R N S INSTITUTE OF TECHNOLOGY

CHANNASANDRA, BANGALORE - 98

INFORMATION AND NETWORK SECURITY

NOTES FOR 8TH SEMESTER INFORMATION SCIENCE

SUBJECT CODE: 06CS835

PREPARED BY

DIVYA K

1RN09IS016

8th Semester

Information Science

Divya.1rn09is016@gmail.com

TEXT BOOKS:

PRINCIPLES OF INFORMATION SECURITY – Michael E Whitman and Herbert J Mattord, 2nd Edition , Thomson

APPLICATIONS AND STANDARDS – NETWORK SECURITY ESSENTIALS, William stallings, Pearson Education

CONTENTS:

UNIT 2, UNIT 3, UNIT 4, UNIT 5, UNIT 7

UNIT 2
SECURITY TECHNOLOGY

INTRODUCTION

Technical controls are essential to a well-planned information security program, particularly to enforce policy for the many IT functions that are not under direct human control. Networks and computer systems make millions of decisions every second and operate in ways and at speeds that people cannot control in real time.

PHYSICAL DESIGN

The physical design of a security program is made up of two parts:

- Security technology
- Physical security

The team responsible for the physical design:

- ✓ Selects specific technologies to support the information security blueprint
- ✓ Identifies complete technical solutions based on these technologies including deployment, operations, and maintenance elements, to improve the security of the environment
- ✓ Designs physical security measures to support the technical solution
- ✓ Prepares project plans for the implementation phase that follows

FIREWALLS

A **firewall** in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the **untrusted network** (for example, the Internet), and the inside world, known as the **trusted network**. The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices. Firewalls can be categorized by processing mode, development era, or structure.

PROCESSING MODES OF FIREWALLS

Firewalls fall into five major processing-mode categories:

- ♥ packet-filtering firewalls,
- ♥ application gateways,
- ♥ circuit gateways,
- ♥ layer firewalls, and
- ♥ hybrids

Packet-Filtering Firewall

- ➢ examines the header information of data packets that come into a network.
- ➢ determines whether to drop a packet (deny) or forward it to the next network connection (allow) based on the rules programmed into the firewall.
- ➢ examine every incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet type, and other key information.
- ➢ scan network data packets looking for compliance with or violation of the rules of the firewall's database.
- ➢ If the device finds a packet that matches a restriction, it stops the packet from traveling from one network to another.
- ➢ The restrictions most commonly implemented in packet-filtering firewalls are based on a combination of the following:
  - IP source and destination address

- Direction (inbound or outbound)
- Protocol (for firewalls capable of examining the IP protocol layer)
- Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and
- destination port requests (for firewalls capable of examining the TCP/UPD layer)

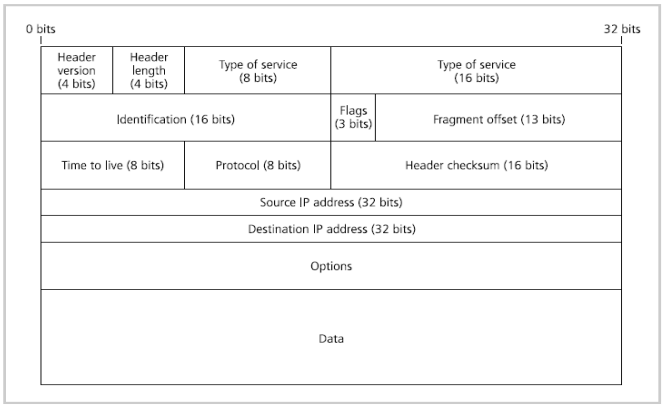


Figure 6-2 IP Packet Structure

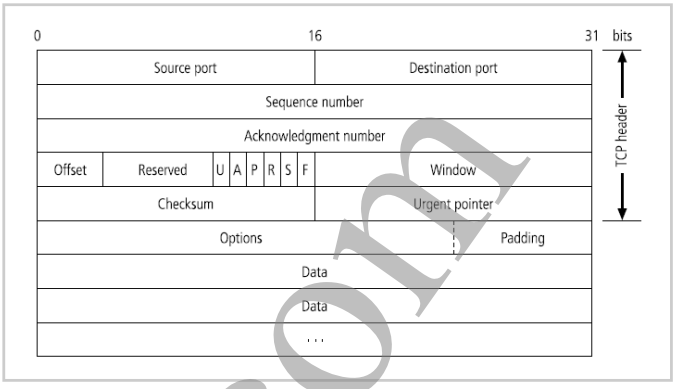


Figure 6-3 TCP Packet Structure

Packet structure varies depending on the nature of the packet. The two primary service types are TCP and UDP (as noted above). Figures 6-3 and 6-4 show the structures of these two major elements of the combined protocol known as TCP/IP.

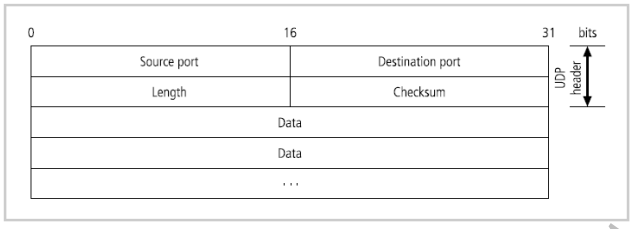


Figure 6-4 UDP Datagram Structure

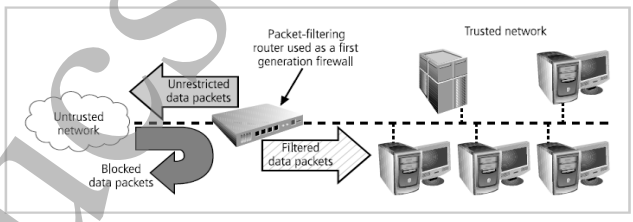


Figure 6-5 Packet-Filtering Router

Simple firewall models examine two aspects of the packet header: the destination and source address. They enforce **address restrictions**.
Figure 6-5 shows how a packet-filtering router can be used as a simple firewall to filter data packets from inbound connections and allow outbound connections unrestricted access to the public network.

Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Table 6-1 Sample Firewall Rule and Format

There are three subsets of packet-filtering firewalls:

- ♠ static filtering,
- ♠ dynamic filtering, and
- ♠ stateful inspection.

★ Static filtering requires that the filtering rules be developed and installed with the firewall. The rules are created and sequenced either by a person directly editing the rule set, or by a person using a programmable interface to specify the rules and the sequence.

★ A dynamic filtering firewall can react to an emergent event and update or create rules to deal with that event. While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the dynamic packet-filtering firewall allows only a particular packet with a particular source, destination, and port address to enter. It does this by opening and closing "doors" in the firewall based on the information contained in the packet header.

★ Stateful inspection firewalls, also called stateful firewalls, keep track of each network connection between internal and external systems using a state table. A state table tracks the state and context of each packet in the conversation by recording which station sent what packet and when.

Source Address	Source Port	Destination Address	Destination Port	Time Remaining in Seconds	Total Time in Seconds	Protocol
192.168.2.5	1028	10.10.10.7	80	2725	3600	TCP

Table 6-2 State Table Entries

Application Gateways

- The application gateway, also known as an application-level firewall or application firewall, is frequently installed on a dedicated computer, separate from the filtering router, but is commonly used in conjunction with a filtering router.
- The application firewall is also known as a proxy server since it runs special software that acts as a proxy for a service request.
- This proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users. These servers can store the most recently accessed pages in their internal cache, and are thus also called *cache servers*.
- One common example of an application-level firewall (or proxy server) is a firewall that blocks all requests for and responses to requests for Web pages and services from the internal computers of an organization, and instead makes all such requests and responses go to intermediate computers (or proxies) in the less protected areas of the organization's network.
- The primary disadvantage of application-level firewalls is that they are designed for one or a few specific protocols and cannot easily be reconfigured to protect against attacks on other protocols.

Circuit Gateways

- The circuit gateway firewall operates at the transport layer.
- They do not usually look at traffic flowing between one network and another, but they do prevent direct connections between one network and another.
- They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall, and then allowing only authorized traffic, such as a specific type of TCP connection for authorized users, in these tunnels.

MAC Layer Firewalls

- MAC layer firewalls are designed to operate at the media access control sublayer of the data link layer (Layer 2) of the OSI network model.
- This enables these firewalls to consider the specific host computer's identity, as represented by its MAC or network interface card (NIC) address in its filtering decisions.
- Thus, MAC layer firewalls link the addresses of specific host computers to ACL entries that identify the specific types of packets that can be sent to each host, and block all other traffic.

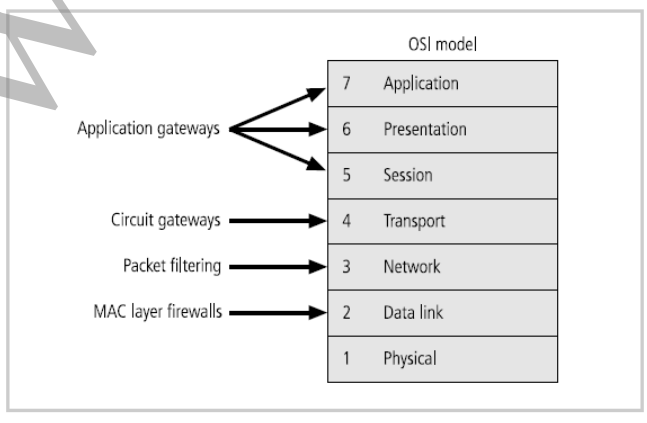


Figure 6-6 Firewall Types and the OSI Model

Hybrid Firewalls

- ♣ Hybrid firewalls combine the elements of other types of firewalls—that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways.
- ♣ A hybrid firewall system may actually consist of two separate firewall devices; each is a separate firewall system, but they are connected so that they work in tandem.
- ♣ An added advantage to the hybrid firewall approach is that it enables an organization to make a security improvement without completely replacing its existing firewalls.

FIREWALLS CATEGORIZED BY GENERATION

- ★ **First generation** firewalls are static packet-filtering firewalls—that is, simple networking devices that filter packets according to their headers as the packets travel to and from the organization's networks.
- ★ **Second generation** firewalls are application-level firewalls or proxy servers—that is, dedicated systems that are separate from the filtering router and that provide intermediate services for requestors.
- ★ **Third generation** firewalls are stateful inspection firewalls, which, as described previously, monitor network connections between internal and external systems using state tables.
- ★ **Fourth generation** firewalls, which are also known as dynamic packet-filtering firewalls, allow only a particular packet with a particular source, destination, and port address to enter.
- ★ **Fifth generation** firewalls include the kernel proxy, a specialized form that works under Windows NT Executive, stack which is the kernel of Windows NT. This type of firewall evaluates packets at multiple layers of the protocol, by checking security in the kernel as data is passed up and down the stack.

FIREWALLS CATEGORISED BY STRUCTURE

Firewalls can also be categorized by the structures used to implement them.

- **Commercial-Grade Firewall Appliances** Firewall appliances are stand-alone, self contained combinations of computing hardware and software. These devices frequently have many of the features of a general-purpose computer with the addition of firmware based instructions that increase their reliability and performance and minimize the likelihood of their being compromised. These variant operating systems are tuned to meet the type of firewall activity built into the application software that provides the firewall functionality.
- **Commercial-Grade Firewall Systems** A commercial-grade firewall system consists of application software that is configured for the firewall application and run on a general-purpose computer. Organizations can install firewall software on an existing general purpose computer system, or they can purchase hardware that has been configured to specifications that yield optimum firewall performance.
- **Small Office/Home Office (SOHO) Firewall Appliances** As more and more small businesses and residences obtain fast Internet connections with digital subscriber lines (DSL) or cable modem connections, they become more and more vulnerable to attacks. One of the most effective methods of improving computing security in the SOHO setting is by means of a SOHO or residential-grade firewall. These devices, also known as broadband gateways or DSL/cable modem routers, connect the user's local area network or a specific computer system to the Internetworking device—in this case, the cable modem or DSL router provided by the Internet service provider (ISP). The SOHO firewall serves first as a stateful firewall to enable inside-to-outside access and can be configured to allow limited TCP/IP port forwarding and/or screened subnet capabilities.
- **Residential-Grade Firewall Software** Another method of protecting the residential user is to install a software firewall directly on the user's system. Many people have implemented these residential-grade software-based firewalls (some of which also provide antivirus or intrusion detection capabilities), but, unfortunately, they may not be as fully protected as they think. The most commonly used of residential-grade software-based firewalls are *McAfee Internet Security, Microsoft Windows Firewall etc.*

FIREWALL ARCHITECTURES

The configuration that works best for a particular organization depends on three factors:

- ✓ The objectives of the network,
- ✓ the organization's ability to develop and implement the architectures, and

- ✓ The budget available for the function.

Although literally hundreds of variations exist, there are four common architectural implementations: Packet-filtering routers, screened host firewalls, dual-homed firewalls, and screened subnet firewalls.

Packet-Filtering Routers

- ♣ Most organizations with an Internet connection have some form of a router at the boundary between the organization's internal networks and the external service provider.
- ♣ Many of these routers can be configured to reject packets that the organization does not want to allow into the network.
- ♣ This is a simple but effective way to lower the organization's risk from external attack.
- ♣ The drawbacks to this type of system include a lack of auditing and strong authentication.
- ♣ Also, the complexity of the ACLs used to filter the packets can degrade network performance.

Screened Host Firewalls

- ♣ Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server.
- ♣ This approach allows the router to pre-screen packets to minimize the network traffic and load on the internal proxy.
- ♣ The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services. This separate host is often referred to as a **bastion host.**
- ♣ Compromise of the bastion host can disclose the configuration of internal networks and possibly provide attackers with internal information. Since the bastion host stands as a sole defender on the network perimeter, it is commonly referred to as the **sacrificial host**.

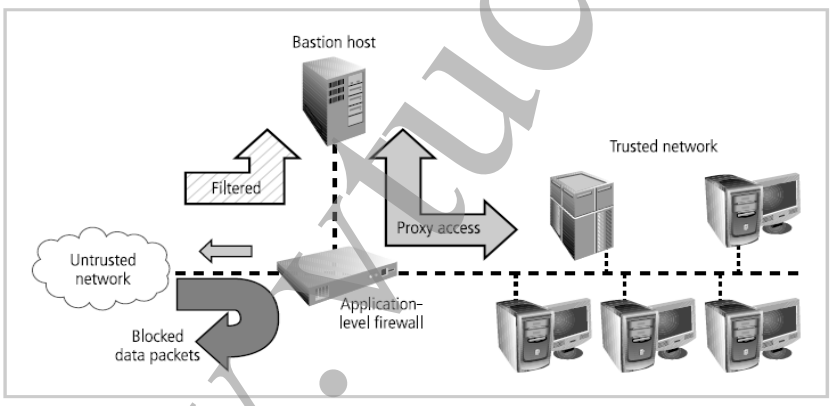


Figure 6-12 Screened Host Firewall

Dual-Homed Firewall

- ♣ One NIC is connected to the external network, and
- ♣ another NIC is connected to the internal network, providing an additional layer of protection.

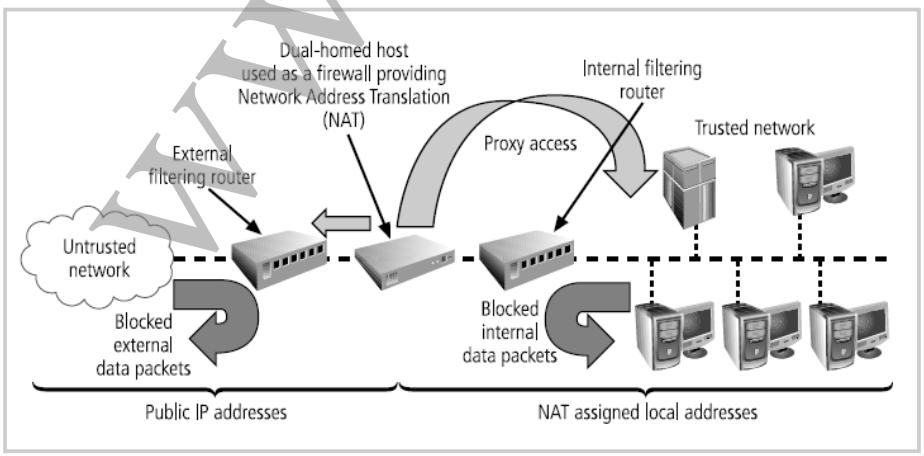


Figure 6-13 Dual-Homed Host Firewall

- With two NICs, all traffic *must* physically go through the firewall to move between the internal and external networks.
- Implementation of this architecture often makes use of NAT.
- NAT is a method of mapping real, valid, external IP addresses to special ranges of non-routable internal IP addresses, thereby creating yet another barrier to intrusion from external attackers.

Screened Subnet Firewalls (with DMZ)

- The architecture of a screened subnet firewall provides a DMZ.
- The DMZ can be a dedicated port on the firewall device linking a single bastion host, or it can be connected to a screened subnet, as shown in Figure 6-14.
- Connections from the outside or untrusted network are routed through an external filtering router.
- Connections from the outside or untrusted network are routed into—and then out of—a routing firewall to the separate network segment known as the DMZ.
- Connections into the trusted internal network are allowed only from the DMZ bastion host servers.
- The **screened subnet** is an entire network segment that performs two functions:
  - it protects the DMZ systems and information from outside threats by providing a network of intermediate security
  - It protects the internal networks by limiting how external connections can gain access to them.
- Another facet of the DMZ is the creation of an area known as an extranet.
- An **extranet** is a segment of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public.

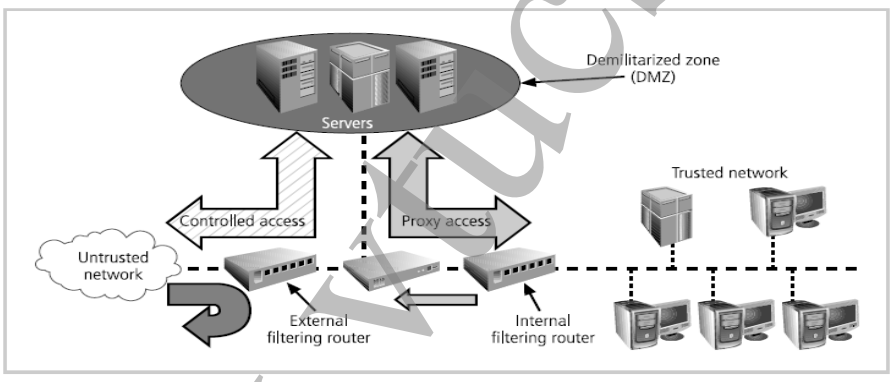


Figure 6-14 Screened Subnet (DMZ)

SOCKS Servers

- SOCKS is the protocol for handling TCP traffic via a proxy server.
- The SOCKS system is a proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation.
- A SOCKS system can require support and management resources beyond those of traditional firewalls since it entails the configuration and management of hundreds of individual clients, as opposed to a single device or small set of devices.

SELECTING THE RIGHT FIREWALL

When trying to determine which the best firewall for an organization is, you should consider the following questions:

1. Which type of firewall technology offers the right balance between protection and cost for the needs of the organization?
2. What features are included in the base price? What features are available at extra cost? Are all cost factors known?
3. How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall?
4. Can the candidate firewall adapt to the growing network in the target organization?

The most important factor is, of course, the extent to which the firewall design provides the required protection. The second most important factor is cost.

CONFIGURING AND MANAGING FIREWALLS

- Once the firewall architecture and technology have been selected, the organization must provide for the initial configuration and ongoing management of the firewall(s).
- Good policy and practice dictates that each firewall device, whether a filtering router, bastion host, or other firewall implementation, must have its own set of configuration rules.
- In fact, the configuration of firewall policies can be complex and difficult.
- IT professionals familiar with application programming can appreciate the difficulty of debugging both syntax errors and logic errors.
- Syntax errors in firewall policies are usually easy to identify, as the systems alert the administrator to incorrectly configured policies.
- Configuring firewall policies is as much an art as it is a science.
- Each configuration rule must be carefully crafted, debugged, tested, and placed into the ACL in the proper sequence—good, correctly sequenced firewall rules ensure that the actions taken comply with the organization's policy.
- In a well-designed, efficient firewall rule set, rules that can be evaluated quickly and govern broad access are performed before ones that may take longer to evaluate and affect fewer cases.

BEST PRACTICES FOR FIREWALLS / FIREWALL RULES

i. All traffic from the trusted network is allowed out.
ii. The firewall device is never directly accessible from the public network for configuration or management purposes.
iii. Simple Mail Transport Protocol (SMTP) data is allowed to enter through the firewall.
iv. ICMP is a common method for hacker reconnaissance and should be turned off to prevent snooping.
v. Telnet (terminal emulation) access to all internal servers from the public networks should be blocked.
vi. HTTP traffic should be blocked from internal networks through the use of some form of proxy access or DMZ architecture.
vii. All data that is not verifiably authentic should be denied.

CONTENT FILTERS:

- Content filter is another utility that can help protect an organisation's systems from misuse and un-intentional denial-of-service problems, and which is often closely associated with firewalls.
- Content filters are also called reverse firewalls because their primary purpose is to restrict internal access to external material.
- Content filters has two components:
  - Rating is like a set of firewall rules for websites and is common in residential content filters. It can be:
    - complex, with multiple access control settings for different levels of the organization.
    - simple, with a basic allow/deny scheme like that of a firewall.
  - The filtering is a method used to restrict specific access requests to the identified resources, which may be websites, servers, or whatever resources the content filter administrator configures
- The most common content filters restrict users from accessing Web sites with obvious non-business related material, such as pornography, or deny incoming spam e-mail.
- Content filters can be small add-on software programs for the home or office, such as NetNanny or SurfControl, or corporate applications, such as the Novell Border Manager.
- The benefit of implementing content filters is the assurance that employees are not distracted by non-business material and cannot waste organizational time and resources.
- The downside is that these systems require extensive configuration and ongoing maintenance to keep the list of unacceptable destinations or the source addresses for incoming restricted e-mail up-to-date.

