Global Information Assurance Certification Paper

THE ETYMOLOGY OF INTRUSION DETECTION SYSTEMS

James L. Arko

GIAC Certification Version 2.0

Security Concerns

Despite the precautions taken by virtually every network administrator, for the small 10-user office to the largest international banking consortium, that administrator's biggest nightmare is breach of network stability and loss of data, whether by misuse of the system by the employees of that organization, or by hacking from juvenile technogeeks. With the Internet and e-mail available to every employee in his/her firm, the network administrator must realize the dangers of inadvertent downloading of viruses by unwitting employees, as well as the possibility of uninvited "guests" utilizing their network bandwidth.

According to *ACM Crossroads Student Magazine,* virtually all major companies have reported at least one major incident of hacking in the past five years. Additionally, information theft is up over 250%, and telecom and computer fraud totaled $10 billion in the US alone during that same time period. With the need for free-flow of information balanced with confidentiality of privileged data, what's an administrator to do? This concern has spawned a new field of study on the electronic frontier – Intrusion Detection.

When the government contacted SRI International in the summer of 1983, a contract to analyze system management facility records led to the development of a first-generation intrusion detection system. This project explored statistical data techniques and audit trail reduction analysis. Records from IBM mainframes later were used to examine rule-based criteria to detect malicious activity.

Now in the year 2001, we are capable of providing real-time detection of security violations on both network and host-based systems. Today science and engineering has enabled security systems administrator to utilize statistical profiling tools to clearly differentiate general-purpose applications from irregular network behavior. It has also shown that statistical anomaly detection is effective at identifying proper operation of user applications and those operations that can be distinguished as abnormal. As security experts try and keep pace with our ever-flourishing technology introductions, we must embrace the science and approach intrusion detection in a methodical manner. As more and more people pioneer across the electronic frontier, we must be wary of the uninvited guest and question the actions of these persons who intend to intrude.

Intrusion Detection

Intrusion detection includes the analysis of statistical data in order to determine the legitimacy of users on a network. As a science, intrusion detection encompasses many actions of which administrators must be aware in order to respond. The type of response required will

depend upon the method of intrusion. The defense against intrusion will depend upon the quality of an organization's security policies that have been set in place, as well as its employment of trained security experts.

For example, many security experts know that the central steps a hacker uses to conduct a successful spoofing attack against a network include:

1. Identification of a target,
2. Anesthetization of the host he intends to impersonate,
3. Forging the address of the host he is impersonating,
4. Connecting to the target, masquerading as the anesthetized host, and
5. Accurately guessing the correct sequence number requested by the target.

The hardest part of this game attacker's play is guessing the correct sequence numbers. After the cracker has contacted the intended target and requested a connection, he must get a response of sequence numbers from the target in order to log these numbers before terminating the connection. When the attacker identifies a pattern in these sequence numbers, he can reliably predict which sequence numbers are required for authentication. Once the attacker has the information, he can perform a spoofing attack. (*Maximum Security – Second Edition*, pp. 559-569.)

A well-placed intrusion detection system would allow the system administrator to see an illegitimate user on the network before the hacker could complete his routine.

Intrusion Detection Systems

One intrusion detection system (IDS) by Axent Techonologies is Intruder Alert. Intruder Alert is a "rules engine." It processes the inputs it receives based on rules or policies established by the network administrator, thus giving the administrator flexibility in designating what types of policies to set. In addition, it provides rules to detect behavioral anomalies. Anomaly detection techniques assume that all intruder's activities are necessarily anomalous. In its simplest form, this means that, in theory, you can establish a normal activity profile for a user. Thus any deviation from this "normal activity" would trigger a flag response which will be brought to the administrator's attention.

Another IDS is auditGUARD by DataLynx, Inc. This system operates on most IBM and Hewlett Packard equipment, and allows you to monitor who did what, where, when, and how by being a complete audit management tool.

In addition to these individual IDSes, there is also a push to establish more powerful IDSes by combining the characteristics of more than one IDS. These are referred to as "hybrid

intrusion detection systems."

