INTRUSION DETECTION SYSTEMS:

Possibilities for the Future

KAREN A. FORCHT

Andersen Consulting Professor of CIS

*CIS/OM Program, College of Business, James Madison University, Harrisonburg, VA 22807,
FORCHTKA@JMU.EDU, 540-568-3057(o)*

CHRISTOPHER ALLEN

4001 Alabama Avenue, NE, St. Petersburg, Florida 33 703

BARBARA BRODMAN

Rt. 2 Box 385, Kents Store, Virginia 23084, (804) 589-3418, gpfbab@mindspring.com

DAVID CORNING

14 Tideview Drive, Dover, New Hampshire 03820, (603) 749-781 6, davidcorning@msn.com

JACOB KOUNS

*3201 Copper Mill Trace, Apt. L, Richmond, Virginia 23294, (804) 74 7-32 79,
jkoun@bellatlantic_net*

Key words: Intrusion detection systems, artificial intelligence, neural networks, operating systems audits, passive protocol analysis, network-based ID systems, signature detection, network interface card, black box, firewall, viruses, Trojan Horse.

Abstract: Man has used Intrusion Detection Systems since the dawn of time. The systems that have been developed for detecting and monitoring Information systems are becoming more accepted as an integral part of security solutions. There are limitations in the success rate and usefulness of the systems in use, however, there are some exciting developments on the horizon. By combining artificial intelligence, neural networks and similar advances in programming, we can look forward to Intrusion Detection Systems that will not only raise the alarm, but take the appropriate action to thwart the attack.

1. INTRODUCTION

The term IDS is fairly new, born out of the cyber world's attraction to anagrams, but the concept of Intrusion Detection Systems has existed since the dawn of time. Organisms developed immune systems designed to detect the existence of unwanted intruders and later, man expanded the use of Intrusion Detection Systems beyond the confines of the human body. Domesticated dogs were used to identify potentially dangerous intruders and then later trained to protect herds. Ever since man has had something of value to protect, Intrusion Detection Systems were used. Today, what we need to do is protect information systems. To do this, we have developed a digital watchdog to protect us from the virtual "wolves" in cyberspace.

1.1 Networking of Computers

The widespread use and networking of computers has created an environment where valuable information can be stolen or sabotaged without a physical presence and with unprecedented stealth. Much like the need to protect important items in the real world, similar security measures must be taken on the digital level to protect our valuables in cyberspace. Intrusion detection is an important component of a security system, and it complements other security technologies. By providing information to site administration, ID allows not only for the detection of attacks explicitly addressed by other security components (such as firewalls and service wrappers), but also attempts to provide notification of new attacks unforeseen by other components. Intrusion detection systems also provide forensic information that potentially allows organizations to discover the origins of an attack. In this manner, ID systems attempt to make attackers more accountable for their actions, and, to some extent, act as a deterrent to future attacks.

1.2 Systems

In general, ID systems are used to detect unauthorized usage or misuse of a computer system. This is done by analyzing and scrutinizing operating system audit trails that form a footprint of system usage and then look for sequences of transactions that suggest suspicious activity. Using this passive protocol analysis, ID systems can identify suspicious activity by recognizing known attack patterns and through statistical behavior anomaly detection (the recognition of deviations from normal activity). ID systems can monitor at both the network and host level and these very often are used in conjunction.

1.3 Network-based Systems

Network based ID systems are designed to detect unauthorized activity throughout a network by monitoring all network traffic passing on the segment where the agent is installed and reacting to any anomaly or signature-based suspicious activity. Host-based ID systems analyze the activity on a particular computer. They can detect attacks that are not detectable by network-based ID systems since they can view events local to a host.

IDS's analyze events using two techniques: 1. signature detection and anomaly detection and 2. honey pots. Signature detection monitors for activity that matches a predefined set of events that are known to be an attack. Signature-based, therefore, must be specifically programmed to detect each known attack. Anomaly-based ID systems find attacks by identifying unusual behavior (anomalies) on a host or network. Anomaly-based IDS defines normal behavior based on a statistical profile or normal usage. It then monitors the host or network to find use that deviates from this defined normal behavior. See Figure 1.1

