Importance of Intrusion Detection System (IDS)

Asmaa Shaker Ashoor (Department computer science, Pune University)
Prof. Sharad Gore (Head department statistic, Pune University)

Abstract: Intruders computers, who are spread across the Internet have become a major threat in our world. The researchers proposed a number of techniques such as (firewall, encryption) to prevent such penetration and protect the infrastructure of computers, but with this, the intruders managed to penetrate the computers. IDS has taken much of the attention of researchers, IDS monitors the resources computer and sends reports on the activities of any anomaly or strange patterns. The aim of this paper is to explain the stages of the evolution of the idea of IDS and its importance to researchers and research centres, security, military and to examine the importance of intrusion detection systems and categories, classifications, and where can put IDS to reduce the risk to the network.

Keywords: Intrusion detection, IDS, anomaly & misuse, NID

INTRODUCTION

Security is an important issue for all the networks of companies and institutions at the present time and all the intrusions are trying in ways that successful access to the data network of these companies and Web services and despite the development of multiple ways to ensure that the infiltration of intrusion to the infrastructure of the network via the Internet, through the use of firewalls, encryption, etc.

But IDS is a relatively new technology of the techniques for intrusion detection methods that have emerged in recent years. Intrusion detection system’s main role in a network is to help computer systems to prepare and deal with the network attacks.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

The purpose of IDS is to help computer systems on how to deal with attacks, and that IDS is collecting information from several different sources within the computer systems and networks and compares this information with pre-existing patterns of discrimination as to whether there are attacks or weaknesses.

INTRUSION DETECTION SYSTEMS: A BRIEF HISTORY

The goal of intrusion detection is to monitor network assets to detect anomalous behaviour and misuse in network. This concept has been around for nearly twenty years but only recently has it seen a dramatic rise in popularity and incorporation into the overall information security infrastructure. Beginning in 1980, with James Anderson's paper, Computer Security Threat Monitoring and Surveillance, the intrusion detection was born. Since then, several polar events in IDS technology have advanced intrusion detection to its current state.

James Anderson's seminal paper, was written for a government organization, introduced the notion that audit trails contained vital information that could be valuable in tracking misuse and understanding of user behaviour. With the release of this paper, the concept of "detecting" misuse and specific user events emerged. His insight into audit data and its importance led to tremendous improvements in the auditing subsystems of virtually every operating system. Anderson's hypothesize also provided the foundation for future intrusion detection system design and development. His work was the start of host-based intrusion detection and IDS in general.

In 1983, SRI International, and Dr. Dorothy Denning, began working on a government project that launched a new effort into intrusion detection system development. Their goal was to analyze audit trails from government mainframe computers and create profiles of users based
upon their activities. One year later, Dr. Denning helped to
develop the first model for intrusion detection, the
Intrusion Detection Expert System (IDES), which provided
the foundation for the IDS technology development that
was soon to follow.

In 1984, SRI also developed a means of tracking and
analyzing audit data containing authentication information
of users on ARPANET, the original Internet. Soon after, SRI
completed a Navy SPAWAR contract with the realization of
the first functional intrusion detection system, IDES. Using
her research and development work at SRI, Dr. Denning
published the decisive work, An Intrusion Detection Model,
which revealed the necessary information for commercial
intrusion detection system development. Her paper is the
basis for most of the work in IDS that followed. The
subsequent iteration of this tool was called the Distributed
Intrusion Detection System (DIDS). DIDS augmented the
existing solution by tracking client machines as well as the
servers it originally monitored. Finally in 1989, the
developers from the Haystack project formed the
commercial company, Haystack Labs, and released the last
generation of the technology, Stalker. Crosby Marks says
that “Stalker was a host-based, pattern matching system
that included robust search capabilities to manually and
automatically query the audit data.” The Haystack
advances, coupled with the work of SRI and Denning,
greatly advanced the development of host-based intrusion
detection technologies.

