WLAN-Sicherheit

de Lorenzo, Hopfgartner, Wilker

May 8, 2011

Übersicht

- Allgemeines
- IEEE 802.11
- Protokolle
- Sniffer
- Zusammenfassung und Fazit

Allgemeines

Entstehung

- Erste Idee zum 'WLAN' bereits um 1940
  - Frequency Hopping
- Erstes WLAN-Netzwerk auf Hawai 1969
- 1999 WLAN im Privatbereich erschwinglich mit Airport-Technologie
  - damaliger Preis: Funkkarte 100 $, Basisstation 300 $

Warum Sicherheit?

- Netzwerkverkehr in Unternehmen bietet zahlreiche Informationen
  - Daten ber Kunden, Firmenprojekte, etc.
- Interesse an Sicherheit im Privatbereich aus Selbstschutz
  - Wardriving, private Dateien, etc.

IEEE 802.11 Standard

- Verabschiedet vom Institut of Electrical and Electronics Engineers(IEEE) 1997
- Datenrate von 1 bzw. 2 MBit/s
- Lizenzfreie ISM Band mit 2,4 GHz

Erweiterungen Teil 1

802.11b

- 1999 zum Standard hinzugefügt um Datenrate zu erhöhen
- Ist am weitesten verbreitete WLAN-Standard
- ISM-Band zur Funkübertragung
- Datenrate 11 MBit/s

802.11a

- 1999 eingeführt
- Verwendet 5GHz-Band anstelle von ISM-Band
- Datenrate bis 54 MBit/s
- Teile des Frequenzbandes werden in Europa vom Radar zur Flugüberwachung genutzt
  - deshalb werden diese Produkte von ETSI in Europa nicht zugelassen
  - wurde im November 2002 in Deutschland freigegeben

Erweiterungen Teil 2

802.11g

- 2003 eingeführt
- Übertragungsgeschwindigkeit für ISM-Band auf 54 MBit/s erhöht

802.11n

- 2009 eingeführt
- Datenrate wurde auf 600 MBit/s erhöht
- verwendet ISM-Band
  - optional kann 5GHz-Band mitverwendet werden

Vor- und Nachteile der Frequenzbänder Teil 1

2,4GHz-Band

- Vorteile
  - freies ISM-Band
  - hohe Verbreitung, geringe Gerätekosten
  - keine aufwendigen Spektrum-Management-Funktionen (TCP) für volle Sendeleistung nötig
- Nachteile
  - ISM-Band wird mit anderen Geräten geteilt werden, dadurch Störungen
  - Störungsfreier Betrieb mit nur maximal 3 Netzwerken am selben Ort möglich

Vor- und Nachteile der Frequenzbänder Teil 2

5GHz-Band

- Vorteile
  - weniger genutzt, dadurch weniger Störungen
  - höhere Reichweite
  - in Deutschland 19 sich nicht überlappende Kanäle
- Nachteile
  - Stärkere Regulierung in Europa
    - auf manchen Kanälen Betrieb im Freien verboten
  - Ad-Hoc Modus wird von meisten Geräten nicht unterstützt
  - geringere Verbreitung, daher wenig verfügbare Geräte auf dem Markt

Vernetzungsarten Teil 1

Independent Basic Service Set/Ad-Hoc Mode

- die einfachste Form
- Teilnehmer kommunizieren direkt miteinander
- jede Station muss sich im Funkbereich der anderen Stationen befinden
- quasi eine Punkt-zu-Punkt-Verbindung
- hat nur eine kleine Reichweite, deshalb nur für kleine Funknetze geeignet
- kann nicht mit anderen LAN verbunden werden

Abbildung 1: Independent Basic Service Set

Vernetzungsarten Teil 2

Infrastructure Basic Service Set/ Infrastructure Mode

- für große WLANs
- Teilnehmer werden über Basisstation(Access Points) miteinander verbunden
- Teilnehmer kommunizieren über Access Point miteinander
- durch die Weiterleitungsfunktion des Access Point's kann der Funkbereich verdoppelt werden
- kann auch mit LANs verbunden werden