©Comstock 2000

Figure 1.1

1.4 Decoy Systems

Complementary to the IDS is the use of Honeypots. Honeypots act as a decoy that appears to have several vulnerabilities, making it attractive to hackers. Set up to look like a legitimate system with legitimate files, the Honeypot will lure the intruder and he/she will believe the information residing there is important. The hope is that the hacker will stay involved with the Honeypot long enough to discern the information about the intruder and the source of the attack necessary to capture him. However, the primary

purpose of the Honeypot is to monitor and learn from the intrusion so systems engineers can determine how the systems were exploited. This information can be used to prevent attacks on real systems. Since the Honeypot should have no other role, any connection attempt to it should be suspicious. (See Figures 1.2, 1.3, 1.4)

1.5 A Basic Network Security Model

Firewalls are not enough

Due the historical minimal effectiveness of Network based ID systems, companies have not yet embraced them, thinking that a Firewall will provide sufficient security. To completely protect an organization however, audits of the network on a regular basis are a necessity.

Figure 1.3

Network Based Intrusion Detection

Network based IDS's are those that monitor traffic on the entire network segment. A Network interface card (NIC) can operate in one of two modes, these being:

Normal Mode, where packets which are destined for the computer (as determined by the Ethernet or MAC address of the packet) are relayed through to the host system.

Promiscuous mode, where all packets that are seen on the Ethernet are relayed to the host system.

A network card can normally be switched from normal mode to promiscuous mode, and vice-versa, by using a low-level function of the operating system to talk directly to the network card to make that change. Network based intrusion detection systems normally require that a network interface card be in promiscuous mode.

Figure 1.4

1.6 Characteristics of a good Intrusion Detection System

An Intrusion Detection System should address the following issues, regardless of what mechanism it is based on:

1. It must run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a "black box". That is, its internal workings should be examinable from outside.
2. It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge base rebuilt at restart.
3. On a similar note to above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted.
4. It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.
5. It must observe deviations from normal behavior.
6. It must be easily tailored to the system in question. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.
7. It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.

2. EXISTING SYSTEMS

Many choices for Intrusion Detection Systems exist, including those that cost tens of thousands of dollars and those that are free. InfoSec Managers need to view those choices within a cost/benefit environment. Understanding these systems and their capabilities is necessary to provide the most cost effective protection. Additionally, most IDS systems only work with one operating system so there are Unix and Windows based IDS's. These usually operate in conjunction with a firewall.

2.1 Unix-Based Systems

Unix has several host based systems each covering different areas.

- The first is **TCP Wrappers**. This program does not change existing configuration files and does not increase overhead. The Wrappers log the name of the existing client host and the requested service. Each packet is logged with a timestamp. When a service is requested (Ftp, Systat, Finger, Telnet etc.). The Wrapper checks its access control list and, if permitted, engages the service. If the connection is not allowed, the packet is dropped and a log entry written.
- **Tripwire** is a program that monitors system files and any file that has been tampered with can be detected. The program uses a cryptographic hash that changes if the file has changed. When a file has been changed, an email alert is sent to provide notification. Tripwire cannot prevent a file change but merely notifies that one has occurred.
- **CMDS** is a log file reader. It builds a profile of systems and reports activity that varies from that norm. It has a capacity to spot new attacks better than signature systems as it does not rely on a catalog of known attacks but logs changes to the system.

2.2 Windows NT Systems

Windows NT suffers from a variety of threats mostly viruses and Trojan Horses. Here are a few NT host based Intrusion Detection Systems.

- **NukeNabber** is the Windows equivalent of TCP Wrappers. This program can identify scans and collect the IP address of scanners. NukeNabber is able to block certain ports to traffic as well as monitor ports and collect data.
- **Back Orifice Friendly** is a program that is designed to detect Back Orifice (BO) probes. Back Orifice is essentially a remote administration tool that allows others to take control of your computer. Once BO is installed on a computer without a password, anyone with a BO program can scan the Internet and log onto an infected computer.

