I CAN DO THIS!! :)

Topics:

- Overview of Security Concept (Chapter 1).***
- User Authentication (Chapter 3).***
- Access Control (Chapter 4).***
    - DISCRETIONARY ACCESS CONTROL (Section 4.3).
    - Example: UNIX Access Control (Section 4.4).
- Database and Data Center Security (Chapter 5).***
- Malicious Software (Chapter 6).***
- Physical and Infrastructure Security (Chapter 16).***
- Denial of Service Attacks (Chapter 7).
- Intrusion Detection (Chapter 8).
- Firewall and Intrusion Prevention Systems (Chapter 9).***
    - Intrusion Prevention Systems (Section 9.6).
- Operating Systems Security (Chapter 12).***
- Cloud and IoT Security (Chapter 13).***
- Security Risk Assessment (Section 14.3).
- Security Auditing (Chapter 18).
- Linux Security (Chapter 25).
- The Bell-Lapadula Model for Computer Security (Section 27.1)
- TCP/IP Headers (Appendix F/slides).***
- Cryptographic Tools (Chapter 2).
- Password-based Authentication (Section 3.2)

Chapter 1- Overview

1.1. Computer Security Concepts
1.2. Threats, Attacks and Assets
1.3. Security Fundamental Requirements
1.4. Fundamental Security Design Principles
1.5. Attack Surfaces and Attack Trees
1.6. Computer Security Strategy
1.7. Standards (ISO, FIPS, HIPAA and RFCs, etc)

CLOS:

1) Describe the key security requirements of confidentiality, integrity, and availability.
2) Discuss the types of security threats and attacks that must be dealt with, and give examples of the types of threats and attacks that apply to different categories of computer and network assets.
3) Summarize the functional requirements for computer security.
4) Explain the fundamental security design principles.
5) Discuss the use of attack surfaces and attack trees.
6) Understand the principle aspects of a comprehensive security strategy.

4 Information Quality Attributes :

- Availability
- Accuracy
- Relevance
- Timelessness

Computer security deals with computer related assets that are vulnerable to a variety of threats and various measures taken to protect those assets.

Key to consider:
1)What assets needs to be protected
2) How are those assets threatened, and
3) What measures can we take to counter those threats.

NIST ⇒ National institute of standard and technology
FIPS ⇒ Federal Information Processing Standard

What is computer security?
It is the measures and controls that are taken to ensure the Confidentiality, Integrity, Availability (Accountability and Authenticity) of information system assets such as hardware, software, firmware (permanent software, aka software for the hardware) and information that is processes, stored or communicated.
FIPS 199, only lists Confidentiality, Integrity and Availability as the 3 main security objectives/requirements for the protection of information system assets, but others in the security field feel Accountability and Authenticity should be included also.

What do we consider as Information system assets?
Hardware
Software (Firmware, which is also type of software)
Data
Communication lines and networks

While Hardware and software may be expensive, unique data cannot replaced.

Describing the Key Security requirements of Confidentiality, Integrity, Availability, Accountability and Authenticity.

Confidentiality:

It means preserving authorized restriction on information access, including the means, which we use, to protect private and proprietary information.

Confidentiality also encompasses concepts of Data confidentiality and Privacy.

Data confidentiality ensures that private or confidential data is not accessible to unauthorized individuals.

Privacy assures that individuals maintain the right to determine what information about them is collected, by whom and how is it stored, and to whom it is disclosed.

A loss of confidentiality is when there unauthorized access or disclosure of information.

Integrity :

Guarding against improper modification or destruction of information, and ensure information non-repudiation and authenticity

Integrity encompasses the key concepts of Data integrity and System Integrity.

Data integrity assures that data or program is not modified or destroyed by unauthorized access.

System integrity ensures that the system works un-impaired, without the influence or manipulation of an unauthorized entity.

A loss of integrity is when there is unauthorized modification, or destruction of information.

Availability:

Assures that system works promptly and authorized users are not denied access

Availability ensures redundancy. Meaning that there are multiple backup and failsafe countermeasures that even if here is a critical system failure then there are measures in place to handle this situation so that the system works promptly and authorized users are not denied access.

A loss of availability means there is a disruption of access to or use of information or information system.

Accountability

Generates the requirement that the action of an entity can be traced back to the entity

A loss of accountability is when events are not logged thus, the actions an entity cannot be traced back to it within a given system environment.

Authenticity

Is the property of being genuine; Being able to be verified and trusted; Confidence in validity of transmission, message, and message originator.

Simply, it means users say who they are and input arriving into the system is from a trusted source.

A loss of authenticity is when trust is lost from the message originator, or the input into the system causes harm.

Non-repudiation:

⇒ means someone cannot deny being responsible for something
⇒ it is the assurance someone cannot deny something
⇒ it ensures that individuals are accountable for what they do
⇒ Prevents either sender or receiver from denying a transmitted message
⇒ When a message is sent, the receiver can prove that the alleged sender in fact sent the message
⇒ When a message is received, the sender can prove that the alleged receiver in fact received the message

CLO #2 Discuss the the types of security threats and attacks that must be dealt with and give examples to the types of threats and attacks that apply to different categories of computer and security asset.

We consider Hardware, Software, Data, and Communication lines and networks to be Information system or Computer system resources.

Hardware: Including computer systems and other data processing, data storage, and data communications devices

Software: Including the operating system, system utilities, and applications.
Data: Including files and databases, as well as security-related data, such as password files.

Communication facilities and networks: Local and wide area network communication links, bridges, routers, and so on.

Table 1.3

Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Action of threat	Consequences of actions
-Exposure, -Interception, -Interference, and -Intrusion.	Causes Undisclosed Disposure, which is breach of confidentiality.
-Masquerade, -Falsification, and -Repudiation.	Causes Deception, which is breach of Integrity.
-Incapacitation, -Corruption, and -Obstruction.	Causes Disruption, which is breach of availability.
-Misappropriation, and -Misuse.	Causes Usurpation, which is breach of confidentiality, integrity and possibly availability. Depneding on nature of misuse.

Key threat of hardware is availability. It is most susceptible to attack and least susceptible to automated controls.

Key threat to software is attack on availability. This is because software can be easily deleted. Software modification + trojan horse viruses can also attack integrity and authenticity.

Security concerns with data include, availability, secrecy and integrity.

Security concerns with Communication lines/centers and networks can be classfied into two types. Active and passive Attacks.

Active attack is when an attacker tried to directly modify or tamper with a system resource or utility. Active attacks are easy to find but hard to deal with. Focus in on detection and recovery. Four categories: Replay Masquerade Modification of message Denial of service	While, an passive attack is when an attacker tries to learn and use the system, which also modifies the use of system resources. Passive attacks hard to find but easy to deal with. Focus is on prevention. Two categories: Traffic analysis. Release of message conents.

Advanced persistent threats (APT) posses the following traits.
These threats are,

1) Organized,
2) Directed,
3) Well Financed,
4) Patient.
5) Silent

The types of attack are either passive or active.
The types of harm these attackers could cause are, Undisclosed Disposure, Deception, Disruption and Usurpation.

3 types of controls, which are Physical, Procedural and Technical, deal with the Human/not-Human, Malicious/not-malicious and Directed/not-directed threats to protect Confidentiality, Integrity and Availability.

Aim of APT attacks vary from stealing intellectual property, infrastructure related data to physical disruption of infrastructure.

Techniques used by APT attacks are,

1) Reconnaissance, involves using a conduit to gain access. For eg, blackmailing employee, or using keyloggers.
2) **Through Social engineering ==>i.e. Tricking users to gain access to system**
    a) **Eg phishing ⇒ impersonating an trusted source/by email, Vishing ⇒ by Voice, Smishing ⇒ by SMS, pharming ⇒ redirected to**

masquerade, Spear phishing website, pretexting. DNS poisoning, and DNS spoofing.

3) Establish a covert backdoor.
4) Establish command and control infrastructure.
5) Achieve objective, and
6) Maintain presence

Some tools used for social engineering to exploit human elements,

1) Spear-Phishing Attack Vectors

2) Website Attack Vectors

3) Infectious Media Generator

4) Create a Payload and Listener

5) Mass Mailer Attack

6) Arduino-Based Attack Vector

7) SMS Spoofing Attack Vector

8) Wireless Access Point Attack Vector

9) QRCode Generator Attack Vector

10) Powershell Attack Vectors

11) Third Party Modules

Solve phishing through MFA and bots using google captcha.

According to a report by the National Research Council, NRC 02, the general vulnerabilities to a computer system or network asset is:

1) System may get leaky, which means a loss of confidentiality since confidential data could get spit out by mistake to unauthorized entity.
2) System may get corrupted, which means system does the wrong thing or gives the wrong answers. Thus, this is a loss of confidentiality.
3) System may become unavailable or very slow. This is an issue to availability.

Vulnerabilities are threat to a system.
An attack is a threat carried out. If successful it leads to serious security violations.
The entity carrying out the threat/attack is called the threat agent.
The attacker represents risk to an asset.

We can distinguish attacks into 2 types:
Active: when an attacker tries to directly alter a system resource or operation of the system.
Passive: when an attackers tries to learn and make use of the system, which affects the system resources.

Attacks can also be classified based on origin of attack.
Inside attack ? an attack initiated inside the security perimeter, by an insider
Outside attack? An attack initiated from outside the security perimeter, by unauthorized or illegal user

Countermeasures are taken to deal with security attacks.

Ideally goal of a countermeasure is prevent the success of an security attack.

If the success of an attack cannot be prevented then the strategy is to detect and recover.
Detect the source of an attack and recover the content that was stolen.

CLO #3 Summarize the functional requirements for computer security

There are 17 functional security requirements.

1) Access Control, which deals with limiting access to information system for everyone.
2) Awareness and training, which deals with managers knowing the risks and personnel being adequately trained.
3) Audit and accountability: deals wirth tracking, logging, information non-repudiation and enforcing accountability.
4) Certification, accreditation and security assessments.
5) Configuration management, which means establishing and maintaining baseline configurations and inventories.
6) Contingency planning (SORRY BUT DONT HAVE TIME TO WRITE ALL :( )
7) Identification and authentication
8) Incident response
9) Maintenance
10) Media protection, which deals with system media.
11) Physical and environment protections
12) Planning
13) Personnel Security
14) Risk assessment
15) Systems and services acquisition
16) System and communication protection
17) System and information integrity.

CLO#4 Explain the fundamental design principles

There are 13 fundamental security design principles:

1) Economy of mechanism
2) Fail-safe defaults
3) Complete mediation
4) Open design
5) Separation of privilege
6) Least privilege
7) Least common mechanism
8) Psychological acceptability
9) Isolation
10) Encapsulation
11) Modularity
12) Layering
13) Least astonishment

CLO#5 Discuss the use of attack surface and attack trees

Attack surface and attack trees are essentially ways by which we identify and classify threats.

An attack surface consists of reachable and exploitable vulnerabilities in a system.

There three types of attack surfaces:
-Software attack surface,
-Network attack surface, and
-Human attack surface.

Identifying attack surfaces allows us to evaluate and classify threats better. After identifying the attack surfaces of our system we can make the surface smaller as to make the task of the threat more difficult.

