conVens
Business Consulting

KRACK

Schwachstelle im WPA2-Protokoll
gefährdet alle WLAN-fähigen Geräte

Andreas Stevens
conVens GmbH

Warum WPA2?

conVens Business Consulting

- Ein unverschlüsseltes WLAN kann von jedem genutzt werden.
- In einem unverschlüsselten Netzwerk können alle Daten mitgelesen werden.
- Mit WPA2 verschlüsselt man ein WLAN.
  - Nur Nutzer mit dem WLAN-Passwort können sich am Access-Point anmelden.
  - Die Übertragung zwischen Client und Access-Point ist verschlüsselt und kann nicht von anderen Teilnehmern im Netzwerk mitgelesen oder manipuliert werden.

Was ist KRACK?

conVens Business Consulting

- **KRACK = K**ey **R**einstallation Att**ack**
- Design-Lücke/Schwachstelle im Wi-Fi Protected Access 2 (WPA2) Protokoll
  - Aushebelung des sogenannten 4-Wege-Handshake, Session-Key wird kompromittiert (Im dritten Schritt kann der Schlüssel mehrfach gesendet werden, bzw. mit Nullen).
  - Attacke zwingt Client zur unverschlüsselten Kommunikation mit dem Access-Point.
- Man-in-the-Middle-Angriff
  - Angreifer kann die Kommunikation zwischen Client und WLAN-Access-Point mittels geklonten Access-Point mitlesen und Daten manipulieren.
  - Angreifer muss in Reichweite des Client und dem Access Point sein.

Wer ist betroffen?

conVens Business Consulting

- **Alle** WLAN-Geräte mit WPA2-Verschlüsselnung, inkl. Personal- und Enterprise-Varianten, auch WPA-TKIP, AES-CCMP.
- Linux und Android ab Version 6.0 (41% der Geräte) besonders gefährdet, da der Aufwand bei diesen Betriebssystemen gering ist.
- Liste bekannter Hersteller bereitgestellt von Carnegie Mellon University: https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4
- AVM-Router laut eigener Aussage nicht betroffen, da die Norm IEEE 802.11r (fast roaming) nicht verwendet wird.
- Telekom: "Aktuell gehen wir von gar keiner oder von einer sehr eingeschränkten Betroffenheit unserer WLAN-Router aus, da unsere Geräte die bei einem Access Point betroffenen WLAN-Standards nicht implementieren.“

Was macht KRACK nicht

conVens Business Consulting

- WLAN-Passwort entschlüsseln / herausgeben
- Zusätzliche SSL/TLS-Verbindung (https bei Webseiten) entschlüsseln

  Aber HTTPS kann von dem Man-in-the-Middle *deaktiviert* werden!
- Auf andere Geräte im WLAN-Netzwerk zugreifen