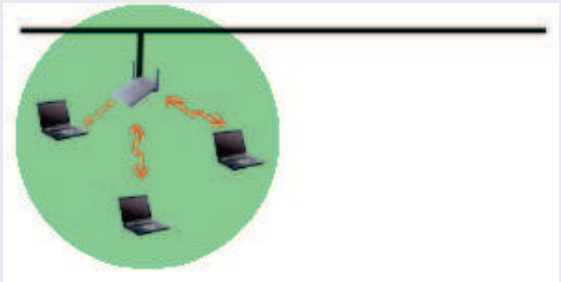


Abbildung 2: Infrastructure Basic Service Set

Vernetzungsarten Teil 3

Extended Service Set

- durch das Verbinden von mehreren Infrastructure Mode erhält man ein Extended Service Set
  - dabei werden die Access Points an ein LAN angebunden
- wird ein größeres Gebiet mit WLAN ausgestattet, dabei können sich Funkzellen überschneiden

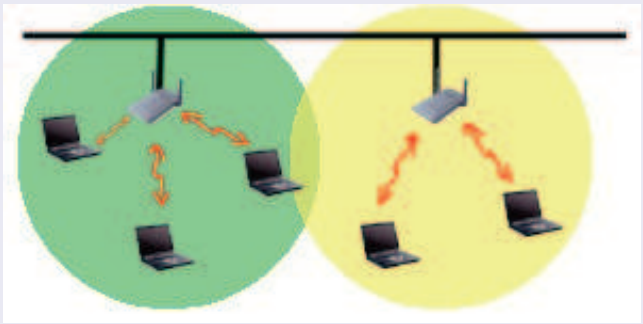


Abbildung 3: Extended Service Set

WEP - Einleitung

Einleitung

- Im September **1999** fertiggestellt
- Teil des IEEE **802.11** Standards
- Ziel - diskrete und integre **Datenübertragung** mittels Funknetzwerk möglich zu machen
- Verschlüsselt in der **Netzwerkebene 2** des OSI-Models

WEP - Authentifizierung

- **Shard Key Authentification**: Authentifizierung über Shared Key
- **Challange-Response**: Client beweist dem Access Point dass er den Shared Key kennt
- → Der **Shared Key** muss vorher bei Client und Access Point hinterlegt werden

WEP - “Bestandteile”

- **Cyclic Redundance Check (CRC)**: Ein Verfahren zur Bestimmung eines Prüfwerts für Daten, um Fehler bei der Übertragung feststellen zu können. Die Prüfsumme ist meist 32 Bit groß.
- **RC-4**
  - Blockchiffre
  - Einfach zu implementieren
  - Variable Schüsselläng (maximal 2048 Bit)
- **Initialisierungsvektor**: 24 Bit Zahl (unverschlüsselt)
- Der **Shared Key** besteht aus 5 oder 13 Zeichen (40 oder 104 Bit)

WEP - Ver-/Entschlüsselung

Verschlüsselung

- Nachricht M $\rightarrow$ Chiffretext C
- $P := M||CRC(M)$
- $Z := RC4(IV||SK)$
- $C := P \otimes Z$

