W-LAN - Sicherheit

Cornelia Mayer
Andreas Pollhammer
Stefan Schwarz

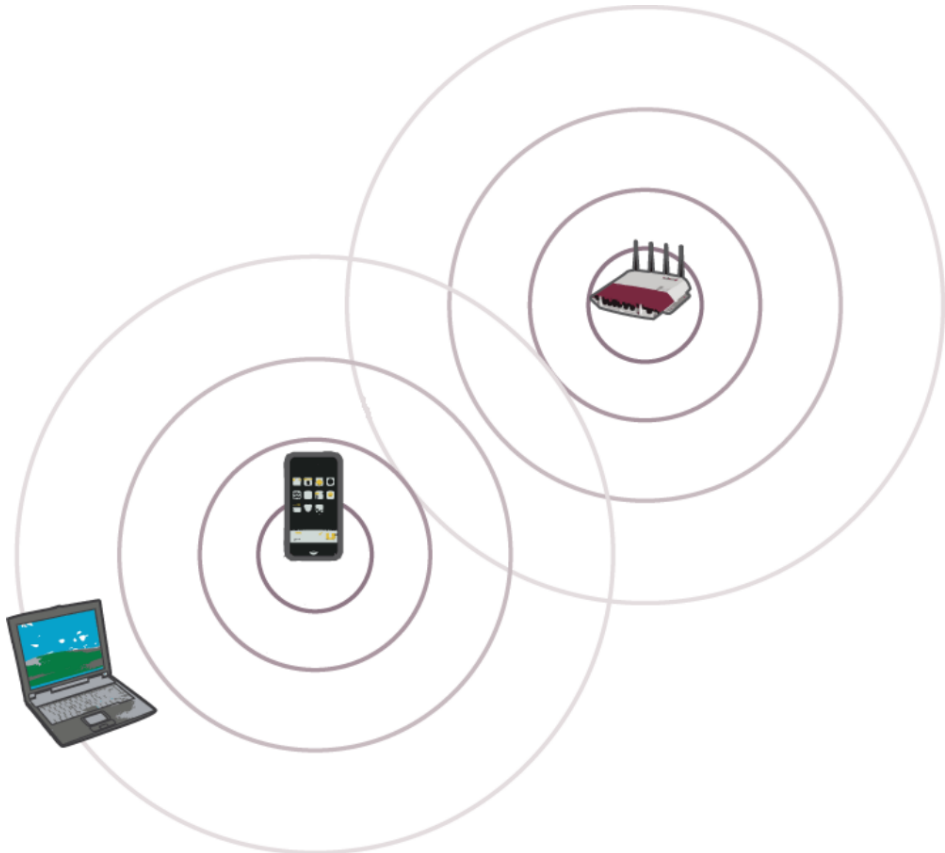
31. Jänner 2014

Gliederung

1. W-LAN - Sicherheit
   - Angriffe in Hotspots
   - WEP
   - WPA/WPA2

Angriffe in Hotspots

- Angriffsarten:
  - Lauscher
  - Accountpiraten
    - ARP-Spoofing
    - Man-in-the-middle
    - Session-Hijacking



Quelle: c't 1/2012

Angriffe in Hotspots

- Angriffsarten:
  - Lauscher
  - Accountpiraten
    - ARP-Spoofing
    - Man-in-the-middle
    - Session-Hijacking

Quelle: c't 1/2012

ARP-Spoofing

Definition (ARP - Address Resolution Protocol)

ARP ist ein Netzwerkprotokoll das zu einer Netzwerkadresse (IP-Adresse) die Hardwareadresse (MAC-Adresse) ermittelt.

- ARP-Request: Who has IP *192.168.178.1* tell *192.168.178.2*
- ARP-Response: *192.168.178.1* is at *AA:BB:CC:DD:EE:FF*

Schwachstellen:

1. Annahme jeglicher ARP-Antworten von allen Systemen
2. Caching der MAC-Adressen

ARP-Spoofing

Definition (ARP - Address Resolution Protocol)

ARP ist ein Netzwerkprotokoll das zu einer Netzwerkadresse (IP-Adresse) die Hardwareadresse (MAC-Adresse) ermittelt.

- ARP-Request: Who has IP *192.168.178.1* tell *192.168.178.2*
- ARP-Response: *192.168.178.1* is at *AA:BB:CC:DD:EE:FF*

Schwachstellen:

1. Annahme jeglicher ARP-Antworten von allen Systemen
2. Caching der MAC-Adressen

ARP-Spoofing

Definition (ARP - Address Resolution Protocol)

ARP ist ein Netzwerkprotokoll das zu einer Netzwerkadresse (IP-Adresse) die Hardwareadresse (MAC-Adresse) ermittelt.

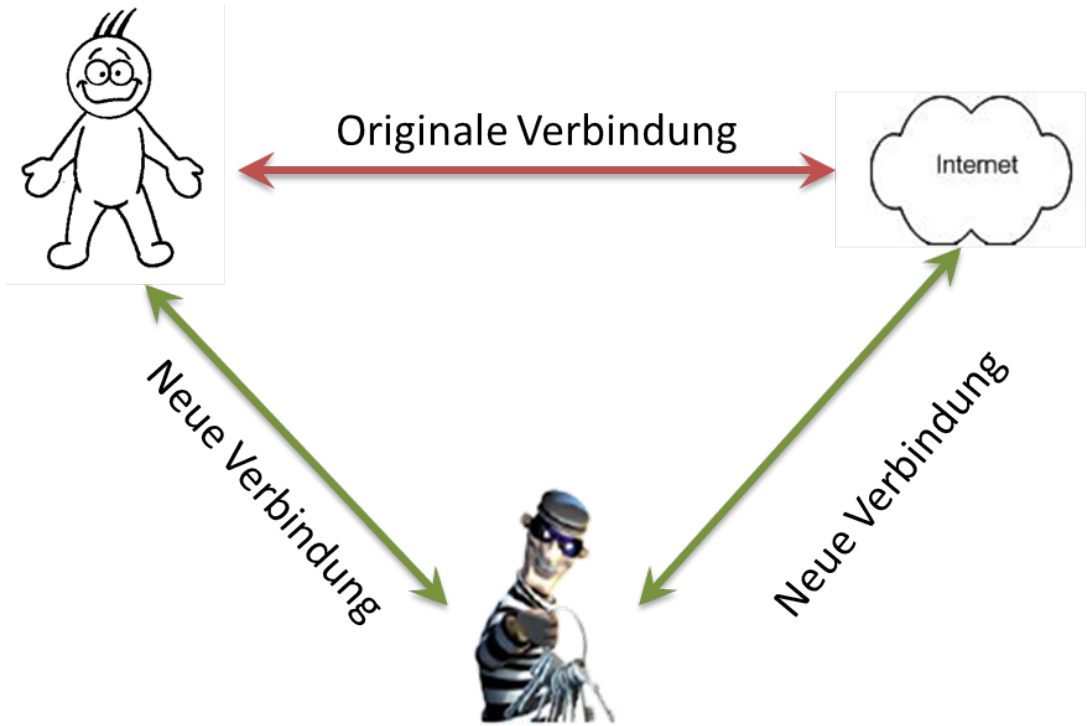
- ARP-Request: Who has IP *192.168.178.1* tell *192.168.178.2*
- ARP-Response: *192.168.178.1* is at *AA:BB:CC:DD:EE:FF*

Schwachstellen:

1. Annahme jeglicher ARP-Antworten von allen Systemen
2. Caching der MAC-Adressen

Man-in-the-middle

- Der Angreifer muss:
  - den Traffic der Clients zu sich lenken
  - den Traffic des Gateway zu sich lenken
  - den Traffic der Clients an das Gateway weiterleiten
  - den Traffic des Gateways an die Clients weiterleiten



Schutz vor Man-in-the-middle Attacken

- Firewalls
- Statische Einträge im ARP-Cache
  - arp -s *IP-Adresse MAC-Adresse*
- Layer-3-Switches
- Tools:
  - XArp (Windows), arpwatch (Linux)

Schutz vor Man-in-the-middle Attacken

- Firewalls
- Statische Einträge im ARP-Cache
  - arp -s *IP-Adresse MAC-Adresse*
- Layer-3-Switches
- Tools:
  - XArp (Windows), arpwatch (Linux)

Schutz vor Man-in-the-middle Attacken

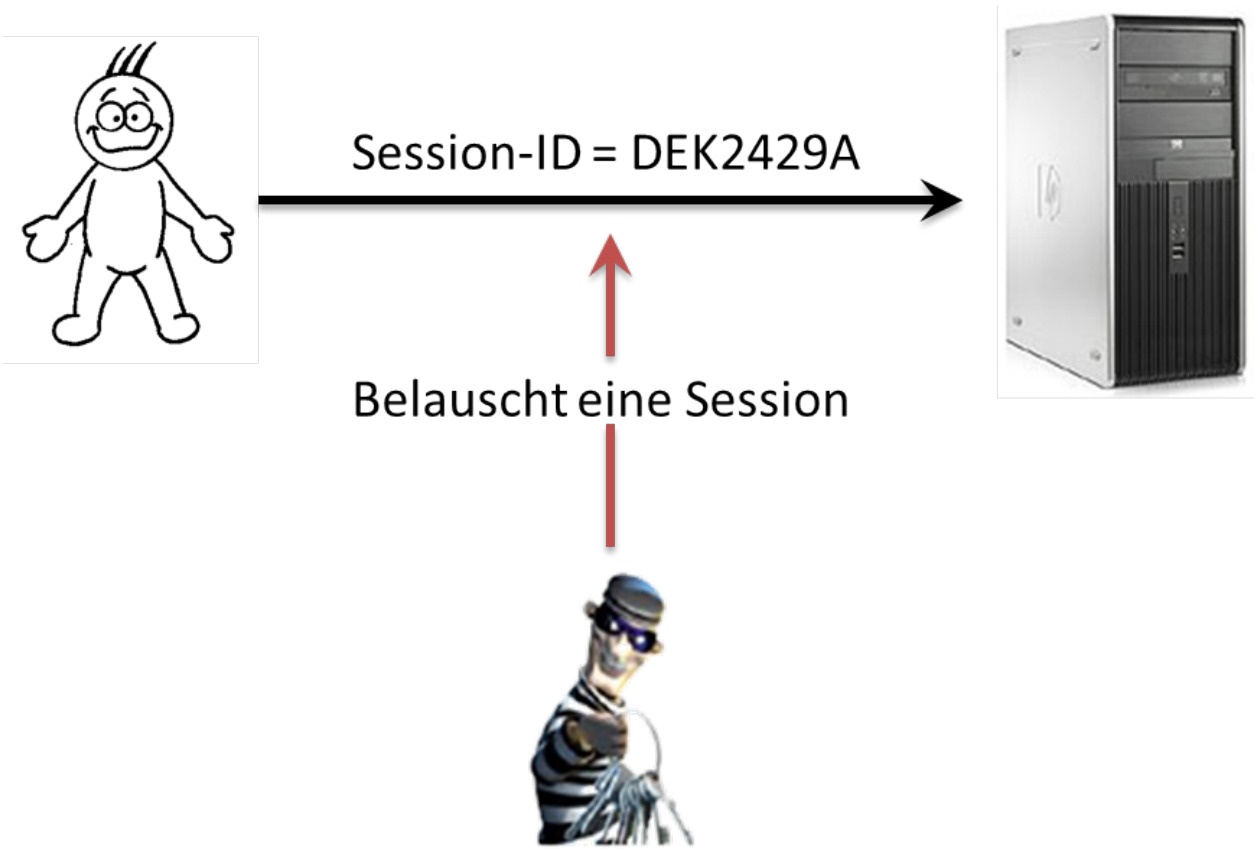
- Firewalls
- Statische Einträge im ARP-Cache
  - arp -s *IP-Adresse MAC-Adresse*
- Layer-3-Switches
- Tools:
  - XArp (Windows), arpwatch (Linux)

Schutz vor Man-in-the-middle Attacken

- Firewalls
- Statische Einträge im ARP-Cache
  - arp -s *IP-Adresse MAC-Adresse*
- Layer-3-Switches
- Tools:
  - XArp (Windows), arpwatch (Linux)

Session-Hijacking

- Mitlesen von Sitzungs-IDs



Session-Hijacking

- Mitlesen von Sitzungs-IDs

DSploit (WiFi Hacking Penetration Suite)

- Hackingtool für Android
- Funktionen:
  - Portscanner
  - Login Cracker (Brute-Force)
  - MITM
  - Session-Hijacking
- kein technisches Verständis notwendig

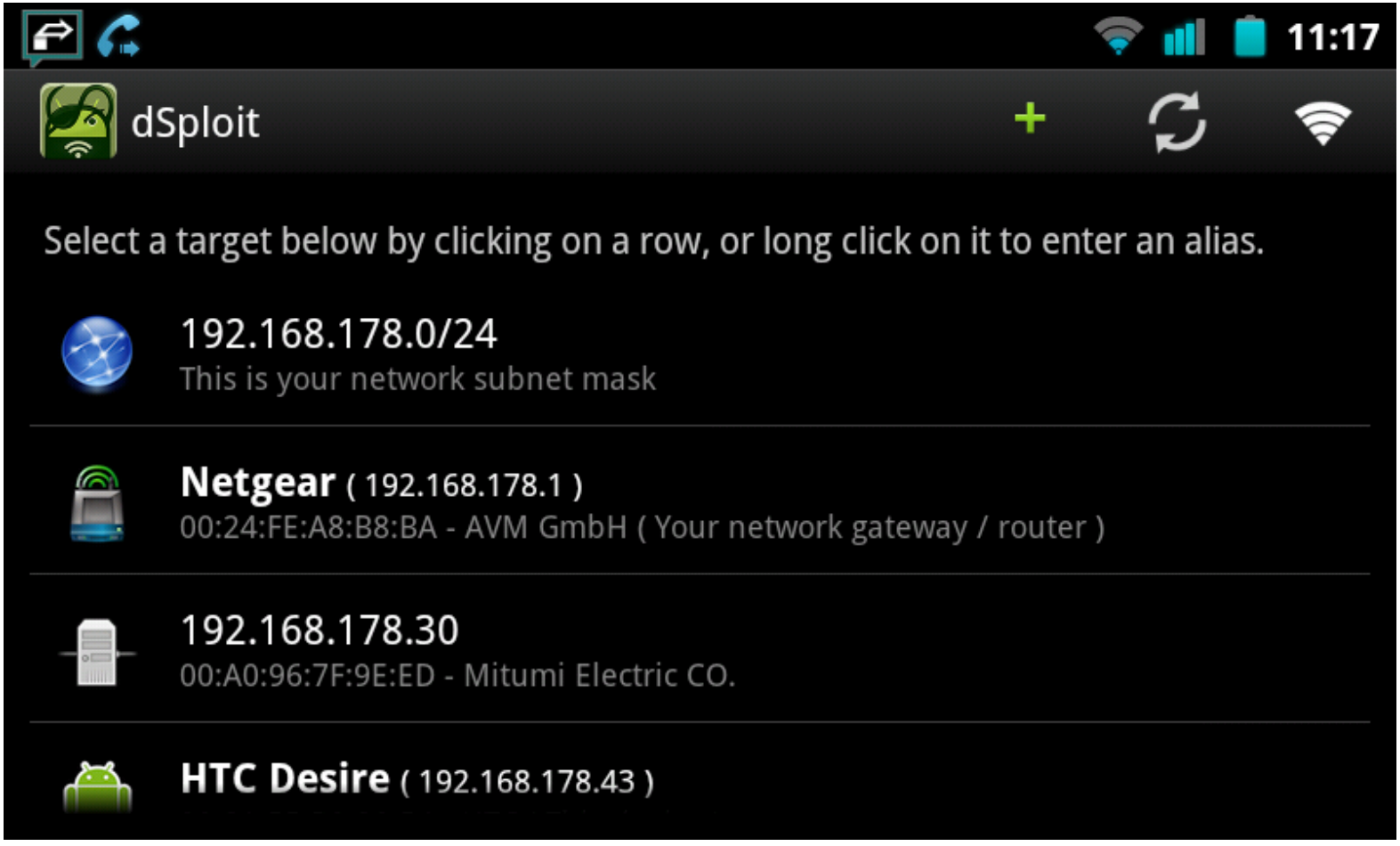
DSploit (WiFi Hacking Penetration Suite)

- Hackingtool für Android
- Funktionen:
  - Portscanner
  - Login Cracker (Brute-Force)
  - MITM
  - Session-Hijacking
- kein technisches Verständis notwendig

