ITS Summary (8 Seiten)

20. September, 2024; rev. 15. Januar 2025

Linda Riesen (rieselin)

1 Vorlesung 02

1.1 Grundbegriffe

- **Plaintext (p):** Unverschlüsselte Nachricht.
- **Ciphertext (c):** Verschlüsselte Nachricht.
- **Key (k):** Ver-/Entschlüsselungsschlüssel.

Work-Faktor: Anzahl der Versuche zur Entschlüsselung, mindestens 128 Bits (=AES Bit Key Length) gilt als sicher. $WF(X) = \sum_{k=1}^{n} kp_k$ und in Bits: $log_2 WF(X)$
CPU Key Brutforce: $3.4 * 10^9 cycles/sec.$ AES: 10 cycles/byte

1.2 Bekannte Hash Funktionen

Funktion	Hash Länge	Work Factor
MD5	128 bit	64 bit
SHA-1	160 bit	80 bit
SHA-2	224 - 512 bit	112 - 256 bit
SHA-3	224 - 512 bit	112 - 256 bit

1.3 Symmetrische Verschlüsselung

Secret Key Encryption: Ver-/Entschlüsselung mit demselben Schlüssel. Typen:

- Block Cipher: Nachricht in Blöcke.
- Stream Cipher: Bitweise Verschlüsselung.

1.4 AES und Modi

AES verwendet Schlüssellängen von 128, 192 und 256 Bit. Modus-Empfehlungen:

Mode	Empfehlung
ECB	Unsicher
CBC	Unsicher
CTR	Unsicher
CCM	Verwendbar
GCM	Bevorzugt

1.5 Public Key Kryptographie

- Klassische Algorithmen: 4096 bit Schlüssel.
- Elliptische Kurven: 256 bit Schlüssel.

Perfect Forward Secrecy schützt Session Keys.

1.6 Diffie-Hellman und RSA

RSA Verschlüsselung: $c = p^e \mod n$; Entschlüsselung: $p = c^d \mod n$. **Diffie-Hellman**: Schlüsselaustausch. **RSA**: Verschlüsselung und Signaturen.

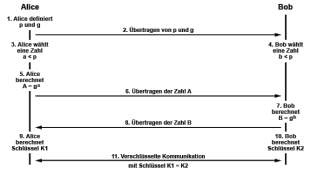


Abbildung 1: Diffie-Hellman

2 Vorlesung 03

2.1 Authentication of Public Keys

Zertifikate authentifizieren öffentliche Schlüssel, ausgestellt von Certification Authorities (CAs).

2.2 Types of Certificates

- TLS-Zertifikate: Domain- und Organisationsvalidierung.
- Code Signing und Client-Zertifikate.

2.3 X.509 Standard

Primärer Zertifikatsstandard, definiert mit ASN.1.

2.4 Certificate Transparency

- Logs: Öffentlich auditiert.
- Monitors: Verdächtige Zertifikate melden.

2.5 Certificate Revocation

Zertifikate können über CRLs oder OCSP zurückgerufen werden.

2.6 Certificate Validation Algorithm

- Prüfen der Kettenbeziehung und Validierung der Signaturen.

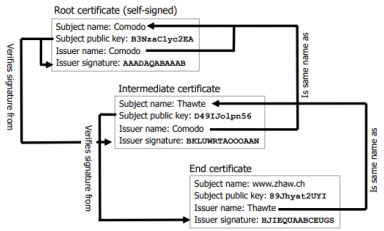


Abbildung 2: Certificate Chains

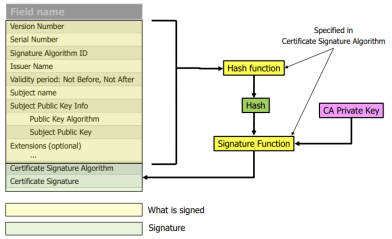


Abbildung 3: Structure of X.509

3 Vorlesung 04

3.1 TLS Overview

TLS sichert Kommunikation und wird für HTTPS, E-Mail, etc. verwendet.

3.2 TLS 1.3 Building Blocks

Verwendet AES, Diffie-Hellman und Zertifikate.

