WLAN an der Ruhr-Universität Bochum

Andreas Jobs, Andreas Noack

13. März 2009

Überblick

Rechenzentrum - Abtl. Rechnernetz

- ca. 40.950 Switchports
- ca. 30.800 Netzwerkanschlüsse
- ca. 9600 aktive Anschlüsse (mittags)
- 1.760 Netzwerkomponenten
- 356 Standorte

Überblick

Rechenzentrum - Abtl. Rechnernetz

- ca. 40.950 Switchports
- ca. 30.800 Netzwerkanschlüsse
- ca. 9600 aktive Anschlüsse (mittags)
- 1.760 Netzwerkomponenten
- 356 Standorte
- 137 Accesspoints

Überblick

Rechenzentrum - Abtl. Rechnernetz

- ca. 40.950 Switchports
- ca. 30.800 Netzwerkanschlüsse
- ca. 9600 aktive Anschlüsse (mittags)
- 1.760 Netzwerkomponenten
- 356 Standorte
- 137 Accesspoints
- 6 Personen (5,5 Stellen)

Warum ein Funknetz?

- Netzversorgung der Freibereiche (zwischen den Hochgebäuden, Forumsplatz, . . .)
- Netzversorgung für Zuhörer in Hörsälen und Seminarräumen

Funknetzplanung

- Ähnliche Sicherheit wie im Kabelnetz
- Authentifizierung erforderlich, da öffentlicher Port
- Geschützte Klartextauthentifizierung benötigt.

Funknetzplanung

- Ähnliche Sicherheit wie im Kabelnetz
- Authentifizierung erforderlich, da öffentlicher Port
- Geschützte Klartextauthentifizierung benötigt.
- WEP und WPA-PSK fallen daher aus
- WPA-EAP (damals) nicht genügend Unterstützung (APs / Klienten)

Funknetzplanung

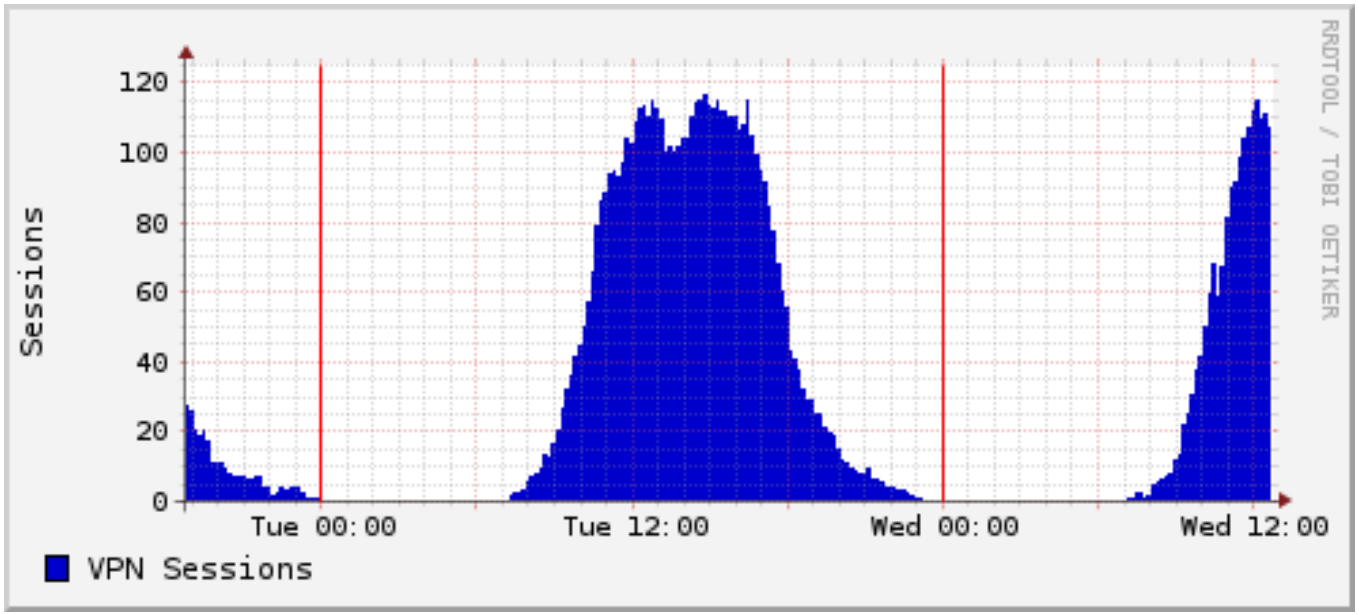
- Ähnliche Sicherheit wie im Kabelnetz
- Authentifizierung erforderlich, da öffentlicher Port
- Geschützte Klartextauthentifizierung benötigt.
- WEP und WPA-PSK fallen daher aus
- WPA-EAP (damals) nicht genügend Unterstützung (APs / Klienten)
- VPN über unverschlüsseltes Wlan