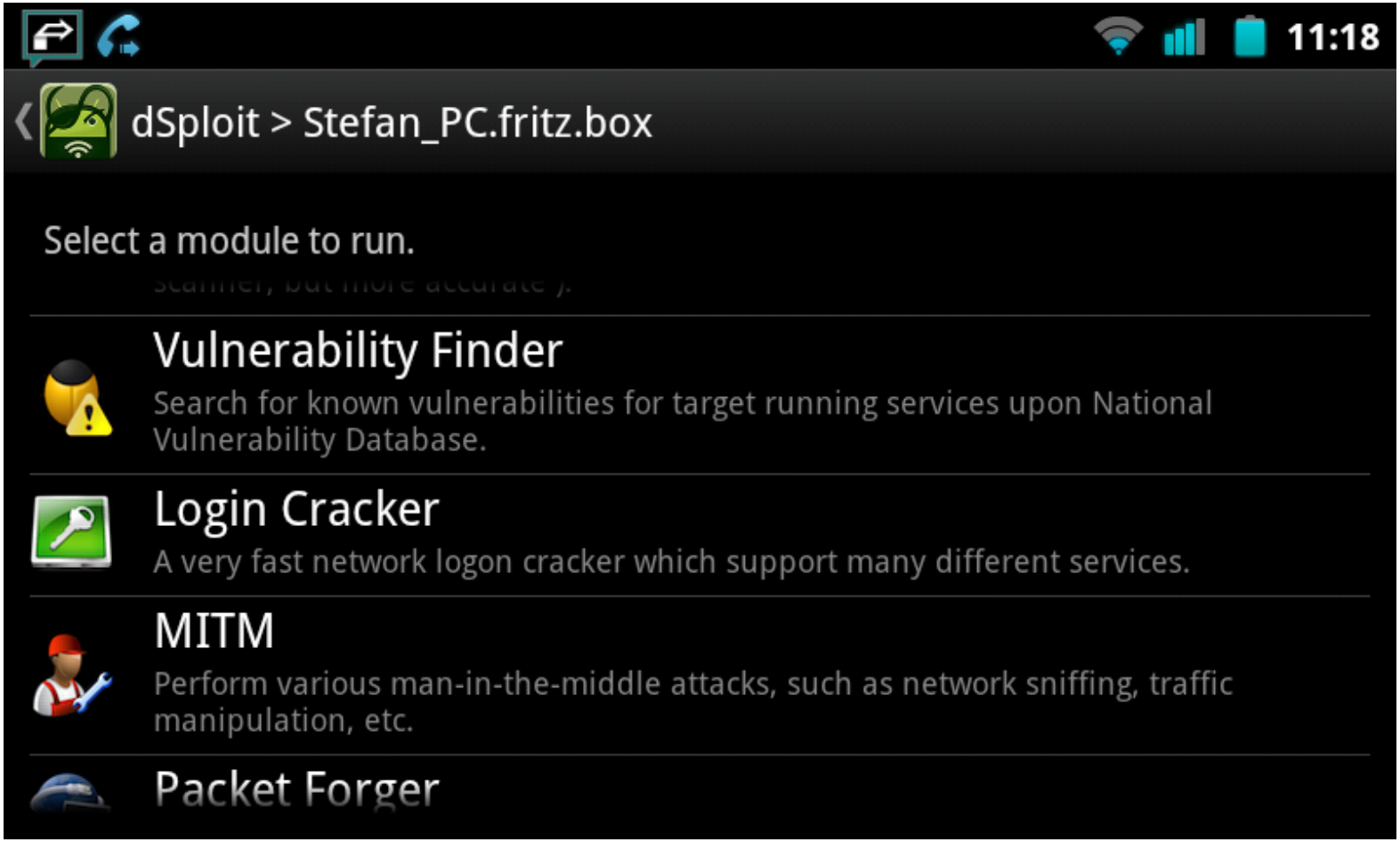
DSploit (WiFi Hacking Penetration Suite)

- Hackingtool für Android
- Funktionen:
  - Portscanner
  - Login Cracker (Brute-Force)
  - MITM
  - Session-Hijacking
- kein technisches Verständis notwendig

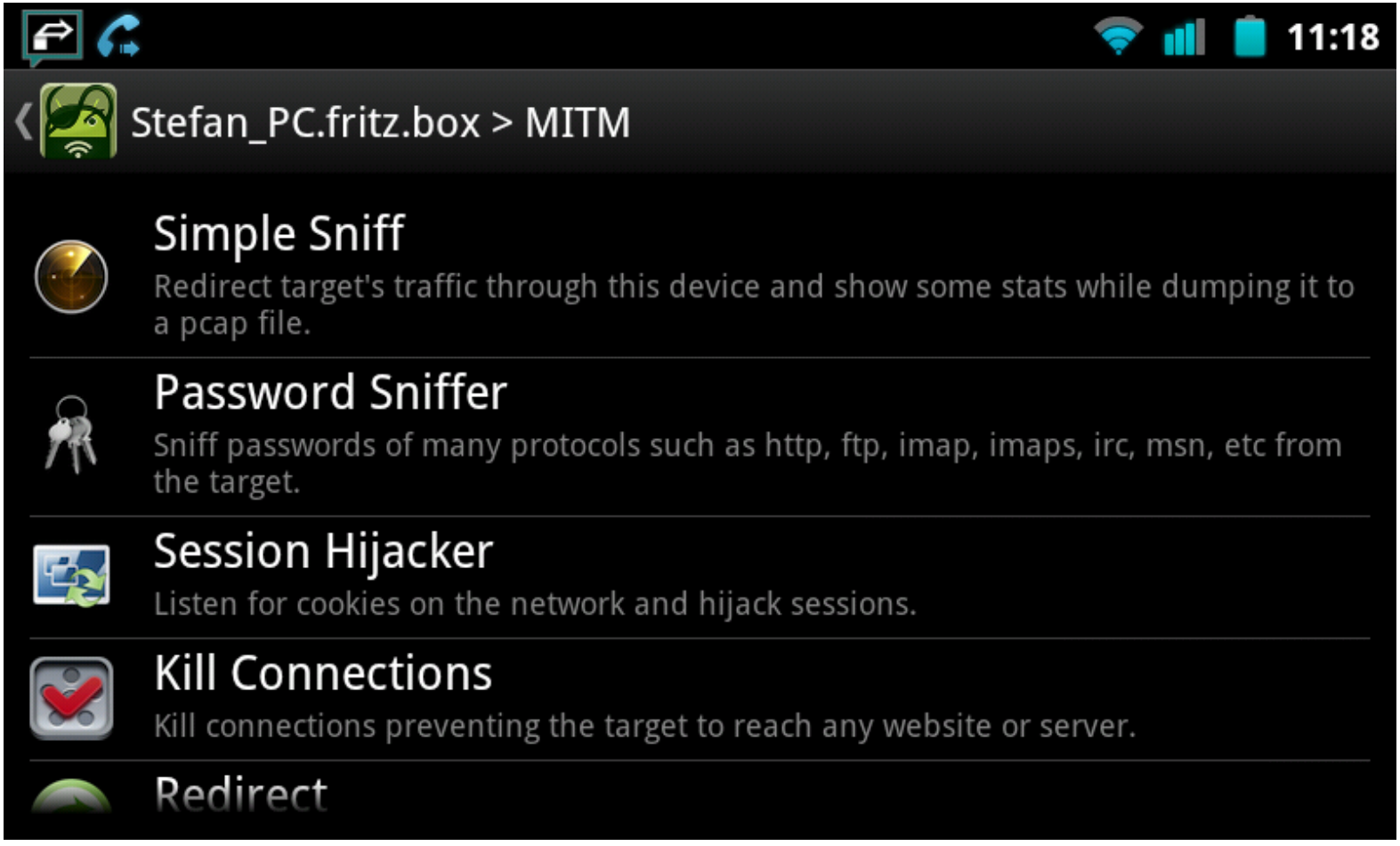
DSploit (WiFi Hacking Penetration Suite) 2



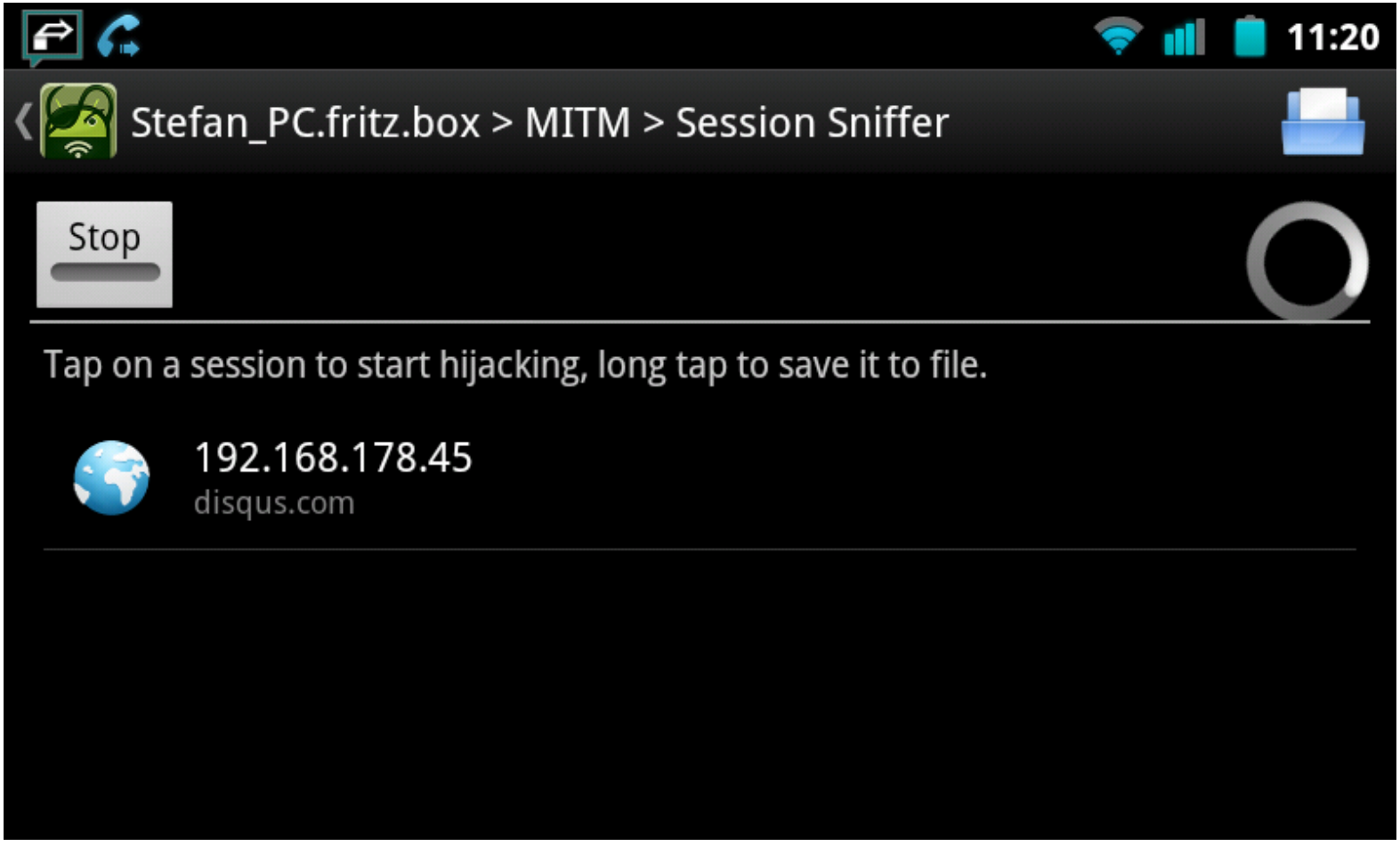
DSploit (WiFi Hacking Penetration Suite) 2



DSploit (WiFi Hacking Penetration Suite) 2



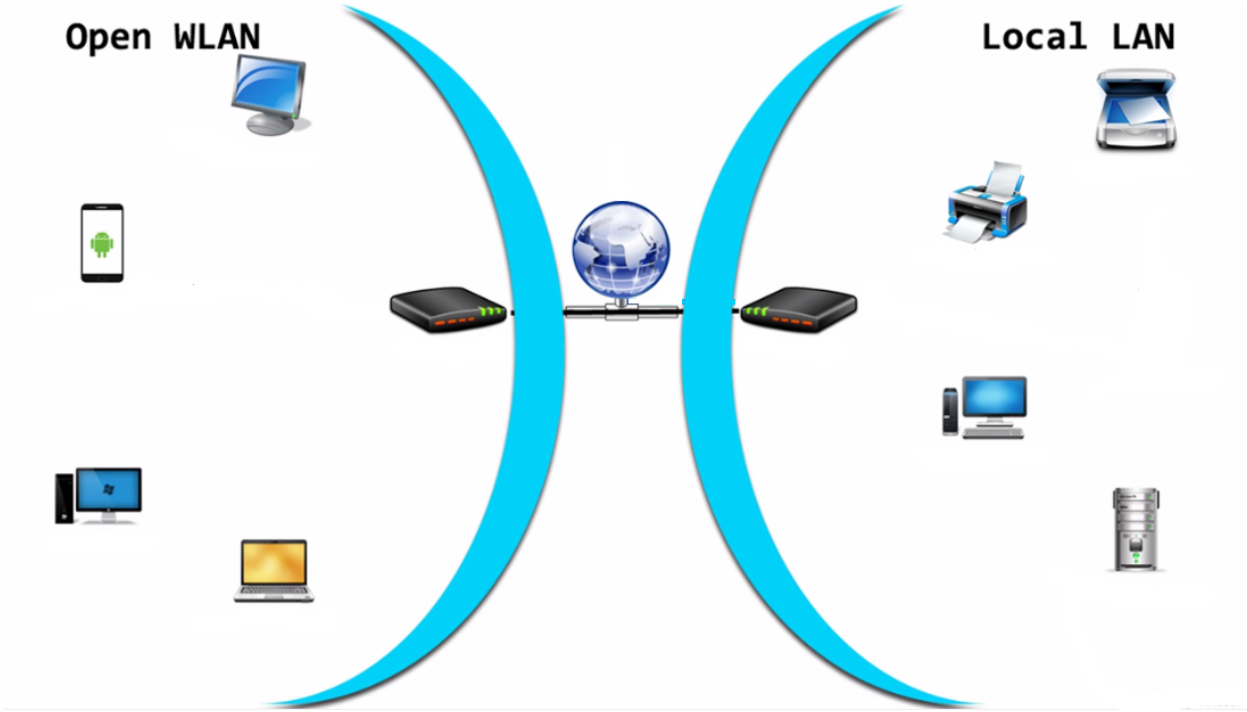
DSploit (WiFi Hacking Penetration Suite) 2



