JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Analysis of Embedded Network Security by Intrusion Detection System

Dr.P.Rajapandian* MCA. M.Phil, .Ph.D.

Associate Professor at Madurai Kamaraj University College

Department of Computer Science

Tamilnadu, India

Abstract

Network Security has traditionally been a subject of intensive research in the area of computing and networking. However, security of embedded systems is often ignored during the design and development period of the product, thus leaving many devices vulnerable to attacks. The growing number of embedded systems today (mobile phones, pay-tv devices, household appliances, home automation products, industrial monitoring, control systems, etc.) is subjected to an increasing number of threats as the hacker community is starting to pay attention to these systems. On the other hand, the implementation of security measures is not easy due to the constraints on resources of this kind of devices. . An Embedded network consists of several devices connected together to form a computing environment. In order to make security in embedded network, the connected device has to be secured In this paper, the embedded device network security is analyzed with the help of Intrusion detection System (IDS) method to secure the embedded network from the attacks.

Key words: *Network Security, IDS, Embedded System.*

1. Introduction

Intrusion detection is defined as the process of observing the events occurring in a computer system or network and analyzing the violations or imminent threats of security policies or standard security practices violation. These violations may be caused by malware such as worms, spyware, virus, unauthorized access to the systems by some attacker, and authorized users misusing their privileges or flaws resulting in granting the attacker an elevated access to the network. An Intrusion Detection System (IDS) is software used for the automation of intrusion detection process. IDS monitor network or system events for malicious activities that tend to compromise the confidentiality, integrity, and availability of network and send a report to the management station. Intrusion detection refers to the process of monitoring the events happening in a computer system or network, examining them for signs of security problems. The general meaning of intrusion detection reminds the analogous monitoring systems in other areas, including burglar alarms and video-monitoring systems found in banks and other renowned stores. Even the warning systems in civil defense and military fall into this functional category. Although the strategies employed are different in the various monitoring systems, yet the basic idea remains the same. The intrusion detection is defined as a process of detecting and responding to malicious activity directed at computing and networkingresources. An IDS gathers and analyses the information within a network or a computer to perceive possible security fissures, which includes both attacks from outside the organization and within the organization. It usesa technology, known as vulnerability assessment or scanning, for assessing the security of a computer or a network. The intrusion detection system procures data about information system to perform the analysis on the security status of that system. The foremost goal of IDS is to detect the security breaches, including both attempted breaches and potential breaches. Simple typical IDS.

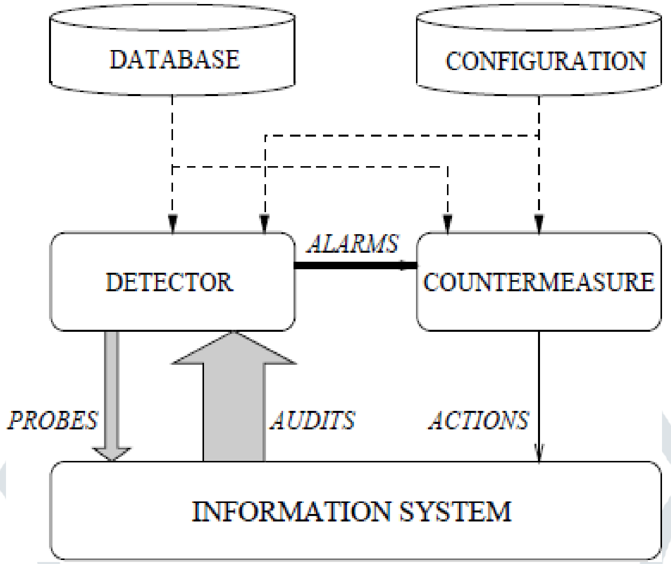

Figure 1: Intrusion detection System

The IDS items can bein the form of packets, audit records of system, computed hash values or other data formats. Analyzers receive input from sensors and then determine the intrusive activity.

The efficiency of an intrusion detection system depends on the following parameters

- **Accuracy:** It deals with the proper discovery of attacks and the non-occurrence of false alarms.
- **Performance:** It is the rate at which audit events are processed.
- **Completeness:** It is the property of an intrusion detection system to identify all attacks.
- **Fault Tolerance:** An intrusion detection system needsto be resilient to attacks, especially denial-of-serviceattacks.

An intrusion detection system has to accomplish and succeed its analysis as quickly as possible in order to empower the security administrator to respond before much damage has been done, and alsoto inhibit the attacker from subverting the audit source or the IDS itself.

