



WLAN - IEEE 802.11 Wireless LAN

- WLAN oder "Wireless Ethernet" ist sehr populäre drahtlose Netzwerktechnologie, die unter dem Namen Wi-Fi von IEEE im Standard 802.11 klassifiziert wurde
- WLAN-Standard IEEE 802.11 wurde entwickelt, um Funk-basierte drahtlose Datenübertragungen auch im Internet zu ermöglichen
- Der Standard spezifiziert das Kommunikationsprotokoll auf den untersten Schichten eines drahtlosen Netzwerks
- WLAN ist heute das am weitesten verbreitete Kommunikationsprotokoll in drahtlosen Netzwerken



- **Mobiles Gerät**
 - WLAN-fähige Geräte
- **WLAN-Antenne**
 - zum Senden und Empfangen der Funksignalen
- **Access Point (AP) / Basisstation**
 - Stellt kabelloses Netzwerk bereit und verbindet mobile Geräte mit einem stationären Netzwerk, z.B. mit dem Internet



Im WLAN gibt es große Sicherheitsrisiken, da es **grundsätzlich schwierig** ist, in drahtlosen Netzwerken Nachrichten und Privatsphäre zu schützen

- Datenpakete werden über Funkverbindungen übertragen und Jeder in Reichweite kann sie empfangen. Damit besteht die permanente Gefahr des Abhörens der Verbindung

Sicherheitsmaßnahmen sind unbedingt erforderlich

- **Besondere Vorsicht** ist geboten bei Nutzung **öffentlicher WLAN-Netzwerke** (Hotel, Flughafen, Bahnhof, City, ...)

Gebräuchliche Sicherheitsmechanismen:

- WLAN-Verschlüsselung – **teilweise unsicher**
- MAC-Adressen-Filter – **unsicher**
- Verstecken der ESSID – **unsicher**
- Generelle Vorsicht beim Surfen,
Verwendung von SSL-Verschlüsselung – **empfohlen**
- Verwendung von verschlüsselten Datentunneln,
sogenannter **VPNs** (Virtual Privat Networks) – **empfohlen**

Bekannte Sicherheitsmechanismen: WLAN-Verschlüsselung (1/3)

WLAN-Verschlüsselung

Verschlüsselung des Netzwerkverkehrs auf der untersten Netzwerkebene

- **Typische Verfahren:**
 - WEP,
 - WPA,
 - **WPA2**
- WEP und WPA gelten heute als **unsicher** und sollten möglichst nicht mehr verwendet werden
 - WEP ist binnen Minuten knackbar, also ein kompletter Zugriff auf das Netzwerk ist möglich
 - WPA ist anfällig für das knacken einzelner Datenpakete, kleine Teile von Nachrichten können also gelesen werden

Bekannte Sicherheitsmechanismen: WLAN-Verschlüsselung (2/3)

WLAN-Verschlüsselung

- Aktuell sicheres Verfahren ist WPA2
 - Möglichst WPA2-CCMP verwenden und nicht WPA2-TKIP
 - (Bisher) keine Schwachstellen (öffentlich) bekannt
- **Trotzdem:** Auch bei Verwendung von WPA2 (natürlich auch bei WEP und WPA) auf **starke Passwörter** achten
 - Schwaches Passwort kann in kurzer Zeit geknackt werden und kompletter Netzwerkzugriff wird möglich (→ siehe Woche 2, Rategeschwindigkeit >1 Mio/Sek)
 - Nutzung eines möglichst eindeutigen Netzwerknamen (ESSID), da häufig verwendete ESSIDs das Erraten von Passwörtern erleichtern

Bekannte Sicherheitsmechanismen: WLAN-Verschlüsselung (3/3)

WLAN-Verschlüsselung

- **WPS – Wi-Fi Protected Setup** ist Verfahren zum (vermeintlich) sicheren Schlüsselaustausch
 - Eingabe von Passwörtern für WPA/WPA2 soll durch einfachere Methoden erleichtert werden
 - Eingabe einer PIN
 - Drücken eines Knopfes am Router
 - Aber: Methoden haben **größere Schwachstellen**, die das Eindringen ins Netzwerk ermöglichen

