CSIT985
Strategic Network Design

Autumn 2024 (JI Wuhan)

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Lecture 8:

Security and Privacy Architecture

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

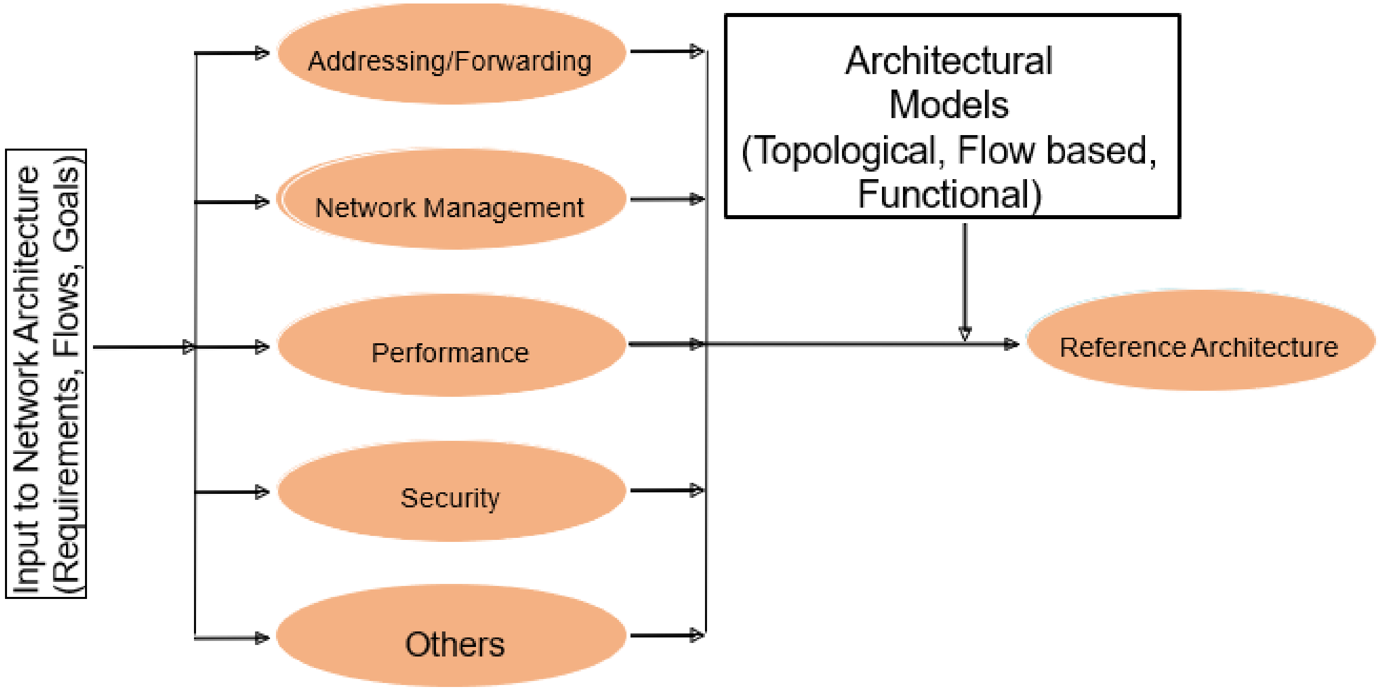
Presented by: Shengbing Tang

Lecturer, CCNU-UOW Joint Institute

Overview

- ❖ Basic Concepts and Mechanisms of Security
- ❖ Three classic security considerations
- ❖ What does it cover?
- ❖ Developing a Security and Privacy Plan
- ❖ Security and Privacy Administration
- ❖ Policies and Procedures
- ❖ Policies Areas
- ❖ Security and Privacy Mechanisms
- ❖ Architectural Considerations

Reminder: Process Model for Component Architecture Approach



Input to Network Architecture (Requirements, Flows, Goals)

Addressing/Forwarding

Network Management

Performance

Security

Others

Architectural Models (Topological, Flow based, Functional)

Reference Architecture

Component Architectures (Based on Network Functions)

(McCabe, 2010, p.227)

Basic Concepts and Mechanisms of Security

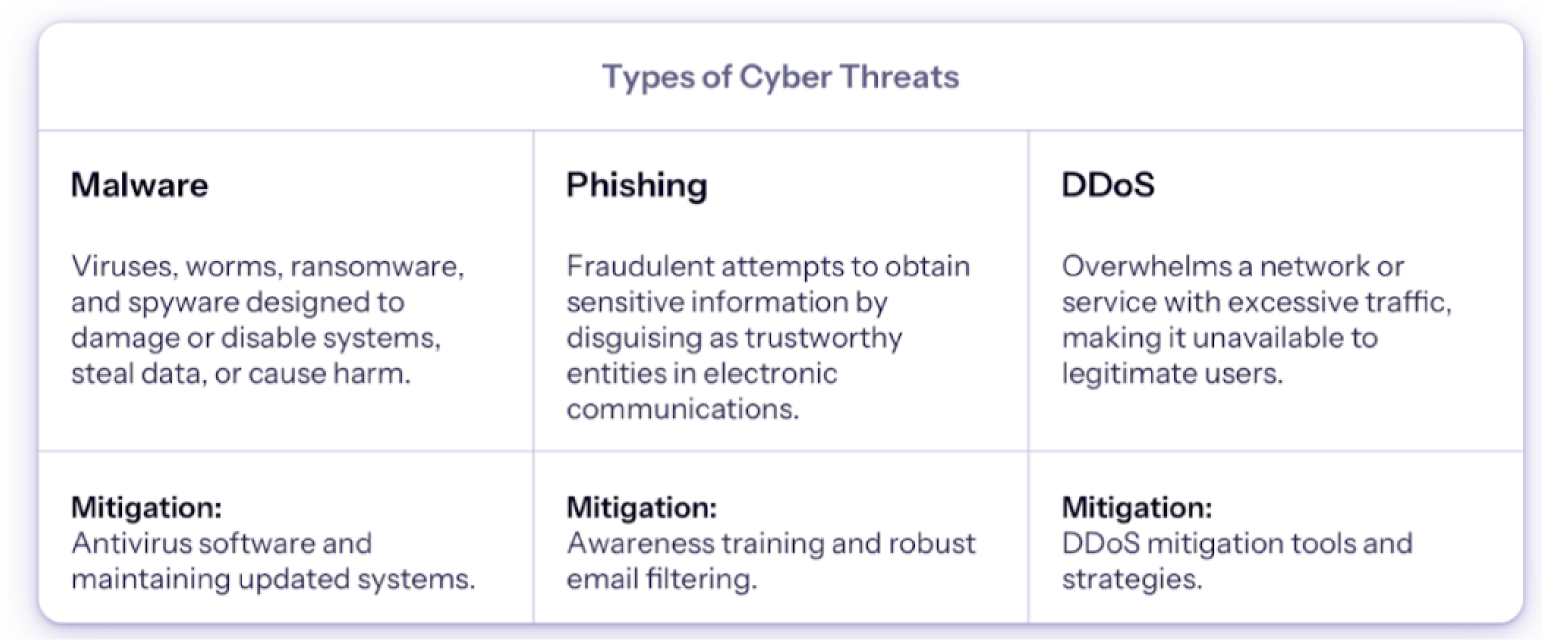
- Network Security
  - □ A rather broad term that essentially focuses on the measures that protect computer networks against unauthorized access and potential misuse, malfunction, modification, destruction, or improper disclosure of network resources.
  - □ The goal is to create a secure environment where users can access and transmit information safely.

Basic Concepts and Mechanisms of Security

- Network Security
  - The protection of networks and their services from unauthorized
    - Modification
    - Destruction
    - Access (this includes privacy)
    - Disclosure (this includes privacy)

