ISSN: 2278-0181

A Cloud Based Security Solution for Personal Computing Devices

Sahil Sakhala
Dept. of Computer Engineering
K.K.W.I.E.E.R
Nasik, India
sahils1210@gmail.com

Bhushan A.Ugale
Dept. Of Information Technology
M.C.O.E.R.C
Nashik,India
bhushan.ugale@gmail.com

Jigneshkumar H. Patel
Dept. Of Information Technology
TITS
Modasa,India
jignesh.dholu@gmail.com

***Abstract*— In today's era of pervasive computing where smart-phones and PC's are an integral part of one's life, malwares are used to invade their privacy and exploit the vulnerabilities of the system. With the dynamically changing styles of cyber threats, different cyber security solutions are proving to be ineffective. User needs to install different cyber security solutions on different systems. In this paper, we propose a cyber security mechanism, in which user will need to register and install lightweight host agent on all the devices which are to be protected. In turn, host agent will direct all the incoming traffic to cloud via proxy server which will not only detect any anomaly but also do vulnerability assessment and in-depth forensic analysis without the intervention from user. It overcomes the drawbacks of current cyber security solutions and hence proves to be cost effective and economic solution to prevent ones assets in cyber space.**

***Index Terms*— pervasive computing, host agent, forensic analysis, vulnerability assessment.**

I. Introduction

In today's hi-tech world, devices such as smart-phones and PC's are an integral part of one's life. They have penetrated in almost all aspects of our life. These devices offer more advanced computing and connectivity functionalities as compared to their contemporary models. With internet as backbone for, following their tremendous popularity, they are attracted by various types of cyber threats. Along with their increasing popularity, cyber threats too have grown tremendously, which if ignored can cause an massive destruction. Since smart-phones use the same software architecture as in PC's, they are vulnerable to similar classes of security risks such as viruses, trojans and worms [1,7].

The common solution which is mostly used by masses to counterfeit these obscure problems is an software which is popularly called as anti-virus. There comes variety of anti-viruses for different platform with different functionalities according to varying monetarily affordability. While a single antivirus engine may be able to detect many types of malware, but 0-day threats and other obfuscated attacks can result in vulnerabilities that are being exploited by malware. This paper suggests a new approach towards enhancing cyber security by using single solution and will consist of multiple, heterogeneous detection engines in parallel [6]. This approach provides several important benefits including better detection of malicious software, enhanced forensics capabilities and better resource management.

II. Need for Cyber Security

Both the devices, smart-phones as well as PC's are equally vulnerable to cyber threats. History is evidence, that large number of malwares have tried to exploit vulnerabilities in both devices and the new attacks are increasing in sophistication. The history of cyber attacks can be traced back to 1970's when "Creeper" worm and "The Reaper" showed up on ARPANET up-till today, when most deadly malware such as "stuxnet" created havoc [2]. More than thousands of malwares are detected each day and much more than that are created per day. If issue of cyber security not take seriously may result in financial loss. Hence, securing ones asset in cyber space is of utmost importance.

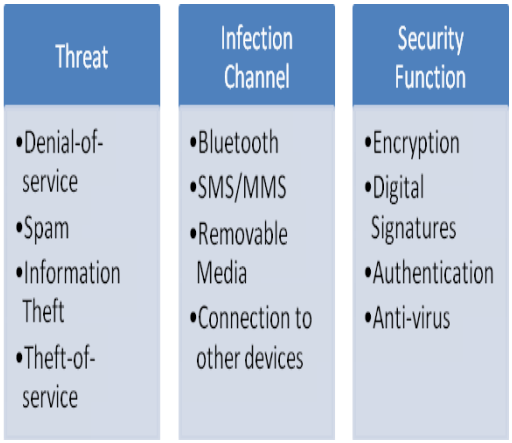

Fig. 1. Taxonomy of cyber security aspects

ISSN: 2278-0181

A. Taxonomy of cyber security aspects

The Figure 1 presents the most frequent types of threats and infection channels, as well as corresponding security functions.

1) Threats:

Denial-of-Service attacks are carried out by flooding with a large number of packets to the device to consume system resources.

Information theft occurs when hackers attack to obtain personal information which might be sensitive or confidential.

Theft-of-service occurs when malware uses smart-phone resources, for instance, to send expensive SMS messages.

Spam categorizes attacks where users are targeted involuntarily with advertising, messaging, and other similar information.

2) Infection Channels:

Bluetooth viruses may infect mobile devices. The Short Message Service (SMS) or Multimedia messaging service (MMS) can be used by smart-phone viruses to spread within networks.

3) Security Function:

Since the sensitive or valuable information is being increasingly stored and/or transmitted over the network, this data should be encrypted to ensure that the confidentiality of the information is not compromised.

III. CURRENT SECURITY SOLUTIONS AND IT'S DRAWBACKS

Whether it's a home desktop computer, college laptop, smart-phone or that terminal at your office, the use of a PC is part of life today. Anti-virus is one of the most widely used tool used by most of the people to defend their privacy in cyber space. To defend ones asset in cyber space, there are alternative solutions along with anti-virus available such as firewalls, intrusion detection system, rootkit detectors and many more. But as PC and smart-phone work on different platforms, separate executable files are required to be installed on both the devices. So a common security solution is available, but in two different ways, because of which user has to pay individually for security of each device.

