HBRO: HYBRID BRO SYSTEM FOR INTRUSION DETECTION IN WIRELESS ENVIRONMENT

Divya*

Tanvi Gupta*

ABSTRACT

In this paper a hybrid BRO system is proposed for network security in wireless environment. Intrusion detection system architecture we followed mechanism to build a four level hierarchical network which enhances network scalability and use both anomaly and signature detection techniques for intrusion detection. There is a brief overview of ids, its type and bro system is given. Wireless Sensor Networks (WSNs) are a new technology foreseen to be used increasingly in the near future due to their data acquisition and data processing abilities. Security for WSNs is an area that needs to be considered in order to protect the functionality of these networks, the data they convey and the location of their members. The purpose of this paper is to describe some new ideas in intrusion detection.

Keywords: *IDS, HBRO, Anomaly detection.*

*Lingaya's university, Faridabad, India.

1. INTRODUCTION

Intrusion: An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. An intrusion takes place when an attacker or group of attackers exploit security vulnerabilities and thus violate the CIA guarantees of a system.

Intrusion detection: It is the process of detecting attempts to gain unauthorized access to a network or to create network degradation.

Intrusion detection system**:** Look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. There are some Intrusion Detection Systems that are proposed or designed for Wireless Ad hoc network. Intrusion detection systems, also known as IDSs. An IDS is an important part of modern network security. Intrusion detection is the monitoring of a computer network with the goal of detecting an attack.

There are two major types of IDSs- Host based IDSs and Network-based IDSs

Characteristics of Intrusion Detection Systems: In order to satisfy its functions, the ideal intrusion detection system should have the following characteristics:

Timeliness: It should detect intrusions either while they are happening or shortly afterwards.

High probability of detection: It should recognize all or most intrusions.

Low false-alarm rate: It should have a low number of false intrusion alarms.

Specificity: In identifying attacks, it should give sufficient characterization data to support an effective response.

Scalability: It should be applicable to large networks.

Low a priori information: It should require a minimum of a priori information about potential attackers and their methods.

2. BASIC TYPES:

2.1 Host based: The host operating system or the application logs in the audit information. These audit information includes events like the use of identification and authentication mechanisms, file opens and program executions, admin activities etc. This audit is then analyzed to detect trails of intrusion.

2.2 Network-Based IDS Systems

Network-based IDS monitors traffic by capturing and analyzing network packets. Advantages: (i) the deployment of these systems has little impact on the existing network; (ii) little effect on the normal network operation and are relatively easy to upgrade, and (iii) robust in the face of attacks and can be made invisible to attackers.(iv) Cost of ownership

reduced. Disadvantages : (i) during peak-traffic periods some packets may go unprocessed and attacks undetected; (ii) encrypted information cannot be analyzed; (iii) attack attempts may be detected but hosts must usually then be investigated manually to determine whether or not they were penetrated and damage caused (iv) attacks involving fragmentation of packets can cause these IDS to crash.

3. DETECTION TECHNIQUES:

3.1 Anomaly-Based Detection

Anomaly detection identifies abnormal behavior. It requires the prior construction of profiles for normal behavior of users, hosts or networks; therefore, historical data are collected over a period of normal operation. IDSs monitor current event data and use a variety of measures to distinguish between abnormal and normal activities. These systems are prone to false alarms, since user's behavior may be inconsistent and threshold levels will remain difficult to fine tune. It is essential that normal data used for characterization are free from attacks. Anomaly detection refers to an approach where a system is trained to learn the “normal behavior” of a network. An alarm is raised when the network is observed to deviate from this learned definition of normality. This type of system is theoretically capable of detecting unknown attacks, overcoming a clear limitation of the misuse approach.

3.2 Signature based IDS:

Signature based approach of misuse detection works just similar to the existing anti-virus software. In this approach the semantic characteristics of an attack is analyzed and details is used to form attack signatures. The attack signatures are formed in such a way that they can be searched using information in audit data logs produced by computer systems. A database of attack signatures is built based on well defined known attacks and the detection engine of an ID compares string log data or audit data against the database to detect attack. Each time a new attack is discovered, the attack signature database has to be quickly updated accordingly for more up-to-date result and accuracy. There are various signature matching algorithms used in various signature based cyber attack detection systems. ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets, as an attack. Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply look for a sub string within a stream of data carried by network packets. When it finds this sub string, it identifies those network packets as vehicles of an attack.

