Wireless-LAN-Sicherheit

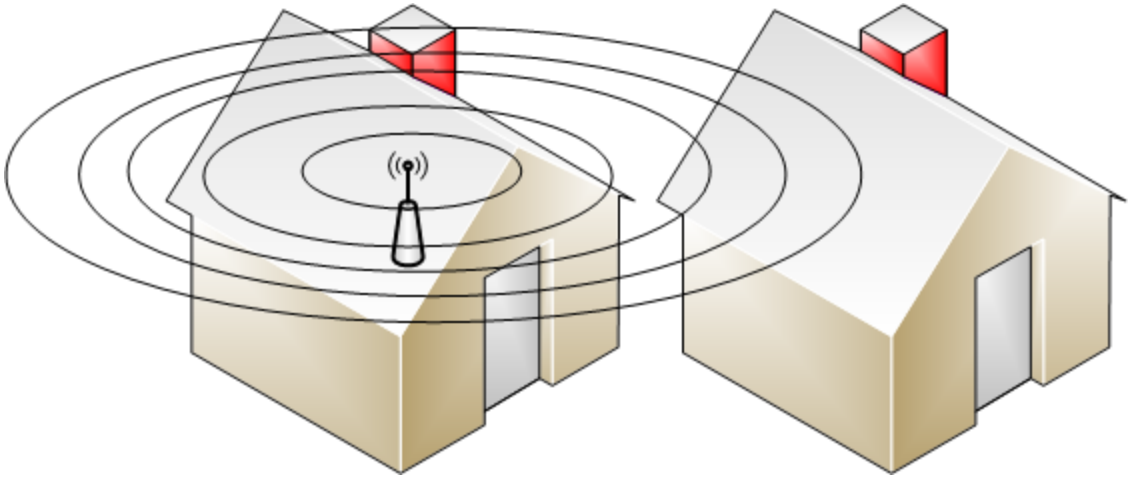
Matthias Wawrzik
PING e.V. Sommerfest
07.08.2010
m.wawrzik@ping.de

Inhalt

1) Grundsätzliches zur Absicherung
2) Gesetzliche Situation
3) Verschlüsselung
    1) WEP
    2) WPA
    3) WPA2
4) Authentifizierung
    1) PSK
    2) 802.1X, RADIUS
5) Zusammenfassung
6) Weitere Maßnahmen

1. Grundsätzliches zur Absicherung

- Funkkommunikation = Broadcast
- Kommunikationsradius schwer einschränkbar



1. Grundsätzliches zur Absicherung

- Begehrter Internet-Anschluss?
  - Download von „Raubkopien“
  - Kriminelle Kommunikationswege
  - Digitale Straftaten
- Brisante Daten im Netzwerk?
  - Industriespionage
  - Teleoffice

2. Gesetzliche Situation

12. Mai 2010, Bundesgerichtshof:

„Haftung des WLAN-Netz-Betreibers – Der Betreiber eines unzureichend gesicherten WLAN-Anschlusses kann als Störer für Rechtsverletzungen Dritter auf Unterlassung und Erstattung von Abmahnkosten in Anspruch genommen werden.“

3. Verschlüsselung

WEP

WPA

WPA2

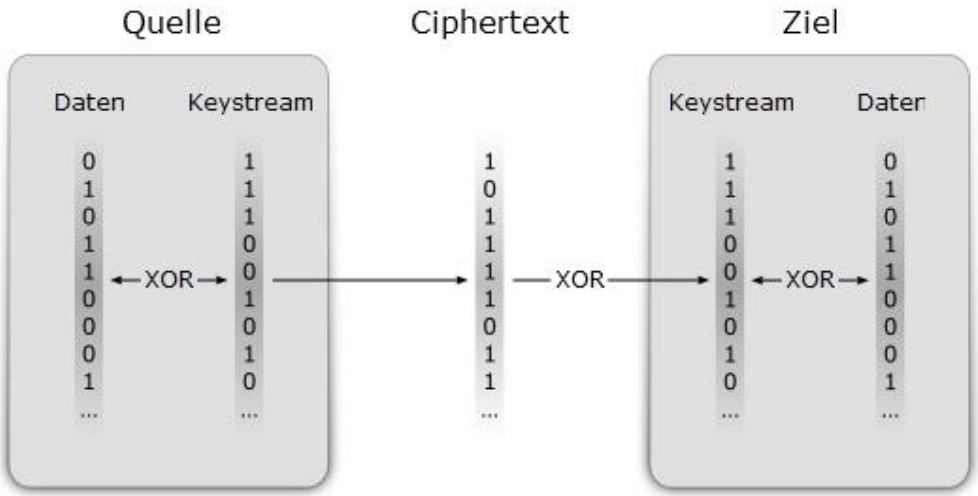
3. Verschlüsselung - WEP

- **W**ired **E**quivalent **P**rivacy

  (dt. eine der Verkabelung entsprechende Privatsphäre)
- früherer Standard im Bereich WLAN
- Verwendet statische Schlüssel zur Absicherung
  - 64 bit
  - 128 bit
- „BD46FE64E848CF9CD8E9E60346“