3.3 TLS Phases

- Handshake: Schlüssel und Algorithmen aushandeln.
- Data Exchange: Sichere Datenübertragung.
- Teardown: Sichere Beendigung.

3.4 Session Resumption

Verwendet Pre-shared Keys zur Reduktion der Serverlast.

3.5 TLS Data Exchange

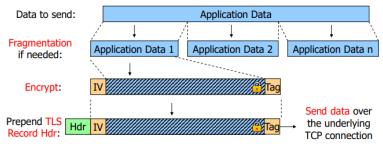


Abbildung 4: TLS Records from Application Data

- Verschlüsselt und authentifiziert mit AEAD Ciphers.
- Verwendet Sequenznummern für Integrität.

3.6 TLS Teardown

Beendet Sessions mit einem `close_notify` Alert.

3.7 DTLS (Datagram TLS)

- TLS für UDP, fügt Sequenznummern und Zuverlässigkeit hinzu.
- Unterstützt Replay Detection.

4 Vorlesung 05

4.1 Secure Communication Protocols

- Ziele: Vertraulichkeit, Integrität, Authentizität (plus Nichtabstreitbarkeit, Anonymität).
- Kryptografische Methoden verwenden, etablierte Protokolle bevorzugen.

4.2 Encryption and Authentication at Layer 2

Encryption

- Schützt kabelgebundene (zusätzliche Verteidigung) und drahtlose (notwendig) Netzwerke.

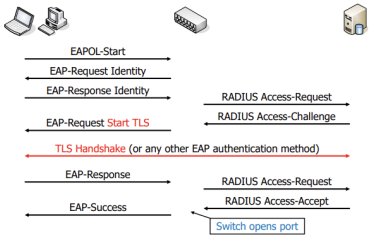


Abbildung 5: Port-Based Access Control

Authentication

- Sicherstellt, dass nur autorisierte Benutzer auf das Netzwerk zugreifen.
- Verwendet EAP (RFC 3748) für die Authentifizierung.

4.3 IEEE 802.1X Access Control

- Verhindert unbefugten Zugriff auf das Netzwerk.
- Delegiert Authentifizierung an einen RADIUS-Server via EAP.

4.4 MACsec (IEEE 802.1AE)

- Verschlüsselt und authentifiziert alle Layer-2-Traffic.
- Schützt physische und virtuelle Verbindungen.

4.5 IEEE 802.11 WLAN Security

Concerns

- Einfache Paketanalyse, Authentifizierung erforderlich.

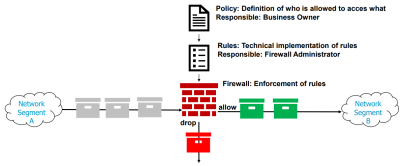


Abbildung 7: Packet Filtering Firewalls

Security Evolution

- WEP: Unsicher aufgrund von Designfehlern. (Uses Static Key = easily guessable)
- WPA/WPA2: Stärkere Verschlüsselung (CCMP empfohlen). Uses Radius server
- WPA3: Aktueller Standard.

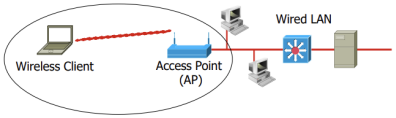


Abbildung 6: Typical WLAN Usage Scenario

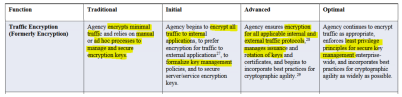
5 Vorlesung 06

5.1 Network Segmentation

- Goals: Improve performance, limit attack damage, protect devices, reduce compliance scope, and limit insider attacks.

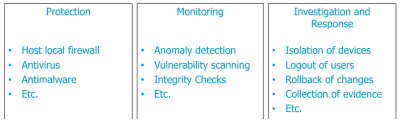
5.2 Zero Trust

- Principles: Verify everything, enforce least privilege, monitor security.



