



Universität
Zürich^{UZH}

Institut für Informatik

Wireless LAN (WLAN) Sicherheit

Prof. Dr. Rolf Oppliger



Übersicht

1. Einführung
2. WEP
3. WPA
4. WPA2
5. Sicherheitsempfehlungen
6. Situation an der UZH (inkl. IFI)
7. Schlussfolgerungen und Ausblick



1. Einführung

- Das **Institute of Electrical and Electronics Engineers (IEEE)** ist u.a. im Bereich der Standardisierung von LAN/MAN-Technologien aktiv (Komitee **IEEE 802**)
- **IEEE 802.11** umfasst eine Familie von Standards für **Wireless LANs (WLANs)**
- Aufgrund der hohen Verwundbarkeit gegenüber passiven Angriffen sind im Rahmen von IEEE 802.11 auch Protokolle für den Einsatz von kryptografischen Sicherheitsverfahren ausgearbeitet und standardisiert worden
- Diese Protokolle zeichnen sich durch unterschiedliche Eigenschaften und kryptanalytische Stärken und Schwächen aus



2. WEP ^{1/4}

- **Wired Equivalent Privacy (WEP)** ist eine kryptografisches Sicherheitsverfahren, das bereits im ursprünglichen, 1999 verabschiedeten IEEE 802.11-Standard vorgesehen war
- Die kryptografische Absicherung der Daten basiert auf **RC4** (Stromchiffrierung mit variabler Schlüssellänge) und **CRC-32** (Prüfsummenbildung)
- Aufgrund der U.S. amerikanischen Exportkontrollen wurde zu Beginn meist **WEP-40** eingesetzt (Schlüssellänge 40 Bit + 24 Bit langer im Klartext übertragener Initialisierungsvektor)
- Später wurde vermehrt auch **WEP-104** eingesetzt (Schlüssellänge 104 Bit + 24 Bit langer Initialisierungsvektor)



WEP ^{2/4}

- Weil RC4 eine Stromchiffrierung ist, muss sichergestellt sein, dass ein WEP-Schlüssel nicht mehrfach eingesetzt wird (ansonsten sind kryptanalytische Angriffe möglich)
- Das kann mit einem „nur“ 24 Bit langen Initialisierungsvektor nicht sichergestellt werden (weil sich WEP-Schlüssel dann zu häufig wiederholen)
- Entsprechend sind aus der Literatur relativ viele (und zum Teil auch effiziente) Angriffe auf den Einsatz von RC4 im Rahmen von WEP bekannt
- Diese Angriffe sind zum Teil in Programmen wie `Aircrack-ng` implementiert



WEP ^{3/4}

- Die Authentifizierung des Client gegenüber dem Access Point ist im Rahmen von WEP optional (**Open System** vs. **Shared Key** Authentifizierung)
- Falls eine Authentifizierung stattfindet, sendet der Access Point dem Client eine Zufallszahl (als **Challenge**), die dieser mit dem WEP-Schlüssel chiffrieren und (als **Response**) zurücksenden muss
- Dieser Challenge-Response-basierte Datenaustausch kann zur Rekonstruktion des WEP-Schlüssels genutzt bzw. missbraucht werden
- Entsprechend wird im Rahmen von WEP meist eine Open System (d.h. keine) Authentifizierung empfohlen



WEP 4/4

- Aufgrund der Mängel sowohl bei der kryptografischen Absicherung der Datenübertragung als auch bei der Authentifizierung der Clients gegenüber dem Access Point gilt WEP heute als verwundbar
- Insbesondere kann WEP für den praktischen Einsatz nicht mehr empfohlen werden
- Der Data Security Standard (DSS) der Payment Card Initiative (PCI) verbietet explizit den Einsatz von WEP seit 2010



3. WPA ^{1/2}

- **Wi-Fi Protected Access (WPA)** ist ein kryptografisches Sicherheitsverfahren, das 2003 von der Wi-Fi Alliance als Antwort auf die Verwundbarkeiten von WEP vorgeschlagen wurde
- WPA umfasst einen grossen Teil des sich damals in Ausarbeitung befindlichen Standards **IEEE 802.11i**
- Insbesondere umfasst WPA das **Temporal Key Integrity Protocol (TKIP)**, das 128 Bit lange Paket-spezifische Schlüssel als Ersatz für die statischen WEP-Schlüssel erzeugt
- WPA nutzt ein Verfahren namens **MICHAEL**, um einen **Message Integrity Check (MIC)** als Ersatz für CRC-32-Prüfsummen zu bilden
- Die kryptografische Absicherung der Datenübertragung ist im Rahmen von WPA gegenüber WEP deutlich verbessert



