Secure Hosts Using Operating System Intrusion Detection In Wireless Sensor Networks

Hannan Ansari, Wasim Khan, Faizan Ahmad

Dept. Of Computer Application, Integral University, Lucknow, India;
Dept. Of Computer Application, Integral University, Lucknow, India.
Dept. Of Computer Application, Integral University, Lucknow, India.
Email: hannan.ansari89@gmail.com, wasimkh@iul.ac.in,faizanahmad4715@rediffmail.com

ABSTRACT: As we know that we are living in Information World or we can say that we are living in Internet World. Now days we are all depend on Internet. It is very difficult for us that how we will secure our data, our system from Hackers, Intruders, Viruses, Worms and Some others Malicious activities. If we protect our Network, Hosts and O.S through any new technologies like IDSs then we can secure 90% transactions over the secure channel during Transmission of data on Internet. Due to these reasons I am focusing on a particular field that name is Operating System. You know that OS is a backbone of a particular system or Host. This Research paper is based on OS level Intrusion detection.

Keywords : WSNs; Computer Network; Advance Computer Network; IDSs; OS level Intrusion detection.

1 INTRODUCTION

INTRUSION DETECTION IS THE PROCESS OF IDENTIFYING AND RESPONDING to suspicious activities targeted at computing and communication resources. **An intrusion detection system** (IDS) monitors and collects data from a target system that should be protected, processes and correlates the gathered information, and initiates responses when evidence of an intrusion is detected. Depending on their source of input, IDSs can be classified into

- ✓ Network-Based IDSs
- ✓ Host-Based IDSs

[1.1] Network-Based Intrusion Detection System:

Network Based Intrusion Detection Systems collect input data by monitoring Network traffic (e.g., packets captured by network interfaces in promiscuous mode). Such type of IDSs is always worked on Network level. According to the users need NIDSs can develop. [1] The Architecture of NIDSs is given Bellow:

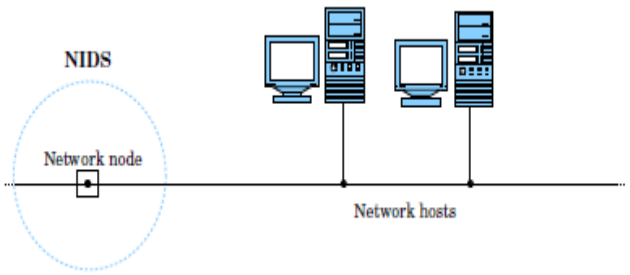

Figure-1: *Architecture of NIDSs*

[1.2] Host-Based Intrusion Detection System:

In Host Based Intrusion Detection Systems useful information always provided by O.S to identify the type's attacks at OS level. Such type of IDSs is always worked on Host level. According to the users need HIDSs can develop. [1]

The Architecture of HIDSs is given Bellow:

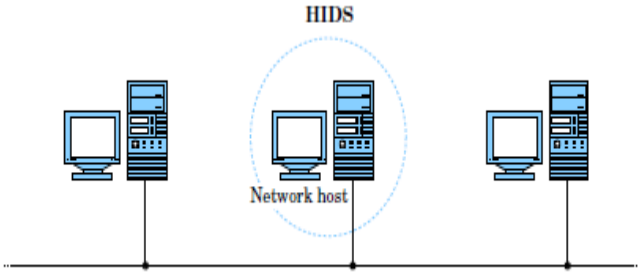

Figure-2: *The Architecture of HIDSs*

HIDS can be classified based on their type of audit data. We choose a characterization based audit data. According to audit data HIDSs can be classified into two fields'

- ✓ Operating System–Level Intrusion Detection Systems
- ✓ Application-Level Intrusion Detection Systems

For each fields we describe how audit data is gathered and also what types of techniques are used for its analysis. [1]

[1.3] OPERATING SYSTEM:

The term Operating System is main part of a particular Host or a System or Computer. In the other word we can say that OS is main part of Computer without OS we can't image about a system. The General Working Concept of OS is described below:

Operating System is nothing but it is Resource Manager; it acts between User and Computer Hardware. It takes the input from users and performs mathematical operation on them and then provides the desire output to the client. So if we are focusing on this field, if we do then we can find 90% to 95% secure transaction over internet.

