Cyber Security - PDF Note - computeroperatorexam.com

9.1 — Key Definitions

Term	Definition
Cyber Security	Practice of protecting computers, networks, and data from unauthorized access, damage, or attack
Computer Security	Safeguarding hardware, software, data from threats
CIA Triad	Confidentiality, Integrity, Availability — the three pillars of security
Cyber Crime	Criminal activities carried out using computers or the Internet
Cyber Law	Legal framework governing computers, Internet, and digital information
ETA 2063	Nepal's Electronic Transaction Act — primary cyber law

CIA Triad:

- **Confidentiality** — Only authorized users access data (passwords, encryption)
- **Integrity** — Data is not altered without authorization (hashing, digital signatures)
- **Availability** — Systems accessible when needed (backups, redundancy)

9.2 — Malware Quick Reference

Malware	Key Feature	Spreads How
Virus	Attaches to host file; needs user action to activate	Running infected file
Worm	Self-replicates without host file; spreads automatically	Network vulnerabilities
Trojan	Disguised as legitimate software; does not replicate	User installs it

Malware	Key Feature	Spreads How
Spyware	Secretly monitors and sends user data to attacker	Bundled with free software
Ransomware	Encrypts files; demands ransom for decryption key	Email, drive-by downloads
Phishing	Fake emails/sites to steal credentials	Email, SMS, phone
Rootkit	Hides malware; gives attacker root/admin access	Exploits, trojans
Adware	Displays unwanted ads; may track behaviour	Bundled software

Virus vs Worm vs Trojan

Feature	Virus	Worm	Trojan
Needs host file	✅	❌	❌
Self-replicates	✅	✅	❌
Needs user action	✅	❌	✅ (install)

Virus Symptoms (7 key points)

1. Computer slows down
2. Programs crash unexpectedly
3. Files deleted or corrupted
4. Unusual error messages
5. Antivirus turns off automatically
6. Hard disk space decreases
7. Frequent pop-ups

Types of Virus (6 types for exam)

1. **Boot Sector** — infects MBR at startup
2. **File Infector** — infects .exe files
3. **Macro** — infects Word/Excel macros

4. **Polymorphic** — changes signature to evade detection
5. **Stealth** — hides from OS/antivirus
6. **Multipartite** — infects both boot sector and files

Social Engineering Techniques

Technique	Method
Phishing	Fake emails/sites
Pretexting	Fabricated scenario (fake IT support)
Baiting	Infected USB left for victim
Tailgating	Physical access by following authorized person
Vishing	Phone-based phishing

DDoS Attack

- Uses a **botnet** (thousands of compromised computers)
- Floods target with traffic → target crashes or slows
- **DoS** = single attacker; **DDoS** = distributed (thousands)
- Countermeasures: CDN, rate limiting, IPS, ISP-level filtering

---

9.3 — Security Mechanisms Summary

9.3.1 — Identity & Access Control

Authentication factors:

- Something you KNOW — password, PIN
- Something you HAVE — smart card, OTP token
- Something you ARE — biometric (fingerprint, face)

MFA: Using two or more factors simultaneously.

AAA Model:

- **Authentication** — Who are you? (login)

- **Authorization** — What can you do? (permissions)
- **Accounting** — What did you do? (logs)

Access Control Models:

Model	Basis
DAC	Owner decides access
MAC	System/policy enforces access levels
RBAC	Access based on role
ABAC	Access based on attributes (time, location)

Principle of Least Privilege: Users get minimum access needed.

9.3.2 — Firewall Types

Firewall Type	OSI Layer	Inspects
Packet Filtering	Layer 3 (Network)	Headers only
Stateful Inspection	Layer 4 (Transport)	Headers + connection state
Proxy/Application	Layer 7 (Application)	Full content
NGFW	All layers	Deep packet + apps + identity

DMZ: Subnet between Internet and internal network — hosts public-facing servers.

