TBI-603 — Network Security & Cyber Law

Comprehensive Unit Notes

Academic Reading Level · All 5 Units

Unit 1 — Introduction to Network Security

1.1 Security Attacks

A security attack is any deliberate action that compromises the confidentiality, integrity, or availability (CIA) of information or network resources. Security attacks are broadly classified into two categories: passive attacks and active attacks.

Passive Attacks

Passive attacks involve monitoring or eavesdropping on communication without modifying the data. The attacker's goal is information gathering, not disruption. Because no data is altered, passive attacks are difficult to detect. The two main types are: (1) **Release of Message Contents** — the attacker reads confidential communication such as emails or file transfers. (2) **Traffic Analysis** — even when messages are encrypted, the attacker observes communication patterns, frequency, and volume to extract useful information. Prevention methods include encryption, VPNs, and secure communication protocols.

Active Attacks

Active attacks involve the modification, interruption, or fabrication of data. Unlike passive attacks, these directly affect system operation and are relatively easier to detect. The four main types are: (1) **Masquerade** — the attacker impersonates an authorized user using stolen credentials. (2) **Replay** — previously captured valid messages are retransmitted to deceive the system. (3) **Modification of Messages** — legitimate data is altered during transmission, for example changing a bank transaction value. (4) **Denial of Service (DoS)** — the attacker floods a system with requests, making it unavailable to legitimate users.

Passive Attack	Active Attack
Monitors data without modification	Modifies, interrupts, or fabricates data
Difficult to detect	Easier to detect
Does not affect system resources	Directly affects system performance
Threatens confidentiality	Threatens integrity and availability

1.2 ISO Security Architecture

The ISO security architecture provides a standardized framework for securing network communication. It is organized around three core components: security attacks (threats to the system), security services (protective functions), and security mechanisms (tools that implement the services).

The six major **security services** are: Authentication (verifying the identity of communicating parties), Access Control (restricting unauthorized access to resources), Data Confidentiality (preventing unauthorized disclosure of information), Data Integrity (ensuring data has not been altered in transit), Non-repudiation (preventing a party from denying an action they performed),

and Availability (ensuring services remain accessible to authorized users).

The primary **security mechanisms** include: encryption (converting plaintext to ciphertext), digital signatures (verifying authenticity and integrity), access control systems (passwords, biometrics, permissions), and authentication exchange protocols such as Kerberos.

1.3 Kerberos Authentication

Kerberos is a network authentication protocol developed at MIT. It uses symmetric key cryptography and a trusted third party to authenticate users without transmitting passwords over the network. The system comprises four components: the Client, the Authentication Server (AS), the Ticket Granting Server (TGS), and the Service Server.

The authentication flow proceeds as follows: The client sends a request to the AS. The AS verifies the user's identity and issues a **Ticket Granting Ticket (TGT)** along with a session key. The client presents the TGT to the TGS to request access to a specific service. The TGS issues a **Service Ticket**. The client presents the Service Ticket to the Service Server, which grants access upon verification.

Advantages: supports mutual authentication, passwords are never transmitted over the network, reduces replay attacks. **Disadvantages:** requires synchronized clocks across all systems, creates a single point of failure if the AS or TGS is compromised.

1.4 X.509 Authentication and Digital Certificates

X.509 is an ITU-T standard for digital certificates used within Public Key Infrastructure (PKI). A Certificate Authority (CA) issues certificates that bind a public key to an entity's identity. Each certificate contains: version number, serial number, issuer name, subject name, public key, expiry date, and the CA's digital signature.

X.509 certificates are used to authenticate servers and users in HTTPS, SSL/TLS, and VPN connections. When a client connects to a server, it verifies the server's certificate against the issuing CA. If valid, a secure encrypted session is established. X.509 provides authentication, confidentiality, integrity, and non-repudiation.

1.5 Diffie-Hellman Key Exchange (Numerical)

Given: $p = 23$, $g = 5$, Alice's private key $a = 6$, Bob's private key $b = 15$.

Alice's public key: $A = g^a \bmod p = 5^6 \bmod 23 = 15625 \bmod 23 =$ **8**

Bob's public key: $B = g^b \bmod p = 5^{15} \bmod 23 =$ **19**

Shared secret (Alice): $K = B^a \bmod p = 19^6 \bmod 23 =$ **2**

Shared secret (Bob): $K = A^b \bmod p = 8^{15} \bmod 23 =$ **2** (both sides arrive at the same value, confirming correctness).

Unit 2 — Application and Transport Layer Security

2.1 Email Security

Email is a primary vector for cyber attacks on organizations. Without security measures, email communication is vulnerable to unauthorized access, spoofing, phishing, malware distribution, and message tampering. Email security addresses five core requirements: confidentiality (encrypting message content), integrity (detecting unauthorized modifications), authentication (verifying sender identity), non-repudiation (preventing denial of sending), and malware protection (filtering malicious attachments).