IDS automate the intrusion detection can be classified are false positives and false negatives. False positives are those sequences of innocuous events that IDS speciously classifies as intrusive, while false negatives refer to intrusion attempts that IDS fails to report. Detection of hostile attacks depends on both the number and type of suitable actions. Figure.2 describes the series of activities performed by an intrusion detection system.

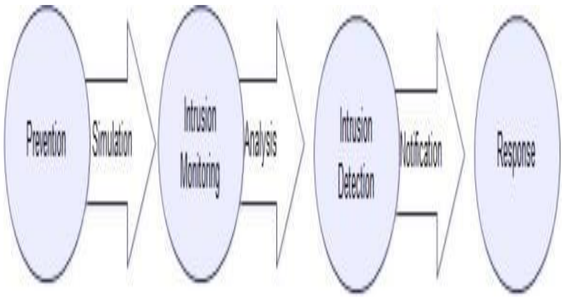

Figure 2: IDS Activities

IDS can be categorized into various types, on the basis of different monitoring and analysis approaches. IDS can monitor events at three levels.

Network-Network-based IDS (NIDS), presently the most common commercial product offering, detect attacks by capturing and analyzing the packets that navigate in a given network link. NIDS consists of a set of single purpose hosts that sniff the network traffic and report the attacks to a single management console. NIDS is secured against attack as no other applications run on hosts are used by it. These NIDSs have "stealth" modes which make it almost impossible for an attacker to detect their presence. NIDS monitors the characteristics of network data and performs the intrusion detection. Most NIDS operate by examining the IP and transport layer headers of discrete packets, the contents of packets, or some other combination.

a) Host- Host-based Intrusion Detection System (HIDS) refers to the class of IDS that resides on a host machine and monitor it. The analysis of activities on the host is done at very fine granularity to determine precisely which processes and users are performing malicious activities on the operating system.

b) Application- Application-based IDS monitor the events transpiring within an application. This IDS detects attacks by analyzing the application's log files. Application-based IDSs are likely to have a fine-grained view of suspicious activity in the application by interfacing with an application directly and having significant application knowledge.

c) IDS can analyze these events using,

d) Signature Detection- Signature-based IDS centers around the usage of expert system to identify the intrusions based on a predetermined knowledge base. It can be used to detect each known attack if properly programmed. This technique is an effective method usedin commercial products for detecting attacks.

e) Anomaly Detection-Anomaly-based IDS finds an attack by identifying the anomalous (i.e. unusual) behavior on a host or a network. The functionality of anomaly based IDS is based on the logic that some attackers behave differently than normal users and hence the attacks can be easily detected by the systems that identify these differences. These systems may generate an overwhelming number of false alarms since the variation of normal user and network behavior can vary haphazardly. Anomaly-based IDS can be used to detect the never-before-seen attacks.

f) Types of Intrusion System: The different types of Intrusion detection systems

- Host based IDS
- Network based IDS
- Application based IDS

Host based IDS views the sign of intrusion in the local system. For analysis they use host system's logging and other information. Host based handler is referred as sensor. Other sources, from which a host-based sensor can obtain data, include system logs and other logs generated by operating system processes and contents of objects not reflected in standard operating system audit and logging mechanisms.Host based system trust strongly on audit trail. The information allows the intrusion detection system to spot subtle patterns of misuse that would not be visible at a higher level of abstraction. The elementary principle in IDS includingNetwork Based Intrusion Detection System (NIDS) originated from anomaly HIDS paper based on Denning's pioneering work.

A host-based IDS provides much more relevantinformation than Network-based IDS. HIDS are used efficiently for analyzing the network attacks, for example, it can sometimes tell exactly what the attacker did, which commands he used, what files he opened, rather than just a vague accusation and there is an attempt to execute a dangerous command. It is less risky to configure.

Advantages of Host based Intrusion Detection Systems:

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Does not require additional hardware
- Lower entry cost

Network based IDS systems collect information from the network itself rather than from each separate host. The NIDS audits the network attacks while packets moving across the network. The network sensors come equipped with attack signatures that are rules on what will constitute an attack and most network-based systems allow advanced users to define their own signatures. Attack on the sensor is based on signature and they are from the previous attacks and the operation of the monitors will be transparent to the users and this is also significant.The transparency of the monitors decreases the likelihood that an adversary will be able to locate it and nullify its capabilities without the efforts. Network Node IDS (NNIDS) agents are deployed on every host within the network being protected.

