Information Security Technical Report (2005) 10, 134–139

Information Security Technical Report

Intrusion Detection Systems and Intrusion Prevention Systems

Andreas Fuchsberger

Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom

Introduction

The tremendous increase in cyber attacks linked with the dependence of modern organisation on the reliability and functionality of their IT structure has led to a change in mindset. As ''IT downtime'' is rising, the priorities are shifting.

As recent surveys show, cyber attacks — especially targeted to the networks — are real, and no longer an unlikely incident that only occur to few exposed networks of organisations in the limelight.

In the struggle to both maintain and implement any given IT security policy, professional IT security management is no longer able to ignore these issues, as attacks on networks become not only more frequent but also more devastating; in many organisations commercial success is directly related to the safe and reliable operation of their networks.

Furthermore, the annual FBI/CSI survey shows that even though virus based attacks are most frequent, attacks based on unauthorized access, as well as Denial of Service attacks both from internal as well as external sources, are increasing drastically.

Quite clearly Internet connection originated attacks are becoming a major concern, as attacks via internal systems and remote dial-ins are decreasing.

This fact finds further explanation, if we look at another research conducted by Carnegie Mellon University examining the relation and development of attack sophistication vs. Intruder technical knowledge.

The chart in Fig. 1 illustrates the trend, indicating that as the intrusion tools become powerful, the attackers require less knowledge themselves. An alarming observation is that as simple attacks are becoming less effective, multiple attacks are being combined to achieve their objectives.

Manual operations such as password guessing or exploitation of known vulnerabilities have become automated with sweepers, sniffers, packet spoofing and automated probes being used, as they are made available to the growing hacking community. It is no longer necessary to be an IT expert. A visit to a site like astalavista.com, diabolo 666 or equivalent chat rooms will offer an abundance of highly sophisticated, prefabricated hacking tools ready for deployment, including easy to understand instructions and ''tweaks'' in order to optimize impact.

In order to respond to this increasing threat the IT security industry provides a range of tools known as vulnerability assessment tools as well as Intrusion Detection Systems (IDS) and in its latest development; Intrusion Prevention Systems (IPS).

Vulnerability assessments and intrusion prevention/intrusion detection are just one aspect of IT security management. However, due to recent

E-mail address: a.fuchsberger@rhul.ac.uk

1363-4127/$ - see front matter
doi:10.1016/j.istr.2005.08.001

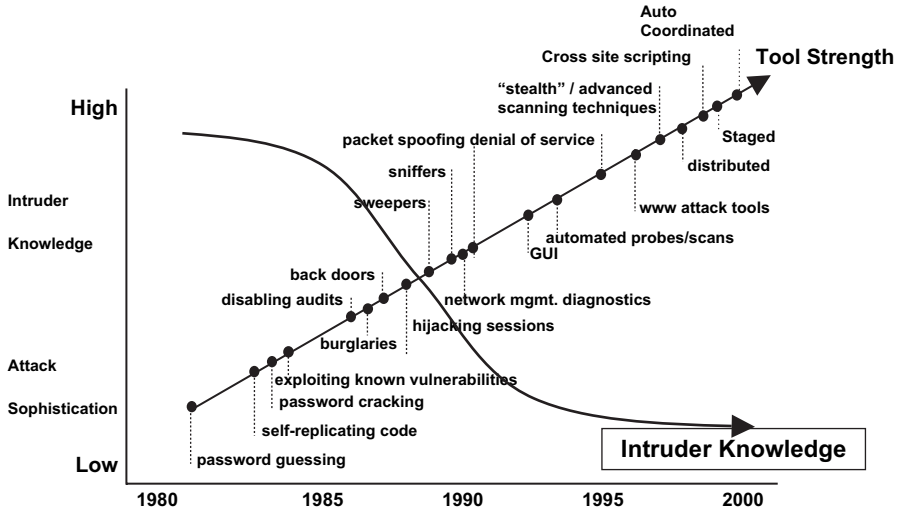

Figure 1 Attack sophistication vs. Intruder technical knowledge (Allen et al., 2000).

developments with the continuing spread of network connectivity, IT security management is faced with yet another challenge, requiring a structured approach for an adequate response.