The two principal email security standards are PGP and S/MIME.

Feature	PGP	S/MIME
Full Form	Pretty Good Privacy	Secure/Multipurpose Internet Mail Extensions
Trust Model	Web of Trust	Certificate Authority (CA)
Certificate	Optional	Mandatory
Primary Use	Individual users	Organizations
Standardization	Less standardized	Widely standardized
Encryption	Public key cryptography	Public key cryptography

2.2 SET Protocol

The Secure Electronic Transaction (SET) protocol was developed by Visa and MasterCard to secure online credit card transactions. Its three core objectives are: ensuring the confidentiality of payment information, authenticating both the buyer and the merchant, and maintaining the integrity of the transaction. SET uses digital certificates for all parties — the customer, merchant, and payment gateway — and relies on a Certificate Authority to issue and validate these certificates.

2.3 SSL and TLS

SSL (Secure Socket Layer) and its successor TLS (Transport Layer Security) are cryptographic protocols that secure communication over networks. TLS is the current standard, offering stronger algorithms and better protection against known attacks. Both protocols provide confidentiality, integrity, and authentication.

The TLS session establishment follows five steps: (1) **Client Hello** — the client sends its supported TLS version, cipher suites, and a random number. (2) **Server Hello** — the server selects a cipher suite, sends its digital certificate and a server random number. (3) **Authentication** — the client verifies the server certificate against a trusted CA. (4) **Key Exchange** — both parties generate a shared session key. (5) **Secure Communication** — all subsequent data is encrypted using the session key.

SSL	TLS
Older protocol, developed by Netscape	Improved version, standardized by IETF
Less secure, weaker algorithms	More secure, stronger cryptography
Vulnerable to known attacks (e.g. POODLE)	Better resistance to attacks
Slower performance	Faster and more efficient

2.4 TLS Handshake and Record Protocols

TLS operates through two sub-protocols. The **Handshake Protocol** runs before data transfer and is responsible for: authenticating the communicating parties, negotiating the cipher suite, and establishing the session keys. The **Record Protocol** operates during data transfer and handles: fragmentation of messages into records, optional compression, encryption of records using the session key, and integrity verification using a Message Authentication Code (MAC).

2.5 Wireless Transport Layer Security (WTLS)

WTLS is a security protocol that forms part of the Wireless Application Protocol (WAP) architecture. It provides the same core security functions as TLS — confidentiality, authentication, and integrity — but is optimized for low-bandwidth wireless networks and resource-constrained mobile devices. WTLS is used in mobile banking, wireless browsing, and mobile commerce applications.

2.6 TLS Record Calculation (Numerical)

Given: message size = 3000 bytes, maximum data per TLS record = 600 bytes, overhead per record = 24 bytes.

Number of records = 3000 / 600 = **5 records**

Total overhead = 5 x 24 = **120 bytes**

Total transmitted bytes = 3000 + 120 = **3120 bytes**

Unit 3 — IP Security and System Security

3.1 IPsec — Authentication Header (AH) and ESP

IPsec is a suite of protocols that provides security for IP-layer communication. It operates through two main protocols: the Authentication Header (AH) and Encapsulating Security Payload (ESP).

Authentication Header (AH) provides data integrity, data origin authentication, and anti-replay protection. It does not provide encryption. AH adds a header containing a Security Parameters Index (SPI), sequence number, and authentication data (a hash of the packet). It is used when confidentiality is not required but packet authenticity must be verified.

Encapsulating Security Payload (ESP) provides confidentiality (encryption), data integrity, authentication, and anti-replay protection. ESP encrypts the payload of the IP packet. It is more widely deployed than AH because it offers a complete security solution.

Feature	AH	ESP
Encryption	No	Yes
Authentication	Yes	Yes
Integrity	Yes	Yes
Anti-replay	Yes	Yes
Protects	Packet header + payload	Payload only (in transport mode)
Privacy level	Lower	Higher

3.2 IPsec Modes — Transport vs Tunnel

Transport Mode protects only the payload (data portion) of the IP packet. The original IP header remains unchanged and visible. This mode has lower overhead and is used for direct host-to-host communication.

Tunnel Mode encrypts and/or authenticates the entire original IP packet — header and payload — and encapsulates it within a new IP packet with a new header. The original IP addresses are completely hidden. Tunnel mode is used in VPNs for site-to-site communication.

