Wie sicher ist ihr WLAN?

DI DI Christoph Lang-Muhr

Agenda

/informatik & security /fh/// st.pölten

- Überblick WLAN
- WLAN Standards
- Verschlüsselungsverfahren
- Bedrohungen

Überblick

- Was ist WLAN?
  - Wireless Local Area Network
  - … auch Wi-Fi genannt (Kunstbegriff – USA, GB, …)
  - Lokales Funknetz
  - Kabellose Netzwerkverbindung – Shared Medium Prinzip
  - … alle Geräte teilen ein Übertragungsmedium
    - **Sicherheit (Abhören, Manipulieren, …)**
    - **Keine eindeutige räumliche Begrenzung**

Überblick

/informatik & security /fh/// st.pölten

- Bestandteile einer WLAN-Umgebung (Minimum)
  - Access Point

WLAN Standards

/informatik & security /fh/// st.pölten

- 1997 Standardisiert
- IEEE 802.11 Standard
  - 802.11 a 5 GHz 54 Mbit/s
  - 802.11 b 2,4 GHz 11 Mbit/s
  - 802.11 g 2,4 GHz 54 Mbit/s
  - 802.11 n 2,4 + 5 GHz 540 Mbit/s
  - **802.11 ac* 5 GHz >1.3 Gbit/s**
  - 802.11 ad** 60 GHz 6.7 Gbit/s

* Aktuelle Entwicklung

** Standard in Vorbereitung

Verschlüsselung

- Warum Verschlüsseln?
  - Wer darf das WLAN benutzen
  - Wer darf Daten im WLAN lesen
  - Wer darf Daten im WLAN senden
- Vertraulichkeit
  - … Daten werden nur zw. berechtigten Sender/Empfänger versandt
- Authentisierung
  - … nur berechtigte Sender dürfen senden – Einschleusung von Nachrichten unterbinden
- Datenintegrität
  - … Daten dürfen am Weg nicht verändert werden

WEP – Wired Equivalent Privacy

- Älteste Verschlüsselung
  - 1999
- Ron Cipher 4 Algorithmus

WEP - Sicherheit

- Komplett Kompromittiert
  - Schwachstellen im Protokoll
  - Schwachstellen im RC4-Algorithmus

- **Keine Vertraulichkeit garantiert**
- **Keine Integrität garantiert**
- **Keine Authentizität garantiert**

WPA – WiFi Protected Access

- 2003 von der Wi-Fi Allianz entwickelt
- Verbesserungen gegenüber WEP
  - Dynamische Schlüsselgenerierung/Paket – TKIP
  - IV auf 48 Bit verdoppelt
  - Integrity Check Value (ICV) eingeführt
  - Message Integrity Check (MIC – Michael) eingeführt
    - Bezieht Headerdaten in die Berechnung mit ein
    - Fungiert als Fehlercounter (Verbindungsabbruch – Replay-Angriff)

WPA – WiFi Protected Access

- Authentifizierungssysteme
  - WPA Personal (WPA-PSK)
    - Für SOHO-User Umgebungen
    - Keine zusätzliche Hardware notwendig
    - Pre-Shared-Key (PSK) Authentifizierung
    - Schlüssel muss jedem Gerät in der WLAN Umgebung bekannt sein
  - WPA Enterprise (WPA-Radius)
    - Für 802.1x Umgebungen
    - Authentifizierung und Key-Management auslagern (Hardware)
    - Schlüssel kann für jeden Client separat generiert werden

WPA - Sicherheit

- Bekannte WEP Schwachstellen ausgebessert
- Wordlist-attacks möglich
  - Grund: Pre-Shared Master Key (PMK)
    besteht aus: Passphrase und SSID
  - PMK in der gesamten BSS (alle verbundenen Geräte)
  - 4-Way-Handshake Schlüssel abhören
- Reauthentication auslösen
  - Unbemerkt am Client Reauthentication auslösen
  - 4-Way-Handshake Schlüssel abhören
- **Qualität der Passphrase bestimmt erheblichen Teil der Sicherheit!**

