**Lernzettel 6: Kommunikationssicherheit**

**1. Bedrohungsmodell**

* **Netzwerke als Kommunikationsinfrastruktur:** Daten werden zwischen verteilten Knoten ausgetauscht, was verschiedene Risiken birgt.
* **Passiver Angreifer:** Überwacht den Datenverkehr, z.B. durch Mithören (Sniffing) oder Verkehrsanalysen, um Informationen zu gewinnen.
* **Aktiver Angreifer:** Manipuliert den Datenverkehr, z.B. durch Spoofing, Flooding oder Replay-Angriffe.

**Lernbrücke:** Während passive Angriffe auf Beobachtung beruhen, erfordern aktive Angriffe direkte Manipulationen, was sie oft riskanter, aber auch potenziell schädlicher macht.

**2. Sichere Tunnel**

* **Definition:** Ein sicherer Tunnel ist eine logische Verbindung zwischen zwei Endpunkten in einem unsicheren Netzwerk, die Vertraulichkeit, Integrität und Authentifizierung gewährleistet.
* **Schlüsselaustausch:** Häufig durch asymmetrische Kryptographie etabliert, gefolgt von der Verwendung symmetrischer Schlüssel für die verschlüsselte Kommunikation.

**Lernbrücke:** Sichere Tunnel bieten Schutz während der Übertragung, aber der Endpunkt bleibt potenziell anfällig, was zusätzliche Sicherheitsmaßnahmen erfordert.

**3. Prinzipien des Protokolldesigns**

* **Schichtenmodelle:** OSI- und TCP/IP-Modelle organisieren die Kommunikation in verschiedene Schichten, wobei jede Schicht spezifische Protokolle und Sicherheitsmaßnahmen implementiert.
* **Kryptographische Sicherheitsfunktionen:** Verschiedene Schichten implementieren spezifische Sicherheitsmechanismen, z.B. SSL/TLS auf der Transportschicht oder IPsec auf der Vermittlungsschicht.

**Lernbrücke:** Die Sicherheitsfunktionen in den unterschiedlichen Schichten sind komplementär und sorgen zusammen für umfassenden Schutz, von der Anwendung bis hinunter zur Netzwerkschicht.

**4. Transport Layer Security (TLS)**

* **Geschichte:** TLS entwickelte sich aus SSL und ist der heutige Standard für sichere TCP-Kommunikation.
* **Konzepte:** TLS basiert auf TCP und bietet zusätzlich Authentifizierung, Integrität und Vertraulichkeit durch kryptographische Verfahren.
* **Protokolle:** TLS verwendet das Record-Protokoll zur sicheren Übertragung und das Handshake-Protokoll zum Aushandeln von Verschlüsselungsparametern.

**Lernbrücke:** TLS sorgt dafür, dass die Kommunikation zwischen Client und Server verschlüsselt und sicher ist, was besonders wichtig ist bei sensiblen Datenübertragungen, wie sie im Web üblich sind.

**5. IP-Sicherheit: IPsec**

* **IPsec Protokoll:** Bietet Sicherheit auf der Vermittlungsschicht durch Authentication Header (AH) und Encapsulating Security Payload (ESP).
* **ESP-Modi:**
  + **Transport-Modus:** Schutz der Nutzdaten zwischen zwei Endgeräten.
  + **Tunnel-Modus:** Schutz des gesamten IP-Pakets zwischen zwei Gateways, oft verwendet in VPNs.

**Lernbrücke:** IPsec ermöglicht eine sichere Kommunikation auf der IP-Ebene, wobei die Wahl zwischen Transport- und Tunnelmodus davon abhängt, ob die Endgeräte oder nur die Gateways gesichert werden sollen.