Advantages of Network based Intrusion Detection Systems:

- Lower Cost of Ownership
- Easier to deploy
- Detect network based attacks
- Retaining evidence
- Real Time detection and quick response.
- Detection of failed attacks

Application based IDS (APIDS) will check the effective behavior and event of the protocol. The system or agent is placed between a process and group of servers that monitors and analyzes the application protocol between devices. Intentional attacks are the malignant attacks carried out by disgruntled employees to cause harm to the
organization and Unintentional attacks causes financial damage to the organization by deleting the important data file. There are numerous attacks have taken place in OSI layer

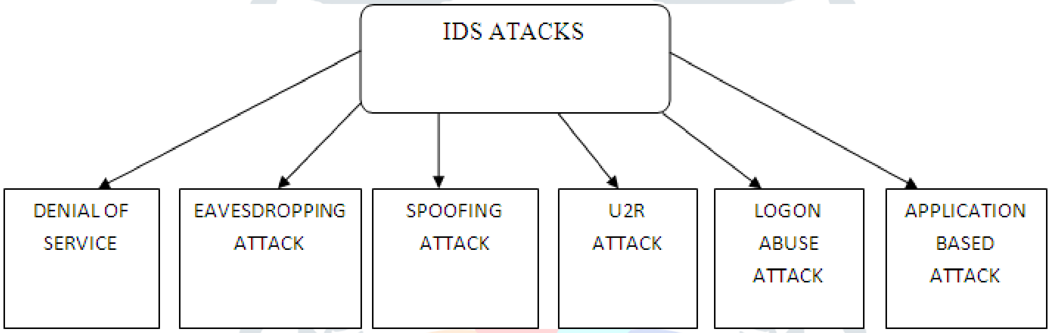

Figure 3: Intrusion Detection Attacks

Denial-of-Service (DOS) Attacks: It tries to deny the authorized users from promoting the requested service. An advanced Distributed Denial of Service occurs in a distributed environment that the attacker sends or floods the server with numerous connection that request to knock the target system .
Eavesdropping Attacks: It is the scheme of interference in communication by the attacker. This attack can be done over by telephone lines or through email.
Spoofing Attacks: This attacker portrays as another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker.
Intrusion attacks or User to Root Attack (U2R): An intruder tries to access the system or route through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle which leads to loss of data.
Logon Abuse Attacks: A logon abuse attack would neglect the authentication and access control mechanisms and grant a user with more advantages.
Application-Level Attacks: The attacker targets the disabilities of application layer. For example, security weakness in the web server or in faulty controls on the server side.

2) Functions if IDS

The IDS consist of four key functions namely, data collection, feature selection, analysis and action.

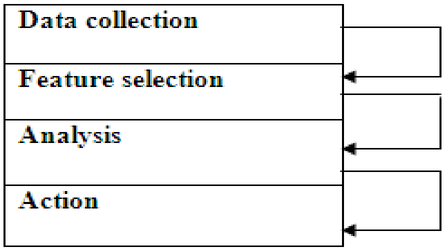

Figure4. Functionality of IDS

Data collection: This module passes the data as input to the IDS. The data is recorded into a file and then it is analyzed. Network based IDS collects and alters the data packets and in host based IDS collects details like usage of the disk and processes of the system.

Feature Selection: To select the particular feature large data is available in the network and they are usually evaluated for intrusion. For example, the Internet Protocol (IP) address of the source and target system, protocol type, header length and size could be taken as a key for intrusion.

Analysis: The data is analyzed to find the correctness. Rule based IDS analyze the data where the incoming traffic is checked against predefined signature or pattern . Another method is anomaly based IDS where the system behavior is studied and mathematical models are employed to it.

Action: It defines about the attack and reaction of the system. It can either inform the system administrator with all the required data through email/alarm icons or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports

3. IDS Life Cycle

Vendors frequently release new IDS products aggressively and compete for market shares. Estimating the new systems is not a relevant task and product calculation information is imperfect. Hiring and retaining the workers to administer security and intrusion detection are the challenging tasks. Faster changes in IT make it problematic for the firm to implement long- term security strategy

Evaluation and Selection: If an organization plans to get IDS it should examine the resources available for the systems operation and maintenance. Lifecycle of a product for economic IDS is accelerated. The third-party evaluation is available and their reports are generally on the surface . This process illustrates about the finding of the intruder and the amount of work required for maintaining the system in the network with traffic and the selection process defines about the identification of character, approaches, accuracy, usability, and effectiveness.

Deployment: Deployment phase includes the working of sensors to maximize protection for the critical assets by configuring the IDS to reflect security policy and installing signatures . Users must develop rules for handling the alerts and to associate alerts with other systems. The Intrusion Detection Working Group of the Internet Engineering Task Force (IETF) is developing common alert format that uses the IDS to alert from different systems and they are reported to a common display console.

