A review on Intrusion Detection System and its future

Minakshi Sahu
Ph.D. in Comp. Sc. (Contd..)
Centurian University of technology
Paralakhemundi.

Susanta Kumar Das
Reader
P.G. Department of Computer Science
Berhampur University

Abstract: Intrusions in computer networks have driven the development of various techniques for intrusion detection systems (IDSs). Intrusion Detection Systems (IDS) have nowadays become a necessary component of almost every security infrastructure. Intrusion Detection is the process of monitoring and identifying attempted unauthorized systems access or manipulation. In this paper we try to summarize the various types of Intrusion detection systems available and explain some key points for each particular type of IDS available in the market today.

I. INTRODUCTION

Network Security has turned out to be a more complicated and challenging area in now a day's network world. When we think of designing a network a key issue to be taken into account is reventing it from the intruders. Intruders may be classified as inside and outside intruders. Inside intruders who belong to the same corporation, access the files of other persons by cracking that person's password, which leads to a heavy loss in network security. Outside intruders are those who don't belong to the corporation but they somehow try to access the important files of the corporation.

Apart, from the general classification of the intruders, we have three more classes of intruder's classification namely masquerader, misfeasor and clandestine user.

- Masquerader is an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
- Misfeasors are those legitimate users who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
- Clandestine users are those who seize supervisory control of the system and use this control to evade auditing and access controls or to suppress audit collection.

Some of the examples of intrusion attempts are

- Attempts to copy the password file at a rate exceeding once every other day.
- Suspicious remote procedure call (RPC) request at a rate exceeding once per week.
- Attempts to connect to non-existent "bait" machines at least every two weeks.

Firewalls generally don't detect the inside intruders because of which we go for the intrusion detection system. These system works based on the predefined set of rules, which are set by the network administrator. So we have to prevent this unauthorized access and increase the network security. To do so we have various tools available like firewalls, Intrusion Detection Systems (IDS).

II. INTRUSION DETECTION SYSTEMS

As defined by Heady et al. [4], an intrusion is *any set of actions that attempt to comprise the integrity, confidentiality or availability of a resource.*

Intrusion leads to violations of the security policies of a computer system, such as unauthorized access to private information, malicious break-in into a computer system, or rendering a system unreliable or unusable.

A full-blown network security system should include the following subsystems:

- Intrusion Detection Subsystem: Distinguishes a potential intrusion from a valid network operation.
- Protection Subsystem: Protects the network and security system itself from being compromised by the network intrusions.
- Reaction Subsystem: This part either traces down the origin of an intrusion or fights back the hackers.

A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly redundant). The premise behind intrusion detection systems is simple: Deploy a set of agents to inspect network traffic and look for the "signatures" of known network attacks. However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks are further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks.

Intrusion detection techniques while often regarded as grossly experimental, the field of intrusion detection has matured a great deal to the point where it has secured a space in the network defense landscape alongside firewalls and virus protection systems. While the actual implementations tend to be fairly complex, and often proprietary, the concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack.

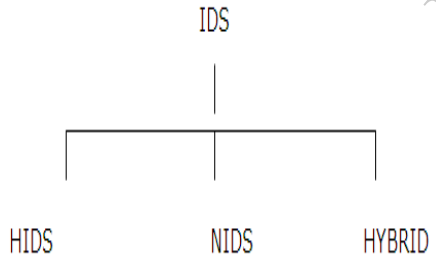
A. CHARACTERISTICS OF GOOD INTRUSION DETECTION SYSTEM

An intrusion detection system should address the following issues, regardless of what mechanism it is based on:

- 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.
- It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.
- On a similar note to above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted.
- It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.
- It must observe deviations from normal behavior.
- 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.
- 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.
- Finally, it must be difficult to fool.

III. CLASSIFICATION OF INTRUSION DETECTION SYSTEMS

Intrusion detection systems fall into one of three categories: Host Based Intrusion Detection Systems (HIDS), Network Based Intrusion Detection Systems (NIDS), and hybrids of the two.