Intrusion Detection Systems (IDS)

History and development

Before the development of modern IDS, intrusion detection consisted of a manual search for anomalies.

In order to do so, log files were examined for events that should or should not occur in regular operation of computer and network. To perform this task manually it is not only strenuous and possibly inaccurate, but also very time and manpower intensive. Therefore, it soon became necessary to develop automated log file readers, searching for logged events indicating irregularities or even an intrusion by unauthorized personnel. However, not every irregularity constituted an actual attack or intrusion, thus the whole process required more thorough investigation.

With further research it became possible to derive ''attack patterns'' from these irregularities, thus the first automated, pattern matching log file readers were developed. It is necessary to point out that this early ID Software (not Systems) was mostly individually developed, programmed and not widely spread, as only very few organisations were in need for this kind of technology before the dawn of the Internet age (Allen et al., 2000).

Again from the annual FBI/CSI survey, it can be easily seen that the source for attacks clearly shifted from internal sources to the Internet; in 2003, 70% of all attacks originated there in comparison to 31% from internal systems.

In consequence the emerging IT security industry introduced network based intrusion detection, which in essence follows the same principal of pattern matching as host based intrusion detection, not by reading log files of a given host, but by monitoring network traffic, searching for attack patterns in the TCP/IP packet stream.

Until this point, intrusion detection had been a post factum analysis of log files, allowing forensic analysis relatively long after the actual event with possible adjustments to the infrastructure.

Due to the availability of adequate processing speed it now became possible not only to look for attack patterns after the event had occurred, but also to monitor in ''realtime'' and trigger alerts if intrusions were detected.

Due to market demand, the IT security industry now started to develop former prototype software into actual Intrusion Detection Systems, consisting of user friendly interfaces, methods to update attack patterns, various methods of alerts and even some automatically triggered reactions or actual prevention methods, able to stop attacks in progress.

Due to the financial losses from computer downtime, loss of image, or even confidential data being affected, in recent years the demand for not only being alerted in the event of an attack, but also to prevent the attack altogether has become an absolute necessity. Especially with the introduction of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, the market demands have grown stronger for Intrusion Prevention Systems (IPS) rather than mere intrusion detection.

These Intrusion Prevention Systems are presently the technological edge of the IDS technology and are found both as stand alone products as well as part of modern firewall systems.

Another observation here is that the current trend of the IT security industry to move from software solutions to appliance based solutions has resulted in a shift of emphasis for example in the firewall industry, which in some instances is providing IDS and IPS as part of their solutions.

A 2002 Gartner Group IT security study claims that any firewall solution not incorporating at least network based IDS would disappear from the market. This shift of emphasis from single function solutions to multipurpose devices is not only a reaction to market demands in terms of cost of ownership, but also a sufficient proof that IDS/IPS solutions have become a key factor in the IT security world.

Methods of intrusion detection

In order to discuss IDS properly it is necessary to distinguish between the different IDS.

Behaviour-based IDS
Statistical Anomaly Detection (or behaviour-based detection) is a methodology where statistical techniques are used to detect penetrations and attacks these begin by establishing base-line statistical behaviour: what is normal for this system? They then gather new statistical data and measure the deviation from the base-line. If a threshold is exceeded, issue an alarm.

Examples of what a behaviour-based IDS might detect:

- the number of failed login attempts at a sensitive host over a period;
- a burst of failed attempts to login: an attack may be under way; or maybe the admin just forgot his password?

This raises the issue of false positives (an attack is flagged when one was not taking place — a false alarm) and false negatives (an attack was missed because it fell within the bounds of normal behaviour). Normal behaviour may overlap with forbidden behaviour. Legitimate users may deviate from the base-line, causing false positives (e.g. user goes on holiday, or works late in the office, or forgets password, or starts to use new application).

