

# Fortgeschrittene Wireless Sicherheitsmechanismen

Was nach WEP  
kommt...

Von P. Infanger

## Inhaltsverzeichnis

- Wieso WEP so schlecht ist
- WPA
- WPA2
- 802.11i
- 802.1x
- Empfehlungen

## Wieso WEP so schlecht ist

- Verschlüsselung Optional!
- Statische WEP Key
  - Kein zentralisiertes Management
  - Schlechter Schutz vor diversen Sicherheitsattacken (wie gesehen:-)
- WEP-IV ist zu schwach, Keylänge zu kurz (auch bei 256Bit!)
- Kein effektiver Weg um mit gestohlenen Adaptern umzugehen
  - Dieb besitzt Zugriff auf das Netzwerk
  - Re-keying aller WLAN Clients notwendig
- Mangelhafte Integration für die Benutzeradministration
  - Separate Datenbank benötigt
  - Benutzer kann höchstens anhand der MAC Adresse identifiziert werden (mangelhaft!)

## WPA, WPA2, 802.11i

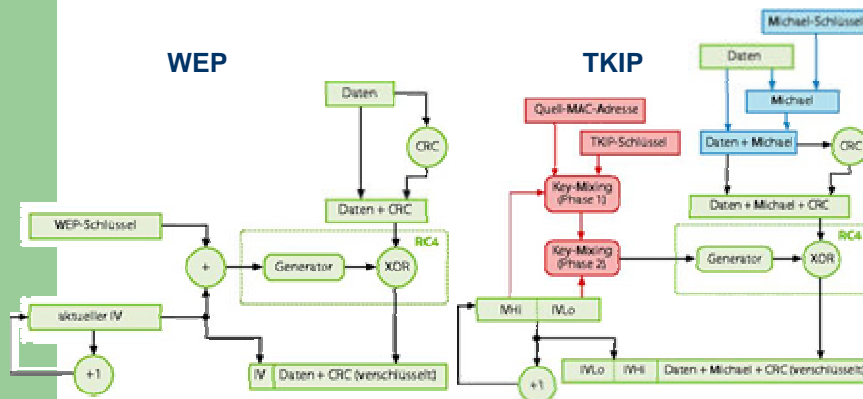
- Verbesserung für WEP musste entwickelt werden (Druck des Marktes!)
- IEEE definierte erst mit 802.11i ein umfassendes WLAN-Sicherheitskonzept (802.11a – 802.11h Priorität eher auf Interoperabilität)
- Aus „Ungeduld“ WPA als „Schnellschuss“ freigegeben, enthält nur Teilmenge des 802.11i Standards

# WPA

- WPA: Wi-Fi Protected Acces (von der Wi-Fi Alliance und Micro\$oft gepusht)
- Löst WEP als Verschlüsselungsmechanismus für WLAN ab
- WPA Vorläufer von 802.11i (war dazumal noch nicht fertig spezifiziert)
- Verwendet TKIP (Temporal Key Integrity Protocol)
- Schutz durch dynamische Schlüssel, die auf dem **TKIP** (Temporal Key Integrity Protocol) basieren
- Authentication von Nutzern mittels **PSK** (Pre-Shared-Keys) oder **EAP** (Extensible Authentication Protocol) über 802.1x
- Pre-Shared-Key wird nur für Authentication verwendet, anschliessend wird er durch einen Session-Key ersetzt
- Nur für Infrastructure-Mode (kein Ad-Hoc!)



# Vergleich WEP und TKIP



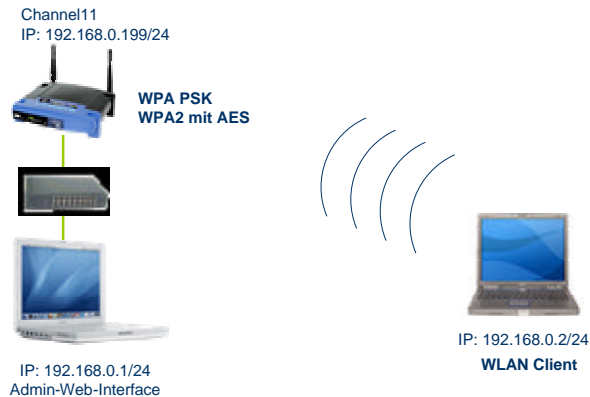
## Zusammenfassung WPA

- Die Algorithmen TKIP und Michael als Ersatz für WEP
- Ein standardisiertes Handshake-Verfahren zwischen Client und AP zur Ermittlung der Sitzungsschlüssel;
- Ein vereinfachtes Verfahren zur Ermittlung des Master Secret per Passphrase, das ohne Radius-Server auskommt sowie
- Die Aushandlung des Verschlüsselungsverfahrens zwischen AP und Client.