→ **WPS sollte also im Router deaktiviert werden**

Bekannte Sicherheitsmechanismen: MAC-Adress-Filter

MAC-Adress-Filter

- Häufig vorgeschlagene Sicherheitsmethode um nur ganz bestimmte Geräte zum Netzwerk zuzulassen und Cyberkriminelle auszusperrern
 - wird im Router konfiguriert
 - für jedes erlaubte Gerät muss dessen Hardwareadresse im Router eingetragen werden
- **Aber:** Schutz ist **nicht ausreichend wirksam**
 - Hardwareadresse eines Geräts ist leicht veränderbar
 - Cyberkriminelle können Adresse eines erlaubten Gerätes abhören und sich dann selbst unter dieser Adresse mit dem Netzwerk verbinden

Bekannte Sicherheitsmechanismen: Verstecken des Netzwerknamens (ESSID)

Verstecken des Netzwerknamens (ESSID)

- Häufig vorgeschlagener Mechanismus, um das eigene Netzwerk vor Cyberkriminellen zu verstecken
 - Es können sich nur Geräte mit dem Netzwerk verbinden, die dessen Netzwerknamen, also seine ESSID kennen
 - ESSID muss beim Einrichten der Verbindung manuell eingegeben werden
- **Aber:** Schutz ist **nicht ausreichend wirksam**
 - Netzwerkverkehr und ESSID kann mit entsprechender Software abgehört und erkannt werden
 - Sobald die ESSID in Erfahrung gebracht ist, kann man sich ganz normal mit dem Netzwerk verbinden

Generelle Vorsicht beim Surfen, Verwendung von SSL-Verschlüsselung

- Wird in öffentlichen Netzwerken gesurft, sollte man sich bewusst machen, dass jeder mithören kann
- Selbst wenn ein öffentliches Netzwerk verschlüsselt ist (z.B. Restaurant- oder Hotel-WLAN), können alle im Netzwerk mitlesen
- **Daher:** Sensible Daten sollten nur über verschlüsselte Verbindungen abgerufen werden
 - Sicherstellung, dass mit HTTPS gesurft wird
 - ...

Generelle Vorsicht beim Surfen, Verwendung von SSL-Verschlüsselung

- **Daher:** Sensible Daten sollten nur über verschlüsselte Verbindungen abgerufen werden
 - Insbesondere bei Eingabe von Nutzer-Passwort-Daten sollte auf SSL-Verbindung geachtet werden
 - Login-Seite selbst sollte schon SSL-gesichert sein, nicht erst nachdem das Login stattgefunden hat
 - Email-Server sollten über SSL abgerufen werden (Konfiguration im Email-Programm)
 - Auch Messenger-Apps (z.B. WhatsApp unter iOS) kommunizieren teils unverschlüsselt
 - ...

Verwendung von verschlüsselten Datentunneln (VPN)

- Nicht alle Dienste und Webseiten stehen in verschlüsselter Form zur Verfügung
- Verschlüsselter Kommunikationskanal in Form eines "**Virtual Private Networks**" (**VPN**) kann alle Daten schützen
- VPN ist ein virtuelles, verschlüsseltes Netzwerk, das auf einem vorhandenen Netzwerk aufbaut
 - Verschlüsselter Datenstrom wird über eine normale, unverschlüsselte Verbindung versendet („Tunneling“)
 - Über VPN kann ein sicheres internes Netzwerk auch für Nutzer aus der Ferne (Remote User) zugänglich gemacht werden
- **Problem:** VPN sind meist schwerer einzurichten

Empfohlene Sicherheitsmaßnahmen

Beim privaten WLAN

- Verwendung von WPA2-CCMP-Verschlüsselung im privaten Bereich
- Auswahl eines starken WLAN-Passworts (muss auch nur einmal im Gerät eingegeben werden)
- WPS am Router ausschalten
- Optional: Verbergen der ESSID, um etwas verborgener zu sein

Beim öffentlichen WLAN

- Verwendung von verschlüsselten Verbindungen und Verzicht auf unverschlüsselte Dienste, falls sensible Daten ausgetauscht werden
- Bessere Alternative: **Verwendung eines VPNs**

Beim privaten WLAN

- Verwendung von WPA2-CCMP-Verschlüsselung im privaten Bereich
- Auswahl eines starken WLAN-Passworts (muss auch nur einmal im Gerät eingegeben werden)
- WPS am Router ausschalten
- Optional: Verbergen der ESSID, um etwas verborgener zu sein

Beim öffentlichen WLAN

- Verwendung von verschlüsselten Verbindungen und Verzicht auf unverschlüsselte Dienste, falls sensible Daten ausgetauscht werden
- Bessere Alternative: **Verwendung eines VPNs**