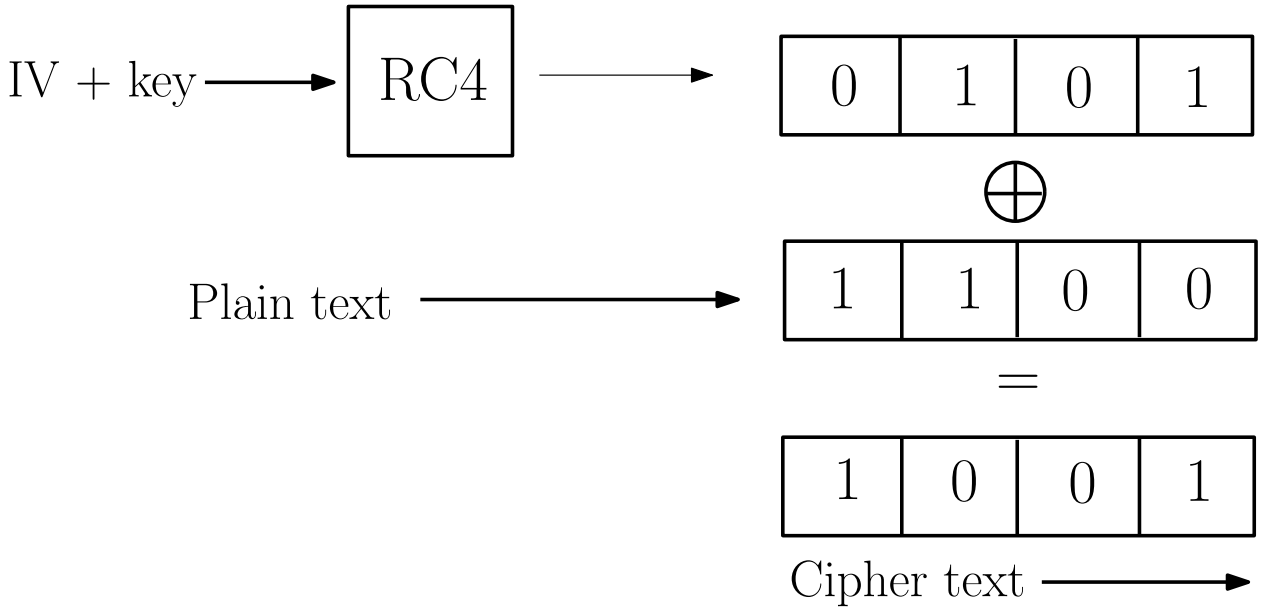
Übertragung

- $IV||C$

Entschlüsselung

- Chiffretext C $\rightarrow$ Nachricht M
- $Z = RC4(IV||SK)$
- $C \otimes Z = P \otimes Z \otimes Z = P$
- $P = M||CRC(M)$

WEP - Ver-/Entschlüsselung (cont.)



WEP - Schwächen

Schwächen

- Zu kurze **Initialisierungsverktoren**
- Bei **Shared-Key-Authentification** ist Klartext und encrypteter Text beobachtbar
- Kleiner Werteraum des **IV** und grosser Anteil an bekannten Daten bei TCP-IP
- Krypt. schwache Schlüssel werden nur z.T. bei der IV-Generierung ausgefiltert
- **Statische Schlüssel**, viele Benutzer verwenden den gleichen Key über Wochen und Monate
- Fehlende Definition zur Wahl des IV im Standard: **Implementationsschwächen**, z.B. Nullinitialisierung, Zähler mit 16 Bit Wraparound, kein Ausfiltern von schwachen IV's
- **CRC32** ist ungeeignet für **Integritätsschutz** der Pakete - somit kein Schutz vor Replay-Attacken

WEP - Lösungen

Lösungen

- Keine **Shared-Key-Authentification**, SSID löschen
- Standardeinstellungen der Hersteller ändern (SSID, Passwort)
- 104 Bit-Keys anstelle 40 Bit-Keys verwenden
- WEP-Keys öfter wechseln
- WLAN-Segmente zusätzlich sichern

WPA - Einleitung

Einleitung

- Zertifizierung **2003**
- Teil des IEEE **802.11i** Standards
- "Nachfolger" von **WEP**
- Unsicher