- Host based Intrusion Detection System

Host-based intrusion detection started in the early 1980s before networks were as prevalent, complex and interconnected as they are today. In this simpler environment, it was common practice to review audit logs for suspicious activity. Intrusions were sufficiently rare that after the-fact analysis proved adequate to prevent future attacks.

Today's host-based intrusion detection systems remain a powerful tool for understanding previous attacks and determining proper methods to defeat their future application. Host-based IDS still use audit logs, but they are much more automated, having evolved sophisticated and responsive detection techniques. Host based IDS typically monitor system, event, and security logs on Windows NT and syslog in UNIX environments. When any of these files change, the HIDS compares the new log entry with attack signatures to see if there is a match. If so, the system responds with administrator alerts and other calls to action.

HIDS have grown to include other technologies. One popular method for detecting intrusions checks key system files and executables via checksums at regular intervals for unexpected changes. The timeliness of the response is in direct relation to the frequency of the polling interval. Finally, some products listen to port activity and alert administrators when specific ports are accessed. This type of detection brings an elementary level of network-based intrusion detection into the host-based environment.

Strengths of Host-Based Intrusion Detection Systems

a. Verifies success or failure of an attack
b. Monitors specific system activities
c. Detects attacks that network-based systems miss
d. Well-suited for encrypted and switched environments
e. Near-real-time detection and response
f. Requires no additional hardware
g. Lower cost of entry

- Network Based Intrusion Detection

Network-based intrusion detection systems use raw network packets as the data source. A network-based IDS typically utilizes a network adapter running in promiscuous mode to monitor and analyze all traffic in real-time as it travels across the network. Its attack recognition module uses four common techniques to recognize an attack signature:

a. Pattern, expression or byte-code matching,
b. Frequency or threshold crossing
c. Correlation of lesser events
d. Statistical anomaly detection

Once an attack has been detected, the IDS' response module provides a variety of options to notify, alert and take action in response to the attack. These responses vary by product, but usually involve administrator notification, connection termination and/or session recording for forensic analysis and evidence collection.

Strengths of Network Intrusion Detection Systems

a. Lowers cost of ownership
b. Detects attacks that host-based systems miss
c. More difficult for an attacker to remove evidence
d. Real-time detection and response
e. Detects unsuccessful attacks and malicious intent
f. Operating system independence

- Hybrid Based Intrusion Detection

Both network and host-based IDS solutions have unique strengths and benefits that complement each other. A next-generation IDS, therefore, must include tightly integrated host and network components. Combining these two technologies will greatly improve network resistance to attacks and misuse, enhance the enforcement of security policy and introduce greater flexibility in deployment options.

A hybrid IDS is a combination of network and host based intrusion detection systems. It provides an interesting blend of the strengths of both HIDS and NIDS. Exactly how this works varies from product to product, making it hard to define a hybrid IDS.

IV. PROS AND CONS OF INTRUSION DETECTION SYSTEMS

Pros of IDS are as follows:

- Detects external hackers and network based attacks.
- Offers centralized management for correlation of distributed attacks.
- Provides the system administrator the ability to quantify attacks.
- Provides an additional layer of protection.
- Provides defense in depth.

Cons of IDS are as follows:

- Generates false positives and negatives.
- Require full time monitoring.
- It is expensive
- Require highly skilled staff's.

V. THE FUTURE OF INTRUSION DETECTION

Intrusion detection fits in with a layered defense approach and intrusion detection technology is still growing and improving. Two things are certain—intrusion detection is still a long way from being mature. Massive changes are in store for both areas. Some of the areas within intrusion detection, in which substantial and beneficial progress is likely to occur. These areas include the following:

a. The continued reduction in reliance on signatures in intrusion detection
b. The growth of intrusion prevention
c. Advances in data correlation and alert correlation methods
d. Advances in source determination
e. Inclusion of integrated forensics functionality in IDSs.
f. Greater use of honeypots.