Basic Concepts and Mechanisms of Security

- Network Security: mitigating threats and vulnerabilities



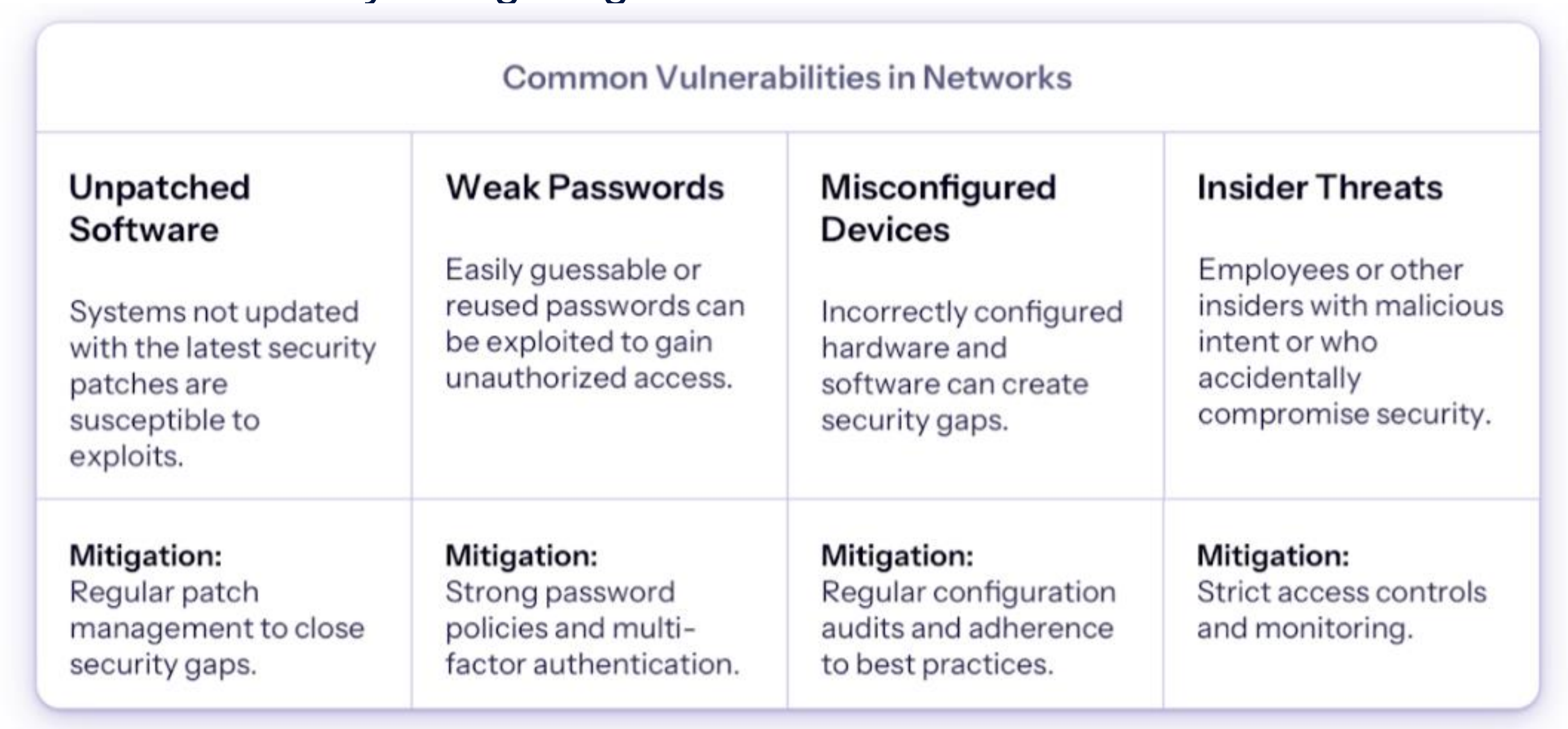
Types of Cyber Threats

Malware	Phishing	DDoS
Viruses, worms, ransomware, and spyware designed to damage or disable systems, steal data, or cause harm.	Fraudulent attempts to obtain sensitive information by disguising as trustworthy entities in electronic communications.	Overwhelms a network or service with excessive traffic, making it unavailable to legitimate users.
Mitigation: Antivirus software and maintaining updated systems.	**Mitigation:** Awareness training and robust email filtering.	**Mitigation:** DDoS mitigation tools and strategies.

DDoS: Distributed Denial of Service

Basic Concepts and Mechanisms of Security

- Network Security: mitigating threats and vulnerabilities

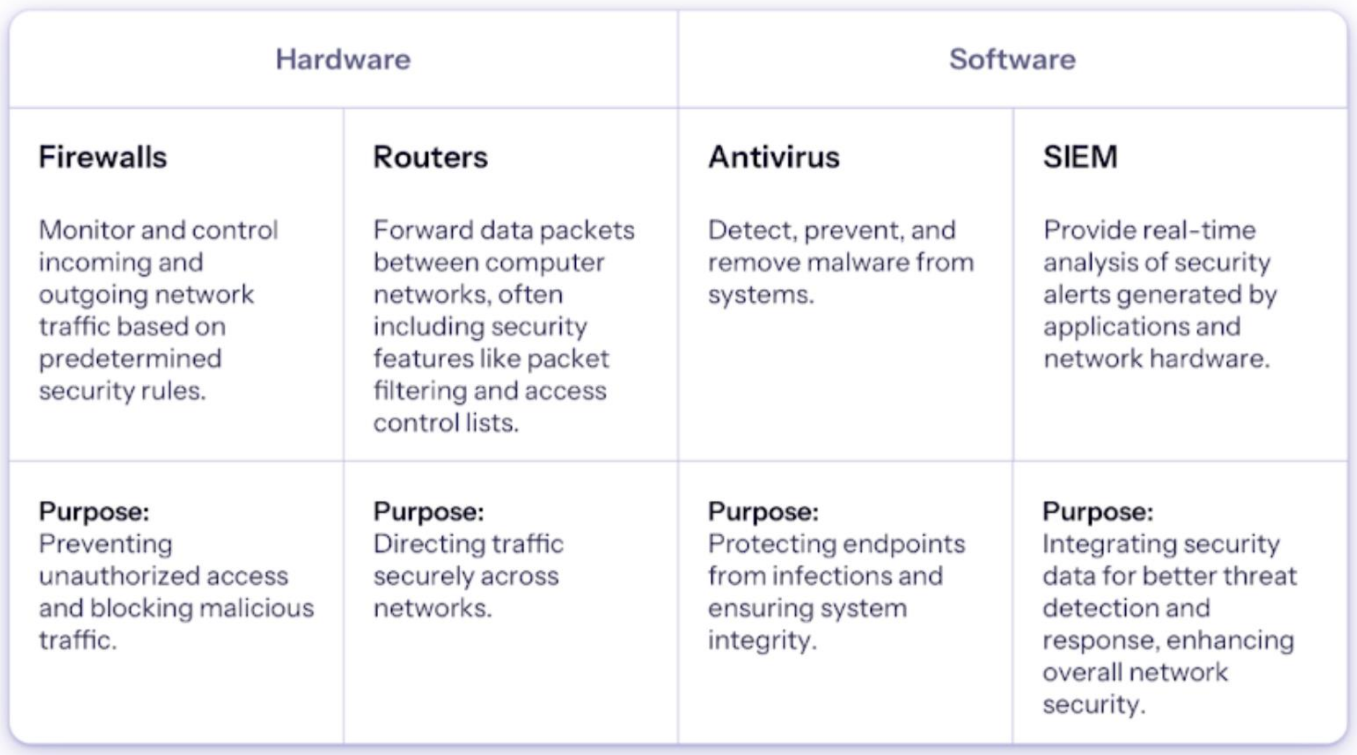


Common Vulnerabilities in Networks

Unpatched Software	**Weak Passwords**	**Misconfigured Devices**	**Insider Threats**
Systems not updated with the latest security patches are susceptible to exploits.	Easily guessable or reused passwords can be exploited to gain unauthorized access.	Incorrectly configured hardware and software can create security gaps.	Employees or other insiders with malicious intent or who accidentally compromise security.
Mitigation: Regular patch management to close security gaps.	**Mitigation:** Strong password policies and multi-factor authentication.	**Mitigation:** Regular configuration audits and adherence to best practices.	**Mitigation:** Strict access controls and monitoring.

Basic Concepts and Mechanisms of Security

- Network Security: components of network security



Hardware		Software	
Firewalls Monitor and control incoming and outgoing network traffic based on predetermined security rules.	**Routers** Forward data packets between computer networks, often including security features like packet filtering and access control lists.	**Antivirus** Detect, prevent, and remove malware from systems.	**SIEM** Provide real-time analysis of security alerts generated by applications and network hardware.
Purpose: Preventing unauthorized access and blocking malicious traffic.	**Purpose:** Directing traffic securely across networks.	**Purpose:** Protecting endpoints from infections and ensuring system integrity.	**Purpose:** Integrating security data for better threat detection and response, enhancing overall network security.

SIEM: Security Information And Event Management

Basic Concepts and Mechanisms of Security

Essential network security strategies

① Firewalls

- Firewalls are security devices or software that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between trusted and untrusted networks, blocking unauthorized access while permitting legitimate communication.
- Depending on the use case, there are several different types of firewalls.

Basic Concepts and Mechanisms of Security

Essential network security strategies

Most commo types of firewalls

- **Stateful firewalls** track the state of active connections and make decisions based on the context of the traffic. By understanding the state of network connections, they offer a more sophisticated level of security than stateless firewalls.
- **Stateless firewalls** filter packets based solely on predefined rules such as IP addresses and port numbers without considering the state of the traffic. They are simpler and faster but less secure compared to stateful firewalls.
- **Next-generation firewalls (NGFWs)** combine traditional firewall capabilities with additional features like Deep Packet Inspection (DPI), Intrusion Detection and Prevention Systems (IDPS), and application awareness. NGFWs provide advanced threat detection and protection.

Basic Concepts and Mechanisms of Security

Essential network security strategies

② Intrusion Detection and Prevention Systems

- Intrusion Detection and Prevention Systems (IDPS) identify and respond to potential threats within a network and are an important part of any network security strategy. They monitor network traffic for suspicious activity, alert administrators, and block or mitigate identified threats.
- IDPS enhances the overall security posture by detecting anomalies and preventing unauthorized access or malicious activities.