An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

CLO#6 Understand the principles aspect of a comprehensive security strategy

The principles of a comprehensive security strategy include,

1) Specification/policy, i..e what is the security scheme suppouse to do?
2) Implementation/mechamuism, i.e. how does it work?
3) Correctness/assurance, i.e. does it really work?

Four courses of action with context to a security implementation are,

1) Prevention,
2) Detection,
3) Recovery, and
4) Response.

For consumers of security products we have the following course of actions:

1) Assurance
2) Evaluation

The different types of standards we consider are:

1) National Institute of Standards and Technology (NIST)
2) Internet Society (ISOC)
3) International Telecommunications Union (ITU-T)
4) International Organization for Standardization (ISO)

Chapter#3- User Authendication

3.1. Digital User Authentication Principles
3.2. Password-Based Authentication
3.3. Token-Based Authentication
3.4. Biometric Authentication
3.5. Remote User Authentication
3.6. Security Issues for User Authentication

1) Discuss the four general means of authenticating a user's identity.
2) Explain the mechanism by which hashed passwords are used for user authentication.
3) Understand the use of the Bloom Filter in password management.
4) Present an overview of token-based user authentication.
5) Discuss the issues involved and the approaches for remote user authentication.
6) Summarize some of the key security issues for user authentication.

These four general means can used alone or in combination.

So, the four general means to authenticate a user's identity are,

1) Something that the individual knows. This includes passwords, PINs, or answers to questions
2) Something that the individual poses. This includes tokens and physical keys such as key cards etc.
3) Something that the individual is (static biometrics). This includes recognition by fingerprint, retina and face.
4) Something that the individual does (dynamic biometric). This includes, recognition by voice pattern, handwriting characteristics, and typing rhythm

CLO#2 Explain the mechanism by which hashed passwords are used for user authenticity

For a UNIX system, when a new user selects or is assigned a password. Then that plaintext password and a salt value (which is pseudo random or random), are taken as inputs for a hash function to produce a hashcode which acts as the encrypted password. The plaintext-salt and the encrypted password are stored in the password file for that user-id.

So when a user logs in, he/she provides the plaintext password which is then combine with the plain-text salt value, and they are then again taken as inputs into the same hashing functions which produce an output. This output is then checked against the stored encrypted password to see if they match. VERYY COOL BOI!!!!

The salt, in this case is a pseudo-random or random, key which is used for encryption.

The salt serves 3 purposes,

1) Prevents duplicates password inputs from having the same hashvalue.
2) It greatly increases the difficulty of dictionary attacks.
3) It becomes nearly impossible to find out whether a person has used the same password on the two or more systems.

Slow hash functions (decent)	Crypt (based on original DES that is 56 bits)	Salt value = 12-bits	Output hash value = 64 bits	25 inner loop iterations (solved by super counter method. Solution to this encryption scheme is available for < 10,000$
Slower hash function (good)	MD5 (similar to SH1)	Salt Value = 48-bits (no limitation on password length)	Output hash value = 128-bits	1,000 inner loop iterations
Slowest hash functions (best)	Bcrypt (based on Blowfish symmetric block cipher) For OpenBSD only.	Salt Value = 128 bits Allows for passwords 55 characters in length.	Output hash value = 192-bits	

From Password P1 lecture slide.

RFC 4949 defines User authentication as, the process of verifying an identity by or for a system entity.

Authentication process consists of two steps,
1)Identification step, which means presenting an identifier to the system.
2) Verification step, which means providing authentication information to the system.

In essence, identification means that users claim to be who they say they are, and user authentication is means of establishing the validity of their claim.

This is different from message authentication, which allows communicating parties to ensure that the contents of the message received has not been altered and that the source is authentic.

4 means for user authentication are,

1) Something that the user knows
2) Something that the user has
3) Something that the user is
4) Something that the user can do

8 Password Vulnerabilities are,

1) Offline dictionary attack, where strong controls are needed. Hacker can get password file from system through which he/she can get can get the ID/password of the user but running the obtained password file against popular hashes.
2) Specific account attack, where attacker targets a specific account and submits password until correct password is discovered.
3) Popular password attack, where attackers tries to submit popular passwords for each user id. A cool countermeasure is to check the IP address of the authentication request and check the cookies for submission patterns.
4) Password guessing against single user, where attacker tries to gain knowledge about account holder and password policies and then tries to guess password.
5) Workstation highjacking, where waits until a logged-in workstation is unattended.
6) Exploiting user mistakes, where attacker exploits users use of same password for multiple devices connected to the same network.
7) Exploiting user mistakes, where attacker takes advantage of user mistake such as writing down password on physical piece of paper.
8) Electronic monitoring, where eavesdropping technique is used by attacker.

Chapter#4

4. Chapter 4- Access Control
    - 4.1. Access Control Principles
    - 4.2. Subjects, Objects and Access Rights
    - 4.3. Discretionary Access Control
    - 4.4. Example: UNIX File Access Control
    - 4.5. Role-BAsed Access Control
    - 4.6. Attribute-Based Access Control

1) Explain how access control fits into the broader context that includes authentication, authorization and audit.
2) Define the three major categories of access control policies.
3) Distinguish among subjects, objects and access rights.
4) Describe the UNIX file access control model.
5) Discuss the principle concepts of role-based access control.
6) Summarize RBAC model.
7) Discuss the principle concepts of attribute-based access control.
8) Explain the identify, credentials, and access management model.
9) Understand the concept of identity federation and its relationship to a trust framework.

Access control implements a security policy that determines who or what has access to a system resource, and the type of access that is permitted on each instance.

Always adhere to the basic requirements for Access control (this applies to the broader context),

1) Limit information system access to authorized users, or processes acting on behalf of authorized users, or devices (such as a other information systems)
2) Limit information system access to types of functions and/or transactions that authorized users are allowed to execute.

Think of access control as a another layer of security.

Key terms to also consider with context to control access,

1) Authentication. This means verification of credentials of a user or information system entity.
2) Authorization. This function determines who is trusted for what purpose.
3) Audit. This means examination and review of system activity to ensure compliance.

Different types of access control policies are,

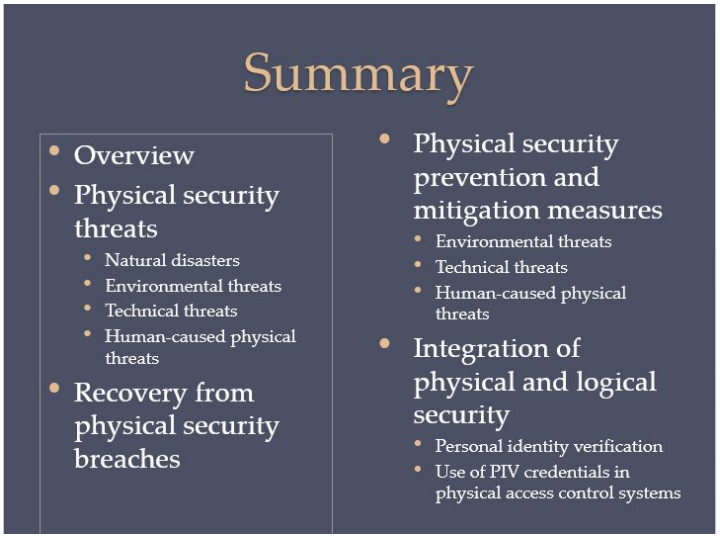
1) Discretionary access control (DAC)
2) Mandatory access control (MAC)
3) Role-based Access control (RAC)
4) Attribute-based access control (ABAC)

CLO#4 Describe the UNIX file access control model

On top of UNIX file access mechanism (user class ---. Group class ---, other class ---. (rwx)) a file in a UNIX system can have a access control list.

To this file, users and groups can be assigned by administrator or super user using “setfacl” command.

Chapter#16



Chapter#6

6. Chapter 6- Malicious Software
   - 6.1. Types of Malicious Software-- Malware
   - 6.2. Advanced Presistent Threat
   - 6.3. Propagation--Infected Content--Viruses
   - 6.4. Propagation--Vulnerability Exploit--Worms
   - 6.5. Propagation--Social Engineering--Spam E-mail, Trojans
   - 6.6. Payload--System Corruption
   - 6.7. Payload--Attack Agent--Zombie, Bots
   - 6.8. Payload--Information Theft-- Keyloggers, Phishing, Spyware
   - 6.9. Payload--Stealthing--Backdoors, Rootkits
   - 6.10. Countermeasures

CLOs

1) Describe three broad mechanisms malware uses to propogate.
2) Understand the basic operation of viruses, worms and Trojans.
3) Describe four broad categories of malware payload.

4) Understand the different threats posed by bots, spyware and rootkits.
5) Describe some malware countermeasure elements.
6) Describe three locations for malware detection mechanism.

Types of Malware are,

1) APT, differ from normal attacks in that they are well planned and financed. Often polotically motivated or state sponsered. Examples include Aurora, RSA, APtT1 and Stuxnet
2) Adware
3) Attack kit, are also called crime-ware, examples = zuzes and angler
4) Auto-rooter
5) Backdoor (trapdoor)
6) Downloader
7) Drive-by-download. This explores browser vulnerabilities. Does not actively propograte like worms. Spreads when users visit malicious websties. “Watering-hole” is a variant this attack, which is more targeted towdards a paticular system user.
8) Exploits
9) Flooders (Ddos clients)
10) Keyloggers
11) Logic Bombs
12) Macro Viruses
13) Mobile Code
14) Rootkit. There are 6 types of root-kits, Persistent, Memory-based, User-mode, Kernel-mode, Virtual machine based and External mode.
15) Spammer program
16) Spyware
17) Trogan horse
18) Virus
19) Worm
20) Zombie, bot

Malware are classified on 4 broad catagories such as,
How does malware spread or propograte to reach the desired target?
What is the malwares payload or actions when it reaches the target?
Malwares that need a host? (parasite code such as viruses)
Malwares that are independent and self-contained? (worms, trograns and bots)
Malwares that does not replicate (trogans and spam emails)
Malwares that does replicate (viruses and worm)

CLO#1 Describe three broad mechanisms that malware use to propagate?

The three propogation mechamisms includes,

1) Infection of exsisting conent by virus, which spreads to other infromation system.
2) Exploit of software vunerability by worm or drive-by-dowanload, that allows for replication of malware
3) Social engineering, where users are convinced to bypass security and install trograns or repond to phising email

CLO#2 Understand the basic operations of viruses, worms and trojans

Virus, replicates itself by copying itslef into surruoinduing files. Spreads like a infection. Easliy spread through network encrinments.
Vrisus can only do what a the executable file it is attatched to can do. Runs secretly.
3 main components of a virus are,
1)Infection mechanism, how it spreds aka infection vector
2) Trigger, how it payload is activived or delivered aka logic bomb
3) Payload, what the virus does (besides spreading)

The 4 phases of the virus are,
1)Dormat Phase,
2)Triggering phase,
3)Propogration phase, and
4)Execution phase.

Macro viruses are viruses that attach themselves onto macros or scripting code. ⇒ melissa virus

There are 2 ways to classify a virus,

1) Classify by target. This inclides 4 types of viruses, which are, bootsector infector, file infector, macro virus and multipartile virus.
2) Classify by concealment strategy. This includes, encrypted viruses, stealth viruses, polymorphic viruses and metamorphic viruse.

Worms actively seek to infect systems and upon infection turn the system into a launch pad for launching more attacks.