WPA – WiFi Protected Access 2

- 802.11i Standard
- 2004 durch die Wi-Fi Allianz veröffentlicht

- Neuer Verschlüsselungsalgorithmus
  - AES (Advanced Encryption Standard) – anstelle von MIC & RC4
    - Alte Hardware ist nicht mehr Kompatibel
  - Grundlage ist der TKIP-Algorithmus

WPA 2 Sicherheit

- Gleiche Attacke wie bei WPA möglich
  - 4-Way-Handshake Schlüssel abhören

- So sicher wie der vergebene Pre-Shared-Key
  - Wörterbuchattacke möglich
  - Mehr Rechenaufwand notwendig durch AES

Bedrohungen

- WLAN Passwort Cracking
- WPS Angriffe
- Man in the Middle Attacken / Phishing Methoden

WLAN Password Cracking - WEP

/informatik & security /fh/// st.pölten

- Seit einiger Zeit Tools im Umlauf (Open Source)
  - Aircrack-ng Suite
- Sehr einfache Bedienung
  - Wenige Zeilen in der Command Line
  - Grafische User Interfaces verfügbar - Fern Wifi Cracker
- Benötigte Hardware
  - WLAN Karte die den Monitoring Modus unterstützt
- Zeitraum der Attacke
    - **Wenige Minuten**

WEP sollte nicht mehr verwendet werden !!!

WLAN Password Cracking – WPA/WPA2

- Seit einiger Zeit Tools im Umlauf (Open Source)
  - Aircrack-ng Suite
- Sehr einfache Bedienung
  - Wenige Zeilen in der Command Line/ Grafische User Interfaces
- Benötigte Hardware
  - WLAN Karte die den Monitoring Modus unterstützt
- Wordlist
  - Liste aller möglichen Passwörter
  - Vorberechnete Passwörter aus dieser Liste (optional)
- Zeitraum der Attacke
  - Wenige Minuten bis Jahre

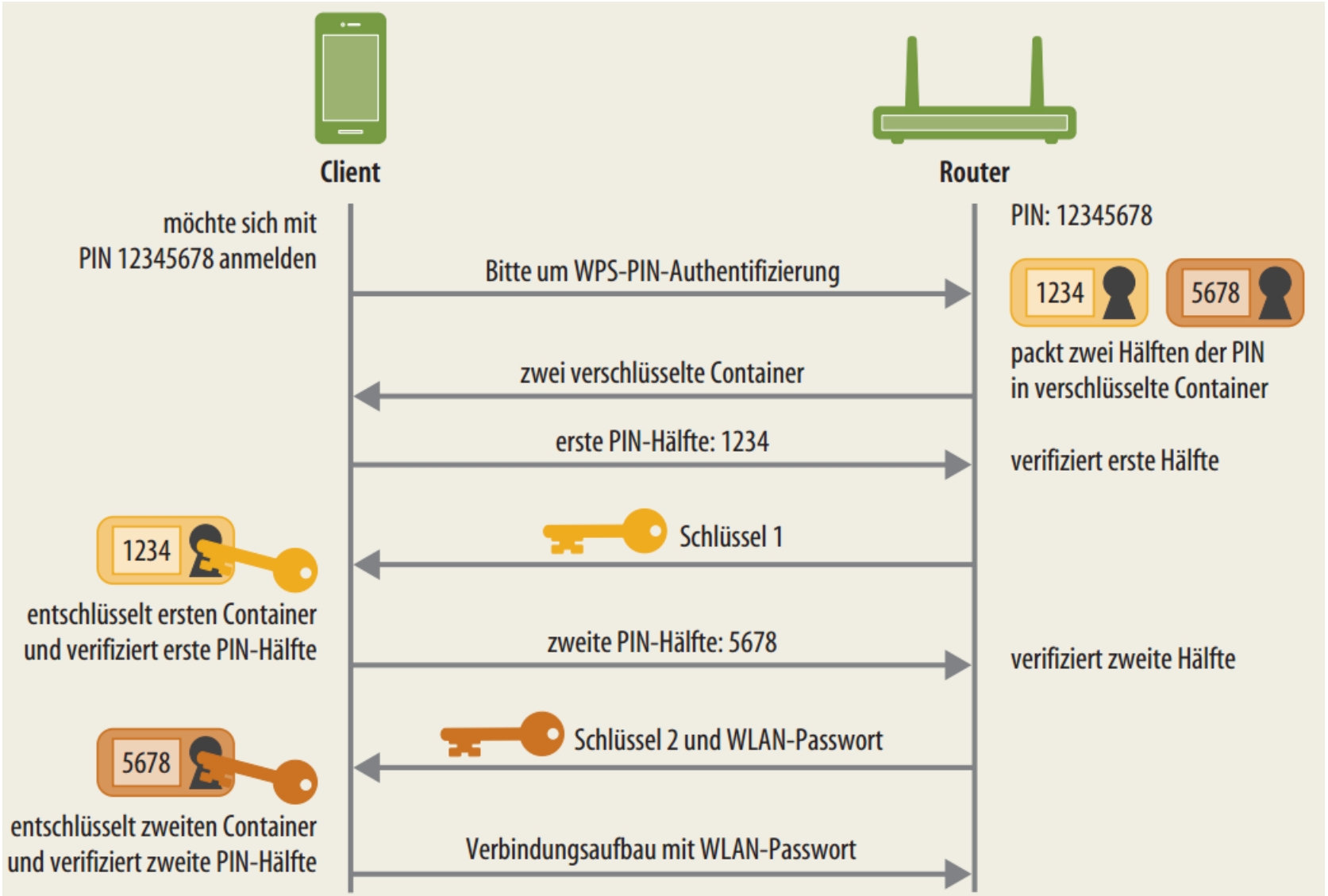
Qualität der Passphrase bestimmt die Sicherheit!