Basic Concepts and Mechanisms of Security

Essential network security strategies

③ Virtual Private Networks

- Virtual Private Networks (VPNs) encrypt data transmitted between remote users and a corporate network to provide secure communication channels over public networks.
- VPNs help keep sensitive information confidential and protected from eavesdropping or interception, making them essential for secure remote access.
- VPNs can also be used for access control, granting users access to certain resources based on their credentials.

Basic Concepts and Mechanisms of Security

Essential network security strategies

④ Encryption

- Encryption is the process of converting data into a coded format to prevent unauthorized access. It is vital for protecting data as they move through the network (in transit) as well as data that remain stored on devices or servers (at rest).

- Encryption ensures that even if data is intercepted or accessed by unauthorized parties, it remains unreadable and secure. Implementing strong encryption protocols is a fundamental aspect of network security to safeguard sensitive information from cyber threats.

Basic Concepts and Mechanisms of Security

Best practices of network security

① **Regular updates and patching**: regularly updating and patching software, firmware, and operating systems is crucial to mitigate vulnerabilities that could be exploited by attackers. Software vulnerabilities are discovered and disclosed frequently, and updates address these vulnerabilities to strengthen the network’s defenses.

② **Continuous monitoring and incident response**: actively monitoring the network for unusual activities or potential security breaches and designing comprehensive incident response plans are essential for promptly addressing and mitigating security incidents. Early detection and rapid response can significantly minimize the impact of security breaches and prevent further damage.

Basic Concepts and Mechanisms of Security

Best practices of network security

③ **Data backup and recovery plans:** implementing regular backups of critical data ensures that data can be restored in the event of a security breach, data loss, or ransomware attack, protects against data loss, and minimizes downtime.

④ **Employee training and awareness:** one of the most basic yet fundamental network security practices is educating employees about cybersecurity risks, safe practices, and policies. Proper security training helps reduce human errors that could compromise network security, as employees are often targets for phishing attacks and social engineering.

Basic Concepts and Mechanisms of Security

- Network Privacy
  - A subset of network security
  - Focus on protection from unauthorized access and disclosure

Three Classic Security Considerations

- CIA triangle
  - Confidentiality
  - Integrity
  - Availability of resources and data

Three Classic Security Considerations

- CIA triangle
  - Confidentiality ensures that only the sender and targeted receiver can access to the exchanged messages
  - Related to *secure communication*

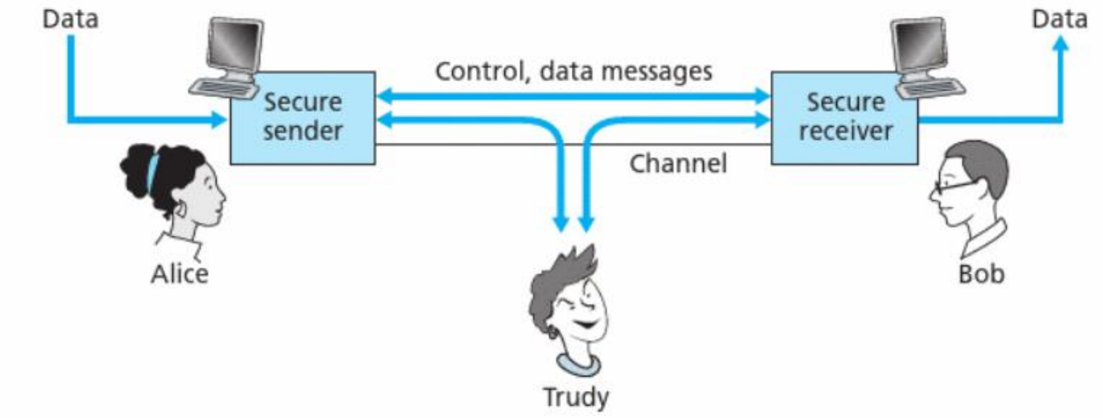


Figure. Sender, Receiver and intruder (Kurose, 2017, p.623)

Three Classic Security Considerations

- CIA triangle
  - Integrity: make sure that the message exchanged between Alice and Bob are not altered in transit.
  - Encryption/decryption techniques

(Kurose, 2017, p.622)

Three Classic Security Considerations

- CIA triangle
  - Availability: make sure that data are available when required
  - E.g. attacks as SYN flood, Denial of Service (DoS) or physical attacks

A SYN flood (half-open attack) is a type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources. By repeatedly sending initial connection request (SYN) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all.

What does it cover?

- A combination of
  - Understanding what security means to all network components
  - Planning and implementation of security policies and mechanisms

What does it cover?

- Must cover
  - Devices
  - Servers
  - Users
  - System data
  - Image and privacy of users and organization

Developing a Security and Privacy Plan

- As always
  - Avoid implementing security mechanisms just because they are interesting or new or because everybody else does it
  - Start simple – work towards a more complex architecture when warranted

Developing a Security and Privacy Plan

- The requirement phase should identify the followings:
  - Which resources need to be protected?
  - What problems (threats) are we protecting against
  - The likelihood of each problem (threat)
- Review and update periodically
- Bear in mind that groups (FAs) have different security needs – hence segmentation of the network is useful

Security and Privacy Administration

Threat analysis

Policies & Procedures

Security and Privacy Administration

- Threat analysis
  - Identifies
    - Assets to be protected
    - Types of security risks (threats) they need to be protected from

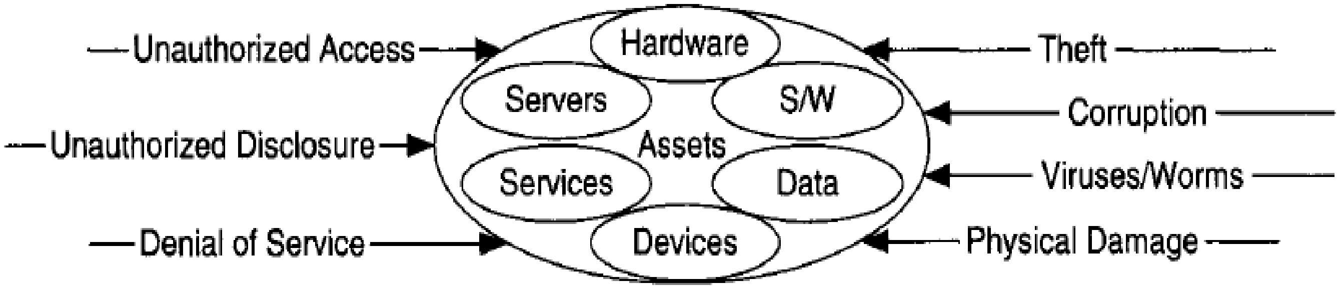


Figure. Potential Assets and Threats to Be Analyzed (McCabe, 2010, p.263)

Security and Privacy Administration

- Threat analysis
  - Assets may include
    - User hardware
    - Servers
    - Specialized devices
    - Network devices
    - Software
    - Services
    - Data

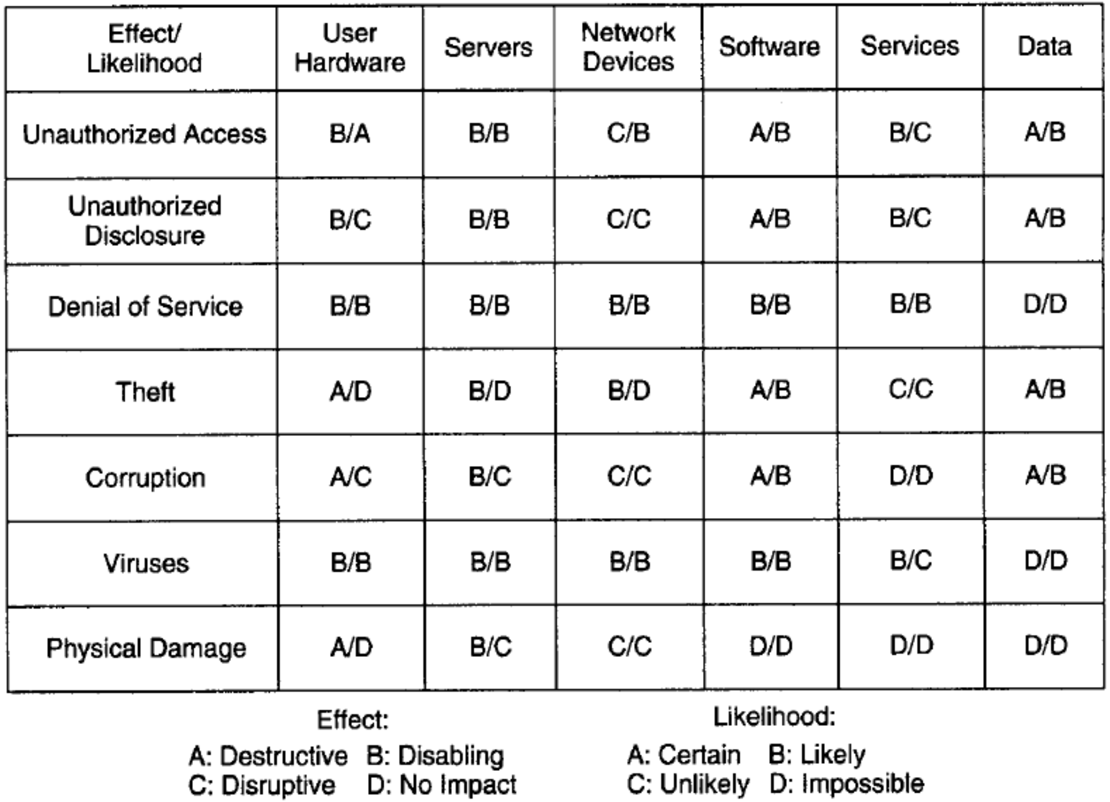
Security and Privacy Administration

- Threats may include
  - Unauthorized access to data, services, software and/or hardware
  - Unauthorized disclosure of information
  - Denial of service (DoS)
  - Theft of data, services, software and/or hardware
  - Corruption of data, services, software and/or hardware
  - Viruses, worms, Trojan horses
  - Physical damage