DSploit (WiFi Hacking Penetration Suite) 2

Schutzmaßnahmen gegen Angriffe in Hotspots

- VPN - Virtual Private Network

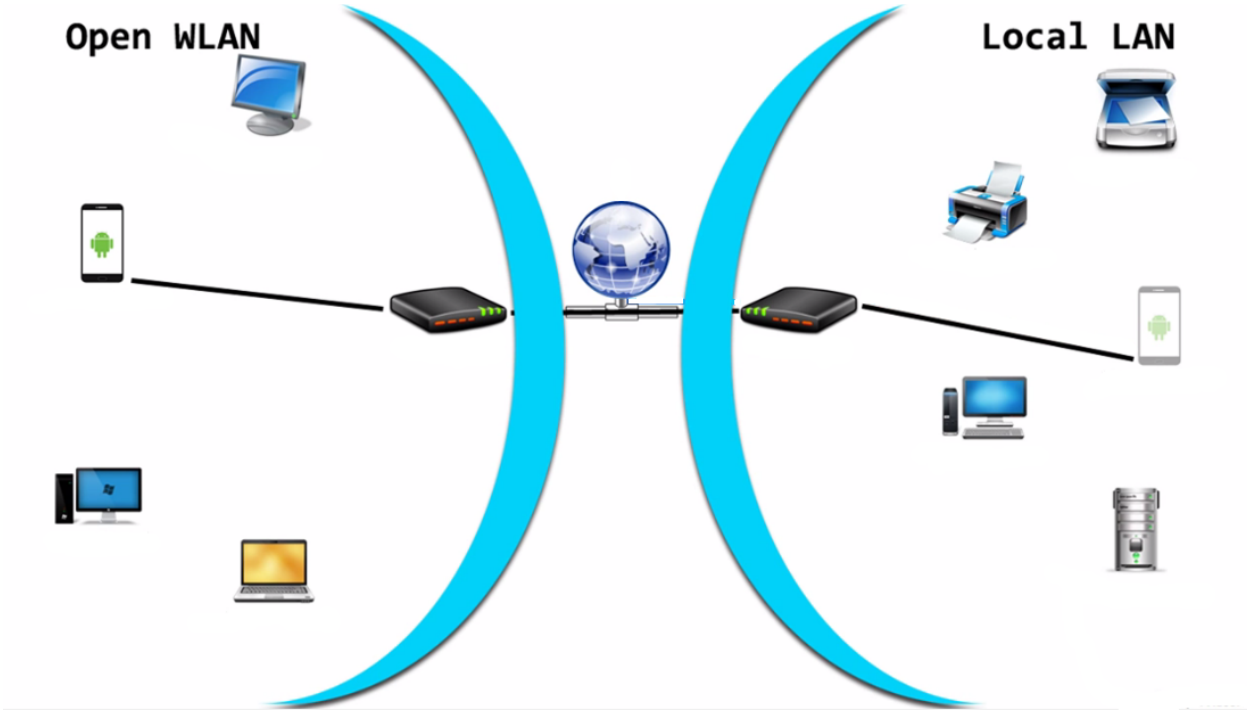


Quelle: sempervideo.de

- UMTS und GPRS

Schutzmaßnahmen gegen Angriffe in Hotspots

- VPN - Virtual Private Network

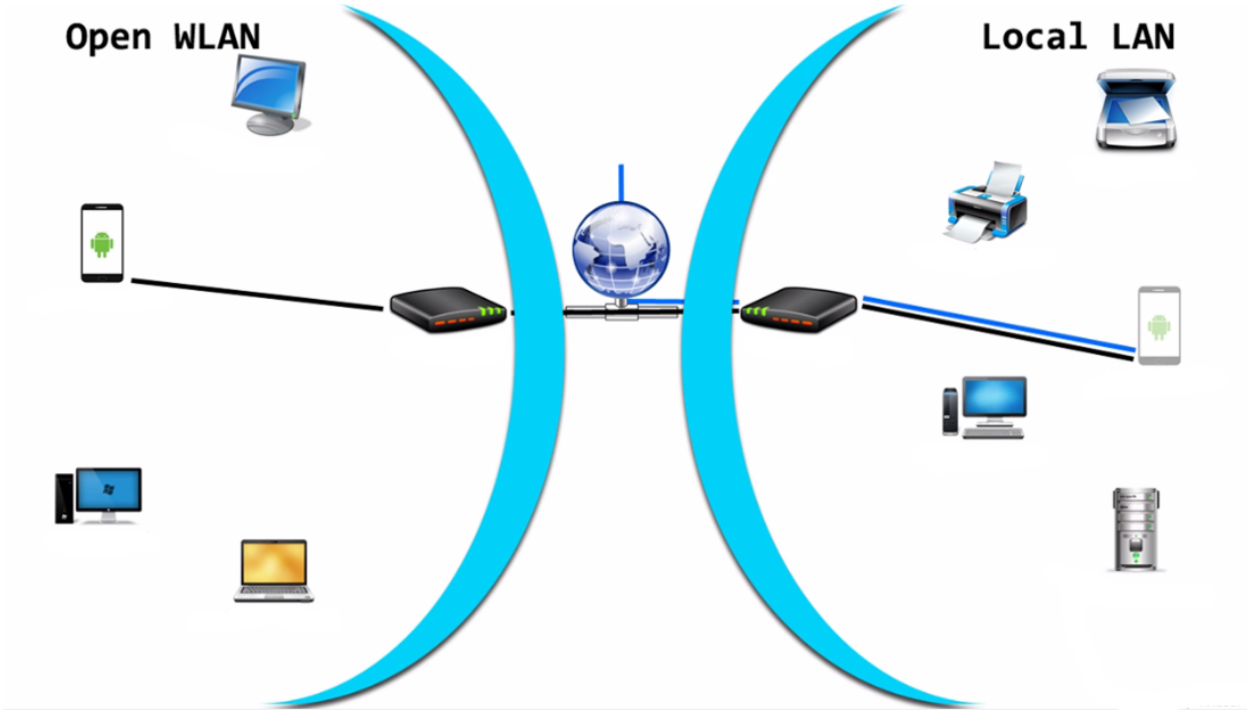


Quelle: sempervideo.de

- UMTS und GPRS

Schutzmaßnahmen gegen Angriffe in Hotspots

- VPN - Virtual Private Network



Quelle: sempervideo.de

- UMTS und GPRS

WEP (Wired Equivalent Privacy)

- Ziele:
  - Schutz der Datenübertragung vor Unbefugten
  - Datenintegrität
  - Authentizität
- Dazu werden verwendet:
  - CRC-32 (Cyclic Redundancy Check)
  - RC4

WEP (Wired Equivalent Privacy)

- Ziele:
  - Schutz der Datenübertragung vor Unbefugten
  - Datenintegrität
  - Authentizität
- Dazu werden verwendet:
  - CRC-32 (Cyclic Redundancy Check)
  - RC4

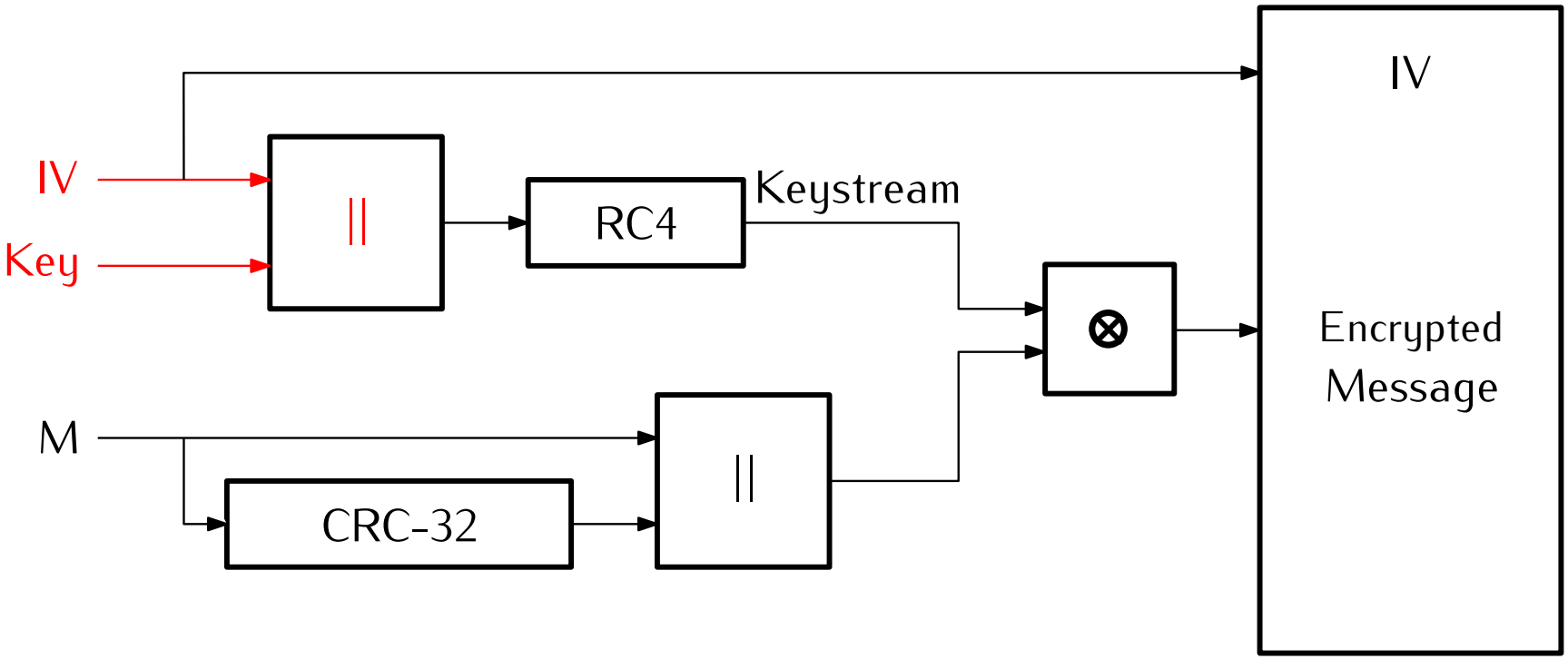
WEP - Merkmale

- Verwendet Shared-Key
  - Befugte haben Key → können Datenpakete ver-/entschlüssen
  - Maximal 4 verschiedene Keys konfigurierbar
  - 40 oder 104 Bit - 5 oder 13 Zeichen
- Arbeitet mit IV = Initialisierungsvektor
  - 4 Byte groß - letztes Byte enthält KeyID
  - In IEEE 802.11 kein Berechnungsverfahren für IV definiert
  - Oft inkrementell erzeugt

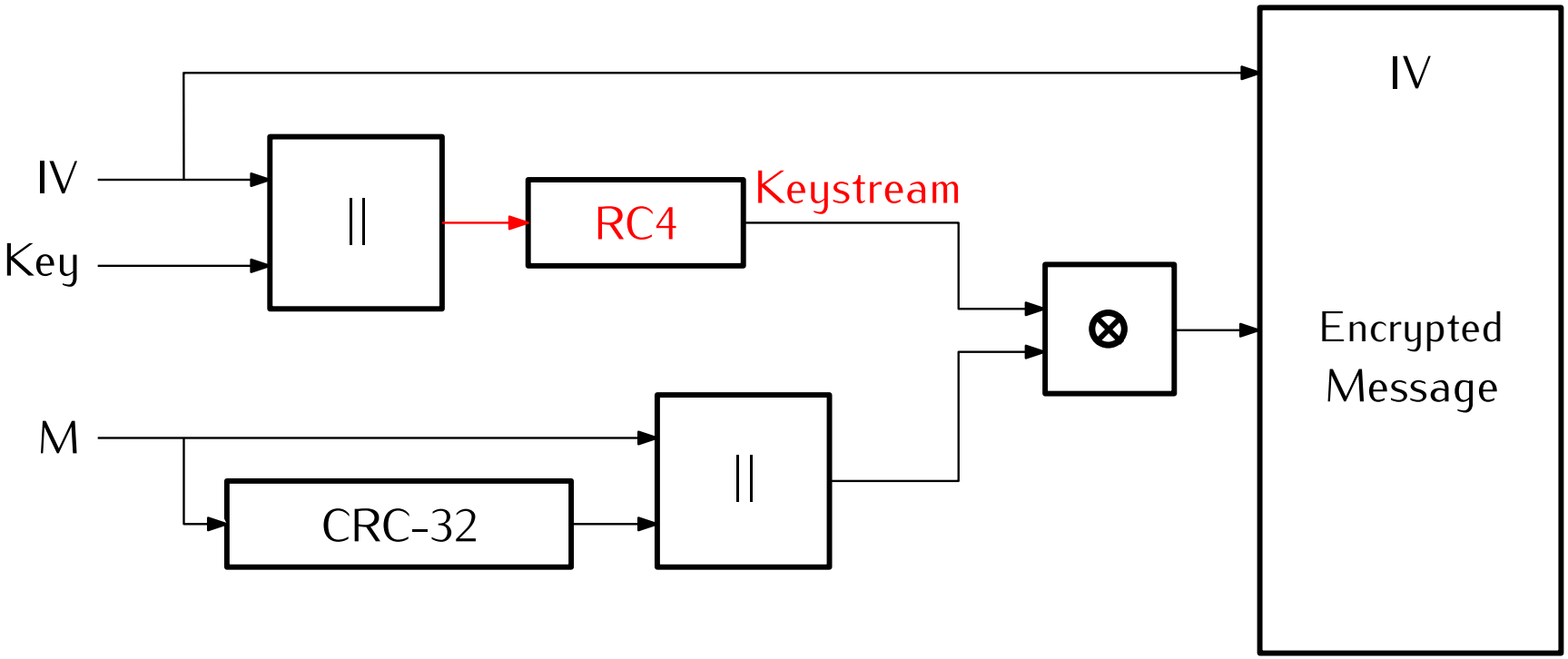
WEP - Merkmale

- Verwendet Shared-Key
  - Befugte haben Key $\rightarrow$ können Datenpakete ver-/entschlüssen
  - Maximal 4 verschiedene Keys konfigurierbar
  - 40 oder 104 Bit - 5 oder 13 Zeichen
- Arbeitet mit IV = Initialisierungsvektor
  - 4 Byte groß - letztes Byte enthält KeyID
  - In IEEE 802.11 kein Berechnungsverfahren für IV definiert
  - Oft inkrementell erzeugt