Hybrid Intrusion Detection Systems

Just what are hybrid intrusion detection systems, and what do these "systems" do? There have been many debates as to exactly what the term hybrid intrusion detection means; most of which are spawned by marketing personnel tossing around terms such as hybrid, multi-tiered, and multiwhomping packet examination. One must acknowledge these soft terms as nothing more than a set of features marketing folks tout which enable distributors to clear warehouses via unwittingly ambitious consumers.

By definition, the term hybrid is usually used as a description for things that are a cross between two other things. Describing something as "hybrid" is meaningless unless you say what it is a hybrid of. Thus, confusion inevitably sets in. Additional confusion arises as administrators running a mixed environment of Windows NT, Sun Microsystems Solaris, and Linux will have to have a variety of agent sensors running to support all three platforms.

A hybrid intrusion detection system is a combination of network and host-based IDSes. Network-based IDSes use network cards operating in an indiscriminate mode (promiscuous) that sniff all packets on each network segment with a host-based IDS (which looks only at packets addressed to the computer on which the IDS sensor resides).

Hybrid systems are quickly becoming necessities for many enterprise-wide environments, primarily because cross-functionality amongst multiple domains mandates a need. Secondly, the enterprise's corporate shareholders assuredly expect a return on their investment. One would not receive such a return if Company A's production environment was known to be vulnerable to multiple inside/outside hack attacks. Additionally, the lofty pricing amongst IDS systems can be intimidating to the corporate "powers that be."

Hybrid systems enable organizations to extensively configure a more secure intrusion detection suite by empowering users. When a security system's engineer deploys a hybrid IDS, he/she knows that no single IDS vendor will be able to take care of the network's needs. What a responsible security system engineer will know is the characteristics of a good hybrid IDS.

1. First, and foremost, it must be difficult to fool.

2. It should be fault tolerant enough to survive a system crash and not need its knowledge base rebuilt upon restart.

3. It must be tailorable to the system in question. All systems have different usage patterns.

4. Integration with other security devices or frameworks should be seamless (i.e. good adaptation).

5. It should have proven success operating in a complex environment similar to your own.

6. Besides proving anomaly detection (i.e. deviations of normal behavior), sensors should be configurable to have duplicate interacts on an alternate network for out-of-band management (i.e. a stealth interface) with proper encryption.

7. More important than all of this, including user functionality, in my opinion is the ability to interpret and collect data that can be used in court against your attackers.

8. Timely signature updates.

9. Signature accuracy.

10. Capable, experienced support staff.

11. Proven installations in complex environments.

12. It must be able to monitor itself to ensure that it has not been subverted.

13. More important than all of this, including user functionality, in my opinion is the ability to interpret and collect data that can be used in court against your attackers.

(*The ABCs of IDSs (Intrusion Detection Systems)*, Carol. Meinel.)

Hybrid IDSes have been introduced by many industry vendors who are at the forefront of today's technology market. Unfortunately there is no single vendor that can produce a "truly secure hybrid IDS". Yes -- I said it – not one. This does not stem from hardware fault tolerance, nor does it fail due to the gregariousness of autonomous networking. A prime factor one may wish to consider is technology itself. Why? Well, technology is contrived by formulating properties of matter by which the applications of science and mathematics are used to make useful things for people. It is only the law of supply and demand that perpetuate what consumers consider useful. Many Americans have yet to even know what an intrusion detection system is, let alone know why it is useful. Many hybrid IDSes are being utilized by major financial institutions, e-businesses, and government offices worldwide.

Functionality across multiple domains and the ability to draw in system logs from the host, passing them to a central console for analysis, is one of many examples of a hybrid IDS position performance marks. Vendors such as Internet Security Systems based in Atlanta, Georgia, offer their version of a hybrid IDS known as the Real Secure Server Sensor. This product is able to handle any networking data rate, making it ideal for large numbers of systems in highly-switched environments. The server senor allows the security administrator to set up permanent blocking rules. For example, a database server can be configured to block and ignore any traffic that does not originate from a specific set of application servers on your network. Even an attacker on the same physical network would be blind to the existence of that server and unable to attack it.

