isec 2024: Fragestunde

2025W03

Netzzugangssicherheit

Org: Blockwoche und dann

5 Tage:
W06: 2025-02-06..-07 (Do/Fr)
W07: 2025-02-11..-13 (Di/Mi/Do)

Block Termine für FG am Do 2025-02-13
(FG = Fachgespräch, hier keine mündlichen Prüfungen (MP))
➔ Für Gruppen, die Aufgaben gern etwas früher abgeben

Weitere FGe ab Ende Februar (2025-02-27)

Blockwoche: FGe am Do 2025-02-13?

Chance: Dann auch mit allem fertig sein!

Voraussetzung:
1. Vor der Blockwoche auf FG vorbereitet sein
2. Aufgabe in der Blockwoche etwas früher abgeben

Do 06	Fr 07	Sa 08	So 09	Mo 10	Di 11	Mi 12	Do 13
X	X				X	X	X
X	X				X	X	FG

Dann bitte einen der Termine am 2025-02-13 buchen

Netzzugangssicherheit

- ~ 1950er: Physische Sicherheit
- ~ 1970er: Login/Passwort
- ~ 1990er: Netzzugang absichern
  - Modem: PPP, EAP, RADIUS
  - Ethernet: 802.1X (2001)
  - WLAN: ???

Ziele Netzzugangssicherheit

- Knappe Ressourcen schuetzen?
- Perimeter-Sicherheit
  - Poor Man's Authorization?

Besonderheiten WLANs

- Leicht abzuhoeren
- Keine Demarkation in "Leitungen"

Sicherheitsziele Uni:

- Vertraulichkeit der Daten und Metadaten
- Zurechenbarkeit
  - Voraussetzung: Authentisierung

Ansätze Netzsicherheit WLANs

- Perimeter-Ansatz (L2)
  - Ausbau der Portsicherheit (802.1X)
  - Authentisierung mit EAP
  - Schlüsselvereinbarung Client/AP
- VPN-Ansatz (L3)
  - Authentisierung und Schlüsselvereinbarung mit Zielnetz via VPN-Protokoll
- kombinierbar!