Function	Traditional	Initial	Advanced	Optimal
Traffic Encryption (Formerly Encryption)	Agency encrypts minimal traffic and relies on manual or ad-hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications[37], to formalize key management policies, and to secure server-service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols.[38] It manages certificates and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.[39]	Agency continues to encrypt traffic as appropriate, enforces least privileged principles for secure key management enterprise-wide, and incorporates best practices for cryptographic agility as widely as possible.

Abbildung 8: CISA Zero Trust Maturity Model



5.3 Device Protection

- Use local firewalls and Endpoint Detection and Response (EDR).

5.4 Application-Level Protection

- Web Application Firewalls (WAF) protect against XSS, SQL injection, and require TLS termination.

5.5 Prohibiting Malicious Sites

- Secure Web Gateway (SWG): URL filtering, Data Leakage Prevention, TLS inspection.

5.6 Cloud Protection

Cloud Access Security Broker (CASB)

- Capabilities: Shadow IT Discovery, Cloud Usage Control, DLP, Anomaly Detection.
- Methods: API scanning, forward/reverse proxy.

5.7 Attack Detection

- Network Detection: Monitors traffic, detects anomalies, analyzes incidents.
- NDR: Automates responses (e.g., firewall updates, isolating devices).

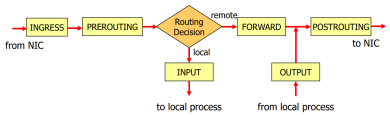


Abbildung 9: Netfilter and the Linux Kernel

- SIEM: Correlates logs for malicious activity, central dashboard, compliance reports.
- SOAR: Extends SIEM with more sources and automation.

5.8 Linux Packet Filtering

- `netfilter` and `nftables`: Support filtering, NAT, and packet manipulation.

5.8.1 Port Scanning

- Determines services on a host (e.g., nmap).
- Techniques: TCP connections, UDP scans, ICMP responses.

6 Vorlesung 07: Distributed Denial of Service (DDoS) Angriffe

DoS: Angriff auf Verfügbarkeit, hindert legitime Nutzer.
DDoS: Angriff von vielen Rechnern gleichzeitig.

6.1 DDoS Attack

Ziel: Überlastung eines Netzwerks oder Dienstes durch massiven Datenverkehr, oft mit Botnets. Typen:

- **Volumetric**: Bandbreitenverbrauch.
- **Protocol**: Ressourcenauslastung.
- **Application Layer**: Legitim wirkender Verkehr, schwer zu erkennen.

6.2 DDoS Botnet

Netzwerk infizierter Geräte (*Bots*), die koordiniert Traffic generieren, um Ziele zu überlasten.

6.3 Häufigste Attacktypen

- **SYN Flood**: Ausnutzen des TCP-Handshakes durch unvollständige Verbindungen, Ressourcenauslastung.
- **DNS Amplification**: Verstärkter Traffic durch öffentliche DNS-Server, Spoofing der Ziel-IP.
- **Application Layer DDoS**: Spezifische Angriffe auf Webanwendungen (z.B. HTTP-Anfragen), schwer erkennbar.

6.4 Schutz vor DDoS

Strategien: Firewall, Lastverteilung, Netzwerkredundanz, DDoS-Schutzdienste, aktuelle Infrastruktur und Notfallpläne.

6.5 Gegenmaßnahmen

- **Blackhole Routing**: Leitet unerwünschten Traffic ins Leere.
- **Traffic Filtering und Rate Limiting**: Reduziert Angriffsintensität.
- **CDNs**: Verteilen Anfragen, reduzieren Last.

7 Vorlesung 08: Virtual Private Network (VPN)

VPN: Private (geschützte) Kommunikation über öffentliche Netzwerke durch Kryptographie.

7.1 Nutzung

- Sichere Verbindung zwischen Firmennetzen.

- Zugriff für Partner oder Kunden auf interne Dienste.
- Mobiler Zugriff von Mitarbeitern auf das Firmennetz.

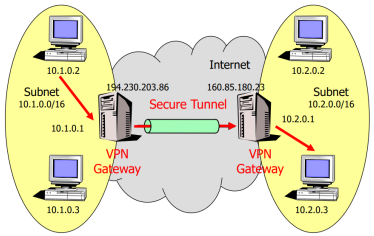


Abbildung 10: VPN Connection

7.2 VPN Protokolle

Offene Standards: Ermöglichen Interoperabilität verschiedener Produkte.