PROTECTING REMOTE CONNECTIONS

In the past, organizations provided the remote connections exclusively through dial-up services like Remote Authentication Service (RAS). Since the Internet has become more widespread in recent years, other options such as virtual private networks (VPNs) have become more popular.

REMOTE ACCESS

- The connections between company networks and the Internet use firewalls to safeguard that interface.
- Unsecured, dial-up connection points represent a substantial exposure to attack.
- An attacker who suspects that an organization has dial-up lines can use a device called a war dialer to locate the connection points.
- A war dialer is an automatic phone-dialing program that dials every number in a configured range (e.g.,
- 555-1000 to 555-2000), and checks to see if a person, answering machine, or modem picks up.
- If a modem answers, the war dialer program makes a note of the number and then moves to the next target number.
- The attacker then attempts to hack into the network via the identified modem connection using a variety of techniques.

RADIUS, TACACS, and Diameter

- RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization's network via a dial-up connection.

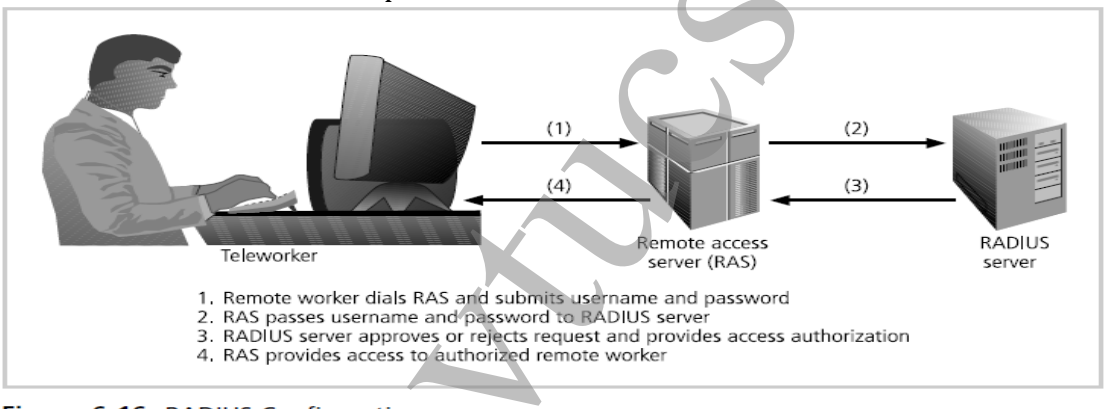


Figure 6-16 RADIUS Configuration

- The **Remote Authentication Dial-In User Service (RADIUS)** system centralizes the management of user authentication by placing the responsibility for authenticating each user in the central RADIUS server.
- When a remote access server (RAS) receives a request for a network connection from a dial-up client, it passes the request, along with the user's credentials, to the RADIUS server.
- RADIUS then validates the credentials and passes the resulting decision (accept or deny) back to the accepting remote access server. Figure 6-16 shows the typical configuration of an RAS system.
- An emerging alternative that is derived from RADIUS is the Diameter protocol.
- The **Diameter protocol** defines the minimum requirements for a system that provides authentication, authorization, and accounting (AAA) services and can go beyond these basics and add commands and/or object attributes.
- Diameter security uses existing encryption standards including Internet Protocol Security (IPSec) or Transport Layer Security (TLS)
- The **Terminal Access Controller Access Control System (TACACS)** is another remote access authorization system that is based on a client/server configuration.
- There are three versions of TACACS: TACACS, Extended TACACS, and TACACS+.
- The original version combines authentication and authorization services.
- The extended version separates the steps needed to authenticate the individual or system attempting access from the steps needed to verify that the authenticated individual or system is allowed to make a given type of connection.

SECURING AUTHENTICATION WITH KERBEROS

Kerberos consists of three interacting services, all of which use a database library:
1. Authentication server (AS), which is a Kerberos server that authenticates clients and servers.
2. Key Distribution Center (KDC), which generates and issues session keys.
3. Kerberos ticket granting service (TGS), which provides tickets to clients who request services.

Kerberos is based on the following principles:

- The KDC knows the secret keys of all clients and servers on the network.
- The KDC initially exchanges information with the client and server by using these secret keys.
- Kerberos authenticates a client to a requested service on a server through TGS and by issuing temporary session keys for communications between the client and KDC, the server and KDC, and the client and server.
- Communications then take place between the client and server using these temporary session key

Figures 6-17 and 6-18 illustrate this process.

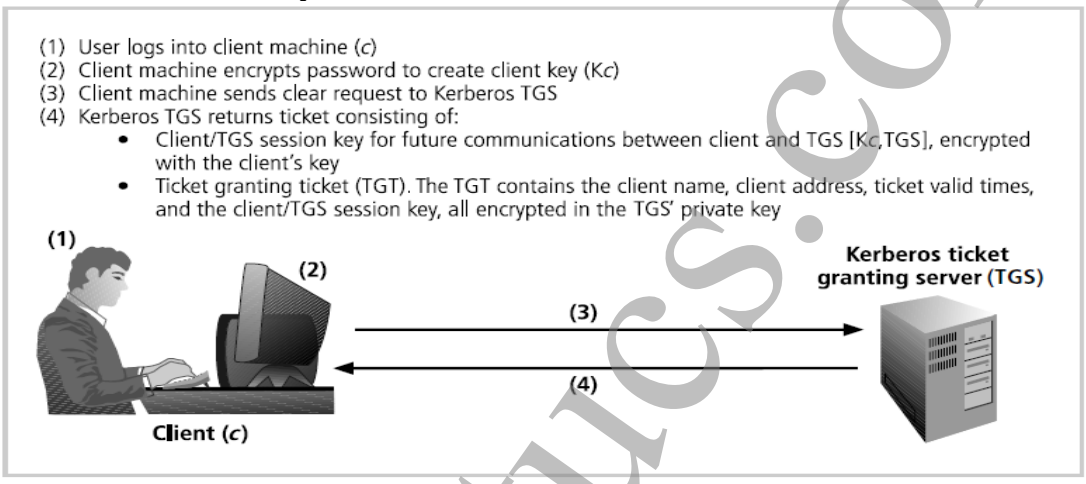


Figure 6-17 Kerberos Login

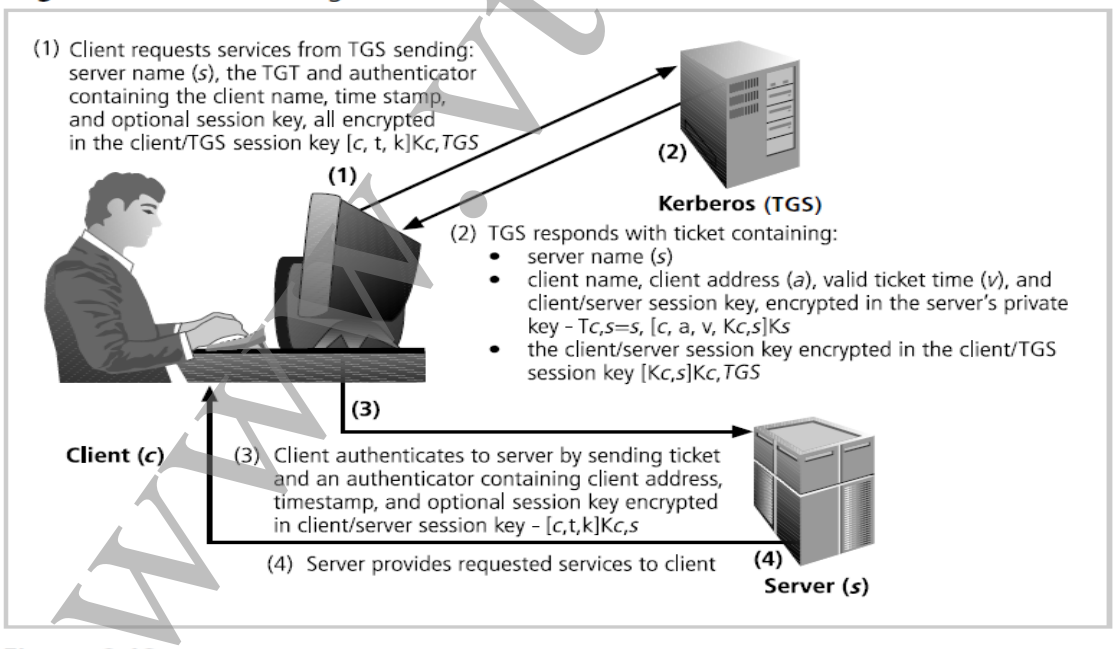


Figure 6-18 Kerberos Request for Services

SESAME

- The **Secure European System for Applications in a Multivendor Environment** (SESAME) is similar to Kerberos in that the user is first authenticated to an authentication server and receives a token.

- The token is then presented to a privilege attribute server (instead of a ticket granting service as in Kerberos) as proof of identity to gain a privilege attribute certificate (PAC).
- SESAME uses public key encryption to distribute secret keys.
- SESAME also builds on the Kerberos model by adding additional and more sophisticated access control features, more scalable encryption systems, improved manageability, auditing features, and the option to delegate responsibility for allowing access.

VIRTUAL PRIVATE NETWORKS

VPN is defined as "a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures."
The VPNC defines three VPN technologies:

- A **trusted VPN**, also known as a legacy VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits. The organization must trust the service provider, who provides contractual assurance that no one else is allowed to use these circuits and that the circuits are properly maintained and protected—hence the name *trusted* VPN.
- **Secure VPNs** use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet.
- A **hybrid VPN** combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following, regardless of the specific technologies and protocols being used:

- ***Encapsulation*** of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network and be usable by the server network environment.
- ***Encryption*** of incoming and outgoing data to keep the data contents private while in transit over the public network, but usable by the client and server computers and/or the local networks on both ends of the VPN connection.
- ***Authentication*** of the remote computer and, perhaps, the remote user as well. Authentication and the subsequent authorization of the user to perform specific actions are predicated on accurate and reliable identification of the remote system and/or user.

VPN can be implemented using either Transport mode or Tunnel mode. [Look at the diagrams & explain something]

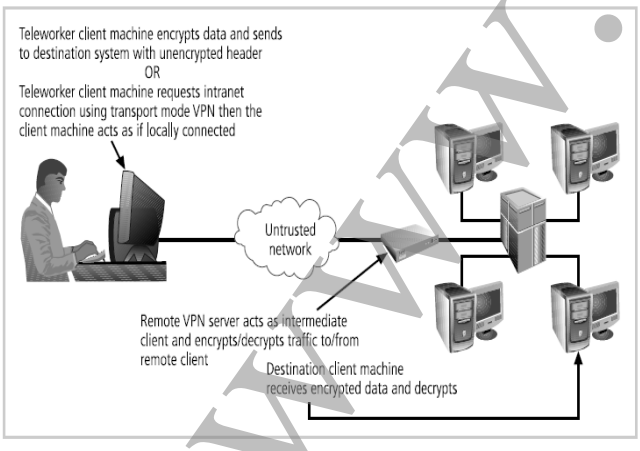


Figure 6-19 Transport Mode VPN

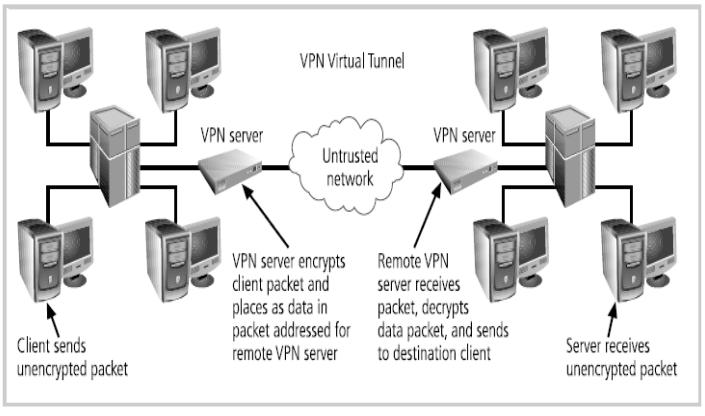


Figure 6-20 Tunnel Mode VPN

UNIT 3
SECURITY TECHNOLOGY – 2

INTRODUCTION

This chapter builds on that discussion by describing additional and more advanced technologies—intrusion detection and prevention systems, honeypots, honeynets, padded cell systems, scanning and analysis tools, and access controls—that organizations can use to enhance the security of their 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 information system, almost always with the intent to do harm.
- ♥ Even when such attacks are self-propagating, as in the case of viruses and distributed denial-of-service attacks, they are almost always instigated by someone whose purpose is to harm an organization.
- ♥ Intrusion ***prevention*** consists of activities that deter an intrusion.
- ♥ Some important intrusion prevention activities are writing and implementing good enterprise information security policy, planning and executing effective information security programs, installing and testing technology-based information security countermeasures (such as firewalls and intrusion detection systems), and conducting and measuring the effectiveness of employee training and awareness activities.
- ♥ Intrusion ***detection*** consists of procedures and systems that identify system intrusions.
- ♥ Intrusion ***reaction*** encompasses the actions an organization takes when an intrusion is detected.
- ♥ These actions seek to limit the loss from an intrusion and return operations to a normal state as rapidly as possible.
- ♥ Intrusion ***correction*** activities finalize the restoration of operations to a normal state and seek to identify the source and method of the intrusion in order to ensure that the same type of attack cannot occur again—thus reinitiating intrusion prevention.

- ★ Information security **intrusion detection systems (IDSs)** became commercially available in the late 1990s.
- ★ An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm.
- ★ This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (an e-mail message or pager alert).
- ★ With almost all IDSs, system administrators can choose the configuration of the various alerts and the alarm levels associated with each type of alert.
- ★ Many IDSs enable administrators to configure the systems to notify them directly of trouble via e-mail or pagers.
- ★ The configurations that enable IDSs to provide customized levels of detection and response are quite complex.
- ★ A current extension of IDS technology is the **intrusion prevention system (IPS)**, which can detect an intrusion and also prevent that intrusion from successfully attacking the organization by means of an active response.
- ★ Because the two systems often coexist, the combined term **intrusion detection and prevention system (IDPS)** is generally used to describe current anti-intrusion technologies.

IDPS TERMINOLOGY

Alert or alarm	An indication that a system has just been attacked or is under attack. IDPS alerts and alarms take the form of audible signals, e-mail messages, pager notifications, or pop-up windows.

Evasion	The process by which attackers change the format and/or timing of their activities to avoid being detected by the IDPS.
False attack stimulus	An event that triggers an alarm when no actual attack is in progress. Scenarios that test the configuration of IDPSs may use false attack stimuli to determine if the IDPSs can distinguish between these stimuli and real attacks.
False negative	The failure of an IDPS to react to an actual attack event. This is the most grievous failure, since the purpose of an IDPS is to detect and respond to attacks.
False positive	An alert or alarm that occurs in the absence of an actual attack. A false positive can sometimes be produced when an IDPS mistakes normal system activity for an attack. False positives tend to make users insensitive to alarms and thus reduce their reactivity to actual intrusion events.
Noise	Alarm events that are accurate and noteworthy but that do not pose significant threats to information security. Unsuccessful attacks are the most common source of IDPS noise, and some of these may in fact be triggered by scanning and enumeration tools deployed by network users without intent to do harm.
Site policy	The rules and configuration guidelines governing the implementation and operation of IDPSs within the organization.
Site policy awareness	A smart IDPS logs events that fit a specific profile instead of minor events, such as file modification or failed user logins. The smart IDPS knows when it does *not* need to alert the administrator
True attack stimulus	An event that triggers alarms and causes an IDPS to react as if a real attack is in progress. The event may be an actual attack, in which an attacker is at work on a system compromise attempt, or it may be a drill, in which security personnel are using hacker tools to conduct tests of a network segment.
Tuning	The process of adjusting an IDPS to maximize its efficiency in detecting true positives, while minimizing both false positives and false negatives.
Confidence value	The measure of an IDPS's ability to correctly detect and identify certain types of attacks.
Alarm filtering	The process of classifying IDPS alerts so that they can be more effectively managed. Alarm filters are similar to packet filters in that they can filter items by their source or destination IP addresses, but they can also filter by operating systems, confidence values, alarm type, or alarm severity.
Alarm clustering and compaction	A process of grouping almost identical alarms that happens at close to the same time into a single higher-level alarm. This consolidation reduces the number of alarms generated, thereby reducing administrative overhead, and also identifies a relationship among multiple alarms. This clustering may be based on combinations of frequency, similarity in attack signature, similarity in attack target, or other criteria that are defined by the system administrators.

WHY USE AN IDPS?

i. To prevent problem behaviours by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system
ii. To detect attacks and other security violations that are not prevented by other security measures
iii. To detect and deal with the preambles to attacks (commonly experienced as network probes and other "doorknob rattling" activities)
iv. To document the existing threat to an organization
v. To act as quality control for security design and administration, especially in large and complex enterprises
vi. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.

- IDPSs can also help administrators detect the preambles to attacks.
- Most attacks begin with an organized and thorough probing of the organization's network environment and its defenses.
- This initial estimation of the defensive state of an organization's networks and systems is called ***doorknob rattling*** and is accomplished by means of ***footprinting*** (activities that gather information about the organization and its network activities and assets) and ***fingerprinting*** (activities that scan network locales for active systems and then identify the network services offered by the host systems).
- A system capable of detecting the early warning signs of footprinting and fingerprinting functions like a neighbourhood watch that spots would-be burglars testing doors and windows, enabling administrators to prepare for a potential attack or to take actions to minimize potential losses from an attack.

- Data collected by an IDPS can also help management with quality assurance and continuous improvement; IDPSs consistently pick up information about attacks that have successfully compromised the outer layers of information security controls such as a firewall.
- The IDPS can also provide forensic information that may be useful should the attacker be caught and prosecuted or sued.

TYPES OF IDP SYSTEMS

- IDPSs operate as network- or host-based systems.
  - A network-based IDPS is focused on protecting network information assets.
  - Two specialized subtypes of network-based IDPS are the wireless IDPS and the network behavior analysis (NBA) IDPS.
    - The wireless IDPS focuses on wireless networks
    - NBA IDPS examines traffic flow on a network in an attempt to recognize abnormal patterns like DDoS, malware, and policy violations.
  - A host-based IDPS protects the server or host's information assets; the example shown in Figure 7-1 monitors both network connection activity and current information states on host servers. The application-based model works on one or more host systems that support a single application and defends that specific application from special forms of attack.

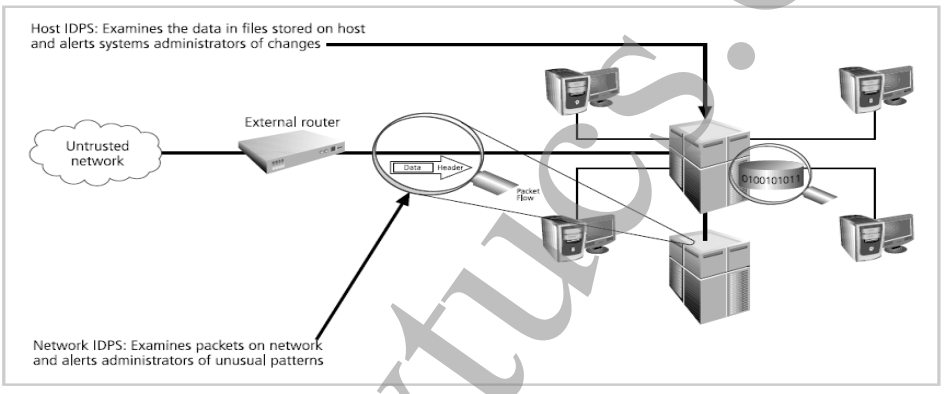


Figure 7-1 Intrusion Detection and Prevention Systems

Network-Based IDPS

- A network-based IDPS (NIDPS) resides on a computer or appliance connected to a segment of an organization's network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks.
- When the NIDPS identifies activity that it is programmed to recognize as an attack, it responds by sending notifications to administrators.
- An NIDPS can detect many more types of attacks than a host-based IDPS, but it requires a much more complex configuration and maintenance program.
- A NIDPS is installed at a specific place in the network from where it is possible to monitor the traffic going into and out of a particular network segment.
- The NIDPS can be deployed to monitor a specific grouping of host computers on a specific network segment, or it may be installed to monitor all traffic between the systems that make up an entire network.
- When placed next to a hub, switch, or other key networking device, the NIDPS may use that device's monitoring port.
- The **monitoring port** also known as a switched port analysis (SPAN) port or mirror port, is a specially configured connection on a network device that is capable of viewing all of the traffic that moves through the entire device.
- To determine whether an attack has occurred or is underway, NIDPSs compare measured activity to known signatures in their knowledge base.
- In the process of **protocol stack verification**, the NIDPSs look for invalid data packets—that is, packets that are malformed under the rules of the TCP/IP protocol.

- ★ In **application protocol verification**, the higher-order protocols (HTTP, FTP, and Telnet) are examined for unexpected packet behavior or improper use.

Advantages of NIDPSs

- ★ Good network design and placement of NIDPS devices can enable an organization to use a few devices to monitor a large network.
- ★ NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.
- ★ NIDPSs are not usually susceptible to direct attack and, in fact, may not be detectable by attackers.

Disadvantages of NIDPSs

- ★ A NIDPS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected.
- ★ NIDPSs require access to all traffic to be monitored.
- ★ NIDPSs cannot analyze encrypted packets, making some of the network traffic invisible to the process.
- ★ NIDPSs cannot reliably ascertain if an attack was successful or not.
- ★ In fact, some NIDPSs are particularly vulnerable to malformed packets and may become unstable and stop functioning

Wireless NIDPS → A wireless IDPS monitors and analyzes wireless network traffic, looking for potential problems with the wireless protocols.
Some issues associated with the implementation of wireless IDPSs include:

- ♠ **Physical security:** Many wireless sensors are located in public areas like conference rooms, assembly areas, and hallways in order to obtain the widest possible network range. Some of these locations may even be outdoors
- ♠ **Sensor range:** A wireless device's range can be affected by atmospheric conditions, building construction, and the quality of both the wireless network card and access point. Some IDPS tools allow an organization to identify the optimal location for sensors by modeling the wireless footprint based on signal strength.
- ♠ **Access point and wireless switch locations:** Wireless components with bundled IDPS capabilities must be carefully deployed to optimize the IDPS sensor detection grid. The minimum range is just that; you must guard against the possibility of an attacker connecting to a wireless access point from a range far beyond the minimum.
- ♠ **Wired network connections:** Wireless network components work independently of the wired network when sending and receiving between stations and access points.
- ♠ **Cost:** The more sensors deployed, the more expensive the configuration.