- Personal firewalls include **Zone Alarm, At Guard and BlackICE Defender**. These firewalls are installed on host computers and detect attacks from the outside as well as notification when applications are trying to connect from the inside.
- Network Based Intrusion Detection is designed to primarily detect attacks from the Internet. Most of the network systems are libcap based. Libcap is used to get information from the operating systems kernel. This deals with the granting of privileges and processes. Libcap then passes the information to the application.
- **Snort** is a lightweight IDS. It is capable of performing real time traffic analysis and packet logging. The program can detect buffer overflows, port scans, CGI attacks and OS fingerprinting attempts. It can be used as a packet scanner or packet logger.
- **Shadow** is a signature based detection system. The basic SHADOW setup is two systems: a data-collection machine known as a sensor, and an analysis station. The sensor sits on the network of interest and captures all the traffic. The raw data files are moved via a secure channel to the analysis station for inspection. Shadow is for Unix based systems.
- **Cisco Secure IDS** is a Unix-based system that features a sensor and a director. The sensor has alarms, which captures important information such as attack description, IP addresses and keystroke capture. Secure IDS is a signature system and can recognize a variety of attacks. The director is a transparent IDS and does not consume system resources.
- **ISS Realsecure** operates under NT and Unix systems. The system features an easy interface that uses red, yellow and green icons to signify alerts. This product also has a sensor and a console. RealSecure detects over 200 attacks but is known to generate false positives.
- **CyberCop Monitor** is a network-based system that monitors incoming and outgoing network traffic. It has a signature database of over 170 attacks and can alert to time spanned attacks. This product also suppresses Denial of Service (DOS) attacks and protects against unauthorized changes to system files.

3. FIREWALLS

Firewalls are the first line of defense for most networks. There are two types: 1. a packet filter that does a quick inspection of packets and 2. a stateful application gateway proxy, which can tear up packets and rewrite them. Firewalls are usually deployed at the point called the Demarc where the ISP's responsibility ends and the company network begins. Simply, firewalls are used to control the access to permitted types of traffic. Firewalls use Access Control Lists (ACL) to allow or deny packets to enter

or leave the network. If a service or entrance is denied, the packet is dropped and not allowed to enter the network. The firewalls are configured using rule sets that can be permissive or restrictive. Security policies tend to be written documents that have no teeth but the firewall can enforce policies by allowing or disallowing events that the security policy prescribes. Of great use to InfoSec professionals is their logging feature. All events are logged and the perusal of logs can contribute greatly to understanding any attempted intrusions. One hides the network behind it. Firewalls also provide protection by providing a translation function. An internal network often has a different IP scheme than the one presented to the public. The firewall translates the external address into the correct internal address and delivers authorized packets to their destination.

4. USER AUTHENTICATION

There is growing need to detect and prevent unauthorized activities both from within and outside an organization. User authentication and access control measures are limited and abusers are finding more and ever more clever ways to compromise such systems. Proactive monitoring of system activity along with immediate responses to a problem are the next best hope for improved Intrusion Detection (perhaps it will now be called Intrusion Detection and Response).

Intrusion Detection Systems will need to utilize Artificial Intelligence, Neural Networks and Expert Systems in order to reach full potential. Recently introduced **Retriever**, a newer product of Symantec Corporation is a proactive network security management tool capable of discovering and mapping network components. It also can identify vulnerabilities and perform network audits. What's new about this software is its ability to predict by performing network security modeling, like a "what-if" analysis and provide the solutions to fix them.

If an IDS sensor can "learn" its surroundings on the network, it will begin to make its own decisions. It will determine normal traffic and thus avoid false-positives. Most sensors simply report comparisons to stored signature files, enabling any signatures not in the database to remain unnoticed. After mapping the network, the IDS could then make intelligent decisions about the proper steps to take. These could be customizable and could include:

- Issuing of an explicit request (or challenge) for further authentication
- Recording of details in an intrusion log for later inspection/investigation
- Immediate notification of the system manager (alarm)
- Phased reduction of permitted behavior

- Locking of the intruders terminal
- Termination of the anomalous session.

4.1 Examples of Attacks

How does this differ from historically used ID systems? Recent attacks that have been detected have continued after the IDS thinks it has stopped. When a user on the Internet begins an attack, the IDS probe sees it and watches the session to determine if it's continuing or if it has stopped. The intruder, however, has manipulated the TTL (Time to Live) flag within a TCP packet and has set it to 1 less than it takes to reach the actual webserver. The packet is then sent out to close the attack, fooling the IDS probe into thinking it's over. Since the TTL of the packet is set one hop less than the webserver, it never makes it there and the attack continues. Mapping the network would allow the IDS probe to know exactly how many hops away all of the servers are located. Then, if this type of packet came in again with an altered TTL, it could realize the webserver did not reset the connection and that the attack is continuing.

Hackers continue to trick IDS probes to disable matching attacks with signatures. IDS probes need to implement "packet scrubbing", causing an alert whenever a command attempts to gain root. Using Artificial Intelligence, the IDS could realize it needs to recompile fragmented packets before assessing the activity.

