

Network Intrusion Prevention Systems

Judy Weng

Faculty, Northwestern Polytechnic University

Glen Qin

Faculty, Northwestern Polytechnic University

ABSTRACT

Over the past several years, networked systems have grown considerably in size and complexity, and become susceptible to attack. At the same time, the knowledge, tools and techniques available to attackers have also grown in proportion. Unfortunately, defensive techniques have not evolved as quickly due to the reactive nature in which they are used. Current security technologies are reaching their limitations, and more innovative solutions are required to deal with current and future classes of threats.

In this paper, The basic computer network concepts and network-based intrusion detection/prevention systems are described, so the readers can define the criterion in selecting an intrusion detection system.

Keywords: Computer Network Architecture, Network Secure, Security Services, Firewall, IDS, IPS

DEFINITION OF A COMPUTER NETWORK

“A computer network is composed of multiple computers connected together using a telecommunication system for the purpose of sharing data, resources and communication. For instance, a home computer network may consist of two or more computers that share files and a printer. The size and scalability of any computer network are determined by the hardware used as well as which protocols are being implemented. An intrusion is an active sequence of related events that deliberately try

to cause harm, such as rendering a system unusable, accessing unauthorized information, or manipulating such information.”

DEFINITION OF SECURITY

The word security can mean different things when taken in different contexts. For instance, we talk about security in relation to national policy, personal safety, financial risk, and privacy of communication. We even use the word to describe our state of emotions. So what is the common thread that links these definitions? Why do we use the same word to describe protection from muggers and protection from hackers?

Security Services and Security Mechanisms

The basic security services in OSI (Bentham, 2002) communications include the following:

1. Authentication: This service may be used to prove that the claimed identity of a communicating principal is valid or that the claimed source of a data unit is valid (i.e., data origin authentication) (Bungale, Goodell and Roussopoulos).
2. Access control: This service can be used to protect the information assets and resources available via OSI from unauthorized access.
3. Data confidentiality: This service protects the data from disclosure to unauthorized principals.
4. Data Integrity: This service ensures that during their transmission the data are not altered by unauthorized principals. This service may have several forms. Connection integrity with recovery provides integrity of the data and also detects modification, insertion, deletion, and replay of data. Selective field connection integrity provides integrity for selective data fields within a connection. Connectionless versions of the above services also exist for connectionless data units (Zhang and Janakiraman).
5. Non-repudiation: This service ensures that a principal cannot deny the transmission or the receipt of a message. This service may take one or both of two forms. With nonrepudiation with proof of origin, the recipient of the data is provided with proof of the origin of data, so that the sender cannot later deny that he or she sent the particular data. With nonrepudiation with proof of delivery, the sender of the data is provided with proof of the delivery of data, so that the receiver cannot later deny having received the particular data.

The implementation of the security services is provided through security mechanisms. These can also be divided into several categories:

1. Encipherment Mechanisms: These mechanisms provide data confidentiality services by transforming the data to forms not readable by unauthorized principals. The encipherment mechanisms can also complement a number of other security mechanisms. The encipherment algorithms are generally divided into symmetric (or secret key), where the same secret key is used for both encipherment and decipherment, and asymmetric (or public key), where two mathematically bounded

keys are used: the public key for encipherment and the private, or secret, key for decipherment. Knowledge of the public key does not imply knowledge of the secret key. Issues related with the management of the keys are raised both in symmetric and asymmetric encipherment mechanisms. Examples of symmetric encipherment algorithms are AES, Twofish, and RC5, where examples of asymmetric encipherment algorithms are RSA and EIGamal (Edney and Arbaugh, 2004).

2. Digital Signatures: Digital signatures are the electronic equivalent of ordinary signatures in electronic data. Such mechanisms are constructed by properly applying asymmetric encipherment. The decipherment of a data unit with the private key of an entity corresponds to the signature procedure of the data units. The result is the digital signature of the particular data unit produced by the holder of the private key. The encipherment of the generated digital signature with the corresponding public key of the particular entity corresponds to the verification procedure. Digital signatures can be used to provide peer entity authentication and data origin authentication, data integrity, and nonrepudiation services. RSA, EIGamal, and DSA are example of signature algorithms (Skavos and Zhang, 2007).

3. Access Control Mechanism: The access control mechanisms are used to provide access control services. These mechanisms may use the authenticated identity of an entity or other information related with an entity in order to determine and enforce the access rights of the entity. The access control mechanisms may also report unauthorized access attempts are part of a security audit trail.