The wireless IDPS can also detect:

- ✓ Unauthorized WLANs and WLAN devices
- ✓ Poorly secured WLAN devices
- ✓ Unusual usage patterns
- ✓ The use of wireless network scanners
- ✓ Denial of service (DoS) attacks and conditions
- ✓ Impersonation and man-in-the-middle attacks

Wireless IDPSs are unable to detect certain passive wireless protocol attacks, in which the attacker monitors network traffic without active scanning and probing.

Network Behavior Analysis System → NBA systems examine network traffic in order to identify problems related to the flow of traffic. They use a version of the anomaly detection method to identify excessive packet flows such as might occur in the case of equipment malfunction, DoS attacks, virus and worm attacks, and some forms of network policy violations. Typical flow data particularly relevant to intrusion detection and prevention includes:

- ▶ Source and destination IP addresses
- ▶ Source and destination TCP or UDP ports or ICMP types and codes

- Number of packets and bytes transmitted in the session
- Starting and ending timestamps for the session

The types of events most commonly detected by NBA sensors include the following:

- ✓ DoS attacks (including DDoS attacks)
- ✓ Scanning
- ✓ Worms
- ✓ Unexpected application services (e.g., tunneled protocols, back doors, use of forbidden application protocols)
- ✓ Policy violations

Host-based IDPS

- ★ A host-based IDPS (HIDPS) resides on a particular computer or server, known as the host, and monitors activity only on that system.
- ★ HIDPSs are also known as ***system integrity verifiers*** because they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files.
- ★ An HIDPS has an advantage over an NIDPS in that it can access encrypted information travelling over the network and use it to make decisions about potential or actual attacks.
- ★ Also, since the HIDPS works on only one computer system, all the traffic it examines traverses that system.
- ★ An HIDPS is also capable of monitoring system configuration databases.
- ★ The HIDPS triggers an alert when one of the following occurs: file attributes change, new files are created, or existing files are deleted.
- ★ An HIDPS can also monitor systems logs for predefined events.
- ★ The HIDPS maintains its own log file so that an audit trail is available even when hackers modify files on the target system to cover their tracks.
- ★ The only time an HIDPS produces a false positive alert is when an authorized change occurs for a monitored file.
- ★ An HIDPS classifies files into various categories and then sends notifications when changes occur.
- ★ Managed HIDPSs can monitor multiple computers simultaneously by creating a configuration file on each monitored host.

Advantages of HIDPSs

- ★ An HIDPS can detect local events on host systems and also detect attacks that may elude a network-based IDPS.
- ★ An HIDPS functions on the host system, where encrypted traffic will have been decrypted and is available for processing.
- ★ The use of switched network protocols does not affect an HIDPS.
- ★ An HIDPS can detect inconsistencies in how applications and systems programs were used by examining the records stored in audit logs.

Disadvantages of HIDPSs

- ★ HIDPSs pose more management issues because they are configured and managed on each monitored host.
- ★ An HIDPS is vulnerable both to direct attacks and to attacks against the host operating system.
- ★ An HIDPS is not optimized to detect multi-host scanning, nor is it able to detect the scanning of non-host network devices, such as routers or switches.
- ★ An HIDPS is susceptible to some denial-of-service attacks.
- ★ An HIDPS can use large amounts of disk space to retain the host OS audit logs; to function properly, it may be necessary to add disk capacity to the system.
- ★ An HIDPS can inflict a performance overhead on its host systems, and in some cases may reduce system performance below acceptable levels.

IDPS DETECTION METHODS

IDPSs use a variety of detection methods to monitor and evaluate network traffic. Three methods dominate: the signature-based approach, the statistical-anomaly approach, and the stateful packet inspection approach.

Signature-Based IDPS

- A signature-based IDPS (sometimes called a knowledge-based IDPS or a misuse-detection IDPS) examines network traffic in search of patterns that match known signatures—that is, preconfigured, predetermined attack patterns.
- Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures, for example:
  - footprinting and fingerprinting activities use ICMP, DNS querying, and e-mail routing analysis;
  - exploits use a specific attack sequence designed to take advantage of a vulnerability to gain access to a system;
  - DoS and DDoS attacks, during which the attacker tries to prevent the normal usage of a system, overload the system with requests so that the system's ability to process them efficiently is compromised or disrupted.
- A potential problem with the signature-based approach is that new attack strategies must continually be added into the IDPS's database of signatures; otherwise, attacks that use new strategies will not be recognized and might succeed.
- Another weakness of the signature-based method is that a slow, methodical attack might escape detection if the relevant IDPS attack signature has a shorter time frame.
- The only way a signature-based IDPS can resolve this vulnerability is to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processing capacity.

Statistical Anomaly-Based IDPS

- The statistical anomaly-based IDPS (stat IDPS) or behavior-based IDPS collects statistical summaries by observing traffic that is known to be normal.
- This normal period of evaluation establishes a performance baseline.
- Once the baseline is established, the stat IDPS periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline.
- When the measured activity is outside the baseline parameters—exceeding what is called the clipping level—the IDPS sends an alert to the administrator.
- The baseline data can include variables such as host memory or CPU usage, network packet types, and packet quantities.
- The advantage of the statistical anomaly-based approach is that the IDPS can detect new types of attacks, since it looks for abnormal activity of any type.
- These systems require much more overhead and processing capacity than signature-based IDPSs, because they must constantly compare patterns of activity against the baseline.
- Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives.
- Because of its complexity and impact on the overhead computing load of the host computer as well as the number of false positives it can generate, this type of IDPS is less commonly used than the signature-based type.

Stateful Protocol Analysis IDPS

- Stateful protocol analysis (SPA) is a process of comparing predetermined profiles of generally accepted definitions of benign activity for each protocol state against observed events to identify deviations.
- By storing relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses, the IDPS can better detect specialized, multisession attacks.
- This process is sometimes called *deep packet inspection* because SPA closely examines packets at the application layer for information that indicates a possible intrusion.
- Stateful protocol analysis can also examine authentication sessions for suspicious activity as well as for attacks that incorporate "unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent, as well as 'reasonableness' for commands such as minimum and maximum lengths for arguments."
- The models used for SPA are similar to signatures in that they are provided by vendors.
- It requires heavy processing overhead to track multiple simultaneous connections.

Log File Monitors

- A log file monitor (LFM) IDPS is similar to a NIDPS.
- Using LFM, the system reviews the log files generated by servers, network devices, and even other IDPSs, looking for patterns and signatures that may indicate that an attack or intrusion is in process or has already occurred.
- LFM is able to look at multiple log files from a number of different systems.
- It requires considerable resources since it involves the collection, movement, storage, and analysis of very large quantities of log data.

IDPS RESPONSE BEHAVIOUR

Each IDPS responds to external stimulation in a different way, depending on its configuration and function.

IDPS Response Options

- When an IDPS detects a possible intrusion, it has a number of response options, depending on the implementing organization's policy, objectives, and system capabilities.
- When configuring an IDPS's responses, the system administrator must exercise care to ensure that a response to an attack (or potential attack) does not inadvertently exacerbate the situation.
- IDPS responses can be classified as active or passive.
    - An active response is a definitive action automatically initiated when certain types of alerts are triggered and can include collecting additional information, changing or modifying the environment, and taking action against the intruders.
    - Passive response IDPSs simply report the information they have collected and wait for the administrator to act.

The following list describes some of the responses an IDPS can be configured to produce.

- **Audible/visual alarm:** The IDPS can trigger a .wav file, beep, whistle, siren, or other audible or visual notification to alert the administrator of an attack. The most common type of such notifications is the computer pop-up, which can be configured with color indicators and specific messages.
- **SNMP traps and plug-ins:** The Simple Network Management Protocol contains trap functions, which allow a device to send a message to the SNMP management console indicating that a certain threshold has been crossed, either positively or negatively.
- **E-mail message:** The IDPS can send e-mail to notify network administrators of an event. Many administrators use smart-phones and other e-mail enabled devices to check for alerts and other notifications frequently. Organizations should use caution in relying on e-mail systems as the primary means of communication between the IDPS and security personnel e-mail is inherently unreliable, and an attacker could compromise the e-mail system and block such messages.
- **Page or phone message:** The IDPS can be configured to dial a phone number and produce an alphanumeric pager or a modem noise.
- **Log entry:** The IDPS can enter information about the event (e.g., addresses, time, systems involved, and protocol information) into an IDPS system log file or operating system log file. These files can be stored on separate servers to prevent skilled attackers from deleting entries about their intrusions.
- **Evidentiary packet dump**: Organizations that require an audit trail of the IDPS data may choose to record all log data in a special way. This method allows the organization to perform further analysis on the data and also to submit the data as evidence in a civil or criminal case. Once the data has been written using a cryptographic hashing algorithm, it becomes evidentiary documentation—that is, suitable for criminal or civil court use.
- **Take action against the intruder:** Known as trap-and-trace, back-hacking, or traceback, this response option involves configuring intrusion detection systems to trace the data from the target system to the attacking system in order to initiate a counterattack. While this may sound tempting, it is ill-advised and may not be legal.
- **Launch program:** An IDPS can be configured to execute a specific program when it detects specific types of attacks. A number of vendors have specialized tracking, tracing, and response software that can be part of an organization's intrusion response strategy.
- **Reconfigure firewall:** An IDPS can send a command to the firewall to filter out suspected packets by IP address, port, or protocol. An IDPS can block or deter intrusions via one of the following methods:

- Establishing a block for all traffic from the suspected attacker's IP address
- Establishing a block for specific TCP or UDP port traffic from the suspected attacker's address or source network, blocking only the services that seem to be under attack.
- Blocking all traffic to or from a network interface.

- **Terminate session:** Terminating the session by using the TCP/IP protocol specified packet *TCP close* is a simple process.
- **Terminate connection:** The last resort for an IDPS under attack is to terminate the organization's internal or external connections. Smart switches can cut traffic to or from a specific port.

Reporting and Archiving Capabilities

Commercial IDPSs can generate routine reports and other detailed information documents, such as reports of system events and intrusions detected over a particular reporting period

Failsafe Considerations for IDPS Responses

Failsafe features protect an IDPS from being circumvented or defeated by an attacker. There are several functions that require failsafe measures. Encrypted tunnels or other cryptographic measures that hide and authenticate communications are excellent ways to secure and ensure the reliability of the IDPS.

SELECTING IDPS APPROACHES AND PRODUCTS

The following considerations and questions may help you prepare a specification for acquiring and deploying an intrusion detection product. [Since it is not very important, I have given brief notes. For Extra info – refer text]

Technical and Policy Considerations

In order to determine which IDPS best meets an organization's needs, first consider the organizational environment in technical, physical, and political terms.

- **What Is Your Systems Environment?**
  - ✓ What are the technical specifications of your systems environment?
  - ✓ What are the technical specifications of your current security protections?
  - ✓ What are the goals of your enterprise?
  - ✓ How formal is the system environment and management culture in your organization?
- **What Are Your Security Goals and Objectives?**
  - ✓ Is the primary concern of your organization protecting from threats originating outside your organization?
  - ✓ Is your organization concerned about insider attack?
  - ✓ Does your organization want to use the output of your IDPS to determine new needs?
  - ✓ Does your organization want to use an IDPS to maintain managerial control (non-security related) over network usage?
- **What Is Your Existing Security Policy?**
  - ✓ How is it structured?
  - ✓ What are the general job descriptions of your system users?
  - ✓ Does the policy include reasonable use policies or other management provisions?
  - ✓ Has your organization defined processes for dealing with specific policy violations?

Organizational Requirements and Constraints

Your organization's operational goals, constraints, and culture will affect the selection of the IDPS and other security tools and technologies to protect your systems.

- **What Requirements Are Levied from Outside the Organization?**
  - ✓ Is your organization subject to oversight or review by another organization?
  - ✓ If so, does that oversight authority require IDPSs or other specific system security resources?
  - ✓ Are there requirements for public access to information on your organization's systems?
  - ✓ Do regulations or statutes require that information on your system be accessible by the public during certain hours of the day, or during certain date or time intervals?
  - ✓ Are there other security-specific requirements levied by law? Are there legal requirements for protection of personal information (such as earnings information or medical records) stored on your systems?
  - ✓ Are there legal requirements for investigation of security violations that divulge or endanger that information?
  - ✓ Are there internal audit requirements for security best practices or due diligence?
  - ✓ Do any of these audit requirements specify functions that the IDPSs must provide or support?

- ✓ Is the system subject to accreditation?
- ✓ If so, what is the accreditation authority's requirement for IDPSs or other security protection?
- ✓ Are there requirements for law enforcement investigation and resolution of security incidents?
- ✓ Do they require any IDPS functions, especially having to do with collection and protection of IDPS logs as evidence?

❖ **What Are Your Organization's Resource Constraints?**

- ✓ What is the budget for acquisition and life cycle support of intrusion detection hardware, software, and infrastructure?
- ✓ Is there sufficient existing staff to monitor an intrusion detection system full time?
- ✓ Does your organization have authority to instigate changes based on the findings of an intrusion detection system?

IDPSs Product Features and Quality

❖ **Is the Product Sufficiently Scalable for Your Environment?**

- ✓ Many IDPSs cannot function within large or widely distributed enterprise network environments.

❖ **How Has the Product Been Tested?**

- ✓ Has the product been tested against functional requirements?
- ✓ Has the product been tested against attack?

❖ **What Is the User Level of Expertise Targeted by the Product?**

- ✓ Different IDPS vendors target users with different levels of technical and security expertise. Ask the vendor what their assumptions are regarding the users of their products.

❖ **Is the Product Designed to Evolve as the Organization Grows?**

- ✓ Can the product adapt to growth in user expertise?
- ✓ Can the product adapt to growth and change of the organization's systems infrastructure?
- ✓ Can the product adapt to growth and change in the security threat environment?

❖ **What Are the Support Provisions for the Product?**

- ✓ What are the commitments for product installation and configuration support?
- ✓ What are the commitments for ongoing product support?
- ✓ Are subscriptions to signature updates included?
- ✓ How often are subscriptions updated?
- ✓ How quickly after a new attack is made public will the vendor ship a new signature?
- ✓ Are software updates included?
- ✓ How quickly will software updates and patches be issued after a problem is reported to the vendor?
- ✓ Are technical support services included? What is the cost?
- ✓ What are the provisions for contacting technical support?
- ✓ Are there any guarantees associated with the IDPS?
- ✓ What training resources does the vendor provide?
- ✓ What additional training resources are available from the vendor and at what cost?

STRENGTHS AND LIMITATIONS OF IDPSs

Strengths of Intrusion Detection and Prevention Systems

- Monitoring and analysis of system events and user behaviors
- Testing the security states of system configurations
- Baselining the security state of a system, then tracking any changes to that baseline
- Recognizing patterns of system events that correspond to known attacks
- Recognizing patterns of activity that statistically vary from normal activity
- Managing operating system audit and logging mechanisms and the data they generate
- Alerting appropriate staff by appropriate means when attacks are detected
- Measuring enforcement of security policies encoded in the analysis engine
- Providing default information security policies
- Allowing non-security experts to perform important security monitoring functions

Limitations of Intrusion Detection and Prevention Systems

- Compensating for weak or missing security mechanisms in the protection infrastructure, such as firewalls, identification and authentication systems, link encryption systems, access control mechanisms, and virus detection and eradication software

- Instantaneously detecting, reporting, and responding to an attack when there is a heavy network or processing load
- Detecting newly published attacks or variants of existing attacks
- Effectively responding to attacks launched by sophisticated attackers
- Automatically investigating attacks without human intervention
- Resisting all attacks that are intended to defeat or circumvent them
- Compensating for problems with the fidelity of information sources
- Dealing effectively with switched networks

DEPLOYMENT AND IMPLEMENTATION OF AN IDPS

The strategy for deploying an IDPS should take into account a number of factors - the number of administrators needed to install, configure, and monitor the IDPS, as well as the number of management workstations, the size of the storage needed for retention of the data generated by the systems, and the ability of the organization to detect and respond to remote threats.

IDPS Control Strategies

An IDPS can be implemented via one of three basic control strategies. A control strategy determines how an organization supervises and maintains the configuration of an IDPS. It also determines how the input and output of the IDPS is managed. The three commonly utilized control strategies are centralized, partially distributed, and fully distributed.

Centralized Control Strategy

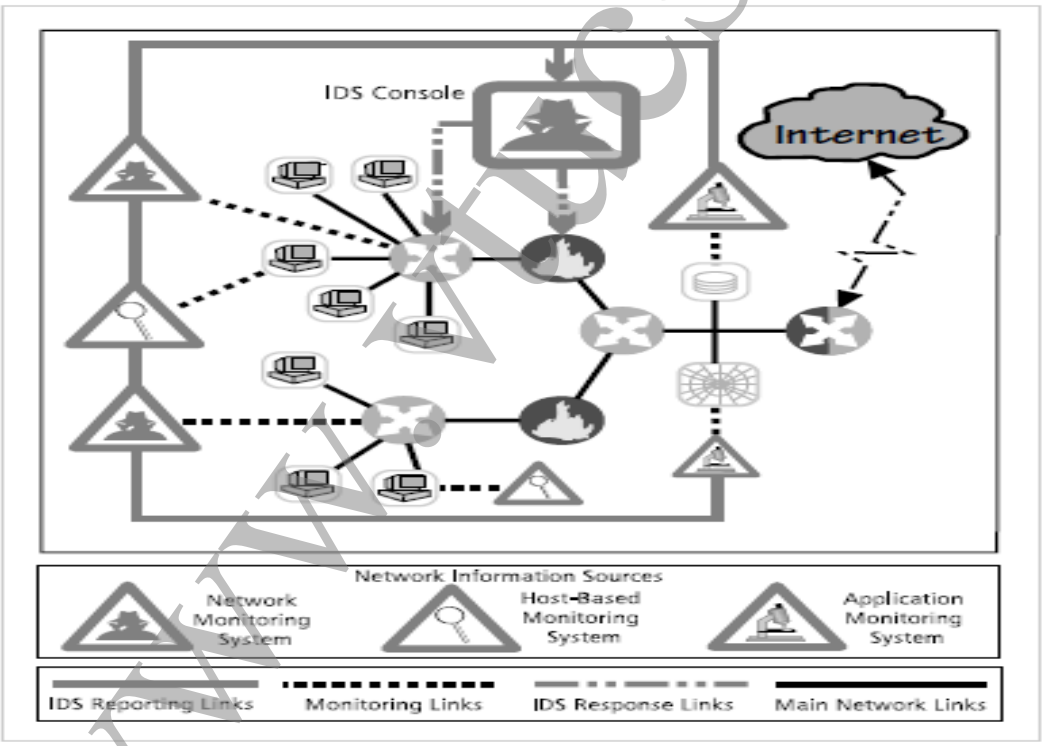


Figure 7-4 Centralized IDPS Control[13]

- All IDPS control functions are implemented and managed in a central location, represented in the figure with the large square symbol labelled "IDPS Console."
- The IDPS console includes the management software, which collects information from the remote sensors (triangular symbols in the figure), analyzes the systems or networks, and determines whether the current situation has deviated from the preconfigured baseline.
- All reporting features are implemented and managed from this central location.
- The primary advantages of this strategy are cost and control.
- With one central implementation, there is one management system, one place to go to monitor the status of the systems or networks, one location for reports, and one set of administrative management.
- This centralization of IDPS management supports task specialization

- This means that each person can focus specifically on an assigned task.
- In addition, the central control group can evaluate the systems and networks as a whole

Fully Distributed Control Strategy

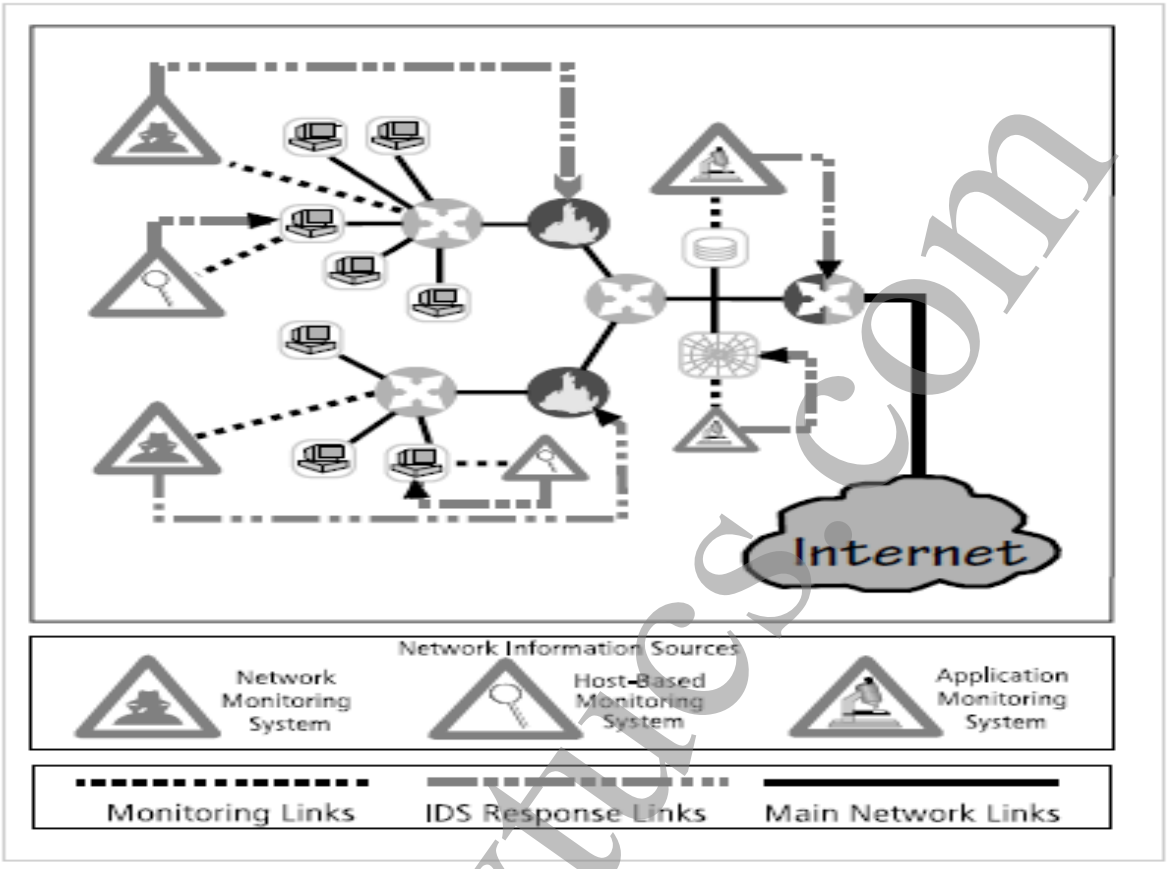


Figure 7-5 Fully Distributed IDPS Control[14]

- A fully distributed IDPS control strategy, illustrated in Figure 7-5, is the opposite of the centralized strategy.
- All control functions (which appear in the figure as small square symbols enclosing a computer icon) are applied at the physical location of each IDPS component.
- Each monitoring site uses its own paired sensors to perform its own control functions to achieve the necessary detection, reaction, and response functions.
- Thus, each sensor/agent is best configured to deal with its own environment.
- Since the IDPSs do not have to wait for a response from a centralized control facility, their response time to individual attacks is greatly enhanced.