If the base-line is adjusted dynamically and automatically, a patient attacker may be able to gradually shift the base-line over time so that his attack does not generate an alarm.

Other issues relevant to behaviour-based IDS are that they are difficult to implement, may be more resource-hungry than knowledge-based IDS and may require frequent fine-tuning by administrator. Today there seems to be lots of research, however there are no known commercial products in use today.

Knowledge-based IDS
Most commercial IDS look for attack signatures: specific patterns of network traffic or activity in log files that indicate suspicious behaviour are known as knowledge-based or misuse detection IDS.

Example signatures might include:

- a number of recent failed login attempts on a sensitive host;
- a certain pattern of bits in an IP packet, indicating a buffer overflow attack;
- certain types of TCP SYN packets, indicating an SYN flood DoS attack.

When an IDS looks for attack signatures in network traffic, it is called a network-based IDS (NIDS). When an IDS looks for attack signatures in log files of hosts, it is called a host-based IDS (HIDS). Naturally, the most effective Intrusion Detection System will make use of both kinds of information.

Host based IDS
Derived from mere log file analysers modern host based Intrusion Detection Systems are designed as host based applications running in the background of presumed critical, sensitive hosts, such as Mail Servers, DNS Servers, web servers, database servers, etc. Especially in e-commerce environments, where sensitive data are stored or availability is critical, host based IDS are found predominantly.

The components are the actual host based IDS application and an IDS management station, where the application is administered from as well as alerts are sent to for further action.

Host based IDS serves the purpose to detect attack patterns that can only or easier to be found on a host level basis.

Network based IDS
A network-based IDS monitors network traffic on packet level. The components are the network based IDS software, running on a dedicated host, connected to the network traffic with a network interface, and again an IDS management station, where the software is administered and alerts are sent to.

In order not to become a target for attack itself it has become standard to ''conceal'' the system, by setting the network interface into ''stealth'' mode as well as ''promiscuous'' mode, the interface itself has no IP address, the IDS probe cannot be addressed by other hosts, but merely copies all passing traffic into its RAM memory.

Here the packets are examined both according to header and payload searching for attack signatures, stored in the IDS Attack signature database, which is the vital part of any IDS software.

If a match is found, the alert is send to the management station via SNMP trap or similar for further action. Due to the delivery method of the alert, some IDS allow for integration with network and security management consoles, such as Tivoli, HP OpenView, NetIQ.

Some IDS even allow an automated response to a recognised attack, such as a connection reset to the source IP or even the automatic reconfiguration of the firewall, e.g. by blocking the affected port.

Intrusion Prevention Systems (IPS)

To many IDS users great dismay, seeing an attack as it occurs is one thing, stopping it is another.

If one might assume that the highest priority of any IT security activity in this area is to prevent an attack and possible related disaster, IDS often deliver little to meet this demand.

Until recently the most IDS could do was to send a reset package to possibly terminate the ongoing attack session, or possibly reconfigure a firewall by simply closing the appropriate port of the affected service. These measures of course were at least partially unsatisfactory e.g. if the attack was not using a session oriented protocol such as UDP.

The term Intrusion Prevention Systems (IPS) is relatively new, often pushed by the marketing departments to move the IDS manufactures away from the negative image of Intrusion Detection Systems. They are essentially a combination of access control (firewall/router) and Intrusion Detection Systems, this alliance coming naturally as both technologies often use shared technologies.

Nearly all modern commercial firewalls use ''stateful'' inspection and commercial IDS use signature recognition. Both technologies need to ''look deep into the packet'' before making an access decision in the case of a firewall or raise an alarm in the case of an IDS. To make this possible in an efficient manner, sufficient processing power is necessary, which has become more easily available in recent years. An IPS works like an in-line network IDS allowing for instant access control policy modifications.

