Lesson 5 : Introduction to Networks Security

N.BERREHOUMA
Department of Computer Science
8 Mai 1945 University, Guelma

April 6, 2025

Overview

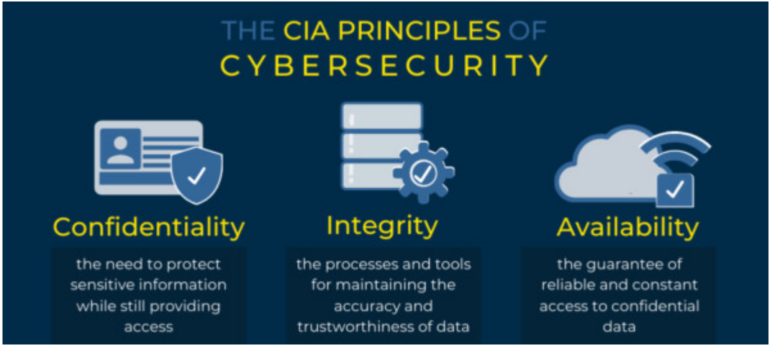
1. **Understanding Network Security**
2. **Security Threats and Vulnerabilities**
3. **Principles of Network Security**
4. **Security Mechanisms**
5. **Security Policies**
6. **Practical Labs**
   - 6.1 Cisco Access Control Lists (ACLs)
   - 6.2 Demilitarized Zones (DMZ)
   - 6.3 Network Address Translation
   - 6.4 Virtual Private Networks

What is Network Security?

- The practice of protecting computer networks and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Importance:
  - Protecting sensitive data (e.g., customer information, financial records).
  - Ensuring business continuity and availability of critical services.
  - Maintaining user privacy and trust.
  - Complying with regulatory requirements (e.g., HIPAA, PCI DSS).

Key Concepts

- Confidentiality: Protecting data from unauthorized disclosure.
- Integrity: Ensuring data accuracy and completeness.
- Availability: Ensuring that network resources and services are accessible when needed.



THE CIA PRINCIPLES OF CYBERSECURITY

Confidentiality

the need to protect sensitive information while still providing access

Integrity

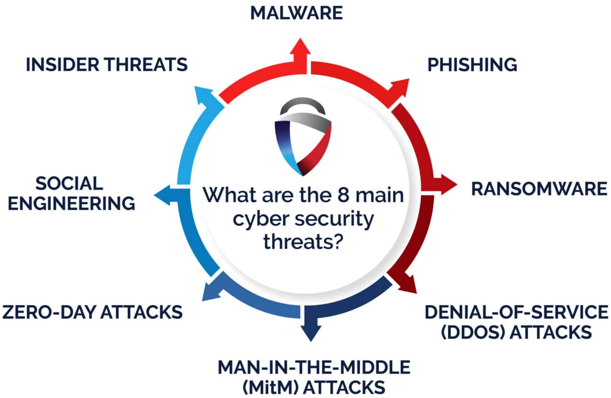
the processes and tools for maintaining the accuracy and trustworthiness of data