Partially Distributed Control Strategy

- A partially distributed IDPS control strategy, depicted in Figure 7-6, combines the best of the other two strategies.
- While the individual agents can still analyze and respond to local threats, their reporting to a hierarchical central facility enables the organization to detect widespread attacks.
- This blended approach to reporting is one of the more effective methods of detecting intelligent attackers, especially those who probe an organization at multiple points of entry, trying to identify the systems' configurations and weaknesses, before they launch a concerted attack.
- The partially distributed control strategy also allows the organization to optimize for economy of scale in the implementation of key management software and personnel, especially in the reporting areas.
- When the organization can create a pool of security managers to evaluate reports from multiple distributed IDPS systems, it becomes better able to detect these distributed attacks before they become unmanageable.

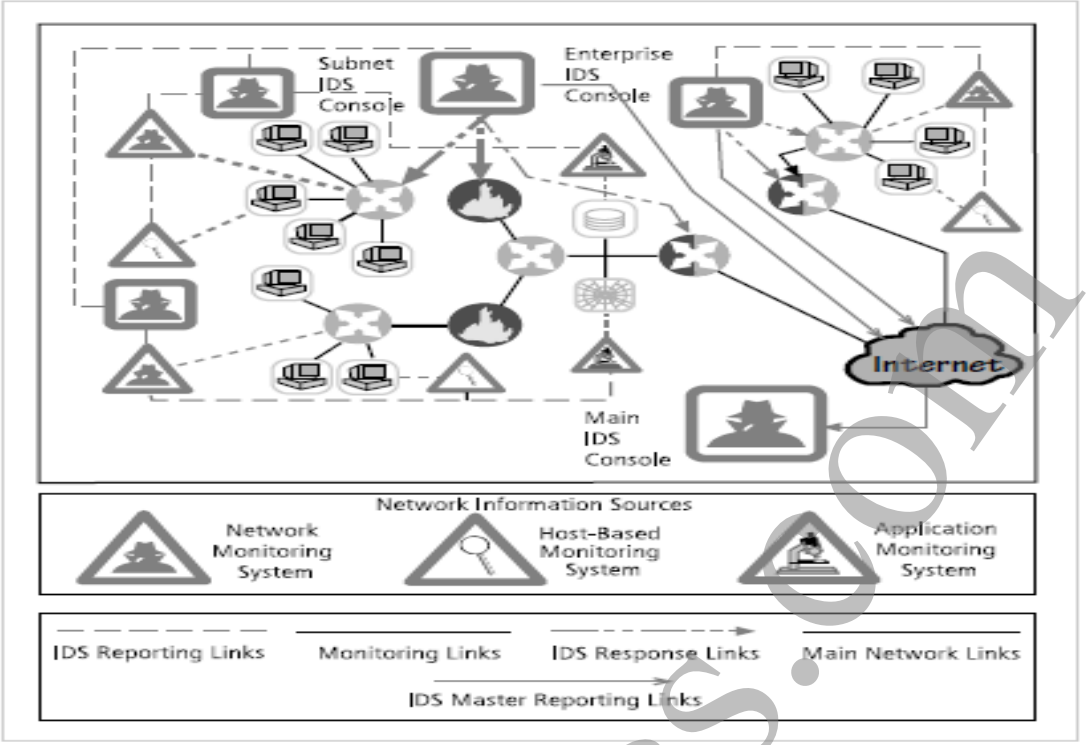


Figure 7-6 Partially Distributed IDPS Control[15]

IDPS Deployment

- Since IDPSs are designed to detect, report, and even react to anomalous stimuli, placing IDPSs in an area where such traffic is common can result in excessive reporting.
- One consideration is the skill level of the personnel who install, configure, and maintain the systems.
- An IDPS is a complex system in that it involves numerous remote monitoring agents (on both individual systems and networks) that require proper configuration to gain the proper authentication and authorization.
- As the IDPS is deployed, each component should be installed, configured, fine-tuned, tested, and monitored.
- A mistake in any step of the deployment process may produce a range of problems—from a minor inconvenience to a network-wide disaster.
- Thus, both the individuals installing the IDPS and the individuals using and managing the system require proper training.

Deploying Network-Based IDPSs

Location 1: Behind each external firewall, in the network DMZ (See Figure 7-7, location 1)

Advantages:

- IDPS sees attacks that originate from the outside that may penetrate the network's perimeter defenses.
- IDPS can identify problems with the network firewall policy or performance.
- IDPS sees attacks that might target the Web server or FTP server, both of which commonly reside in this DMZ.
- Even if the incoming attack is not detected, the IDPS can sometimes recognize, in the outgoing traffic, patterns that suggest that the server has been compromised.

Location 2: Outside an external firewall (See Figure 7-7, location 2)

Advantages:

- IDPS documents the number of attacks originating on the Internet that target the network.
- IDPS documents the types of attacks originating on the Internet that target the network.

Location 3: On major network backbones (See Figure 7-7, location 3)

Advantages:

- IDPS monitors a large amount of a network's traffic, thus increasing its chances of spotting attacks.
- IDPS detects unauthorized activity by authorized users within the organization's security perimeter.

Location 4: On critical subnets (See Figure 7-7, location 4)
Advantages:

- IDPS detects attacks targeting critical systems and resources.
- This location allows organizations with limited resources to focus these resources on the most valuable network assets.

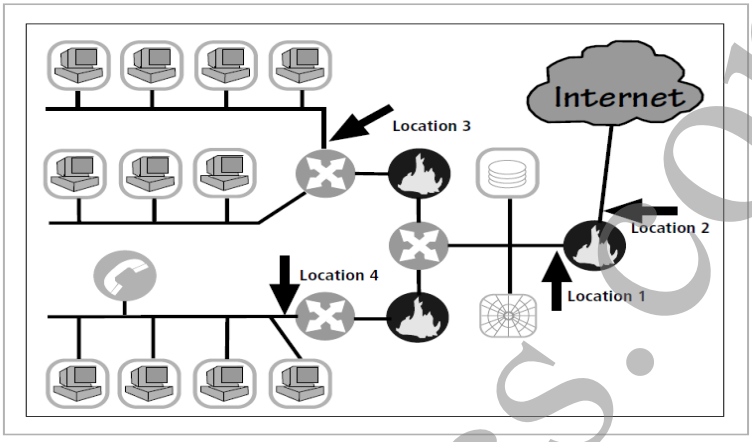


Figure 7-7 Network IDPS Sensor Locations[17]

Deploying Host-Based IDPSs

- The proper implementation of HIDPSs can be a painstaking and time-consuming task, as each HIDPS must be custom configured to its host systems.
- Deployment begins with implementing the most critical systems first.
- Practice helps the installation team gain experience and also helps determine if the installation might trigger any unusual events.
- Gaining an edge on the learning curve by training on nonproduction systems benefits the overall deployment process by reducing the risk of unforeseen complications.
- Installation continues until all systems are installed.
- To provide ease of management, control, and reporting, each HIDPS should, as discussed earlier, be configured to interact with a central management console.
- During the system testing process, training scenarios can be developed that will enable users to recognize and respond to common attack situations.
- To ensure effective and efficient operation, the management team can establish policy for the operation and monitoring of the HIDPS.

MEASURING THE EFFECTIVENESS OF IDPSs

When selecting an IDPS one typically looks at the following four measures of comparative effectiveness:

- **Thresholds:** A threshold is a value that sets the limit between normal and abnormal behavior. Thresholds usually specify a maximum acceptable level, such as x failed connection attempts in 60 seconds, or x characters for a filename length. Thresholds are most often used for anomaly-based detection and stateful protocol analysis.
- **Blacklists and whitelists:** A blacklist is a list of discrete entities, such as hosts, TCP or UDP port numbers, ICMP types and codes, applications, usernames, URLs, filenames, or file extensions, that have been associated with malicious activity. Blacklists, also known as hot lists, typically allow IDPSs to block activity that is highly likely to be malicious, and may also be used to assign a higher priority to alerts that match blacklist entries. A whitelist is a list of discrete entities that are known to be benign. Whitelists are typically used on a granular basis, such as protocol-by-protocol, to reduce or ignore false positives involving known benign activity from trusted hosts. Whitelists and blacklists are most commonly used in signature-based detection and stateful protocol analysis.

- **Alert settings:** Most IDPS technologies allow administrators to customize each alert type. Examples of actions that can be performed on an alert type include:
  - Toggling it on or off
  - Setting a default priority or severity level
  - Specifying what information should be recorded and what notification methods (e.g., e-mail, pager) should be used
  - Specifying which prevention capabilities should be used
    Some products also suppress alerts if an attacker generates many alerts in a short period of time and may also temporarily ignore all future traffic from the attacker. This is to prevent the IDPS from being overwhelmed by alerts.
- **Code viewing and editing**: Some IDPS technologies permit administrators to see some or all of the detection-related code. This is usually limited to signatures, but some technologies allow administrators to see additional code, such as programs used to perform stateful protocol analysis.

Some of these testing processes will enable the administrator to do the following:

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

HONEY POTS, HONEY NETS, AND PADDED CELL SYSTEMS

- Honeypots are decoy systems designed to lure potential attackers away from critical systems.
- In the industry, they are also known as decoys, lures, and fly-traps.
- When a collection of honeypots connects several honeypot systems on a subnet, it may be called a honeynet.
- A honeypot system (or in the case of a honeynet, an entire subnetwork) contains pseudo-services that emulate well-known services, but is configured in ways that make it look vulnerable to attacks.
- Honeypots are designed to do the following:
  - Divert an attacker from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond
- Because the information in a honeypot appears to be valuable, any unauthorized access to it constitutes suspicious activity.
- Honeypots are instrumented with sensitive monitors and event loggers that detect attempts to access the system and collect information about the potential attacker's activities.
- A **padded cell** is a honeypot that has been protected so that that it cannot be easily compromised—in other words, a hardened honeypot.
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS.
- When the IDPS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm.

The advantages and disadvantages of using the honeypot or padded cell approach are summarized below:

Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker.
- Attackers' actions can be easily and more extensively monitored, and the records can be used to refine threat models and improve system protections.
- Honeypots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implications of using such devices are not well understood.
- Honeypots and padded cells have not yet been shown to be generally useful security technologies.

- An expert attacker, once diverted into a decoy system, may become angry and launch a more aggressive attack against an organization's systems.
- Administrators and security managers need a high level of expertise to use these systems

TRAP-AND-TRACE SYSTEMS

- These systems use a combination of techniques to detect an intrusion and then trace it back to its source.
- The trap usually consists of a honeypot or padded cell and an alarm.
- While the intruders are distracted, or trapped, by what they perceive to be successful intrusions, the system notifies the administrator of their presence.
- The trace feature is an extension to the honeypot or padded cell approach.
- The trace—which is similar to caller ID—is a process by which the organization attempts to identify an entity discovered in unauthorized areas of the network or systems.
- If the intruder is someone inside the organization, the administrators are completely within their power to track the individual and turn him or her over to internal or external authorities.
- If the intruder is outside the security perimeter of the organization, then numerous legal issues arise.
- The trap portion frequently involves the use of honeypots or honeynets.
- When using honeypots and honeynets, administrators should be careful not to cross the line between enticement and entrapment.
- Enticement is the act of attracting attention to a system by placing tantalizing information in key locations.
- Entrapment is the act of luring an individual into committing a crime to get a conviction.
- Administrators should also be wary of the *wasp trap syndrome*.
- In this syndrome, a concerned homeowner installs a wasp trap in his back yard to trap the few insects he sees flying about.
- Security administrators should keep the wasp trap syndrome in mind before implementing honeypots, honeynets, padded cells, or trap-and-trace systems.

ACTIVE INTRUSION PREVENTION

- One tool that provides active intrusion prevention is known as LaBrea
- LaBrea is a "sticky" honeypot and IDPS and works by taking up the unused IP address space within a network.
- When LaBrea notes an ARP request, it checks to see if the IP address requested is actually valid on the network.
- If the address is not currently being used by a real computer or network device, LaBrea pretends to be a computer at that IP address and allows the attacker to complete the TCP/IP connection request, known as the three-way handshake.
- Once the handshake is complete, LaBrea changes the TCP sliding window size to a low number to hold open the TCP connection from the attacker for many hours, days, or even months.
- Holding the connection open but inactive greatly slows down network-based worms and other attacks.
- It allows the LaBrea system time to notify the system and network administrators about the anomalous behavior on the network.

SCANNING AND ANALYSIS TOOLS

- Scanning tools are, as mentioned earlier, typically used as part of an attack protocol to collect information that an attacker would need to launch a successful attack.
- The **attack protocol** is a series of steps or processes used by an attacker, in a logical sequence, to launch an attack against a target system or network.
- One of the preparatory parts of the attack protocol is the collection of publicly available information about a potential target, a process known as footprinting.

- **Footprinting** is the organized research of the Internet addresses owned or controlled by a target organization.

PORT SCANNERS

- Port scanning utilities, or **port scanners**, are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information.
- These tools can scan for specific types of computers, protocols, or resources, or their scans can be generic.
- It is helpful to understand the network environment so that you can use the tool most suited to the data collection task at hand.
- The more specific the scanner is, the more useful the information it provides to attackers and defenders.
- However, you should keep a generic, broad-based scanner in your toolbox to help locate and identify rogue nodes on the network that administrators may be unaware of.
- A port is a network channel or connection point in a data communications system.
- Within the TCP/IP networking protocol, TCP and User Datagram Protocol (UDP) port numbers differentiate the multiple communication channels that are used to connect to the network services being offered on the same network device.
- Each application within TCP/IP has a unique port number.

FIREWALL ANALYSIS TOOLS

- Understanding exactly where an organization's firewall is located and what the existing rule sets on the firewall do are very important steps for any security administrator.
- There are several tools that automate the remote discovery of firewall rules and assist the administrator (or attacker) in analyzing the rules to determine exactly what they allow and what they reject.
- The Nmap tool has option called *idle scanning* will allow the Nmap user to bounce your scan across a firewall by using one of the idle DMZ hosts as the initiator of the scan.
- Another tool that can be used to analyze firewalls is Firewalk which uses incrementing Time-To-Live (TTL) packets to determine the path into a network as well as the default firewall policy.
- A final firewall analysis tool worth mentioning is HPING, which is a modified ping client.
- It supports multiple protocols and has a command-line method of specifying nearly any of the ping parameters.
- Regardless of the tool that is used to validate or analyze a firewall's configuration, it is user intent that dictates how the information gathered is used;
- In order to defend a computer or network well, it is necessary to understand the ways it can be attacked.
- Thus, a tool that can help close up an open or poorly configured firewall will help the network defender minimize the risk from attack.

OPERATING SYSTEM DETECTION TOOLS

- Detecting a target computer's operating system is very valuable to an attacker, because once the OS is known, all of the vulnerabilities to which it is susceptible can easily be determined.
- There are many tools that use networking protocols to determine a remote computer's OS.
- One specific tool worth mentioning is XProbe, which uses ICMP to determine the remote OS.
- When run, XProbe sends many different ICMP queries to the target host.
- As reply packets are received, XProbe matches these responses from the target's TCP/IP stack with its own internal database of known responses.
- Xprobe is very reliable in finding matches and thus detecting the operating systems of remote computers.
- System and network administrators should take note of this and restrict the use of ICMP through their organization's firewalls and, when possible, within its internal networks.

VULNERABILITY SCANNERS

- **Active vulnerability scanners** scan networks for highly detailed information.
- An active scanner is one that initiates traffic on the network in order to determine security holes.
- This type of scanner identifies exposed usernames and groups, shows open network shares, and exposes configuration problems and other vulnerabilities in servers.
- Vulnerability scanners should be proficient at finding known, documented holes.
- There is a class of vulnerability scanners called blackbox scanners, or fuzzers.
- Fuzz testing is a straightforward testing technique that looks for vulnerabilities in a program or protocol by feeding random input to the program or a network running the protocol.
- Vulnerabilities can be detected by measuring the outcome of the random inputs.
- Nessus scanner has a class of attacks called *destructive*.
- A **passive vulnerability scanner** is one that listens in on the network and determines vulnerable versions of both server and client software.
- Passive scanners are advantageous in that they do not require vulnerability analysts to get approval prior to testing.
- These tools simply monitor the network connections to and from a server to obtain a list of vulnerable applications.
- Furthermore, passive vulnerability scanners have the ability to find client-side vulnerabilities that are typically not found by active scanners.

PACKET SNIFFERS

- A **packet sniffer** (sometimes called a network protocol analyzer) is a network tool that collects copies of packets from the network and analyzes them.
- It can provide a network administrator with valuable information for diagnosing and resolving networking issues.
- In the wrong hands, however, a sniffer can be used to eavesdrop on network traffic.
- There are both commercial and open-source sniffers.
- To use a packet sniffer legally, the administrator must
  - (1) be on a network that the organization owns,
  - (2) be under direct authorization of the owners of the network, and
  - (3) have knowledge and consent of the content creators.
- If all three conditions are met, the administrator can selectively collect and analyze packets to identify and diagnose problems on the network.
- Conditions one and two are self-explanatory.
- The third, consent, is usually handled by having all system users sign a release when they are issued a user ID and passwords.
- Many administrators feel that they are safe from sniffer attacks when their computing environment is primarily a switched network environment.

WIRELESS SECURITY TOOLS

- A wireless connection, while convenient, has many potential security holes.
- An organization that spends all of its time securing the wired network and leaves wireless networks to operate in any manner is opening itself up for a security breach.
- As a security professional, you must assess the risk of wireless networks.
- A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.
- Example – NetStumbler, AirSnare
- The tools discussed so far help the attacker and the defender prepare themselves to complete the next steps in the attack protocol: attack, compromise, and exploit.

UNIT 4
CRYPTOGRAPHY

INTRODUCTION

- The science of encryption, known as **cryptology**, encompasses *cryptography* and *cryptanalysis*.
- **Cryptography**, which comes from the Greek words *kryptos*, meaning "hidden," and *graphein*, meaning "to write," is the process of making and using codes to secure the transmission of information.
- Cryptanalysis is the process of obtaining the original message (called the **plaintext**) from an encrypted message (called the **ciphertext**) without knowing the algorithms and keys used to perform the encryption.
- **Encryption** is the process of converting an original message into a form that is unreadable to unauthorized individuals—that is, to anyone without the tools to convert the encrypted message back to its original format.
- **Decryption** is the process of converting the ciphertext message back into plaintext so that it can be readily understood.

TERMINOLOGY

- ★ **Algorithm:** The programmatic steps used to convert an unencrypted message into an encrypted sequence of bits that represent the message; sometimes refers to the programs that enable the cryptographic processes
- ★ **Cipher** or **cryptosystem:** An encryption method or process encompassing the algorithm, key(s) or cryptovariable(s), and procedures used to perform encryption and decryption
- ★ **Ciphertext** or **cryptogram:** The encoded message resulting from an encryption
- ★ **Code:** The process of converting components (words or phrases) of an unencrypted message into encrypted components
- ★ **Decipher:** To decrypt, decode, or convert, ciphertext into the equivalent plaintext
- ★ **Encipher:** To encrypt, encode, or convert, plaintext into the equivalent ciphertext
- ★ **Key** or **cryptovariable:** The information used in conjunction with an algorithm to create the ciphertext from the plaintext or derive the plaintext from the ciphertext; the key can be a series of bits used by a computer program, or it can be a passphrase used by humans that is then converted into a series of bits used by a computer program
- ★ **Keyspace:** The entire range of values that can be used to construct an individual key
- ★ **Link encryption:** A series of encryptions and decryptions between a number of systems, wherein each system in a network decrypts the message sent to it and then re-encrypts it using different keys and sends it to the next neighbor, and this process continues until the message reaches the final destination
- ★ **Plaintext** or **cleartext:** The original unencrypted message, or a message that has been successfully decrypted
- ★ **Steganography:** The hiding of messages—for example, within the digital encoding of a picture or graphic
- ★ **Work factor:** The amount of effort (usually in hours) required to perform cryptanalysis to decode an encrypted message when the key or algorithm (or both) are unknown

ELEMENTS OF CRYPTOSYSTEMS

Cryptosystems are made up of a number of elements or components – algorithms, data handling techniques, and procedures and process steps – which are combined in multiple ways to ensure confidentiality and provide authentication and authorization for business processes.

