9.1 Introduction to Cyber Security

A. What is Cyber Security?

- **Definition:** The practice of protecting **computers, servers, mobile devices, electronic systems, networks, and data** from digital attacks, damage, or unauthorized access.
- **Other names:** Information Technology (IT) security, electronic information security.

B. Core Goals of Cyber Security (CIA Triad) – *Important for Exam*

Principle	Meaning	Example
Confidentiality	Only authorized people can access data	Encryption, passwords, access controls
Integrity	Data is accurate and has not been tampered with	Hashing, checksums, digital signatures
Availability	Data and systems are accessible when needed	Backups, redundancy, DDoS protection

C. Why is Cyber Security Important? (Government Context - Nepal)

- Protects **citizen data** (e.g., citizenship, passport, tax records)
- Prevents **financial fraud** (government bank accounts)
- Ensures **continuity of e-governance services** (online portals, payments)
- Defends against **cyber espionage** (foreign or internal threats)
- Maintains **public trust** in digital government services

D. Types of Cyber Security (Broad Areas)

Type	Protects
Network Security	Internal network from intruders
Application Security	Software and apps from vulnerabilities
Information Security	Data integrity and privacy
Operational Security	Processes and decisions handling data
Disaster Recovery	Business continuity after breach
End-user Education	Training people against threats (phishing, etc.)

9.2 Common Security Threats

A. Social Engineering

- **Definition:** Manipulating **people** into revealing confidential information or performing actions (instead of hacking technical systems).
- **Why dangerous:** Humans are the weakest link in security.
- **Common techniques:**

Technique	How it works	Example
Phishing	Fake emails pretending to be legitimate	"Your account will be closed. Click this link."
Spear Phishing	Targeted phishing at a specific person	Email to a government officer with their real name and title
Vishing	Voice phishing (phone calls)	Caller pretending to be IT support asking for password
Smishing	SMS phishing	Text message with fake bank alert link
Pretexting	Creating a fake scenario to get info	"I'm from HR, please confirm your login details."
Baiting	Offering something enticing to trick user	Free USB drive left in parking lot containing malware
Tailgating	Following authorized person into secure area	Walking behind an employee through a secured door

B. Distributed Denial of Service (DDoS)

- **Definition:** An attack that floods a target (website, server, network) with so much traffic that it becomes **overwhelmed and unavailable** to legitimate users.
- **How it works:**
  1. Attacker controls a **botnet** (thousands of infected computers - zombies).
  2. All botnet computers send requests to the target simultaneously.
  3. Target's resources are exhausted (bandwidth, CPU, memory).
  4. Real users cannot access the service.
- **DDoS vs DoS:**
  - **DoS (Denial of Service):** From one computer (easier to block).
  - **DDoS (Distributed):** From many computers (much harder to stop).

Common DDoS attack types:

Type	Target
Volume-based	Bandwidth (UDP floods, ICMP floods)
Protocol-based	Server resources (SYN floods)
Application-layer	Web server (HTTP floods)

Real-world impact: Government websites, banks, election portals can be taken offline.

C. Malware (Malicious Software)

Malware is any software intentionally designed to cause damage, steal data, or gain unauthorized access.

1. Viruses

- **Definition:** Malicious code that attaches itself to clean files and **spreads to other files and computers** when the infected file is executed.
- **Requires human action:** User must open an infected file, run a program, or boot from an infected USB.
- **Effect:** Can corrupt files, delete data, steal information.

2. Worms

- **Definition:** Standalone malware that **replicates itself and spreads automatically** without any human action.
- **How it spreads:** Exploits network vulnerabilities, sends copies via email, instant messages, or network shares.
- **Difference from virus:** Worm does not need to attach to an existing file or program.
- **Effect:** Consumes bandwidth, overloads networks, can deliver payloads (ransomware, backdoors).

Example: *ILOVEYOU worm (2000)* – caused billions in damage.