4.2 Expert Systems Examples

The use of a general expert system applied to Intrusion Detection has only recently been taken seriously. The reasons for this are related to low performance, difficult integration and language complexity. However, the Production-Based Expert System Toolset (P-Best) is sufficiently fast for real-time detection of attack methods such as SYN flooding and buffer overruns. It also is interoperable with OS libraries and easily integrated into anomaly and misuse detection. Providing strategies and mechanisms for understanding the state of a given environment, this can derive logical inferences that can lead to conclusions, such as deductive reasoning or bottom up reasoning.

P-Best is now being applied to the analysis of network traffic streams. It analyzes TCP/IP packet streams for low level layer attacks and higher layer attacks involving vulnerable network service layer protocols like FTP, SMTP and HTTP. An Internet accessible P-Best translation service that will allow users to develop and compile rule sets into self contained expert systems.

4.3 Artificial Intelligence

Artificial Intelligence is used to solve complex that are:

- Usually resolved by an expert
- Not amenable to straight forward solution by numerical computation; or, if they might theoretically be solved numerically, the computations would take an impractically long time and/or use too much computational resources
- Usually solved by people using rules of thumb (heuristics), that work most of the time but with no guarantees
- Ill-defined
- Related to situations that constantly change over time (i.e. are dynamic), so that a better solution is likely to be made by someone (or some software) that can take the changes into account as they happen, rather than set up rules for decision making in advance by trying to anticipate what changes may happen
- Not readily solvable by breaking the problem into interacting sub-problems
- Highly dependent on the context within which the problem occurs in terms of determining an adequate solution

“Artificial Intelligence is no match for natural stupidity”

-Anonymous

4.4 Active Evidential Reasoning

Active Evidential Reasoning, inspired by model-based reasoning, plan recognition and automated diagnoses systems in order to improve ID capabilities. ICE (Intelligent Correlation of Evidence) systems are capable of the detection and diagnosis of threats by correlating evidence from configuration examination, host audit data, network sniffers, agent-based evidence collectors and predictive analysis techniques. Using such diverse and redundant evidence sets allows the detection of intrusions by highly skilled hackers who try to conceal their actions. Also, after collecting corroborating and refuting evidence such a system can tune its internal models, resulting in fewer false alarms. The US Air Force's Rome Laboratory is researching these systems in order to add response to network Intrusion detection.

4.5 Neural Networks

Neural Networks process information the way biological nervous systems, such as the brain, do. Their basic concept is in the structure of the information processing system. Made up of many connected processing neurons, a neural network system uses the technique of learning by example to resolve problems. The neural network is configured for specific applications, such as pattern recognition, through a learning process called training. "Neural networks can differ on:

- the way their neurons are connected
- the specific kinds of computations their neurons do
- the way they transmit patterns of activity throughout the network
- the way they learn, including their learning rate

Neural networks are being increasingly used to solve real world problems that are so complex that they do not have a defined algorithmic solution. Neural networks can solve problems people can solve. These include pattern recognition, forecasting and analyses.

4.6 Distributed Agents

Most Intrusion Detection Systems in large networks must use several distributed agents instead of one large module. These agents need to use artificial intelligence in order to handle the various intrusion problems. Using a Bayesian alarm network to work as an independent agent to narrow detection efforts to a specific type of the attack in a large network, such as a denial of service, worm or virus, would allow more knowledge about the attack within the system. Individual nodes of the network could develop their own model of the Bayesian alarm network and agents could communicate between themselves and with a common security database. Networks should be set up hierarchically so that the top level Bayesian alarm network that is interconnected to the lower level networks and data could substitute for a distributed Intrusion Detection System.

4.7 Inference Logic

Inference Logic for automated reasoning about misuse in computer and network operations is beginning to be realized and holds the greatest promise for IDS development. InfoSec Managers can look forward to a broad array of new products that will utilize these increasingly more usable systems for Security confidence.

Maintaining network security is not a serial process, and not a series of discrete steps, with 'security' being the end product. Previous security models have failed to properly emphasize the interdependence of the critical elements of the security process, hence, we use of the term "security ecosystem", rather than merely "security cycle" or "security wheel". The security ecosystem is a community of dynamic, evolving processes functioning as an organic unit that protects the network through a combination of preventative and proactive measures. An organization's security ecosystem should be a balance of the continuous processes of risk assessment (assess), network monitoring (monitor), risk countermeasures (respond), and policy review and enforcement (policy). If one of these critical elements is missing, or practiced sporadically, this will upset the balance that optimally exists between these processes.