WPA ^{2/2}

- Allerdings sind in der jüngeren Vergangenheit auch Angriffsmöglichkeiten gegen WPA aufgezeigt worden
- Im Rahmen von WPA kann die Authentifikation auf der Basis eines **Pre-Shared Keys (PSK)** oder eines dedizierten Authentifizierungsservers (im Sinne von IEEE 802.1X) erfolgen
- Im zweiten Fall können verschiedene Protokolle auf der Basis des **Extensible Authentication Protocols (EAP)** genutzt werden (z.B. EAP-MSCHAP, EAP-OTP, EAP-TLS, EAP-PEAP, EAP-SIM, ...)
- In Heim- und kleineren Geschäftsinstallationen dominiert WPA- PSK
- Dieses Verfahren ist verwundbar gegenüber Wörterbuchangriffen, d.h. die Netzwerkschlüssel müssen genügend Entropie enthalten bzw. genügend lang sein



4. WPA2

- **Wi-Fi Protected Access 2 (WPA2)** ist 2004 verabschiedet worden und entspricht dem definitiv verabschiedeten Standard IEEE 802.11i (zusammen mit 802.1X)
- In WPA2 wird in erster Linie das **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)** auf der Basis von AES-128 genutzt
- Damit kann simultan die Vertraulichkeit und die Integrität von Nachrichten gesichert werden (Counter Mode und CBC-MAC)
- Die meisten Angriffsmöglichkeiten gegen die kryptografische Absicherung der Datenübertragung im Rahmen von WPA funktionieren nicht für WPA2
- Wörterbuchangriffe sind aber immer noch möglich



5. Sicherheitsempfehlungen

- Default-Werte für Service Set Identifiers (SSIDs) und Passwörter ersetzen (genügend lange Passwörter wählen)
- WLAN-Geräte (z.B. Access Point) so konfigurieren, dass sie nicht über das WLAN (um)konfiguriert werden können
- WLAN-Geräte bei Nichtgebrauch ausschalten
- Sendeleistung der WLAN-Geräte den Gegebenheiten anpassen
- Regelmässige Firmware-Updates einspielen
- Komplementärer Einsatz von Firewall-Technologien
- Andere IP-Adresse für den Router (192.168.1.1 bzw. 192.168.0.1)
- Zugriffskontrolle auf der Basis von MAC-Adressen
- Deaktivierung der SSID-Übermittlung



6. Situation an der UZH (inkl. IFI)

- 3 WLANs (gemäss <http://www.id.uzh.ch/dl/mobil/wlan.html>)
 - SSID `uzh`
 - Authentifikation gemäss IEEE 802.1X (EAP-PEAPv0 und EAP-MSCHAPv2) auf der Basis der UniAccess-Kontodaten
 - Verschlüsselung auf der Basis von WPA2 (AES)
 - SSID `public`
 - keine Authentifikation bzw. Authentifikation über HTTPS/Browser
 - Verschlüsselung auf der Basis von WEP
 - SSID `eurodam` (education roaming) ~ analog `uzh`



7. Schlussfolgerungen und Ausblick

- Das Thema Sicherheit ist seit dem Aufkommen der verschiedenen WLAN-Technologien leider nur pragmatisch angegangen worden
- Entsprechend gibt es verschiedene Verfahren, die auch unterschiedlich resistent gegenüber den relevanten Angriffen sind
- WPA2 scheint heute im praktischen Einsatz sicher zu sein
- Ernstzunehmende Verwundbarkeiten gibt es nur beim Einsatz von PSKs, d.h. es muss darauf geachtet werden, dass die Netzwerkschlüssel genügend Entropie haben bzw. hinreichend lang sind
- Sehr oft werden über Wireless-Verbindungen auch andere kryptografische Sicherheitsprotokolle genutzt (insbesondere auf der Basis von IPsec oder SSL/TLS)