3. Trojans (Trojan Horses)

- **Definition:** Malware that **disguises itself as legitimate software** to trick users into installing it.
- **How it works:** User downloads a "free game," "software crack," or "email attachment" that looks safe but contains hidden malicious code.
- **Does NOT self-replicate** (unlike viruses/worms).
- **Effect:** Creates backdoors, steals passwords, logs keystrokes, installs other malware.

Example: Fake antivirus software that actually installs ransomware.

4. Spyware

- **Definition:** Software that **secretly monitors and collects user activity** without their knowledge.
- **What it collects:** Browsing habits, keystrokes, login credentials, credit card numbers, personal information.
- **How it infects:** Bundled with free software, malicious links, drive-by downloads.
- **Legitimate vs malicious:** Some companies use spyware for marketing; malicious spyware is for theft.

5. Ransomware (Important - very common now)

- **Definition:** Malware that **encrypts the victim's files** and demands payment (ransom) to decrypt them.
- **How it spreads:** Phishing emails, malicious ads, infected downloads.
- **Effect:** All files become inaccessible until ransom is paid (usually in cryptocurrency).
- **Government impact:** Hospitals, police departments, and government offices have been paralyzed by ransomware.

6. Phishing (Also listed under Social Engineering)

- **Definition:** Fraudulent attempt to obtain sensitive information by **disguising as a trustworthy entity** in electronic communication.
- **Primary target:** Login credentials, credit card numbers, personal identification.

7. Other Malware Types (Know for exam)

Type	Description
Adware	Displays unwanted advertisements; can be bundled with free software
Keylogger	Records every keystroke typed on a keyboard
Rootkit	Hides deep in operating system; gives attacker administrator access
Botnet malware	Turns infected computer into a "zombie" for DDoS attacks
Logic bomb	Malicious code that activates at a specific time or condition

Quick Comparison Table (Malware)

Malware	Self-replicates?	Requires user action?	Primary damage
Virus	Yes (attaches to files)	Yes	File corruption, spread
Worm	Yes (automatic)	No	Network overload, bandwidth
Trojan	No	Yes (deception)	Backdoor, data theft
Spyware	No	Yes (bundled)	Privacy violation
Ransomware	Can spread	Yes (phishing)	File encryption, extortion

9.3 Security Mechanisms

9.3.1 Identity and Access Control (IAC)

Definition: The process of ensuring that **only authorized users** can access specific resources, and only in approved ways.

A. Identification vs Authentication vs Authorization

Term	Meaning	Example
Identification	Claiming who you are	Username, email address, ID card number
Authentication	Proving you are who you say you are	Password, fingerprint, OTP
Authorization	Determining what you are allowed to do	Read-only access, admin privileges

B. Authentication Factors (Something you...)

Factor	Example	Strength
Knowledge (something you know)	Password, PIN, answer to security question	Weak (can be stolen/phished)
Possession (something you have)	Smartphone (OTP), smart card, hardware token	Stronger
Inherence (something you are)	Fingerprint, face recognition, iris scan	Strongest (biometrics)
Location (somewhere you are)	GPS, IP address range	Contextual
Behavior (something you do)	Typing pattern, mouse movement	Advanced

C. Multi-Factor Authentication (MFA) / Two-Factor Authentication (2FA)

- **Definition:** Using **two or more different authentication factors** to verify identity.
- **Example:** Password (knowledge) + OTP sent to phone (possession).
- **Why important:** Even if password is stolen, attacker cannot log in without the second factor.

D. Access Control Models

Model	Rule	Example
DAC (Discretionary)	Owner decides who accesses	File permissions in Windows
MAC (Mandatory)	System enforces rules (government/military)	Security clearance levels
RBAC (Role-based)	Access based on job role	"Manager," "Employee," "Guest"

In government: RBAC is very common. A data entry operator cannot access admin settings.