Operation and use: Organization administers the IDS to monitor the host and to respond the report as an alert. It establishes the roles and responsibilities for analyzing and monitoring the outcomes of both manual and automatic responses. Smart intruders who realize that IDS has been deployed on a network attack that they force it to provide false report.

Maintenance: Maintenance includes installation of signatures and IDS upgrades. Sensor placement should be revisited periodically to ensure that system or network changes. An organization mustattract, train and retain qualified technical staff to operate and maintain IDS technologies.

4. Attacks on Embedded System

It is possible to classify the attacks based on their final goal, functional objective and on the method used to execute them. Our classification is based on of attacks. At the top level, attacks are classified into four main categories based on the final goal of the attack. Cloning, Theft-of-Service, Spoofing and Feature unlocking.The second level of classification is the functional objective of the attack. Here we would distinguish between attacks against privacy (the goal of these attacks will be gaining knowledge of sensitive information manipulated, stored or communicated by an embedded system); attacks against integrity (these attacks will try to change data or code within an embedded system); attacks against availability (a.k.a “Denial of Service”attack, these attacks disrupt the normal operation of the system).The third level of classification is based on the method used to execute the attack. These methods are grouped into three categories. Physical attacks, Side-channel attacks and software attacks.

5. Security Issues in Embedded System

A system is secure if it could be used only for the purpose for which it is intended and only by the prescribed and authorized user and is available to provide service at any time. This statement is also true for embedded systems in general. Before we discuss the types of attacks and security issues, it is imperative to understand the lifecycle and design and development methodologies related to hardware devices and embedded systems. Hardware devices and embedded systems can be implemented in a number of ways depending upon the application of the particular system under development.

6. Conclusion and Future Work

The main objective of this paper is to provide an overview of the necessity and utility of intrusion detection system on embedded network. The IDS is becoming essential for day today security for network user. There is a lack of security on present embedded systems. Security is not usually taken into account during the design phase of the product and it is difficult to implement once the product is completed. Even in those cases where security has been a concern from the beginning, the developer must face important hardware constraints to include security measures. Security should be integrated into the product during the conceptual design phase and should be taken into account for every part of the design.

There is an increasing number of security threats over embedded systems and various hacker attacks that jeopardise the commercial viability of new products or that can endanger the correct operation of existing ones. As 100% security does not exists an attacker having enough time, resources and motivation could always break into any system. For this reason, manufacturers must secure their products against specific threats trying to achieve a balance between the cost of security implementation and the benefits obtained.

However the implementation of security measures is not enough. It is also necessary to verify the effectiveness of these measures and even check for gaps or hidden threats. The product must be regularly monitored and updated in order to have the greatest effect possible against attacks. To accomplish this definition of new security evaluation methodologies that take into consideration the changing nature of security and will assure that the product will remain secure is necessary.

Reference

[1]. Maqbool BB, Bashir U, Chahcoo M. "Intrusion Detection and Prevention System: Issues andChallenges. International Journal of Computer Applications. 2013; 76.17.

[2]. Mukherjee, Biswanath L, Heberlein T, Levitt KN.Network intrusion detection. IEEE network. 1994;8(3): 26-41.

[3]. Corinne Lawrence- “IPS – The Future of Intrusion Detection”- University of Auckland - 26th October 2004.

[4]. Karthikeyan .K.R and A. Indra- “Intrusion Detection Tools and Techniques a Survey”

[5]. “Intrusion Detection and Intrusion Prevention”-Ed Sale VP of Security Pivot Group, LLC

[6] Weingart, S. 2000. Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses.*Workshop on Cryptografic Hardware and Embedded Systems*.

[7]Kuhn, M. 1997. *The TrustNo1 Cryptoprocessor Concept*. CS555 Report, Purdue University.Kommerling, O., Kuhn, M. 1999. Design principles for tamper resistant smartcards processors. In proceedings USENIX Workshop on Smartcard Technology

[8]. Wenke Lee ,Salvatore J. Stolfo “Adaptive Intrusion Detection: aData Mining Approach” 2000

[9]. Tao Peng, Wanli Zuo “Data Mining for Network Intrusion Detection System in Real Time” IJCSNS International Journal ofComputer Science and Network Security, VOL.6 No.2B, February2006

[10]. Anazida Zainal, Mohd Aizaini Maarof and Siti Mariyam Shamsuddin “Data Reduction and Ensemble Classifiers in Intrusion Detection” in 2008IEEE.