Availability

the guarantee of reliable and constant access to confidential data

Figure: CIA Principals of networking Security

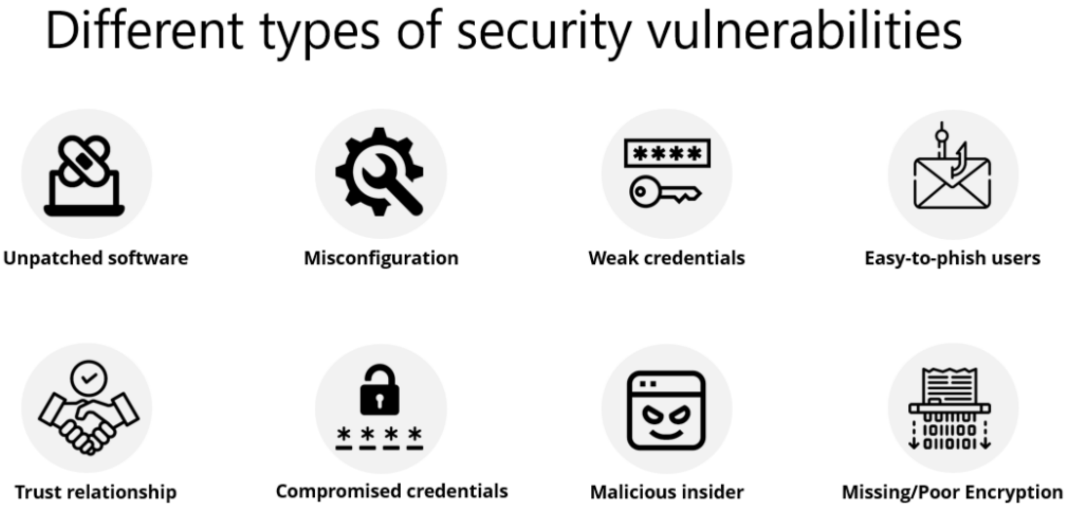
Threats


MALWARE
PHISHING
RANSOMWARE
DENIAL-OF-SERVICE (DDOS) ATTACKS
MAN-IN-THE-MIDDLE (MitM) ATTACKS
ZERO-DAY ATTACKS
SOCIAL ENGINEERING
INSIDER THREATS
What are the 8 main cyber security threats?

8 Main Cybersecurity Threats - Definitions

- **Malware** - Malicious software designed to harm, exploit, or infiltrate computer systems without the user's consent. Includes viruses, worms, trojans, and spyware.
- **Insider Threats** - Security risks that originate from within an organization, typically by employees, contractors, or business partners who misuse their access to harm systems or data.
- **Social Engineering** - Psychological manipulation of people into performing actions or divulging confidential information, often through pretexting, baiting, or other deceptive techniques.
- **Zero-Day Attacks** - Exploits targeting previously unknown vulnerabilities in software or hardware, giving developers "zero days" to fix the issue before attacks occur.
- **Man-in-the-Middle (MitM) Attacks** - When an attacker secretly intercepts and potentially alters communications between two parties who believe they are directly communicating with each other.
- **Phishing** - Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity in electronic communications, typically via email.
- **Ransomware** - Malware that encrypts a victim's files and demands payment

Vulnerabilities



Different types of security vulnerabilities

- Unpatched software
- Misconfiguration
- Weak credentials
- Easy-to-phish users
- Trust relationship
- Compromised credentials
- Malicious insider
- Missing/Poor Encryption

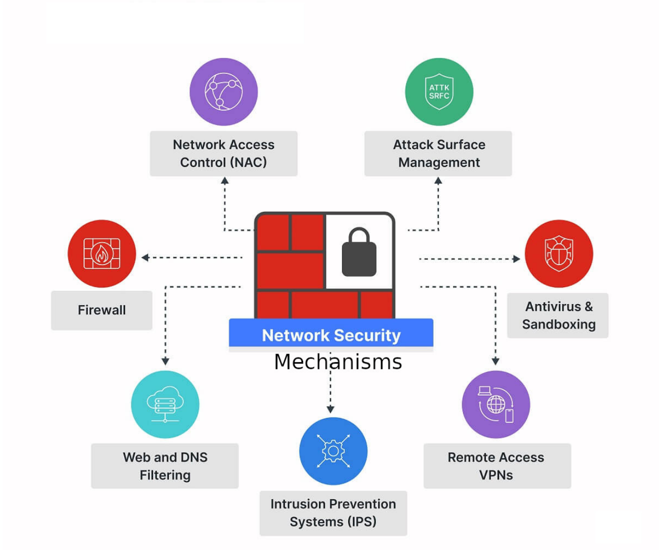
Different Types of Security Vulnerabilities - Definitions

- **Unpatched Software** - Systems or applications with known security flaws that have not been updated, leaving them vulnerable to exploitation by attackers.
- **Misconfiguration** - Incorrect or insecure setup of systems, networks, or applications that inadvertently exposes vulnerabilities or provides unnecessary access.
- **Weak Credentials** - Easily guessable or crackable passwords/passphrases that provide insufficient protection against brute force or credential stuffing attacks.
- **Easy-to-Phish Users** - Human vulnerability to social engineering attacks due to lack of awareness training or inherent trust in communications.
- **Trust Relationship** - Overly permissive access granted between systems, services, or organizations that can be exploited to move laterally through networks.
- **Compromised Credentials** - Stolen or leaked usernames/passwords that attackers use to gain unauthorized access while appearing as legitimate users.
- **Malicious Insider** - Authorized individuals who intentionally abuse their access privileges to steal data or harm systems.
- **Missing/Poor Encryption** - Failure to properly encrypt sensitive data (in transit or at rest), making it easily readable if intercepted or accessed.