Anti-virus can't function as much efficiently on smart-phones as it does on PC because limited storage, power and computational resources. Though anti-virus works well on PC, but it can considerably consume system resources and slow down PC to some extent. Morever, if two or more anti-virus are installed on same system, they may conflict [3,8]. To overcome such limitations, Cloud Computing provides plenty of software, processing power and services over internet. Comparatively it reduces bandwidth usage, processing power and energy consumption.

IV. CLOUD COMPUTING

Cloud computing has completely revolutionized the way of storing and accessing the data and the way we store and retrieve information and run applications. Cloud computing can be used by anyone without having any end-user knowledge which are storage, data access, security and software services. Cloud computing has emerged as a new computing paradigm providing hosted services by exploiting the concept of dynamically scalable and shared resources accessible over the internet [4].

V. PROPOSED SOLUTION

In our proposed model, we stress on decreasing cost and using resources optimally. The user has to register and install a light weight host agent on the device i.e. smart-phone or PC they want to be protected. The host agent will make an copy of the system after installation and preserve that copy in the cloud. In cloud, it will perform vulnerability assessment with the help of detection engine where multiple anti-virus will work simultaneously to detect any threat [9]. The usage of multiple detection engine increases its coverage detection, which can be seen from fig.2.

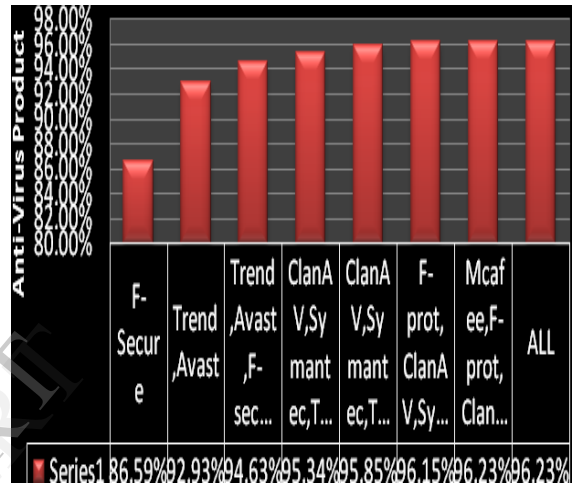

Fig. 2. Detection rate

If any anomaly is detected, it will notify user. This will be one of the key feature of our proposed model because in current security solutions, the product starts protecting device once it is installed, no matter in what condition the system is before its installation. After installation of host agent, if user tries to download any file from internet, the host-agent will redirect it to cloud.

Hence user can protect their devices using one single detection engine instead of purchasing different security solutions for PC and smart-phone. It will provide a layer over traditional network security appliances, giving user the ability to attempt to conduct predictive threat modeling. The user's threat modeling feature can identify the weak points likely to be targeted by an attacker.

While diverting the traffic to the cloud, proxy server will also function for detection of an anomaly in network. It will detect any malicious activity in the network and notify user before attack can actually occur and malware can propagate in the system, thus resisting theft-of-identity.

ISSN: 2278-0181

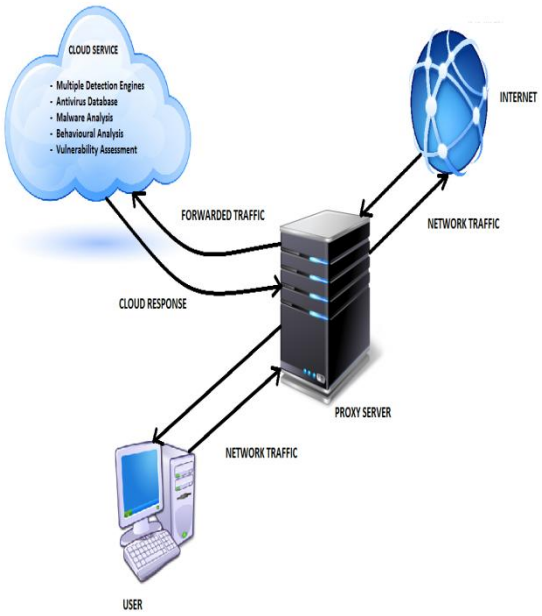

Fig. 3. System Architecture

VI. Conclusion

This paper presented an ideal way to optimize protection and in-depth forensic analysis of smart-phone and PC using host agent. The host agent clusters all user and sensor inputs to the device, it consigns them to the emulation environment, and it waits for emulation environment in order to take the required actions because of which end-user need not to have any knowledge regarding it. Hence it will prove to be an extremely cost sensitive approach and better utilization of system resources for anomaly detection in all personal computing devices.

References

[1] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier, "A Cloud-based Intrusion Detection and Response System for Mobile Phones," IEEE, 2011.

[2] https://sites.google.com/site/whymalwaresucks/part-a/some-famous-malware-and-a-brief-history

[3] http://www.ehow.com/list_7285310_disadvantages-antiviruses_.html.

[4] 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.

[5] S. Xiaonan and W. Wolfgang, "The Use of Computational Intelligence in Intrusion Detection SystemsP: A Review," Soft Computing, no. November, 2008.

[6] http://www.yuvaengineers.com/anomaly-detection-for-smart-phones-using-cloud-based-intrusion-detection-and-response-system-sahil-sakhala-kshitij-khakurdikar/

[7] 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.

[8] http://anti-virus-software-review.toptenreviews.com/mobile-phones-are-under-malware-attack.html/?cmpid=ttr-bnd

[9] S. Xiaonan and W. Wolfgang, "The Use of Computational Intelligence in Intrusion Detection SystemsP: A Review," Soft Computing, no. November, 2008.