7.2.1 IPsec

- Arbeitet auf Netzwerkebene (Layer 3).
- Bietet Vertraulichkeit, Authentifizierung und Integrität.
- Unterstützt Key-Exchange (IKE) mit Public Key oder PreShared Secrets.
- Schutz: Authentifizierte, verschlüsselte IP-Pakete (**ESP**).

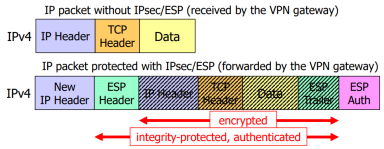


Abbildung 11: IPSec with Tunnel Mode

7.2.2 OpenVPN

- Schlankeres Protokoll, läuft im User-Space.
- Nutzt TLS für Authentifizierung und Schlüsselaustausch.
- Anwendungsschicht-Tunnel über UDP/TCP.

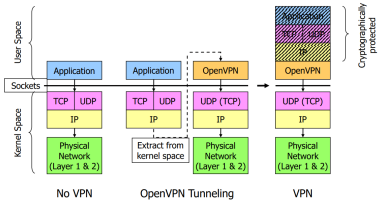


Abbildung 12: Open VPN Protocol Stack

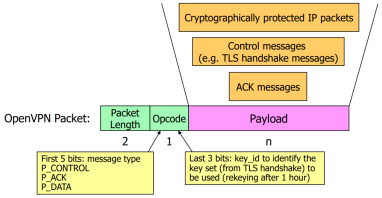


Abbildung 13: Open VPN Packet Format

7.2.3 Vergleich: IPsec vs. OpenVPN

- Beide sind sicher.
- **IPsec:** Professioneller, mehr kommerzielle Produkte.
- **OpenVPN:** Einfacher, läuft im User-Space.

7.2.4 WireGuard

- Layer-3-Protokoll, schlanke Konfiguration.

- Moderne Kryptographie (ChaCha20, Curve25519).
- Kleinere Angriffsfläche, PFS, DoS-Schutz.
- 1-RTT Handshake.

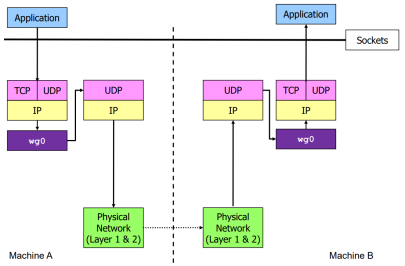


Abbildung 14: WireGuard Message Flow

8 Vorlesung 09: Pentesting

Abbildung 15: Tests compared

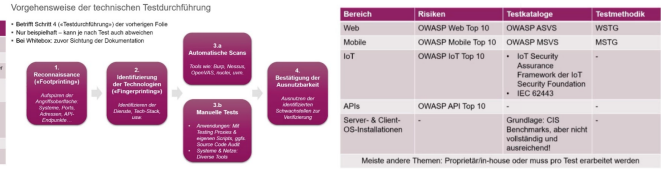


Abbildung 16: Vorgehen Technische Durchführung

Abbildung 17: Risiko Standards

Pentesting reduziert Risiken, eliminiert sie jedoch nicht.

8.1 3 Common Vulnerabilities

XSS: Script-Injection, Abwehr durch Sanitizing/Encoding.
SQL Injection: Schutz durch Parameterized Queries.
IDOR: Unvorhersehbare UIDs, Zugriffslogik nutzen.

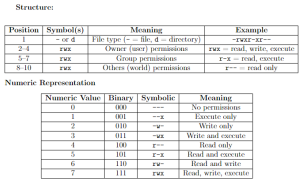


Abbildung 19: Linux Access Control

8.2 Best Defense Tips

Least privilege, Zero Trust, Defense in Depth, sichere Programmierung, Reduktion von Komplexität/Angriffsfläche.

