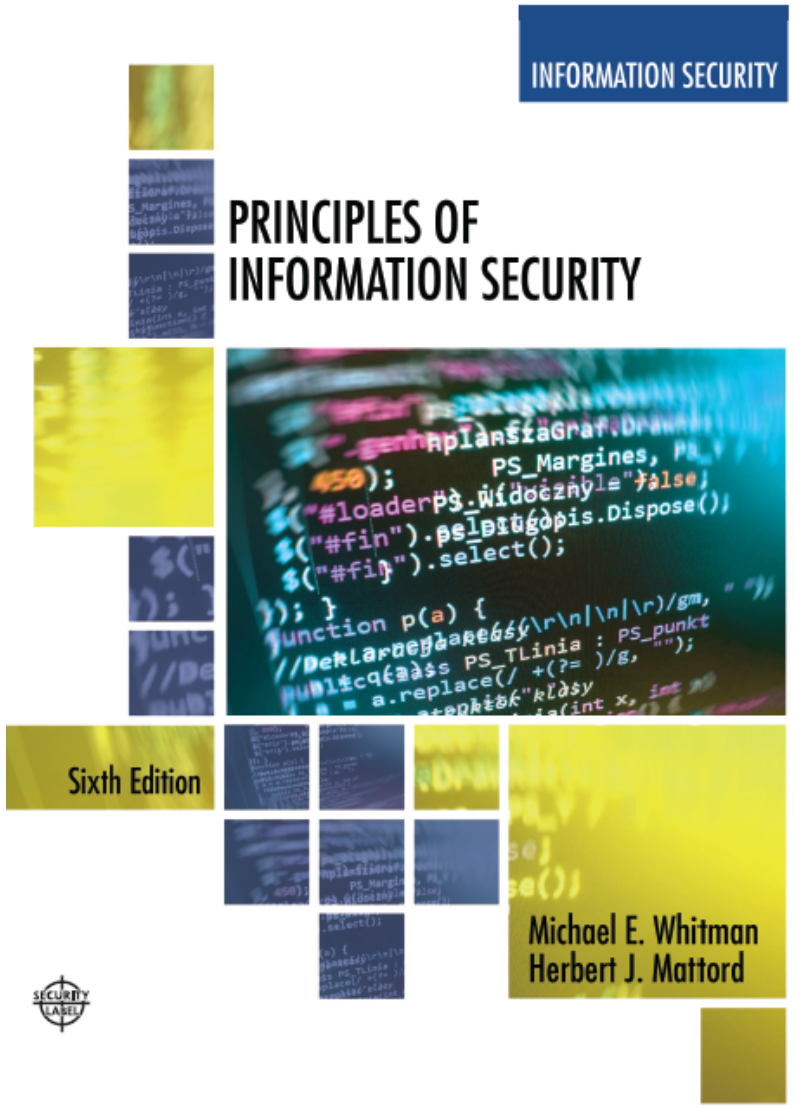


Source: Principles of Information Security

Chapter 7

Security Technology & Tools:

Intrusion Detection & Prevention Systems

Dr. Ibrahim Waziri Jr.

Learning Objectives

Upon completion of this material, you should be able to:

- Identify and describe the categories and models of intrusion detection and prevention systems
- Describe the detection approaches employed by modern intrusion detection and prevention systems
- Define and describe honeypots, honeynets, and padded cell systems
- List and define the major categories of scanning and analysis tools, and describe the specific tools used within each category

Introduction

- Protection of organizations assets relies at least as much on managerial controls as on technical safeguards.
- Properly implemented technical solutions guided by policy are essential to an information security program.
- Advanced technologies can be used to enhance the security of information assets.

Intrusion Detection and Prevention Systems

An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an organization's information systems.