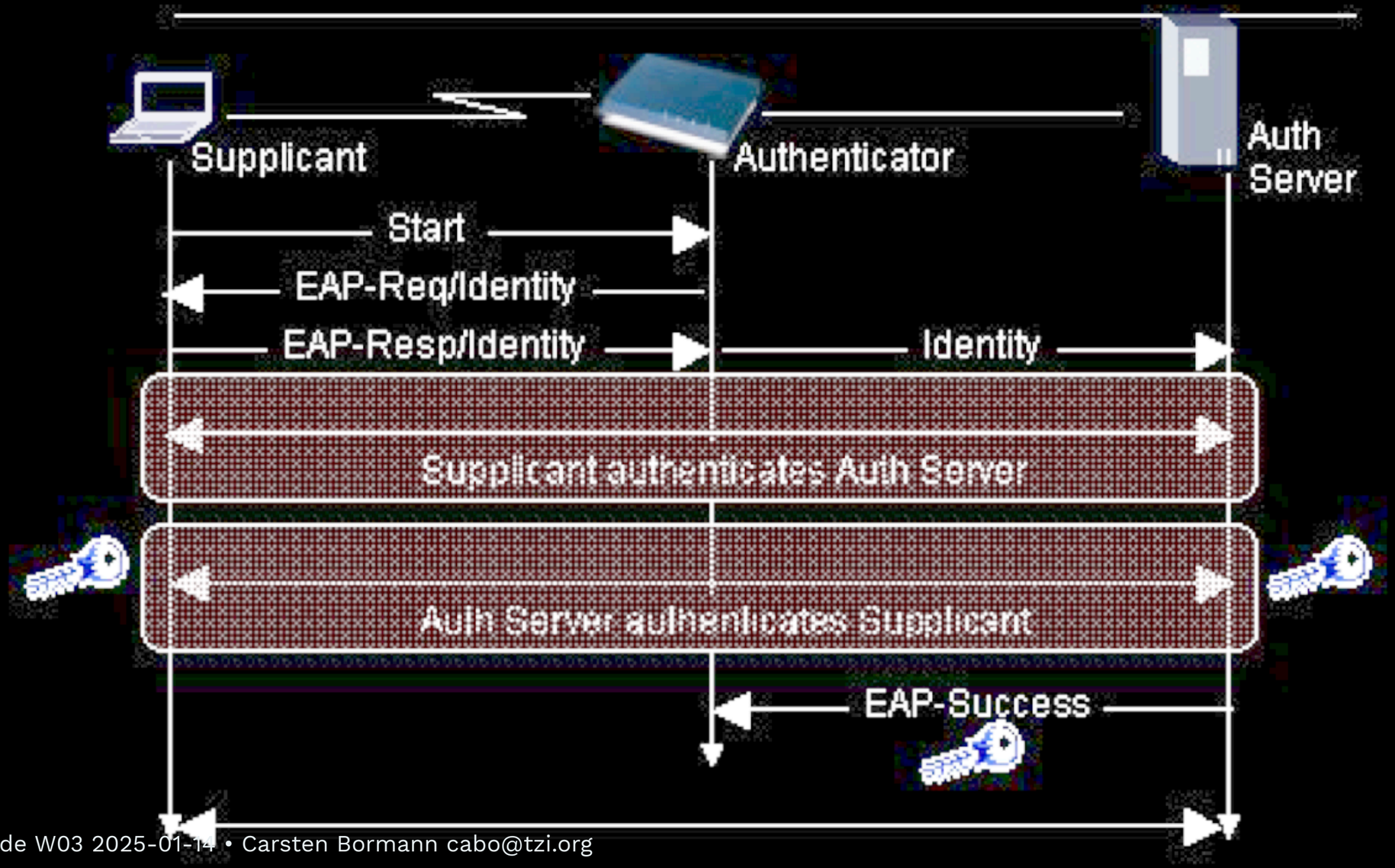
Nicht wirklich Sicherheit 💀

- Netzzugang: Web Diverter
  - ~ MAC als Passwort
- Verbergen der SSID
  - Bringt sehr wenig
- MAC als Passwort
  - Unsicher (leicht abzuhören)
  - Komplexer Betrieb
  - Durch MAC-Randomisierung veraltet