[2] OPERATING SYSTEM–LEVEL INTRUSION DETECTION:

In Host Based Intrusion Detection Systems useful information always provided by OS to identify the type's attacks at OS level. And this useful information can be in different-different granularity and also level of abstraction. However, it usually belongs to low-level system operations such as System Calls, File System Modifications and User logons. Because of these operations show a low–level event stream and also they usually contain reliable information and difficult to tamper with unless the system is compromised at kernel level. Here the following, some OS level Auditing Data-gathering techniques are presented. Then different analysis methods that use this type of information are described.

[2.1] AUDIT DATA GATHERING:

Auditing is a new technique to collect information regarding the activity of users and applications. The OS is usually regarded as a trusted entity of a Host, because it is a resource manager, it controls access to resources, such as memory and files. Therefore several existing audit mechanisms are implemented within the OS. [1] OS audit data is not suitable for intrusion detection. Therefore in many cases, we see that the audit records produced by OS level auditing facilities, it contains irrelevant information and sometimes it provides lack of useful information. For the resultant, Intrusion Detection Systems has to access the OS directly to gather required data. [1][2] In past years, Several Researchers have worked on OS to identify what kind of information should be provided to "Intrusion Detection System" to be able to identify or detect intrusions effectively. For example, Lunt (1993) suggested the use of IDS-specific audit trails. Daniels and Spafford extended this initial idea and identified the audit data that OS needs to provide to support the detection of attacks against the transmission control protocol/Internet protocol (TCP/IP) stack (1999). [1] The availability of OS level auditing technique always depends on the only operating System. Now some examples are given here: Sun's OS (first SunOS and later Solaris) provide some auditing information by Basic Security Module (BSM). The BSM is a type of Kernel extension that's allows one to log events at the system call level. The different auditing levels are specified and, in addition to system calls, security-relevant higher-level events can be generated as well (e.g., login events). Auditing is always disabled by the root user, and making such type of facility vulnerable to abuse by an intruder, hacker and attacker who gains administrative privileges on the Host side. [1][3]

- **BSM** always produces audit records that are stored in audit files in a form of Binary format; the reason is that binary format always provides more space efficient. The main thing is that: the contents of an audit file will be available in human-readable format using The Praudit tool.

Thu Sep 10 23:01:29 2014 -> UID:root EUID:root RUID:root - From machine:log1 execve() + /usr/bin/sparcv7/ps + cmdline:ps,-ef + success

Thu Sep 10 23:01:50 2014 -> UID:root EUID:root RUID:root - From machine:log1 execve() + /usr/bin/tail + cmdline:tail,/etc/system + success

Thu Sep 10 23:11:18 2014 -> UID:root EUID:root RUID:root - From machine:log1 execve() + /usr/bin/pwd + cmdline:pwd + success

Thu Sep 10 23:11:20 2014 -> UID:root EUID:root RUID:root - From machine:log1 execve() + /usr/bin/ls + cmdline:ls,-l + success

Thu Sep 10 23:11:33 2014 -> UID:root EUID:root RUID:root - From machine:log1 execve() + /usr/bin/ls + cmdline:ls,-l + success

Figure 3: BSM Audit records.

- **SNARE** (System intrusion analysis and reporting environment): It wraps system calls in routines that gather the log information about process that always execute security relevant system calls. The other property of SNARE is it also supports simple pattern matching operations on the audit records produced, and these audit records can be used as a rudimentary form for Intrusion Detection.

- **LIDS** (Linux Intrusion Detection System): LIDS, According to its name, it is not an intrusion detection system but it also provides some additional features to its auditing capabilities. An access control layer that is complements and this access control layer always allow one to specify access for files, process and devices.[1][5]

[3] PROTECTION TECHNIQUE FOR OPERATING SYSTEM:

If we try to protect our Operating System through the Intrusion Detection then we have to know the Basic functionality of Operating System. It means that we must understand the architecture of Operating System. Operating system is nothing but it is a resource manager, without Operating System we cannot imagine about Computer. Inside the Operating System there are several components, among them a one term comes that's name is Kernel, as we know that Kernel is heart of Operating System. It works an intermediate entity between Computer Hardware and System calls. [6]

[3.1] MISUSE-BASED APPROACHES:

Misuse detection systems contain some number of sample attack descriptions and that description are able to identify or able to match against the stream of audit data and then compare to look for evidence that one of the modeled attack is accruing. It usually provides an attack language that is used to description the attacks that have to be detected and these languages provide mechanisms and abstractions for identifying the manifestation of an attack. The suitable example of detection languages for host based intrusion detection Systems are P-Best. [1][4][3]