Worm expliots software vunrearablituies in client and server programs
To replicatem, worms needs access to remote systems. This includes, electronic mail or instant messaging facility by emailing or instant messaging itself to replicate. File sharing by creating copy in file system. Remote execution Capability, remote file acess or tranfer capability, and remote login capability.

How worms targets is by,

1) Scanning
2) Random
3) Hit-list
4) Topological, this means use info from infected host to find other machines.
5) Local subnet

Morris worm, 1988. This was designed to spread on UNIX systems.

5 characteristics of wrom technology are,

1) Multiplatform,
2) Multi-exploit
3) Ultrafast spreading
4) Polymorphic

5) Metamorhphic

NIST SP 800-28 defines mobile code as, “ programs that can be shipped unchanged to heterogeneous platforms and be executed with identical semantics.

Mobile code takes advanage of, Java applets, ActiveX, Javascript, VBscript.

Common was to use mobile code for malisuous operations on local system are,

1) Cross-site scripting
2) Interactive and dynamic websites
3) Email attachments
4) Downloads from untrusted sites or untrusted software.

Bots use IRC servers (internet chat relay) where the bots are all connected to the same channel and intrpret messages as commands.

CLO#3 Describe four broad categories of malware payloads.

Payload actions are performed once malware reaches target system.
The four catagories for malware payloads incude,

1) Corruption of sytem or data files. This includes data destruction and ransomwae, real-world destruction and logic bomb. (eg, chernobyl virus, Klez, and Ransomware.) (logic bomb is code embedded in malware, waiting to explode when triggered by action, event or condition.)
2) Theft of service, where system is made a zombie agent of attack, as a part of botnet. (Botnet is a collection of bots that are capable of acting in a coordinated manner, to perform attacks such as DDos, Spamming, sniffing traffic, speading malware and keylogging, etc.)
3) Theft of information from system/keylogging (examples of this include, keylogger and spyware)
4) Stealthing/hiding it's presence on the system

CLO#5 describe malware countermeasure elements

The ideal strategy is prevention. This includes, policy, awareness, vulnerability mitigation, and threat mitigation.

If prevention fails then strategy is to,

1) Detect

2) Identify, and
3) Recover.

-Generations of Anti-virus Scanner, are from 1 to 4. We are currently at fourth generation, which is fully featured protection.

Simple scanner to hueristic scanners to activity traps to fully featured protection.

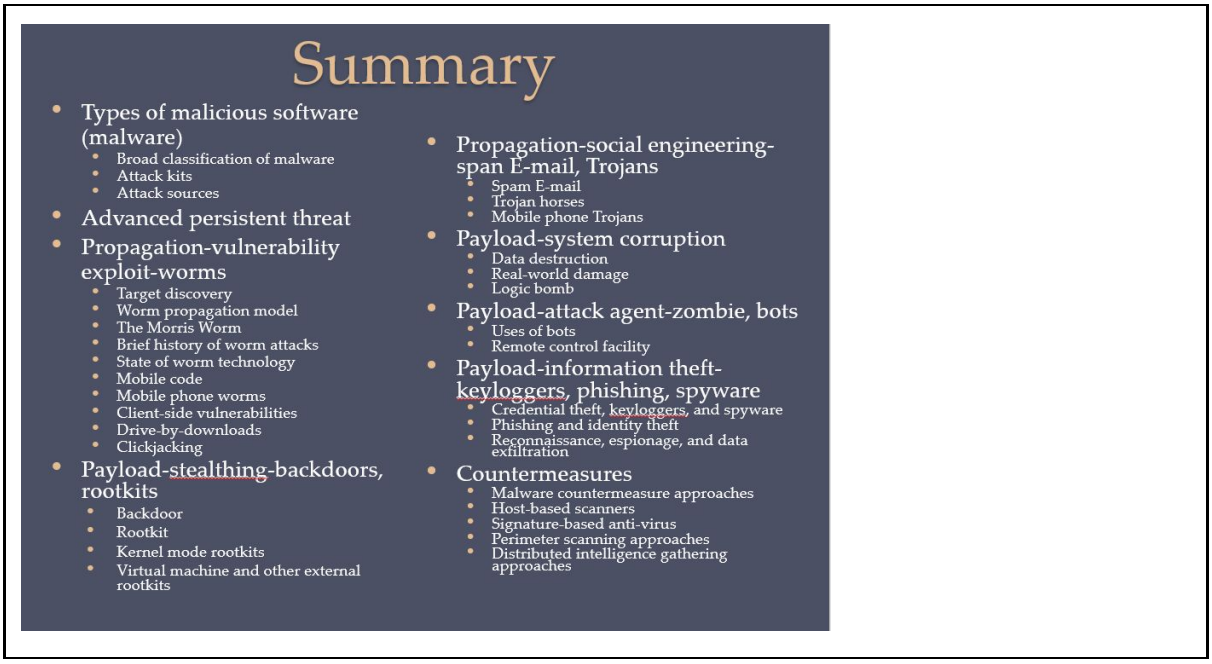
-Sandbox analysis is another method for detecting and analyzing malware.

-Host-based Behaviour - Blocking software. Is a type of malware blocking software that integrates with host and monitors program behaviour in real-time. This is not anti-virus software. Blocking software monitors programs realtime and has advantage over anti-vrius software. Limitation is that malicious software often runs before all it's behaviour is identified so it can cause harm before it is detected.

-Perimeter Scanning Approaches. Is uses anti-virus software on a firewall inside the email and web proxy servies, which are running on the systems. To detect malware content on whole network. However, since it cannot detect any other types of behavious except malware content, it is useless when set up on a already infected system.

There are two types of monitoring software. This includes, Ingress and Egress monitoring.
Ingress for monitoring incoming traffic and Egres for monitoring outgoing traffic.
Remeber, both these approches are limited to scanning only malware content.

CLO#4



COVER THIS CLO FOR SSL/TLS Slides and GO OVER THE ASMMERIC AND SYMMETRIC STUFF

EXTRA NOTES FOR SHIEEEEZZZZ :) ;) :) :P
Four general means to authenticate a user are,

1) Something that the user knows, such as passwords, PIN or answers etc
2) Something that the user has. This includes tokens (which are a series of special bits that circulate in a given network, and act as tickets) and physical keys such as key cards.
3) Something that the user is (static biometrics). This, includes recognition by fingerprint, face or retina
4) Something the user can do (dynamic biometrics). This includes, recognition by voice patter, typing pattern or handwriting characteristics.

Topics: You should focus on the following sections; however, many topics are interrelated).

- Denial of Service Attacks (Chapter 7).
- Intrusion Detection (Chapter 8).
- Intrusion Prevention Systems (Section 9.6).
- Operating Systems Security (Chapter 12).
- Cloud and IoT Security (Chapter 13).
- Security Risk Assessment (Section 14.3).
- DISCRETIONARY ACCESS CONTROL (Section 4.3).
- Example: UNIX Access Control (Section 4.4).
- Security Auditing (Chapter 18).
- Linux Security (Chapter 25).
- The Bell-Lapadula Model for Computer Security (Section 27.1)

- TCP/IP Headers (Appendix F/slides).
- Overview (Chapter 1).
- Cryptographic Tools (Chapter 2).
- Password-based Authentication (Section 3.2)

Chapter 7: Denial-of-service attacks

Ch7. Denial-of-service attacks
- 7.1. Denial-of-service attacks
- 7.2. Flooding attacks
- 7.3. Distributed denial-of-service attacks
- 7.4. Application-based bandwidth attacks
- 7.5. Reflector and Amplifier attacks
- 7.6. Defences against Denial-of-service attacks
- 7.7. Responding to a Denial-of-service attack

CLOS:
1) Explain the basic concept of a denial-of-service attack
2) Understand the nature of flooding attacks
3) Describe distributed denial-of-service attacks
4) Explain the concept of an application-based bandwidth attack and give some examples.
5) Present an overview of reflector and amplifier attacks
6) Summarize the some of the common defense against denial-of-service attacks
7) Summarize common response to denial-of-service attacks

DoS is an attack on availability of blocking or hindering the provisioning of some service.

CLO#1 Explain the basic concept of a denial-of-service attack (DoS)
NIST defines denial-of-service attacks as an action that prevents or impairs the authorized use of a network, system or application by exhausting resources such as CPU, bandwidth and disk space

3 categories of resources that can be affeced by DoS attacks:
1) Network bandwitdth ⇒ relates to the capacity of links, which connects an organizations server to the internet.
    a) It is usual in an overloaded TCP/IP network that legitimate users expwericnes degraged or no service.
    b) The DoS attack for this cattagory of resource takes advanatage of the ISP routers ability to handle a higer capacity of traffic then the organizartion's link can handle. Thus, the router discards packets, only delivering what can be handled by the link.
    c) The goal of attacker is to overwhelm the link with illegitamate traffic effectively definying legitae user access to the server.
    d) Takes advanatahe of ISP routers high capacity taffirc handling & the server in-ability to filter malicious from actual traffic.

2) System Resoruces
    a) Attacks target the network handling software of the system, causing it to overwhelm and crash. Meaning that until the software is reloaded the system will not be able to communicate over the network.
    b) This is acchomplished by sending specific packets that use up limited resources on the system or packets whose structure triggers specific bugs in the system.
    c) Known as packet poisoning.
        i) Ping to death and teardrop attacks that targeted old windows 9x system were of this form.
        ii) Spcifically, bugs that targeted the windows network code that handeled ICMP echo request packets and packet fragmnetation.
    d) Resourcess that are targeted involve temporary buffers, table of open connections and similar memory data structures.
        i) SYN spoofing tragets table of TCP connections on the server.
3) Application resources
    a) An attack on a sepcific application, such as a webserver (which allwos user to make database queires), usually deals with sending legitimate requests that are expensiev and use up resrouces on that applcation, effectibely denying legitimate users acess. This type of attack is called cyberslam.

Overloaded TCP/IP network link (link between a orgranization and it's ISP) ⇒ some customers might lose service or the quaility might degrade

Types of DoS attacks are:
1) Classical aka Flooding attack
    a) Aka flooding ping attack.
    b) Aim is to overwhlem is the capacity of network connection to the target organization.
    c) Traffic can be handeled by higher capacity links on the path but packets are discarded as capacity decreases.
    d) 2 main issues
        i) Soucre of the attack can be clearly identified, and
        ii) A response can be sent back from target to attacker from the ping request requetess, effectively reflecting the attack …..but attacker can have link of higher capacity.
    e) Netwrok performance is noticabley affected.
2) Source address spoofing
    a) Using forged soruce addresses
        i) These soruces addresses can be forged by using the RAW SOCKET INTERFACE on the OS
        ii) Attacker can be harder to identify because of this
    b) Attacker generates a larger volume of packeyts with the traget as the destination address.
    c) Congestion occurs at the last router, connecting to the to lower capacity organzation link
    d) Requries network engineers to specifically query flow of information from their routers
    e) In response to ping requets from spoofed addresses ICMP echo requtes packets are geneested. This is known was backscatter traffic. This traffic

i.e. the type of packets can be analyzed to undersyand the type and size of attack.

f) Security researchers analyze these blocks of un-sed IP to analyze the routes, which help in monitoring attacks.

Side note: The development of TCP/IP took place in a trusting environment. TCP/IP simply does not include the ability by default, to ensure that the source address correspondes to the orginating system.