Security and Privacy Plan

- Gathering of security and privacy data
    - List the threats and assets via threat analysis worksheet (Figure below)
    - Results are determined during requirements analysis process
    - Combine with list of current threats
    - Threat analysis is subjective
        - Reduce subjectivity by involving various groups within the organization
    - Repeat periodically
        - As organization grows degree and types of threats will change

Security and Privacy Plan – Example Result



Effect/ Likelihood	User Hardware	Servers	Network Devices	Software	Services	Data
Unauthorized Access	B/A	B/B	C/B	A/B	B/C	A/B
Unauthorized Disclosure	B/C	B/B	C/C	A/B	B/C	A/B
Denial of Service	B/B	B/B	B/B	B/B	B/B	D/D
Theft	A/D	B/D	B/D	A/B	C/C	A/B
Corruption	A/C	B/C	C/C	A/B	D/D	A/B
Viruses	B/B	B/B	B/B	B/B	B/C	D/D
Physical Damage	A/D	B/C	C/C	D/D	D/D	D/D

Effect:
A: Destructive B: Disabling
C: Disruptive D: No Impact

Likelihood:
A: Certain B: Likely
C: Unlikely D: Impossible

Figure. An Example of Threat Analysis Worksheet for a Specific Organization (McCabe, 2010, p.364)

Security and Privacy Plan – Assessing Risk

- For each threat to each service (threat analysis sheet), we must identify:
  1. Probability of any threat
  2. Cost or damage involved

- The cost or damage will depend to some extent on the goals of the network

- If the probability and cost are high, we MUST develop a strategy to negate/reduce the risk to acceptable levels

Policies and Procedures

- Trade-offs are necessary when developing policies and procedures
- Security can be double-edged sword
- Don’t confuse security with excessive control over users and their actions
  - This can occur when rules, regulations and security guardians are placed above organizational goals and work

Policies and Procedures

- Security policies and procedures are formal statements on rules for system, network and information access and use
  - They define how the system can be used with minimal risk exposure
  - Clarify to users
    1. What the threats are
    2. What can be done to reduce them
    3. Consequences of NOT helping to reduce them

Policies and Procedures

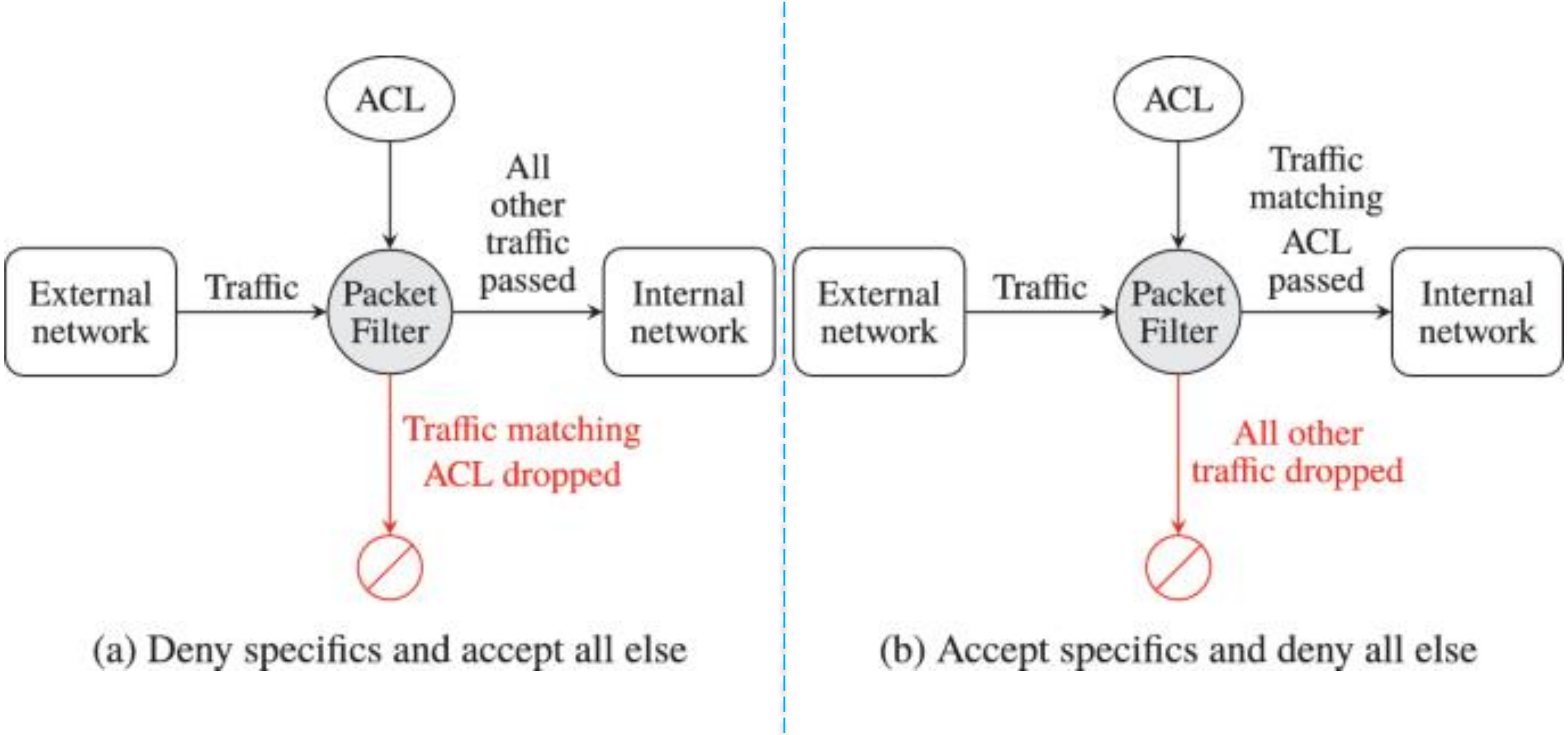

ACL
All other traffic passed
External network
Traffic
Packet Filter
Internal network
Traffic matching ACL dropped
(a) Deny specifics and accept all else
ACL
Traffic matching ACL passed
External network
Traffic
Packet Filter
Internal network
All other traffic dropped
(b) Accept specifics and deny all else

Figure. An example of security philosophies

Policies and Procedures

- Should include
  - Privacy statements
    - Monitoring, logging and access
  - Accountability statements
    - Responsibilities and auditing
  - Authentication statements
    - Password policies and remote access
  - Reporting violations
    - Contact information and procedure

Policies and Procedures

- Examples
  - Acceptable use statements
  - Security incident handling procedures
  - Configuration modification policies
  - Network access control lists
- Should describe how and why

Policies Areas

- User access to the System
  - Authorization to use
  - Authentication of identify and use of passwords
  - Training and acceptance of responsibility for compliance
  - Expectations of right to privacy
- Administrator skills and requirements for Certification
  - Superusers and administrators

Policies Areas

Password Authentication

- Falls into the “something you know” category
- Is the most common form of authentication

https://www.logintc.com/types-of-authentication/password-authentication/

Policies Areas

Password Authentication: what is username and password authentication?

- □ Authentication is the process of who the user claims to be. There are three factors of authentication:
  1. **Something you know** – such as a password, PIN, personal.
  2. **Something you have** – a physical item, such as a cellphone or card.
  3. **Something you are** – biometric data such as fingerprint or facial recognition.
- □ Every time you have signed up for a website, you have been asked to create a username and password. This has become almost second nature for some users to set up their accounts without much thought about the credentials they choose.

Policies Areas

Password Authentication: How to Implement password authentication?

① Registering with username and password
② Enforcing password rules
③ Storing the users credentials
④ Handling Returning Users

Policies Areas

Password Authentication Vulnerabilities

User Generated Credentials: users create a password that’s easy to remember but aren’t up to date on password security best practices, or subconsciously use patterns to generate their passwords.