WPA - Anforderungen

Unterschiede zu WEP

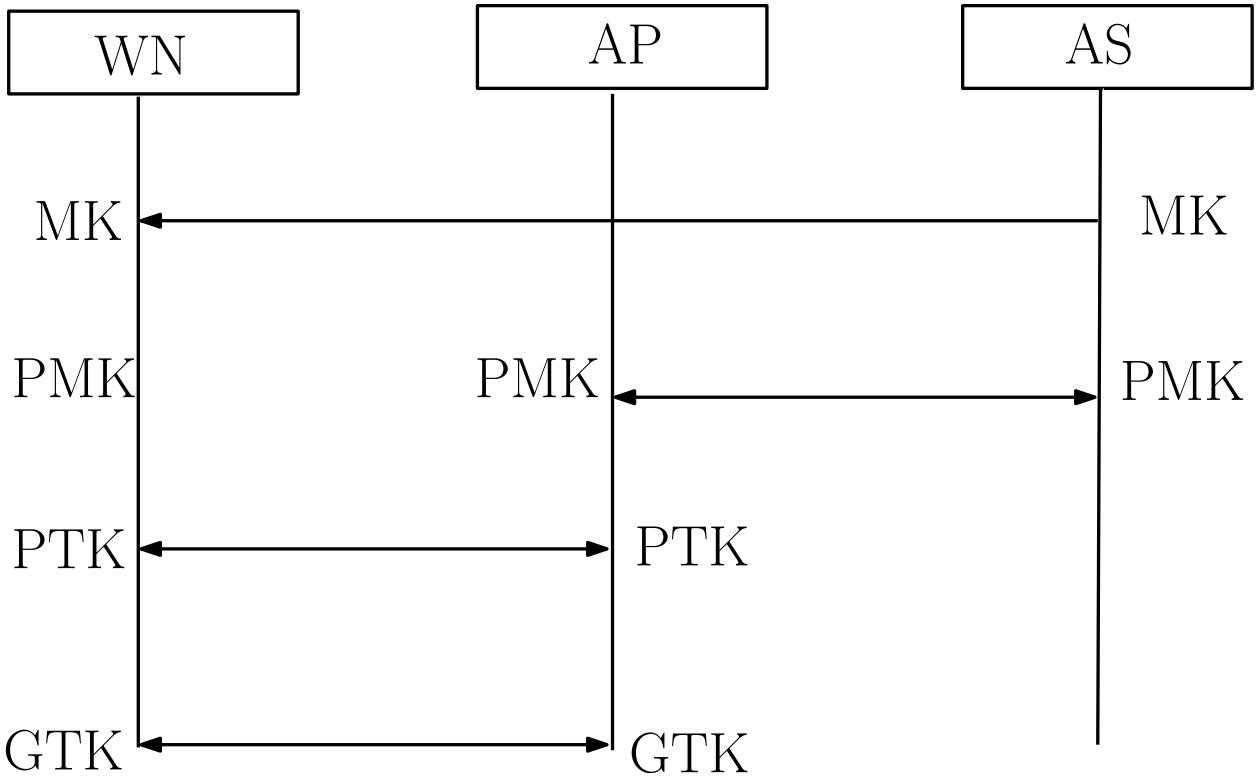
- WPA sollte auf WEP/ RC4 -Hardware implementierbar sein
- **Temporal Key Integrity Protocol (TKIP)** ist das Herzstück des WPA Standards.
- 48-bit Initialisierungs Vektoren
- Integritätssicherung per **Message Integrity Check** Algorithmus
- Authentifizierung mittels **Pre-Shared Key (PSK)** bzw. **Extensible Authentification Protocol (EAP)**

WPA - Schlüsselerzeugung

Schlüsselerzeugung

- PSK: 8-63 ASCII-Zeichen (Passphrase)
- Aus PSK und SSID wird mittels *Hash* der **Pairwise Master ekey (PMK)** berechnet:
  $hash(PSK, SSID) = PMK$
- PMK wird zur Authentifizierung und zur temporären Schlüsselerzeugung verwendet (4-Way Handshake)
- Aus PMK wird mittels Pseudozufallsahlen-Funktion (PZ) der **Parwise Transient Key (PTK)** berechnet:
  $PZ(PMK, Z_1, Z_2, MAC_{AP}, MAC_{Client} = PTK$
- PTK hat zeitlich begrenzte Gültigkeit