WPS-WiFi Protected

/informatik & security /fh/// st.pölten

- Erstmaliger Verbindungsaufbau mit PIN
  - Um bessere Passwörter verwenden zu können ohne Sie sich merken zu müssen.
  - mit 8 stelligem PIN zum Erhalt des WLAN-Passwortes
- Mehrere Methoden
  - PBC – Push Button Methode - WLAN-Passwort wird kurze Zeit nach Drücken des Button gesendet
  - Internal Registrar - Pin des Clients muss am WLAN Access Point eingegeben warden
  - **External Registrar – PIN des Routers/APs am Client eingeben**
    - **Router lauscht immer auf PINs**

WPS – WiFi Protected Setup



WPS - Angriff

/informatik & security /fh/// st.pölten

- Designschwäche
  - Router/AP antwortet welcher Teil welcher Teil des PINs falsch wahr → drastische Reduzierung des Rechenaufwandes
  - Fehlerhafte Implementierung in den Geräten – Pixie Dust Schwachstelle
- Tools im Umlauf (Open Source)
  - Reaver, WPSCrack, Theiver, PixieWPS, wash
  - Grafische Tools – Fern Wifi Cracker

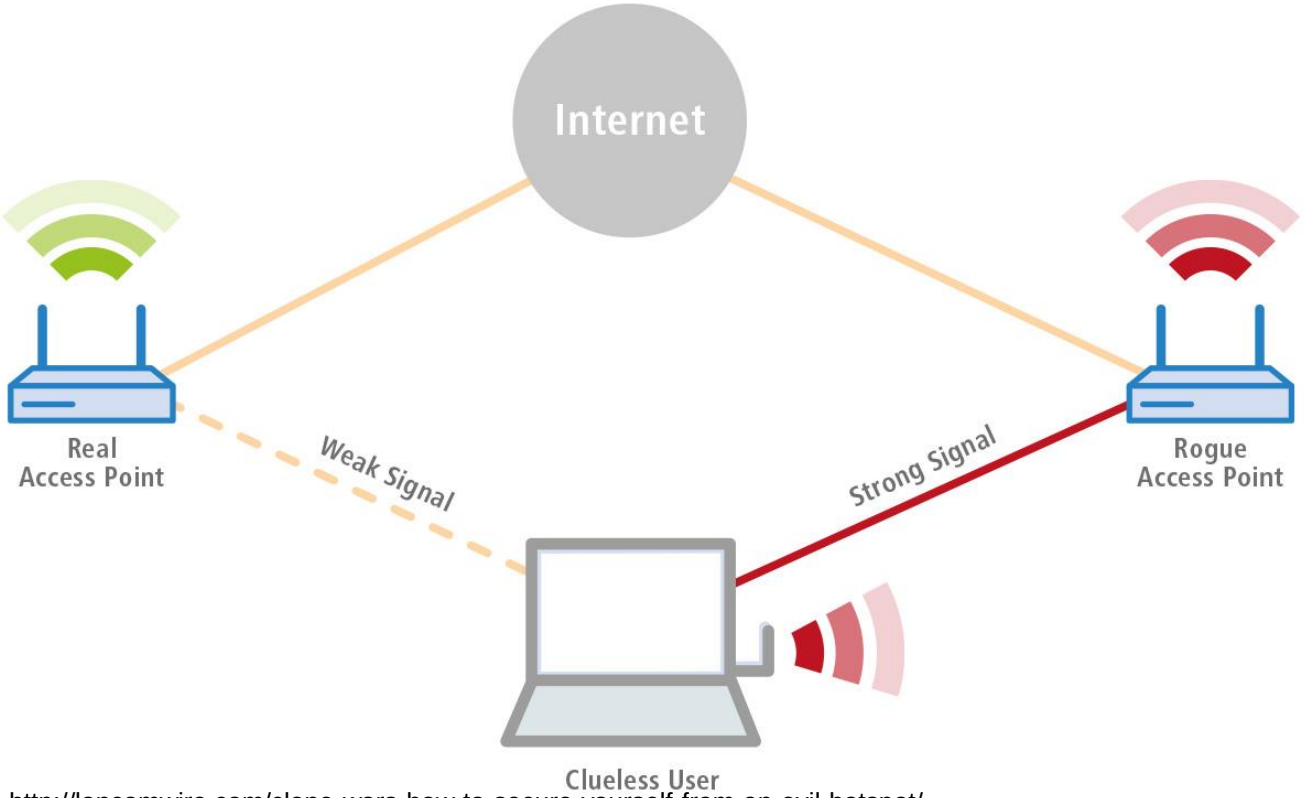
WPS - Angriff

- Sehr einfache Bedienung
  - Wenige Zeilen in der Command Line
- Benötigte Hardware
  - WLAN Karte die den Monitoring Modus unterstützt
- Zeitraum der Attacke