Although many vendors are producing intrusion detection systems, organizations need to be aware that having the latest and greatest security gadget attached to their networks is not a fire-and-forget solution to intrusion detection. Hybrid IDSes that act as centralized points of control and monitoring are still based on purely reactionary technology Virus signature updating is a constant source of frustration among many security administrators, as is finding and retaining qualified incident response personnel.

The bottom line on hybrid intrusion detection systems is this: Many systems will operate with high LAN speeds, and some will even eliminate excessive thresholds of false positives if they are configured properly with well-defined policies. Hybrid systems are expensive, costing between $30,000 and $60,000 in licensing fees alone. A decent IDS in a middleware environment will still require products from many vendors. They also will do an organization no good unless management works with its well-trained information assurance personnel to properly support and configure their hybrid IDS. This ensures an enterprise does not have incomplete IDS coverage.

Customers should not be overly-enthusiastic or have unrealistic expectations of the systems themselves. In order to make a hybrid IDS, or any IDS, function properly, you will always rely on the help and expertise of network and systems administrators.

Future Indications

For personnel who manage large heterogeneous networks, it can be a daunting task to try and find a single-vendor IDS solution. Most organizations have tried without success. Through this trial and error process, the Department of Defense, in conjunction with the Defense Advanced Research Projects Agency (DARPA), is studying ways to standardize IDS reporting formats. DARPA's funding for this project has brought forth a study into what they call the Common Intrusion Detection Format, or CIDF for short. This report format is vying for acceptance with an XML-based reporting format that the Internet Engineering Task Force has proposed.

By utilizing some sort of common data exchange format, law enforcement, response teams, users, and vendors would be able to not only exchange data, but also communicate about it. The need for this type of information exchange is certainly real given the horrific events of September 11, 2001. With the desire for dissemination of information and data across the Internet, and the need for information security, government funding is surely going to enable the security industry to grow exponentially over the next 5-10 years.

Recommendations

In closing, my advice to network administrators and security gurus would be:

First, know your target audience. Are you dealing with a small to medium-sized company whose information is primarily kept in-house and whose primary security issues are viruses which can unwittingly be downloaded via a received e-mail? Or are you dealing with a governmental entity or an international firm with offices in many countries that need to share

highly-confidential information, but also want to distribute "public information" via a website?

Second, know your employees. What types of applications are they running? What do they need access to in the way of e-mail and Internet? What areas of your local system do they need to access in order to do their job? How can you structure your on-site system to ensure that personnel will have access only to areas of your network that they need in order to do their job?

Third, know your operating system and its built-in "security features." Know what types of protection those features provide, and what they leave vulnerable.

Fourth, if you determine that an IDS is necessary, familiarize yourself with the various IDSes available; whether your firm needs a host-based IDS, a network-based IDS, or a hybrid IDS; the cost to your company of purchasing those IDSes; and the administrative cost of implementing those IDSes.

Fifth, know how "the powers that be" think, and make your pitch for security accordingly.

BIBLIOGRAPHY

HTTP://enterprisesecurity.symantec.com/products/products.cmf

HTTP://www.dlxguard.com/faqs.htm

HTTP://security.ittoolbox.com

HTTP://www.iss.net/securing_ebusiness/security_products/intrusion_detection

HTTP://www.messageq.com/security

HTTP://www.sans.org/newlook/resources/idfaq/communication.htm

HTTP://www.intrusion.com

HTTP://cert.org

Anonymous. Maximum Security, Second Edition. Indianapolis. SAMS. ISBN: 0-672-31341-3.

Crume, Jeff. Inside Internet Security – What Hackers Don't Want You To Know. London. Addison-Wesley. ISBN: 0-201-67516-1.

HTTP://www.darpa.mil

HTTP://www.ietf.org

HTTP://www.cnn.com

Cole, Eric. Hackers Beware. Indianapolis. New Riders. ISBN: 0-7357-1009-0.