## WPA2, 802.11i

- Da WPA den **RC4 Algorithmus** nutzt, welcher bereits als gebrochen gilt, wurde im Februar 2004 die Erweiterung von WPA auf WPA2 angekündigt
- In WPA2 wurde nicht nur der vollständige 802.11i-Standard umgesetzt, sondern es nutzt auch den Verschlüsselungsalgorithmus AES-CCM (Advanced Encryption Standard, Counter with CBC-MAC)
- 802.11i Spezifikation seit Juni 2004 festgelegt.  
(Es dauerte solange weil zuerst gewisse Funktionalitäten, vor allem im Roaming und Telefoniebereich, entwickelt werden mussten)

## Demonstration WPA + WPA2



## Benutzerfreundlichere Varianten

- Man hat gemerkt, dass der DAU überfordert ist mit allen möglichen und unmöglichen Konfigurationsparameter
- Verschiedene Firmen haben daraufhin WPA-PSK „benutzerfreundlich“ verpackt.
- z.B.:
  - Netgear Touchless WiFi Security Assistant
  - Linksys Secure Easy Setup
  - Zyxel OTIST (One-Touch-Intelligent-Security-Technology) (<http://www.studerus.ch/otist.cfm>)
  - Weitere...

## Zyxel OTIST (One-Touch-Intelligent-Security-Technology)

- Zitat Zyxel: „Bei der WPA-Pre-Shared-Key-Methode (PSK) melden sich alle Benutzer eines Netzwerks mit dem gleichen Initial-Kennwort an. Die Sicherheit des Netzwerks hängt damit also klar von der Qualität des Initial-Kennworts ab.“
- Der Access-Point scannt nach dem Start seine Umgebung während **kurzer Zeit ab** und versucht mit einem Client, der OTIST aktiviert hat, einen WPA-PSK auszuhandeln.
- Auf diese Weise wird ein komplexes Initial-Kennwort erstellt, ohne Tippfehler auf den Client übertragen, und abgespeichert.



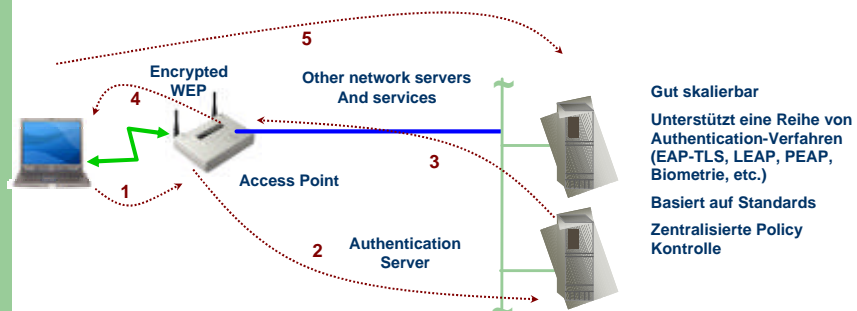
## Vorteile und Nachteile von WPA bzw. WPA2

- Vorteile:
  - Bessere Verschlüsselung
  - Pre-Shared-Keys für kleinere Umgebungen, Authentication-Server für grössere Umgebung möglich
  - WPA2 mit AES möglich
  - In WindowsXP SP2 dabei
  - IEEE Standard
- Nachteile:
  - Mehr Rechenleistung notwendig (ev. Hardware-Update)
  - Neue Software (Treiber) notwendig
  - Anfällig auf schwache Passwörter (Wörterbuchattacken etc.) und DoS Angriffe wegen Message-Integrity-Check-Algorithmus
  - Nur für Infrastructure-Mode (kein Ad-Hoc Netzwerk)