- **Intrusion detection:** consists of procedures and systems that identify system intrusions. Intrusion detection systems detect a violation of its configuration and activate alarm.
- **Intrusion prevention:** consists of activities that deter an intrusion.
- **Intrusion reaction:** encompasses actions an organization undertakes when intrusion event is detected.
- **Intrusion correction:** activities complete restoration of operations to a normal state and seek to identify source and method of intrusion.

Why Use an IDPS & Types of IDPS

IDPS detect and deal with preambles to attacks

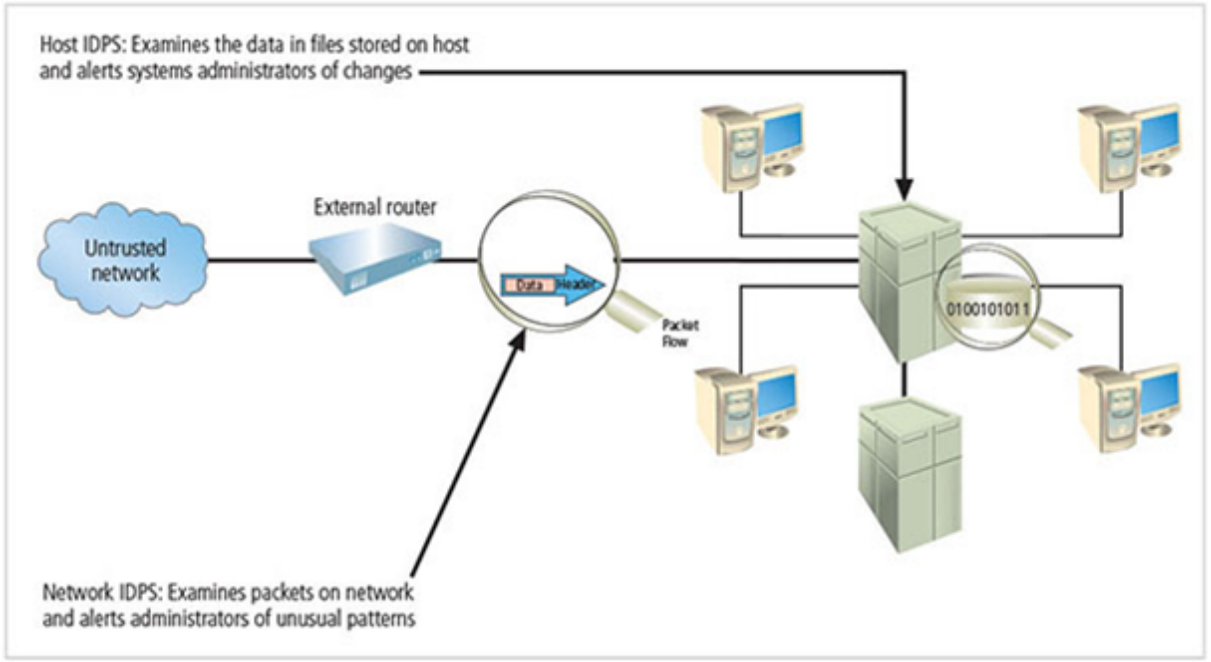
Detection: Identify and report an intrusion

Prevention: Contain an attack and prevent/mitigate the loss or damage

Data collection: allows the organization to examine what happened after an intrusion and why.

Types of IPDS:

- Host-based (HIDPS)
- Network-based (NIDPS)
  - Wireless IDPS
  - Network Behavior Analysis IDPS



NIDPSs

- Focused on protecting network information assets.
- Resides on a computer or an appliance connected to a segment of an organization's network; looks for indications of attack
- Implementation of TCP/IP stack:
- **Wireless NIDPS** - Monitors and analyzes wireless network traffic
- Network behavior analysis systems - Identify problems related to the flow of traffic.