Filter can be implemented on routers to check if source address is valid but ISPs' do not implement them, eeven after reccomandations from experts.

3) SYN spoofing
    a) Common DoS attack
    b) Attack abikitu of a sevrer to respond to SYN requests by overflowing the TCP table that is used to manange them.
    c) Thus, legitimate users are deined acess to the server
    d) Hence an attack on suystem resoruces, specifially the network handligng code in the OS.
    e) RST packet can be sent back, which thwarts the attack, if the forged address belongs to a legitimate system.

When they say valid packets are dropped that means legitamate users are denied proper acess.

Any packets used in reponse by the server only take up capacity and space on the link
CLO#2: Describe the nature of a flooding attack
Flooding attacks are based on the network protocol used
The aim is to overload the capacity of the link connecting to a sever (of some organization)
Virtually any network packet can be used/
For example,
There is:

1) ICMP Flood
2) UDP Flood
3) TCP-SYN Flood

Catagries of resources affected are:

1) Network bandwidth resource
2) System resource (often the software handling software is owerwhellm or crashed using special packets)
3) Application resource (such as webserver allowing user to make queries. Make legitimate requests which consumes a large amount of resources.)

Flooding attack ⇒
The simplest classical DoS attack is the flooding attack on an organization.

Source Address Spoofing ⇒
A common characteristic of packets that are used for flooding attacks is that they come from forged IPs. (easy to generate via Raw socket interface from OS)
SYN spoofing ⇒
The other classical common DoS attack, which uses spoofed addresses to send SYN requets to target server, effectibvely targeting the TCP table space of that sever and hoping to owewhem the sever by sending invalid requets using spoofed sorource addres.

Flooding attack is not the same as a DDoS attack.
Flooding ⇒ aims to overload the capacity of the network connection by overwhelming the link with large volumes of malicous traffic, causing routers to drop packets. Thus probability of legitimae users receviing degraded or legitimate traffic is high. Bc that is what usually occus when TCP/IP connection is overloaded.

DDoS on the other hand, uses flaws on the OS or a common application to install a software; effectively making that system a zombie.
Nowdays attackers use IRC instant messaging software to handle mutiple zombie systems.
Large collections of systems under the control of one attacker, form a botnet.

Attacks that use multiple systems and attack target indirectly (increase distance between them and the target by having intermediaries) are:

1) DDoS attacks
2) Reflector attacks
3) Amplifier attacks

TFN (tribal flow network) ⇒ old DDoS attack that used a CLI as it's handler (nowdays attacker use an IRC (internet relay chat) or an instant messaging server program or Web-based HTTP server to manage communication with agents)

Application based bandwidth attacks
A potential effective strategy for DDoS attacks is to make the target execute resource-consuming requests which is disproportionate to the attack effort.

Application based bandwidth attacks attempt to take advantage of disproportionately large resource consumption at a sevrer. Two protcol that are examples of this are:

1) SIP floods - Used in VoIP protocol to initiate the connection. Overload the proxy server and target with INVITE requests.
    a) 2 ways for proxy server
        i) Deplete resources in processing requests
        ii) Consume network capacity.
2) HTTP based attacks
    a) HTTP flood ⇒ flood webserver with HTTP requests
        i) Spidering ⇒ bots following HHTTP link and following all links on the provided website in a recursive way.
    b) Slowloris ⇒ send valid HTTP requets but intentonally never complete them.

Reflection Attacks ⇒ a variant of this is the Amplification attack ⇒ a variant of this is the DNS amplification attack.
I.e. these attacks all share the trait of having intermediary and trying to condut attack without alerting the intermediary.

Attacker sends address to a know service on the intermediary with spoofed address of target system. The intermediary responds by sending packets the trarget system, efflectivey reflecting the attack off the intermediary.

Goal is to generate large volumes or flood the link without alerting the intermediary.

Apmplication attack ⇒ sending the address to a service on intermediary and this time mutiple reponses are reflected back to the target. This is done as the original request is sent to the broadcast address on some network and all hosts might respond. Essentiaolly amplifying the attack.

DNS amplification attack:

1) Contrasts with the regular definition of amplification attack.
2) Takes advayaghe of the DNS protocol where one small request is turned into multiple larger requests.
3) 60-byte UDP requet is turned into 512-byte UDP response packet.
4) 4000 bytes to suppourt extended DNS features such as IPv6

To deal with Source Address Spoofign ISP could implement anti-spoofing fillyers on their router to ensure that valid source IP are being used for all packets by their customer. While filtering inccurs a small pefromance cost so does the cost of havign high volume of malcious traffic used for DoS attack.

To defend aganst SYN spoofing ⇒ use modified TCP request handling code. SYN cookies which do not take up memory resources, until the 3-way handshake is complete, effective reducing the potential of table overflowing.
How it works ? instead of saving infomation critical for establisng connetion ON the server in the List of TCP connections, the info is cryptographicallluy encoded into a cookie and sent as seq numebr back to the clident as SYN-ACk packet. Onece the incremented seq vale is recieved from the ACK packet from clident. Then that critical information is reconstructed, as it would have been saved in the table of TCP connections.
Or could use selective drop or random drop to remove incomplete tcp table entry if table is full

Best defence against broadcast amplification is to block use of IP-directed broadcast at the ISP or organizational server level, who is being used as a a intermediary

4 lines of defence against DoS attacks
Attack preventon and preemption (before attack)
Attack detection and filtering (during the attack)

Attack source traceback and identification (during the attack back)
Attack reaction (after the attack)

In essence there are 8 things for DoS attack prevention:

1) Block spoofed source adddresses
2) Filter used to ensure path baack to the claimed soruce adddress is the one being used by the current packet
3) Use modfied TCP connection handling code.
4) Block IP directed broadcasts
5) Block suspicipus services and combinationss
6) Manage application attacks with a form of graphical puzzle (captha) to distinguuish legitimage human requests
7) Good general system practises
8) Used mirrioed and replication servers when high performace and reliability is required.

Responding to DoS attacks
Good Incident response plan included 3 things⇒

1) Details on how to contact technical personal for ISP
2) Neeeded to impose traffic filtering upstream
3) Details of how to respond to the attack

Responding to DoS attacks

1) Identify type of attack
2) Have ISP traceback packet flow back to soruce
3) Implement contingency plan
4) Update Incident response plan.

Distributed Denial of Service attacks
Use of multiple systems to generate attacks
Attacker uses flaw in OS or vunurabiluty in a common application, and intalls their program into it (making it a zombie)
Large collections of systems under the control of one attacker, forming a botnet.

Ch8. Intrusion Detection
- 8.1. Intruders
- 8.2. Intrusion Detection
- 8.3. Analysis Approaches
- 8.4. Host-based Intrusion Detection
- 8.5. Network-based intrusion Detection
- 8.6. Distributed or Hybrid Intrusion Detection
- 8.7. Intrusion Detection Exchange Format
- 8.8. Honeypots 200
- 8.9. Example System: 302

CLOs:
1) Distinguish among various types of intruders beharvior patterns
2) Understand the basic principles of and requirements for intrusion detection
3) Discuss the key features of host-based intrusion detection
4) Explain the concept of distribted host-based intrusion detection
5) Define the intrusion detection exchange format (**intentionally incomplete**)
6) Explain the purpose of honeypots
7) Present an overview of snort

CLO#1 Distinguish among various types of intruders beharvior patterns
Perimeter defences: Firewalls and network-based IDSs.

Class of intruders include
1) Cybercriminal ⇒ organized gorp with goal of financial reward
2) Activists ⇒ insiders or outsider who are motivaed by social or political causes.
3) State Sponsored organizations ⇒ sponsored by government to conduct espoionage or sabotage activities
4) Others ⇒ hacker with motivations other than the ones listed above.

Examples of intrusion:
1) Performing a root-level compromise of a email server.
2) Defacing a website.
3) Gussing and cracking passwords.
4) Copying a database containing credit card numbers.
5) Viewing sensitive data, including payroll and medical information without authorization
6) Running a packet sniffer on a workstation to capture usename and passwords.
7) Using a permission error on an anonymous FTP server to distribute pirated software and music files.
8) Dialing into a unsecured modem and gaining internal network access.
9) Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password.
10) Using an unattended, logging-in workstation without permission.

Zero-day exploits: vulnerabilities that are unknown previously.

Key Security Strategy: defense-in-depth.
IDSs, IPSs, encryption of sensitive information, detailed audit trails, strong authentication and authorization controls, firewalls, activity management of operating system and

application security.

Wide range of attacks included in intruder behaviour are:

1) Target Acquisition and Information Gathering.
    a) Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific Web server and OS used.
    b) Gather information on target network using DNS lookup tools such as dig, host, and others; and query WHOIS database.
    c) Map network for accessible services using tools such as NMAP.
    d) Send query e-mail to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
    e) Identify potentially vulnerable services, for example, vulnerable Web CMS.
2) Initial access
    a) Brute force (guess) a user's Web content management system (CMS) password.
    b) Exploit vulnerability in Web CMS plugin to gain system access.
    c) Send spear-phishing e-mail with link to Web browser exploit to key people.
3) Privilege Escalation
    a) Scan system for applications with local exploit.
    b) Exploit any vulnerable application to gain elevated privileges.
    c) Install sniffers to capture administrator passwords.
    d) Use captured administrator password to access privileged information.
4) Information Gathering or System Exploits
    a) Scan files for desired information.
    b) Transfer large numbers of documents to external repository.
    c) Use guessed or captured passwords to access other servers on network.
5) Maintaining Access
    a) Install remote administration tool or rootkit with backdoor for later access.
    b) Use administrator password to later access network.
    c) Modify or disable anti-virus or IDS programs running on system.
6) Covering Tracks
    a) Use rootkit to hide files installed on system.
    b) Edit logfiles to remove entries generated during the intrusion.

CLO#2: Understand the basic principles of and requirements for intrusion detection

Security intrusion: unauthorized act of bypassing the security mechanism of a system.

Intrusion detection: hard or software function that gathers and analyzes information from various areas within a computer or network to identify possible security intrusion.

An IDS has three logical components:

1) Sensors:
2) Analyzers
3) User interfaces

Single sensor and analyzer can be:
1) HIDS on host or

2) NIDS in a firewall device.

IDSs are classified by source and type of data anaylzed:

1) Host-based IDS (HIDS): montors the chatacteristics of a single host and the events occuring within that host, such as process identifiers and system calls they make for evidence of sus activity.
2) Network-based IDS (NIDS): monitors network traffic for particular network segments or devices and analyzed traffic, transport, and application protocols to identify suspicious activity.
3) Distributed or hybrid IDS: combine information from a number or sensors, ofen both host and network-based, in central analyzer that able to better identify and report intrusion activity.

A *DLL* is a library that contains code and data that can be used by more than one program at the same time. For example, in Windows operating systems, the Comdlg32 *DLL* performs common dialog box related functions.

CLO#3: Discuss the key features of host-based intrusion detection

IDS can can halt an attack before any damage is done but it's main purpose is to detect intrusions, log suspicious events and send alerts.

However, the **primary benefit** of a HIDS is that it can detect both external and internal intrusions, something that is not possible with either network-based IDSs or firewalls.

HIDS IDSs can use either anomaly or signature and heuristic approaches to detect unauthorized behaviour on the monitored host.

