

Introduction to Computer Security

Introduction to Computer Security

Key concepts, goals, and foundational practices

1. What Is Computer Security?

Term	Definition
Computer Security	The protection of information systems (hardware, software, data, and networks) from unauthorized access, use, disclosure, disruption, modification, or destruction.
Cybersecurity	A broader umbrella that includes computer security plus the security of internet-connected devices, cloud services, and the overall digital ecosystem.
InfoSec	Short for <i>information security</i> – focuses on safeguarding data regardless of its form (digital, printed, spoken).

2. Core Objectives – The CIA Triad

Goal	What It Means	Typical Controls
Confidentiality	Ensuring that only authorized subjects can view data.	Encryption, access?control lists (ACLs), authentication mechanisms.
Integrity	Guaranteeing that data is accurate, complete, and unaltered without detection.	Checksums, digital signatures, version control, audit logs.
Availability	Making sure resources are accessible to legitimate users when needed.	Redundant hardware, load balancing, DoS mitigation, regular backups.

Other useful extensions: Authentication, Non?repudiation, Accountability.

3. Threat Landscape

Category	Examples	Typical Impact
----------	----------	----------------

Introduction to Computer Security

Malware	Viruses, worms, ransomware, trojans, spyware	Data loss, system downtime, financial extortion
Phishing & Social Engineering	Deceptive emails, pretexting, baiting	Credential theft, unauthorized access
Network Attacks	Man-in-the-middle, DDoS, port scanning	Service disruption, data interception
Insider Threats	Malicious employees, accidental leaks	Data exfiltration, sabotage
Vulnerabilities	Unpatched OS, insecure APIs, misconfigurations	Exploits leading to remote code execution, privilege escalation

4. Fundamental Security Controls

4.1 Preventive Controls

- **Authentication** – passwords, multi-factor authentication (MFA), biometrics.
- **Authorization** – role-based access control (RBAC), least-privilege principle.
- **Encryption** – at rest (disk, database) and in transit (TLS/SSL).
- **Firewalls & IDS/IPS** – packet filtering, intrusion detection/prevention.

4.2 Detective Controls

- **Logging & Monitoring** – system/event logs, SIEM (Security Information & Event Management).
- **Integrity Checking** – file hashes, configuration baselines.
- **Security Audits** – periodic reviews, penetration testing, vulnerability scanning.

4.3 Corrective Controls

- **Patch Management** – timely application of software updates.
 - **Incident Response** – containment, eradication, recovery, post-mortem analysis.
 - **Backup & Restore** – regular, tested backups stored off-site or in the cloud.
-

Introduction to Computer Security

5. Security Development Lifecycle (SDL)

1. **Requirements** – Define security objectives early (compliance, privacy, threat model).
 2. **Design** – Apply secure architecture patterns (defense in depth, sandboxing).
 3. **Implementation** – Follow secure coding standards (input validation, error handling).
 4. **Verification** – Code reviews, static analysis, dynamic testing.
 5. **Release** – Harden configurations, sign binaries, generate release notes.
 6. **Maintenance** – Ongoing patching, monitoring, and incident handling.
-

6. Common