Attack Vectors (Detailed Study)

Attack vectors are the paths, techniques, or mechanisms used by attackers to gain unauthorized access to systems, networks, or sensitive information. They describe **how an attack is delivered**, not the attack itself.

Understanding attack vectors is essential for designing effective security controls and defensive strategies.

1. Social Engineering Attack Vector

Definition

Social engineering is an attack vector that exploits human psychology instead of technical vulnerabilities to manipulate individuals into revealing sensitive information or performing unauthorized actions.

Why Social Engineering Works

- Humans trust authority and familiarity
- Emotional triggers override rational thinking
- Technical security controls are bypassed

Common Techniques

- Phishing (email-based deception)
- Smishing (SMS-based deception)
- Vishing (voice-based deception)
- Pretexting (fake scenarios or identities)
- Baiting (malicious incentives such as free USB drives)

Attack Flow

1. Attacker studies the target
2. Trust is established through impersonation
3. Victim performs the requested action
4. Sensitive data or access is obtained

Example

An attacker impersonates IT support and convinces an employee to share login credentials to “resolve an urgent issue.”

CIA Triad Impact

- Confidentiality: Credential disclosure
- Integrity: Account misuse
- Availability: Possible ransomware follow-up

Defensive Measures

- Security awareness training
- Verification procedures
- Multi-Factor Authentication

2. Wireless Attack Vector

Definition

Wireless attacks exploit vulnerabilities in Wi-Fi and wireless communication protocols to intercept, manipulate, or redirect network traffic.

Why Wireless Networks Are Vulnerable

- Shared communication medium
- Public and open networks
- Weak encryption or misconfiguration

Common Wireless Attacks

- Evil Twin (fake access point)
- Man-in-the-Middle attacks
- Packet sniffing
- Deauthentication attacks

Attack Flow

1. Attacker creates or targets a wireless network
2. Victim connects unknowingly
3. Traffic is intercepted or modified
4. Credentials or sessions are hijacked

Example

An attacker sets up a fake “Free Airport Wi-Fi” network to capture user credentials and session cookies.

CIA Triad Impact

- Confidentiality: Data interception
- Integrity: Session manipulation
- Availability: Network disruption

Defensive Measures

- Strong Wi-Fi encryption (WPA3)
- VPN usage on public networks
- Wireless intrusion detection

3. Insider Threat Attack Vector

Definition

An insider threat is an attack vector originating from individuals within an organization who have authorized access to systems or data.

Types of Insider Threats

- Malicious insiders (intentional harm)
- Negligent insiders (careless behavior)
- Compromised insiders (accounts taken over)

Why Insider Threats Are Dangerous

- Bypass perimeter defenses
- Appear as legitimate activity
- Difficult to detect

Attack Flow

1. Insider gains or already has access
2. Misuses privileges
3. Data is stolen, modified, or destroyed

Example

A disgruntled employee copies sensitive customer data before resigning.

CIA Triad Impact

- Confidentiality: Data exfiltration
- Integrity: Unauthorized modifications
- Availability: System sabotage

Defensive Measures

- Least privilege access
- User activity monitoring
- Audit logs and alerts

High-Value Exam Summary

- Social Engineering exploits human psychology
- Wireless attacks exploit insecure radio communication
- Insider threats exploit trusted access

One-Line Definitions

- Social Engineering: Manipulating people to bypass security
- Wireless Attacks: Exploiting insecure wireless networks
- Insider Threats: Security risks from trusted internal users

Revision chart 1 – Attack Vectors (How attacks enter)

Attack Vector	Entry Point	Typical Examples
Social Engineering	Human trust	Phishing, Vishing, Smishing
Network	Open services/protocols	DDoS, MITM
Web Application	Input fields & logic	SQL Injection, XSS
Credential-Based	Authentication systems	Brute Force, Credential Stuffing
Malware Delivery	File execution	Email attachments, USB
Wireless	Wi-Fi/Bluetooth	Evil Twin, Weak Wi-Fi
Insider	Authorized users	Data theft, sabotage

Revision chart 2 – Attack Types (What the attacks does)

Attack Type	Primary Goal	Core Action
Phishing	Steal credentials	Deception
Malware	Compromise system	Malicious code
DDoS	Disrupt service	Traffic flooding
SQL Injection	Manipulate database	Inject SQL
Brute Force	Crack accounts	Password guessing
Ransomware	Extort victim	Encrypt data

Revision chart 3 – Attack Vector vs Attack Type

Scenario	Attack Vector	Attack Type
Fake bank email	Social Engineering	Phishing
Malicious attachment	Malware Delivery	Malware
Traffic flood	Network	DDoS
Login bypass	Web Application	SQL Injection
Password guessing	Credential-Based	Brute Force
Encrypted files	Phishing + Malware	Ransomware