Advantages of NIDPSs	Disadvantages of NIDPSs
Good network design and placement of NIDPS can enable an organization to monitor a large network with few devices	Can become overwhelmed by network volume and fail to recognize attacks
NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations	Require access to all traffic to be monitored
NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers	Cannot analyze encrypted packets
	Cannot reliably ascertain if an attack was successful or not

HIDPS

- Resides on a particular computer or server (host) and monitors activity only on that system
- Benchmarks and monitors the status of key system files and detects when intruder creates, modifies, or deletes files
- Advantage over NIDPS: can access encrypted information traveling over network and make decisions about potential/actual attacks

Advantages of HIDPSs	Disadvantages of HIDPSs
Can detect local events on host systems and detect attacks that may elude a network-based IDPS	Vulnerable both to direct attacks and attacks against the host operating system
Functions on host system, where encrypted traffic will have been decrypted and is available for processing	Can inflict a performance overhead on its host systems
Not affected by use of switched network protocols	Pose more management issues
Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs	Does not detect multihost scanning, nor scanning of non-host network devices
	Can use large amounts of disk space
	Susceptible to some DoS attacks

IDPS Detection Methods & Response Behavior

Detection Methods:

- Signature-based detection - knowledge-based detection
- Anomaly-based detection - behavior-based detection
- Stateful protocol analysis
- Log file monitors

Response Behavior:

IDPS response to external stimulation depends on the configuration and function; many response options are available.

- Generate reports
- Failsafe
- Active or Passive Response:

Strengths and Limitations of IDPSs

Strengths	Limitations
Monitoring and analysis of system events and user behaviors	Compensating for weak/missing security mechanisms in protection infrastructure
Testing the security states of system configurations	Instantaneously detecting, reporting, responding to attack when there is heavy network or processing load
Baselining the security state of a system and tracking changes	Detecting new attacks or variants of existing attacks
Recognizing patterns of system events corresponding to known attacks	Effectively responding to attacks by sophisticated attackers
Recognizing activity patterns that vary from normal activity	Automatically investigating attacks without human intervention
Managing OS audit and logging mechanisms and data they generate	Resisting attacks intended to defeat or circumvent them
Alerting appropriate staff when attacks are detected	Compensating for problems with fidelity of information sources
Measuring enforcement of security policies encoded in the analysis engine	Dealing effectively with switched networks
Providing default information on security policies	
Allowing non-security experts to perform important security monitoring functions	

Selecting IDPS & Implementation Strategies

Selecting IDPS

- Technical and policy considerations
- Organizational requirements and constraints
- IDPSs product features and quality

Implementation strategies:

- Centralized
- Fully distributed
- Partially distributed

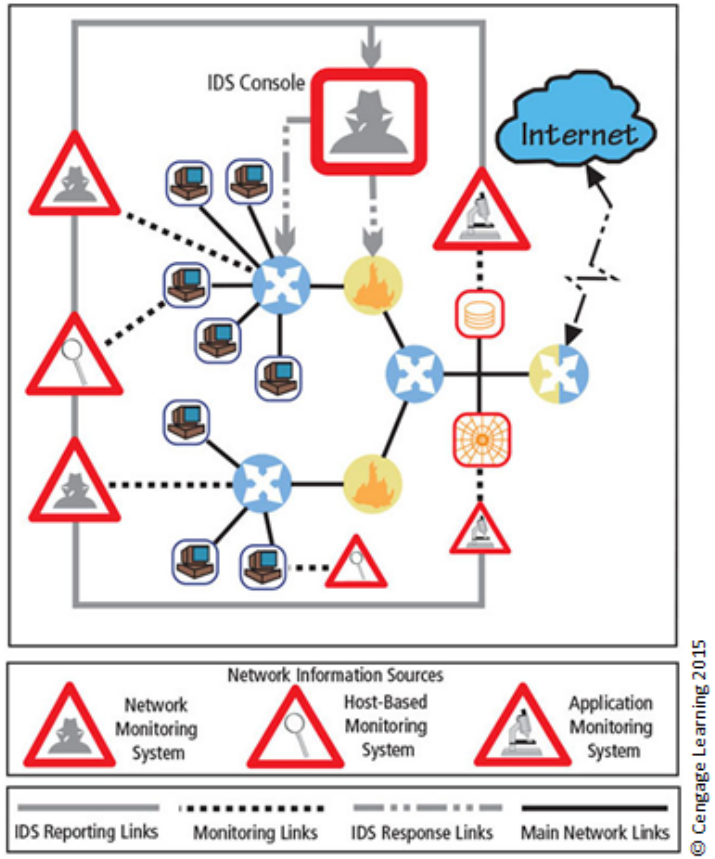


Figure 1: Centralized IDPS

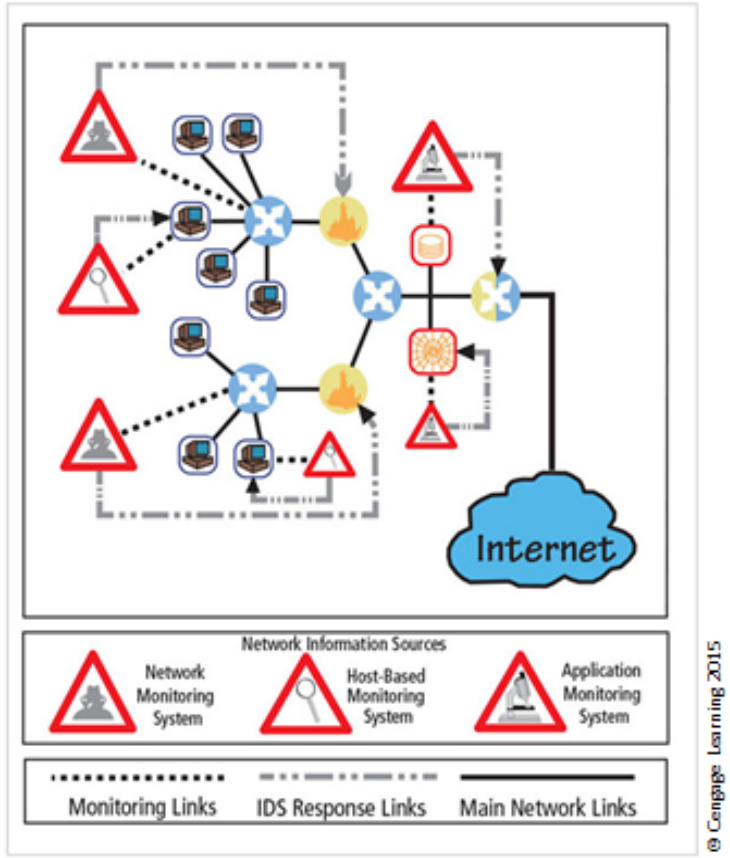


Figure 2: Fully distributed IDPS

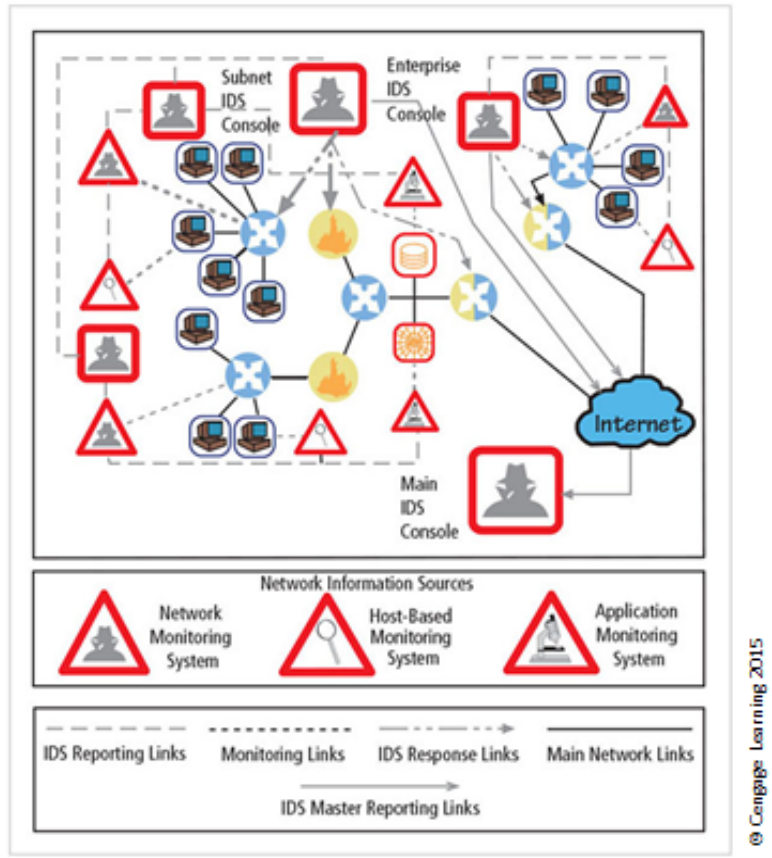


Figure 3: Partially distributed IDPS

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

Deploying of an IDPS

Deploying network-based IDPSs

- NIST recommends four locations for NIDPS sensors
  - Location 1: Behind each external firewall, in the network DMZ
  - Location 2: Outside an external firewall
  - Location 3: On major network backbones
  - Location 4: On critical subnets

Deploying host-based IDPSs

- Proper implementation of HIDPSs can be a painstaking and time-consuming task.
- Deployment begins with implementing most critical systems first.
- Installation continues until either all systems are installed or the organization reaches planned degree of coverage it will accept.