3. Verschlüsselung - WEP

- Prinzip:
  - Keystream wird aus Schlüssel gebildet (RC4)
  - Daten + Keystream bilden Übetragungsdaten
  - Der Empfänger entschlüsselt die Daten wieder



3. Verschlüsselung – WEP

Sicherheitsrisiken:

- WEP lässt sich in < 1 min knacken
- Voraussetzung: aktiver Datentransfer
- Passives Monitoring zum Errechnen des WEP-Schlüssels
- Flooding mit ARP-Requests

3. Verschlüsselung – WPA

- **W**i-Fi **P**rotected **A**ccess
- Nachfolger von WEP
- Zertifizierung 2003
- Nutzt dynamische Schlüssel durch TKIP
- Unterstützung von Authentifizierungsmethoden

3. Verschlüsselung – WPA

Sicherheitsrisiken:

- Auch in kürzerer Zeit entschlüsselbar
- Angriffe speziell gegen das TKIP-Protokoll
- durch GPU-Berechnungen beschleunigt
- Brute-Force oder Wörterbuchattacken

3. Verschlüsselung – WPA2

- Nachfolger von WPA
- Derzeit aktueller und sicherster Standard
- Nutzt zu TKIP zusätzlich CCMP (AES) zum Verschlüsseln
- Gefahren durch TKIP somit umgangen

4. Authentifizierung

- „Anmeldung“
- Sicherstellung von
  - Identität
  - Authorität
- Leitet in den verschlüsselten Datenverkehr
- Ab WPA: 2 verschiedene Methoden
  - PSK
  - 802.1X

4. Authentifizierung - PSK

- **P**RE-**S**HARED-**K**EY (dt. ausgeteilter Schlüssel)
- Simple Methode für private Netzwerke
- Identisches Passwort auf allen Teilnehmern
- SICHER:
  - Möglichst komplexe Passwörter
  - Mindestens 20 Zeichen (gegen Brute Force)
  - Groß- und Kleinschreibung, Zahlen, Sonderzeichen
  - Keine echten Wörter (Wörterbuchattacke)
  - „bzZB23;2!sdLL!“7§44Vse=(eSFc/-84“

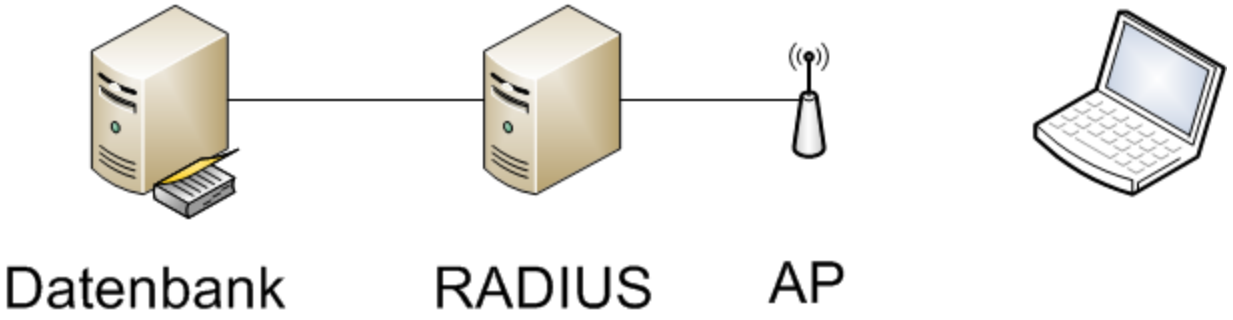
4. Authentifizierung – 802.1X

- Kein PSK zur Authentifizierung
- ca 40 verschiedene Authentifizierungsprotokolle
- Nutzt grundsätzlich alternative Daten:
  - Benutzername und Passwort
  - Zertifikate
- Anwendungszweck
  - Große Netzwerke
  - Individuelle Login-Daten

4. Authentifizierung – 802.1X

Beispiele:

- EAP-TLS
- LEAP
- PEAP-MSCHAPv2



5. Zusammenfassung

- Bei WEP-only Geräten:
  - Kauf neuer Hardware
- Bei WPA/WPA2 fähigen Geräten:
  - Wenn möglich, auf WPA2-PSK (CCMP/AES) stellen
  - Möglichst langes und komplexes Passwort
  - Für Profis: Nutzung von WPA2-802.1X

6. Weitere Maßnahmen

„Mehr Sicherheit bedeutet in der Regel weniger Komfort, es gilt den bestmöglichen Kompromiss zu finden “

6. Weitere Maßnahmen

- MAC-Filterung

00:1E:2F:BA:D3:11

- Jedes Netzwerkgerät besitzt einmalige MAC
- Access-Control-List mit zugelassenen MACs
- Nachteil:
  - Umständliche Skalierbarkeit
  - MAC auf Client leicht änderbar

6. Weitere Maßnahmen

- Drosselung der Sendeleistung
- „verstecken“ der SSID
- Abschalten von DHCP
- Zeitabschalten
- Logische Trennung von LAN und WLAN
- Verschlüsselung in darüber liegenden Protokollen (VPN)

Abschluss

Vielen Dank für Ihre Aufmerksamkeit!