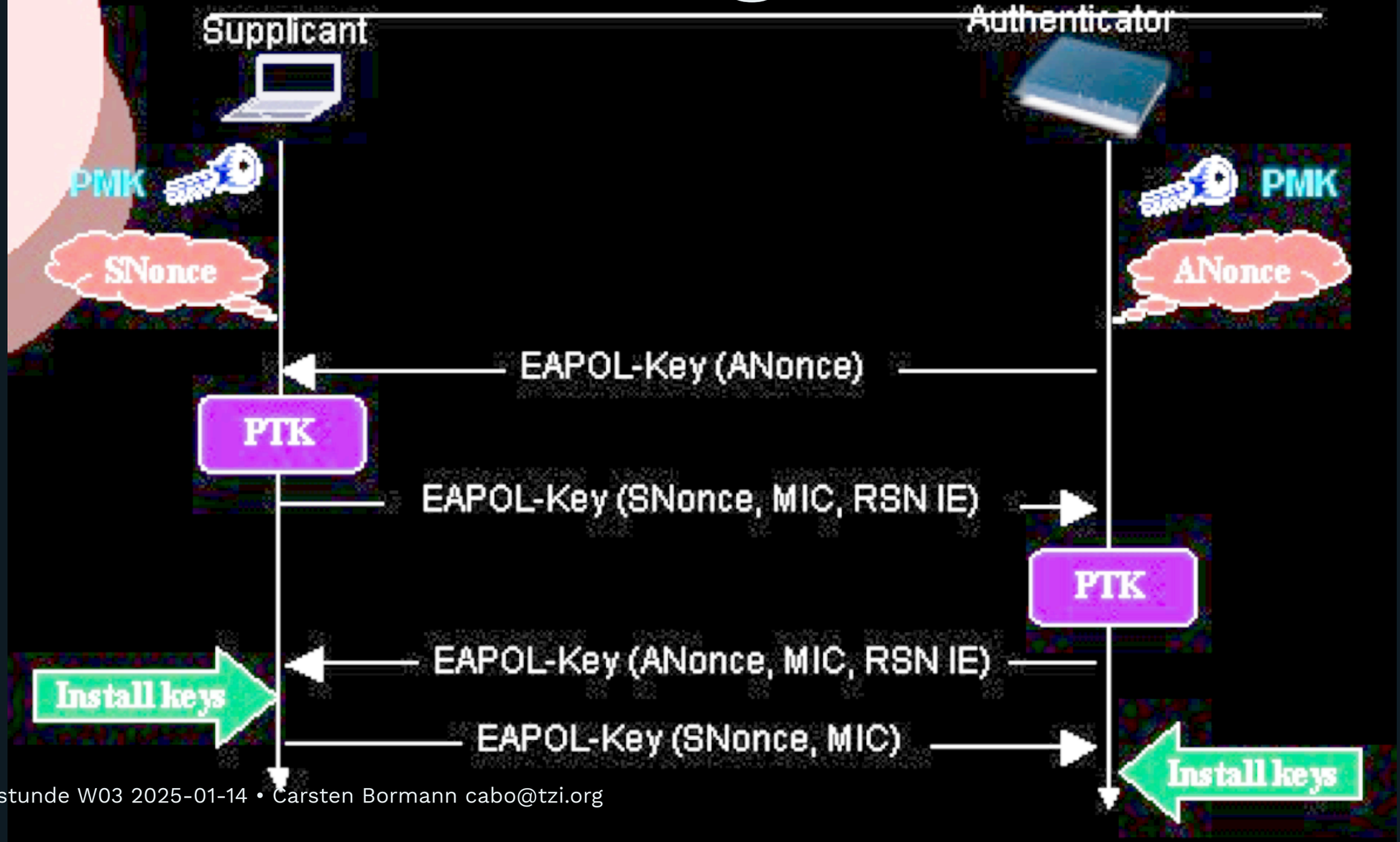
Historie WLAN-Sicherheit

- WEP
  - "Export-Krypto"
  - Krypto veraltet
- WPA (ohne 2)
  - WEP-Kompatibel (~ 2004?)
  - Nicht mehr nötig
- WPA2
  - PSK
  - "Enterprise" (EAP)
- WPA3
  - Modernere Algorithmen
  - SAE (~ RFC 7664), PMF, OWE (RFC 8110)

WPA(2) Enterprise (EAP over WLAN)



WPA(2) 4-way handshake



WPA(2) Group Transient Key

- IEEE 802.11: Broadcast von AP to Station
- Braucht gemeinsamen Schlüssel
  - Bisher nur pairwise key
- Group Transient Key (GTK)
  - AP ➔ Sta, sobald pairwise key da
  - nach jeder Dis-Assoziierung neu!
  - WEP Key-ID für rollover

WPA3

— Chance zur Modernisierung; Modernere Algorithmen

— SAE (Dragonfly ~ RFC 7664), PMF, OWE (RFC 8110)

SAE

Woher PMK (Pairwise Master Key)?
WPA(2)-PSK: unmittelbarer Einsatz des Passworts

WPA3: SAE — Simultaneous Authentication of Equals
PAKE: Password-Authenticated Key Establishment
(… Agreement, … Exchange)
SAE ~ Dragonfly (RFC 7664, Independent Submission)

PMF

PMF: Protected Management Frames

OWE

OWE: Opportunistic Wireless Encryption (OWE) (RFC 8110)
Unauthentisierter Diffie-Hellman (FFC/ECC)
"no-hassle advanced cryptography" (Dan Harkins)

1. PMK ist ephemer [✔]
2. MITM bleibt möglich (via Rogue AP, "Evil Twin") [✗]

➔ Wi-Fi CERTIFIED Enhanced Open™