As nearly all modern firewalls follow the principal of stateful inspection, from analysing the state of the applied protocol it is a relatively small step to analyse for attack signatures on the same level.

The technologies are so close that in a 2004 study the Gartner Group claimed that by 2005 only integrated firewalls with IDS (i.e. IPS) will survive.

With the arrival of DDoS attacks such as the recent ''W32.Blaster.Worm'' the market trend is clearly focussing on IPS rather than IDS.

Predominantly an IPS is not only found on security appliances, such as certain firewalls, but also on stand alone appliances delivered. The idea to implement IPS here is driven by commercial as well as technical aspects. To-date IPS have had the most success with ''flood'' (i.e. DoS) type attacks.

For example, in the case of the IPS Appliance ''Attack Mitigator'' by Toplayer which was derived from a former layer 7 switch, it is planned to extend the IPS functionality to also incorporate IDS using the open source Snort IDS, in order to extend the comparatively small amount of attacks that can be prevented to ''at least'' see the attacks that cannot be prevented.

With the progress of technical sophistication in the hacker methods, especially modern DoS or DDoS attacks, attack signatures are not easily detected. Generically one may assume that an attack signature is derived from a stream of packets with a malicious content in both the packet header and the packet payload.

Modern flood attacks such as ''trin00'' and ''Stacheldraht'' in essence direct perfectly legal http packets to the target. Only the indication of the IP source address and the sheer amount of http request gave an indication that the whole progress is an attack.

Definition of an IPS

An IPS can be defined as an in-line product that focuses on identifying and blocking malicious network activity in real time. In general, there are two categories:

- rate-based products; and
- content-based (also referred to as signature- and anomaly-based).

The devices often look like firewalls and often have some basic firewall functionality. But firewalls block all traffic except that for which they have a reason to pass, whereas IPS pass all traffic except that for which they have a reason to block.

Rate-based IPS

Rate-based Intrusion Prevention Systems block traffic based on network load, for example, too many packets, or too many connects, or too many errors. In the presence of too much of anything, a rate-based IPS kicks in and blocks, throttles or otherwise mediates the traffic. Most useful rate-based IPS include a combination of powerful configuration options with range of response technologies. For example, limit queries to the DNS server to 1000 per second and/or offer other simple rules covering bandwidth and connection limiting.

A rate-based Intrusion Prevention System can set a threshold of maximum amount of traffic to be directed at a given port or service. If the threshold is exceeded, the IPS will block all further traffic of the source IP only, still allowing other users (source IPs) to use that service.

Disadvantages of rate-based IPS
The biggest problem with deploying rate-based IPS products is deciding what constitutes an overload. For any rate-based IPS to work properly, the network owner needs to know not only what ''normal'' traffic levels are (on a host-by-host and port-by-port basis) but also other network details, such as how many connections their web servers can handle. However, most commercial products do not yet provide any help in establishing this base-line behaviour, but require the services of a ''trained'' product specific systems engineer who often spend hours on site setting-up the IPS. Because rate-based IPS require frequent tuning and adjustment, they will be most useful in very high-volume Web, application and mail server environments.

Content-based products

Content-base Intrusion Prevention Systems block traffic based on attack signatures and protocol anomalies; they are the natural evolution of the Intrusion Detection Systems and firewalls. They block the following:

- Worms — (e.g. Blaster and MyDoom) that match a signature can be blocked.
- Packets that do not comply with TCP/IP RFCs can be dropped.
- Suspicious behaviour such as port scanning triggers the IPS to block future traffic from a single host.

The best content-based IPS offer a range of techniques for identifying malicious content and many options for how to handle the attacks, such as simply dropping bad packets to dropping future packets from the same attacker, and advanced reporting and alerting strategies.

As content-based IPS offer IDS-like technology for identifying threats and blocking them, they can be used deep inside the network to complement firewalls and provide security policy enforcement as they often require less manual maintenance and fine-tuning to perform a useful function than their rate-based cousin.