Realisierung

- PPTP und L2TP übermitteln Logininformationen unverschlüsselt
- IPSec mittels Cisco-VPN Concentrator

Realisierung

- PPTP und L2TP übermitteln Logininformationen unverschlüsselt
- IPSec mittels Cisco-VPN Concentrator
- Allgemein gute Akzeptanz



Die Weiterentwicklung

- Immer mehr mobile Geräte (Mobiltelefone, PDAs . . .)
- wenige unterstützen den Cisco VPN Klienten

Die Weiterentwicklung

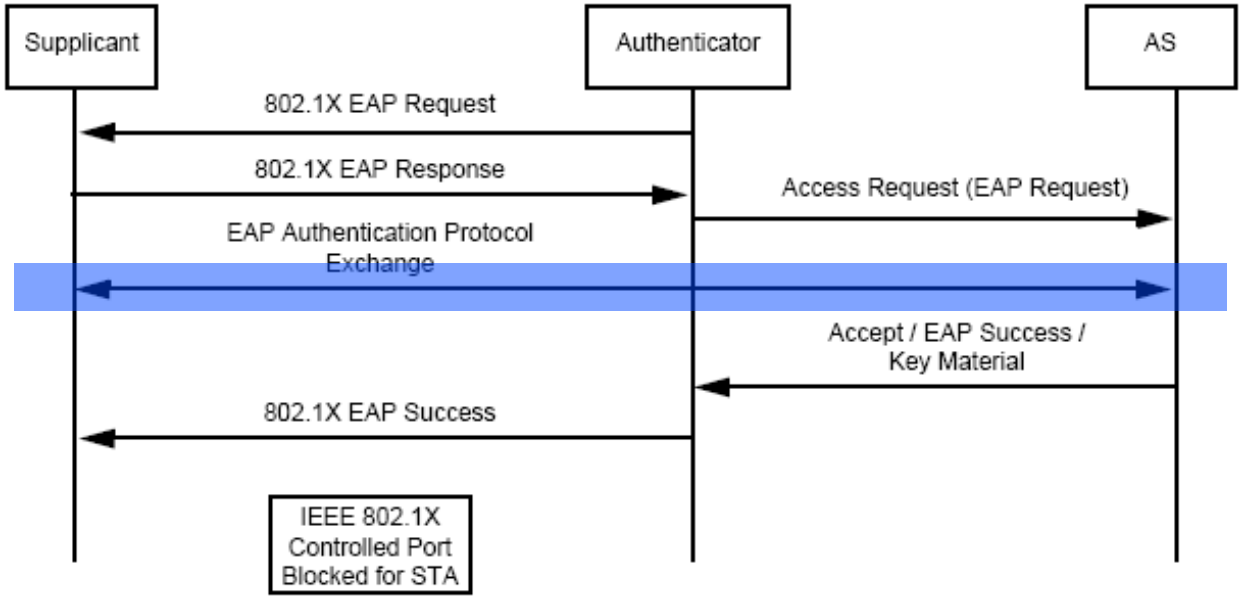
- Immer mehr mobile Geräte (Mobiltelefone, PDAs . . .)
- wenige unterstützen den Cisco VPN Klienten
- (Bessere) Integration ins Betriebssystem
- Möglichkeiten des EduRoam nutzen.