CIPHER METHODS

There are two methods of encrypting plaintext: the ***bit stream method or the block cipher method***. In the bit stream method, each bit in the plaintext is transformed into a cipher bit one bit at a time. In the block cipher method, the message is divided into blocks, for example, sets of 8-, 16-, 32-, or 64-bit blocks, and then each block of plaintext bits is transformed into an encrypted block of cipher bits using an algorithm and a key.
Bit stream methods commonly use algorithm functions like the exclusive OR operation (XOR), whereas block methods can use substitution, transposition, XOR or combination of these.

SUBSTITUTION CIPHER

To use a substitution cipher, you substitute one value for another, for example a letter in the alphabet with the letter three values to the right. Or you can substitute one bit for another bit that is four places to its left.

Initial alphabet yields	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption alphabet	DEFGHIJKLMNOPQRSTUVWXYZABC

Within this substitution scheme, the plaintext MOM would be encrypted into the ciphertext PRP.
This type of substitution is based on a **monoalphabetic substitution**, because it only uses one alphabet. More advanced substitution ciphers use two or more alphabets, and are referred to as **polyalphabetic substitutions**.

Plaintext =	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution cipher 1 =	DEFGHIJKLMNOPQRSTUVWXYZABC
Substitution cipher 2 =	GHIJKLMNOPQRSTUVWXYZABCDEF
Substitution cipher 3 =	JKLMNOPQRSTUVWXYZABCDEFGHI
Substitution cipher 4 =	MNOPQRSTUVWXYZABCDEFGHIJKL

Example TEXT → WKGF
T is transformed to W – referring to second row
E is transformed to K – referring to third row and so on

- ★ An advanced type of substitution cipher that uses a **simple polyalphabetic** code is the **Vigenère cipher**.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 8-2 The Vigenère Square

- ★ The cipher is implemented using the Vigenère square (or table), which is made up of twenty-six distinct cipher alphabets.

- ★ You could perform an encryption by simply starting in the first row and finding a substitute for the first letter of plaintext, and then moving down the rows for each subsequent letter of plaintext.
- ★ With this method, the word SECURITY in plaintext becomes TGFYWOAG in ciphertext.

TRANSPOSITION CIPHER

Transposition cipher (or **permutation cipher**) simply rearranges the values within a block to create the cipher text. This can be done at the bit level or at the byte (character) level.

Key pattern: 1→4, 2→8, 3→1, 4→5, 5→7, 6→2, 7→6, 8→3

In this key, the bit or byte (character) in position 1 (with position 1 being at the far right) moves to position 4 (counting from the right), and the bit or byte in position 2 moves to position 8, and so on.

The following rows show the numbering of bit locations for this key; the plaintext message 00100101011010111001010101010100, which is broken into 8-bit blocks for clarity; and the cipher text that is produced when the transposition key depicted above is applied to the plaintext:

```
Bit locations:          87654321 87654321 87654321 87654321
Plaintext 8-bit blocks: 00100101|01101011|10010101|01010100
Ciphertext:             00001011|10111010|01001101|01100001
```

Reading from right to left in the example above, the first bit of plaintext (position 1 of the first byte) becomes the fourth bit (in position 4) of the first byte of the cipher text. Similarly, the second bit of the plaintext (position 2) becomes the eighth bit (position 8) of the cipher text, and so on.

To examine further how this transposition key works, look at its effects on a plaintext message comprised of letters instead of bits. Replacing the 8-bit block of plaintext with the example plaintext message presented earlier, "SACK GAUL SPARE NO ONE," yields the following:

```
Letter locations: 87654321|87654321|87654321|87654321|
Plaintext:        SACKGAUL|SPARENOO|NE      |        |
Key: Same key as above, but characters transposed, not bits.
Ciphertext:       UKAGLSCA|ORPEOSAN|  E  N  |        |
```

For example, if you are the recipient of the Caesar cipher text shown below you would make a square of five columns and five rows, and then write the letters of the message into the square, filling the slots from left to right, top to bottom. Then you read the message from the opposite direction—that is, from top to bottom, left to right.

```
Ciphertext: SGS_NAAPNECUAO_KLR _ _ _ _ EO
            S G S _ N
            A A P N E
            C U A O
            K L R _ _
            _ _ E O _
```

Reading from top to bottom, left to right reveals the plaintext "SACK GAUL SPARE NO ONE."

EXCLUSIVE OR

The exclusive OR operation (XOR) is a function of Boolean algebra in which two bits are compared, and if the two bits are identical, the result is a binary 0. If the two bits are not the same, the result is a binary 1.

First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

Table 8-3 XOR Truth Table

Text Value	Binary Value
CAT as bits	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 0 0
VVV as key	0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0
Cipher	0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1 0

Table 8-4 Example XOR Encryption

VERNAM CIPHER

- ★ Also known as the one-time pad, the Vernam cipher uses a set of characters only one time for each encryption process.
- ★ To perform the Vernam cipher encryption operation, the pad values are added to numeric values that represent the plaintext that needs to be encrypted.
- ★ Each character of the plaintext is turned into a number and a pad value for that position is added to it.
- ★ The resulting sum for that character is then converted back to a ciphertext letter for transmission.

Plaintext:	S	A	C	K	G	A	U	L	S	P	A	R	E	N	O	O	N	E
Plaintext value:	19	01	03	11	07	01	21	12	19	16	01	18	05	14	15	15	14	05
One-time pad text:	F	P	Q	R	N	S	B	I	E	H	T	Z	L	A	C	D	G	J
One time pad value:	06	16	17	18	14	19	02	09	05	08	20	26	12	01	03	04	07	10
Sum of plaintext and pad:	25	17	20	29	21	20	23	21	24	24	21	44	17	15	18	19	21	15
After modulo Subtraction:				03								18						
Ciphertext:	Y	Q	T	C	U	T	W	U	X	X	U	R	Q	O	R	S	U	O

- ★ The decryption process works as follows: "Y" becomes the number 25, from which we subtract the pad value for the first letter of the message, 06. This yields a value of 19, or the letter "S."

BOOK OR RUNNING KEY CIPHER

- ★ The ciphertext consists of a list of codes representing the page number, line number, and word number of the plaintext word.
- ★ The algorithm is the mechanical process of looking up the references from the ciphertext and converting each reference to a word by using the ciphertext's value and the key.
- ★ To decrypt the ciphertext, the receiver acquires the book and turns to page 259, finds line 19, and selects the eighth word in that line.

HASH FUNCTIONS

- ★ Hash functions are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content.
- ★ While they do not create a ciphertext, hash functions confirm message identity and integrity, both of which are critical functions in e-commerce.
- ★ Hash algorithms are public functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value.
- ★ The message digest is a fingerprint of the author's message that is compared with the recipient's locally calculated hash of the same message.
- ★ If both hashes are identical after transmission, the message has arrived without modification.
- ★ Hashing functions do not require the use of keys, but it is possible to attach a ***message authentication code (MAC)***—a key-dependent, one-way hash function—that allows only specific recipients (symmetric key holders) to access the message digest.
- ★ Because hash functions are one-way, they are used in password verification systems to confirm the identity of the user.
- ★ The number of bits used in the hash algorithm is a measurement of the strength of the algorithm against collision attacks.
- ★ A recent attack method called rainbow cracking has generated concern about the strength of the processes used for password hashing.

- ★ In general, if attackers gain access to a file of hashed passwords, they can use a combination of brute force and dictionary attacks to reveal user passwords.
- ★ Passwords that are dictionary words or poorly constructed can be easily cracked.
- ★ Well-constructed passwords take a long time to crack even using the fastest computers, but by using a rainbow table—a database of precomputed hashes from sequentially calculated passwords—the rainbow cracker simply looks up the hashed password and reads out the text version, no brute force required.
- ★ This type of attack is more properly classified as a ***time–memory tradeoff attack.***
- ★ ***Salting*** is the process of providing a non-secret, random piece of data to the hashing function when the hash is first calculated.
- ★ The use of the salt value creates a different hash and when a large set of salt values are used, rainbow cracking fails since the time-memory tradeoff is no longer in the attacker's favor.

CRYPTOGRAPHIC ALGORITHMS

In general, cryptographic algorithms are often grouped into two broad categories: symmetric and asymmetric. Symmetric and asymmetric algorithms are distinguished by the types of keys they use for encryption and decryption operations.

SYMMETRIC ENCRYPTION

- ★ Encryption methodologies that require the same secret key to encipher and decipher the message are using what is called private key encryption or symmetric encryption.
- ★ Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that the encryption and decryption processes are executed quickly by even small computers.
- ★ One of the challenges is that both the sender and the recipient must have the secret key.
- ★ The primary challenge of symmetric key encryption is getting the key to the receiver, a process that must be conducted out of band to avoid interception.

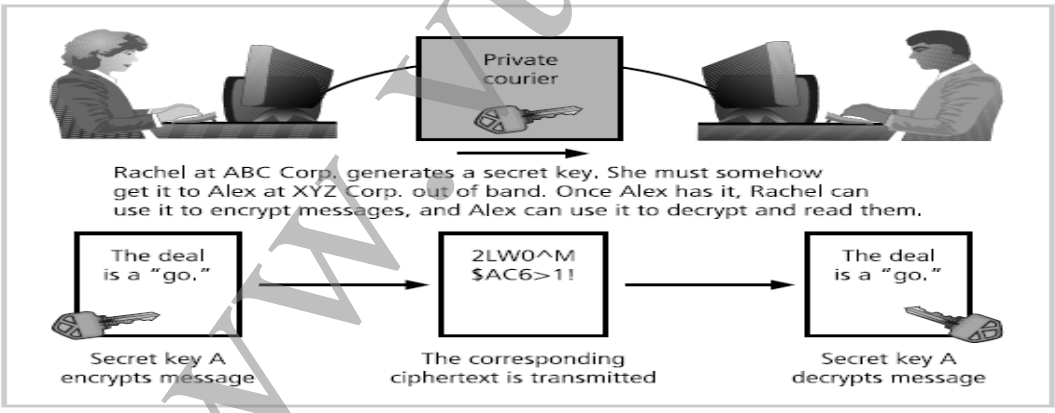


Figure 8-5 Example of Symmetric Encryption

Popular symmetric encryption cryptosystems are:

- DES
  - Data Encryption Standard
  - Developed by IBM
  - Uses a 64-bit block size & a 56-bit key
- 3DES
  - Triple DES - Advanced application of DES
- AES
  - Advanced Encryption Standard
  - Successor to 3DES
  - Implements a block cipher called Rijndael Block Cipher with a variable block length and key length of 128, 192 or 256 bits

ASYMMETRIC ENCRYPTION

- ★ **Asymmetric encryption** uses two different but related keys, and either key can be used to encrypt or decrypt the message.
- ★ If, however, key A is used to encrypt the message, only key B can decrypt it, and if key B is used to encrypt a message, only key A can decrypt it.

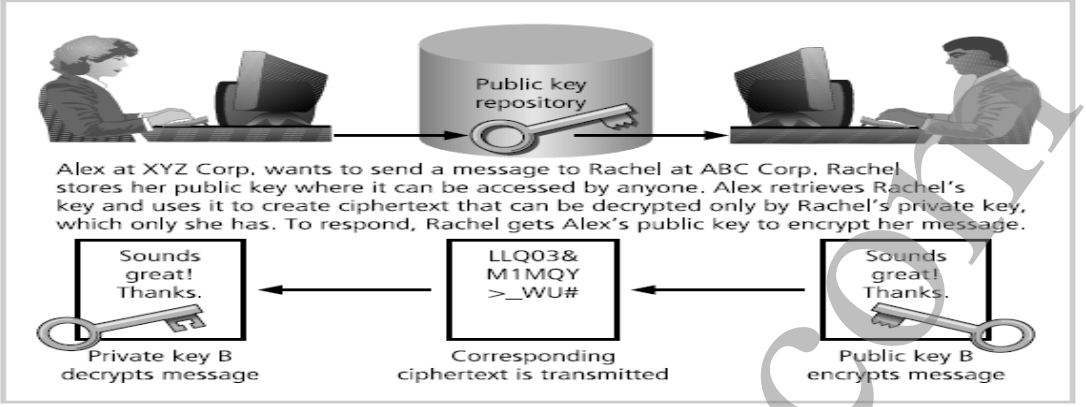


Figure 8-6 Example of Asymmetric Encryption

- ★ Asymmetric encryption can be used to provide elegant solutions to problems of secrecy and verification.
- ★ This technique has its highest value when one key is used as a private key, which means that it is kept secret known only to the owner of the key pair, and the other key serves as a public key, which means that it is stored in a public location where anyone can use it.
- ★ This is why the more common name for asymmetric encryption is **public-key encryption**.
- ★ Asymmetric algorithms are one-way functions.
- ★ A one-way function is simple to compute in one direction, but complex to compute in the opposite direction.
- ★ This is the foundation of public-key encryption.
- ★ The **RSA algorithm** was the first public key encryption algorithm.
- ★ The problem with asymmetric encryption, as shown earlier in the example in Figure 8-6, is that holding a single conversation between two parties requires four keys.

ENCRYPTION KEY SIZE

When deploying ciphers, users have to decide on the size of the key. [Refer Text - if interested – not so important.]

CRYPTOGRAPHIC TOOLS

- ★ Public Key Infrastructure
- ★ Digital Signature
- ★ Digital Certificate
- ★ Hybrid Cryptographic Systems
- ★ Steganography

PUBLIC KEY INFRASTRUCTURE

- ★ **Public-key Infrastructure (PKI)** is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.
- ★ PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).
- ★ These processes include the following:
  - ***Authentication:*** Individuals, organizations, and Web servers can validate the identity of each of the parties in an Internet transaction.
  - ***Integrity:*** Content signed by the certificate is known to not have been altered while in transit from host to host or server to client.

- ***Privacy:*** Information is protected from being intercepted during transmission.
- ***Authorization:*** The validated identity of users and programs can enable authorization rules that remain in place for the duration of a transaction; this reduces some of the overhead and allows for more control of access privileges for specific transactions.
- ***Non-repudiation:*** Customers or partners can be held accountable for transactions, such as online purchases, which they cannot later dispute.

★ A typical PKI solution protects the transmission and reception of secure information by integrating the following components:

- A **certificate authority (CA)**, which issues, manages, authenticates, signs, and revokes users' digital certificates, which typically contain the user name, public key, and other identifying information.
- A **registration authority (RA)**, which operates under the trusted collaboration of the certificate authority and can handle day-to-day certification functions, such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates.
- **Certificate directories,** which are central locations for certificate storage that provide a single access point for administration and distribution.
- **Management protocols,** which organize and manage the communications among CAs, RAs, and end users. This includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and enabling the transfer of certificates and status information among the parties involved in the PKI's area of authority.
- **Policies and procedures,** which assist an organization in the application and management of certificates, in the formalization of legal liabilities and limitations, and in actual business use.

★ Common implementations of PKI include systems that issue digital certificates to users and servers; directory enrolment; key issuing systems; tools for managing the key issuance; and verification and return of certificates.

★ These systems enable organizations to apply an enterprise-wide solution that provides users within the PKI's area of authority the means to engage in authenticated and secure communications and transactions.

★ The strength of a cryptosystem relies on both the raw strength of its key's complexity and the overall quality of its key management security processes.

★ PKI solutions can provide several mechanisms for limiting access and possible exposure of the private keys.

DIGITAL SIGNATURE

- Digital signatures were created in response to the rising need to verify information transferred via electronic systems.
- Asymmetric encryption processes are used to create digital signatures.
- When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message.
- When the decryption is successful, the process verifies that the message was sent by the sender and thus cannot be refuted.
- This process is known as **non-repudiation** and is the principle of cryptography that underpins the authentication mechanism collectively known as a digital signature.
- Digital signatures are, therefore, encrypted messages that can be mathematically proven authentic.
- The management of digital signatures is built into most Web browsers.
- In general, digital signatures should be created using processes and products that are based on the **Digital Signature Standard** (DSS).
- This process first creates a message digest using the hash algorithm, which is then input into the digital signature algorithm along with a random number to generate the digital signature.
- The digital signature function also depends upon the sender's private key and other information provided by the CA.

DIGITAL CERTIFICATES

- A digital certificate is an electronic document or container file that contains a key value and identifying information about the entity that controls the key.
- The certificate is often issued and certified by a third party, usually a certificate authority.
- A digital signature attached to the certificate's container file certifies the file's origin and integrity.
- This verification process often occurs when you download or update software via the Internet.
- Digital certificates authenticate the cryptographic key that is embedded in the certificate.
- When used properly these certificates enable diligent users to verify the authenticity of any organization's certificates.
  - The CA application suite issues and uses certificates (keys) that identify and establish a trust relationship with a CA to determine what additional certificates (keys) can be authenticated.
  - Mail applications use Secure/Multipurpose Internet Mail Extension (S/MIME) certificates for signing and encrypting e-mail as well as for signing forms.
  - Development applications use object-signing certificates to identify signers of object-oriented code and scripts.
  - Web servers and Web application servers use Secure Sockets Layer (SSL) certificates to authenticate servers via the SSL protocol (which is described shortly) in order to establish an encrypted SSL session.
  - Web clients use client SSL certificates to authenticate users, sign forms, and participate in single sign-on solutions via SSL.

Example → An X.509 v3 certificate binds a **distinguished name (DN)**, which uniquely identifies a certificate entity, to a user's public key.

X.509 v3 Certificate Structure
Version
Certificate Serial Number
Algorithm ID • Algorithm ID • Parameters
Issuer Name
Validity • Not Before • Not After
Subject Name
Subject Public Key Info • Public Key Algorithm • Parameters • Subject Public Key
Issuer Unique Identifier (Optional)
Subject Unique Identifier (Optional)
Extensions (Optional) • Type • Criticality • Value
Certificate Signature Algorithm
Certificate Signature

Table 8-8 X.509 v3 Certificate Structure[11]

HYBRID CRYPTOGRAPHY SYSTEMS

- The most common hybrid system is based on the **Diffie-Hellman key exchange**, which is a method for exchanging private keys using public key encryption.
- Diffie-Hellman key exchange uses asymmetric encryption to exchange **session keys**.
- These are limited-use symmetric keys for temporary communications; they allow two entities to conduct quick, efficient, secure communications based on symmetric encryption, which is more efficient than asymmetric encryption for sending messages.
- Diffie-Hellman provides the foundation for subsequent developments in public key encryption.
- It protects data from exposure to third parties, which is sometimes a problem when keys are exchanged out-of-band.

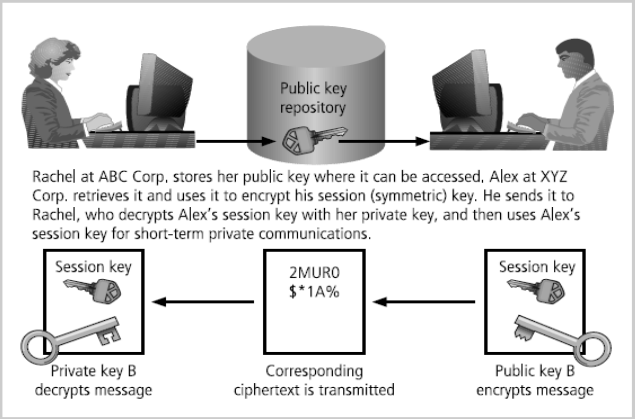


Figure 8-9 Example of Hybrid Encryption

STEGANOGRAPHY

- The word steganography—the art of secret writing—is derived from the Greek words *steganos*, meaning "covered" and *graphein*, meaning "to write."
- While Steganography is technically not a form of cryptography, it is another way of protecting the confidentiality of information in transit.
- The most popular modern version of Steganography involves hiding information within files that contain digital pictures or other images.
- To understand how this form of steganography works, you must first know a little about how images are stored.
- Most computer graphics standards use a combination of three color values—red, blue, and green (RGB)—to represent a picture element, or pixel.
- Each of the three color values usually requires an 8-bit code for that color's intensity (e.g., 00000000 for
- no red and 11111111 for maximum red).
- Each color image pixel requires 3 colors 8 bits 24 bits to represent the color mix and intensity.
- An image that is 1024x768 pixels contains 786,432 groups of 24 bits to represent the red, green, and blue data.
- The raw image size can be calculated as 1024x768x24, or 5.66 megabytes.
- There are plenty of bits in this picture data file in which to hide a secret message.
- To the naked eye, there is no discernable difference between a pixel with a red intensity of 00101001 and another slightly different pixel with a red intensity level of 00101000.
- This provides the steganographer with one bit per color (or three bits per pixel) to use for encoding data into an image file.
- If a steganographic process uses three bits per pixel for all 786,432 pixels, it will be able to store 236 kilobytes of hidden data within the uncompressed image.
- Some steganographic tools can calculate the maximum size image that can be stored before being detectable.
- Messages can also be hidden in non-image computer files that do not utilize all of their available bits by placing the data in places where software ignores it and humans almost never look.

ATTACKS ON CRYPTOSYSTEMS

- An attacker may obtain duplicate texts, one in cipher text and one in plaintext, and thus reverse-engineer the encryption algorithm in a **known-plaintext attack** scheme.
- Alternatively, attackers may conduct a **selected-plaintext attack** by sending potential victims a specific text that they are sure the victims will forward on to others. When the victim does encrypt and forward the message, it can be used in the attack if the attacker can acquire the outgoing encrypted version.

In general, attacks on cryptosystems fall into four general categories: man-in-the-middle, correlation, dictionary, and timing.

- **Man-in-the-middle attack**
  - ✓ Attempts to intercept a public key or even to insert a known key structure in place of the requested public key.
  - ✓ Thus, attackers attempt to place themselves between the sender and receiver, and once they've intercepted the request for key exchanges, they send each participant a valid public key, which is known only to them.
  - ✓ Establishing public keys with digital signatures can prevent the traditional man-in-the-middle attack, as the attacker cannot duplicate the signatures.

- **Correlation Attacks**
  - ✓ Correlation attacks are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the cipher text generated by the cryptosystem.
  - ✓ Differential and linear cryptanalysis, which are advanced methods of code breaking that are beyond the scope of this text, have been used to mount successful attacks on block cipher encryptions such as DES.
  - ✓ The only defence against this attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of key changes.