[3.2] ANOMALY-BASED APPROACHES:

Anomaly Based techniques follow such type of approach that is complementary to misuse-based approach. In anomaly based approach, the detection is based on models of normal behavior of users and applications, and these users and applications are called profiles. Any deviations from established profiles are interpreted as attacks. [4][3] The main advantage of this approach is that it is able to identify previously unknown attacks. By defining an expected, normal behavior, any abnormal action can be detected, whether it is part of the threat

model or not. The advantage of being able to detect previously unknown attacks is usually paid for with a high number of false positives. [1][5]

[4] ATTACKS IN WIRELESS SENSOR NETWORKs:

According to security point of view security vulnerability is major problem in Wireless Sensor Network, An adversary or malicious activities can perform harmful steps for a single host or whole network. Due to these reasons the term attacks categorize into two fields: active attacks and passive attacks. Further both attacks categorize into several fields. [8]

[4.1] ACTIVE ATTACKS:

In this type of attacks an adversary or malicious activities can perform harmful steps for single host or complete network.it changes the system resources or effect their operations. In this attack some terms come that name is: masquerade, replay, modification of message and denial of service, these are the type of active attacks. [8]

[4.2] PASSIVE ATTACKS:

In this type of attacks, a user can attempt to learn or make use of information from the system but doesn't affect the system resources. It means such type of attacks is always fruitful for systems as well as users. In these categories there are two types of attacks come that's name is: release of the message Contents and Traffic attack analysis. [1][8] Through both type of attacks a user can understand in a better way that which type of attack is happening on given system or network and if we know that the type of attack then the job of security precise for a host or network. It means that we will only focus on given types of attacks and related solutions. [8][1]

[5] THE MAJOR ROLE OF OPERATING SYSTEM LEVEL INTRUSION DETECTION IN WIRELESS SENSOR NETWORK:

Wireless Sensor Network is also type of network, which has light weight, low coast, small memory size, limited power and energies supply. It is nothing but it is a simple network which has limited nodes, and these nodes are connected with each other. It is worked like ordinary network with simple and precise protocols. [8] It is a very difficult to manage a single host or network which is based on wireless sensor networks. Microsoft Windows also gives an auditing system that can be leveraged to perform host based intrusion detection. According to auditing system it produces three event logs, namely: the system log, the security log and the application log. [1] If we apply an OS level Intrusion Detection on a host or on a network then we will find that given host or network is more secure and accessible for their clients. [8][1]

[6] CONCLUSION:

For security purpose an intrusion detection system plays a big role in area of Computer network. When we talk about OS level intrusion detection system it provides some reliable way to protect a system or host or a network. It means OS level intrusion detection system is suitable for a particular computer or Host. In this paper we focused the thought of security that how we will secure the particular host using OS level intrusion detection system in wireless sensor network.

REFERENCES

[1] Vigna, Giovanni, and Christopher Kruegel. *Host-based intrusion detection*. na, 2006.

[2] Rahmatian, Mehryar, et al. "Hardware-Assisted Detection of Malicious Software in Embedded Systems." *Embedded Systems Letters, IEEE* 4.4 (2012): 94-97.

[3] Mirza, Muhammad Bilal, et al. "Malicious Software Detection, Protection & Recovery Methods: A Survey."

[4] Ying, Lin, Zhang Yan, and Ou Yang-jia. "The design and implementation of host-based intrusion detection system." *Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on*. IEEE, 2010.

[5] Bazzi, Ahmad, and Yoshikuni Onozato. "IDS for detecting malicious non-executable files using dynamic analysis." *Network Operations and Management Symposium (APNOMS), 2013 15th Asia-Pacific*. IEEE, 2013.

[6] Ansari, Alam, Arijit Chattopadhayay, and Suvrojit Das. "A kernel level vfs logger for building efficient file system intrusion detection system." *Computer and Network Technology (ICCNT), 2010 Second International Conference on*. IEEE, 2010.

[7] Sa-ngounwong, Sathaporn, and Pornsiri Muenchaisri. "Runtime Detection of Software Modification Using RSCA Method." *International Proceedings of Computer Science & Information Technology* 39 (2012).

[8] Ansari, Hannan, Sachin Kumar Patel, and Sachida Nanda Barik. "Survey on Wireless Sensor Networks." (2014).