Der Enterprise-Modus von IEEE 802.11 WLAN

- Authentifikation mit IEEE 802.1X gegenüber einem zentralen Server (z.B. RADIUS oder Diameter)
  - Eine Passwortdatenbank für alle
  - Höhere Sicherheit (Details folgen)
- Der Betrieb einer beliebigen Anzahl von Accesspoints als Extended Service Set (ESS) ist mit einem RADIUS-Server möglich
- Für WEP, WPA und WPA2 (IEEE 802.11i) notwendig: Gemeinsames Schlüsselmaterial nach erfolgreicher Authentifikation

Der Enterprise-Modus von IEEE 802.11 WLAN

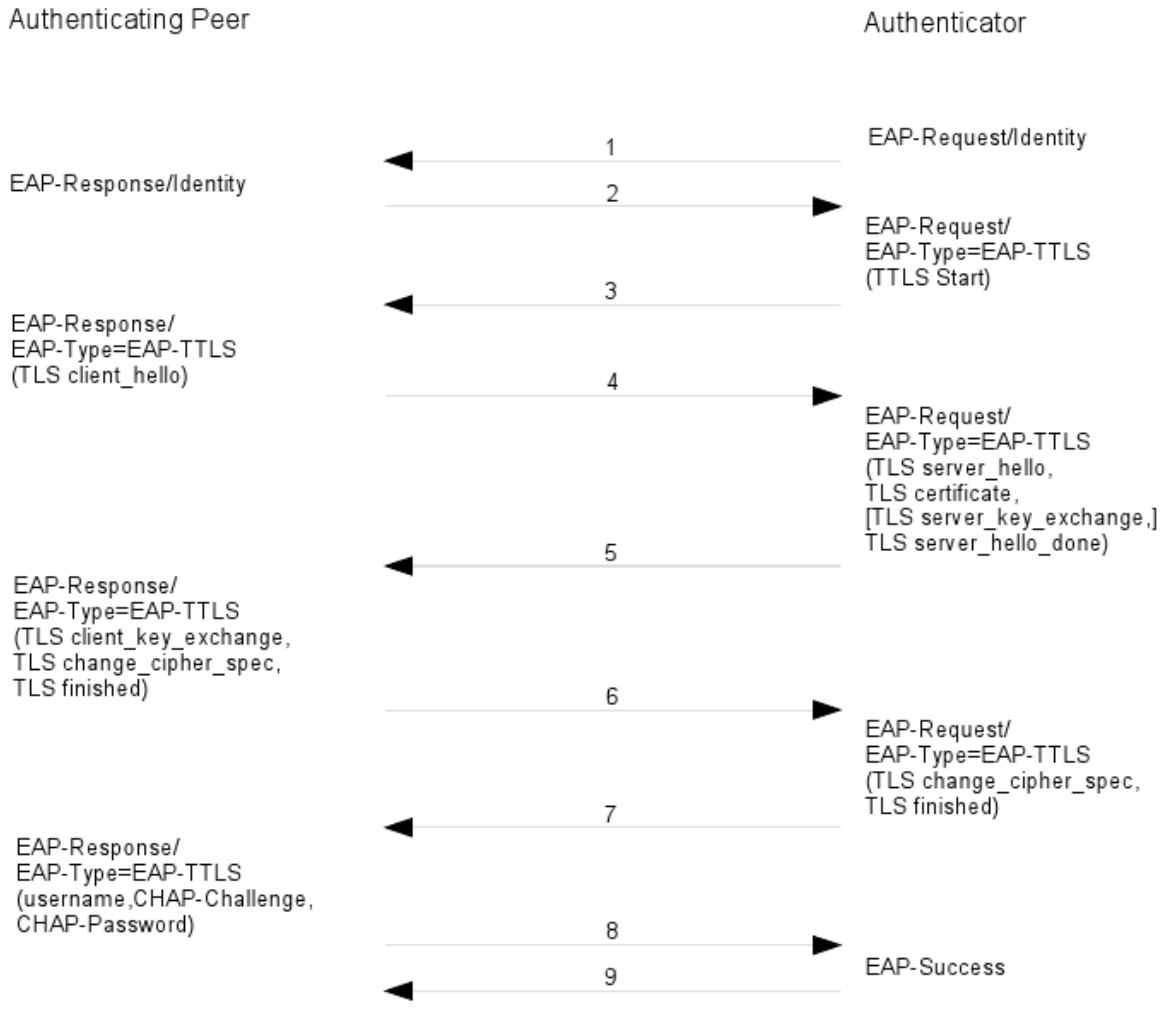
- Die Authentifikations-/Schlüsselaustauschverfahren (EAP) sind austauschbar und erweiterbar
- EAP - **E**xtensible **A**uthentication **P**rotocol
- Abbildung zeigt 802.1X Authentifikation mit EAP Protokoll
  Quelle: [802.11i]