- **Dictionary Attacks**
  - ✓ The attacker encrypts every word in a dictionary using the same cryptosystem as used by the target in an attempt to locate a match between the target cipher text and the list of encrypted words.
  - ✓ Dictionary attacks can be successful when the cipher text consists of relatively few characters, as for example files which contain encrypted usernames and passwords.
  - ✓ An attacker who acquires a system password file can run hundreds of thousands of potential passwords from the dictionary he or she has prepared against the stolen list.
  - ✓ After a match is found, the attacker has essentially identified a potential valid password for the system.

- **Timing Attacks**
  - ✓ The attacker eavesdrops on the victim's session and uses statistical analysis of patterns and inter-keystroke timings to discern sensitive session information.
  - ✓ While timing analysis may not directly result in the decryption of sensitive data, it can be used to gain information about the encryption key and perhaps the cryptosystem.
  - ✓ Having broken an encryption, the attacker may launch a **replay attack**, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a secure source.

- **Defending Against Attacks**
  - ✓ Encryption is a very useful tool in protecting the confidentiality of information that is in storage or transmission.
  - ✓ Over millennia, mankind has developed dramatically more sophisticated means of hiding information from those who should not see it, but no matter how sophisticated encryption and cryptosystems have become, they retain the flaw that was present in the very first such system: If you discover the key, that is, the method used to perform the encryption, you can read the message.
  - ✓ Thus, key management is not so much the management of technology but rather the management of people.
  - ✓ Encryption helps organizations secure information that must travel through public and leased networks by guarding the information against the efforts of those who sniff, spoof, and otherwise skulk around.

UNIT 5
INTRODUCTION TO NETWORK SECURITY, AUTHENTICATION APPLICATIONS

THE OSI SECURITY ARCHITECTURE

Table 1.1 Threats and Attacks (RFC 2828)

Threat A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
Attack An assault on system security that derives from an intelligent threat. That is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

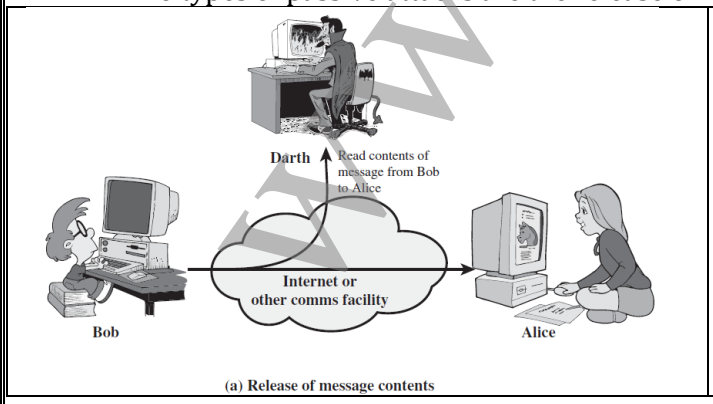
SECURITY ATTACKS

Classified as -

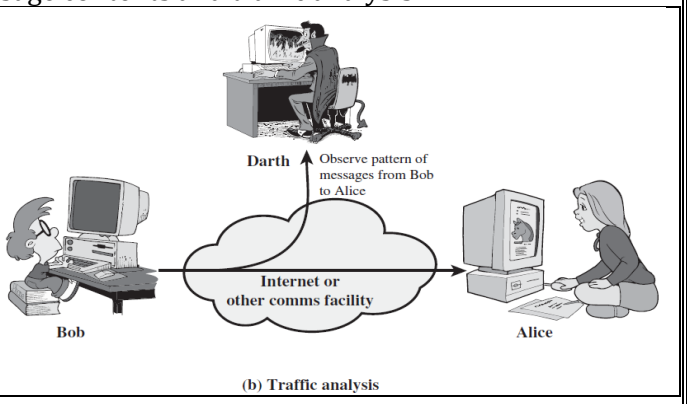
- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- An active attack attempts to alter system resources or affect their operation.

Passive Attacks

- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.
- Two types of passive attacks are the release of message contents and traffic analysis.



(a) Release of message contents

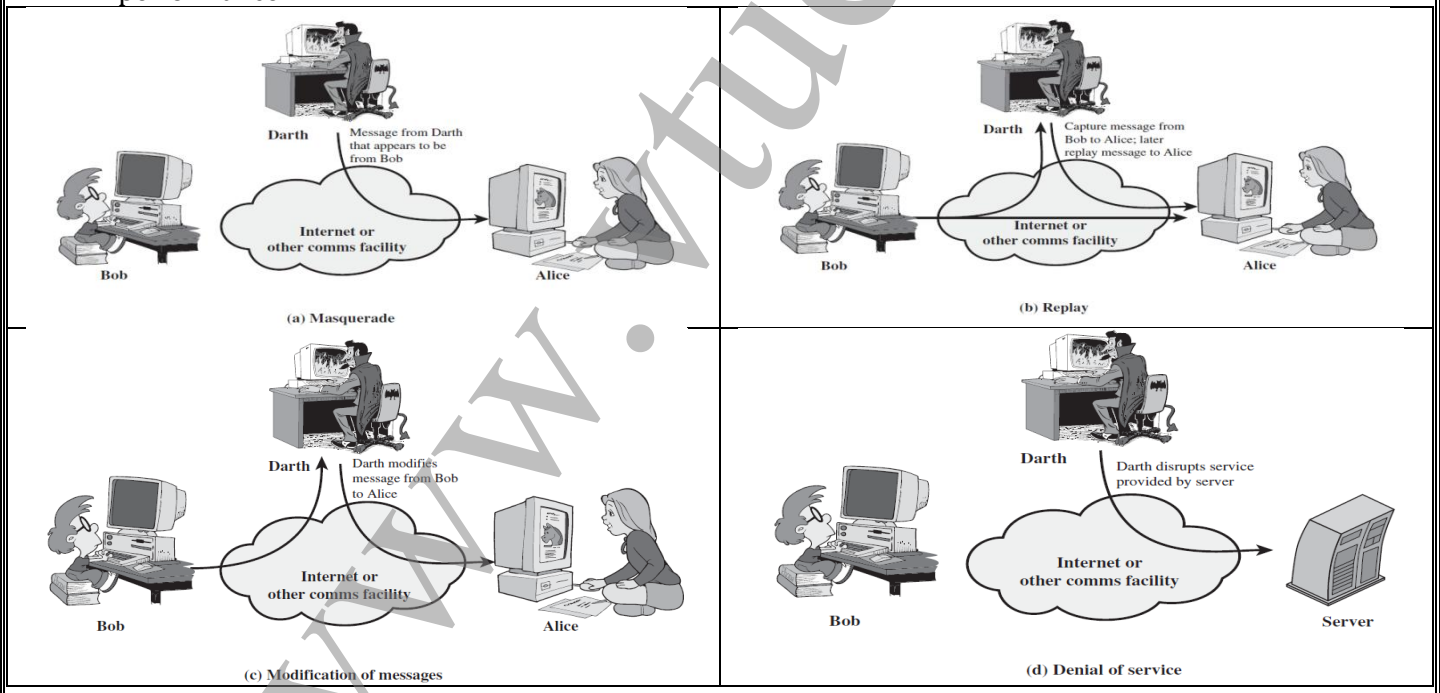


(b) Traffic analysis

- **Release of message contents** → A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- **Traffic analysis** → Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent still might be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Active Attacks

- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.
- A **masquerade** takes place when one entity pretends to be a different entity (Figure 1.3a). A masquerade attack usually includes one of the other forms of active attack.
- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 1.3b).
- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 1.3c).
- The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure 1.3d). This attack may have a specific target. Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.



Passive Attacks	Active attacks
It is indirect attack	It is direct attack
Very difficult to detect because they do not involve any alteration of data	Comparatively not very difficult to detect
Measures are available to prevent their success, usually by means of encryption	Quite difficult to prevent absolutely because it requires physical protection of all communication facilities and paths at all times
Involves eavesdropping on, or monitoring of,	Involve some modification of the data stream or the

transmissions	creation of a false stream
Two types → release of message contents and traffic analysis	Four categories → masquerade, replay, modification of messages and denial of service
Goal → prevention rather than detection	Goal → detect and recover from any disruption or delays caused by them

SECURITY SERVICES & SECURITY MECHANISMS

This topic does not require everything in detail (exam point of view). Hence, I have put only the tables which contains a short summary. Interested students can refer text book for more details.

Table 1.2 Security Services (X.800)

AUTHENTICATION The assurance that the communicating entity is the one that it claims to be. **Peer Entity Authentication** Used in association with a logical connection to provide confidence in the identity of the entities connected. **Data-Origin Authentication** In a connectionless transfer, provides assurance that the source of received data is as claimed. **ACCESS CONTROL** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do). **DATA CONFIDENTIALITY** The protection of data from unauthorized disclosure. **Connection Confidentiality** The protection of all user data on a connection. **Connectionless Confidentiality** The protection of all user data in a single data block. **Selective-Field Confidentiality** The confidentiality of selected fields within the user data on a connection or in a single data block. **Traffic-Flow Confidentiality** The protection of the information that might be derived from observation of traffic flows.	**DATA INTEGRITY** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). **Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. **Connection Integrity without Recovery** As above, but provides only detection without recovery. **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. **Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. **Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

A MODEL FOR NETWORK SECURITY

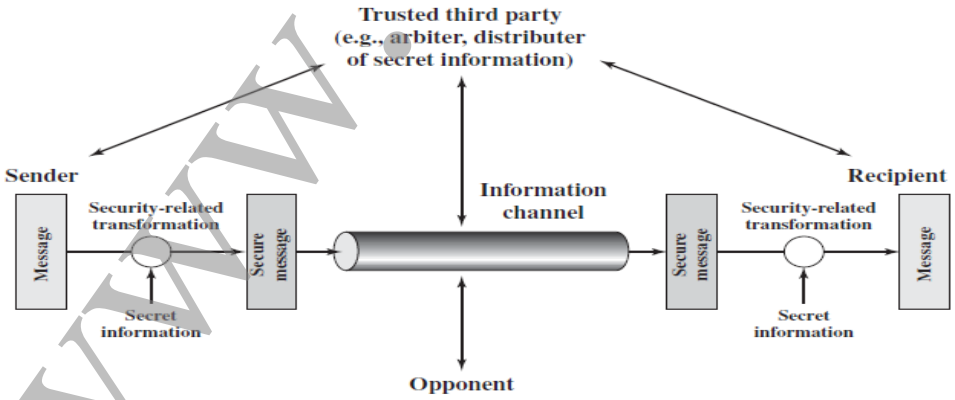


Figure 1.4 Model for Network Security

- A message is to be transferred from one party to another across some sort of Internet service.
- The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.
- All of the techniques for providing security have two components:
  - A security-related transformation on the information to be sent.
  - Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

- A trusted third party may be needed to achieve secure transmission.
- This general model shows that there are four basic tasks in designing a particular security service:
  - Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
  - Generate the secret information to be used with the algorithm.
  - Develop methods for the distribution and sharing of the secret information.
  - Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.
- A general model of these other situations is illustrated by Figure 1.5, which reflects a concern for protecting an information system from unwanted access.
- The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).
- Programs can present two kinds of threats:
  1. **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
  2. **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

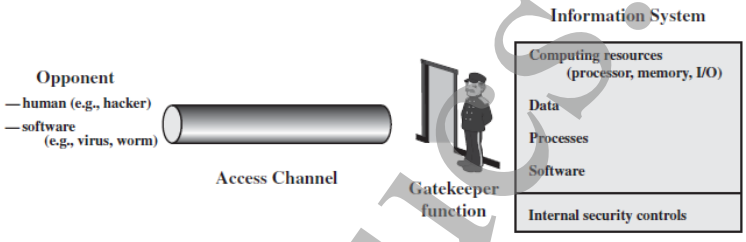


Figure 1.5 Network Access Security Model

- The **security mechanisms** needed to cope with unwanted access fall into two broad categories.
- The first category might be termed a gatekeeper function.
- It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks.
- Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

INTERNET STANDARDS AND THE INTERNET SOCIETY

This topic is not so important and has not been asked in the exam till date. Hence, interested students can refer text book.

KERBEROS

Kerberos is a key distribution and user authentication service developed at MIT.
In particular, the following three threats exist:

1. A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
2. A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.
3. A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on symmetric encryption, making no use of public-key encryption.

Kerberos Version 4

Version 4 of Kerberos makes use of DES, in a rather elaborate protocol, to provide the authentication service.

❖ A Simple Authentication Dialogue

- ✓ In an unprotected network environment, any client can apply to any server for service.
- ✓ The obvious security risk is that of impersonation.
- ✓ An opponent can pretend to be another client and obtain unauthorized privileges on server machines.
- ✓ To counter this threat, servers must be able to confirm the identities of clients who request service.
- ✓ An alternative is to use an **authentication server (AS)** that knows the passwords of all users and stores these in a centralized database.

(1) $C \rightarrow AS: \quad ID_C \| P_C \| ID_V$

(2) $AS \rightarrow C: \quad Ticket$

(3) $C \rightarrow V: \quad ID_C \| Ticket$

$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$

where

C	= client
AS	= authentication server
V	= server
ID_C	= identifier of user on C
ID_V	= identifier of V
P_C	= password of user on C
AD_C	= network address of C
K_v	= secret encryption key shared by AS and V

- In this scenario, the user logs on to a workstation and requests access to server V.
- The client module C in the user's workstation requests the user's password and then sends a message to the AS that includes the user's ID, the server's ID, and the user's password.
- The AS checks its database to see if the user has supplied the proper password for this user ID and whether this user is permitted access to server V.
- If both tests are passed, the AS accepts the user as authentic and must now convince the server that this user is authentic.
- To do so, the AS creates a **ticket** that contains the user's ID and network address and the server's ID.
- This ticket is encrypted using the secret key shared by the AS and this server.
- This ticket is then sent back to C.
- Because the ticket is encrypted, it cannot be altered by C or by an opponent.
- With this ticket, C can now apply to V for service.
- C sends a message to V containing C's ID and the ticket.
- V decrypts the ticket and verifies that the user ID in the ticket is the same as the unencrypted user ID in the message.
- If these two match, the server considers the user authenticated and grants the requested service.

❖ A More Secure Authentication Dialogue

Once per user logon session:

(1) $C \rightarrow AS: \quad ID_C \| ID_{tgs}$

(2) $AS \rightarrow C: \quad E(K_c, Ticket_{tgs})$

Once per type of service:

(3) $C \rightarrow TGS: \quad ID_C \| ID_V \| Ticket_{tgs}$

(4) $TGS \rightarrow C: \quad Ticket_v$

Once per service session:

(5) $C \rightarrow V: \quad ID_C \| Ticket_v$

$Ticket_{tgs} = E(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$

$Ticket_v = E(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$

1. The client requests a ticket-granting ticket on behalf of the user by sending its user's ID to the AS, together with the TGS ID, indicating a request to use the TGS service.
2. The AS responds with a ticket that is encrypted with a key that is derived from the user's password (Kc). If the correct password is supplied, the ticket is successfully recovered.
3. The client requests a service-granting ticket on behalf of the user.
4. The TGS decrypts the incoming ticket using a key shared only by the AS and the TGS (K_{tgs}) and verifies the success of the decryption by the presence of its ID.
5. The client requests access to a service on behalf of the user.

- ✓ First, we would like to minimize the number of times that a user has to enter a password.

- ✓ The second problem is that the earlier scenario involved a plaintext transmission of the password. An eavesdropper could capture the password and use any service accessible to the victim.
- ✓ To solve these additional problems, we introduce a scheme for avoiding plaintext passwords and a new server, known as the **ticket-granting server (TGS)**.
- ✓ The new (but still hypothetical) scenario is shown above table
- ✓ Figure 4.1 gives just an overview of kerberos

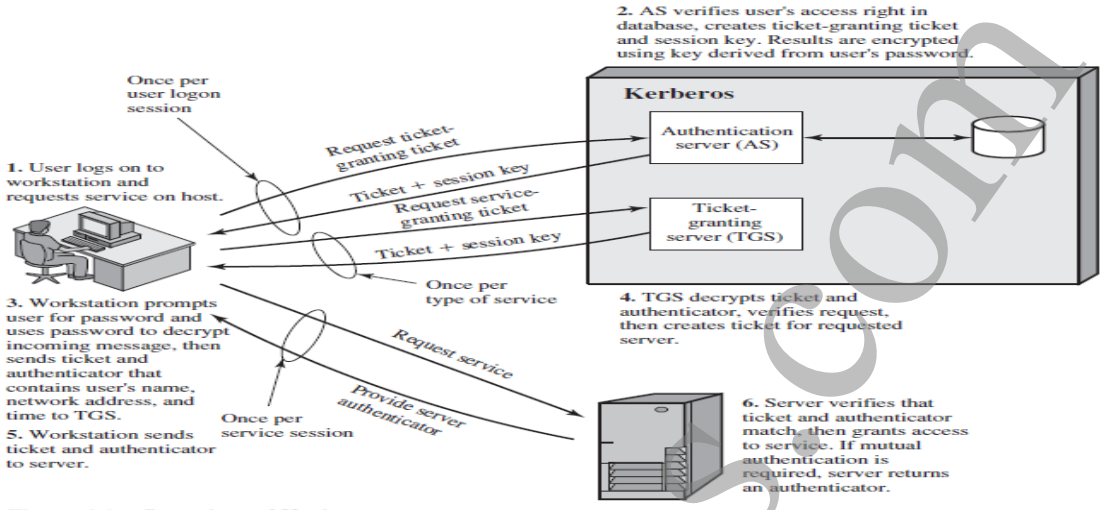


Figure 4.1 Overview of Kerberos

Kerberos Realms and Multiple Kerberi

[Not very important for exam – not been asked till date. Interested students can refer text book]

If this is asked, then draw the figure 4.2 and explain the answer in your own words

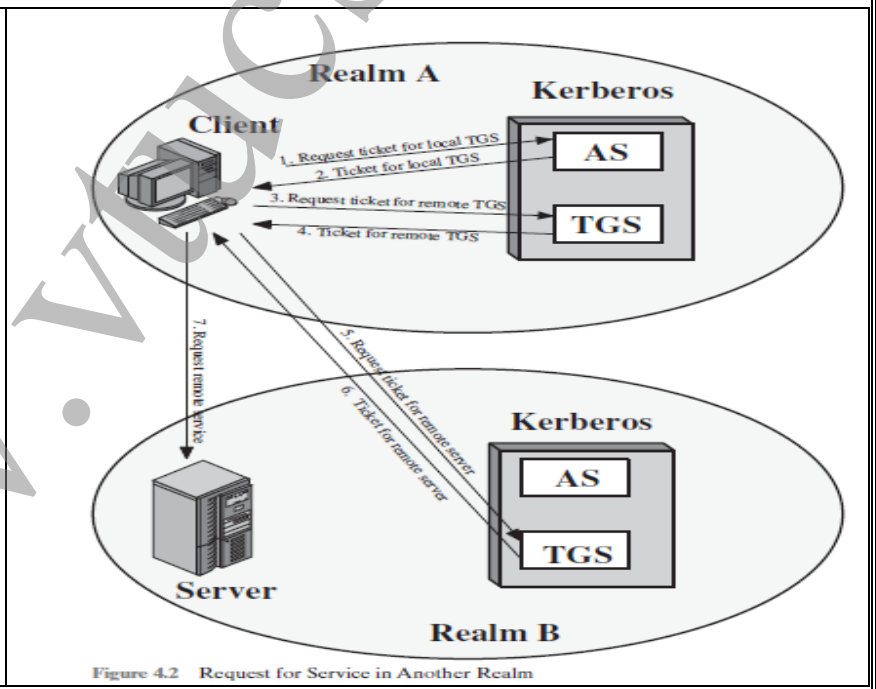


Figure 4.2 Request for Service in Another Realm

Differences between Kerberos version 4 and version 5.

1. **Encryption system dependence:** Version 4 requires the use of DES. In version 5, cipher text is tagged with an encryption-type identifier so that any encryption technique may be used.
2. **Internet protocol dependence:** Version 4 requires the use of Internet Protocol (IP) addresses. Other address types, such as the ISO network address, are not accommodated. Version 5 network addresses are tagged with type and length, allowing any network addresses type to be used.
3. **Message byte ordering:** In version 4, the sender of a message employs a byte ordering of its own choosing and tags the message to indicate least significant byte in lowest address or most significant

byte in lowest address. In version 5, all message structures are defined using Abstract Syntax Notation One (ASN.1) and Basic Encoding Rules (BER), which provide an unambiguous byte ordering.

4. **Ticket lifetime:** Lifetime values in version 4 are encoded in an 8-bit quantity in units of five minutes. In version 5, tickets include an explicit start time and end time, allowing tickets with arbitrary lifetimes.
5. **Authentication forwarding:** Version 4 does not allow credentials issued to one client to be forwarded to some other host and used by some other client. Version 5 provides this capability.
6. **Inter-realm authentication**: In version 4, interoperability among *N* realms requires on the order of *N*2 Kerberos-to-Kerberos relationships. Version 5 supports a method that requires fewer relationships.

Deficiencies of version 4

1. ***Double encryption*** → that tickets provided to clients are encrypted twice—once with the secret key of the target server and then again with a secret key known to the client. The second encryption is not necessary and is computationally wasteful.
2. ***PCBC encryption*** → Encryption in version 4 makes use of a nonstandard mode of DES known as propagating cipher block chaining (PCBC). It has been demonstrated that this mode is vulnerable to an attack involving the interchange of ciphertext blocks.
3. ***Session keys*** → Each ticket includes a session key that is used by the client to encrypt the authenticator sent to the service associated with that ticket. However, because the same ticket may be used repeatedly to gain service from a particular server, there is the risk that an opponent will replay messages from an old session to the client or the server.
4. ***Password attacks*** → Both versions are vulnerable to a password attack. The message from the AS to the client includes material encrypted with a key based on the client's password. An opponent can capture this message and attempt to decrypt it by trying various passwords.