Brute Force Attacks: a brute force attack occurs when a computer program runs through every password combination until they find a match. The system will run through all one-digit combinations, two-digit combinations, and so forth until your password is finally cracked. Some programs will specifically focus on combing through the most commonly used dictionary words, while other programs will target popular passwords against a list of possible usernames.

Policies Areas

How are Passwords Stored?

When a user creates a password, a copy of that credential is stored by the system or website in a secure password database against which the server can compare any further login attempts. Since all those passwords are stored in a centralized location, it’s important that password-based authentication systems ensure **top-notch security** for those databases.

Typically, passwords are stored in an **encrypted** fashion so that even if a hacker is able to access the database, the information they see would be of no use to them.

Policies Areas

- System configuration and management
  - Maintenance
  - Virus/Trojan protection
  - Patching operating systems and applications
  - Monitoring CERT advisories
  - Who can and cannot connect devices to the network
  - What data gets back up
  - What data get stored offsite
  - Contingency computing plans

Security and Privacy Mechanisms

- Physical security and awareness
- Protocol and application security
- Encryption/decryption
- Network perimeter security
- Remote access security

Physical Security

- Access controlled rooms for servers and specialized devices
- Back-up power sources and power conditioning
- Off-site storage and archival
- Alarm systems

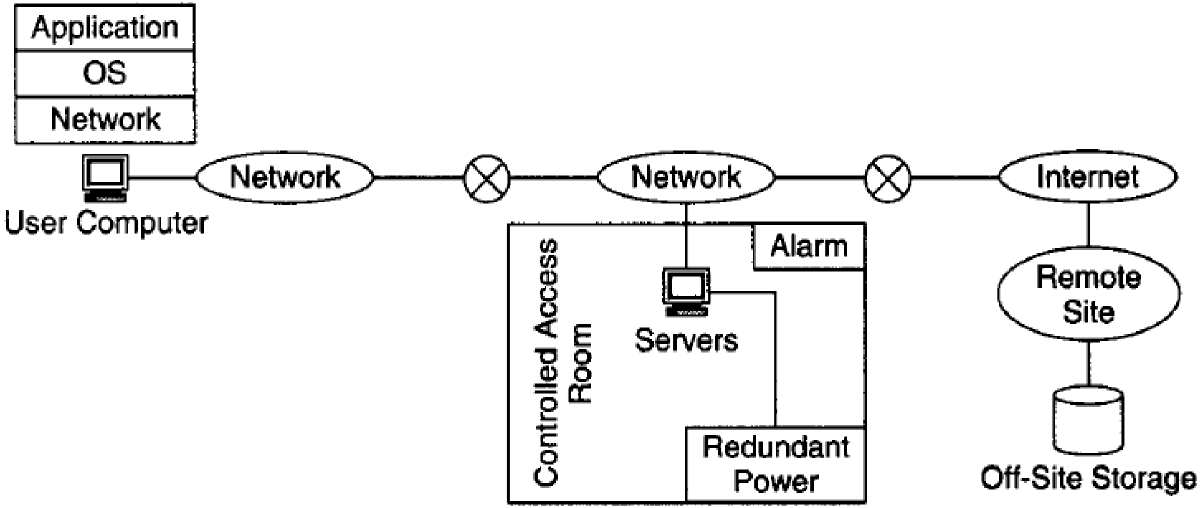


Figure. Areas of Physical Security (McCabe, 2010, p.368)

Physical Security

- **Back-up power sources: UPS (Uninterruptible Power Supplies)**

□ A type of continual power system that provides automated backup electric power to a load when the input power source or mains power fails.

□ A UPS differs from a traditional auxiliary/emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions by switching to energy stored in battery packs, supercapacitors or flywheels.

□ The on-battery run-times of most UPSs are relatively short (only a few minutes) but sufficient to "buy time" for initiating a standby power source or properly shutting down the protected equipment.

□ A UPS is typically used to protect hardware such as computers, hospital equipment, data centers, telecommunications equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption or data loss.

Physical Security

- Natural disasters need to be considered
  - Fire – sprinkler – Water – pumping, elevation
  - Wind (hurricane proof buildings)
  - Dust and heat (air-conditioning)
- User awareness – information push and information pull

Protocol & Application Security

IPSec

- □ Protocol for providing authentication and encryption/decryption between devices at the Network Layer
- □ A set of communication rules or protocols for setting up secure connections over a network.
- □ IPSec adds encryption and authentication to make the protocol more secure

Protocol & Application Security

IPsec can be used to do the following:

□ Provide router security when sending data across the public internet.

□ Encrypt application data.

□ Authenticate data quickly if the data originates from a known sender.

□ Protect network data by setting up encrypted circuits, called IPsec tunnels, that encrypt all data sent between two endpoints.

Protocol & Application Security

How does IPSec work?

Computers exchange data with the IPSec protocol through the following steps:

① The sender computer determines if the data transmission requires IPSec protection by verifying against its security policy. If it does, the computer initiates secure IPSec transmission with the recipient computer.

② Both computers negotiate the requirements to establish a secure connection. This includes mutually agreeing on the encryption, authentication, and other security association (SA) parameters.

③ The computer sends and receives encrypted data, validating that it came from trusted sources. It performs checks to ensure the underlying content is reliable.

④ Once the transmission is complete or the session has timed out, the computer ends the IPSec connection.

Protocol & Application Security

What are the IPSec protocols?

It consists of a header, payload, and trailer.

① A header is a preceding section that contains instructional information for routing the data packet to the correct destination.

② Payload is a term that describes the actual information contained within a data packet.

③ The trailer is additional data appended to the tail of the payload to indicate the end of the data packet.

Protocol & Application Security

What are IPSec modes?

IPSec operates in two different modes with different degrees of protection.

① **Tunnel:** The IPSec tunnel mode is suitable for transferring data on public networks as it enhances data protection from unauthorized parties. The computer **encrypts all data**, including the payload and header, and appends a new header to it.

② **Transport:** IPSec transport mode **encrypts only the data packet's payload and leaves the IP header in its original form**. The unencrypted packet header allows routers to identify the destination address of each data packet. Therefore, IPSec transport is used in a close and trusted network, such as securing a direct connection between two computers.

Protocol & Application Security

- IPSec tunnel mode

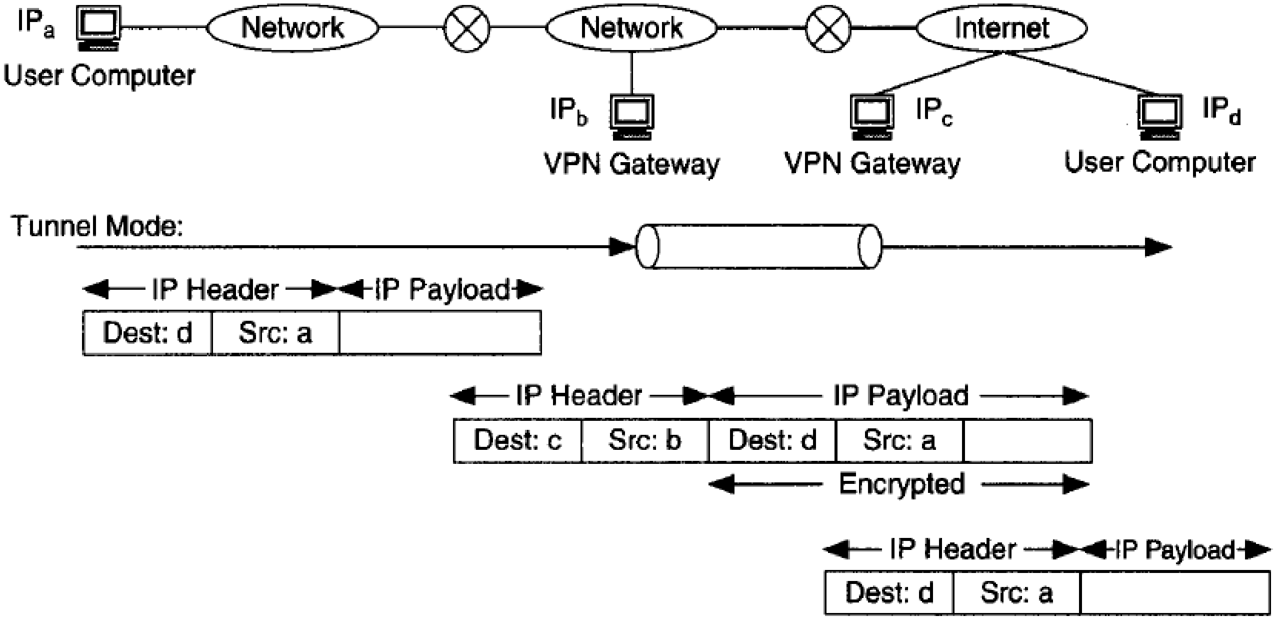


Figure. The Tunnel Mode of IPSec (McCabe, 2010, p.370)