Datasources and Sensor of HIDS:

1) System call traces
2) Audit (log file) records)
3) File integrity checksums
4) Registry access

Table 8.2 Linux System Calls and Windows DLLs Monitored

(a) Ubuntu Linux System Calls

accept, access, acct, adjtime, aiocancel, aioread, aiowait, aiowrite, alarm, async_daemon, auditsys, bind, chdir, chmod, chown, chroot, close, connect, creat, dup, dup2, execv, execve, exit, exportfs, fchdir, fchmod, fchown, fchroot, fcntl, flock, fork, fpathconf, fstat, fstat, fstatfs, fsync, ftime, ftruncate, getdents, getdirentries, getdomainname, getdopt, getdtablesize, getfh, getgid, getgroups, gethostid, gethostname, getitimer, getmsg, getpagesize, getpeername, getpgrp, getpid, getpriority, getrlimit, getrusage, getsockname, getsockopt, gettimeofday, getuid, gtty, ioctl, kill, killpg, link, listen, lseek, lstat, madvise, mctl, mincore, mkdir, mknod, mmap, mount, mount, mprotect, mpxchan, msgsys, msync, munmap, nfs_mount, nfssvc, nice, open, pathconf, pause, pcfs_mount, phys, pipe, poll, profil, ptrace, putmsg, quota, quotactl, read, readlink, readv, reboot, recv, recvfrom, recvmsg, rename, resuba, rfssys, rmdir, sbreak, sbrk, select, semsys, send, sendmsg, sendto, setdomainname, setdopt, setgid, setgroups, sethostid, sethostname, setitimer, setpgid, setpgrp, setpgrp, setpriority, setquota, setregid, setreuid, setrlimit, setsid, setsockopt, settimeofday, setuid, shmsys, shutdown, sigblock, sigpause, sigpending, sigsetmask, sigstack, sigsys, sigvec, socket, socketaddr, socketpair, sstk, stat, stat, statfs, stime, stty, swapon, symlink, sync, sysconf, time, times, truncate, umask, umount, uname, unlink, unmount, ustat, utime, utimes, vadvise, vfork, vhangup, vlimit, vpixsys, vread, vtimes, vtrace, vwrite, wait, wait3, wait4, write, writev

(b) Key Windows DLLs and Executables

comctl32
kernel32
msvcpp
msvcrt
mswsock
ntdll
ntoskrnl
user32
ws2_32

CLO#4: Explain the concept of distribted host-based intrusion detection
HIDSs are often focused on single-system and stand-alone operations. The typical organization, however, needs to defend a distributed collection of hosts supported by a LAN or internetwork.

Thus a distributed IDS can be centralized or decentralized. But the overall architecture consists of three main components:

1) Host agent module
2) LAN monitor agent module
3) Central manager module

The scheme is designed to be independent of any operating system or system auditing implementation. Figure 8.3 shows the general approach that is taken. The agent captures each audit record produced by the native audit collection system.
A filter is applied that retains only those records that are of security interest. These records are then reformatted into a standardized format referred to as the host

A NIDS monitors traffic at selected points on a network or interconnected set of networks. Two main types of network sensors:

1) Inline sensor: inserted into a network segment so the traffic that it is monitoring must pass through the sensor.
2) passive sensor monitors a copy of network traffic; the actual traffic does not pass

through the device. From the point of view of traffic flow, the passive sensor is more efficient than the inline sensor, because it does not add an extra handling step that contributes to packet delay.

Type of attacks suitable for signature detection:

1) Application layer reconnaissance and attacks
    a)

    Application layer protocols usually analyzed:
    DynamicHost Configuration Protocol (DHCP), DNS, Finger, FTP, HTTP, InternetMessage Access Protocol (IMAP), Internet Relay Chat (IRC), Network FileSystem (NFS), Post Office Protocol (POP), rlogin/rsh, Remote Procedure Call(RPC), Session Initiation Protocol (SIP), Server Message Block (SMB), SMTP,SNMP, Telnet, and Trivial File Transfer Protocol (TFTP), as well as database protocols, instant messaging applications, and peer-to-peer file sharing soft-ware. The NIDS is looking for attack patterns that have been identified as tar-geting these protocols. Examples of attack include buffer overflows, password guessing, and malware transmission.

2) Transport layer reconnaissance and attacks
    a)

    NIDSs analyze TCP and UDP traf-fic and perhaps other transport layer protocols. Examples of attacks are unusual packet fragmentation, scans for vulnerable ports, and TCP-specific attacks such as SYN floods.

3) Network layer reconnaissance and attacks
    a)

    NIDSs typically analyze IPv4, IPv6,ICMP, and IGMP at this level. Examples of attacks are spoofed IP addresses and illegal IP header values.

4) Unexpected application services
    a)

    The NIDS attempts to determine if the activity on a transport connection is consistent with the expected application protocol. An example is a host running an unauthorized application service.

5) Policy violations
    a)

    Examples include use of inappropriate websites and use of forbidden application protocols.

Attacks suitable for anomaly detection:

1) DoS
    a)

Such attacks involve either significantly increased packet traffic or significantly increase connection attempts, in anattempt to overwhelm the target system. These attacks are analyzed in Chapter 7.Anomaly detection is well-suited to such attacks.

2) Scanning
   a)

A scanning attack occurs when an attacker probes a target network or system by sending different kinds of packets. Using the responses received from the target, the attacker can learn many of the system's characteristics and vulnerabilities. Thus, a scanning attack acts as a target identification tool for an attacker. Scanning can be detected by atypical flow patterns at the application layer (e.g., banner grabbing 3), transport layer (e.g., TCP and UDP port scan-ning), and network layer (e.g., ICMP scanning)

3) Worms
   a)

Worms 4 spreading among hosts can be detected in more than one way.Some worms propagate quickly and use large amounts of bandwidth. Wormscan also be detected because they can cause hosts to communicate with each other that typically do not, and they can also cause hosts to use ports that they normally do not use. Many worms also perform scanning. Chapter 6 discusses worms in detail

Stateful Protocol Analysis: subset of anomaly analysis.
SPA understands andtracks network, transport, and application protocol states to ensure they progress as expected. A key disadvantage of SPA is the high resource use it requires.

any particular product or implementation, but its functional components are the key elements of any IDS. The functional components are as follows:

- **Data source:** The raw data that an IDS uses to detect unauthorized or undesired activity. Common data sources include network packets, operating system audit logs, application audit logs, and system-generated checksum data.
- **Sensor:** Collects data from the data source. The sensor forwards events to the analyzer.
- **Analyzer:** The ID component or process that analyzes the data collected by the sensor for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator. In many existing IDSs, the sensor and the analyzer are part of the same component.
- **Administrator:** The human with overall responsibility for setting the security policy of the organization, and, thus, for decisions about deploying and configuring the IDS. This may or may not be the same person as the operator of the IDS. In some organizations, the administrator is associated with the network or systems administration groups. In other organizations, it is an independent position.
- **Manager:** The ID component or process from which the operator manages the various components of the ID system. Management functions typically include sensor configuration, analyzer configuration, event notification management, data consolidation, and reporting.
- **Operator:** The human that is the primary user of the IDS manager. The operator often monitors the output of the IDS and initiates or recommends further action.

In this model, intrusion detection proceeds in the following manner. The sensor monitors data sources looking for suspicious activity, such as network sessions showing unexpected remote access activity, operating system log file entries showing a user attempting to access files to which he or she is not authorized to have access, and application log files showing persistent login failures. The sensor communicates suspicious activity to the analyzer as an event, which characterizes an activity within a given period of time. If the analyzer determines that the event is of interest, it sends an alert to the manager component that contains information about the unusual activity that was detected, as well as the specifics of the occurrence. The manager component issues a notification to the human operator. A response can be initiated automatically by the manager component or by the human operator. Examples of responses include logging the activity; recording the raw data (from the data source) that characterized the event; terminating a network, user, or application session; or altering network or system access controls. The security policy is the predefined, formally documented statement that defines what activities are allowed to take place on an organization's network or on particular hosts to support the organization's requirements. This includes, but is not limited to, which hosts are to be denied external network access.

CLO#6: Explain the purpose of honeypots

Honeypots are designed to:

1) Divert an attacker from accessing critical systems.
2) Collect information about the attacker's activity.

3) Encourage the attacker to stay on the system long enough for administrators to respond.

Honeypots are classified into:

1) Low interaction honeypots: Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems.
2) High interaction honeypots: Is a real system, with a full operating system,services and applications, which are instrumented and deployed where they can be accessed by attackers.

CLO7: Present an overview of snort

Snort is a lightweight IDS that has the following characteristics:

1) Easily deployed on most nodes (host, server, router) of a network.
2) Efficient operation that uses small amount of memory and processor time.
3) Easily configured by system administrators who need to implement a specific security solutuion in a short amount of time.

A SNORT installation consists of four logical components:

1) Packet decoder
2) Detection enginer
3) Logger
4) Alerter

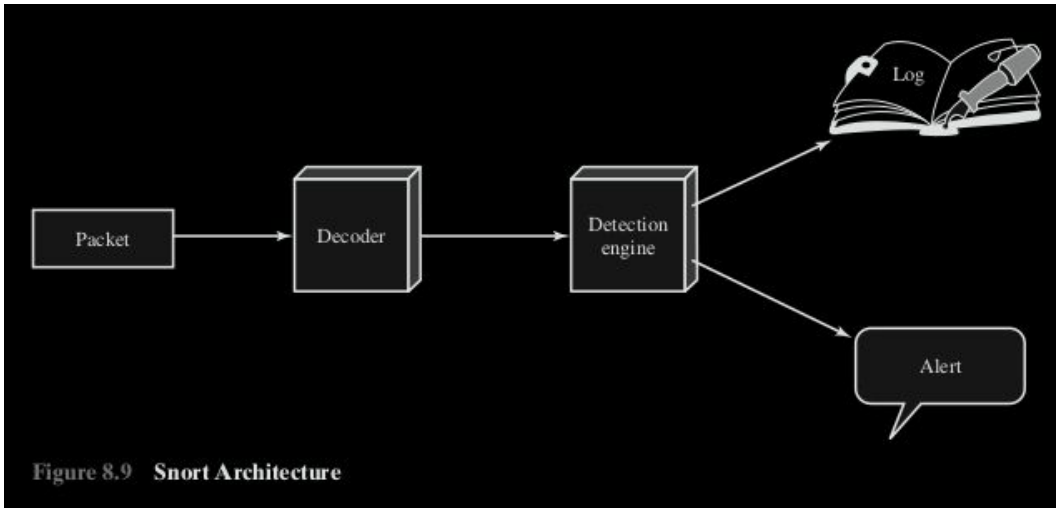


Figure 8.9 **Snort Architecture**

SORT rules:

SNORT uses simple, flexiable rule definition language that generates rules by detection system engine. Each rule consists of a fixed header and zero or more options.