IDS vs IPS vs Firewall

	Firewall	IDS	IPS
Action	Block by rules	Detect + alert only	Detect + block actively
Position	Perimeter	Network tap	Inline
Response	Proactive	Passive	Active

IDS Detection Methods:

- **Signature-based** — matches known attack patterns
- **Anomaly-based** — detects deviations from normal baseline
- **Heuristic-based** — uses rules and algorithms

9.3.3 — Email Filtering Techniques

1. Keyword/content filtering
2. Blacklist/whitelist
3. SPF — verifies sending mail server is authorized
4. DKIM — verifies email not tampered (digital signature)
5. DMARC — policy for failed SPF/DKIM checks
6. Attachment scanning with antivirus
7. URL reputation checking
8. Sandboxing suspicious attachments
9. Machine learning/AI classification

9.3.4 — Antivirus Detection Methods

Method	Detects New Threats?
Signature-based	❌ No (only known)
Heuristic analysis	⚠️ Partially
Behavioral monitoring	✅ Yes
Sandboxing	✅ Yes
Machine learning	✅ Yes
Cloud reputation	✅ Yes

Safe Computing Practices (top 5 for exam):

1. Install and update antivirus
2. Keep OS patched/updated
3. Use strong passwords + MFA
4. Take regular backups (3-2-1 rule)
5. Never click suspicious links or attachments

9.4 — Digital Signature

How it Works (must memorize for exam)

Signing:

```
Document → Hash Function → Digest → Encrypt with PRIVATE KEY → Digital Signature
```

Verification:

```
Received Signature → Decrypt with Sender's PUBLIC KEY → Original Digest
Received Document → Hash → New Digest
Compare: Match = authentic ✅ | No match = tampered ❌
```

Key Concepts

Term	Meaning
Hash function	Converts data to fixed-length digest; one-way; avalanche effect
Public key	Shared openly; verifies signature
Private key	Kept secret; creates signature
Digital Certificate	CA-issued document binding public key to identity
Certificate Authority (CA)	Trusted organization that issues/signs digital certificates
PKI	Framework managing keys, certificates, CAs
Non-repudiation	Signer cannot later deny signing

Hash Algorithms

Algorithm	Bits	Status
MD5	128	❌ Broken
SHA-1	160	⚠️ Deprecated
SHA-256	256	✅ Standard

Controller of Certification Authority (CCA) — Nepal

- Grants, renews, revokes CA licenses
- Supervises licensed CAs
- Maintains certificate repository
- Sets standards for CA operations
- Operates under ETA 2063

Applications of Digital Signature

- E-government document signing
- Online banking and e-commerce
- Legal contract signing
- Software code signing (verifying OS/app authenticity)
- Email security (S/MIME)
- SSL/TLS certificates for HTTPS

Exam Frequency Table

Topic	Exam Questions	Frequency
Computer security definition	MD Q22	🔴 High
Computer virus — causes, symptoms	MD Q27	🔴 High
5 types of computer virus + protection	MD Q28	🔴 High
Security threats + protection measures	LQ Set 2 B	🔴 High
Cyber crime + threats	LQ Set 5 B	🔴 High
Digital signature + CA duties	LQ Set 10 B	🔴 High

> **All 6 exam questions for Unit 9 are rated HIGH frequency — every topic must be studied.**

Defense in Depth — Layer Model

```
Human Layer         → Security awareness training, MFA
Perimeter           → Firewall (packet filter → NGFW)
Network             → IDS/IPS, network segmentation
Email               → Email filtering (SPF, DKIM, sandboxing)
Endpoint            → Antivirus, EDR, patch management
Data                → Encryption, digital signatures, access control
Identity            → Authentication (passwords + MFA + biometrics)
Physical            → Locks, CCTV, access cards
```

Related Pages

- [[Q-Cyber-Security-Introduction]] — CIA triad, cyber crime, cyber law
- [[Q-Security-Threats-Malware-Social-Engineering]] — All malware types, social engineering, DDoS
- [[Q-Security-Mechanisms-Identity-Access-Firewall-IDS-IPS]] — Firewalls, IDS, IPS, access control
- [[Q-Email-Filtering-Antivirus]] — Email security, antivirus detection methods
- [[Q-Digital-Signature]] — PKI, CA duties, CCA Nepal
- [[synthesis-computer-network]] — Unit 8 — networks that cyber security protects
- [[00-MOC]] — Full vault navigation