Principles of Network Security

- Defense in Depth: Implementing multiple layers of security controls to provide comprehensive protection.
- Least Privilege: Granting users only the minimum necessary privileges to perform their job duties.
- Separation of Duties: Distributing critical tasks among multiple individuals to prevent fraud and abuse.
- Need-to-Know Basis: Restricting access to information based on job requirements.
- Regular Security Assessments: Conducting regular security audits and penetration tests to identify and address vulnerabilities.

Security Mechanisms



Key Network Security Mechanisms - Definitions

- **Network Access Control (NAC)** - Security solution that enforces policies on devices attempting to access network resources, ensuring compliance with security standards before granting access.
- **Attack Surface Management** - Continuous process of identifying, classifying, and reducing all possible points (the "surface") where an unauthorized user could try to enter or extract data from a network.
- **Firewall** - Network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
- **Web and DNS Filtering** - Security measures that block access to malicious or inappropriate websites and monitor/control Domain Name System (DNS) requests to prevent phishing and malware infections.
- **Intrusion Prevention Systems (IPS)** - Security technology that examines network traffic flows to detect and prevent vulnerability exploits, typically by dropping malicious packets or resetting connections.
- **Remote Access VPNs** - Virtual Private Networks that allow secure, encrypted connections for remote users to access an organization's network as if they were

Security Policies

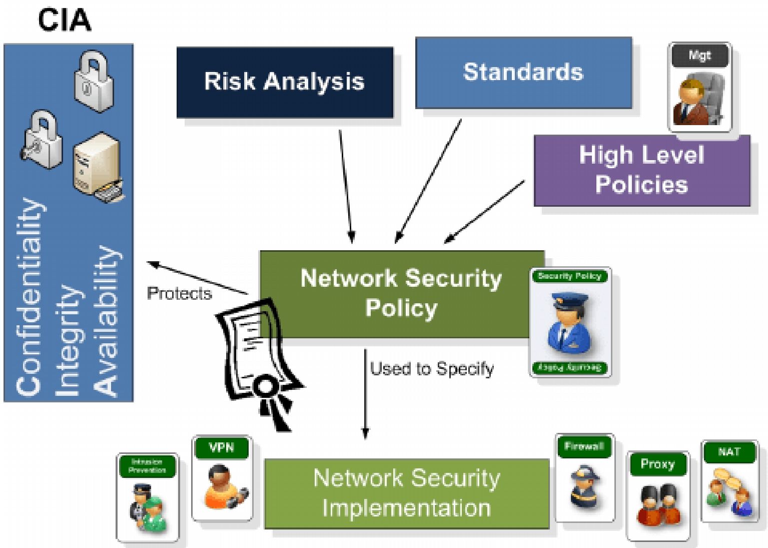
Definition

Formal documents that outline rules, procedures, and technical controls for protecting network infrastructure and data

Importance :

- Providing a framework for security decisions and actions.
- Ensuring consistent application of security controls.
- Communicating security expectations to employees and users.
- Meeting compliance requirements.