A header had the following elements:

- Action
- Protocol
- Src IP
- Src Port
- Direction
- Dst IP
- Dst Port

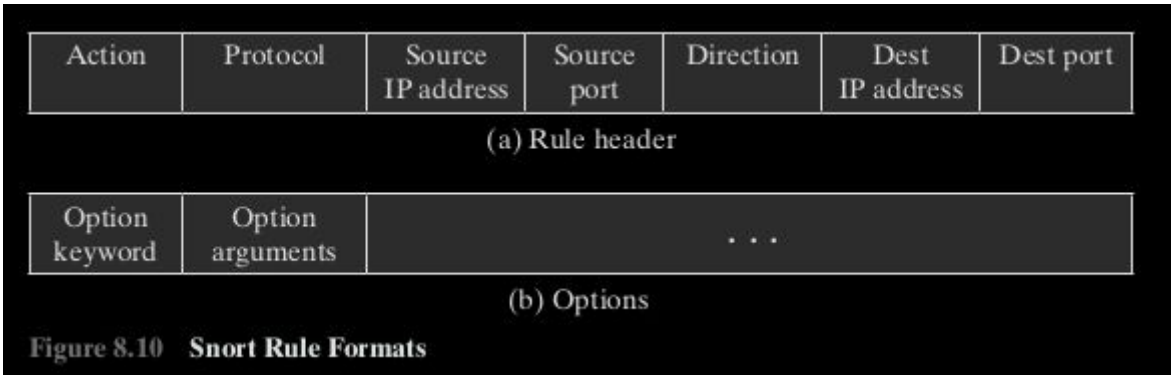


Figure 8.10 **Snort Rule Formats**

Ch9.

9. Chapter 9- Firewall and Intrusion Prevention Systems
   - 9.1. The Need for firewall.
   - 9.2. Firewall Characteristics and Access Policy.
   - 9.3. Types of Firewall.
   - 9.4. Firewall Basing.
   - 9.5. Firewall Location and Configurations.
   - 9.6. Intrusion Prevention Systems.
   - 9.7. Example: Unified Threat Management Products.

1) Explain the role of firewalls as part of a computer and network security strategy.
2) List the key characteristics of firewalls.
3) Discuss the various basing options for firewalls.
4) Understand the relative merits of various choices for firewall location and configurations.
5) Distinguish between firewalls and intrusion prevention systems.

Following notable **developments** in technology have been made:

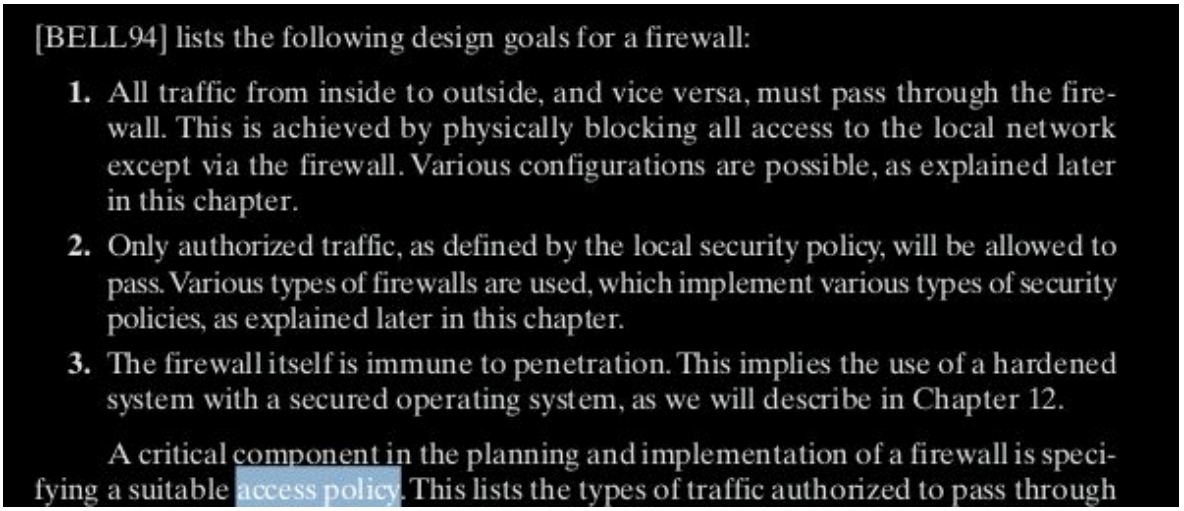
- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe.
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two.
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN).
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN.
- Enterprise cloud computing, which we will describe further in Chapter 13, with virtualized servers located in one or more data centers that can provide both internal organizational and external Internet accessible services.

CLO#1 Explain the role of firewalls as part of a computer and network security strategy.

The Internet isn't a service you connect too, you become part of it. The firewall is inserted between the premises network and the Internet to establish a **controlled link** and erect an outer security wall or perimeter. The goal of this perimeter is to protect the premises

network from Internet-based attacks and provide a single choke point where security and auditing can be imposed. It can be combined with IDSs, IPSs, encryption of sensitive information, detailed audit trails, strong authentication and authorization controls, activity management of operating system and application security- to provide “defense-in-depth”.

CLO#2 List the key characteristics of firewalls.



[BELL94] lists the following design goals for a firewall:

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter.
3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system, as we will describe in Chapter 12.

A critical component in the planning and implementation of a firewall is specifying a suitable access policy. This lists the types of traffic authorized to pass through

Before proceeding to the details of firewall types and configurations, it is best to summarize what one can expect from a firewall. The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that attempts to keep unauthorized users out of the protected network, prohibit potentially vulnerable services from entering or leaving the network, and provide protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
4. A firewall can serve as the platform for IPSec. Using the tunnel mode capability described in Chapter 22, the firewall can be used to implement virtual private networks.

Firewalls have their limitations, including the following:

1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have wired or mobile broadband capability to connect to an ISP. An internal LAN may have direct connections to peer organizations that bypass the firewall.
2. The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
4. A laptop, PDA, or portable storage device may be used and infected outside the corporate network, then attached and used internally.

CLO#3 Discuss the various basing options for firewalls.

9.3 TYPES OF FIREWALLS

A firewall can monitor network traffic at a number of levels, from low-level network packets, either individually or as part of a flow, to all traffic within a transport connection, up to inspecting details of application protocols. The choice of which level is appropriate is determined by the desired firewall access policy. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative

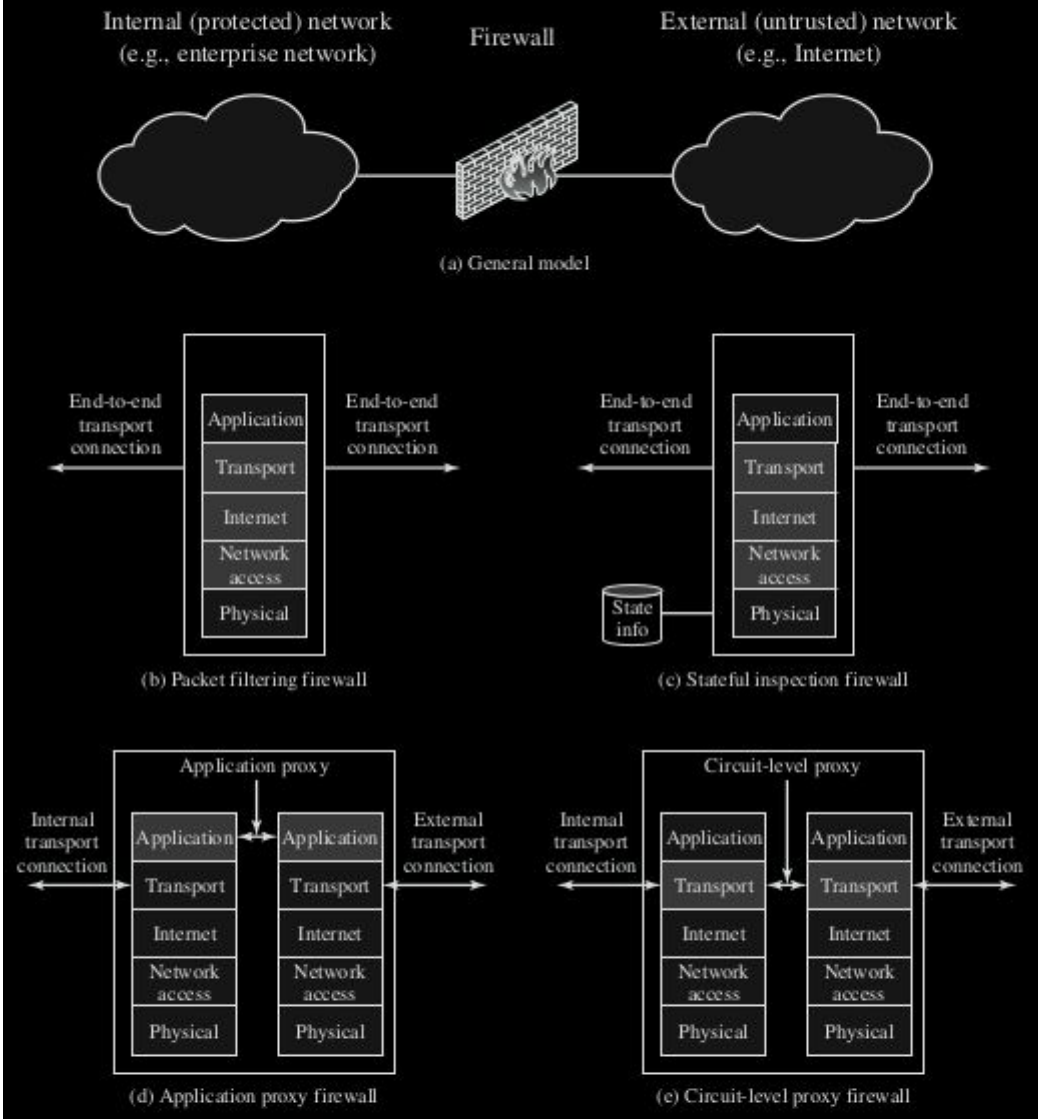


Figure 9.1 **Types of Firewalls**

filter, rejecting any packet that meets certain criteria. The criteria implement the access policy for the firewall that we discussed in the previous section. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. In this section, we look at the principal types of firewalls.

CLO#4 Understand the relative merits of various choices for firewall location and configurations.

DMZ Networks

Figure 9.2 illustrates a common firewall configuration that includes an additional network segment between an internal and an external firewall (see also Figure 8.5). An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate website, an e-mail server, or a DNS (domain name system) server.