Future developments

Recently, the IT security market is experiencing a definite trend towards appliance solutions where firewall vendors as well as IDS vendors attempt to integrate various IT security solutions into one, usually proprietary appliance, running on proprietary or specifically hardened OS appliances.

The advantage is a lower cost of ownership as the vendor offers a dedicated support with hardware replacement on the next business day. Aside from that proprietary hard and software is less likely to be hacked in comparison to common software such as Unix and Microsoft derivates.

This approach is interesting to the small and medium enterprise market, where the total IT budget may be equal to the cost of one high-end firewall application.

Some of these one appliance solutions attempt to deliver URL filtering, stateful inspection firewalling, VPN gateway, content filtering (virus) as well as IDS and IPS functionalities.

In recent years IT security management tools have arrived on the horizon with the intention to display the truly important, security relevant information gathered from all relevant sources throughout the network on a single central console.

In essence, the architecture consists of a central console that receives alerts from various log parsing agents distributed throughout the network. The intriguing approach of these tools is that aside from the classical pattern matching conducted by various IDS, relevant log file data from routers and OS are parsed and examined for information the user may specifically look for. Thus, it resembles a type of customizable host based IDS with the ability to create customized patterns that are not ''off the rack'' but instead represent the individual situation and concerns of the network.

Regardless of these deficiencies the vendors of these management tools have recognised a growing need for consolidating IT security relevant information, vendor-independently, as a latent need.

Considering the vast amount of IT security issues ranging from classic firewall, over content filtering, virus detection, VPN gateways, vulnerability assessment, and authentication issues to IDS, the amount of supposed security relevant information is enormous.

Assuming the further development of combined attacks such as ''W32.Blaster.Worm'', which eventually become orchestrated, the need for cooperation between vendors, manifesting itself in common API allowing for centralized management and correlation will become vital.

Summary

Hacking attacks, be that from the inside of a given network by a disgruntled employee or by a hacker via an Internet connection, are facts of the IT world. The same applies to DoS and especially DDoS attacks, in the latest state even combining delivery methods from other known cyber attacks such as a worm.

The trend manifested in various surveys indicates that these attacks are more likely to increase rather than to diminish.

IDS/IPS are not intended to substitute or compensate for the lack of suitable IT security management structure, or can they compensate for flawed integration of other IT security necessities such as faulty key management, or a lack of user awareness to IT security issues.

Intrusion Detection Systems can be seen as an additional second line of defence complementing traditional perimeter security controls for defending a network from attack. With the increased ''deperimeterisation'' it is becoming more difficult to apply security access controls. Intrusion Detection Systems can be used to alarm for attacks within a network but provide little or no mechanism for actively acting on an attack in progress. Intrusion Prevent Systems provide a mechanism for acting on attacks underway by combing IDS and firewall technology.

Only if all IT security components are professionally maintained, frequently revaluated, manageable and flexible to be adapted to future changing needs, one may assume to be on the right path, as IT security still is, and probably always will be, a route to follow rather than a destination to be reached.

References

Allen J, Christie A, Fithen W, McHugh J, Pickel J, Stoner E. State of the practice of intrusion detection technologies, Carnegie Mellon University Technical Report CMU/SEI-99-TR-028; 2000.

CSI/FBI annual computer crime and security survey. Computer Security Institute, <http://www.gocsi.com>.

Andreas Fuchsberger is a lecturer in the Information Security Group (ISG) at Royal Holloway, University of London, where he lectures in the areas of computer and network security as well as for the new academic year a new course on software security. He has over 18 years of experience in teaching and running training classes in IT security architecture, design and programming. He has published articles on programming and network security, intrusion detection/prevention and vulnerability analysis. He rejoined the ISG in 2003 after working for a number of IT security product manufactures in Europe and the US. Andreas holds MBCS CITP and CISSP credentials. He is a Chartered Engineer (CEng) of the Engineering Council UK and a registered European Engineer (Eur.Ing).