4. TYPES OF ATTACKS:

All sorts of network attacks can be clubbed together into major categories:

4.1. **Denial of Service Attacks**. This category of network attacks disables server operations by overwhelming the host with "trash" packets or by sending so much traffic that the host cannot service "real" requests.

4.2. **Application Attacks.** Many popular server applications experience attacks designed to take advantage of a specific flaw in their protocol or access methods.

4.3. **Trojans Horse Attacks**. Another type of application attack of growing concern is based on "hidden code," commonly called a Trojan Horse, which allows remote access to the infected host. Back Orifice 2000 and NetBus are two examples of grave concern to NT/2000 system administrators these days.

4.4 **Password Attacks.** These attacks comprise network sniffing and brute force attacks. Network sniffing concentrates on two areas:

Acquiring clear-text passwords (the situation when Windows systems exchange passwords with any non-Windows operating system, such as UNIX or Novell) via network capture or file infiltration.

Grabbing the encrypted value of an NT system password from a network packet or the password file and trying to decrypt the packet or file to expose the passwords that would allow a valid login to the host. Password attacks cannot be stopped by a packet-filtering firewall, but can be greatly reduced. Network access controls manage the network protocols and addresses allowed to pass through the firewall, providing a more definitive sense of control over where a password attack can originate.

Time-based security policies further define network access to the target system by allowing only specific transactions to take place at particular times of the day. And,

Connection logging allows for accurate and timely recording of all traffic activity. These are the types of firewall facilities you need to protect against Password attacks.

4.5. **URL Based Attacks**. These attacks are initiated by exploiting the vulnerabilities in many web servers and web-based applications that allow malicious code to be included as part of a URL. These attacks can result in denial-of-service, unauthorized file access or remote machine compromise.

5. EXISTING BRO SYSTEM

Bro is used by sites requiring flexible, highly customizable intrusion detection. It is currently developed for six Internet applications: FTP, Finger, Portmapper, Ident, Telnet and Rlogin.

Bro is a powerful, but largely unknown open source network intrusion detection system. Bro was originally written by Vern Paxson at Lawrence Berkeley National Lab and the International Computer Science Institute. Bro is an open- source , Unix-based Network Intrusion Detection System (NIDS) that monitors network traffic looking for suspicious activity. Bro detects intrusions by first parsing network traffic to extract is application-level semantics and then executing event oriented analyzers that compare the activity with patterns deemed troublesome. It is important to understand that Bro was initially developed as a research platform for intrusion detection and traffic analysis.

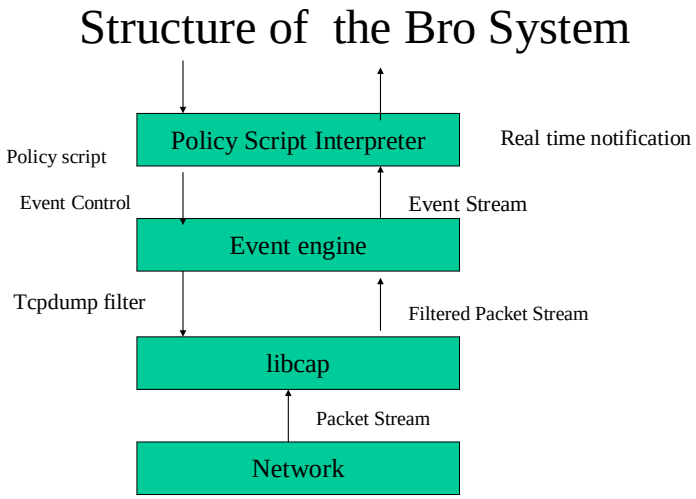

Fig1: Intrusion detection by Arun hodigere

Design goals for Bro:

- High-speed, large volume monitoring
- No packet filter drops
- Real time notification
- Mechanism separate from policy
- Extensible
- Monitor will be attacked

6. HBRO ARCHITECTURE:

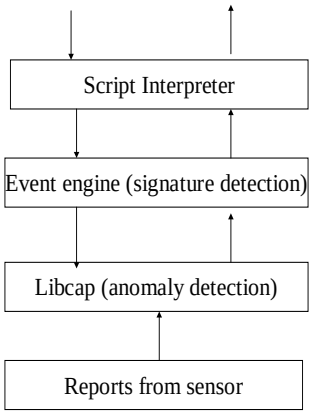

Fig2: HBro architecture

Reports from sensor: It collects the network traffic of the leaf level sensor when it acts as an LPA or it receives reports from lower layer IDA. Collected sensor traffic data is then abstracted to a set of variables called stimulus vector to make the network status understandable to the higher layer processor of the agent. These are deployed in a network or on a device to collect data. They take input from various sources, including network packets, log files, and system call traces. Input is collected, organized,and then forwarded to one or more analyzers.