9.3.2 Use of Firewalls, IDS, and IPS

A. Firewall

- **Definition:** A network security system that **monitors and controls incoming and outgoing traffic** based on predefined security rules.
- **Analogy:** A security guard at the entrance of a building checking IDs.
- **Types:**

Type	Description
Packet-filtering firewall	Examines each packet header (IP, port). Fast but basic.
Stateful inspection firewall	Tracks active connections; more intelligent.
Proxy firewall	Acts as intermediary between users and internet.
Next-Gen firewall (NGFW)	Includes deep packet inspection, IPS, application awareness.

- **Where placed:** Between internal network and external network (e.g., at internet gateway).

B. IDS (Intrusion Detection System)

- **Definition:** A system that **monitors network traffic** and **alerts** administrators when suspicious activity is detected.
- **Analogy:** A security camera that records and alerts, but does not stop the intruder.
- **Key characteristics:**
  - **Passive** (detects and logs, but does not block)
  - Generates alerts (email, console, log)
  - Types: Network-based (NIDS) and Host-based (HIDS)

C. IPS (Intrusion Prevention System)

- **Definition:** A system that **monitors network traffic AND actively blocks/thwarts** detected threats in real-time.
- **Analogy:** A security guard who stops and arrests the intruder.
- **Key characteristics:**
  - **Active** (can drop packets, block IPs, reset connections)
  - Usually placed inline with traffic flow
  - Can be network-based (NIPS) or host-based (HIPS)

Comparison Table:

Feature	Firewall	IDS	IPS
Primary function	Block/allow based on rules	Detect and alert	Detect and block
Active or passive	Active	Passive (alert only)	Active
Location	Network perimeter	Monitor point (often mirrored traffic)	Inline (traffic passes through)
Reaction	Drops/allows packets	Sends alert	Drops packets, blocks IP, resets connection
Can it stop zero-day?	No (rule-based)	Partial (signature + anomaly)	Partial (signature + anomaly)

Common practice: Many modern devices combine **Firewall + IPS** (called Next-Generation Firewall).

9.3.3 Email Filtering

- **Definition:** The use of software to **automatically scan, categorize, and block or quarantine** incoming and outgoing email messages based on policies.
- **Purpose:** Stop spam, phishing, malware, and sensitive data leaks.

Common email filtering techniques:

Technique	Purpose
Spam filtering	Block unwanted bulk email (advertisements, scams)
Phishing detection	Identify fake emails pretending to be legitimate
Malware scanning	Scan attachments for viruses, trojans, ransomware
Content filtering	Block emails containing sensitive keywords (e.g., "password", "confidential")
Attachment blocking	Block dangerous file types (.exe, .scr, .zip with password)
Sender reputation check	Block emails from known malicious IPs or domains
DMARC / DKIM / SPF	Verify that email really came from claimed domain (prevents spoofing)

Why important for government: Prevents spear-phishing attacks targeting government officers. Many data breaches start with a malicious email.

9.3.4 Use of Antivirus Software

- **Definition:** Software designed to **detect, prevent, and remove** malware (viruses, worms, trojans, spyware, ransomware, etc.).
- **How it works:**
  1. **Signature-based detection:** Compares files against a database of known malware signatures (fingerprints). Requires regular updates.
  2. **Heuristic-based detection:** Analyzes behavior and code patterns to detect new, unknown malware (zero-day).
  3. **Behavioral monitoring:** Watches program actions in real-time (e.g., "This program is trying to encrypt all files").
  4. **Sandboxing:** Runs suspicious files in an isolated environment to see what they do.