Networking Security Policy



CIA

Confidentiality

Integrity

Availability

Risk Analysis

Standards

High Level Policies

Network Security Policy

Protects

Used to Specify

Network Security Implementation

Essential Network Security Policies

Access Control

- **RBAC**: Role-based permissions
- **Least Privilege**: Minimum access needed
- **MFA**: Multi-factor authentication
- **VPN**: Secure remote access

Data Protection

- Encryption (TLS/IPSec)
- Data classification tiers
- Secure disposal procedures

Infrastructure

- Firewall rules (default-deny)
- IDS/IPS configurations
- Patch management schedule
- Network segmentation

Monitoring

- Log retention (90+ days)
- SIEM alert thresholds
- Regular pentesting

User Policies

- **AUP**: Approved services list
- Password complexity rules
- Phishing reporting

Response

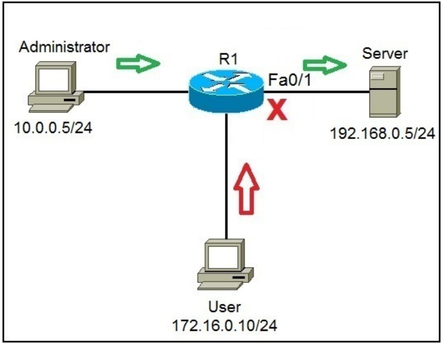
- Incident reporting flow
- Containment playbooks
- Forensic preservation

All policies must be: Documented • Enforced • Reviewed annually • Updated for new threats

Cisco Access Control Lists (ACLs)

What are ACLs?

- Rules to **filter traffic** (allow/deny) on interfaces
- Applied **inbound** (to router) or **outbound** (from router)
- Two types: **Standard (1-99)** and **Extended (100-199)**



ACL Syntax

Standard ACL (Simple Filtering)

```
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny any
```

Extended ACL (Granular Control)

```
access-list 101 permit tcp
  192.168.1.0 0.0.0.255
  any eq 80
```

Key Points: - Order matters (top-down processing) - Implicit "deny any" at the end - Wildcard mask subnet mask

Practice: Block HTTP but Allow DNS

```
! Extended ACL to block web traffic
access-list 110 deny tcp any any eq 80
access-list 110 permit udp any any eq 53
access-list 110 permit ip any any

! Apply to inbound traffic on Fa0/0
interface FastEthernet0/0
 ip access-group 110 in
```

- Denies HTTP (port 80)
- Allows DNS (port 53)
- Permits all other IP traffic

Verifying ACLs

Key Commands

```
show access-lists        # List all ACLs
show ip interface        # Check ACL application
debug ip packet          # Troubleshoot (use carefully!)
```

Example Output

```
ACL 110 deny tcp any any eq www
    (5 matches)
ACL 110 permit udp any any eq domain
    (12 matches)
```

Common ACL Mistakes

Errors to Avoid

- Wrong order (e.g., "deny any" before specific rules)
- Incorrect wildcard masks (e.g., ‘0.0.0.255‘ vs ‘255.255.255.0‘)
- Forgetting to apply ACL to an interface

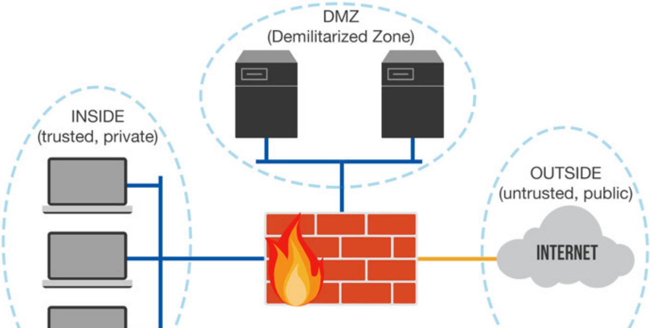
Pro Tips

- Test ACLs in a lab first!
- Use named ACLs for readability
- Add comments with `remark`

DMZ (Demilitarized Zone) in Network Security

What is a DMZ?

- Isolated subnet for **public-facing services** (web servers, email, etc.)
- Acts as a buffer zone between **Internet** and **internal network**
- Key principle: **"Defense in Depth"**



DMZ Design Principles

Common Topologies

- **Dual-Firewall**: - Outer FW: Internet → DMZ - Inner FW: DMZ → Internal
- **Single-Firewall**: - Multiple interfaces (Untrust/DMZ/Trust)