9 Vorlesung 10 + 11

Abbildung 18: Access Control Components

- **Authentication** Faktoren: Wissen, Besitz, Identität. Passwörter gelten als schwach.
- **Password Defense Tips** MFA, Passwortmanager, lange Passwörter, keine E-Mails, gesalzene/gehashte Speicherung.
- **Precompiled Dictionary Attacks** Wörterbuchangriffe mit Variationen, Schutz durch Salt/Pepper/Key Stretching (z.B. bcrypt, Argon2).

9.1 Multi-Factor Authentication

Phishing anfällig, aber zusätzlicher Schutz.

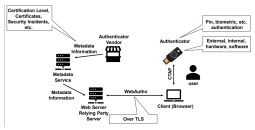


Abbildung 20: FIDO2

Abbildung 21: MFA Fatique

Password-less Authentication Biometrie für kryptographischen Schlüssel, SSO für mehrere Apps (z.B. FIDO2).
User Authentication Protocols Direkte und indirekte Authentifizierung (z.B. Kerberos, OAuth 2.0).

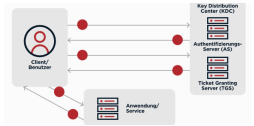


Abbildung 22: Kerberos Ablauf

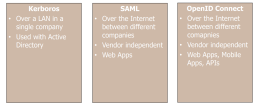


Abbildung 23: Three Main User Auth Protocols

10 Vorlesung 12: Access Control Models

	Based on	Models	Rules made by	Configured by	Enforced by
DAC	identity *e.g., computer, user, group*	no standard model (OS specific impl.) *ACLs and capabilities are two different approaches to DAC*	owner *typically restricted by (un)written policies/guidelines*	owner *administrator has the power to override*	OS
MAC	security level *e.g. (unclassified, restricted, secret, top secret)*	•Windows MIC (label-based) •SE Linux (label-based) •AppArmor (name-based)	security officer	admin(s) *labels and rules*	OS
RBAC	role *e.g., job function*	INCITS 359:2004: •Core RBAC •Hierarchical RBAC •Constraint RBAC Non-standard: •SELinux •Java EE	Business/security officer	application or OS admin(s)	RBAC System *transparent such as in SELinux or application-aware such as in RBAC enabled applicati*

Abbildung 24: Access Control Models

10.1 Access Control Models

DAC: Nutzer kontrollieren Zugriffe.
MAC: Systemweite Regeln (nur Admins änderbar).
RBAC: Rollenbasierte Rechte, natürliche Definition.
ABAC: Attributbasierte Kontrolle (z.B. Zeit, Ort).

Begriff	Definition*
Datenschutz	Wahrung der Persönlichkeitsrechte von betroffenen Personen bei der Bearbeitung von Personendaten
Datensicherheit	Technische und organisatorische Massnahmen zur Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten sowie der Nachvollziehbarkeit
Bearbeitung	Jeder Umgang mit Personendaten wie z.B. Beschaffung, Aufbewahrung, Verwendung, Umarbeitung, Bekanntgabe, Archivierung und Vernichtung, unabhängig von angewandten Mitteln und Verfahren
Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen
Betroffene Person	Alle natürlichen Personen, über die Daten bearbeitet werden
Verantwortlicher	Privater oder Bundesorgan, der oder das allein oder mit anderen über Zweck und Mittel einer Bearbeitung entscheidet

*Definitionen gemäss Art. 5 des Schweizer Datenschutzgesetzes (DSG)

Abbildung 25: Datenschutz Begriffe

10.2 Security Policy

Effizientes Rechtemanagement, Informationssicherheit und Compliance.

11 Vorlesung 14

DSGVO anwendbar in den EU- und EWR-Staaten (EWR = Europäischer Wirtschaftsraum (z.B. Fürstentum Liechtenstein, Norwegen, Island))

Gemäss Art. 3 DSGVO ebenfalls anwendbar auf Unternehmen:

- mit Niederlassung oder Auftragsverarbeiter in der EU
- welche Personen in der EU Waren oder Dienstleistungen anbieten (auch kostenlos)
- welche das Verhalten von Personen in der EU beobachten (z.B. via Tracking auf Websites)