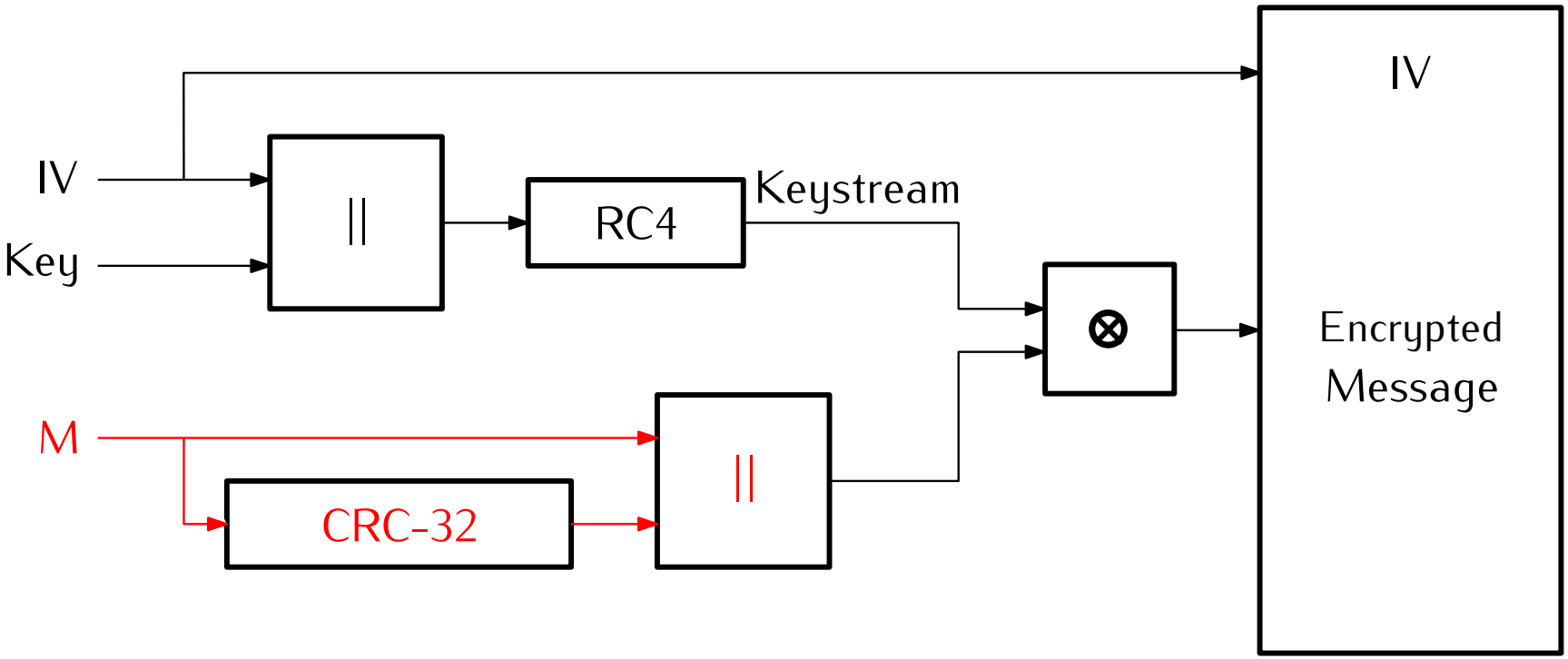
WEP - Verschlüsselung



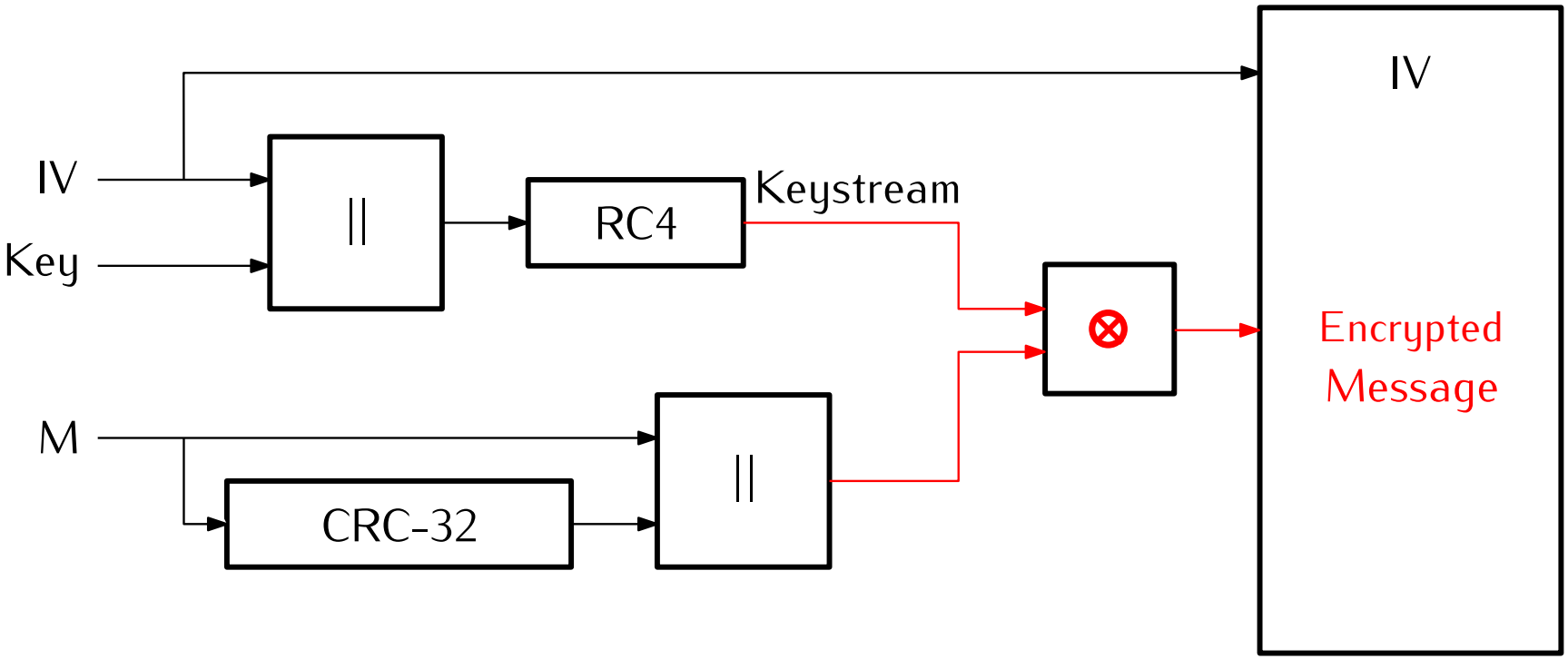
WEP - Verschlüsselung



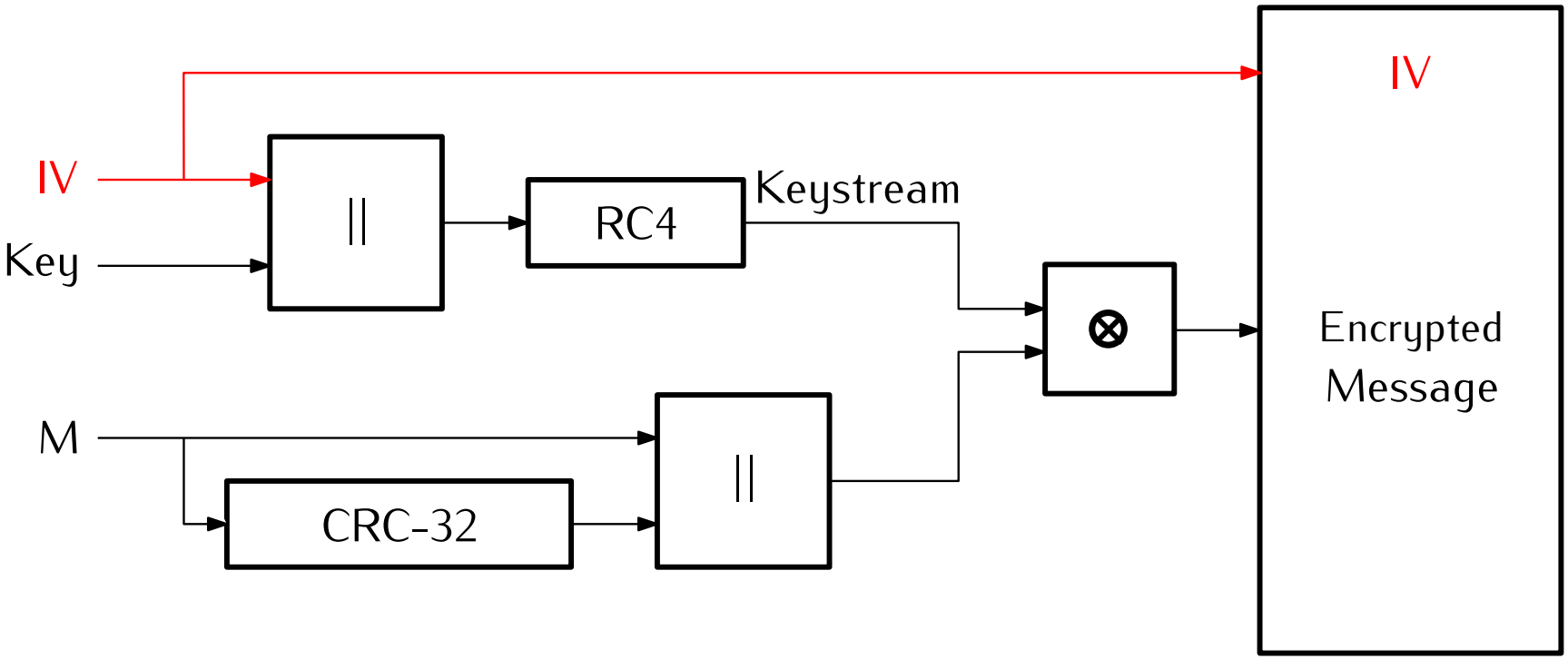
WEP - Verschlüsselung



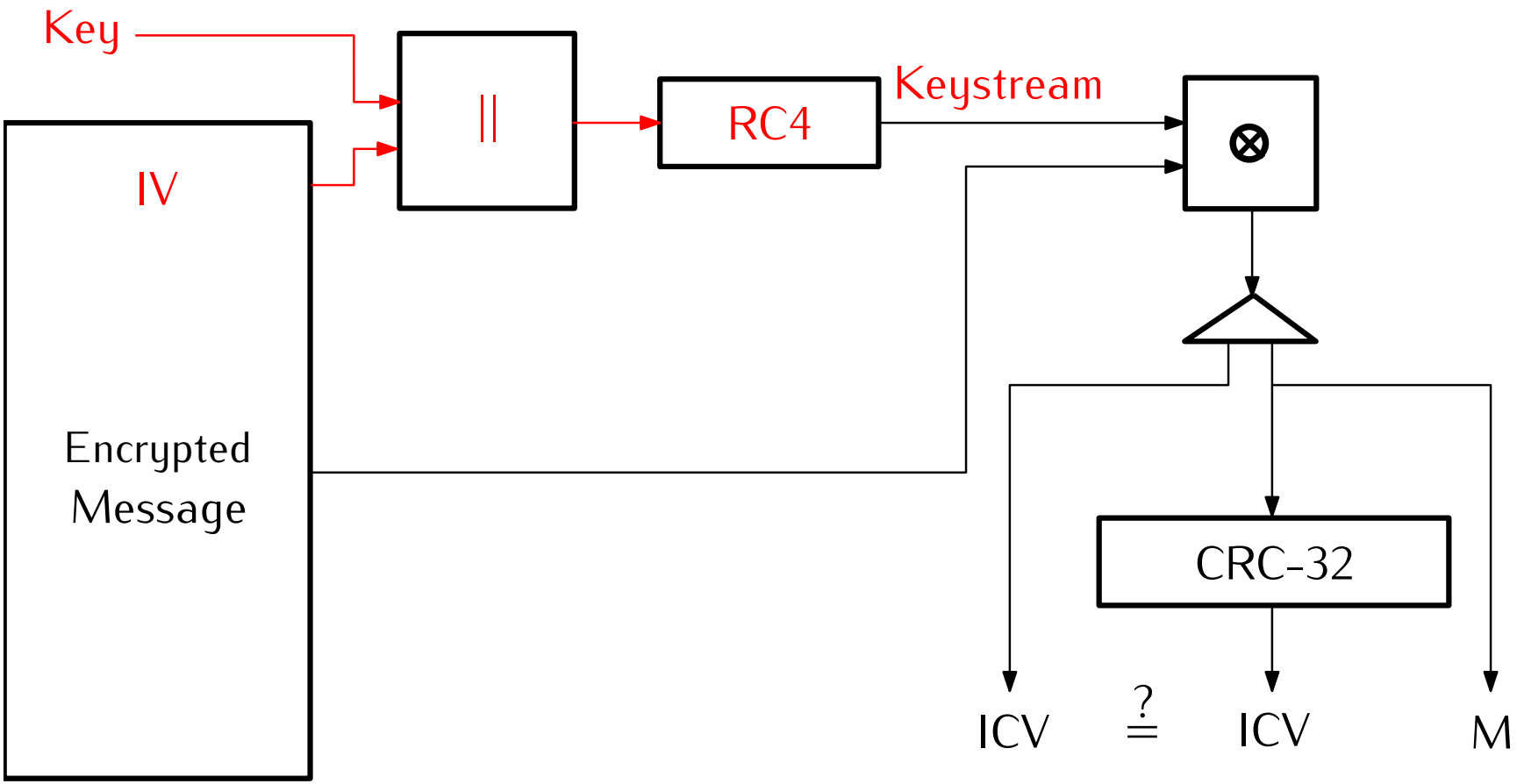
WEP - Verschlüsselung



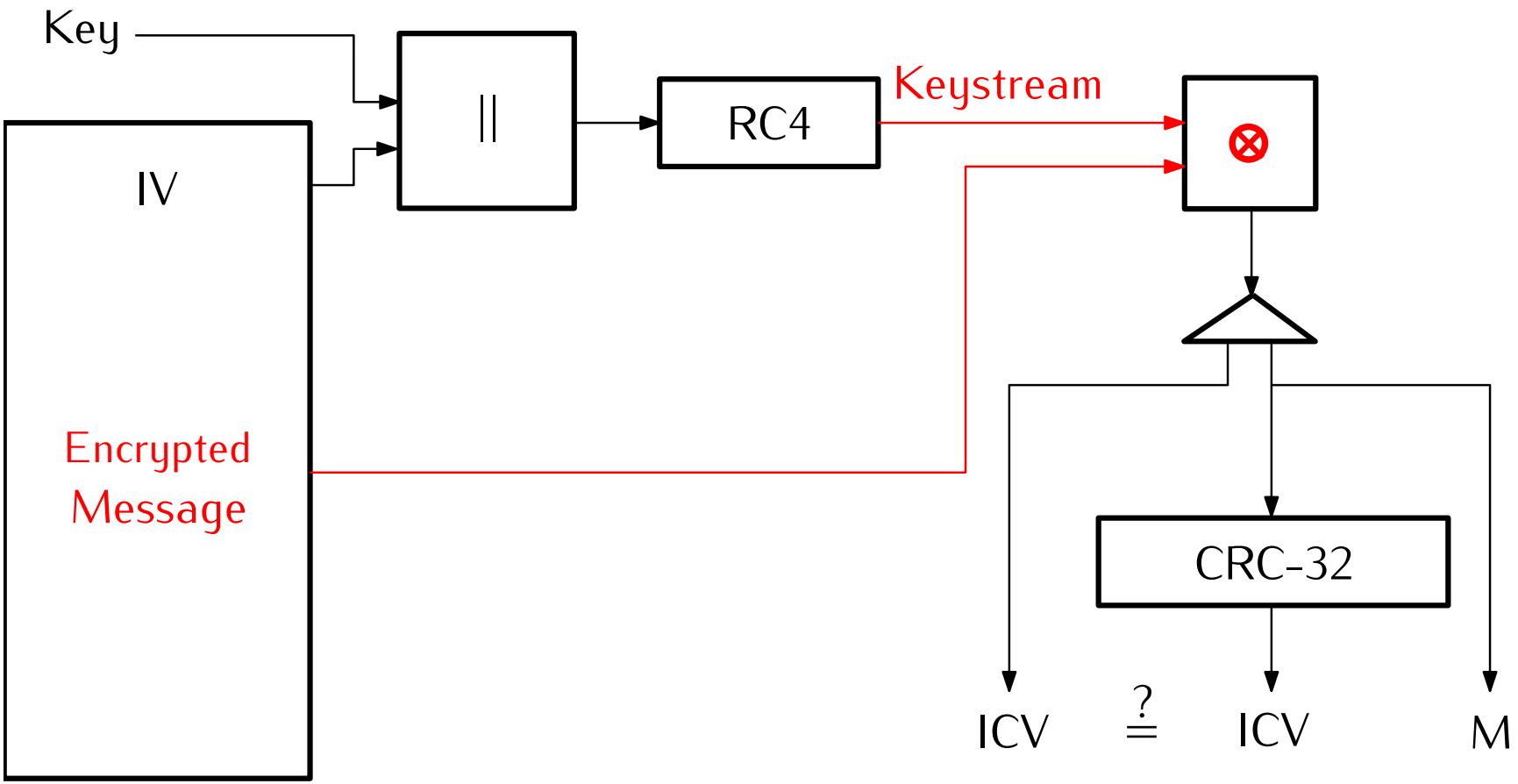
WEP - Verschlüsselung



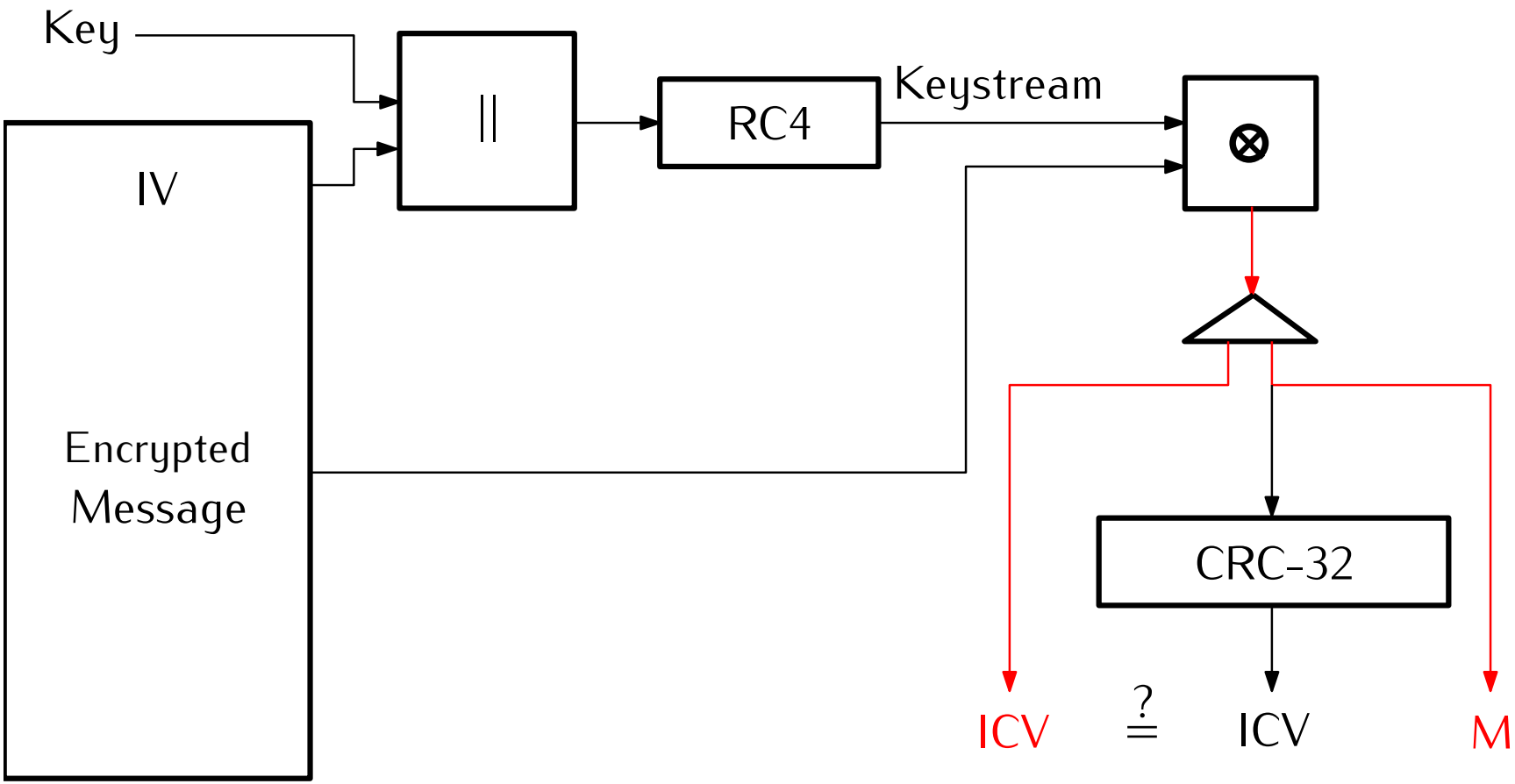
WEP - Entschlüsselung



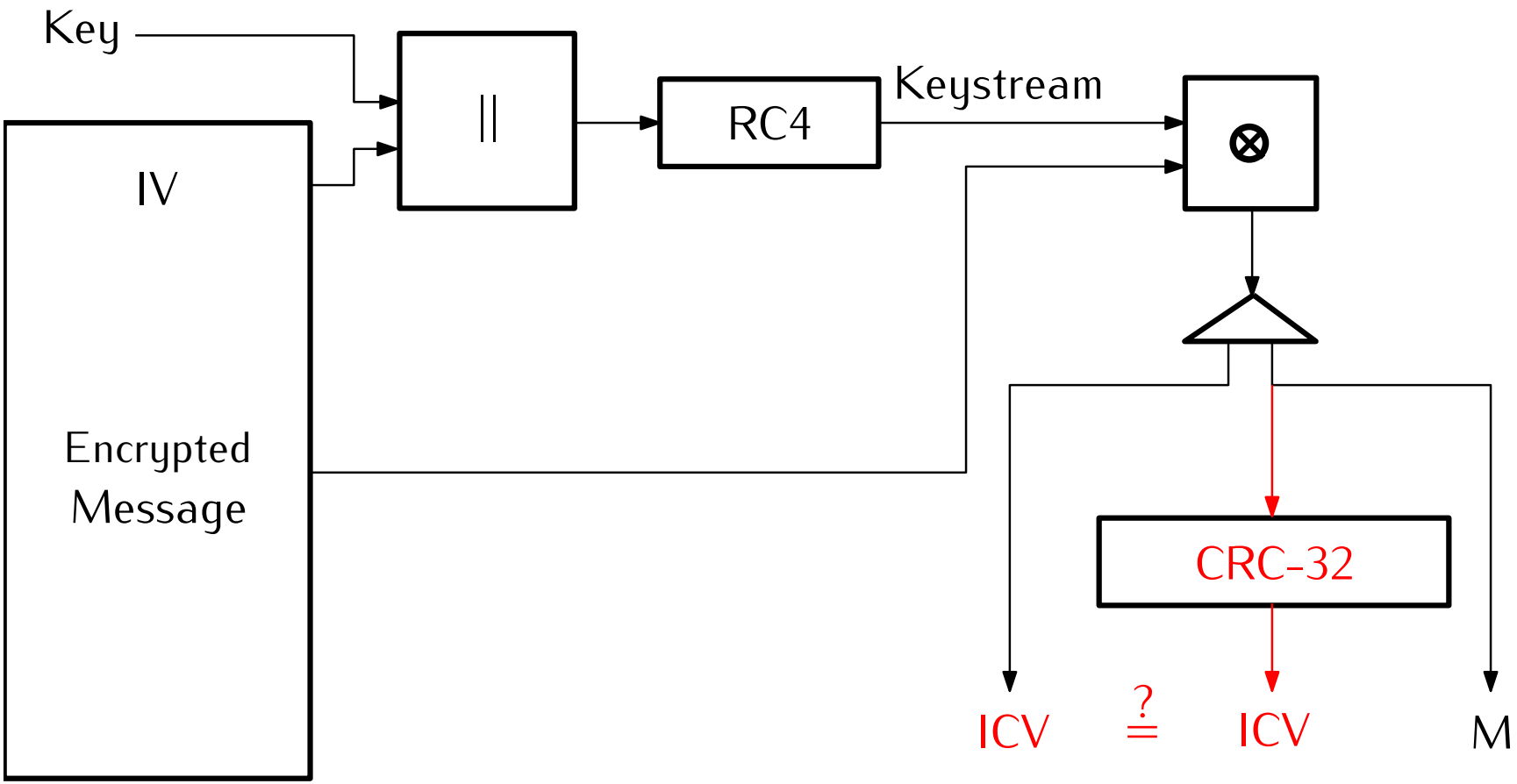
WEP - Entschlüsselung



WEP - Entschlüsselung

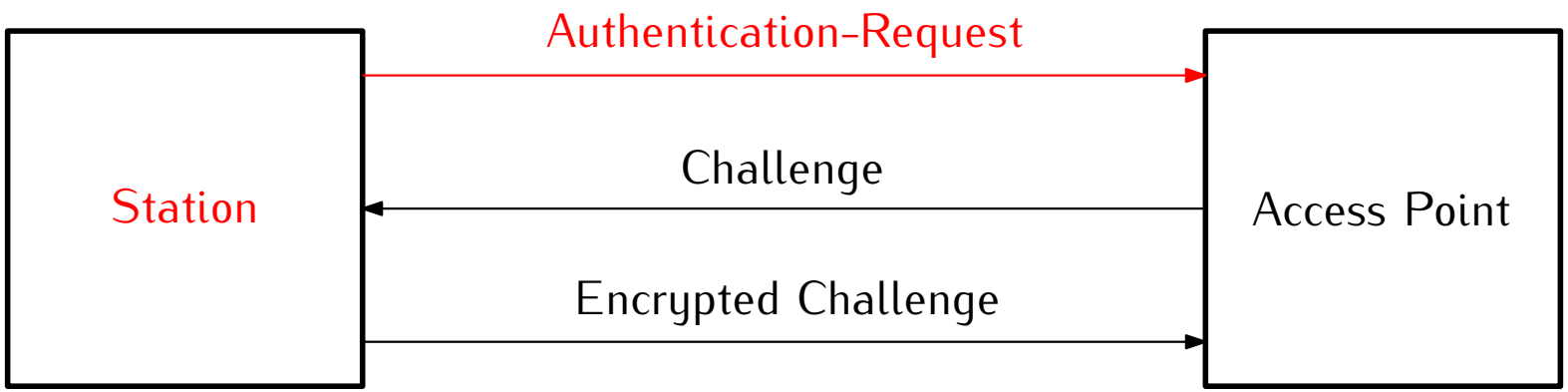


WEP - Entschlüsselung



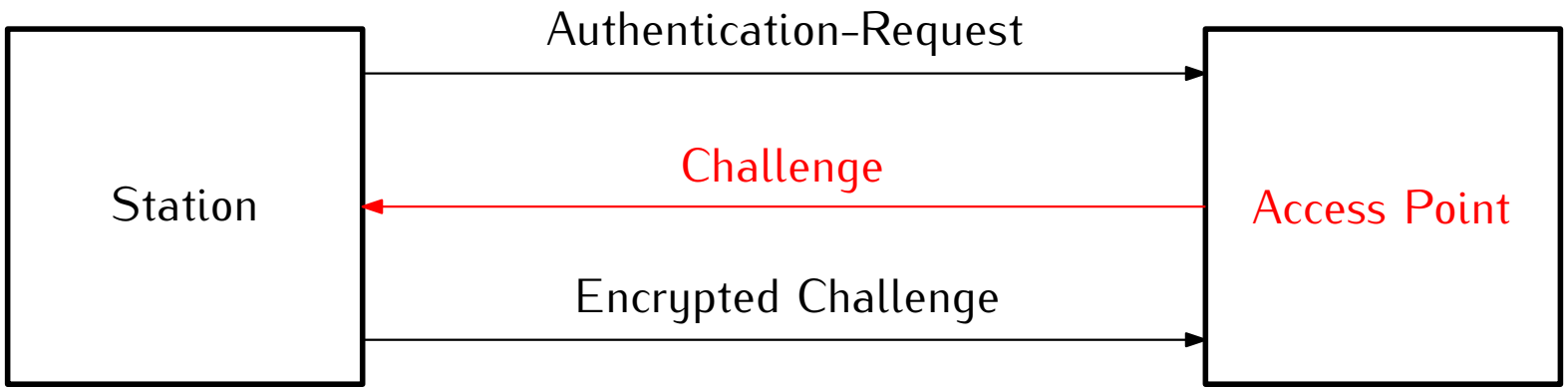
WEP - Authentizität

- Open-System-Authentication
  - Request - Antwort
  - Entscheidungsgrundlage nicht in IEEE 802.11 definiert
- Shared-Key-Authentication
  - Challenge-Response-Verfahren



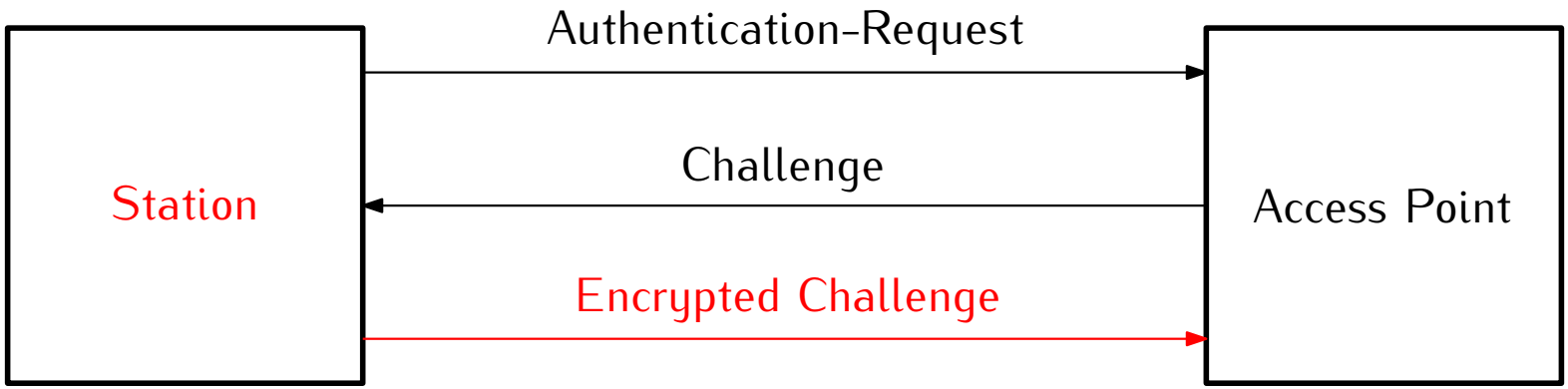
WEP - Authentizität

- Open-System-Authentication
  - Request - Antwort
  - Entscheidungsgrundlage nicht in IEEE 802.11 definiert
- Shared-Key-Authentication
  - Challenge-Response-Verfahren



WEP - Authentizität

- Open-System-Authentication
  - Request - Antwort
  - Entscheidungsgrundlage nicht in IEEE 802.11 definiert
- Shared-Key-Authentication
  - Challenge-Response-Verfahren



WEP - Schwachstellen

- Shared-Key-Authentication
  - Angreifer hat Klartext, verschlüsselter Text und IV
  - Kann Schlüsselstrom herleiten
  - Kann sich für jede Challenge authentifizieren

WEP - Schwachstellen

- IV-Kollisionen
  - $2^{24} = 16.777.216$ verschiedene IVs
  - Genug solche gleich kodierte Nachrichten $\rightarrow$ Key berechnen
  - Reinjection (Aircrack)
    - ARP-Request abfangen und wiedereinspeisen
    - Genug IV-Schlüsseltext-Pärchen sammeln $\rightarrow$ Key berechnen