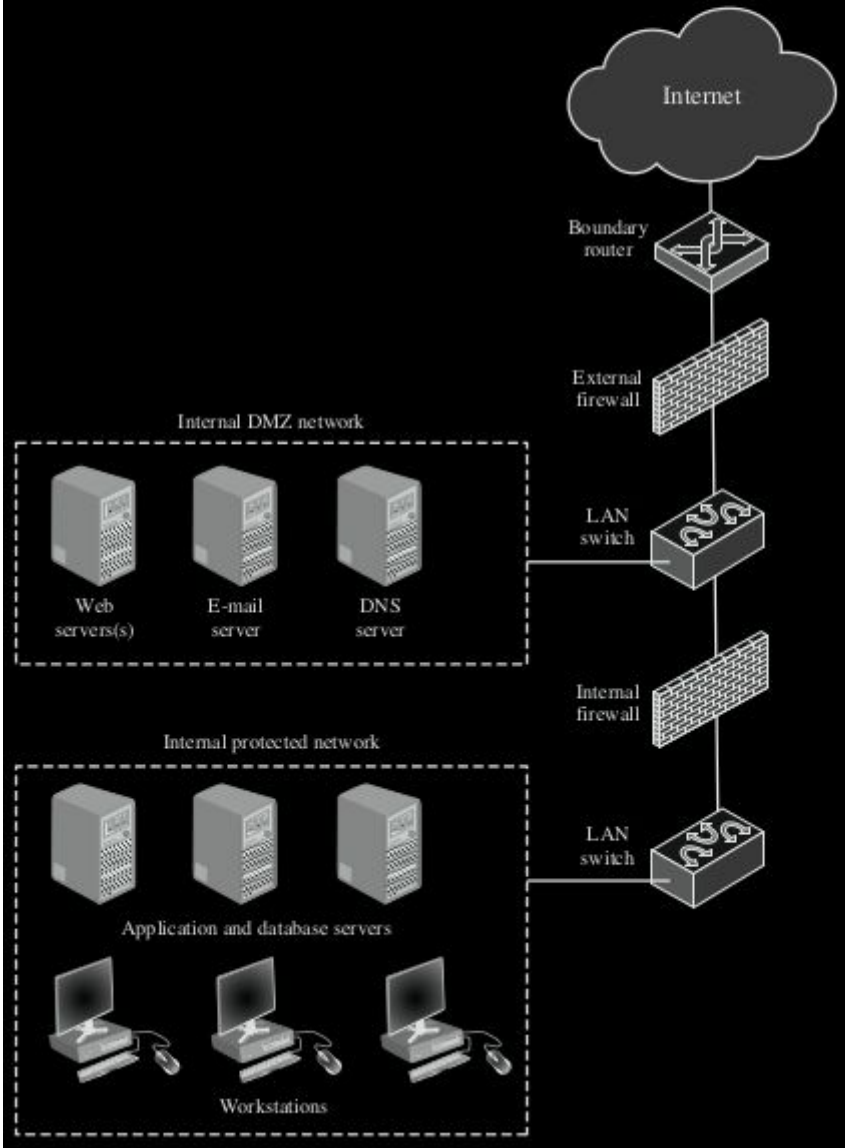


Figure 9.2 **Example Firewall Configuration**

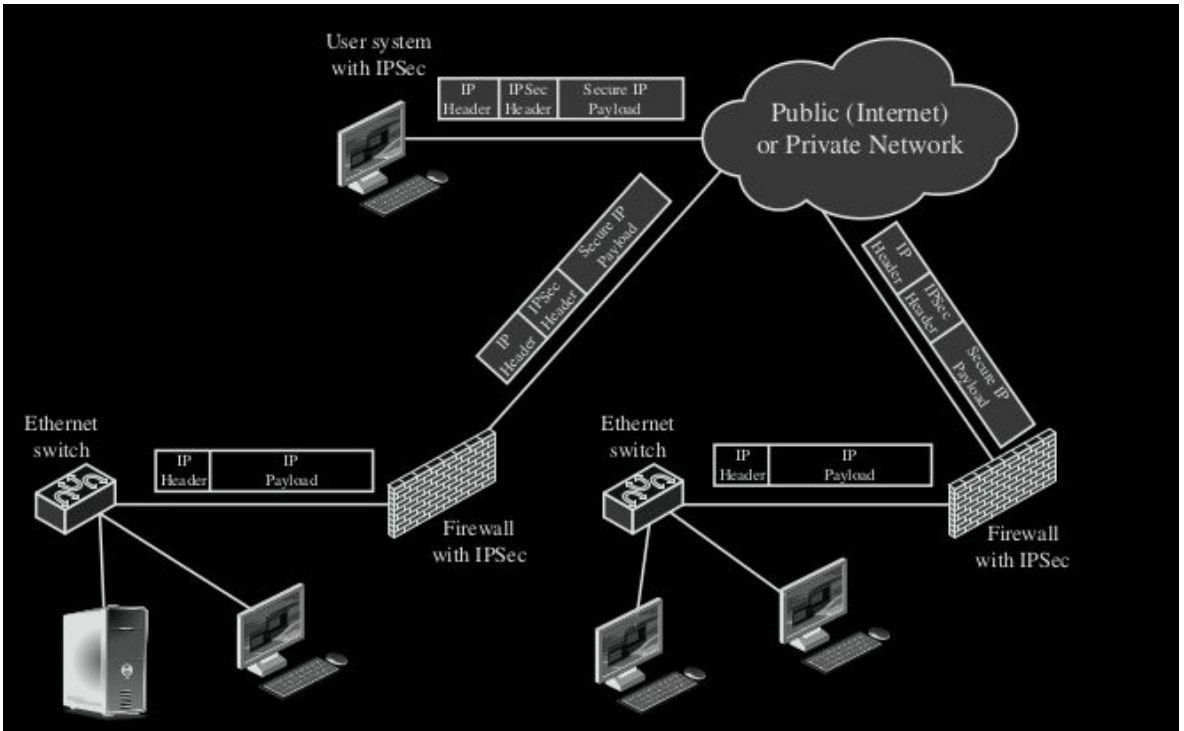


Figure 9.3 **A VPN Security Scenario**

A logical means of implementing an IPSec is in a firewall, as shown in Figure 9.3. If IPSec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted. In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses. IPSec could be implemented in the boundary router, outside the firewall. However, this device is likely to be less secure than the firewall, and thus less desirable as an IPSec platform.

With distributed firewalls, it may make sense to establish both an internal and an external DMZ. Web servers that need less protection because they have less critical information on them could be placed in an external DMZ, outside the external

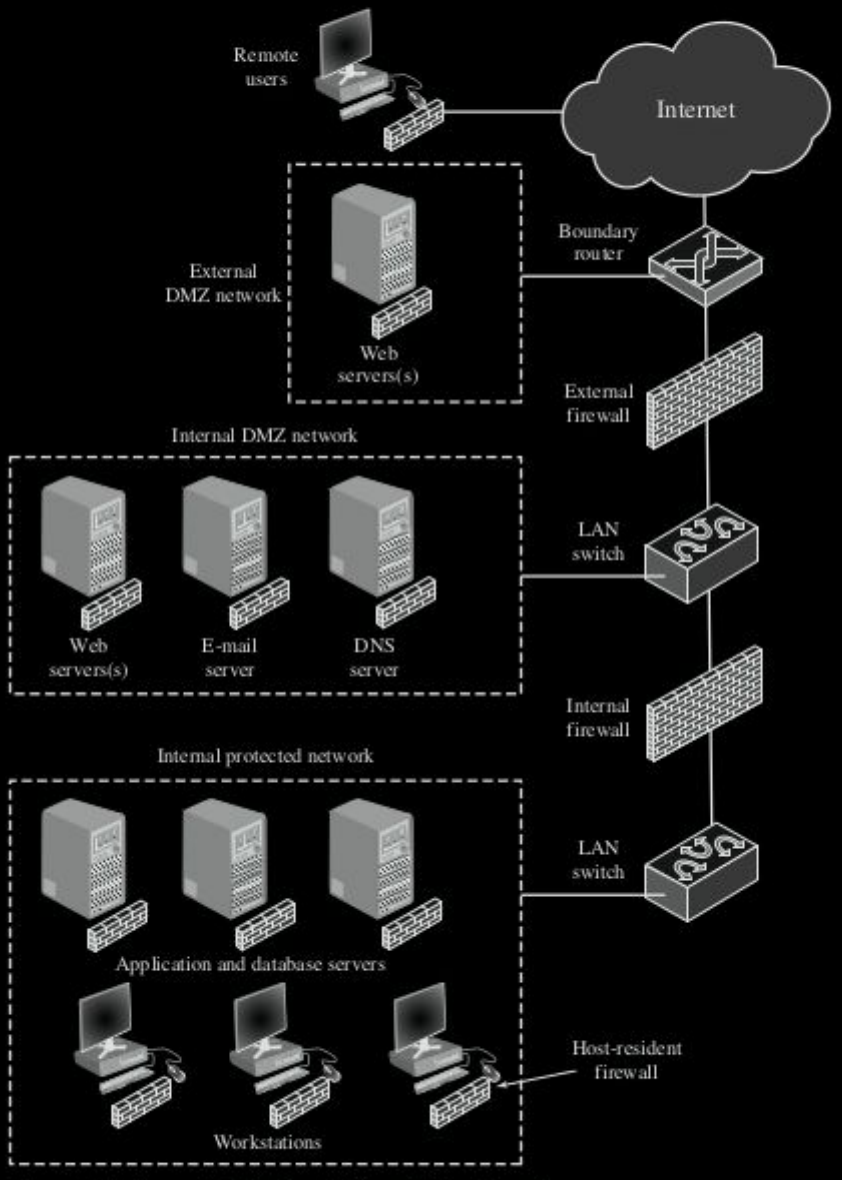
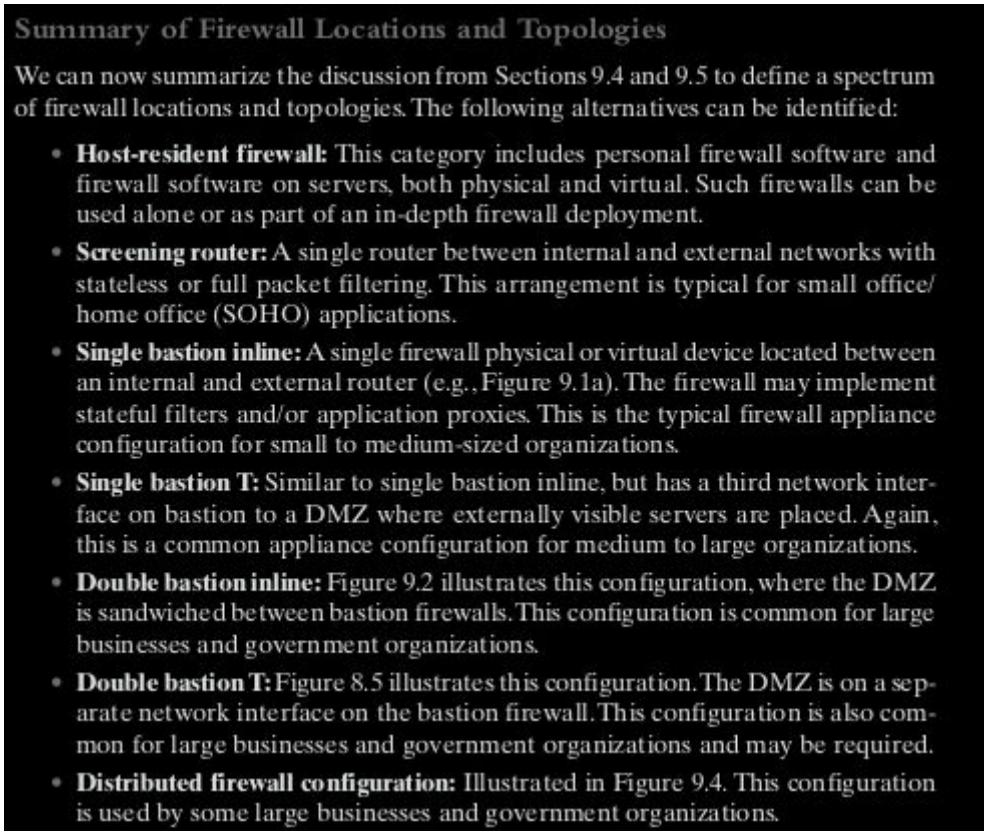


Figure 9.4 **Example Distributed Firewall Configuration**

firewall. What protection is needed is provided by host-based firewalls on these servers.