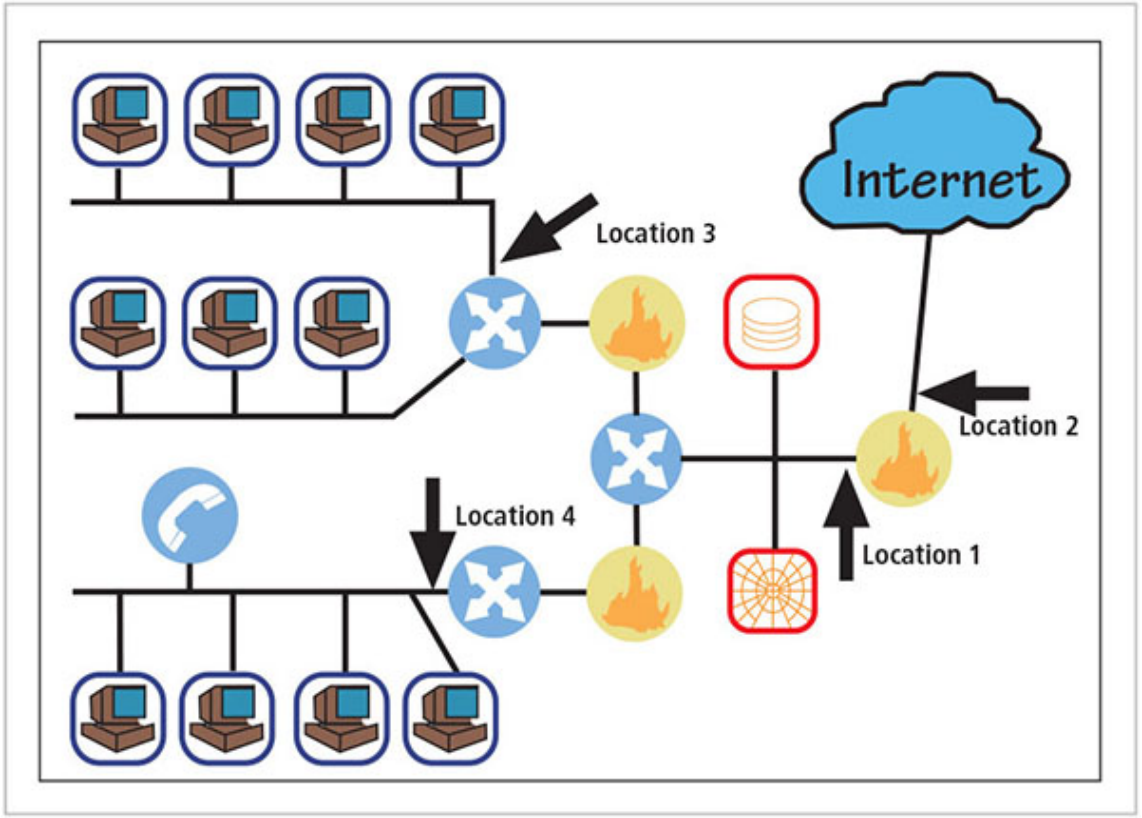


Figure: NIST NIDPS deployment recommendation

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

Measuring the Effectiveness of IDPSs

IDPSs are evaluated using four dominant metrics:

- Thresholds
- Blacklists/Whitelists
- Alert settings
- Code Viewing/Editing.

Vendors provide testing mechanisms--some of these testing processes will enable the administrator to:

- Record and retransmit packets from real virus or worm scan
- Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYN packets)
- Conduct a real virus or worm scan against a hardened or sacrificial system

Testing process should be as realistic as possible.

Honeypots, Honeynets, and Padded Cell Systems

Honeypots: decoy systems designed to lure potential attackers away from critical systems

Honeynets: several honeypots connected together on a network segment

Padded cell system: protected honeypot that cannot be easily compromised

Trap & Trace: Use a combination of techniques to detect an intrusion and trace it back to its source.

Advantages	Disadvantages
Attackers can be diverted to targets they cannot damage	Legal implications of using such devices are not well understood—Entrapment & Enticement
Administrators have time to decide how to respond to an attacker	Honeypots and padded cells have not yet been shown to be generally useful security technologies
Attackers' actions can be easily and more extensively monitored, and records can be used to refine threat models and improve system protections	An expert attacker, once diverted into a decoy system, may become angry and launch a more aggressive attack against an organization's systems
Honeypots may be effective at catching insiders who are snooping around a network	Administrators and security managers need a high level of expertise to use these systems

Scanning and Analysis Tools

Scanning tools: typically are used to collect information that an attacker needs to launch a successful attack.

Attack protocol: is a logical sequence of steps or processes used by an attacker to launch an attack against a target system or network.

Footprinting: process of collecting publicly available information about a potential target.

Fingerprinting: systematic survey of target organization's Internet addresses collected during the footprinting phase to identify network services offered by hosts in that range.

Port Scanners: Tools used by both attackers and defenders to identify/fingerprint computers active on a network and other useful information.

Firewall Analysis Tools: Tools that help close an open or poorly configured firewall thus help the network defender minimize risk from attack.

Operating System Detection Tools: Provides the ability to detect a target computer's operating system.

Vulnerability Scanners: Examine networks for highly detailed information; initiate traffic to determine security holes

Packet Sniffers: Network tool that captures copies of packets from network and analyzes them.

Summary

- Intrusion detection system (IDPS) detects violation of its configuration and activates alarm.
- A network-based IDPS (NIDPS) monitors network traffic and then notifies the appropriate administrator when a predefined event occurs.
- A host-based IDPS (HIDPS) resides on a particular computer or server and monitors activity on that system.
- Signature-based IDPSs, also known as knowledge-based IDPSs, examine data traffic for patterns that match signatures—preconfigured, predetermined attack patterns.
- Statistical anomaly-based IDPSs, also known as behavior-based IDPSs, collect data from normal traffic and establish a baseline.
- Selecting IDPS products that best fit an organization's needs is challenging and complex.
- Honeypots are decoy systems; two variations are known as honeynets and padded cell systems.
- Scanning and analysis tools are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of a network.