IT-Sicherheit – Sicherheit vernetzter Systeme

Vorlesung im Wintersemester 2023/2024 (LMU)

08.02.2024
WS 2023/2024

Organisatorisches
Klausur

- Termin
  - **26.02.2024, 15 - 18 Uhr**
  - **KEINE Nachholklausur**
- Anmeldung verpflichtend über Moodle
  - ab 01.02.2024
  - **spätestens bis** Fr. 18.02.2024
- Präsenzklausur - Closed Book
- Räume am Campus Großhadern
- Details warden via Moodle bekannt gegeben

Wdh: Grundlagen

- Ziele der Informationssicherheit
  - Vertraulichkeit (Confidentiality) → Schutz vor unbefugter Offenlegung
  - Integrität (Integrity) → Übereinstimmung, Korrektheit, Vollständigkeit
  - Verfügbarkeit (Availability) → Fehlertoleranz, Robustheit, …
  - Verbindlichkeit → Authentizität, Revisionsfähigkeit, Beherrschbarkeit
- Kategorisierung von Sicherheitsmaßnahmen
  - Organisatorisch / technisch
  - Prävention / Detektion / Reaktion

Wdh: Grundlagen

- Technik & Organisation - ISO/IEC 27000
  - Grundprinzipien des Qualitätsmanagement für Management der Informationssicherheit
  - ISO/IEC 27001 legt „Mindestanforderungen" an ein ISMS fest
  - Risikomanagement:
    (Identifikation, Analyse, Bewertung von Risiken + Behandlung z.B. durch Maßnahmen)
  - Kontinuierliche Verbesserung

Wdh: Grundlagen

- Angreifermodell?
- Angriffsarten? (aktiv, passiv, Social Engineering)
- Angriffe, die im Rahmen der VL behandelt wurden?
  - DoS/DDoS (Smurf, DNS/SNMP/NTP Amplification, …)
  - Malicious Code (Viren, Würmer, Trojanische Pferde, Rootkits)
  - Buffer Overflows
  - XSS
  - Portscans, Sniffing
  - Social Engineering

Wdh: Rechtliche Grundlagen

- "Antragsdelikt" vs. „Offizialdelikt"
- Wichtige Paragraphen:
  - §202a (Ausspähen von Daten)
  - §202b (Abfangen von Daten)
  - §202c (Vorbereitung des Abfangens oder Ausspähen von Daten, "**Hackerparagraph**")
  - §303a (Datenveränderung)
  - §303b (Computersabotage)

Wdh: Rechtliche Grundlagen

- Datenschutz, u.a. EU-DSGVO
  - Informationelle Selbstbestimmung?
  - Grundprinzipien im Datenschutz?
    - Verbot mit Erlaubnisvorbehalt (Rechtsgrundlage oder Einwilligung)
    - Datensparsamkeit
    - Zweckbindung
    - Transparenz
  - EU-DSGVO: Informations-/Auskunftspflichten, Sicherheit in der Verarbeitung, **Melden von Datenschutzvorfällen, Datenschutzfolgenabschätzung,** Privacy by design, AV-Vereinbarungen

Wdh: Kryptographie

- Kryptographische Methoden
  - Symmetrisch / Asymmetrisch ((DES, 3DES), **AES / RSA**, …)
  - Block- / Stromchiffren (DES, AES / RC_4 → WEP)

- ~~(Data Encryption Standard (DES)~~
  - ~~Initialpermutation (IP) des 64 – Bit Input-Blocks~~
  - ~~**16** schlüsselabhängige Iterationen (Funktion f)~~
  - ~~Inverse Initialpermutation (IIP)~~
  - ~~DES-Funktion f? → Phasen/Ablauf?~~
  - ~~Entschlüsselung? Prinzipiell gleich, Schlüsselreihenfolge umgekehrt)~~

- RSA: Verschlüsselungsexponent e meist gegeben. Wie errechnet sich zugehöriges d für Entschlüsselung?

Wdh: Kryptographie

- Konfusion?
  → Vom Chiffretext kann möglichst wenig auf den Klartext geschlossen werden
- Diffusion?
  → Kleine Änderungen im Klartext große Änderungen am ausgegebenen Chiffretext
- Feistel-Chiffre? Ist AES also eine Feistel-Chiffre?
- ECB vs. CBC?

