-22 Dec. 2012.
[3]. Amir Houmansadr, Saman A. Zonouz, and Robin Berthier,"A Cloud-based Intrusion Detection and Response System for Mobile Phones," Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on, vol., no., pp.31-32, 27-30 June 2011.
[4]. Dr.Marwan Omar, Dr. Maurice Dawson,"Reseach in Progress-Defending Android Smartphones from Malware Attacks," Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on, vol., no., pp.288-292, 6-7 April 2013.
[5]. Muhamed Halilovic, Abdulhamit Subasi, "Intrusion Detection on Smartphone".
[6]. Masoud Ghorbanian, Bharanidharan Shanmugam, Ganthan Narayansamy, Norbik Bashah Idris,"Signature-Based Hybrid Intrusion Detection System(HIDS) for Android Devices," Business Engineering and Industrial Applications Colloquium (BEIAC), 2013 IEEE, vol., no., pp.827-831, 7-9 April 2013.
[7]. Asaf Shabtai, Yuval Elovici,"Applying Behavioral Detection on Android-Based Devices," Mobile Wireless Middleware, Operating Sys-tems, and Applications, Springer, vol.48, no., pp.235-249, 2010.
[8]. Namita Jacob,"Intrusion Detection In Cloud for Smart Phones," IJREAT International Journal of Research in Engineering & Advanced Technology on, vol.1, no.1, pp., March 2013.
[9]. Han Bing,"Analysis and Research of System Security Based on An-droid." Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on, vol., no., pp.581-584, 12-14 Jan. 2012.
[10]. McAfee Threat Report: Second Quarter 2013: http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q2-2013.pdf
[11]. Jazilah Jamaluddin, Nikoletta Zotou, Reuben Edwads, Paul Coulton,"Mobile Phone Vulnerabilities: A New Generation of Malware," Consumer Electronics, 2004 IEEE International Symposium on, vol., no., pp.199-202, 1-3 Sept. 2004.
[12]. National Institute of Standards and Technology. The NIST definition of cloud computing: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, (retrieved at2012-05-10).
[13]. Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, Farnam Jahanian,"Virtualized In-Cloud Security Services For Mobile Devices," MobiVirt '08 Proceedings of the First Workshop on Virtualization in Mobile Computing on, vol., no., pp.31-35, 2008.
[14]. Hatem Hamed, Mahmoud Al-Hoby,"Managing Intrusion Detection as a Service in Cloud Networks," International Journal of Computer Applications on, vol.41 no.1, pp.35-40, March 2012.
[15]. Asaf Shabtai,"Malware Detection on Mobile Devices," Mobile Data Mangament (MDM), 2010 Eleventh International Conference on, vol., no., pp.289-290, 23-26 May 2010.