WEP - Schwachstellen

- Kurze Shared-Keys
  - Brute-Force-Methode

WEP - Schutzmaßnahmen

- Nicht benutzen!
- WPA/WPA2 verwenden!

WPA

- WPA = Wi-Fi Protected Access (31.10.2002)
- Durch die Wi-Fi Alliance (http://www.wi-fi.org)
- keine neue Hardware erforderlich
- nur Firmware Update
- WPA $\subset$ IEEE 802.11i (23.7.2004)
- IEEE 802.11i $\rightarrow$ WPA2.

WPA

- WPA = Wi-Fi Protected Access (31.10.2002)
- Durch die Wi-Fi Alliance (http://www.wi-fi.org)

- keine neue Hardware erforderlich
- nur Firmware Update
- WPA $\subset$ IEEE 802.11i (23.7.2004)
- IEEE 802.11i $\rightarrow$ WPA2.

WPA

- WPA = Wi-Fi Protected Access (31.10.2002)
- Durch die Wi-Fi Alliance (http://www.wi-fi.org)

- keine neue Hardware erforderlich
- nur Firmware Update
- WPA $\subset$ IEEE 802.11i (23.7.2004)
- IEEE 802.11i $\rightarrow$ WPA2.

WPA

- WPA = Wi-Fi Protected Access (31.10.2002)
- Durch die Wi-Fi Alliance (http://www.wi-fi.org)

- keine neue Hardware erforderlich
- nur Firmware Update
- WPA $\subset$ IEEE 802.11i (23.7.2004)
- IEEE 802.11i $\rightarrow$ WPA2.

Neuerungen in WPA/WPA2

- WPA:
  - Temporal Key Integrity Protocol (TKIP)
  - Message Integrity Check (MIC)
- WPA2:
  - CCMP, Advanced Encryption Standard (AES)
  - jedoch: Abwärtskompatibel zu TKIP/RC4
- Authentisierung:
  - Personal $\rightarrow$ PSK
  - Enterprise $\rightarrow$ 802.1X/RADIUS

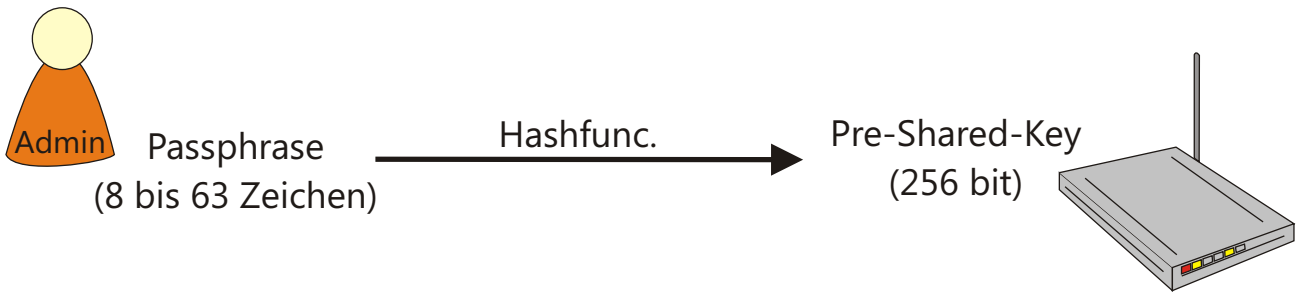
Neuerungen in WPA/WPA2

- WPA:
  - Temporal Key Integrity Protocol (TKIP)
  - Message Integrity Check (MIC)
- WPA2:
  - CCMP, Advanced Encryption Standard (AES)
  - jedoch: Abwärtskompatibel zu TKIP/RC4
- Authentisierung:
  - Personal $\rightarrow$ PSK
  - Enterprise $\rightarrow$ 802.1X/RADIUS