Typical DMZ Services

- Web Servers (HTTP/HTTPS)
- Email Gateways (SMTP)
- FTP Servers
- VPN Gateways

Cisco DMZ Implementation

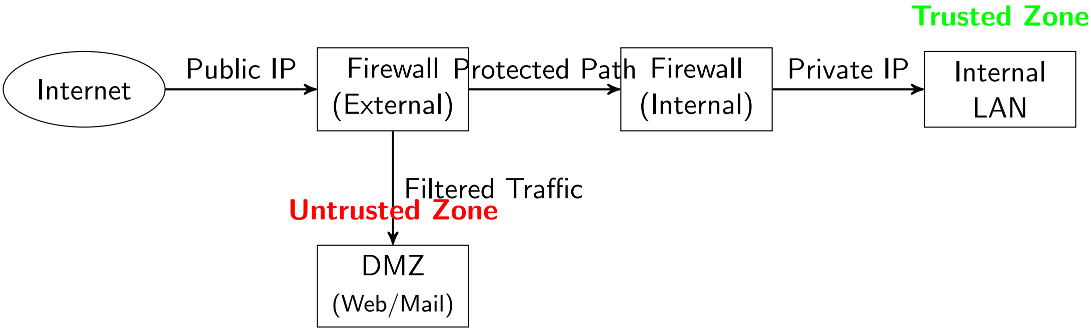
```
! Configure interfaces
interface Gig0/0   # Internet-facing
 ip address 203.0.113.1 255.255.255.0

interface Gig0/1   # DMZ
 ip address 192.168.1.1 255.255.255.0

interface Gig0/2   # Internal LAN
 ip address 10.0.0.1 255.255.255.0

! ACL for DMZ (allow web traffic only)
access-list DMZ-IN permit tcp any 192.168.1.0 0.0.0.255 eq 80
access-list DMZ-IN deny ip any any
```

Cisco DMZ Architecture



DMZ Security Policies

Critical Rules

- **Default-Deny**: Block all traffic not explicitly allowed
- **No Direct Internal Access**: DMZ servers shouldn't initiate connections to LAN
- **Logging**: Monitor all DMZ traffic
- **Patch Management**: Weekly updates for DMZ systems

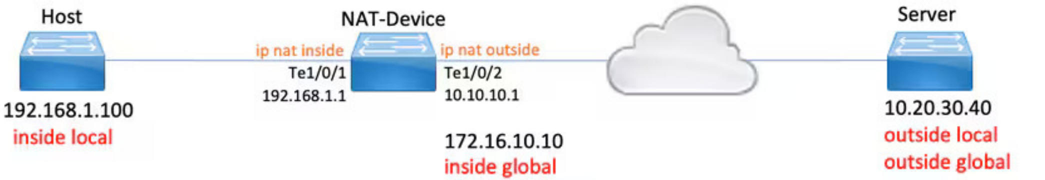
Never Place in DMZ:

- Domain Controllers Servers
- Internal file shares

Network Address Translation (NAT)

Why NAT?

- Conserves IPv4 addresses
- Hides internal network topology
- Allows LAN devices to access Internet



NAT Types on Cisco Routers

Static NAT (1-to-1)

```
ip nat inside source static
  192.168.1.10 203.0.113.5
```

Dynamic NAT (Pool)

```
ip nat pool PUBLIC 203.0.113.10
  203.0.113.20 netmask 255.255.255.0
ip nat inside source list 1 pool PUBLIC
```

PAT (Overload)

```
ip nat inside source list 1
  interface Gig0/0 overload
```

PAT Configuration Example

```
! Define inside/outside interfaces
interface GigabitEthernet0/0
 ip nat outside
interface GigabitEthernet0/1
 ip nat inside

! ACL for NAT eligible traffic
access-list 1 permit 192.168.1.0 0.0.0.255

! Enable PAT (Overload)
ip nat inside source list 1
  interface Gig0/0 overload
```

Key Commands

`show ip nat translations` `debug ip nat`

Verifying NAT Operation

Sample Output

```
NAT# show ip nat translations
Pro  Inside global     Inside local      Outside local
tcp  203.0.113.5:1050  192.168.1.10:1050 172.16.1.1:80
```

- `show ip nat statistics`
- Check interface NAT assignments
- Verify ACL matches
- Test end-to-end connectivity

IpSec and VPN