Transport Mode	Tunnel Mode
Protects payload only	Protects entire original packet
Original IP header visible	Original IP header hidden
Lower overhead	Higher overhead
Used for host-to-host communication	Used in VPNs (site-to-site)
Faster	More secure

3.3 Intrusion Detection Systems (IDS)

An intrusion is any unauthorized attempt to access, damage, or misuse a computer system. An Intrusion Detection System (IDS) monitors network traffic and system activity to identify suspicious or malicious behavior and generate alerts for administrators.

There are two types of IDS: **Host-based IDS (HIDS)** monitors activity on a single host system, examining log files, file integrity, and system calls. **Network-based IDS (NIDS)** monitors traffic across the entire network, analyzing packet headers and payloads for known attack signatures or anomalies.

3.4 Firewalls

A firewall is a security system — hardware or software — that controls network traffic based on predefined security policies. The three core design principles are: (1) all traffic between networks must pass through the firewall, (2) only traffic explicitly authorized by the security policy is permitted, (3) the firewall itself must be immune to compromise.

Firewall types include: **Packet Filtering** (inspects individual packets against rules), **Stateful Inspection** (tracks connection states to allow only legitimate traffic), **Proxy Firewall** (acts as an intermediary between client and server), and **Application Firewall** (filters traffic at the application layer).

3.5 Trusted Systems

A trusted system is an operating system or computing environment that reliably enforces a defined security policy. Features include: mandatory access control, user authentication, audit trails (logs of all security-relevant events), data integrity verification, and security monitoring. Trusted systems are essential in environments with multiple users requiring different privilege levels.

3.6 Program Security

Program security refers to protecting software applications from unauthorized access, modification, and exploitation. Common threats include buffer overflows, malware injection, code injection attacks, and exploitation of software bugs. Security measures include secure coding practices, input validation, access control enforcement, antivirus protection, and regular patch management.

3.7 Malicious Code — Viruses, Worms, and Others

Type	Definition	Key Characteristic
Virus	Attaches itself to a host file	Requires user action to spread; executes when infe
Worm	Self-replicating malware	Spreads automatically through networks; no host fil
Trojan	Disguised as legitimate software	Creates backdoors; steals data without user knowle
Spyware	Secretly collects user data	Operates silently; includes keyloggers and tracking
Ransomware	Encrypts victim's files	Demands payment for decryption key

Unit 4 — Cyber Law and Basics of Network Security

4.1 Cyber Law, Cyber Crime, and Cyber Criminals

Cyber law refers to the body of laws and regulations governing internet usage, digital communication, electronic commerce, and activities in cyberspace. It provides the legal framework within which digital transactions are recognized and cyber offences are punished.

Cyber crime is any illegal activity carried out using a computer, network, or the internet. Common examples include hacking, identity theft, online fraud, phishing, cyber stalking, and unauthorized data access.

A **cyber criminal** is an individual or group that commits cyber crimes. This includes hackers, fraudsters, malware developers, and cyber terrorists.

4.2 The Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is India's primary legislation governing electronic transactions and cyber activities. It was enacted in response to the growing need for legal recognition of digital processes and was influenced by the UNCITRAL Model Law on Electronic Commerce.

Five core objectives of the IT Act:

1. Provide legal recognition to electronic records and digital transactions.

2. Grant legal validity to digital signatures.

3. Promote and regulate electronic commerce.

4. Define and prescribe penalties for cyber crimes.

5. Facilitate and support e-governance — the delivery of government services through electronic means.

Scope: The Act applies to electronic records, digital signatures, cyber offences, electronic contracts, and online communication across India.

4.3 Legal Recognition of Electronic Records

Electronic records include emails, digital documents, electronic contracts, and digital databases. Prior to the IT Act, only physical documents had legal standing. The IT Act grants electronic records the same legal validity as paper documents, enabling paperless transactions, digital business contracts, and electronic government records to be recognized in a court of law.

4.4 Legal Recognition of Digital Signatures

A digital signature is a cryptographic mechanism used to verify the authenticity and integrity of an electronic document. Under the IT Act, a digitally signed document is legally equivalent to one signed by hand. Digital signatures fulfill four key functions: **Authentication** (confirms the

identity of the signer), **Integrity** (ensures the document has not been altered after signing), **Non-repudiation** (the signer cannot deny having signed the document), and **Security** (protects the authenticity of electronic communications).

Government applications include: income tax e-filing, e-tendering for public procurement, issuance of digital certificates, and passport services.

4.5 Cyber Law in E-Commerce and E-Governance

In **e-commerce**, cyber law provides legal recognition to online contracts, protects consumers from digital fraud, supports secure payment systems through digital signatures, and mandates data protection for customer information.

In **e-governance**, cyber law enables governments to deliver services digitally, reduce dependence on paper documentation, authenticate official communications using digital signatures, improve administrative transparency, and reduce operational costs.