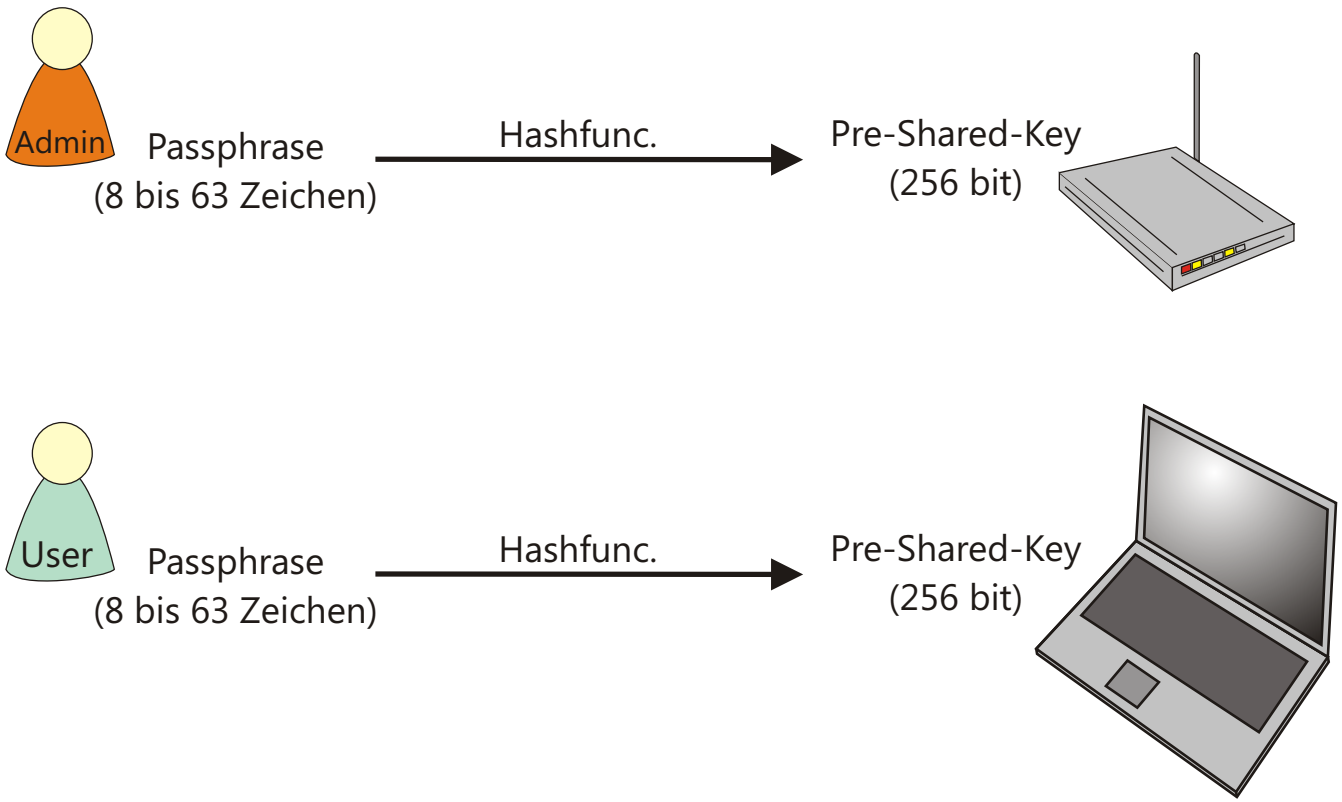
Neuerungen in WPA/WPA2

- WPA:
  - Temporal Key Integrity Protocol (TKIP)
  - Message Integrity Check (MIC)
- WPA2:
  - CCMP, Advanced Encryption Standard (AES)
  - jedoch: Abwärtskompatibel zu TKIP/RC4
- Authentisierung:
  - Personal $\rightarrow$ PSK
  - Enterprise $\rightarrow$ 802.1X/RADIUS