A. LOWER RELIANCE ON SIGNATURE-BASED INTRUSION DETECTION

The signature approach to intrusion detection, which traces back to the early 1990s, represents a major advance over the previous statistical-based approaches of the 1980s. Signatures are not only a relatively straightforward and intuitive approach to intrusion detection, but they are also efficient-often a set of only a few hundred signatures can result in reasonably high detection rates. Signature-based IDSs have proven popular and useful, so much so that you can count of some of these tools being available for a long time. Signature-based intrusion detection is beset with numerous limitations, however, including the following:

Because attacks have to occur before their signatures can be identified, signatures cannot be used in discovering new attacks. The "white hat" community is thus always one step behind the "black hat" community when it comes to new attack signatures.

Many signatures in IDSs are badly outdated. One can always "weed out" obsolete signatures, but doing so requires a reasonable amount of unnecessary effort; good IDS vendors do not include such signatures in their products' signature sets in the first place.

Some attacks do not have single distinguishing signatures, but rather a wide range of possible variations. Each variation could conceivably be incorporated into a signature set, but doing so inflates the number of signatures, potentially hurting IDS performance. Additionally, keeping up with each possible variation is for all practical purposes an impossible task.

Signatures are almost useless in network-based IDSs when network traffic is encrypted.

The black hat community is becoming increasingly better in evading signature-based IDSs.

B. INTRUSION PREVENTION

Intrusion prevention is another area that will grow dramatically in the future. Intrusion prevention is in its infancy. Anyone who thinks that IPSs and IDSs are diametrically opposed or that IPSs will eventually supplant IDSs is badly mistaken, however. An IDS is like a burglar alarm, something that provides information about past and ongoing activity that facilitates risk and threat assessment as well as investigations of suspicious and possibly wrongful activity. IPSs are designed to be defensive measures that stop or at least limit the negative consequences of attacks on systems and networks, not to yield the wealth of information that IDSs typically deliver.

One of the major, new offshoots of the last permutation of intrusion prevention discussed here is called "active defense. Active defense means analyzing the condition of systems and networks and doing what is appropriate to deal with whatever is wrong. According to Dave Dittrich of the University of Washington, there are four levels of active defense:

a. Local data collection, analysis, and blocking
b. Remote collection of external data
c. Remote collection of internal data
d. Remote data alteration, attack suppression, and "interdiction"

One of the most important (and controversial) facets of the active defense approach to intrusion prevention is determining the appropriate response. The notion of appropriate response includes a consideration called "proportionality of response," which ensures that the response is proportional to the threat. In the case of a host that is flooding a network with fragmented packets, blocking traffic sent from that host is almost certainly the most appropriate response. If several dozen hosts known to be operated by an ISP repeatedly attack an organization's network, blocking all the traffic from the range of IP addresses owned by that ISP might be the most appropriate response. Some advocates of the active defense approach even believe that if a remote host is repeatedly attacking an organization's network, counterattacking that host, perhaps by flooding it with fragmented packets, thereby causing it to crash is the appropriate course of action. Although intrusion prevention appears promising, (as mentioned) it is very much in its infancy. Attack stave-off rates for intrusion prevention systems are nowhere as high as they need to pose a major deterrent to attacks. Additionally, false

alarms can easily cause what effectively amounts to DoS within individual systems.

Intrusion prevention systems of the future are likely to be able to prevent a wider range of attacks, not only at the level of the individual host, but also within organizations' networks and possibly even within the Internet itself. The last possibility is particularly intriguing. Perhaps some organization such as the U.S. government's federal incident response team, FedCIRT, will continuously monitor all traffic bound for U.S. government sites and stop selectively malicious packets long before they reach the gateways of the government sites for which they are destined.

C. DATA AND ALERT CORRELATION

Data correlation is becoming increasingly important. IDSs, firewalls, personal firewalls, and TCP wrappers are each capable of generating large amounts of data; collectively, they are capable of overwhelming intrusion detection analysts with data. Data aggregation helps ensure that data are available in a single location; data correlation enables analysts to recognize patterns in these data. Although current data correlation methods are for the most part not very sophisticated, future data correlation is likely to become much better. How will data correlation algorithms need to change? Waltz and Llinas (in Multisensor Data Fusion, Boston: Artech House, 1990) have developed criteria for systems designed to fuse data must be able to, saying that these systems must be able to do the following:

- Distinguish parameters of interest from noise.
- Distinguish among different objects in space and time
- Adequately track and capture each desired type of event and data
- Sample the data and events of interest with sufficient frequency
- Provide accurate measurements
- Ensure that each variable that is measured adequately represents the desired
- Types of categories.
- Provide access to both raw and correlated data
- Preserve the temporal characteristics of data and events

It is unlikely that all systems designed to fuse data will meet every one of these requirements. The more of these requirements that a system meets, however, the more useful in data fusion/correlation it is likely to be. Currently, one of the greatest barriers to automated data fusion has been the lack of a common format for data from intrusion detection systems. Although common formats have been proposed, little agreement has resulted. Agreement upon a single data format would thus constitute a giant step forward.

D. SOURCE DETERMINATION

Source determination means determining the origin of network traffic. Given how easy it is to spoof IP addresses, any source IP address in conventional IP packets must be viewed with suspicion. Tools that fabricate packets, inserting any desired IP address into the IP headers, are freely available on the Internet. Many countermeasures, most notably strong authentication methods (such as the use of Smart Cards) and digital signatures, can remove doubt concerning the identity of individuals who initiate transactions, but they are not designed to identify the source IP addresses from which transactions originate. IPsec, the secure IP protocol, effectively removes any doubt concerning the validity of IP source addresses, but IPsec has, unfortunately, not grown in popularity in proportion to its many merits.

E. INTEGRATED FORENSICS CAPABILITIES

Forensics means using special procedures that preserve evidence for legal purposes. When people think of forensics, they normally envision investigators archiving the contents of hard drives to a machine that runs forensics software, making hard copies of audit logs, and labeling and bagging peripherals such as keyboards and mice. Many people fail to realize that IDSs are potentially one of the best sources of forensics data, especially if the IDSs capture and store keystrokes. A few IDS vendors are starting to build forensics capabilities into their products, capabilities that enable those who use the systems to make copies of IDS output, create a hash value of the output (to ensure its integrity), search it for special keywords or graphic content, and so on.

F. USE OF HONEYPOTS IN INTRUSION DETECTION

A honeypot is a decoy server that looks and acts like a normal server, but that does not run or support normal server functions. The main purpose of deploying honeypots is to observe the behavior of attackers in a safe environment, one in which there is (at least in theory) no threat to normal, operational systems. Having proven especially useful as a reconnaissance tool that yields information concerning what kinds of attacks is occurring and how often, honeypots have gained a great deal of acceptance within the information security arena.

VI. CONCLUSION

The intrusion detection and intrusion prevention arenas are extremely dynamic, with new findings, functions, and models being created all the time. A considerable amount of research on data visualization methods for intrusion detection data is also currently being conducted. At some point, the major breakthroughs from this research will be incorporated into IDSs of the future, resulting in output that will be much more useful in terms of identifying threat magnitudes, patterns of elements within incidents, and so forth.

REFERENCES

[1]. Biswanath Mukherjee, L Todd Heberlein and Karl N Levitt. Network Intrusion Detection, IEEE Network, May/June 1994, pages 26-41.
[2]. Carolyn Meinel, ABCs of IDSs, An article on Intrusion Detection, November 2002.
[3]. Dorothy E Denning. An Intrusion Detection Model. In IEEE Transactions on Software Engineering, Number 2, page 222, February 1987.
[4]. R. Heady, G. Luger, A. Maccabe, and B. Mukherjee. A Method To Detect Intrusive Activity in a Networked Environment. In Proceedings of the 14th National Computer Security Conference, pages 362-371, October 1991.

[5]. S. Wu and W. Banzhaf, “The Use of Computational Intelligence in Intrusion Detection Systems: A Review,” Applied Soft Computing, vol.10, p. 1-35, 2010.
[6]. Sandeep Kumar. Classification and Detection of Computer Intrusions. Ph.D. Dissertation, August 1995.
[7]. Sundaram A., "An Introduction to Intrusion Detection", http://www.acm.org/crossroads/xrds2-4/intrus.html
[8]. Teresa F Lunt. A survey of intrusion detection techniques. In Computers and Security, 12(1993), pages 405-418.