Protocol & Application Security

IPSec transport mode

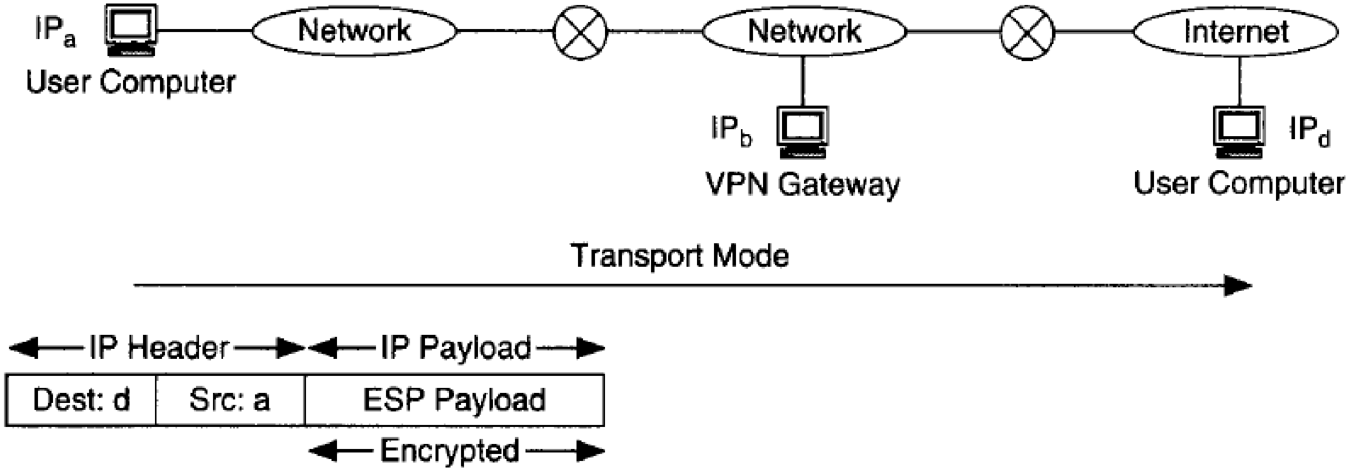


Figure. The Transport Mode of IPSec (McCabe, 2010, p.369)

Protocol & Application Security

Simple Network Management Protocol Version 3 (SNMPv3)

- □ An advanced version of SNMP.
- □ Primarily used for network management, SNMPv3 ensures secure access to devices by providing enhanced security features.
- □ Unlike its predecessors, SNMPv3 supports strong authentication and encryption, making it a go-to choice for managing complex network environments securely.
- □ SNMPv3 is crucial in contemporary network management for its ability to provide secure and reliable data about network devices.
- □ Its enhanced security features make it well-suited for modern, sensitive environments where data integrity and privacy are paramount.

Protocol & Application Security

- SNMPv3 – USM (User-based Security Model)
  - Protects against
    - The modification of information,
    - Masquerades,
    - Disclosure (eaves dropping)
    - Message stream modification

Protocol & Application Security

- **Packet filtering** – explicitly denies or permits packets access on the basic of **IP addresses or port numbers** (services)

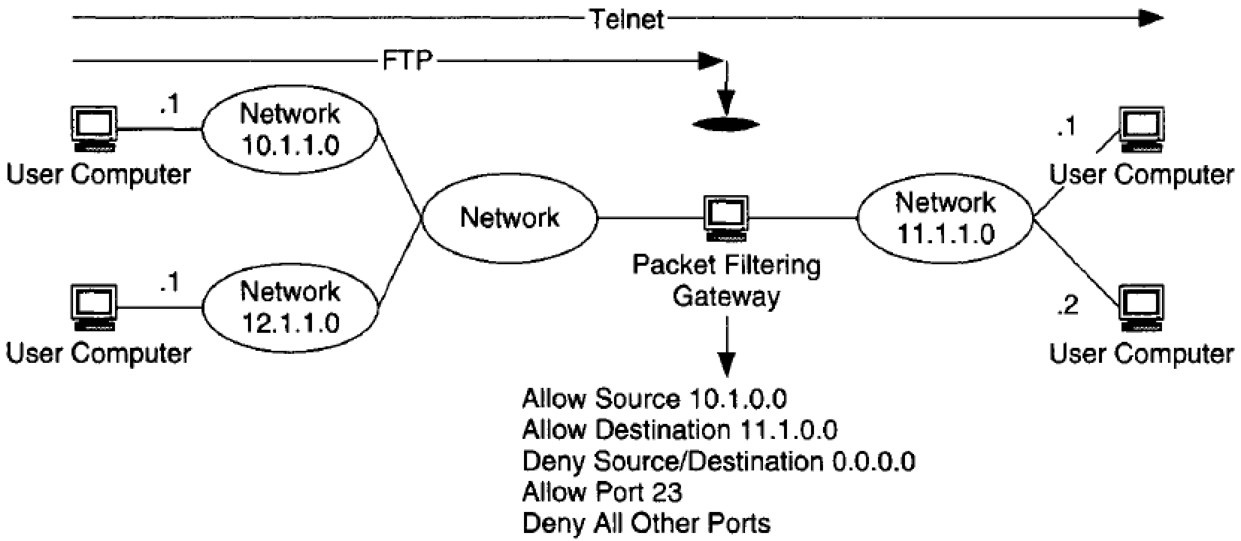


Figure. An Example of Packet Filtering (McCabe, 2010, p.371)

Encryption/decryption

- Encryption/decryption (E/D) prevents information being usable to attacker
- Two main types:
  - Private key
    - E.g. DES (data encryption standard), triple DES, etc.
  - Public key infrastructure (PKI)

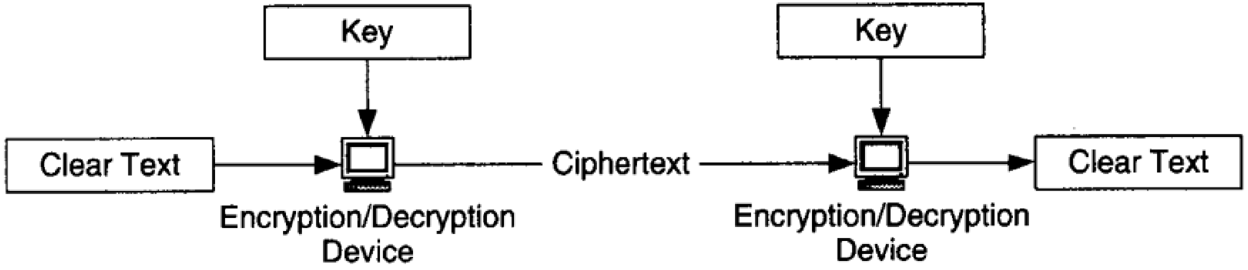
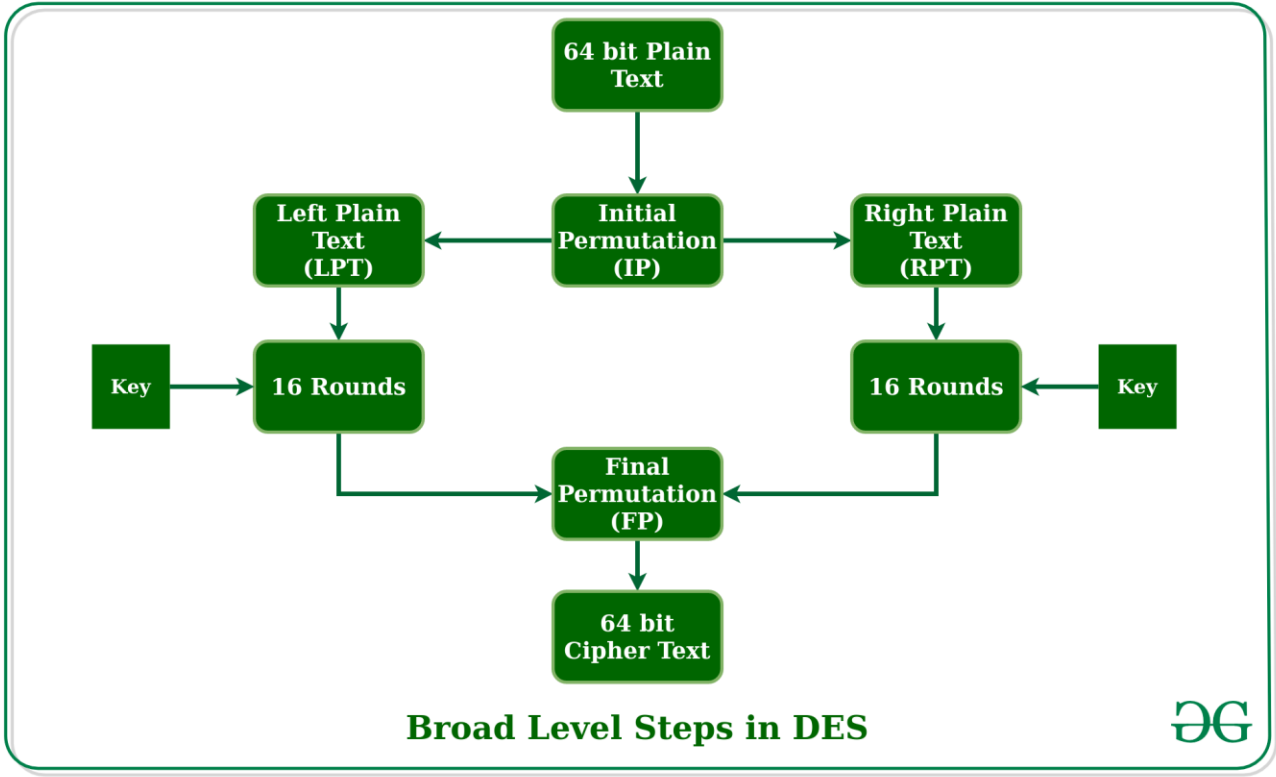