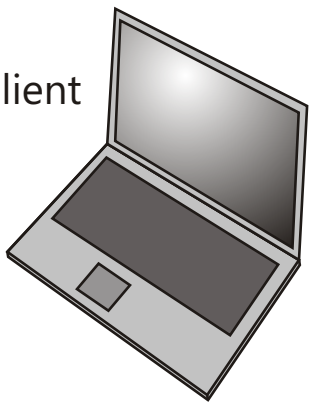
Pre-Shared-Key

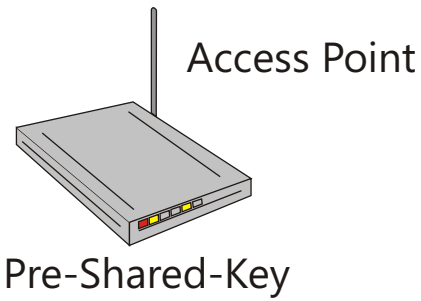


Pre-Shared-Key

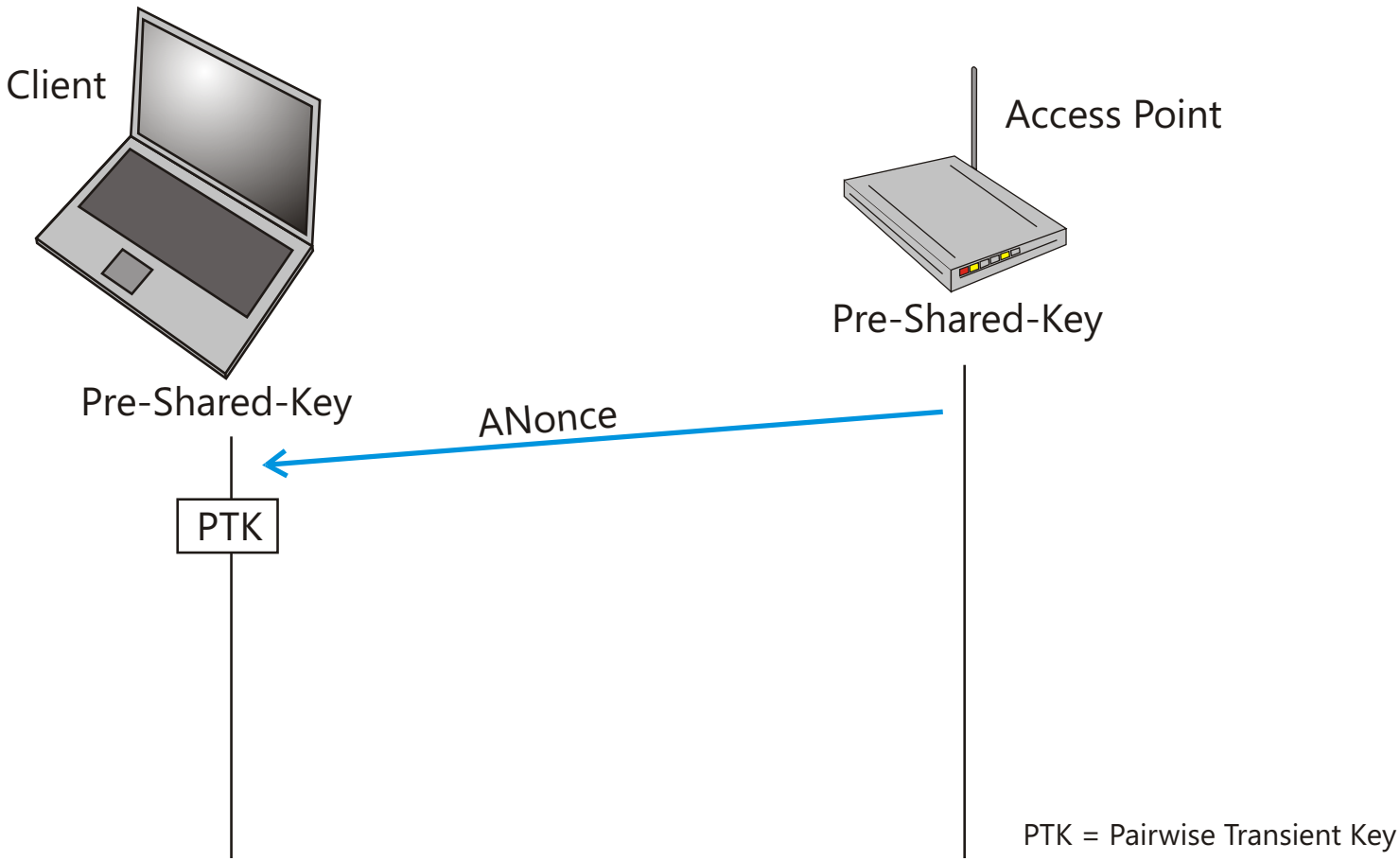


4-Way-Handshake

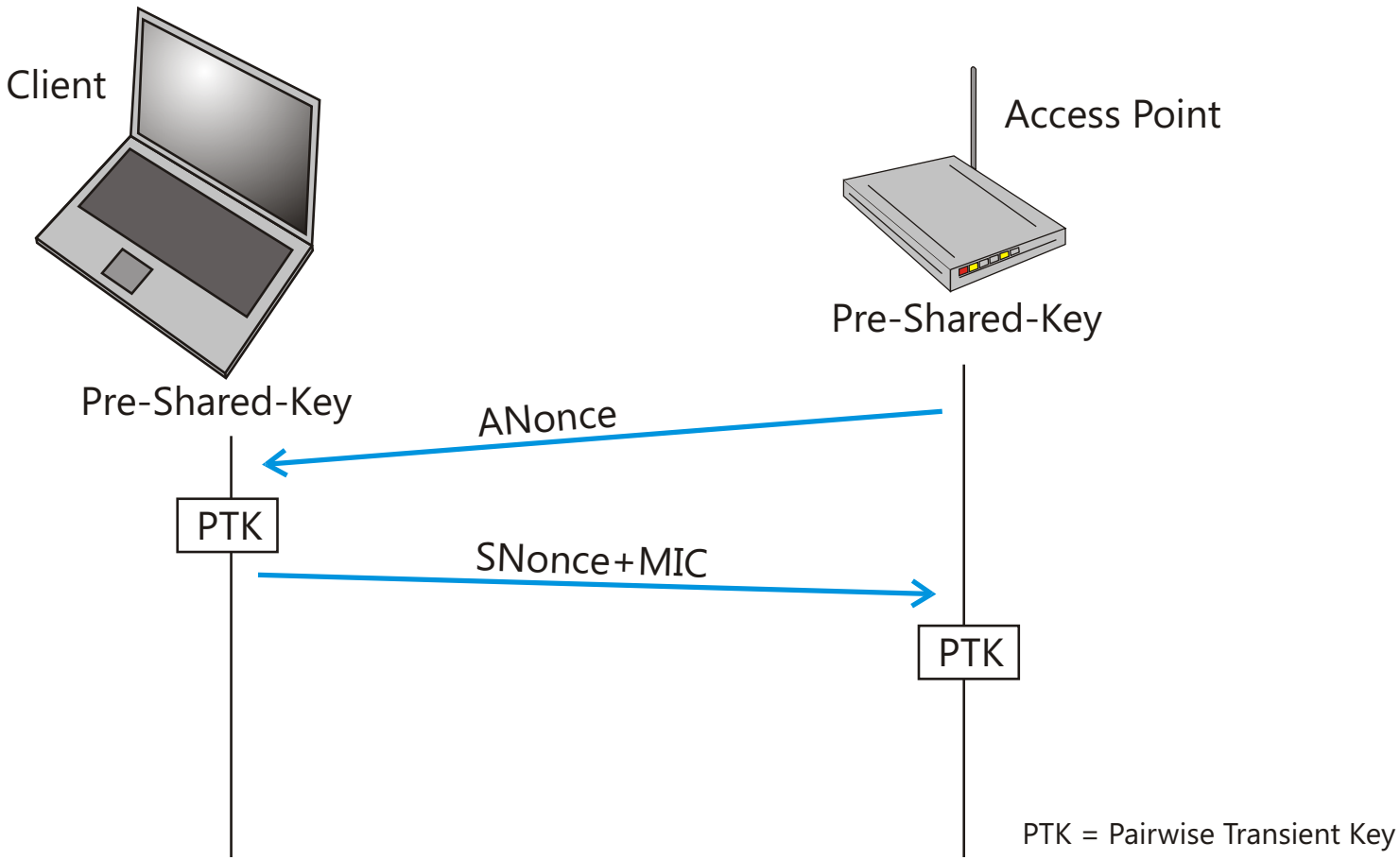




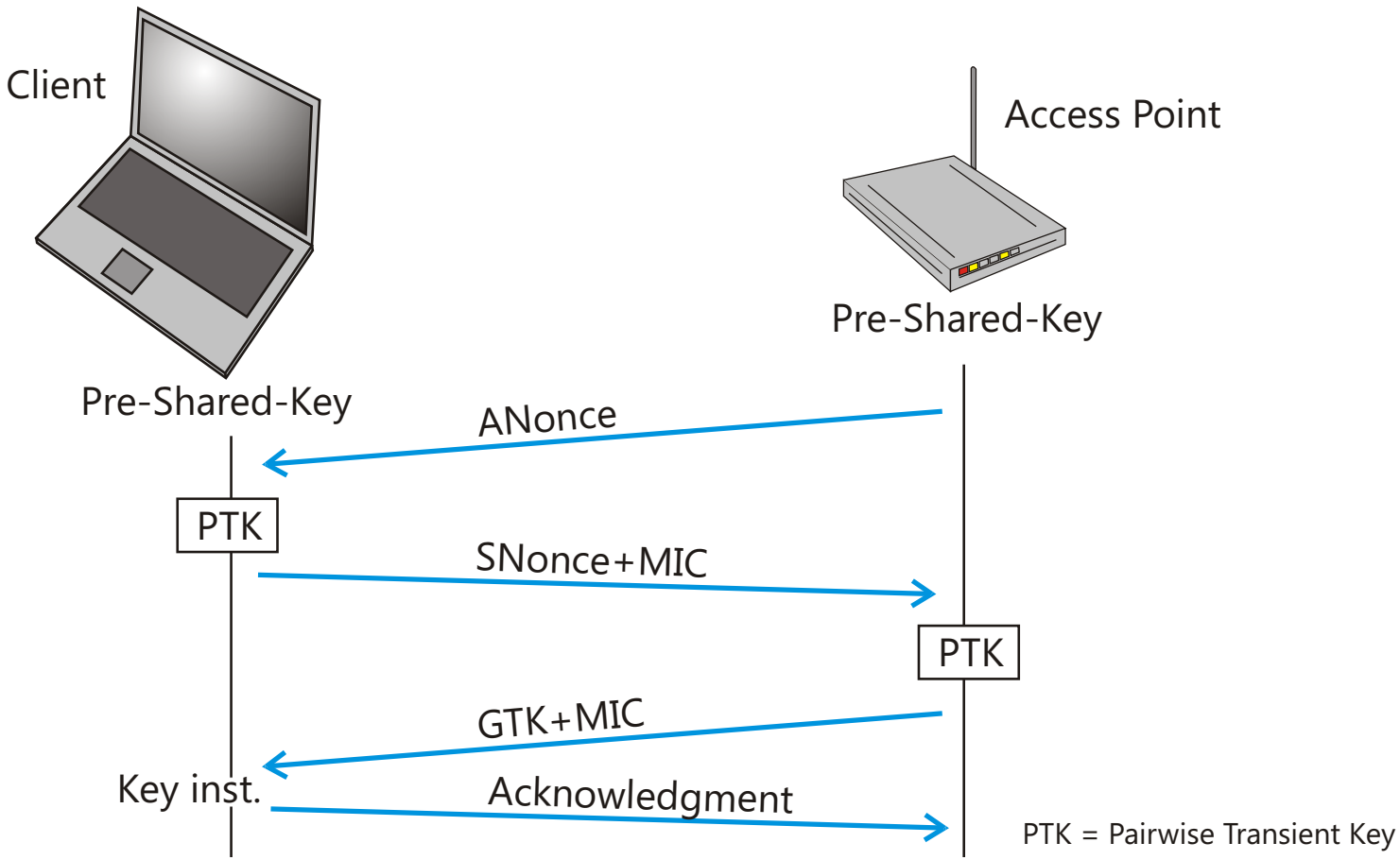
4-Way-Handshake



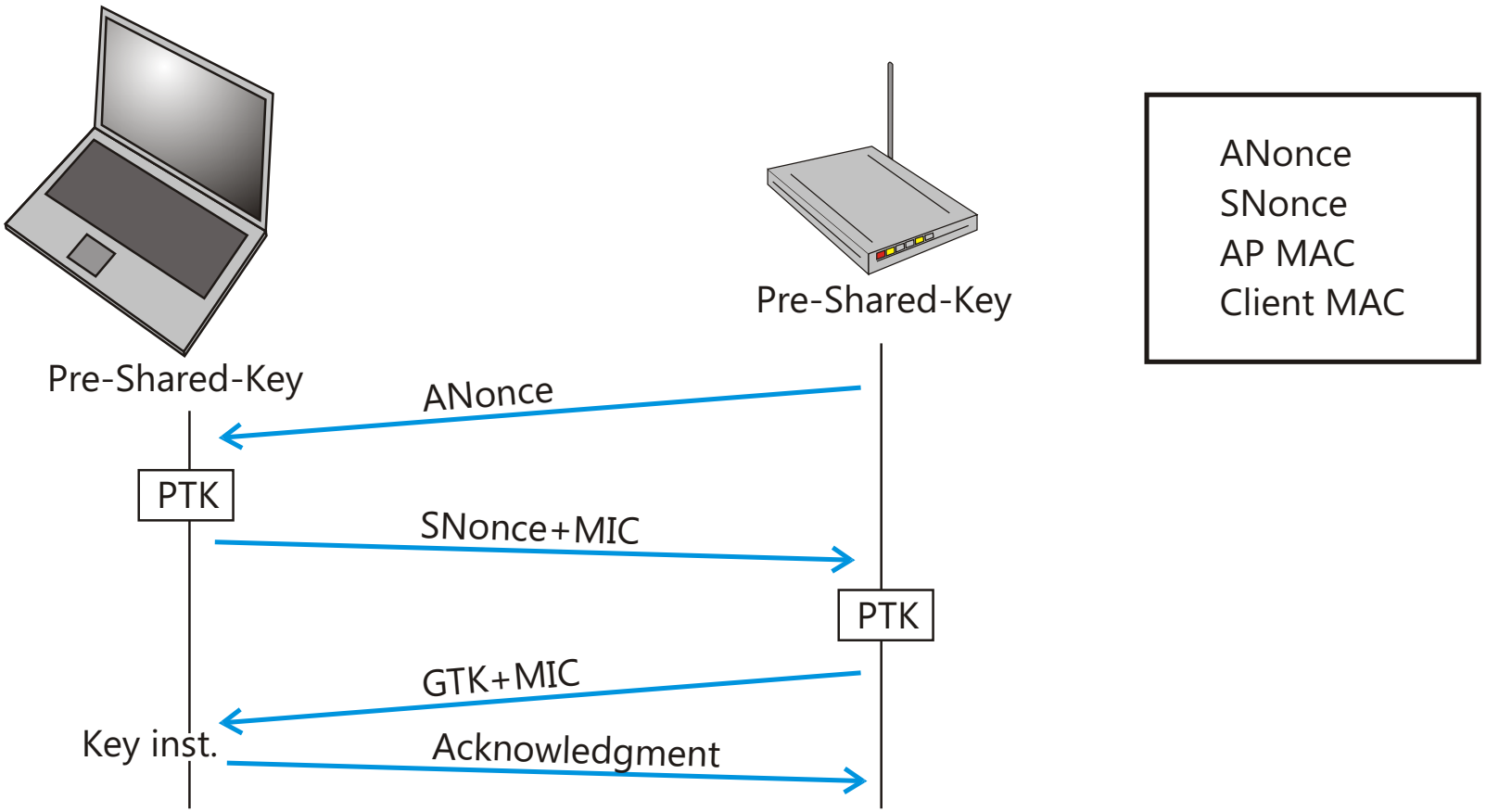
4-Way-Handshake



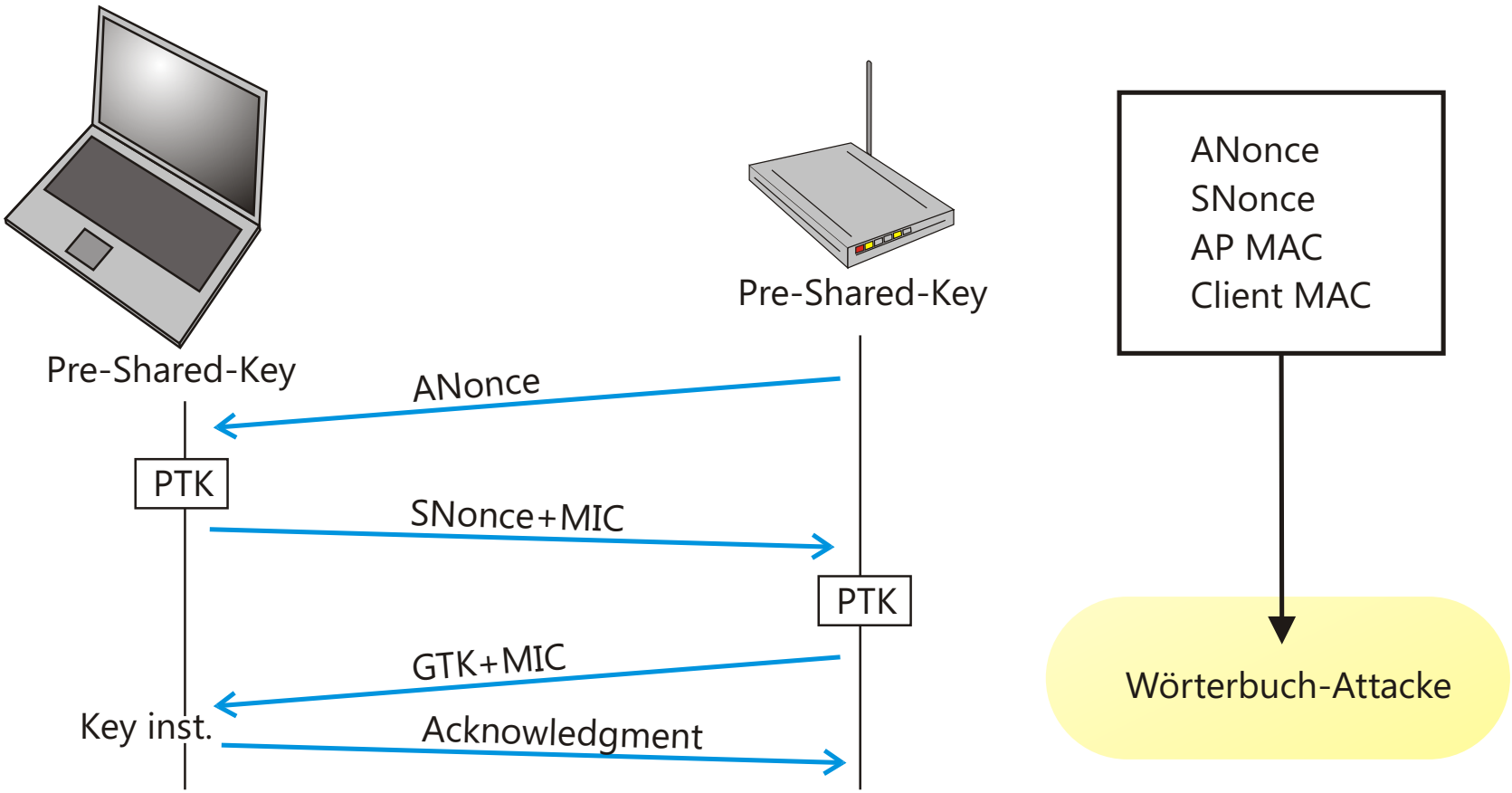
4-Way-Handshake



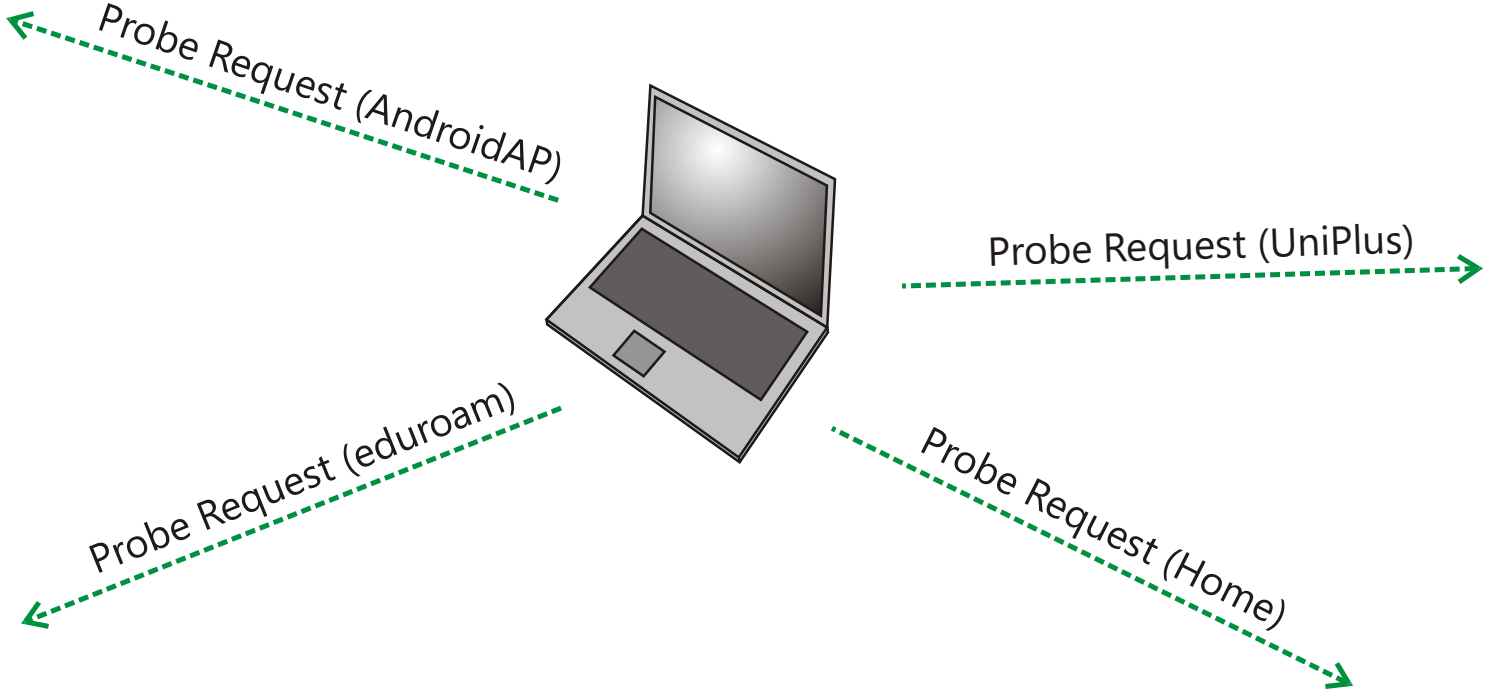
Wörterbuch-Attacke



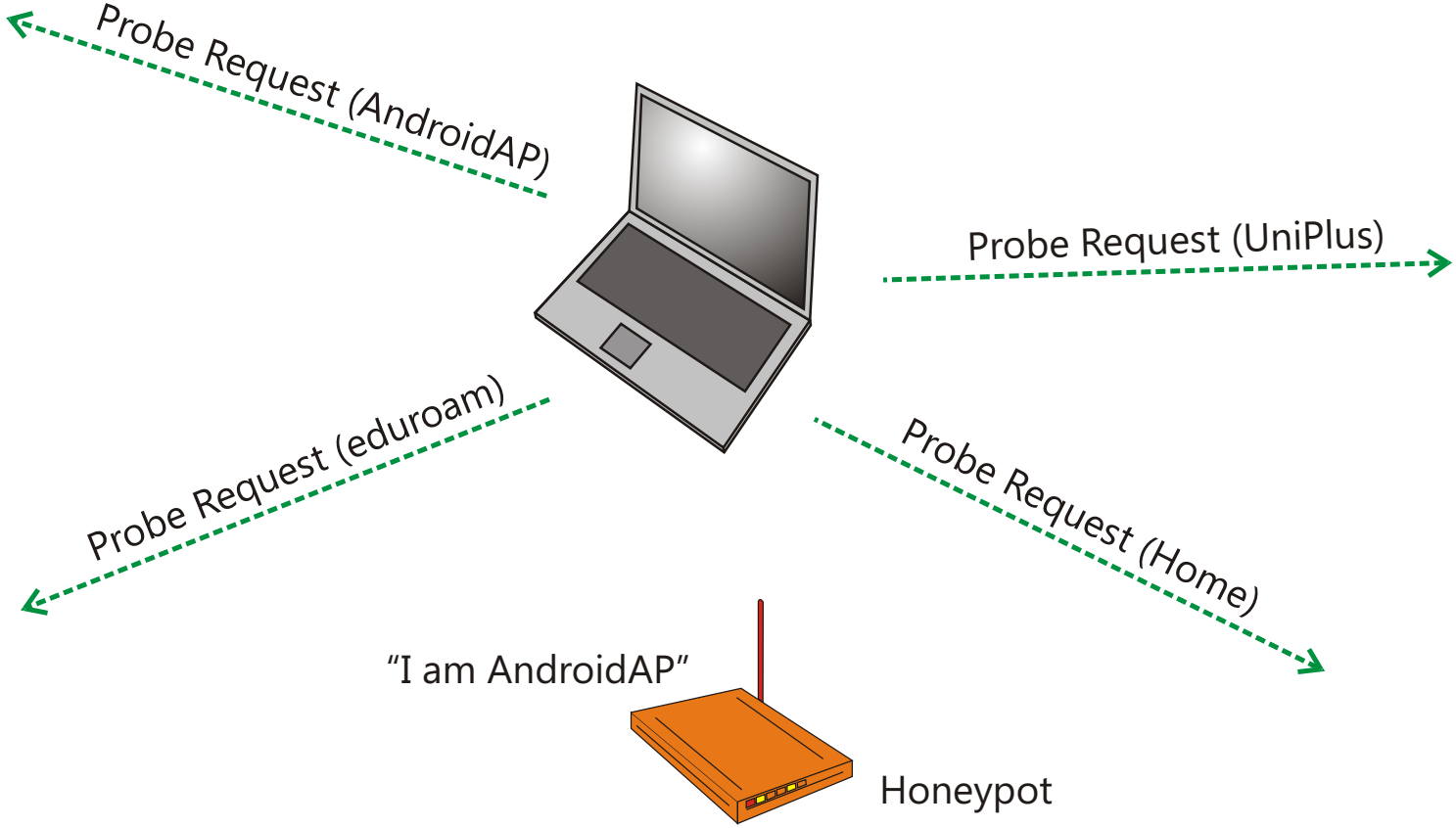
Wörterbuch-Attacke



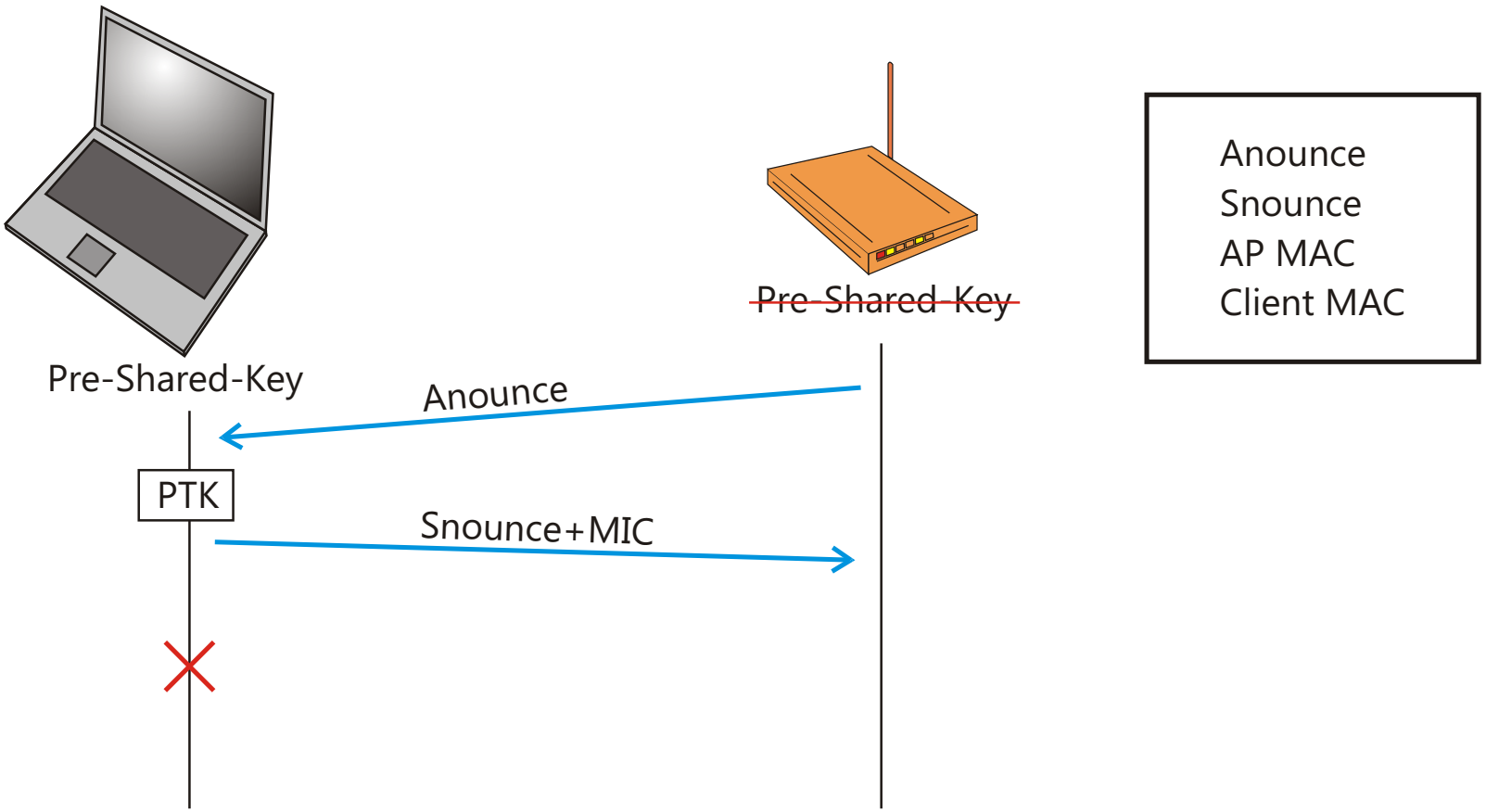
Wörterbuch-Attacke (ohne AP)