4. Data Integrity Mechanisms: These mechanisms provide data integrity services by appending some kind of checksums to the data which may prove alternation of the data. Data integrity may involve a single data unit or field or a stream of data units or fields. In general, provision of the second without the first is not practical (Zhou, Karunasekera and Leckie).

5. Authentication Mechanisms: These mechanisms provide authentication services by assuring the identity of a principal. Examples of such mechanisms are passwords, cryptographic techniques, and biometrics.

6. Traffic-Padding Mechanisms. These mechanisms provide protection from traffic analysis attacks. Several network protocols and security mechanisms include padding mechanisms to protect the exchanged communication. These can be effective only if the traffic padding is protected by a confidentiality service.

7. Routing Control Mechanisms: These mechanisms allow the selection of a specific route for the communicating data, either dynamically or statistically through prearranged routes. Moreover, by applying security policies, data carrying certain security labels may be routed through certain sub-networks, relays, or links. Hackers, viruses, and malicious programs frequently exploit the security vulnerabilities of routing protocols when launching network security attacks.

8. Notarization Mechanisms: *Notarization* mechanisms work in a manner analogous to that of a notary public. They depend on the availability of a trusted third-party entity and an underlying protocol or mechanism that is sufficient to allow this third party to verify a given transaction. Time-stamping services would be an example of such a notarization mechanism. A notarization mechanism may be supported by other mechanisms such as digital signatures, encipherment, or integrity mechanisms.

Table 1 describes the relationship between security services and security mechanisms. If a mechanism is indicated as appropriate for a given service, this may be either on its own or in combination with other mechanisms.

| Service | Encipherment | Digital Signature | Access Control | Data Integrity | Authentication Exchange | Traffic Padding | Routing Control | Notarization |
|---------------------------------------|--------------|-------------------|----------------|----------------|-------------------------|-----------------|-----------------|--------------|
| Peer entity authentication | X | X | | | X | | | |
| Data origin authentication | X | X | | | | | | |
| Access control service | | | X | | | | | |
| Connection confidentiality | X | | | | | | X | |
| Connectionless confidentiality | X | | | | | | X | |
| Selective field confidentiality | X | | | | | | | |
| Traffic flow confidentiality | X | | | | | X | X | |
| Connection integrity with recovery | X | | | X | | | | |
| Connection integrity without recovery | X | | | X | | | | |
| Selective field connection integrity | X | | | X | | | | |
| Connectionless | X | X | | X | | | | |

| | | | | | | | | |
|-------------------------------------------|---|---|--|---|--|--|--|---|
| integrity | | | | | | | | |
| Selective field connectio nless integrity | X | X | | X | | | | |
| Nonrepud iation of origin | | X | | X | | | | X |
| Nonrepud iation of delivery | | X | | X | | | | X |

Table 1: Relationship between Security Services and Mechanisms

Network Security Attacks

Network security attacks of various types happen every day on networks. In order for huge denial of service (DoS) attacks to take place (Mayank and Cascade), literally thousands of networks worldwide must have been compromised. Those perpetrating such attacks don't use their own bandwidth. Using their own networks would mean being caught pretty quickly. It doesn't take long to tie an IP address to a name and address (Mirkovic, Dietrich, Dittrich and Reiher, 2005).

Some network security attacks are listed below (Douligeris and Serpanos, 2007):

- a. Email Based Network Security Attacks
- b. Logon Abuse Attacks
- c. Spoofing Attacks
- d. Intrusion Attacks (Vlachos, Androutsellis-Theotokis and Spinellis).
- e. Denial of Service (DoS) Network Security Attacks
- f. Worms & Trojans

Network Security Methods

When we think of network security, we need to think of the perimeter, which might contain any or all of the following (Dubin):

- Static Packet filter
- Stateful firewall
- Proxy Firewall
- IDS
- VPN device

INTRUSION DETECTION SYSTEM

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activities. The intrusion-detection part of the name is a bit of a misnomer, as an IDS does not actually detect intrusions – it detects activities in traffic that may or may not be an intrusion. Intrusion detection is typically one part of an overall protection system that is installed around a system or device – it is not a stand-alone protection measure (Endorf, Schultz and Mellander, 2004).

An intrusion can generally be described as the act of entering without permission. Thus intrusion detection is the process of identifying such unauthorized action. However, before one can identify if something is unauthorized, one must understand what is authorized. Thus in the specific case of computer networks, the goal of intrusion detection is to identify network communications that violate the operational policy of the computer network. If such a policy is poorly defined or not defined at all, then little can be expected of intrusion detection.