Figure. Encryption/Decryption of Network Traffic (McCabe, 2010, p.372)

Encryption/decryption

DES (data encryption standard)



Broad Level Steps in DES

Encryption/decryption trade-off

- Network performance can be degraded by 15-85% through application of E/D

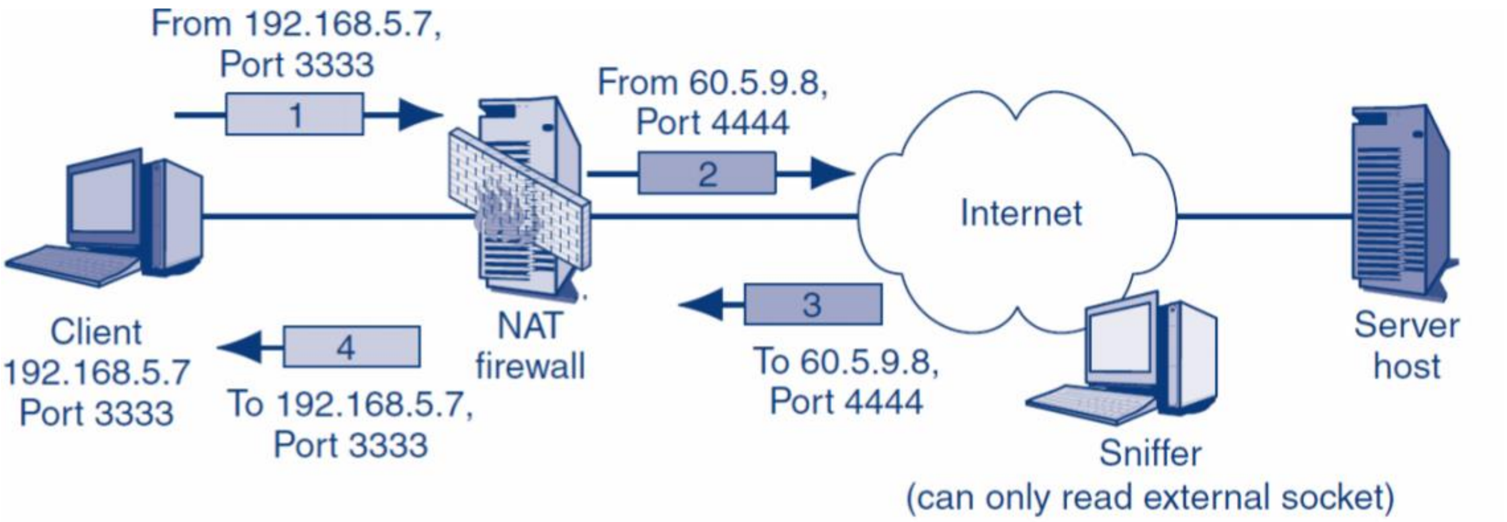
- E/D requires administration and maintenance and does not come cheaply.

Network Perimeter Security

- Network Address Translation (NAT) applies protection at external interfaces

- NAT is used to create bindings between public and private internet addresses
  - Static NAT – one-one address binding (servers)
  - Dynamic NAT – one-to-many address binding (generic devices)

Network Perimeter Security



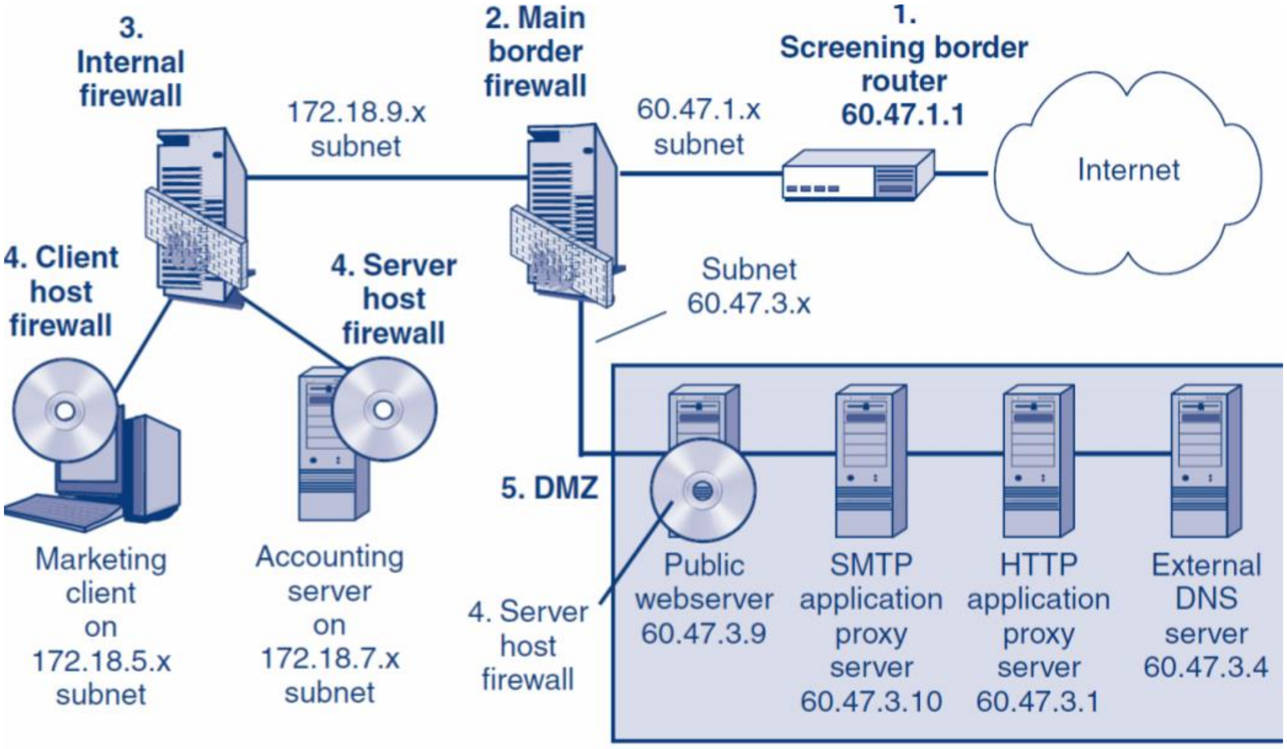
Translation table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	3333	60.5.9.8	4444
. . .	. . .	. . .	. . .

Network Perimeter Security

- Firewalls, demilitarized zones (DMZs), isolation LANS (iLANs)
  - Packet filtering
  - Application proxies with filtering gateways

Network Perimeter Security

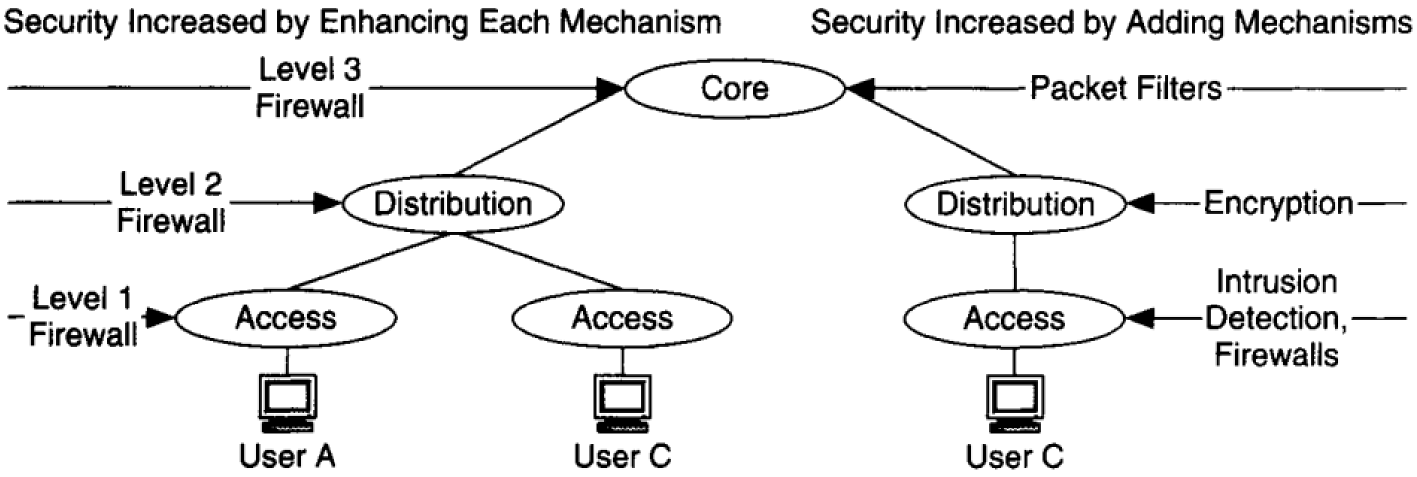

3. Internal firewall
2. Main border firewall
1. Screening border router 60.47.1.1
172.18.9.x subnet
60.47.1.x subnet
Internet
4. Client host firewall
4. Server host firewall
Subnet 60.47.3.x
5. DMZ
Marketing client on 172.18.5.x subnet
Accounting server on 172.18.7.x subnet
4. Server host firewall
Public webserver 60.47.3.9
SMTP application proxy server 60.47.3.10
HTTP application proxy server 60.47.3.1
External DNS server 60.47.3.4