Wdh: Kryptographische Hashfunktionen

- Hashfunktionen injektiv? → Nein! → Kollisionen sind möglich!
- Wahrscheinlichkeit > 0,5 für Kollision → 2^{k/2}
- ~~Konstruktion kryptog. Hash-Funktionen (Merkle-Damgard-Prinzip?)~~
  - ~~Kompressionsfunktion G~~
  - ~~Klartext m wird in Blöcke M_i zerlegt~~
  - ~~Hashverfahren vorbelegt mit IV~~
  - ~~Letzter Block mit ggf. auf vorgegebene Länge aufgefüllt werden (Padding)~~
  - ~~Kompressionsfunktion? → DES, Dedizierte Hash-Funktionen~~

Wdh: Authentisierung

- Biometrie
  - Fehlerarten? False Acceptance Rate / False Rejection Rate / Crossover ErrorRate
- Datenursprung? Verschlüsselung, Dig. Signatur, MAC, HMAC
  - Verschlüsselung? Symmetrisch vs. asymmetrisch?
  - Dig. Signatur: Auth. ja, Signatur kann jeder verifizieren, Bob nicht auth.
  - Hash-Fkt. mit Geheimnis S
  - MAC = A(M, K), A = Algorithmus, M Klartext, K Schlüssel nur Alice/Bob bekannt
  - Hashed MAC ? Warum? Hashes schneller als z.B. DES, aber verwenden keinen Schlüssel → HMAC

Wdh: Needham-Schröder

- Trusted Third Party *Trent*
- Verwendet i.A. symmetrische Verschlüsselung
- Trent teilt mit jedem Kommunikationspartner eigenen Schlüssel
- Alle Schlüssel bleiben gültig → Schritt 3 **Replay Attack** → Sequenznummer, Timestamps, Gültigkeitsdauer beschränken

Wdh: Kerberos & Access Control & Zertifikate

- Kerberos? → Ablauf im VL Skript / Übung
- Zugriffskontrollstrategien:
  - Mandatory Access Control → **Systemglobal**, Regelbasiert → Bell-LaPadula
  - Discretionary Access Control → Eigentümerprinzip
  - RBAC → Rollen statt Subjekte (Vorteile?)
- Referenzmonitor?
- **Zertifikate? Inhalt? Aufgaben einer CA? CA Hierarchie/Cross-Zertifizierung?**

Wdh: Netzsicherheit / Data Link Layer

- Schicht 1: VPWS (Punkt zu Punkt), VPLS (Punkt zu Multipunkt)
- Schicht 2/3/4:
  - VLAN: Broadcast-Domains über selben phys. Link
  - **VLAN-Tagging** → VLAN-Tag definiert Broadcast-Domain!
  - VLAN-Tag (32-Bit)
    - Tag Protocol Identifier (TPID): 0x8100
    - Priority (3 Bit) → Übertragungssteuerung z.B. Video-/Telefonie
    - Canonical Format Indicator: bei Ethernet 0
    - VLAN-ID: 12 Bit → 0 und 0xFFF reserviert → 4094 VLANs möglich
- PPP (Point to point protocol)
  - Verbindungsaufbau über Wählleitungen (DSL, ISDN, …)
  - Link Control Protocol / Network Control Protocol (→ Schicht 3), d.h. über PPP-Link verschiedene Schicht-3 Protokolle möglich
  - Auth optional → kann in LCP ausgehandelt werden (PAP, CHAP, EAP)

Wdh: PAP, CHAP, EAP

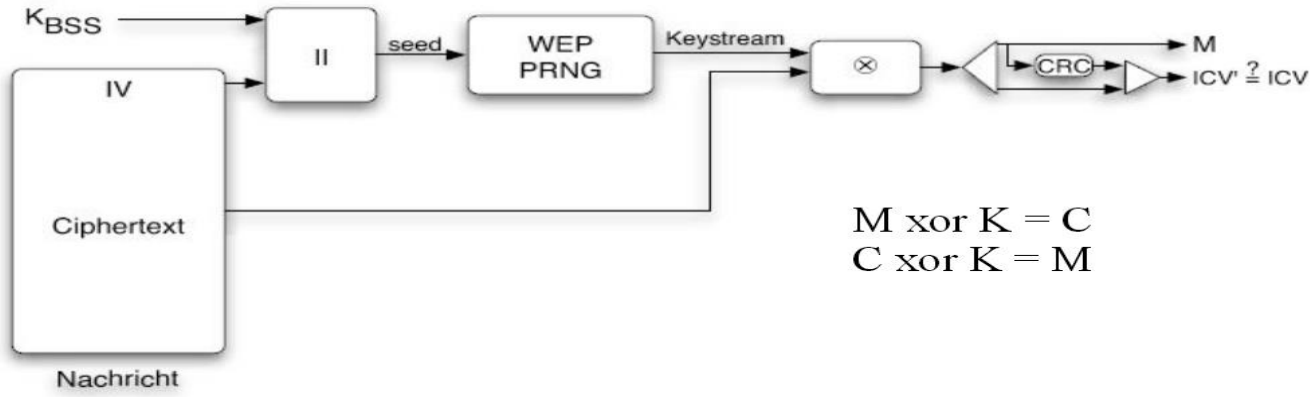
- PAP = Password Authentication Protocol
  - Authentisierende Entität kennt ID und Passwort aller Clients
  - Client wird über LCP zur Auth via PAP aufgefordert
  - Client schickt ID und Passwort im Klartext (→ keine Verschlüsselung)
  - Server schickt ACK zurück
- CHAP = Challenge-Handshake Authentication Protocol
  - Basiert auf gemeinsamen Geheimnis (Passwort) K_AB
- **EAP = Extensible Authentication Protocol**
  - Auth-Framework: EAP-MD_5, … EAP-OTP, **EAP-TLS**