The two major benefits of network security can be considered as visibility and control. Control is provided by firewalls and access control lists in routers, among other things. Control should be an instantiation of the operational policy, but often, due to human error or other reasons, loopholes exist in policy. Visibility allows one the ability to recognize when and where those loopholes exist and provides the intelligence to modify control systems appropriately (Northcutt, 1999).

STANDARD IDS SYSTEM

Figure 1 shows the standard IDS System.

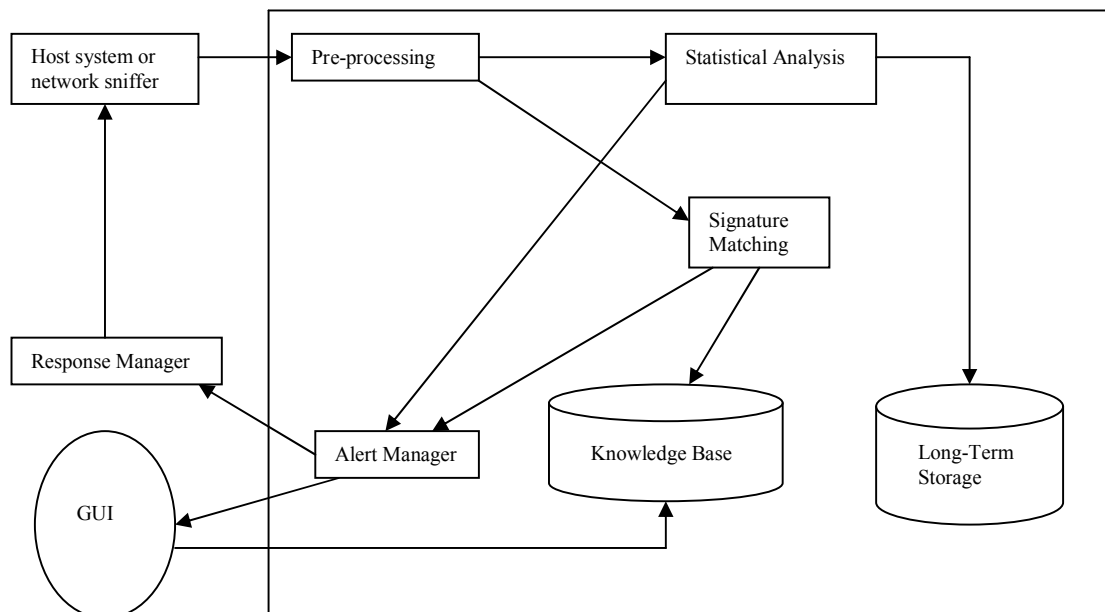


Figure 1: A standard IDS System.

TYPES OF IDS SYSTEMS

IDSs fall into one of three categories: host-based intrusion-detection system (HIDS), network-based intrusion-detection system (NIDS), and a hybrid of the two.

The Hierarchical Intrusion Detection (HIDS) system is a distributed anomaly detection system that bases decisions on statistical preprocessing and neural network classification. The hierarchy in HIDS is related to the way it is deployed across several scopes of network tiers. Each tier contains several intrusion/fault detection agents (IDAs), which monitor network activity and make individual decisions based on input from lower-level IDAs and its own analysis. The output is reported to higher level IDAs and included in the user interface.

HIDS arrives at its decisions through the use of a statistical preprocessor and a neural network classifier. The statistical preprocessor develops a stimulus vector in relation to preexisting reference models. The stimulus vector is then analyzed by the neural network classifier to decide whether the event is normal or not.

A HIDS system will require some software that resides in the system and can scan all host resources for activity; some just scan syslog and event logs for activity. It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.

NIDS systems are designed to examine network traffic to identify threats by detecting scans, probes, and attacks. One of the goals of intrusion detection is to assist the user in ensuring that the systems can handle those threats properly. A NIDS receives all packets in a particular network segment, including switched networks via one of several methods, such as taps or port mirroring. It carefully reconstructs the streams of traffic to analyze them for patterns of malicious behavior. Most NIDSs are equipped with facilities to log their activities and report or alarm on questionable events. In addition, many high-performance routers offer NID capability.

The early IDS work discussed in the previous section are forms of host-based IDSs, as mentioned earlier. There are several problems with host-based IDSs:

1. Scalability: If an entire organization is to be monitored, the host-based IDS must be installed on each computer in the organization.
2. Resources: Host-based IDSs must dedicate some portion to detection processing, potentially taking clock cycles away from conducting the actual organizational operations.
3. Infrastructure Protection: Host-based IDSs do detect attacks against network infrastructure.