Architectural Considerations

- Evaluation of potential security mechanisms
- Internal and external relationships

Evaluation of Security Mechanisms

- Access/distribution/core architectural model is useful starting point for applying security mechanisms



(McCabe, 2010, p.377)

Evaluation of Security Mechanisms

- It may be more helpful to determine security perimeters and organize levels of security as embedded zones

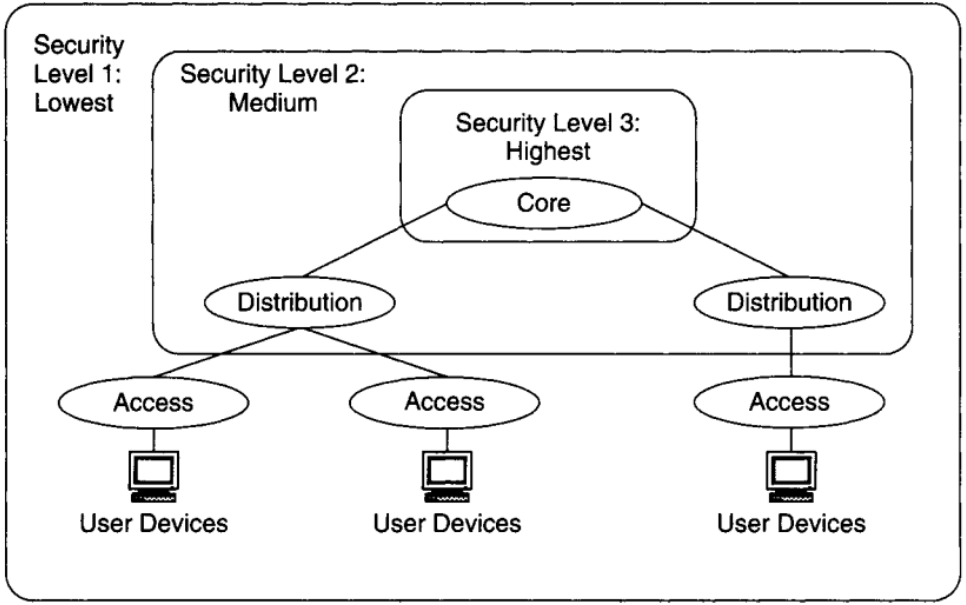


Figure. Security Zones Embedded within Each Other (McCabe, 2010, p.379)

Evaluation of Security Mechanisms

- Alternatively, you can develop a less hierarchical (flatter) security plan (Fig 9.14)

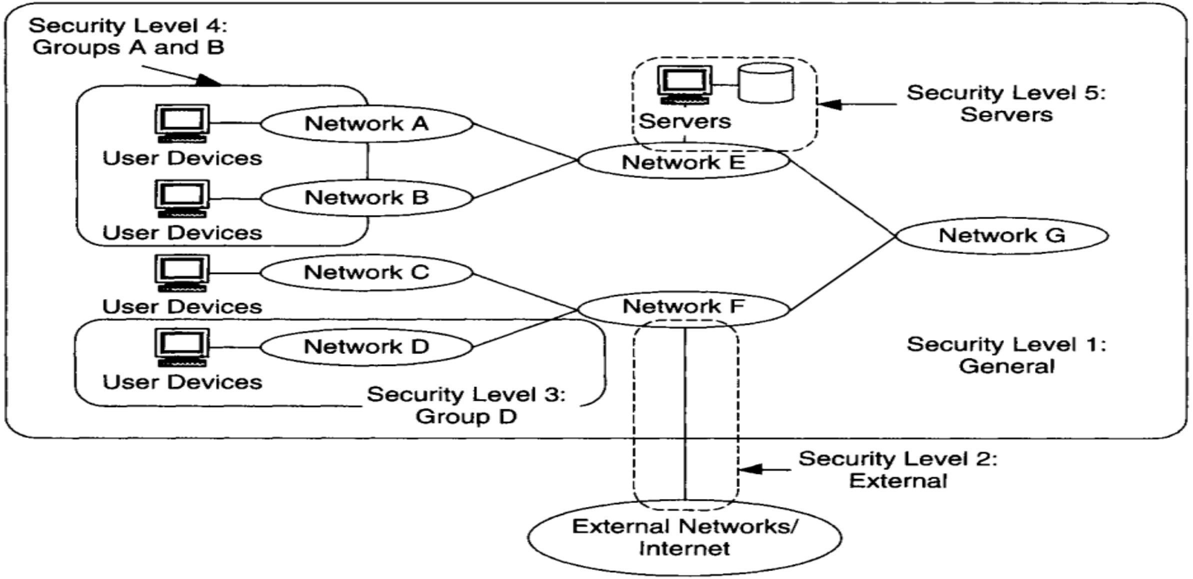


Figure. Developing security Zones throughout a Network (McCabe, 2010, p.379)

Internal Relationship

- Interactions within the security architecture
  - Trade-offs
  - Dependencies
  - Constraints
- E.g. NAT, encryption/decryption mechanisms

External Relationship

- Security and Addressing/Routing
  - Relevant to NAT
  - Dynamic address works against address – specific measures and logging
- It is difficult to understand what is going on when addresses are changing frequently

External Relationship

- Security and Network Management
  - Security depends on configuring, monitoring, management and verification of security levels
  - Out-of-band network management may be a necessary fall back position as security vulnerabilities are associated with in-band network management.

External Relationship

- Security and Performance
  - Security and performance are at odds
  - Hence the selective application of security (as opposed to blanket application) is one response

External Relationship

- Security mechanisms may restrict or preclude performance within each zone

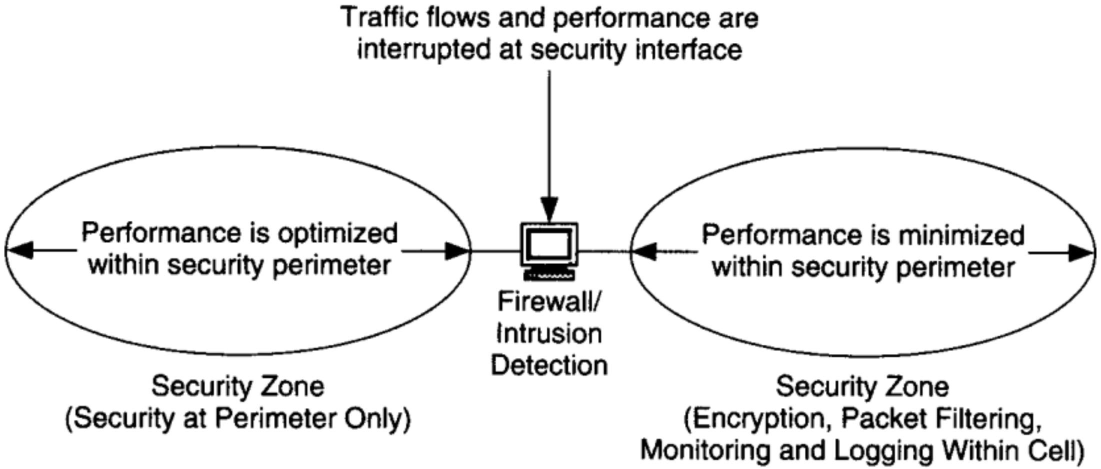

Traffic flows and performance are interrupted at security interface
Performance is optimized within security perimeter
Firewall/ Intrusion Detection
Performance is minimized within security perimeter
Security Zone (Security at Perimeter Only)
Security Zone (Encryption, Packet Filtering, Monitoring and Logging Within Cell)

FIGURE 9.15 Security Mechanisms May Restrict or Preclude Performance within Each Zone

(McCabe, 2010, p.381)

References and Reading

- **Chapter 9** - McCabe, J. D. (2010). *Network Analysis, Architecture, and Design*. San Diego, CA, USA: Elsevier Science.
- **Chapter 5** -Kurose, J. F. (2017). Computer networking : a top-down approach (Seventh, global edition. ed.). Boston: Pearson.

Thank you
Q&A ?

UNIVERSITY
OF WOLLONGONG
AUSTRALIA