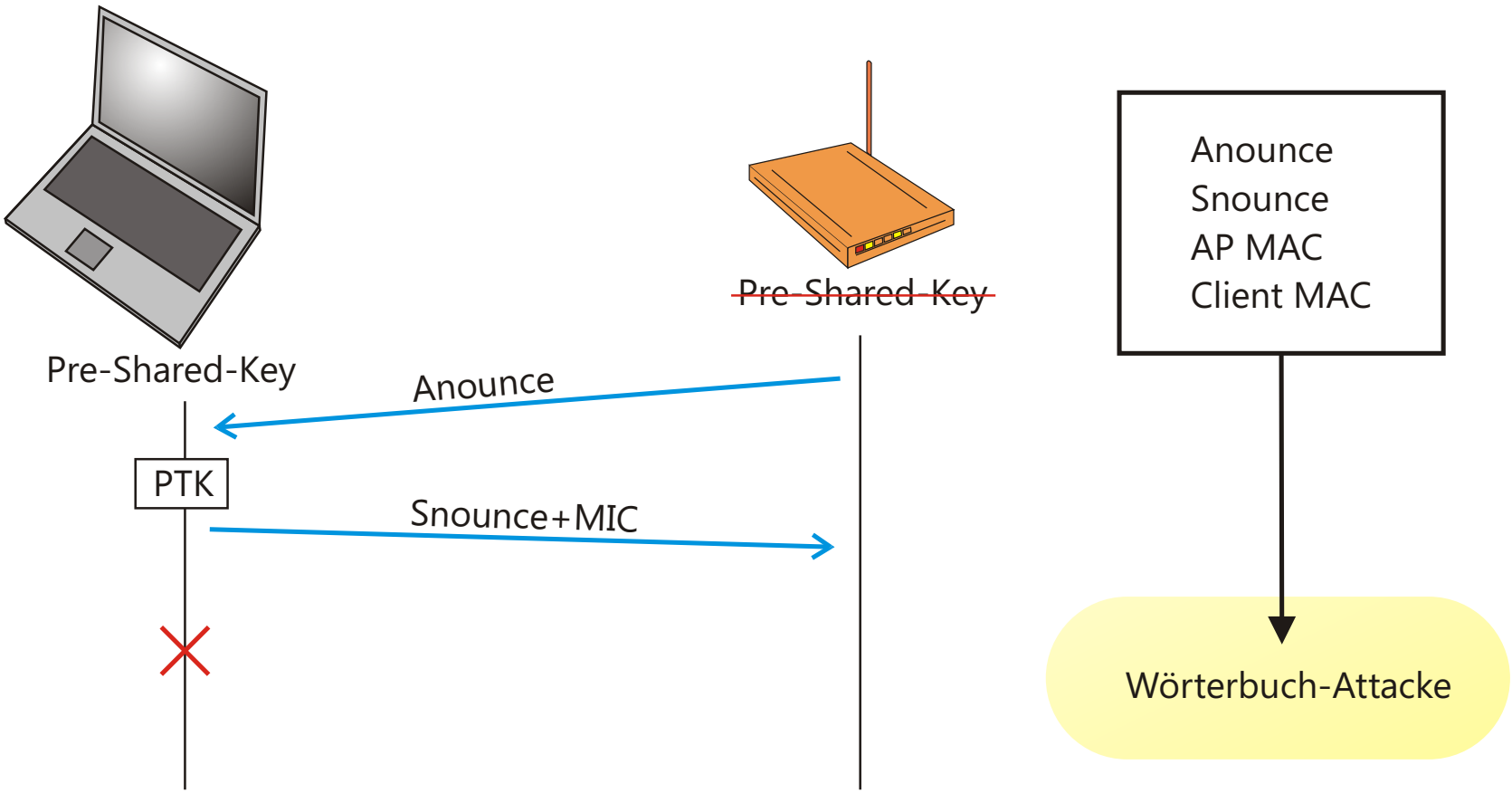
Wörterbuch-Attacke (ohne AP)



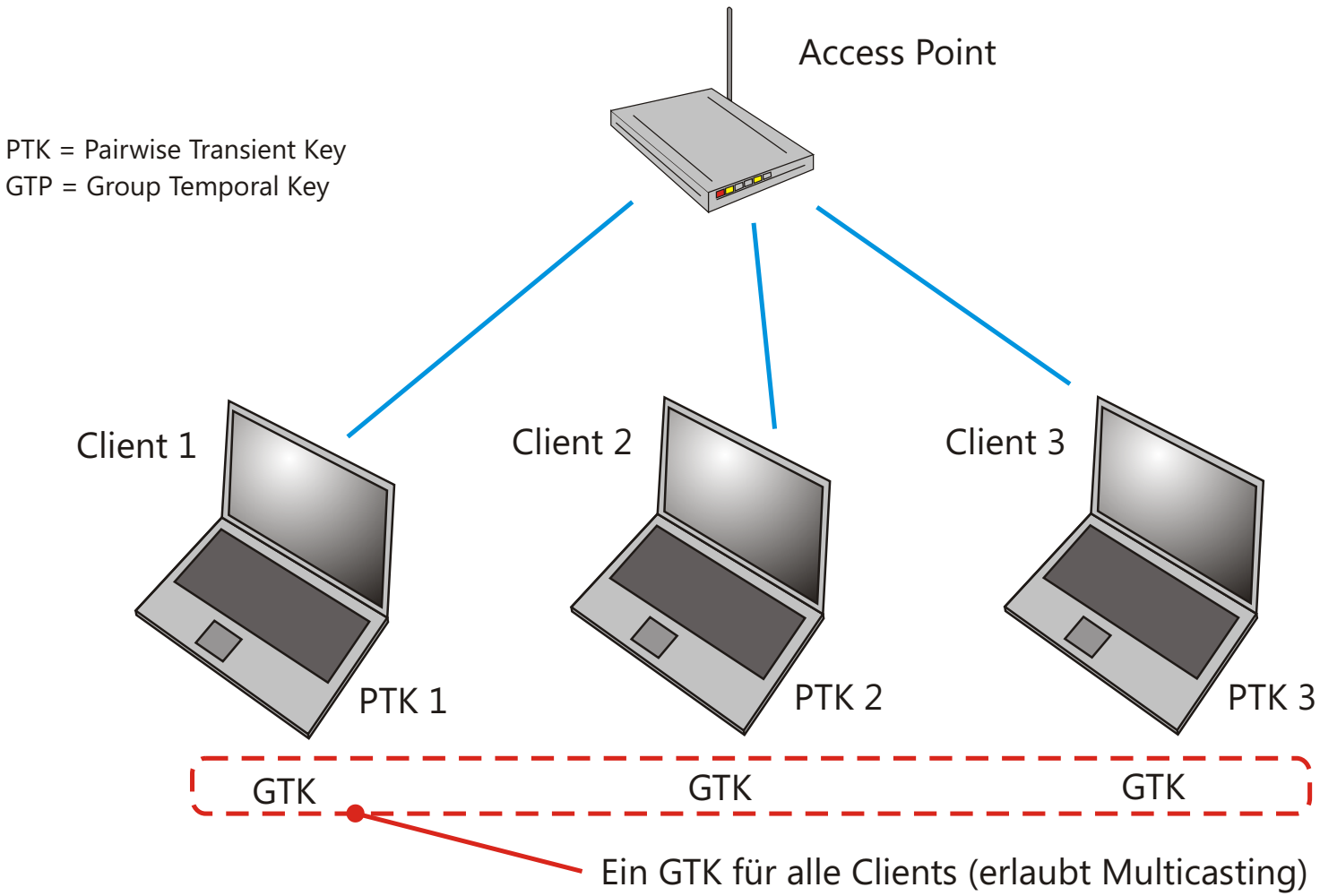
Wörterbuch-Attacke (ohne AP)



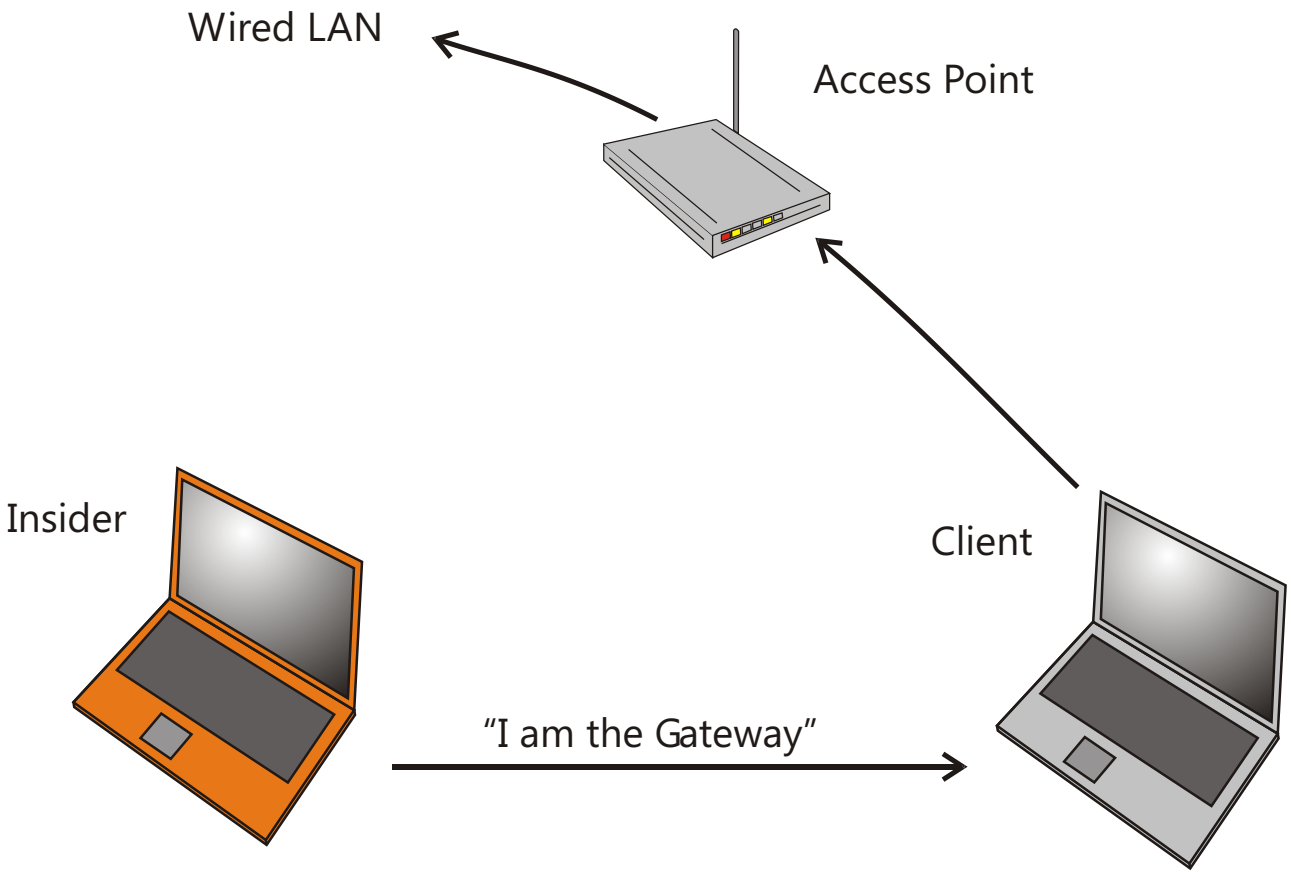
Wörterbuch-Attacke (ohne AP)



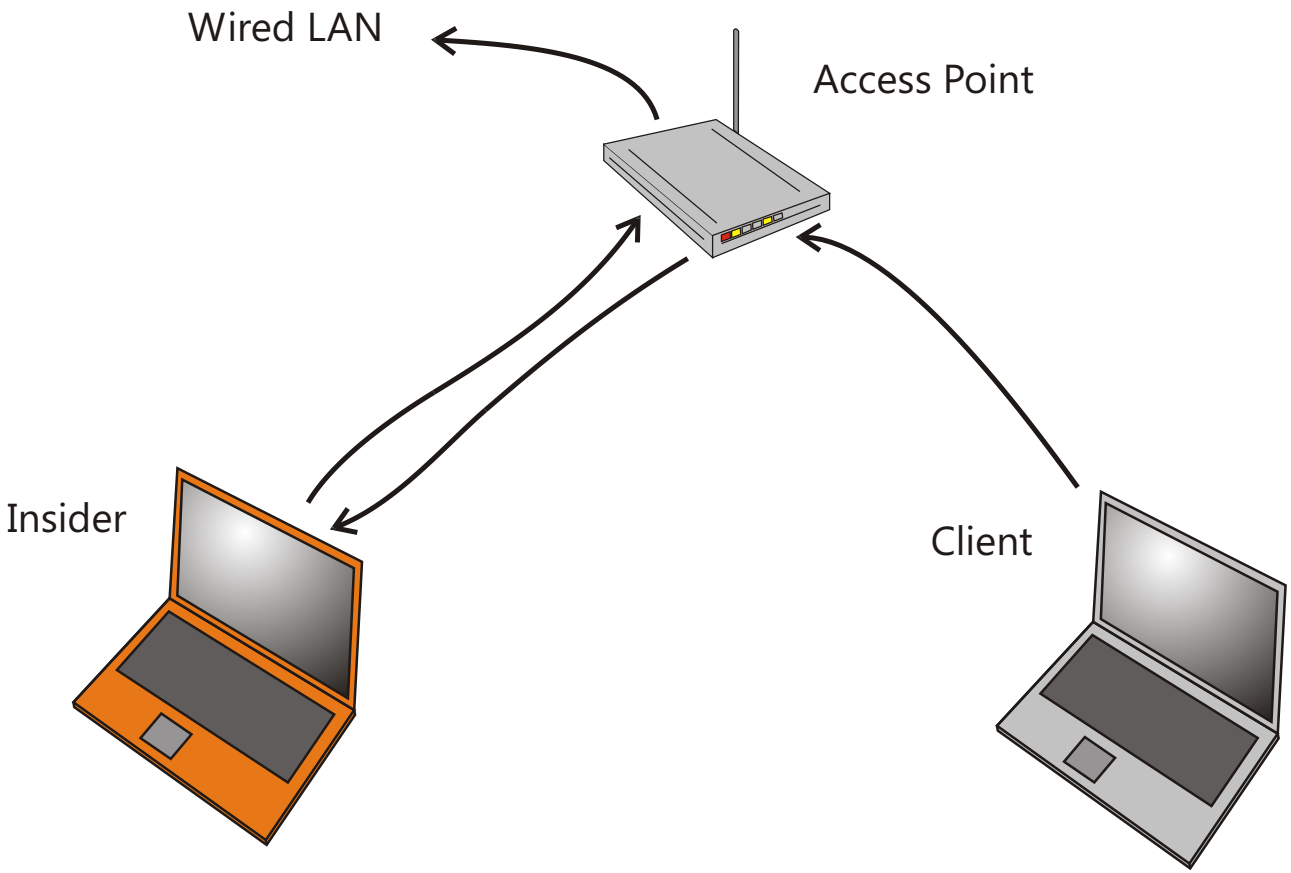
Hole 196


Access Point
PTK = Pairwise Transient Key
GTP = Group Temporal Key
Client 1
Client 2
Client 3
PTK 1
PTK 2
PTK 3
GTK
GTK
GTK
Ein GTK für alle Clients (erlaubt Multicasting)

Hole 196 - ARP Poisoning



Hole 196 - Man-in-the-Middle



Danke für Ihre Aufmerksamkeit!