4. Forensics: If a host is comprised, then the resident IDS must be considered compromised. Consequently, these logs are of questionable value in legal proceedings.

These concerns and others led to the development of the first NIDS by Heberlein et al. in 1989. Heberlein et al's system, dubbed the network security monitor (NSM), takes advantage of the broadcast nature of the early Ethernet to monitor network communications at a single point instead of each host. NSM can be considered a hybrid IDS in that it incorporates ideas from both anomaly and signature detection.

A hybrid IDS combines a HIDS, which monitors events occurring in the host system, and a NIDS, which monitors network traffic.

INTRUSION-PREVENTION SYSTEMS

It is still early in the development of intrusion-prevention systems (IPSs), but generally an IPS sits inline on the network and monitors it, and when an event occurs, it takes action based on prescribed rules. This is unlike IDSs, which do not sit inline and are passive. Because IPSs take detection a step further, some see them as next-generation IDS systems. Others, however, think in broader terms and consider the IPSs yet another tool in the security infrastructure that could help prevent intrusions. IPS has developed out of IDS, but the two are really different security products that have different functionalities and strengths (Huang).

STANDARD IPS SYSTEM

Figure 2 shows the working of a standard IPS system.

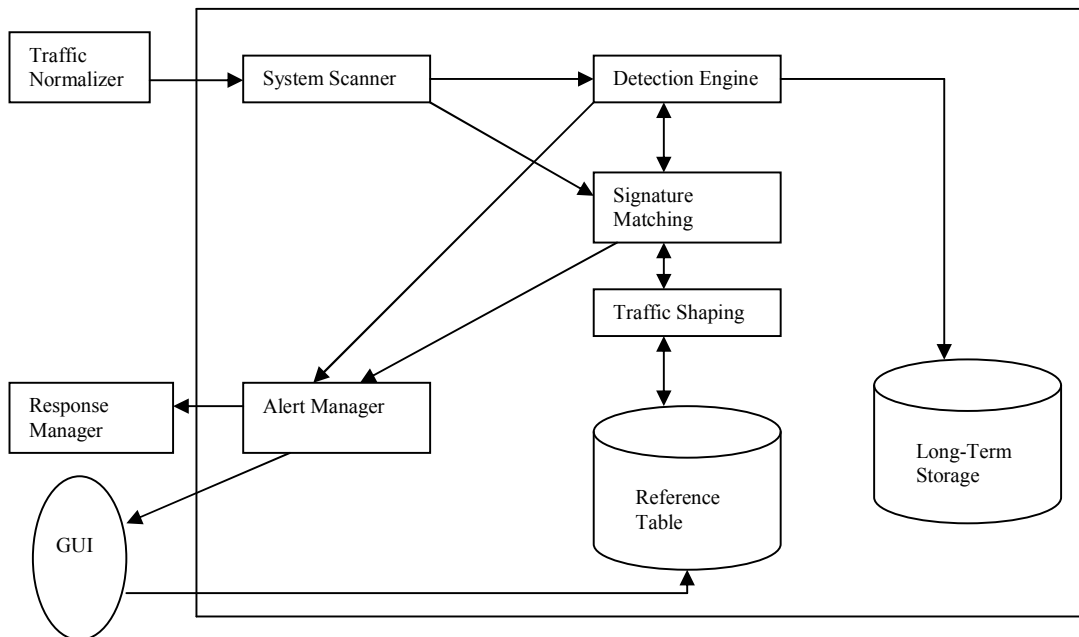


Figure 2: Standard IPS System.

NETWORK-BASED VERSUS HOST-BASED INTUSION-DETECTION SYSTEMS

Table 2 shows some of the differences between a HIDS and a NIDS.

| NIDS | HIDS |
|------------------------------------------------------------------|------------------------------------------------------------------|
| Broad in scope (watching all network activities) | Narrow in scope (watching only specific host activities) |
| Easier setup | More complex setup |
| Better for detecting attacks from the outside | Better for detecting attacks from the inside |
| Less expensive to implement | More expensive to implement |
| Detection is based on what can be recorded on the entire network | Detection is based on what any single host can record |
| Examines packet headers | Does not see packet headers |
| Near real-time response | Usually only responds after a suspicious log entry has been made |

| OS-independent | OS-specific |
|------------------------------------------------|---------------------------------------------------|
| Detects network attacks as payload is analyzed | Detects local attacks before they hit the network |
| Detects unsuccessful attack attempts | Verifies success or failure of attacks |

Table 2: Network-Based versus host-based intrusion-detection systems.