4.6 Scanning Techniques

Scanning is the process of identifying active systems, open ports, running services, and potential vulnerabilities in a network. It is used by both security professionals (for auditing) and attackers (for reconnaissance).

Technique	Method	Purpose
Ping Sweeping	Sends ICMP Echo Requests to multiple IPs	Identifies which hosts are active on the network
Port Scanning	Probes TCP/UDP ports (SYN scan, connect scan)	Identifies open ports and running services
ICMP Scanning	Uses ICMP message types	Network mapping and host discovery
Active Fingerprinting	Sends crafted packets, analyzes responses	Identifies OS and software versions
Passive Fingerprinting	Observes existing traffic without sending packets	Identifies OS/software covertly

Unit 5 — Buffer Overflow and DoS Attacks

5.1 Buffer Overflow Attacks

A buffer overflow occurs when a program writes more data to a buffer than its allocated memory size can accommodate. The excess data overwrites adjacent memory locations, potentially allowing an attacker to inject and execute arbitrary malicious code. Buffer overflows are among the most common and dangerous software vulnerabilities.

Type	Memory Area	Cause	Primary Risk
Stack Overflow	Stack memory	Unsafe functions, excessive input data	Overwrites return address; enables arbitra
Heap Overflow	Heap (dynamic) memory	Errors in dynamic memory allocation	Corrupts heap structures; leads to system
Integer Overflow	CPU registers / variables	Arithmetic result exceeds variable storage capacity	Produces incorrect values; causes unexpe

5.2 Internal Attacks

Internal attacks originate from within an organization, typically carried out by employees or other authorized users who misuse their access privileges. Common forms include:

Email abuse — using organizational email to distribute spam, leak sensitive data, or deliver phishing messages. **Mobile phone misuse** — using work devices to exfiltrate data or introduce malware into the network. **Instant messenger threats** — distributing malware links or leaking confidential information through chat applications. **FTP upload abuse** — uploading unauthorized or malicious files to organizational servers. **Shoulder surfing** — physically observing another user entering credentials or accessing sensitive information.

Prevention measures include: employee security awareness training, strict access control policies, activity monitoring systems, and clearly defined acceptable use policies.

5.3 DoS and DDoS Attacks

A **Denial of Service (DoS)** attack is an attempt to make a system or service unavailable to legitimate users by overwhelming it with traffic or requests. A single system is used to conduct the attack.

A **Distributed Denial of Service (DDoS)** attack achieves the same objective but uses a large number of compromised systems — collectively called a **botnet** — to launch the attack simultaneously. DDoS attacks are significantly harder to detect and mitigate due to their distributed nature and massive traffic volume.

Feature	DoS	DDoS
Attack source	Single system	Multiple systems (botnet)
Detection difficulty	Easier to detect	Harder to detect and block
Scale	Smaller scale	Large scale

Traffic volume	Lower	Massive

5.4 DoS Attack Variants

Attack	Protocol	Mechanism	Effect
Ping of Death	ICMP	Sends ICMP packets exceeding 65,535 bytes	System instability upon receipt
SYN Flooding	TCP	Sends SYN requests without completing the three-way handshake	Exhausts server connection tables; legitima
Smurf Attack	ICMP	Spoofs victim's IP; sends ICMP broadcast to network	ICMP responses overwhelm the victim
UDP Flooding	UDP	Floods target with large volumes of UDP packets	Bandwidth and processing resource exhau

5.5 Mitigation Strategies

Effective mitigation against network attacks requires a layered approach: **Firewalls** filter unauthorized traffic at the network perimeter. **Intrusion Detection and Prevention Systems (IDS/IPS)** identify and block suspicious activity in real time. **Traffic filtering and rate limiting** reduce the impact of flooding attacks. **Load balancing** distributes traffic to prevent single-point saturation. **Patch management** closes known software vulnerabilities exploited by buffer overflow attacks. **Multi-factor authentication (MFA)** reduces the risk of unauthorized internal access. **Employee training** addresses the human element in internal attacks. **Regular data backups** ensure recovery capability following a successful attack.

5.6 IP Address Hiding and Tracing

Attackers use several techniques to conceal their origin IP address: **Proxy Servers** (routing traffic through an intermediary), **VPNs** (masking the real IP behind a VPN server address), **TOR Network** (routing traffic through multiple anonymizing nodes), and **IP Spoofing** (forging the source IP address in packet headers).

Investigators use the following techniques to trace attack sources: **Traceroute** (mapping the packet path between systems), **Packet Analysis** (examining captured packets for origin information), **Log Analysis** (reviewing server and firewall logs for suspicious entries), and **Network Monitoring** (tracking traffic patterns over time to identify anomalies).