ISSN : 0974 - 7435 Volume 8 Issue 10

BioTechnology
An Indian Journal

FULL PAPER

BTAIJ, 8(10), 2013 [1353-1356]

Study of intrusion detection systems

Cao Yonghui
School of Economics & Management, Henan Institute of Science and Technology, Xinxiang.R. China, 453003, (CHINA)

ABSTRACT

This paper presents the methodologies of IDS technologies. Essentially, any system requiring security must be protected from attacks. Intrusion-detection systems are used to detect unusual activity in a network of computer systems to identify if activity is unfriendly or unauthorized in order to enable a response to that violation. To achieve this, there are two main types of IDS: network-based and host-based. This paper outlines these two types of IDS respectively and highlights the advantages of each kind.

KEYWORDS

Intrusion detection systems;
Network-based IDS;
Host-based IDS.

INTRODUCTION

Virtually all existing intrusion detection methods are network-centric; however, with the wide-scale proliferation of wireless computing devices, there is a growing need for an efficient host-centric method. To our knowledge, there is nothing in the literature where anyone has theorized and then built an efficient fully host-centric application for the sake of IDS for smaller mobile devices.

Security and power are collectively the two most significant and frustrating issues presently facing wireless systems and network developers. Wireless networks are vulnerable to anyone who knows how to intercept radio waves at the proper frequencies. Since the data is sent through the air, many traditional "wired" network security measures are considerably less effective. Authentication is the most important step for setting up a secure channel for administrators and data authenticity is the most prominent security risk from a user's point of view. Market pressure for authentication to be faster, transparent and more robust is at odds with constraints of small mobile computing. Computing power and bandwidth are scarce commodities. The use of a computationally intensive cryptosystem, such as RSA, may not be a palatable choice in such environments nor is the use of digital signatures to sign every packet with its private key entirely feasible since these measures are prohibitively inefficient. In short, authentication will continue to be a problem and intrusions will occur sooner or later.

As attacks on computer systems are becoming increasingly numerous and sophisticated, there is a growing need for intrusion detection and response systems to dynamically adapt to better detect and respond to a variety of attacks. Unfortunately, intrusion detection and response systems have not kept up with the increasing frequency and sophistication of these threats. All of the evaluations performed to date indicate that IDSs are only moderately successful at identifying known intru-

sions and quite a bit worse at identifying those that have not been seen before. Given the wide-scale proliferation of wireless computing devices (which are by default not configured secure), this reality is even more worrisome.

As existing intrusion detection methods are network-centric, there is a growing need for an efficient host-centric method that can be incorporated or stand alone. The number and diversity of computers often make it impossible to protect each computer individually with host-based IDS. In addition, these systems are generally very expensive and very "power-hungry" because of all the CPU time needed for analysis 5. It is primarily due to these shortcomings that there is scarcely any mobile host-based IDS offered today. Many organizations recognize this potential problem, but few have instituted effective protection programs to build and integrate a host-centric method or one that takes into account the security benefits of correlating feedback from mobile-hosts.

NETWORK-BASED IDS AND HOST-BASED IDS

Essentially, any system requiring security must be protected from attacks. In order to do this, a good defense requires two types of actions. First, it requires a passive defense consisting of knowledge, effectiveprocedures and equipment properly initializedand maintained. Second, it calls for a strategy to react and resolve the problems associated with the attacks when, or preferably before, they occur. Intrusion detection systems monitor "traffic" or "operations" from a particular site and report these conditions to a central controller (human or machine). In effect, intrusion- detection systems are used to detect unusual activity in a network of computer systems to identify if activity is unfriendly or unauthorized in order to enable a response to that violation. When an intrusion is detected, the intrusion-detection system can react in a number of ways from alerting a systems administrator and/or recommending various actions to automatically kicking the intruder off the network or shutting down the violated host itself. To achieve this, there are two main types of IDS: network-based and host-based.

Network-based IDS

Network-based ID systems (NIDS) monitor network traffic between hosts. These monitors can be located inside the intranet between selected subsystems or host computers or at a gateway or firewall between a corporate intranet and the outside Internet (also known as router-based monitoring) to ensure safe, reliable connections between computers over large networks. When a sensor notices a violation in the network policy, which sets how the network manages things such as packet flow, it sends an alarm to the centrally located director console. When it detects an attack or misuse, it passes an alarm to a network management console for action by an administrator, or it can be configured to automatically terminate a connection, reconfigure firewalls or do anything else the user might want to have happen if an attack occurs. Though a few are more sophisticated and analyze protocol- specific information, many current network-based ID systems are quite primitive, only watching, for example, the words and commands of a hacker's vocabulary.

The intent of strategically placing IDS within different network locations is to examine data packets before they are allowed to enter an intranet system. For example, E-mails, programs, and Internet packets are monitored for "signatures" that are unauthorized as part of a behavior analysis based on the content and format of data packets. This labor- intensive method is designed to prevent unauthorized access to a system's intranet infrastructure. The problem is that this system relies upon known signatures and causes system performance problems and false alarms as traffic density increases. In addition, this type of IDS is unable to stop encrypted packets or system attacks from "inside" the intranet, unlike host-based IDS which detects malicious behavior outright.