INTRUSION-DETECTION SYSTEMS VERSUS INTRUSION-PREVENTION SYSTEMS

IDS and IPS technology each has its own place in a security program because they perform separate functions. Table 3 presents some of the differences between them (Karlof and Wagner).

| IDS | IPS |
|---------------------------------------------------------|---------------------------------------------------------|
| Installed on network segments (NIDS) and on host (HIDS) | Installed on network segments (NIPS) and on host (HIPS) |
| Sits on network passively | Sits inline (not passive) |
| Cannot parse encrypted traffic | Better at protecting applications |
| Central management control | Central management control |
| Better at detecting hacking attacks | Ideal for blocking web defacement |
| Alerting product (reactive) | Blocking product (proactive) |

Table 3: Intrusion-Detection Systems vs. Intrusion-Prevention Systems.

WHY IDSs AND IPSs ARE IMPORTANT

IDSs and IPSs are important for many organizations, from small offices to large multinational corporations. IDSs and IPSs offer many benefits (Scarfone and Mell):

- Greater proficiency in detecting intrusions than by doing it manually

- In-depth knowledge base to draw from
- Ability to deal with large volumes of data
- Near real-time alerting capabilities that help reduce potential damages
- Automated responses, such as logging off a user, disabling a user account or launching automated scripts
- Strong deterrent value
- Built-in forensic capabilities
- Built-in reporting capabilities

SUMMARY

In this article, an attempt is made to arrive at an in-depth understanding of defense so as to improve the security of a networked organization. There is also a discussion of the basic concepts of intrusion detection. The authors look at the origins of intrusion detection and prevention and examine how it has evolved over the years.

References

Bentham, J (2002). *TCP/IP Lean – Web Servers for Embedded Systems* (Second Edition).

Bungale, P. P., Goodell, G. and Roussopoulos, M. Conservation vs. consensus in peer-to-peer preservation systems.

http://iptps05.cs.cornell.edu/PDFs/CameraReady_214.pdf

Douligeris, C. and Serpanos, D. N. (2007). Network Security – Current Status and Future Directions.

Dubin, J. Intrusion detection and prevention: More than a firewall.

http://searchsmb.techtarget.com/tip/0,289483,sid44_gci1267542,00.html

Edney, J and Arbaugh, W. A. (2004). *Real 802.11 Security Wi-Fi Protected Access*

and 802.11i.

Endorf, C, Schultz, E and Mellander, J. (2004) Intrusion Detection and Prevention.

Huang, N-F. Intrusion detection and prevention system (IPS) –Technology, applications, and trend.

http://www.apan.net/meetings/taipei2005/presentation/APAN_IPS_NFHU_ANG_0826-2005.pdf

Karlof, C. and Wagner, D. Secure routing in wireless sensor networks: attacks and Countermeasures. <http://www.cs.berkeley.edu/~ckarlof/papers/senroute-adnj.pdf>

Mayank, M. Cascade: an attack resistant peer-to-peer system.

<http://mnl.cs.stonybrook.edu/home/mayank/CascadeReport.pdf>

Mirkovic, L., Dietrich, S., Dittrich, D. and Reiher, P. (2005). *Internet*

Denial of Service – Attack and Defense Mechanisms.

Northcutt, S. (1999). *Network Intrusion Detection – An Analyst’s Handbook.*

Northcutt, S., Zeltser, L., Winters, S. Frederick, K. K. and Ritchey, R. H. (2003) *Inside*

Network Perimeter Security.

Scarfone, K. and Mell, P. Guide to intrusion detection and prevention systems

(IDPS). <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

Sklavos, N. and Zhang, X. (2007). Wireless Security and Cryptography –

Specifications and Implementations.

Vlachos, V., Androutsellis-Theotokis, S. and Spinellis, D. Security

applications of peer-to-peer networks.

<http://www.spinellis.gr/pubs/jrnl/2004-CompSec-p2pav/html/VAS04.pdf>

Zhang, Q. and Janakiraman. A. Distributed Approach to Network Intrusion

Detection and Prevention.

<http://cse.seas.wustl.edu/Research/FileDownload.asp?176>

Zhou, C. V., Karunasekera, S. and Leckie, C. A Peer-to-Peer Collaborative Intrusion

Detection System. <http://www.cs.mu.oz.au/~cvzhou/pub/icon05.pdf>