Wdh: PPTP, MS-CHAP v1/v2, 802.1X

- PPTP = Point-to-Point Tunneling Protocol
  - PPP nur direkt verbundene Systeme
  - PPTP = PPP über Internet
  - Transport von PPP PDUs in IP-Paketen gekapselt mit Generic Router Encapsulation Protocol (GRE)
- MS-CHAPv1
  - C → S (Login Request)
  - S → C (Challenge C)
  - C → S (DES (K_L, C), DES (K_N, C)) K_N|K_L Hash (LAN-Manager, NT-Hash)
  - S → C (success/failure)
- **802.1X → Port-based Network Access Control**

Wdh: WLAN - WEP

- WEP:
  - Klartext M || CRC(M) mit Bitstrom **XORen**
  - Bitstrom mittels RC_4 (WEP PRNG)
  - Initialisierungsvektor IV (**24 Bit**) + 40 Bit Schlüssel → Seed für PRNG



M xor K = C
C xor K = M

Wdh: WLAN - WPA

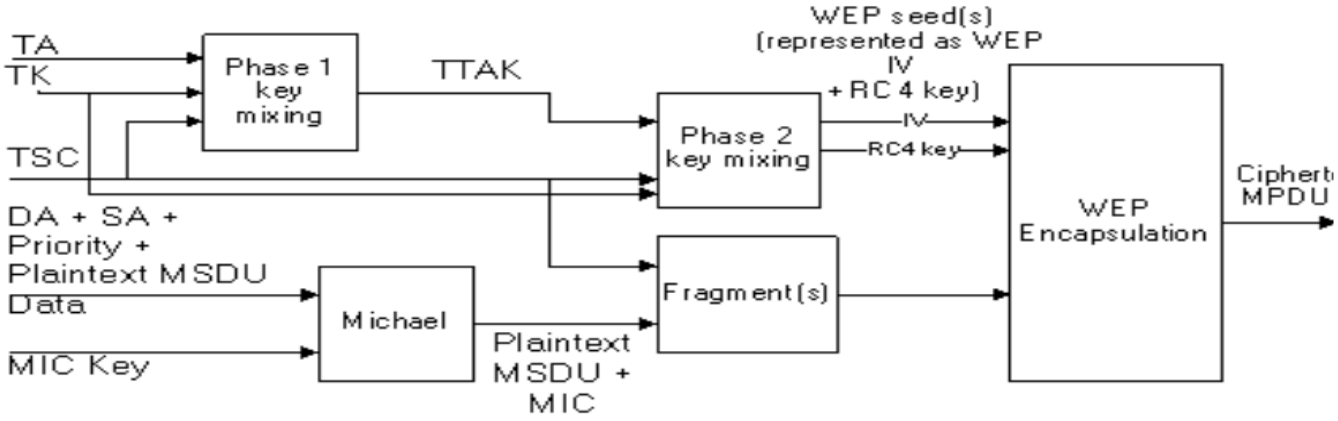
WPA:

- Vertraulichkeit: → TKIP, Rekeying, Hierarchie von Schlüsseln
- Integrität: → MICHAEL
- Authentisierung: → Preshared Key (PSK), aber auch 802.1X

- TKIP Schlüsselhierarchie:
  - Temporal Key (AP → STA, STA → AP)
    - Rekey key Message enthält Material damit STA und AP ableiten können
  - Pairwise Transient Key (PTK)
    - Sichern Übertragung temporärer Schlüssel
    - 1 Schlüssel zur Sicherung Schlüsselmaterial
    - 1 Schlüssel zur Sicherung rekey key Nachricht
  - Pairwise Master Key (PMK)

Wdh: WLAN - WPA

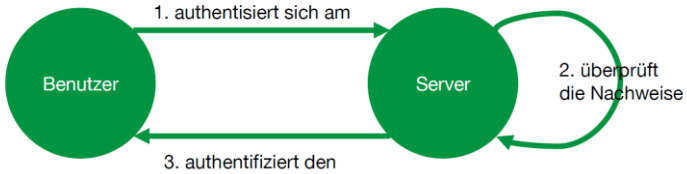
- WPA (Verschlüsselung)



Aufgabe 1: (T) Zutrittskontrolle
(c) Aus welchen Verfahrensschritten besteht die ZuKo?

1. **Authentisierung**
   Vorlegen eines Nachweises zur Echtheit eines Attributes
   → welche Arten von Nachweisen gibt es?

2. **Authentifizierung**
   Überprüfen des vorgelegten Nachweises



3. **Autorisierung**
   Überprüfen, ob das (nachweislich echte) Attribut ausreicht, um das angefragte Recht/Zutritt unter den gegebenen Umständen (Uhrzeit etc.) zu erlangen

⚠ Spoiler: Kapitel 10