Host-based IDS

Host-based intrusion detection systems (HIDS) directly monitor the computers on which they run, often through tight integration with the operating system. Traditionally, host-based IDS employ intelligent agents or sensors to continuously review computer audit logs for suspicious activity, and they compare each change in the logs to a library of attack signatures or user profiles. These dedicated desktop systems can also poll key

system files and executable files for unexpected changes. Host-based IDSs are generally more effective than networked-based IDS because they monitor insiders with the same vigilance as outsiders and are not affected by network encryption schema.

ADVANTAGES OF NETWORK AND HOST-BASED IDS

Monitoring activity on a system using network and/or host-based Intrusion detection in real time or after the fact for the purpose of identifying attempts or successful intrusion of the system has its strengths and weaknesses. The advantages of each IDS presented above are outlined below in TABLE 1:

HYBRID IDS

NIDS and HIDS approaches can be complementary. For example, one possible strategy is to implement network-based monitoring and add agents on particularly sensitive hosts. By observing data at all levels of the host's network protocol stack, the ambiguities of platform-specific traffic handling and the problems associated with cryptographic protocols can be resolved. The data and event streams observed by these agents are those observed by the system itself. Thus, such an approach offers advantages of both alternatives listed above while maintaining the ability to observe the entire communication between victim and attacker. Like all host-based approaches however, the hybrid approach implies a performance impact on every monitored system and requires additional support to correlate events on multiple hosts.

Consequently, an innovative hybrid approach that leverages these advantages and helps to overcome these associated problems is desirable. B-bid is such a hybrid approach that is accomplished using HIDE, SPIE and HASTE.

TABLE 1 : Advantages to Network and Host-based IDS

Network-based IDS	Host-based IDS
Faster detection: A network-based monitor will typically detect a problem in seconds or milliseconds. Most host-based approaches depend on auditing logs every few minutes.	More cost-effective: It may be more cost-effective for small numbers of hosts.
Less visible: A monitor is less visible and accessible than a host, and thus less vulnerable to attack. Unlike a host, a network-based monitor doesn't have to respond to pings, allow access to its local storage, let users run programs on it, or allow access to multiple users.	More granular: It can easily monitor activities, such as access to sensitive files, directories, programs, or ports, that are difficult to deduce from protocol-based clues.
Bigger perimeter: The network-based approach may be able to stop an attack at the perimeter of the network, before the perpetrator accesses a host.	More customizable: Per-host customization is easy with a separate agent for each host.
Fewer monitors: Fewer monitors are needed because one monitor can protect a shared network segment. In contrast, an agent per host is needed, which can be costly and hard to manage. On the other hand, in switched environments, a monitor per host may be needed because every host is on its own segment.	Tighter perimeter: Once a perpetrator has obtained a password and user name for a host, the host- based agent has the best chance of distinguishing harmful from normal activities.
Fewer resources: It doesn't take up any resources on the protected device.	Fewer hosts: The host-based approach may not require a dedicated hardware platform.
	Less traffic-sensitive: An agent is unlikely to miss any activity due to traffic loads.

REFERENCES

[1] R.Winkler; Intrusion Detection Systems, Proc.Eleventh IEEE Intl.Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 19-27, Jun. **(2002)**.

[2] M.Hurwicz; Cracker Tracking Tighter Security with Intrusion Detection, Byte, May, **(1998)**.

[3] T.Verwoerd, R.Hunt, Intrusion detection techniques and approaches, Computer Communications, **25(15)**, 1356-1365, Sep., **(2002)**.

[4] S.Jha, O.Sheyner, J.Wing; Two Formal Analyses of Attack Graphs, Computer Security Foundations Workshop, Proc.,15th IEEE,.49-63, Jun., **(2002)**.

[5] S.C.Lee,; D.V.Heinbuch;; Training a neural-network based intrusion detector to recognize novel attacks,

IEEE Transactions on Systems, Man and Cybernetics, Part A, **31(4)**, 294 -299, Jul., **(2002)**.

[6] J.E Dickerson, J.Juslin, O.Koukousoula, J.A.Dickerson; Fuzzy intrusion detection, IFSA World Congress and 20th NAFIPS International Conference, Joint 9th, **3**, 25-28 **(2001)**.

[7] C.Ko, M.Ruschitzka, K.Levitt; Execution monitoring of security-critical programs in distributed systems: a specification-based approach, Proc. IEEE Symposium on Security and Privacy,175 187, 4-7 May, **(1997)**.

[8] T.Mudge Power; A First-Class Architectural Design Constraint, IEEE Computer, 52-58, Apr., **(2001)**.

[9] J.McHugh, A.Christie, J.Allen; Defending Yourself: The Role of Intrusion Detection Systems, Software Engineering Institute, CERT Coordination Center IEEE, 42-51, Sep., **(2000)**.

[10] L.Kanishka, A.Raghunathan, D.Sujit, D.Panigrahi; Battery-Driven System Design: A New Frontier in Low Power Design?, Dept. of ECE, UC San Diego, La Jolla, CA.C & C Research Labs., NEC USA, Princeton, NJ, 1-7.