Libcap/anomaly: It's the packet capture library used by tcpdump. Isolates Bro from details of the network link technology. It filters the incoming packet stream from the network to extract the required packets**.** It analyzes the vector from the sensors to detect anomaly in network traffic. Usually statistical method or artificial intelligence is used in order to detect this kind of attack. Profile of normal activity which is propagated from Base station is stored in the database.

Event engine/ signature: The filtered packet stream from the libcap is handed over to the Event Engine. It performs several integrity checks to assure that the packet headers are well formed. It looks up the connection state associated with the tuple of the two IP addresses and the two TCP or UDP port numbers**.** It maintains a database called Signature Record of the typical known unauthorized malicious threats and high risk activities and compares the reports from the preprocessor against the known attack signatures. If match is not found then

misuse intrusion is supposed to be detected and signature processor passes the relevant data to the next higher layer for further processing.

Script interpreter: It sends reports for the higher layer agent or base station. It can be used to display the agent status through a user interface. It then executes scripts written in the Bro language which generates events like logging real-time notifications, recording data to disk or modifying internal state.

Operation for detection:

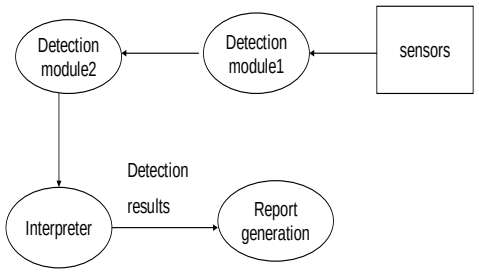

Fig3: shows the operation of detection.

7. CONCLUSION

A hybrid intrusion detection system is a part of the defensive operations that complements the defenses such as firewalls. They help in detecting attacks and other security violations. It doesn't compensate for bad security. These are a highly flexible security tool that can be used in a variety of different deployments. These are tools to

acquire knowledge. The education they provide is their most important contribution. They also require substantial resources to operate correctly. It can provide a fantastic

learning tool in computer security. These are a cheap and simple way to add protection to a network and help developing new ways for countering them. It Acts as quality control for security design and implementation.

REFERENCES

[1] Mohammad Saiful Mamun, "HIERARCHICAL DESIGN BASED INTRUSION DETECTION SYSTEM FOR WIRELESS AD HOC SENSOR NETWORK", A.F.M. Sultanul Kabir in (IJNSA), Vol.2, No.3, July 2010.

[2] Miguel A. Calvo Moya, "ANALYSIS AND EVALUATION OF THE SNORT AND BRO NETWORK INTRUSION DETECTION SYSTEMS" September 2008.

[3] Bridges, Susan, and Rayford B. Vaughn. 2000. "Intrusion Detection Via Fuzzy Data Mining." In Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122. Ottawa, Canada.

[4] Bezroukov, Nikolai.19 July 2003."Intrusion Detection (general issues).Softpanorama: Open Source SoftwarecEducational Society. Nikolai Bezroukov.

[5] Network-based Hybrid Intrusion Detection and Honeysystems as Active Reaction Schemes Pedro García-Teodoro in 2007.

[6] Arun Hodigere , " Intrusion Detection", source unknown.

[7] Cliff, A. Password Crackers - Ensuring the Security of Your Password. Unknown: SecurityFocus.com, 2001, accessed 12 October 2004.

[8] Clarke, Roger. *Conventional Public Key Infrastructure:* An Artefact Ill-Fitted to the Needs of the Information Society. Canberra : Clarke, 2000, accessed 12 Oct. 2004.

[9] @stake. @stake LC 5. Cambridge: @stake, undated, accessed 12 October 2004.Blanding, Steven F. "Secured Connections to External Networks," in Information Security Management Handbook, 4th Edition, Harold F. Tipton andMicki Krause. Boca Raton: Auerbach, 2000 .

[10] New Methods of Intrusion Detection using Control- Loop Measurement *May 16, 1996*