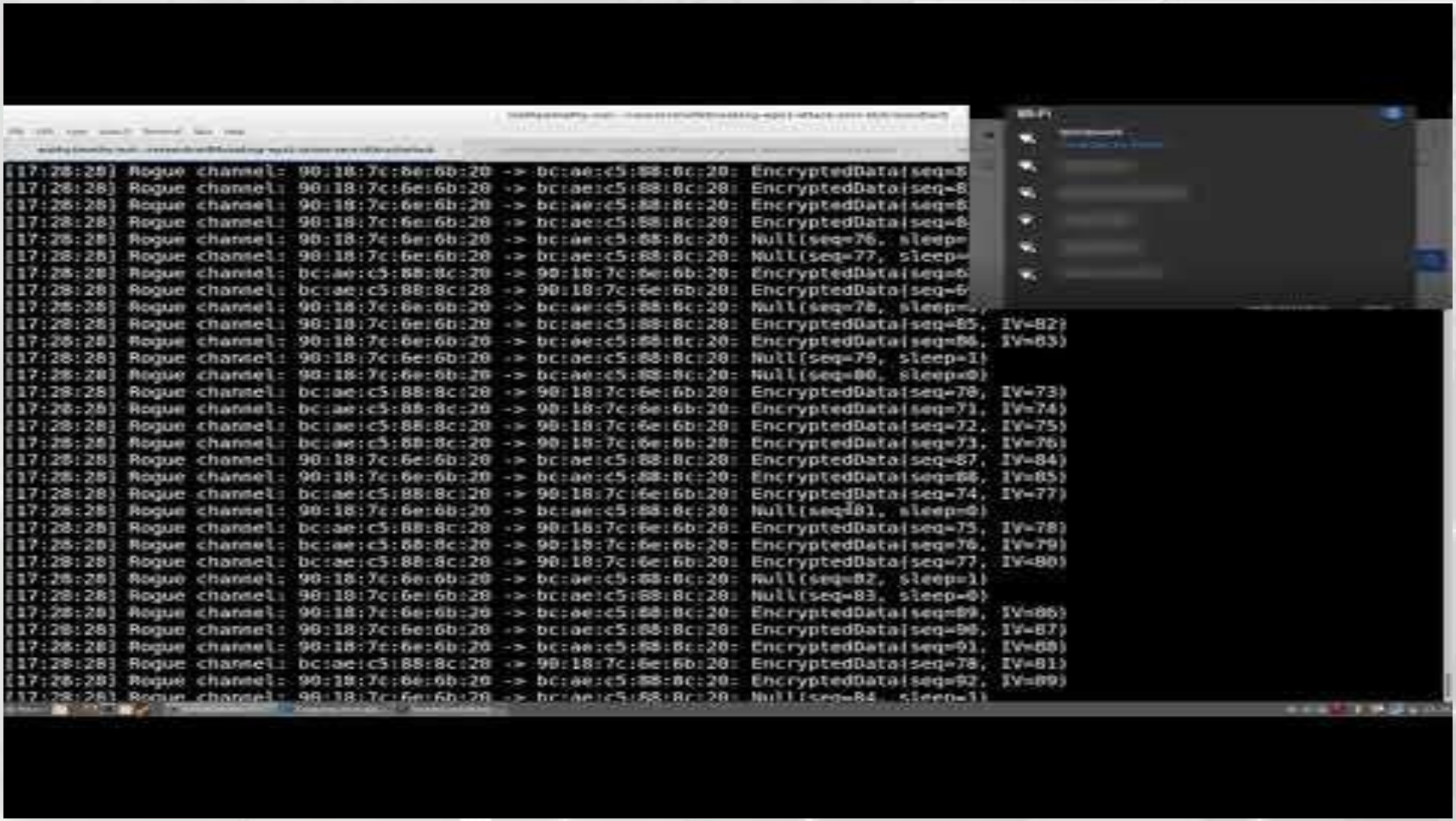
Wie schütze ich mich?

conVens Business Consulting

- Sicherheits-Updates einspielen (wenn verfügbar).
- Zusätzlich SSL/TLS (z.B. HTTPS-Verbindungen beim Online-Banking, Logins) verwenden und darauf achten, dass die Verschlüsselung aktiv ist / angewendet wird.
- Virtual Private Network (VPN) nutzen.
- Kein WLAN nutzen (nicht praktikabel).

Demo

conVens
Business Consulting



https://www.youtube.com/watch?v=Oh4WURZoR98&feature=youtu.be

Danke

conVens
Business Consulting

Andreas Stevens
Geschäftsführer

conVens GmbH

Sittarder Str. 25
52538 Gangelt

Telefon +49 24 54 / 935 19 27
Telefax +49 24 54 / 935 19 29

Web www.convens.de
E-Mail kontakt@convens.de

Quellenangaben:

conVens Business Consulting

- Mathy Vanhoef & Frank Piessens - KU Leuven, Belgien
  - https://www.krackattacks.com/
  - https://doi.org/10.1145/3133956.3134027
- Heise Security:
  - https://www.heise.de/security/meldung/WPA2-Forscher-entdecken-Schwachstelle-in-WLAN-Verschluesselung-3862379.html
  - https://www.heise.de/security/meldung/Details-zur-KRACK-Attacke-WPA2-ist-angeschlagen-aber-nicht-gaenzlich-geknackt-3862571.html
  - https://www.heise.de/security/meldung/KRACK-Hersteller-Updates-und-Stellungnahmen-3863455.html
- Avira:
  - https://blog.avira.com/de/wpa2-wifi-krack/