WEP - 4-Way Handshake



WPA - Ver-/Entschlüsselung

Verschlüsselung

- **Verschlüsselung**: Nachricht P $\rightarrow$ Chiffretext C
- $P := M||MIC(M||CRC(M||MIC(M)$
- $Z := RC4(IV||K_{Session})$
- $C := P \otimes Z$

Übertragung

- **Übertragung** : $IV||C$

Entschlüsselung

- **Entschlüsselung**: Chiffretext C $\rightarrow$ Nacricht M
- $Z = RC4(IV||K_{Session})$
- $C \otimes Z = P \otimes Z \otimes Z = P$
- $P = M||MIC(M)||CRC(M||MIC(M))$

WPA - Angriffsmöglichkeiten

Angriffsmöglichkeiten

- "**Brute Force**" Attacke
- z.B. "WPA Cracker"
- Zu simpel gewählte **PSK**s machen Einbrüche leichter
- M. Beck und E. Tews ''*A Practical Message Falsification Attack on WPA*" in 10 $\rightarrow$ 15 Minuten geknackt
- "**Man in the Middle**" Attacke mit gerichteten Antennen

WPA - Sicherheitsmaßnahmen

Sicherheitsmaßnahmen

- **Wichtigste:** Sichere **Pass Phrase** wählen (PSK)
- Standard Passwort des **Access-Point** (AP) ändern
- SSID des AP sollte keine Rückschlüsse auf verw. Hardware zulassen
- WLAN-Geräte sollten nicht per WLAN konfiguriert werden
- Im Access Point sollte, sofern vorhanden, die **Fernkonfiguration** abgeschaltet werden
- WLAN-Geräte sollten ausgeschaltet werden, solange sie nicht genutzt werden
- Die Reichweite des WLANs minimieren
- Regelmäßige **Firmware-Aktualisierungen**

WPA2 (Wi-Fi Protected Access)

- auch bekannt als IEEE 802.11i Standard
- 2004 ratifiziert
- verwendet AES (Advanced Encryption Standard) zur Verschlüsselung
- TKIP ist auch vorhanden um mit existierender WPA Hardware kompatibel zu sein
- Authentifizierung : aufgeteilt in User und Enterprise Mode

WPA2 - Authentifizierung Teil 1

Authentifizierung im Personal mode

- kein Authentifizierungsserver notwendig
- ausgeführt zw. Client und AP
- der AP generiert einen 256-bit PSK aus einem plain-text (8 bit 63 characters)

WPA2 - Authentifizierung Teil 2

Authentifizierung im Enterprise mode (Teil 1)

- baut auf dem IEEE 802.1X Authentifizierungsstandard auf
- Hauptkomponenten
  - Client verbindet sich mit Netzwerk
  - Authentifikator (AP) stellt Zugangskontrolle bereit
  - Authentifizierungsserver (RADIUS) trifft Authorisierungsentscheidungen
- der Authentifikator teilt jeden virtuellen port in 2 logische ports, aus denen sich die PAE (Port Access Entity) bildet
  - einen für den Service
  - einen für die Authentifikation

WPA2 - Authentifizierung Teil 3

Authentifizierung im Enterprise mode (Teil 2)

- Authentifizierungs-PAE ist immer offen für Authentifizierungsrahmen
- Service-PAE nur offen bei erfolgreicher Authentifizierung durch RADIUS Server
- Client und AP kommunizieren über Layer 2 EAPoL (EAP über LAN)
- der Authentifikator konvertiert EAPoL Nachrichten in RADIUS Nachrichten und sendet sie zum RADIUS Server
- RADIUS Server bearbeitet die Authentifizierungsanfrage
- Client und Authentifikator haben einen geheimen MK (Master Key)