    - Wenige Minuten bis 10 Stunden (ca. 11.000 Versuche) – bei Brute Force
    - Bis zu 30 min bei Routern mit der Pixie Dust Schwachstelle

WPS deaktivieren !!!

Man in the Middle Attacken

- User ist das Ziel des Angriffes
- Angreifer platziert sich zwischen User und Router/AP



http://lancomwire.com/clone-wars-how-to-secure-yourself-from-an-evil-hotspot/

Man in the Middle Attacken

/informatik & security /fh/// st.pölten

- Bedrohungen
  - Mitlesen der übertragenden Daten
  - Manipulieren der übertragenen Daten
  - Malware in den Datenstrom einbetten
  - Phising Attacken

- Tools im Umlauf (Open Source)
  - Pineapple – Wifi Honeypot (Hardware)
  - Wifi Pumpkin
  - Wifiphisher – Versucht über eine Phising Site das WLAN Passwort zu erhalten

Man in the Middle Attacken

/informatik & security /fh/// st.pölten

- Gegenmaßnahmen
  - Detektieren von Rogue Access Points durch die bestehende WLAN Infrastruktur → Deaktivierung
  - Aktuelle Betriebssysteme verbinden sich nicht mehr zu bereits bekannten WLANs die plötzlich ohne Passwort verfügbar sind
  - Verschlüsselung des Datenverkehrs
    - SSL im Browser nutzen
    - VPN in unsicheren Umgebungen nutzen