The Version 5 Authentication Dialogue

Table 4.3 Summary of Kerberos Version 5 Message Exchanges

(1) C → AS $Options \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $Realm_c \| ID_C \| Ticket_{tgs} \| E(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $Realm_c \| ID_C \| Ticket_v \| E(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Options \| Ticket_v \| Authenticator_c$

(6) V → C $E_{Kc,v} [TS_2 \| Subkey \| Seq\#]$

$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,v}, [ID_C \| Realm_c \| TS_2 \| Subkey \| Seq\#])$

(c) Client/Server Authentication Exchange to obtain service

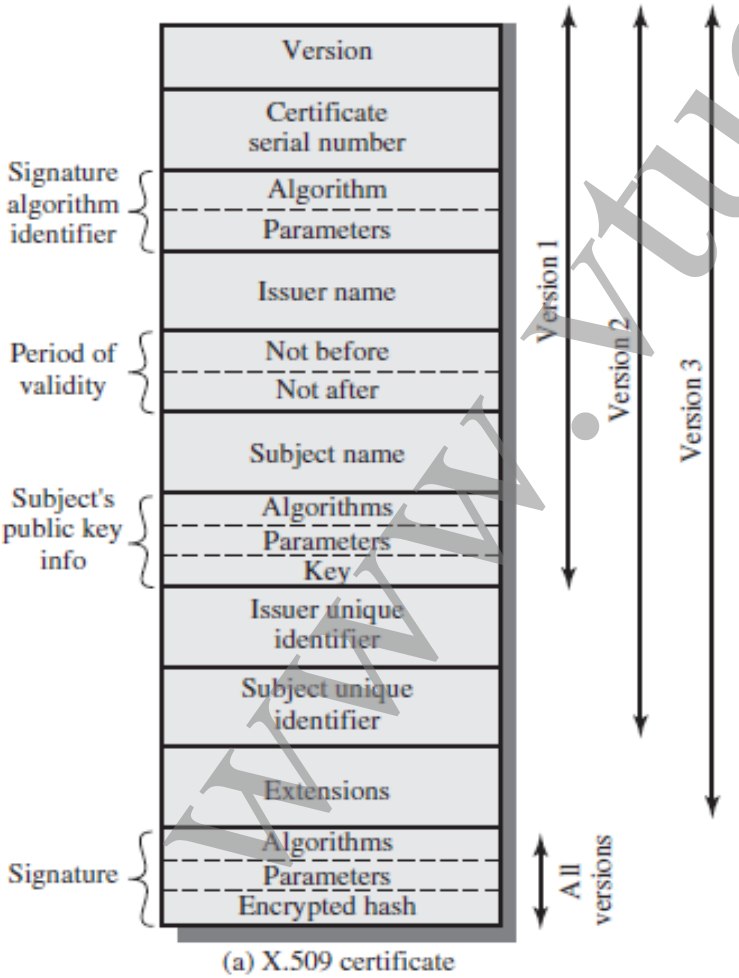
- First, consider the **authentication service exchange**. Message (1) is a client request for a ticket-granting ticket. As before, it includes the ID of the user and the TGS. The following new elements are added:
  - **Realm:** Indicates realm of user.
  - **Options:** Used to request that certain flags be set in the returned ticket.
  - **Times:** Used by the client to request the following time settings in the ticket:
    from: the desired start time for the requested ticket
    till: the requested expiration time for the requested ticket
    rtime: requested renew-till time

• **Nonce:** A random value to be repeated in message (2) to assure that the response is fresh and has not been replayed by an opponent.

- Message (2) returns a ticket-granting ticket, identifying information for the client, and a block encrypted using the encryption key based on the user's password.
- Let us now compare the **ticket-granting service exchange** for versions 4 and 5. We see that message (3) for both versions includes an authenticator, a ticket, and the name of the requested service.
- Message (4) has the same structure as message (2). It returns a ticket plus information needed by the client, with the information encrypted using the session key now shared by the client and the TGS.
- Finally, for the **client/server authentication exchange**, several new features appear in version 5. In message (5), the client may request as an option that mutual authentication is required. The authenticator includes several new fields:
  • **Subkey:** The client's choice for an encryption key to be used to protect this specific application session. If this field is omitted, the session key from the ticket ($K_{c,v}$) is used.
  • **Sequence number:** An optional field that specifies the starting sequence number to be used by the server for messages sent to the client during this session. Messages may be sequence numbered to detect replays.

X.509 AUTHENTICATION SERVICE

General format of a X.509 public key certificate

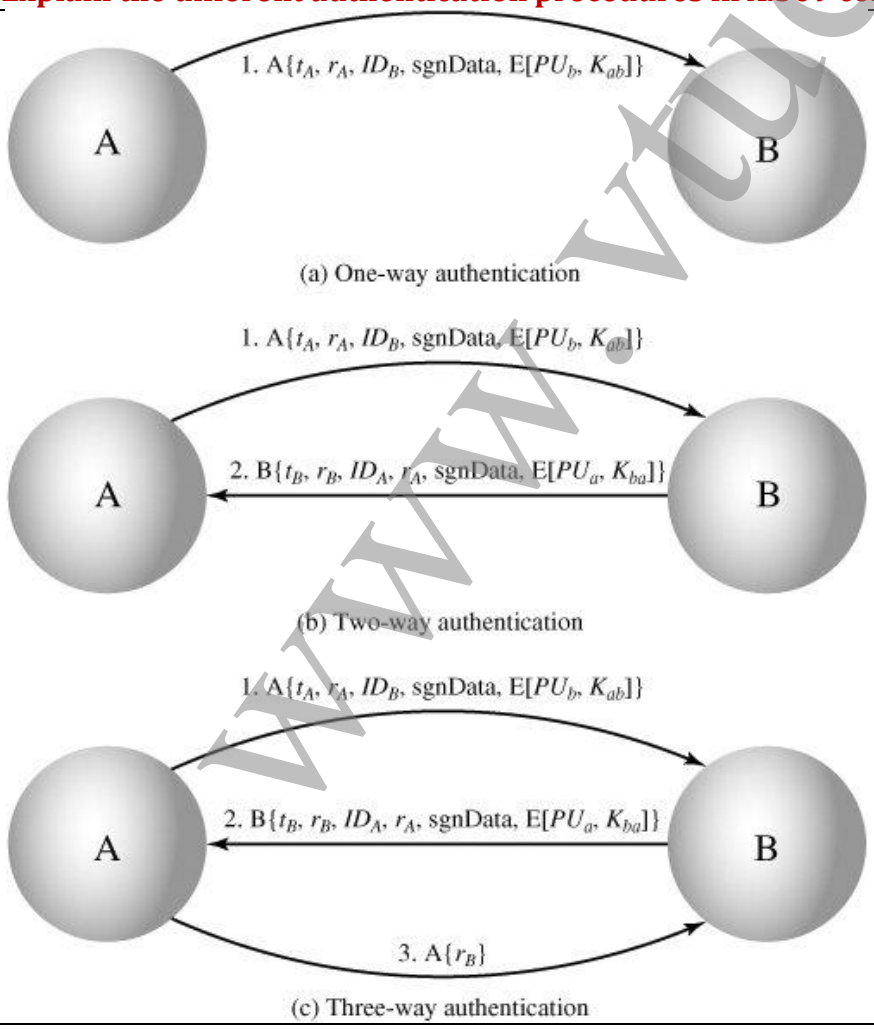


(a) X.509 certificate

Figure 4.4 X.509 Formats

• **Version:** Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3.
• **Serial number:** An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.
• **Signature algorithm identifier:** The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility.
• **Issuer name:** X.500 name of the CA that created and signed this certificate.
• **Period of validity:** Consists of two dates: the first and last on which the certificate is valid.
• **Subject name:** The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.
Subject's public-key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.
• **Issuer unique identifier:** An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.
• **Subject unique identifier:** An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.
• **Extensions:** A set of one or more extension fields. Extensions were added in version 3 and are discussed later in this section.
• **Signature:** Covers all of the other fields of the certificate; it contains the hash code of the other fields encrypted with the CA's private key. This field includes the signature algorithm identifier.

Explain the different authentication procedures in X.509 certificate.



Three alternative authentication procedures:
- One-Way Authentication
- Two-Way Authentication
- Three-Way Authentication

All use public-key signatures.

❖ **<u>One-way Authentication</u>**
1 message (A->B) used to establish
- the identity of A and that message is from A
- message was intended for B
- integrity & originality of message

❖ **<u>Two-way Authentication</u>**
2 messages (A->B, B->A) which also establishes in addition:
- the identity of B and that reply is from B
- that reply is intended for A
- integrity & originality of reply

❖ **<u>Three-way Authentication</u>**
3 messages (A->B, B->A, A->B) which enables above authentication without synchronized clocks

X.509 Version 3

The X.509 version 2 format does not convey all of the information that recent design and implementation experience has shown to be needed. [FORD95] lists the following requirements not satisfied by version 2:

1. The Subject field is inadequate to convey the identity of a key owner to a public key user. X.509 names may be relatively short and lacking in obvious identification details that may be needed by the user.
2. The Subject field is also inadequate for many applications, which typically recognize entities by an Internet e-mail address, a URL, or some other Internet-related identification.
3. There is a need to indicate security policy information. This enables a security application or function, such as IPSec, to relate an X.509 certificate to a given policy.
4. There is a need to limit the damage that can result from a faulty or malicious CA by setting constraints on the applicability of a particular certificate.
5. It is important to be able to identify different keys used by the same owner at different times.

Key and Policy Information

This area includes:

- **Authority key identifier:** Identifies the public key to be used to verify the signature on this certificate or CRL.
- **Subject key identifier:** Identifies the public key being certified. It is useful for subject key pair updating.
- **Key usage:** May indicate one or more of the following: digital signature, non-repudiation, key encryption, data encryption, key agreement, CA signature verification on certificates, and CA signature verification on CRLs.
- **Private-key usage period:** Indicates the period of use of the private key corresponding to the public key.
- **Certificate policies:** Certificates may be used in environments where multiple policies apply.
- **Policy mappings:** Used only in certificates for CAs issued by other CAs.

Certificate Subject and Issuer Attributes

The extension fields in this area include:

- **Subject alternative name:** Contains one or more alternative names, using any of a variety of forms. This field is important for supporting certain applications, such as electronic mail, EDI, and IPSec, which may employ their own name forms.
- **Issuer alternative name:** Contains one or more alternative names, using any of a variety of forms.
- **Subject directory attributes:** Conveys any desired X.500 directory attribute values for the subject of this certificate.

Certification Path Constraints

The extension fields in this area include:

- **Basic constraints:** Indicates if the subject may act as a CA. If so, a certification path length constraint may be specified.
- **Name constraints:** Indicates a name space within which all subject names in subsequent certificates in a certification path must be located.
- **Policy constraints:** Specifies constraints that may require explicit certificate policy identification or inhibit policy mapping for the remainder of the certification path.

UNIT 7
IP SECURITY

IP-level security encompasses three functional areas: authentication, confidentiality, and key management.

IP SECURITY OVERVIEW

Applications of IPsec

IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

- *Secure branch office connectivity over the Internet:* A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
- *Secure remote access over the Internet*: An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.
- *Establishing extranet and intranet connectivity with partners:* IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- *Enhancing electronic commerce security:* Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

Figure 8.1 is a typical scenario of IPsec usage.

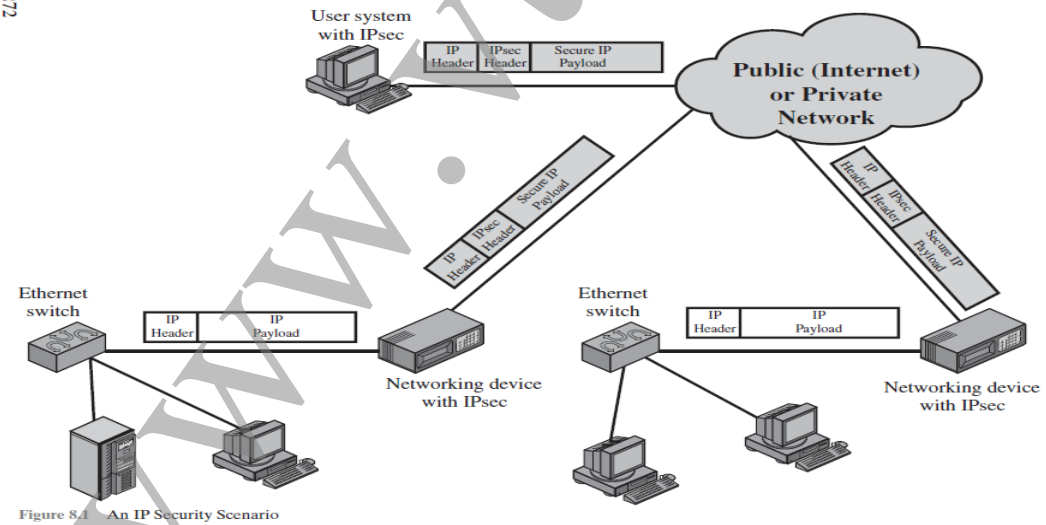


Figure 8.1 An IP Security Scenario

Benefits of IPsec

Some of the benefits of IPsec:

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.

- IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPsec can provide security for individual users if needed.

Routing Applications

IPsec can assure that

- A router advertisement comes from an authorized router.
- A neighbor advertisement comes from an authorized router.
- A redirect message comes from the router to which the initial IP packet was sent.
- A routing update is not forged.

IP SECURITY ARCHITECTURE

IPsec Documents

IPsec encompasses three functional areas: authentication, confidentiality, and key management.

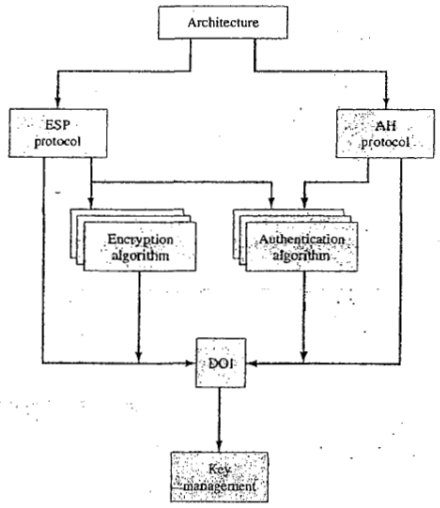


Figure 6.2 IPSec Document Overview

Architecture: Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.
Encapsulating Security Payload (ESP): ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication.
Authentication Header (AH): AH is an extension header to provide message authentication.
Encryption Algorithm: A set of documents that describe how various encryption algorithms are used for ESP
Authentication Algorithm: A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP
Key Management: document that describes key management schemes.
Domain of Interpretation(DOI): contains values needed for the other documents to relate to each other.

IPsec Services

IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, Authentication Header (AH); and a combined encryption/ authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP). RFC 4301 lists the following services:

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Security Associations

An association is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.
A security association is uniquely identified by three parameters.

- **Security Parameters Index (SPI):** A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- **IP Destination Address:** This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.
- **Security Protocol Identifier:** This field from the outer IP header indicates whether the association is an AH or ESP security association.

Security Association Database (SA Parameter)

A security association is normally defined by the following parameters in an SAD entry.

- **Security Parameter Index:** A 32-bit value selected by the receiving end of an SA to uniquely identify the SA.
- **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers.
- **Sequence Counter Overflow:** A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA
- **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay.
- **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH
- **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP
- **Lifetime of this Security Association:** A time interval or byte count after which an SA must be replaced with a new SA or terminated, plus an indication of which of these actions should occur.
- **IPsec Protocol Mode:** Tunnel, transport, or wildcard.
- **Path MTU:** Any observed path maximum transmission unit and aging variables

Security Policy Database (SA Selectors)

Each SPD entry is defined by a set of IP and upper-layer protocol field values, called *selectors*.
The following selectors determine an SPD entry:

- **Remote IP Address:** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
- **Source IP Address:** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
- **userID:** a user identifier from the operating system
- **data sensitivity level:** used for systems providing information flow security
- **transport layer protocol:** this may be an individual protocol number, a list of protocol numbers, or a range of protocol numbers
- **source and destination ports:** these may be individual TCP or UDP port values, an enumerated list of ports or a wildcard port

Transport and Tunnel Modes

Table 8.1 Tunnel Mode and Transport Mode Functionality

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

- Transport mode provides protection primarily for upper-layer protocols.
- Tunnel mode provides protection to the entire IP packet.

AUTHENTICATION HEADER

- The Authentication Header provides support for data integrity and authentication of IP packets
- The data integrity feature ensures that undetected modification to a packet's content in transit is not possible
- The authentication feature enables an end system or network device to authenticate the user or application and filter traffic accordingly
- It also prevents the address spoofing attacks
- It also guards against the replay attack

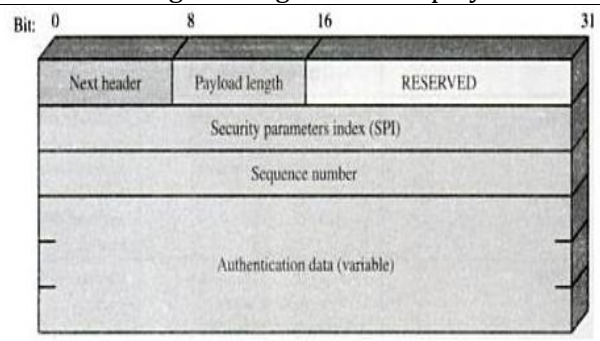


Figure 6.3 IPSec Authentication Header

The Authentication Header consists of the following fields (Figure 6.3):

- **Next Header (8 bits):** Identifies the type of header immediately following this header.
- **Payload Length (8 bits):** Length of Authentication Header in 32-bit words, minus 2. For example, the default length of the authentication data field is 96 bits, or three 32-bit words. With a three-word fixed header, there are a total of six words in the header, and the Payload Length field has a value of 4.
- **Reserved (16 bits):** For future use.
- **Security Parameters Index (32 bits):** Identifies a security association.
- **Sequence Number (32 bits):** A monotonically increasing counter value, discussed later.
- **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value (ICV), or MAC, for this packet, discussed later.

Anti-Replay service

- A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination
- The sequence number field is designed to thwart such attacks
- When a new SA is established, the sender initializes a sequence number counter to 0
- Each time a packet is sent on this SA, the sender increments the counter and places the value in sequence number field
- Thus, the first value to be used is 1
- If anti-replay is enabled, the sender must not allow the sequence number to cycle past $2^{32} - 1$ back to 0
- The IPSec authentication document dictates that the receiver should implement a window of size W

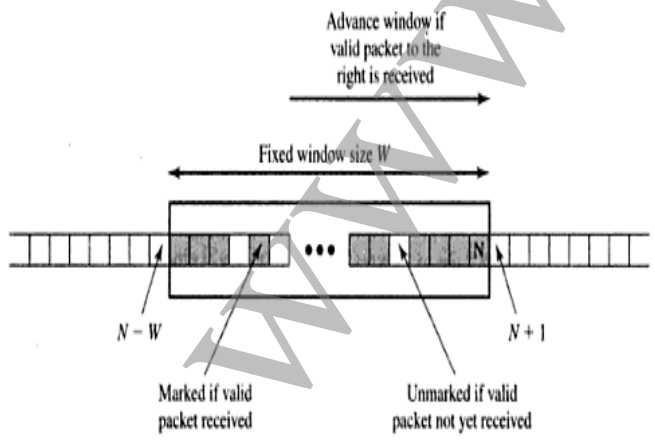


Figure 6.4 Antireplay Mechanism

1. If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.
2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
3. If the received packet is to the left of the window, or if authentication fails, the packet is discarded; this is an auditable event.

Transport and Tunnel Modes

Figure 6.5 shows two ways in which the IPSec authentication service can be used. In one case, authentication is provided directly between a server and client workstations; the workstation can be either on the same network as the server or on an external network. As long as the workstation and the server share a protected secret key, the authentication process is secure. This case uses a transport mode SA. In the other case, a remote workstation authenticates itself to the corporate firewall, either for access to the entire internal network or because the requested server does not support the authentication feature. This case uses a tunnel mode SA.