5. REFERENCES

1. Escamilla, Terry. 1998. *Intrusion Detection: Network Security beyond the Firewall*. Wiley Computer Publishing.
2. Sams, Net. 1997. *Maximum Security: A Hackers Guide to Protecting your internet Site and Network*. Macmillan Computer Publishing.
3. Tipton, Harold F. and Krause, Micki. 2000. *Information Security Management Handbook*, 4th Edition. CRC Press.
4. SC Magazine. *Buyers Bible 2001*. December, 2000. pp.48-62.
5. Bauer, R. Kenneth and Halme, Lawrence R. *AIN'T Misbehaving: A taxonomy of Anti-Intrusion Techniques*. SANS Institute Resources.
6. *Intrusion Detection Primer*. http://www.linuxsecurity.com/feature_stories/feature_store-8.html
7. Elson, David. *Intrusion Detection, Theory and Practice*. March 27, 2000. Securityfocus.com <http://www.securityfocus.com/>
8. Fried, Stephen. *Information Security, The Big Picture*. Sans GAIC 2000.
9. Furnell, Steven M. and Dowland, Paul S. *A Conceptual Architecture for real time Intrusion Monitoring*. *Information Management and Computer Security*. 8/2/2000. MCB University Press.
10. Hart, Rod; Morgan, Darren and Tran, Hai. *An Introduction to automated Intrusion Detection Approaches*
11. *Information Management and Computer Security*. 7/2/1999. MCB University Press
12. Hoglund, Greg and Gary, John. *Multiple Levels of Desynchronization and other concerns with testing an IDS System*. Updated August 11, 2000 <http://securityfocus.com/frames/?focus=ids&content=/focus/ids/articles/desynch.html>
13. Hartley, Bruce. *Honeypots: A new Dimension to Intrusion Detection*" <http://www.advisor.com/MIS>

14. Klug, David. Honey Pots and Intrusion Detection. September, 2000. SANS Institute Resources.
15. Lindqvist, Ulf and Porras, Phillip A. Detecting Computer and Network Misuse Through the Production Based Expert System Toolset (P-Best). Swedish National Board for Industrial and Technical Development.
16. Merkow, Mark. Standing Sentry Over Your Network update April 13, 2000. <http://securityfocus.com/focus/ids/articles/markmerkow.html>
17. Metaxiotis, K.S. and Samouilidis, J.E. Expert Systems in Medicine: academic illusion or real power? Information Management and Computer Security. 2000 MCB University Press.
18. Me and my SHADOW Using the new SANS intrusion-detection software with Solaris. http://www.sunworld.com/sunworldonline/swol-09-1998/swol-09-security_p.html
19. Northcutt, Stephen. Intrusion Detection, The Big Picture. Sans GAIC 2000.
20. Price, Katherine. Introduction to Intrusion Detection. 9/22/00. COAST <http://www.cerias.purdue.edu/coast/intrusion-detection/ids.html>
21. Thomas, Benjamin D. Intrusion Detection Primer. Linuxsecurity.com
22. Turrell, Timothy. IDS September 2000. SANS Institute Resources.
23. Intrusion Detection FAQ. http://www.sans.org/newlook/resources/IDFAQ/behavior_based.htm
24. http://www.home.cs.utwente.nl/~aps/IDS_onderzoek.shtml
25. [http://www.cs.nps.navy.mil/people/faculty/rowe/ids_tutor.html](http://www.cs.nps.navy.mil/people/faculty/rowe/ids/ids_tutor.html)
26. <http://www.geek-girl.com/ids0280.html>
27. <http://www.robertgraham.com/mirror/Ptacek-Newsham-Evasion-9-8.html>
28. <http://www.networkintrusion.co.uk/>
29. <http://csrc.ncsl.nist.gov/nistbul/it199-11.txt>
30. Continuous Adaptive Risk Management. Hiverworld, Inc. <http://www.hiverworld.com/>
31. http://www.secinf.net/info/ids/nn-idse/paperF13_2.html
32. Glossary of Artificial Intelligence Terms. SHAI http://www.shai.com/ai_general/glossary.htm
33. NSA Glossary of Terms Used in Security and Intrusion Detection. SANS Institute Resources. <http://www.sans.org/newlook/resources/glossary.htm>