Summary of Firewall Locations and Topologies

We can now summarize the discussion from Sections 9.4 and 9.5 to define a spectrum of firewall locations and topologies. The following alternatives can be identified:

- **Host-resident firewall:** This category includes personal firewall software and firewall software on servers, both physical and virtual. Such firewalls can be used alone or as part of an in-depth firewall deployment.
- **Screening router:** A single router between internal and external networks with stateless or full packet filtering. This arrangement is typical for small office/home office (SOHO) applications.
- **Single bastion inline:** A single firewall physical or virtual device located between an internal and external router (e.g., Figure 9.1a). The firewall may implement stateful filters and/or application proxies. This is the typical firewall appliance configuration for small to medium-sized organizations.
- **Single bastion T:** Similar to single bastion inline, but has a third network interface on bastion to a DMZ where externally visible servers are placed. Again, this is a common appliance configuration for medium to large organizations.
- **Double bastion inline:** Figure 9.2 illustrates this configuration, where the DMZ is sandwiched between bastion firewalls. This configuration is common for large businesses and government organizations.
- **Double bastion T:** Figure 8.5 illustrates this configuration. The DMZ is on a separate network interface on the bastion firewall. This configuration is also common for large businesses and government organizations and may be required.
- **Distributed firewall configuration:** Illustrated in Figure 9.4. This configuration is used by some large businesses and government organizations.

CLO#5 Distinguish between firewalls and intrusion prevention systems.

Not useful but dece to know….
We have reviewed a number of approaches to countering mali-cious software and network-based attacks, including antivirus and antiworm products,IPS and IDS, and firewalls. The implementation of all of these systems can provide an organization with a defense in depth using multiple layers of filters and defense mechanisms to thwart attacks. The downside of such a piecemeal implementation is the need to configure, deploy, and manage a range of devices and s oftware packages.In addition, deploying a number of devices in sequence can reduce performance.

The market analyst firm IDC refers to such a device as a unified threat management (UTM) system and defines UTM as follows: “Products that include multiple security features integrated into one box. To be included in this category, [an appliance] must be able to perform network firewalling, network intrusion detection and prevention and gateway anti-virus. All of the capabilities in the appliance need not be used concurrently, but the functions must exist inherently in the appliance.”

Figure 9.6 is a typical UTM appliance architecture. The following functions are noteworthy:

1. Inbound traffic is decrypted if necessary before its initial inspection. If the device functions as a VPN boundary node, then IPSec decryption would take place here.

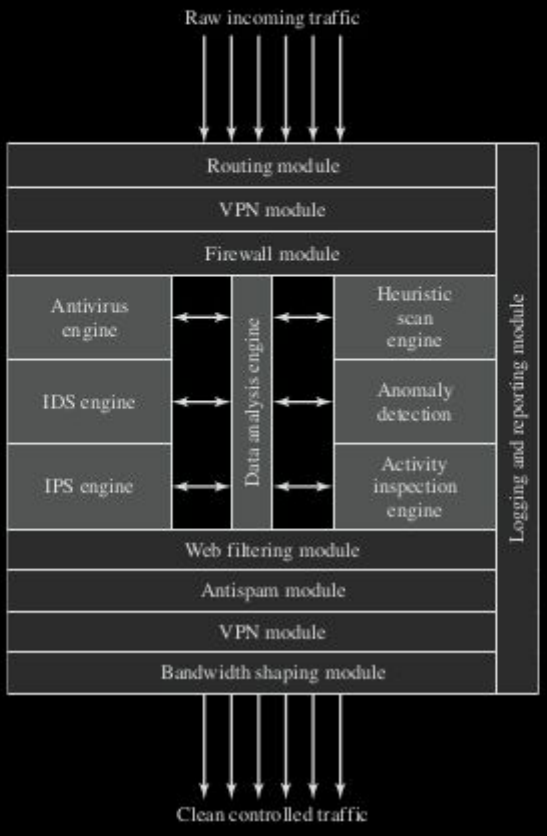


Figure 9.6 **Unified Threat Management Appliance**
Source: Based on [JAME06].

2. An initial firewall module filters traffic, discarding packets that violate rules and/or passing packets that conform to rules set in the firewall policy.
3. Beyond this point, a number of modules process individual packets and flows of packets at various protocols levels. In this particular configuration, a data analysis engine is responsible for keeping track of packet flows and coordinating the work of antivirus, IDS, and IPS engines.
4. The data analysis engine also reassembles multipacket payloads for content analysis by the antivirus engine and the Web filtering and antispam modules.
5. Some incoming traffic may need to be reencrypted to maintain security of the flow within the enterprise network.
6. All detected threats are reported to the logging and reporting module, which is used to issue alerts for specified conditions and for forensic analysis.
7. The bandwidth-shaping module can use various priority and quality-of-service (QoS) algorithms to optimize performance.

As an example of the scope of a UTM appliance, Tables 9.3 and 9.4 list some of the attacks that the UTM device marketed by Secure Computing is designed to counter.

Table 9.3 Sidewinder G2 Security Appliance Attack Protections Summary—Transport-Level Examples

Attacks and Internet Threats		Protections	
TCP			
• Invalid port numbers • Invalid sequence • Numbers • SYN floods • XMAS tree attacks • Invalid CRC values • Zero length • Random data as TCP • Header	• TCP hijack attempts • TCP spoofing attacks • Small PMTU attacks • SYN attack • Script Kiddie attacks • Packet crafting: different TCP options set	• Enforce correct TCP flags • Enforce TCP header length • Ensures a proper three-way handshake • Closes TCP session correctly • 2 sessions one on the inside and one of the outside • Enforce correct TCP flag usage • Manages TCP session timeouts • Blocks SYN attack	• Reassembly of packets ensuring correctness • Properly handles TCP timeouts and retransmits timers • All TCP proxies are protected • Traffic Control through access lists • Drop TCP packets on ports not open • Proxies block packet crafting
UDP			
• Invalid UDP packets • Random UDP data to bypass rules	• Connection pediction • UDP port scanning	• Verify correct UDP packet • Drop UDP packets on ports not open	

Table 9.4 Sidewinder G2 Security Appliance Attack Protections Summary—Application-Level Examples

Attacks and Internet Threats	Protections
DNS	
Incorrect NXDOMAIN responses from AAAA queries could cause denial-of-service conditions.	• Does not allow negative caching • Prevents DNS cache poisoning
ISC BIND 9 before 9.2.1 allows remote attackers to cause a denial of service (shutdown) via a malformed DNS packet that triggers an error condition that is not properly handled when the rdataset parameter to the dns_message_findtype() function in message.c is not NULL.	• Sidewinder G2 prevents malicious use of improperly formed DNS messages to affect firewall operations. • Prevents DNS query attacks • Prevents DNS answer attacks
DNS information prevention and other DNS abuses.	• Prevent zone transfers and queries • True split DNS protect by Type Enforcement technology to allow public and private DNS zones. • Ability to turn off recursion
FTP	
• FTP bounce attack • PASS attack • FTP Port injection attacks • TCP segmentation attack	• Sidewinder G2 has the ability to filter FTP commands to prevent these attacks • True network separation prevents segmentation attacks.
SQL	
SQL Net man in the middle attacks	• Smart proxy protected by Type Enforcement technology • Hide Internal DB through nontransparent connections.
Real-Time Streaming Protocol (RTSP)	
• Buffer overflow • Denial of service	• Smart proxy protected by Type Enforcement technology • Protocol validation • Denies multicast traffic • Checks setup and teardown methods • Verifies PNG and RTSP protocol and discards all others • Auxiliary port monitoring
SNMP	
• SNMP flood attacks • Default community attack • Brute force attack • SNMP put attack	• Filter SNMP version traffic 1, 2c • Filter Read, Write, and Notify messages • Filter OIDS • Filter PDU (Protocol Data Unit)
SSH	
• Challenge Response buffer overflows • SSHD allows users to override "Allowed Authentications" • OpenSSH buffer_append_space buffer overflow • OpenSSH/PAM challenge Response buffer overflow • OpenSSH channel code offer-by-one	Sidewinder G2 v6.x's embedded Type Enforcement technology strictly limits the capabilities of Secure Computing's modified versions of the OpenSSH daemon code.

(Continued)

Table 9.4 *(Continued)*

Attacks and Internet Threats	Protections
SMTP	
• Sendmail buffer overflows • Sendmail denial of service attacks • Remote buffer overflow in sendmail • Sendmail address parsing buffer overflow • SMTP protocol anomalies	• Split Sendmail architecture protected by Type Enforcement technology • Sendmail customized for controls • Prevents buffer overflows through Type Enforcement technology • Sendmail checks SMTP protocol anomalies
• SMTP worm attacks • SMTP mail flooding • Relay attacks • Viruses, Trojans, worms • E-mail addressing spoofing • MIME attacks • Phishing e-mails	• Protocol validation • Antispam filter • Mail filters—size, keyword • Signature antivirus • Antirelay • MIME/Antivirus filter • Firewall antivirus • Antiphishing through virus scanning
Spyware Applications	
• Adware used for collecting information for marketing purposes • Stalking horses • Trojan horses • Malware • Backdoor Santas	• SmartFilter® URL filtering capability built in with Sidewinder G2 can be configured to filter Spyware URLs, preventing downloads.

Ch12. OS Security

- 12.1. Introduction to OS security
- 12.2. System Security Planning
- 12.3. OS hardening
- 12.4. Application Security
- 12.5. Security Maintenance
- 12.6. Linux/Unix Security
- 12.7. Windows Security
- 12.8. Virtualization Security

CLOs

1) List the steps needed in the process of securing a system.
2) Detail the need for planning system security.
3) List the basic steps used to secure the based operating system
4) List the additional steps needed to sure key applications.
5) List steps needed to maintain security.
6) List some specific aspects of securing UNIX/Linux systems.
7) List some specific aspects of securing Windows systems.
8) List steps needed to maintain security in virtualized systems.

CLO#2 Detail the need for planning system security.
CLO#3 List the basic steps used to secure the based operating system
CLO#4 List the additional steps needed to sure key applications.
CLO#5 List steps needed to maintain security.

CLO#6 List some specific aspects of securing UNIX/Linux systems.
CLO#7 List some specific aspects of securing Windows systems.
CLO#8 List steps needed to maintain security in virtualized systems.

Ch13. Cloud and IoT Security
- 13.1. Cloud Computing
- 13.2. Cloud Security Concepts
- 13.3. Cloud Security Approaches
- 13.4. The Internet of Things
- 13.5. IoT security

CLOs
1)

Ch14. Section 14.3 ⇒ Security Risk Assessment

Ch4. Discretionary Access Control
- 4.1. Unix Access control

Ch18. Security Auditing
- 18.1. Security Auditing Architecture
- 18.2. Security Audit Trail
- 18.3. Implementing the Logging function
- 18.4. Audit Trail Analysis
- 18.5. Security Information and Event Management

Ch25. Linux Security

Ch27.1 The Bell-Lapdulla Model for Computer Security

TCP/IP Headers (Appendix F/slides).
Ch1 Overview (Chapter 1).
Ch2 Cryptographic Tools (Chapter 2).

Ch3	Password-based Authentication (Section 3.2)