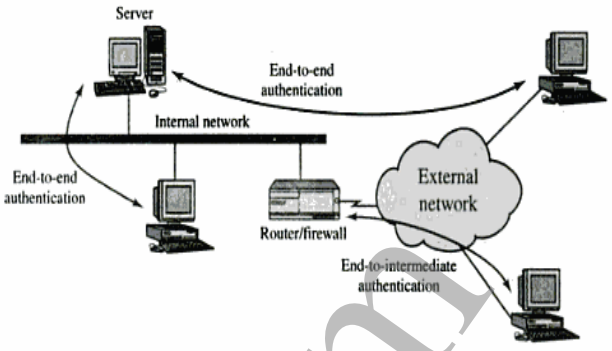


Figure 6.5 End-to-End versus End-to-Intermediate Authentication

- For transport mode AH using IPv4, the AH is inserted after the original IP header and before the IP payload
- Authentication covers the entire packet, excluding mutable fields in the IPv4 header that are set to zero for MAC calculation
- For tunnel mode AH, the entire original IP packet is authenticated and the AH is inserted between the original IP header and a new outer IP header
- The inner IP header carries the ultimate source and destination address
- The outer IP header may contain different IP addresses

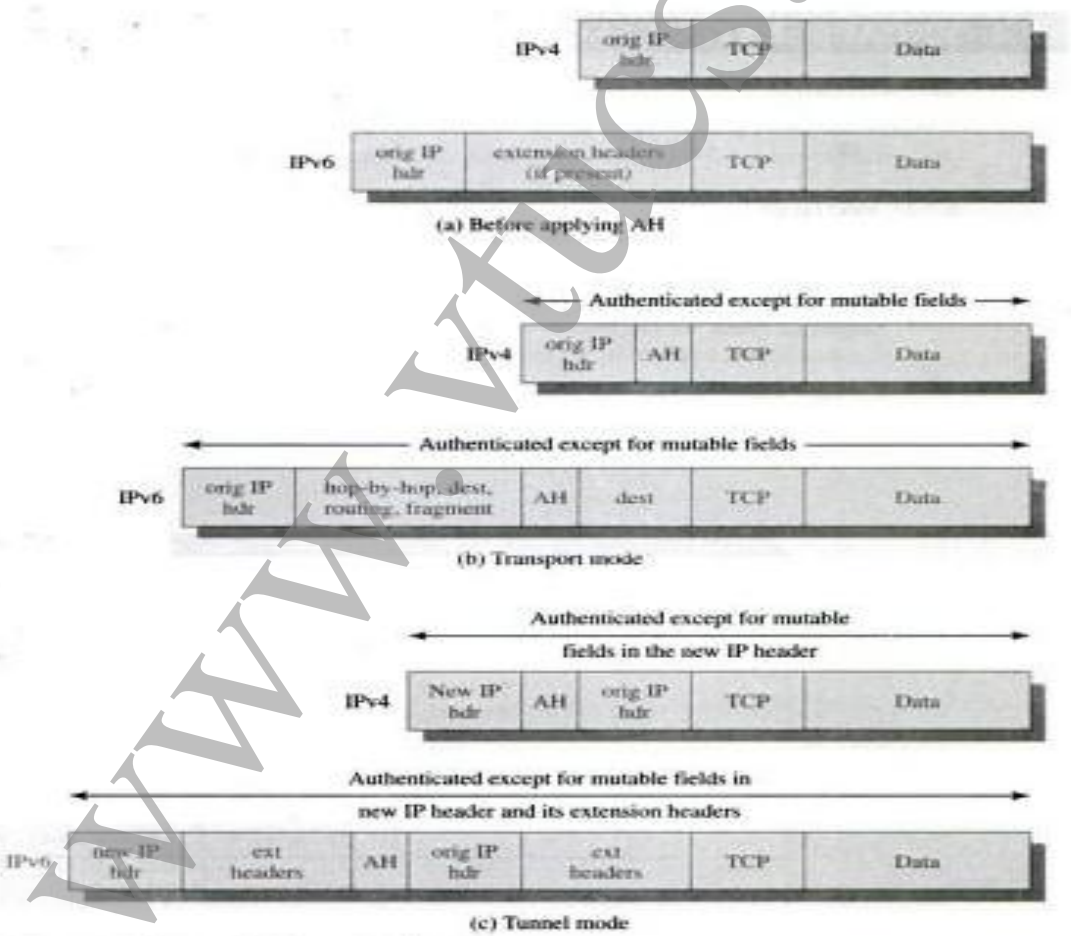


Figure 6.6 Scope of AH Authentication

ENCAPSULATING SECURITY PAYLOAD

ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality.

ESP Format

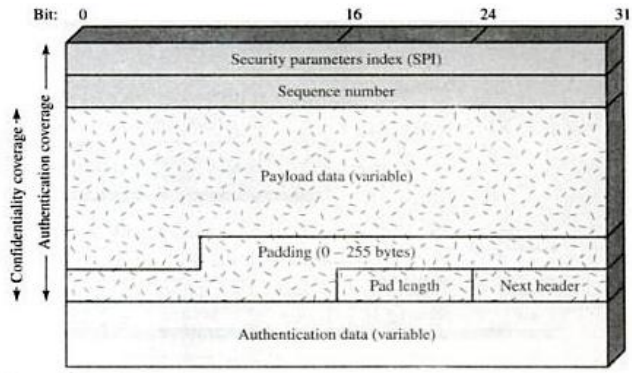


Figure 6.7 IPSec ESP format

- **Security Parameters Index (32 bits):** Identifies a security association.
- **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
- **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- **Padding (0–255 bytes):** The purpose of this field is discussed later.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
- **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
- **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.

Encryption and Authentication Algorithms

The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service.
These include:

- Three-key triple DES
- RC5
- IDEA
- Three-key triple IDEA
- CAST
- Blowfish

Padding

The Padding field serves several purposes:
• If an encryption algorithm requires the plaintext to be a multiple of some number of bytes, the Padding field is used to expand the plaintext to the required length.
• The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word.
• Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.

Transport and Tunnel Modes

Figure 8.7 shows two ways in which the IPsec ESP service can be used. In the upper part of the figure, encryption (and optionally authentication) is provided directly between two hosts. Figure 8.7b shows how tunnel mode operation can be used to set up a ***virtual private network***.

Transport mode operation may be summarized as follows.

1. At the source, the block of data consisting of the ESP trailer plus the entire transport-layer segment is encrypted and the plaintext of this block is replaced with its ciphertext to form the IP packet for transmission. Authentication is added if this option is selected.
2. The packet is then routed to the destination. Each intermediate router needs to examine and process the IP header plus any plaintext IP extension headers but does not need to examine the ciphertext.
3. The destination node examines and processes the IP header plus any plaintext IP extension headers.

Tunnel mode ESP is used to encrypt an entire IP packet. The following steps occur for transfer of a transport layer segment from the external host to the internal host.

1. The source prepares an inner IP packet with a destination address of the target internal host.
2. The outer packet is routed to the destination firewall.
3. The destination firewall examines and processes the outer IP header plus any outer IP extension headers. This packet is then transmitted in the internal network.
4. The inner packet is routed through zero or more routers in the internal network to the destination host.

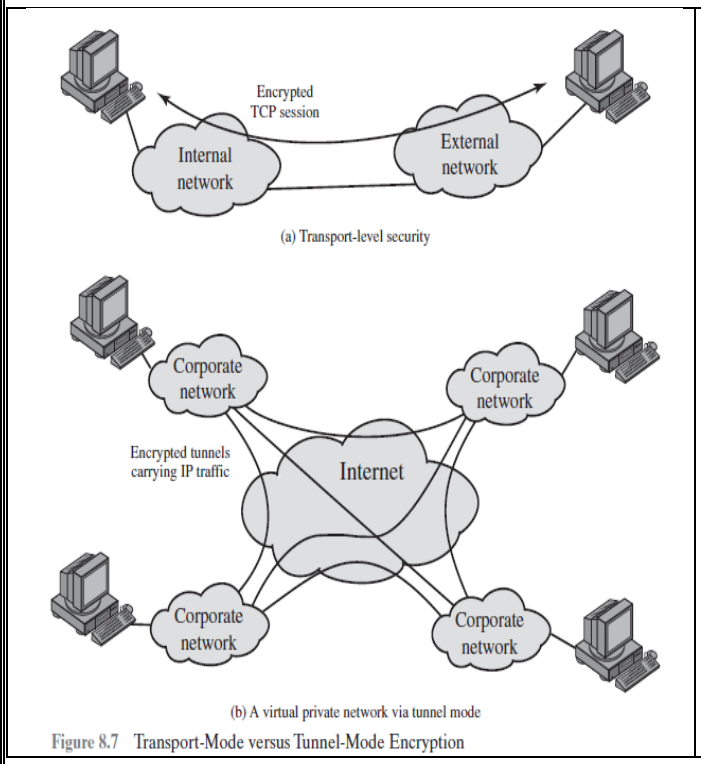


Figure 8.7 Transport-Mode versus Tunnel-Mode Encryption

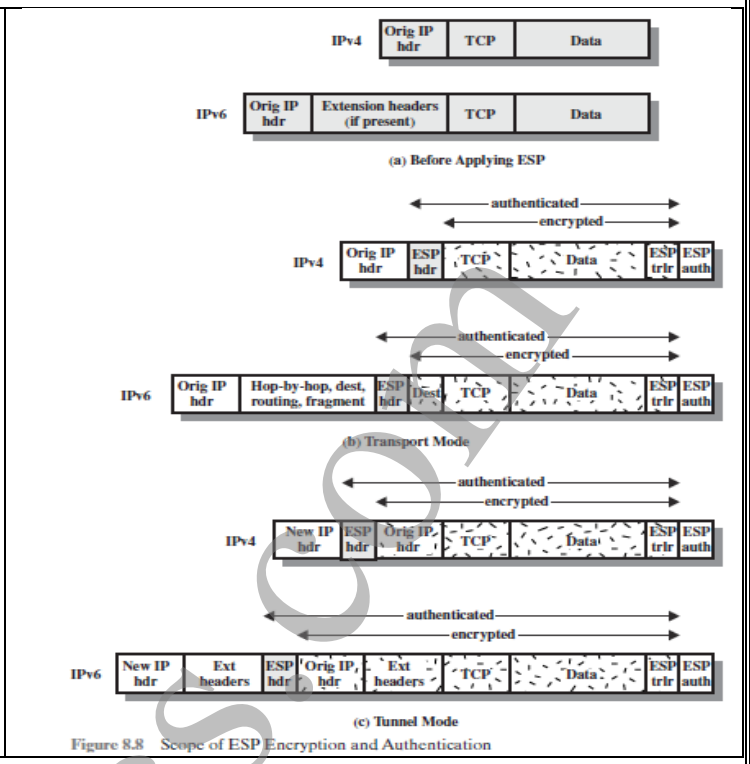


Figure 8.8 Scope of ESP Encryption and Authentication

COMBINING SECURITY ASSOCIATIONS

The term security association bundle refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPsec services. The SAs in a bundle may terminate at different endpoints or at the same endpoints. Security associations may be combined into bundles in two ways:

- **Transport adjacency:** Refers to applying more than one security protocol to the same IP packet without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPsec instance: the (ultimate) destination.
- **Iterated tunneling:** Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPsec site along the path.

Authentication Plus Confidentiality

ESP with Authentication Option

There are actually two subcases:

- **Transport mode ESP:** Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected.
- **Tunnel mode ESP:** The entire inner IP packet is protected by the privacy mechanism for delivery to the inner IP destination.

Transport Adjacency

Another way to apply authentication after encryption is to use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA.

Transport-Tunnel Bundle

The use of authentication prior to encryption might be preferable for several reasons. First, because the authentication data are protected by encryption, it is impossible for anyone to intercept the message and alter the authentication data without detection. Second, it may be desirable to store the authentication information with the message at the destination for later reference.

Basic Combinations of Security Associations

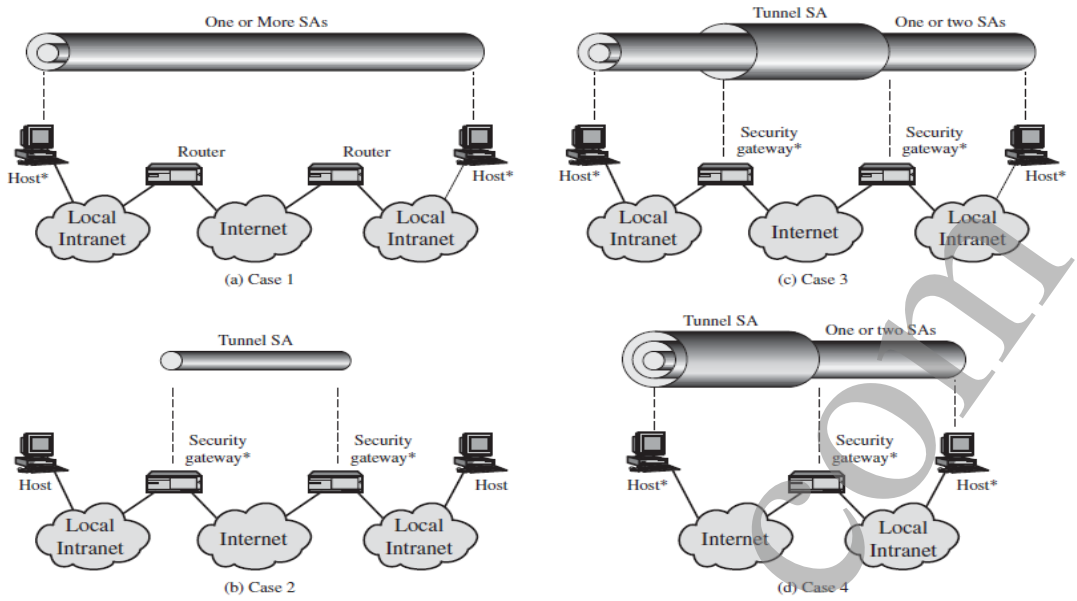


Figure 8.10 Basic Combinations of Security Associations

Case 1.

All security is provided between end systems that implement IPsec. For any two end systems to communicate via an SA, they must share the appropriate secret keys. Among the possible combinations are

a. AH in transport mode
b. ESP in transport mode
c. ESP followed by AH in transport mode (an ESP SA inside an AH SA)
d. Any one of a, b, or c inside an AH or ESP in tunnel mode

Case 2.

Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec. This case illustrates simple virtual private network support. The security architecture document specifies that only a single tunnel SA is needed for this case. The tunnel could support AH, ESP, or ESP with the authentication option. Nested tunnels are not required, because the IPsec services apply to the entire inner packet.

Case 3.

This builds on case 2 by adding end-to-end security. The same combinations discussed for cases 1 and 2 are allowed here. The gateway-to-gateway tunnel provides either authentication, confidentiality, or both for all traffic between end systems. When the gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality. Individual hosts can implement any additional IPsec services required for given applications or given users by means of end-to-end SAs.

Case 4.

This provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall. Only tunnel mode is required between the remote host and the firewall. As in case 1, one or two SAs may be used between the remote host and the local host.

KEY MANAGEMENT

The key management portion of IPsec involves the determination and distribution of secret keys. A typical requirement is four keys for communication between two applications: transmit and receive pairs for both integrity and confidentiality. The IPsec Architecture document mandates support for two types of key management:

- **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems.
- **Automated:** An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.

The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley and consists of the following elements:

- **Oakley Key Determination Protocol:** Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.
- **Internet Security Association and Key Management Protocol (ISAKMP):** ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

Oakley Key Determination Protocol

It is a refinement of the Diffie-Hellman key exchange algorithm. The Diffie-Hellman algorithm has two attractive features:

- Secret keys are created only when needed. There is no need to store secret keys for a long period of time, exposing them to increased vulnerability.
- The exchange requires no pre-existing infrastructure other than an agreement on the global parameters.

The oakley key determination algorithm is characterized by five important features:

- It employs a mechanism known as cookies to thwart clogging attacks.
- It enables the two parties to negotiate a *group*; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange.
- It uses nonces to ensure against replay attacks.
- It enables the exchange of Diffie-Hellman public key values.
- It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

ISAKMP mandates that cookie generation satisfy three basic requirements:

- The cookie must depend on the specific parties.
- It must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity
- The cookie generation and verification methods must be fast to thwart attacks intended to sabotage processor resources

Three different **authentication** methods can be used with Oakley:

- **Digital signatures:** The exchange is authenticated by signing a mutually obtainable hash; each party encrypts the hash with its private key. The hash is generated over important parameters, such as user IDs and nonces.
- **Public-key encryption:** The exchange is authenticated by encrypting parameters such as IDs and nonces with the sender's private key.
- **Symmetric-key encryption:** A key derived by some out-of-band mechanism can be used to authenticate the exchange by symmetric encryption of exchange parameters.

ISAKMP

- It defines procedures and packet formats to establish, negotiate, modify, and delete security associations.
- As part of SA establishment, IKE defines payloads for exchanging key generation and authentication data.
- These payload formats provide a consistent framework independent of the specific key exchange protocol, encryption algorithm, and authentication mechanism.

ISAKMP Header Format

An ISAKMP message consists of an ISAKMP header followed by one or more payloads. All of this is carried in a transport protocol. The specification dictates that implementations must support the use of UDP for the transport protocol. Figure 8.12a shows the header format for an ISAKMP message.

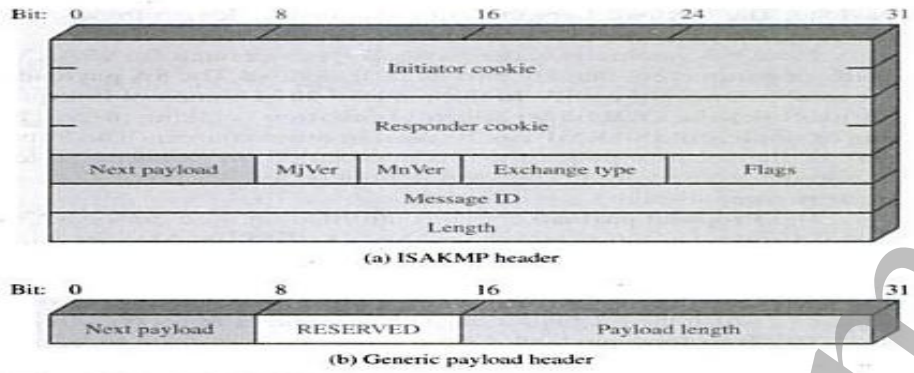


Figure 6.12 ISAKMP Formats

It consists of the following fields.

- *Initiator SPI (64 bits):* A value chosen by the initiator to identify a unique ISAKMP security association (SA).
- *Responder SPI (64 bits):* A value chosen by the responder to identify a unique ISAKMP SA.
- *Next Payload (8 bits):* Indicates the type of the first payload in the message
- *Major Version (4 bits):* Indicates major version of ISAKMP in use.
- *Minor Version (4 bits):* Indicates minor version in use.
- *Exchange Type (8 bits):* Indicates the type of exchange
- *Flags (8 bits):* Indicates specific options set for this ISAKMP exchange.
- *Message ID (32 bits):* Used to control retransmission of lost packets and matching of requests and responses.
- *Length (32 bits):* Length of total message (header plus all payloads) in octets.

ISAKMP Payload Types

- Proposal payload → contains information used during SA negotiation
- Transform payload → defines a security transform to be used to secure the communication channel for the designated protocol
- Key exchange payload → can be used for a variety of key exchange techniques
- Identification payload → used to determine the identity of communicating peers and may be used for determining authenticity of information
- Certificate payload → transfers a public-key certificate
- Hash payload → contains data generated by a hash function over some part of the message and ISAKMP state
- Signature payload → contains data generated by a digital signature function over some part of the message and ISAKMP state
- Nounce payload → contains random data used to guarantee liveness during an exchange and protect against replay attacks
- Notification payload → contains either error or status information associated with this SA
- Delete payload → indicates one or more SAs that the sender has deleted from its database

ISAKMP Exchanges

- Base exchange → allows key exchange and authentication material to be transmitted together
- Identity protection exchange → expands the base exchange to protect the users' identities
- Authentication only exchange → used to perform mutual authentication, without a key exchange
- Aggressive exchange → minimizes the number of exchanges at the expense of not providing identity protection
- Information exchange → used for one-way transmittal of information for SA management.

INFORMATION AND NETWORK SECURITY

Previous VTU Question Bank

Special thanks to: SHARVANI
for compiling these questions

UNIT 2

1. Explain the firewall rules.
2. Explain the screened subnet firewall.
3. Explain the major steps specified in BS7799:2 documents. How these steps help in security planning.
4. What is a firewall? Show the working of a screened host and dual homed firewall.
5. Explain the categories of firewall based on the processing mode.
6. What are virtual private networks? Explain the different techniques to implement a VPN.
7. Draw a schematic diagram of a packet filtering router used a s a firewall and explain its function using a sample firewall rule.
8. Describe the steps involved in Kerberos login and Kerberos request for services with illustrations.
9. Explain the firewall rules.

UNIT 3

1. How do signature based IDPs differ from behaviour based IDPs?
2. Explain venerability scanners.
3. How can a firewall be configured and managed? Give examples.
4. Explain the 2 modes of VPN.
5. Explain network based intrusion detection and prevention systems.
6. Describe the need of operating system detecting tools.
7. Describe the following terms wrt IDS: (i) alerts (ii) false attack stimulus (iii)false negative (iv) false positive (v) true attack stimulus
8. Discuss the reasons for acquisition of IDS by organizations.
9. Explain the difference btw host IDS and network IDS with diagrams.
10. Define the terms: honey pots, honey net and padded cells.
11. With a schematic diagram, explain the centralized control strategy implementation of IDS.
12. Give the advantages and disadvantages of using honey pots.

UNIT 4

1. What are the differences between digital signature and digital certificate?
2. Explain 2 methods of encrypting plain text.
3. What is an intrusion? Briefly explain any 8 IDPS terminologies.
4. What is an encryption? Discuss the symmetric and asymmetric encryption methods.
5. List out the elements of cryptosystems and explain transposition cipher technique.
6. Who can attack cryptosystems? Discuss the diff categories of attacks on cryptosystems.
7. Define the following terms: algorithm, cipher, key, link encryption, work factor
8. Distinguish btw symmetric and asymmetric encryption with examples.
9. Describe the terms: authentication, integrity, privacy, authorization, plaintext, steganography and non repudiation.
10. Discuss the “man in the middle” attack.
11. Explain different categories of attacks on cryptosystems.

UNIT 5

1. What are the diff btw active and passive security attacks?
2. Explain the different authentication procedures in X.509 certificate.
3. Write the summary of Kerberos version 5 message exchanges.
4. What is meant by info security? Discuss the 3 aspects of info security.
5. Briefly explain the 4 types of attacks that are normally encountered.
6. Explain the network security model.
7. List diff btw Kerberos version 4 and version 5.
8. Describe briefly the various security attacks and specific security mechanisms covered by X.800.
9. Describe the authentication procedure covered by X.809.
10. Discuss active security attacks.
11. Explain the general format of a X.509 public key certificate.
12. Explain Kerberos 4 message exchanges.

UNIT 7

1. Explain the format of an ESP packet in IP security.
2. Why does ESP include a padding field?
3. Give an example of an aggressive Oakley key.
4. Give the general structure of IPSEC authentication header. Describe how anti reply service is supported.
5. With a neat diagram, discuss the basic combinations of security associations.
6. Describe the SA parameters and SA selectors in detail.
7. Describe the Oakley key determination protocol.
8. Describe the benefits of IPSEC.
9. What is security association? Discuss the parameters used to describe a security association.
10. Describe the transport and tunnel modes used for IPSec AH authentication bringing out their scope relevant to IPV4
11. Mention the applications of IPSec.
12. Explain the security association selectors that determine a security policy database entry.
13. Draw a diagram of IPSec ESP format and explain.
14. Mention the important features of Oakley algorithm.

*****ALL THE BEST*****