Popular antivirus software (examples for knowledge):

- Paid: Norton, McAfee, Kaspersky, Bitdefender
- Free: Avast, AVG, Microsoft Defender (built into Windows)

Best practices for antivirus in government offices:

Practice	Why
Keep definitions updated	New malware appears daily
Run scheduled scans	Detect dormant malware
Enable real-time protection	Blocks malware before execution
Do not disable for convenience	One disabled AV = security hole
Use centralized management	IT team can monitor all office computers

Limitations of antivirus:

- Cannot stop all zero-day attacks (brand new malware)
- Cannot stop social engineering (user willingly giving password)
- Cannot stop DDoS attacks (network-level problem)
- Must be combined with firewalls, IDS/IPS, and user training.

9.4 Digital Signature: Concept and Applications

A. What is a Digital Signature?

- **Definition:** A **mathematical technique** used to validate the **authenticity and integrity** of a digital message, document, or software.
- **Analogy:** Like a handwritten signature or a sealed stamp, but much more secure and impossible to forge.
- **Not the same as:** Digitized image of a signature (scan of handwritten signature) – that is NOT a true digital signature.

B. How Digital Signatures Work (Basic Concept)

Digital signatures use **Public Key Cryptography (Asymmetric Encryption)** :

Key Type	Purpose	Who has it?
Private Key	Creates the signature	Only the signer (kept secret)
Public Key	Verifies the signature	Anyone who needs to verify

Process:

1. **Signing:** Sender uses their **private key** to encrypt a hash (digital fingerprint) of the document. This encrypted hash is the digital signature.
2. **Sending:** Sender sends original document + digital signature.
3. **Verification:** Receiver uses sender's **public key** to decrypt the signature and compare it with a new hash of the received document.
4. **Result:**
   - If hashes match → Document is **authentic** (from real sender) and **unmodified**.
   - If hashes do not match → Document is tampered or sender is fake.

C. What Digital Signatures Provide (Core Security Goals)

Goal	Meaning
Authentication	Confirms the identity of the signer (you know who signed it)
Integrity	Proves the document has not been altered after signing
Non-repudiation	Signer cannot later deny signing (legally binding)

D. Legal Status in Nepal (Important for Exam)

- **Electronic Transaction Act, 2063 (ETA 2063)** provides legal recognition to digital signatures in Nepal.
- The Act defines two types:

Type	Definition	Use
Digital Signature	Uses asymmetric crypto (public/private key) with a licensed Certifying Authority (CA)	Legally binding, high-security (e.g., company registration, tax filing)
Electronic Signature	Broader term (biometric, PIN, scanned signature, etc.)	Lower-security transactions

In Nepal: Digital signatures issued by **licensed Certifying Authorities** (e.g., NIC Asia, IT Solutions Nepal) are legally valid. The **Controller of Certifying Authorities (CCA)** under MoCIT regulates them.

E. Applications of Digital Signatures (Exam Focus)

Sector	Application
Government (Nepal)	E-procurement (PPMO - Public Procurement Monitoring Office), tax filing (IRD), company registration (OCR), online application forms (PSC)
Banking & Finance	Digital loan agreements, secure fund transfers, KYC documents
Legal	Digitally signed contracts, court document filing
Software distribution	Microsoft, Adobe, Google sign their software to prove it is genuine (not tampered)
Email security	S/MIME or PGP signatures to verify sender
PDF documents	Digitally signed PDFs (Adobe Sign, DocuSign, local solutions)

F. Benefits of Digital Signatures in E-Governance

Benefit	Explanation
Cost saving	No paper, printing, physical delivery, or storage
Time saving	Minutes instead of days (no physical signatures needed)
Security	Much harder to forge than handwritten signature
Legal validity	Recognized by Nepali law (ETA 2063)
Audit trail	Records exactly who signed what and when

G. Digital Signature vs Handwritten Signature

Feature	Handwritten	Digital
Uniqueness	Medium (can be forged)	High (cryptographically unique)
Verifiability	Requires expert	Instant (software checks)
Non-repudiation	Weak (can claim forgery)	Strong (private key controlled by signer)
Document integrity	Does not detect changes	Any change invalidates signature
Remote use	No (must be present)	Yes (anywhere with internet)