Commercial development of intrusion detection
technologies began in the early 1990s. Haystack Labs was
the first commercial vendor of IDS tools, with its Stalker
line of host-based products. SAIC was also developing a
form of host-based intrusion detection, called Computer
Misuse Detection System (CMDS). Simultaneously, the Air
Force’s Crypto logic Support Canter developed the
Automated Security Measurement System (ASIM) to
monitor network traffic on the US Air Force’s network.
ASIM made considerable progress in overcoming
scalability and portability issues that previously plagued
NID products. Additionally, ASIM was the first solution to
incorporate both a hardware and software solution to
network intrusion detection. ASIM is still currently in use
and managed by the Air Force’s Computer Emergency
Response Team (AFCERT) at locations all over the world.
As often happened, the development group on the ASIM
project formed a commercial company in 1994, the Wheel
Group. Their product, Net Ranger, was the first
commercially viable network intrusion detection device.

The intrusion detection market began to gain in popularity
and truly generate revenues around 1997. In that year, the
security market leader, ISS, developed a network intrusion
detection system called Real Secure. A year later, Cisco
recognized the importance of network intrusion detection
and purchased the Wheel Group, attaining a security
solution they could provide to their customers. Similarly,
the first visible host-based intrusion detection company,
Centrex Corporation, emerged as a result of a merger of the
development staff from Haystack Labs and the departure of
the CMDS team from SAIC. From there, the commercial
IDS world expanded its market-base and a roller coaster
ride of start-up companies, mergers, and acquisitions ensued.

![Cyber Incidents Reported to US-CERT in 2006 - 2008, estimates 2009 -2010](chart.png)

**Figure 1: Number of incidents reported**

The above chart from US-CERT shows how the cyber
incidents rose in current internet network environment; this
gives requirement of IDS deployment in network security
model.

Network intrusion detection actually deals with
information passing on the wire between hosts. Typically
referred to as “packet-sniffers,” network intrusion detection
devices intercept packets travelling in and out in network
along various communication mediums and protocols,
usually TCP/IP. Once captured, the packets are analyzed in
a number of different ways. Some IDS devices will simply
compare the packet to a signature database consisting of
known attacks and malicious packet “fingerprints”, while
others will look for anomalous packet activity that might
indicate malicious behaviour.
The IDS basically monitors network traffic for activity that falls within the banned activity in the network. The IDS main job is to give alerts to network admins for allowing them to take corrective action, blocking access to vulnerable ports, denying access to specific IP addresses or shutting down services used to allow attacks. This is nothing but front line weapon in the network admin's war against hackers. This information is then compared with predefined blueprints of known attacks and vulnerabilities.

Categories of intrusion detection system

Intrusion detection systems are classified into three types:

1. **Signature based detection systems**
   
   Signature based detection system (also called misuse based), this type of detection is very effective against known attacks, and it depends on the receiving of regular updates of patterns and will be unable to detect unknown previous threats or new releases.

2. **Anomaly based detection system**
   
   This type of detection depends on the classification of the network to the normal and anomalous, as this classification is based on rules or heuristics rather than patterns or signatures and the implementation of this system we first need to know the normal behavior of the network.

3. **Specification based detection system**
   
   Anomaly based detection system unlike the misuse based detection system because it can detect previous unknown threats, but the false positives to rise more probably.

CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Intrusion detection systems are classified into three types:

1. **Host based IDS (HIDS)**
   
   This type is placed on one device such as server or workstation, where the data is analyzed locally to the machine and are collecting this data from different sources. HIDS can use both anomaly and misuse detection systems.

2. **Network based IDS (NIDS)**
   
   NIDS are deployed on strategic points in network infrastructure. The NIDS can capture and analyze data to detect known attacks by comparing patterns or signatures of the database or detection of illegal activities by scanning traffic for anomalous activity. NIDS are also referred as “packet-sniffers”. Because it captures the packets passing through communication mediums.

3. **Hybrid based IDS**
   
   The management and alerting from both network and host-based intrusion detection devices, and provide the logical complement to NID and HID - central intrusion detection management.
CONCLUSION

An intrusion detection system is a part of the defensive operations that complements the defences such as firewalls, UTM etc. The intrusion detection system basically detects attack signs and then alerts. According to the detection methodology, intrusion detection systems are typically categorized as misuse detection and anomaly detection systems. The deployment perspective, they are be classified in network based or host based IDS. In current intrusion detection systems where information is collected from both network and host resources. In terms of performance, an intrusion detection system becomes more accurate as it detects more attacks and raises fewer false positive alarms.

REFERENCES