## 802.1x Übersicht

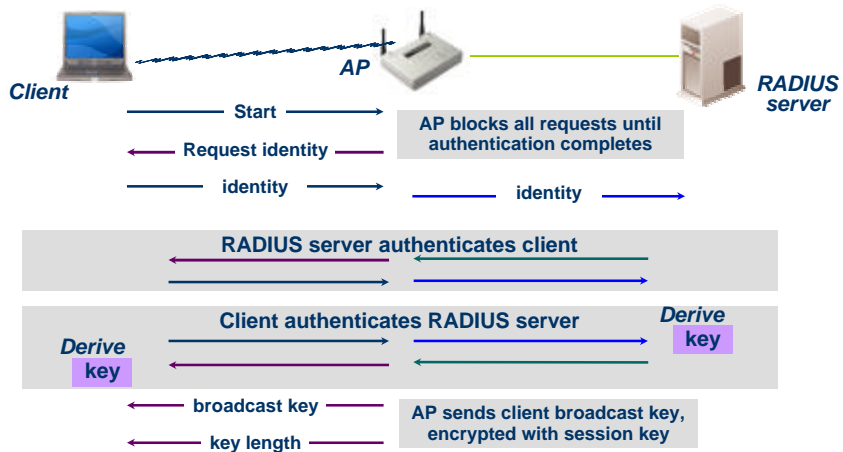
- Zentralisierte, skalierbare, benutzerbasierende Authentication
- Gegenseitige Authentication
- Verschiedene Authentication möglich
- Dynamic WEP Key Unterstützung
- WEP Key Erneuerung

## 802.1x in WLAN Environment



- 1) Benutzer verlangt Zugriff. AP verhindert Netzwerkzugriff.
- 2) Verschlüsselte Credentials werden zum Authentication-Server gesendet.
- 3) Authentication-Server validiert Benutzer und erteilt Zugriffsberechtigung.
- 4) AP öffnet Port und es werden dynamische WEP Keys dem Client zugewiesen (verschl.).
- 5) Wireless Client kann nun sicher auf die Netzwerkdienste zugreifen.

## 802.1X Authentication Prozess



## Vorteile von 802.1x für WLAN

- Sehr gut skalierbar
- Unterstützt eine Reihe von Authentication Verfahren
  - EAP-Cisco Wireless (LEAP)
  - EAP-TLS mit Windows XP und anderen Windows Versionen
  - PEAP
  - Weitere, je nach Entwicklungsstand
- Eine Standards-basierende Lösung
- Ermöglicht zentralisierte Policy Kontrolle
  - Session Timeout triggert die Re-Authentication und somit neuen WEP Key

## EAP-Cisco Wireless (LEAP) vs. EAP-TLS vs. PEAP

	LEAP	EAP-TLS	PEAP
Static Password Support	Yes	No	Yes
One Time Password Support	No	No	Yes
MS Windows password change	No	???	Yes
Requires <b>Server</b> (RADIUS) X.509v3 Certificate?	No	Yes	Yes
Requires <b>Client</b> X.509v3 Certificate?	No	Yes	No
Microsoft Backend DB Support?	Yes	Yes	Yes
LDAP/NDS Backend DB Support?	No	Yes	Yes

## EAP, LEAP, PEAP, ... ???

- EAP: (Extensible Authentication Protocol)  
Protokoll zur Authentifizierung von Clients. Es kann zur Nutzerverwaltung auf RADIUS-Server zurückgreifen.
- LEAP: (Lightweight EAP)  
Cisco Variante von EAP (offiziell keine Details veröffentlicht!)
- PEAP: (Protected EAP)  
Ursprünglich eine IETF Arbeitsgruppe, heute stark in Microsoft Umgebungen eingesetzt
- EAP-TLS: (Transport Layer Security, RFC 2246)  
gilt als das sicherste EAP Verfahren

## WLAN sicher machen:

- Default Einstellungen ändern (SSID, Passwörter, IP-Adressen, Routingprotokolle, Keys, etc.)
- SSID Broadcast abschalten
- SSID mit Sonderzeichen ausstatten
- Konfiguration des AP's via WLAN abschalten (auch SNMP!)
- Separates WLAN-Segment bilden, ohne DHCP und ev. mit Firewall/Paketfilter gesichert
- Sendeleistung begrenzen
- Firmwareupdate einspielen (z.B. wegen bekannter Backdoors)
- WPA, WPA2 oder 802.1x aktivieren
- Generell: niemals Trivialpasswörter verwenden
- Vertrauen ist gut, Kontrolle ist besser
- VPN verwenden

## Links

- <http://www.drizzle.com/~aboba/IEEE/>
- <http://www.heise.de/newsticker/meldung/48624>
- [http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_qanda\\_item0900aecd801e3e59.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item0900aecd801e3e59.shtml)
- <http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/netqa0900aecd801764fe.html>
- <http://www.microsoft.com/austria/technet/articles/cable-guy-wpa2.mspix>
- <http://www.microsoft.com/germany/technet/sicherheit/mvp/wlan.mspix>
- <http://www.wireless-forum.ch/forum/printview.php?t=4600&start=0>