WPA2 - Schlüsselerzeugung

4-Way Handshake

- für PTK (Pair-wise Transient Key) und GTK (Group Transient Key)-Erzeugung
- 4 EAPoL-Key Nachrichten zw Client und dem AP
- folgende Schritte:
  - Bestätigung,dass Client den PMK (notwendig für Erzeugung des PTK) kennt
  - erzeuge neuen PTK: zusammengesetzt aus KCK (Key Confirmation Key), KEK (Key Encryption Key) and TK (Temporal Key)
  - Encryption und integrity keys installieren
  - Transport des GTK verschlüsseln
  - Cipher suite Auswahl bestätigen

Group Key Handshake

- für GTK-Erneuerung oder um einen Host zu trennen
- benutzt den KEK (Key Encryption Key) für die GTK Verschlüsselung

WPA2 - Verschlüsselung Teil 1

- verwendet AES, ein block cipher
- 128-bit key length
- bits werden in Plaintext-Blöcken verschlüsselt
- AES verwendet das Counter-Mode/CBC-Mac Protocol (CCMP)
- CCM ermöglicht einen single key zur Verschlüsselung und Authentifizierung zu verwenden
- zwei Modes verarbeitet in CCM beinhalten Counter mode (CTR), erreicht Daten-Verschlüsselung und Daten-Integrität von Cipher Block Chaining Message Authentication Code (CBC-MAC)
- AES verwendet einen 128-bit Initialisierungsvektor (IV)

WPA2-Verschlüsselung Teil 2

MIC (Message Integrity Code) berechnen

- IV wird mit AES und TK verschlüsselt ... 128-bit Ergebnis
- Ergebnis wird XOR mit den nächsten 128-bit Daten
- Ergebnis von XOR wiederholt step 1 und 2 bis alle 128 Blöcke im 802.11 payload ausgenutzt sind
- die ersten 64 bits werden verwendet um MIC zu erzeugen

WPA2-Verschlüsselung Teil 3

Daten und MIC verschlüsseln mittels Counter Mode Algorithmus

- Counter initialisieren wenn nicht vorhanden, sonst erhöhen
- ersten 128-bits verschlüsselt mit AES und TK ...128-bit Ergebnis
- XOR wird auf das Ergebnis angewendet
- die ersten 128-bits Daten produzieren den ersten 128-bit verschlüsselten Block
- Step 1-4 wird wiederholt bis die 128-bit Blöcke verschlüsselt sind
- Counter auf 0 setzen und ihn verschlüsseln mit AES und XOR mit MIC (hängt Ergebnis, verschlüsselten Rahmen, an).

WPA2 - Entschlüsselung

Steps

- Mit dem gleichen Algorithmus wie bei Verschlüsselung wird Counter Wert abgeleitet
- Counter Wert und verschlüsselte Teil des 802.11 payload werden entschlüsselt mit dem Counter Mode Algorithmus und TK ...Ergebnis = MIC und entschlüsselte Daten
- mittels CBC-MAC Algorithmus wird MIC wiederberechnet

Vorteile des WPA2

Zusätzlich zu den Verschlüsselungsvorteilen, hat WPA2 zwei weitere Erweiterungen zur Unterstützung von schnellem Roaming.

- PMK Caching Support
- Pre-authentication Support

Ermöglicht WPA2 die Roaming-Zeit von mehr als einer Sekunde zu weniger als 1/10 Sekunde zu veringern.

Tools

Tools

- inSSIDer, ein aktiver WLAN-Sniffer
- Kismet, ein passiver WLAN-Sniffer
- Aircrack, WEP-Cracker

Zusammenfassung und Fazit

Vielen Dank für eure Aufmerksamkeit

Referenzen