Bekannte und verbreitete EAP Protokolle

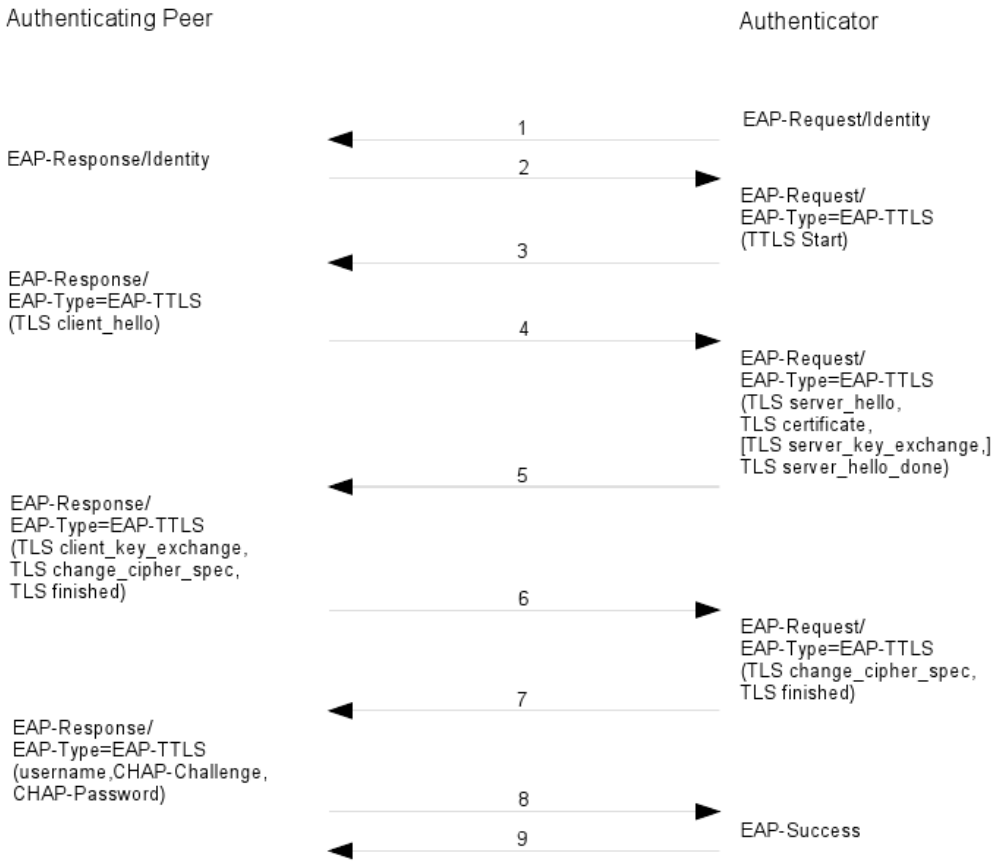
- **Triviale Protokolle** *(kein Schlüsselaustausch)*:
  - EAP-PAP (Passwort im Klartext)
  - EAP-MD5 (Challenge-Response mit MD5)
  - EAP-MSCHAP (Challenge-Response von Microsoft)
- **TLS-basierende Protokolle**:
  - EAP-TLS (Client- und Serverzertifikat)
  - EAP-PEAP (Serverzertifikat, Client-Auth. mit innerem EAP-Protokoll)
  - EAP-TTLS (Serverzertifikat, Client-Auth. mit innerem Protokoll)
- **Weitere Protokolle**:
  - EAP-PSK (Pre-Shared Key, basierend auf AES)
  - EAP-SIM (Auth. mit SIM-Karte/Mobilfunk)
  - ...

Beispiel für ein EAP-Protokoll

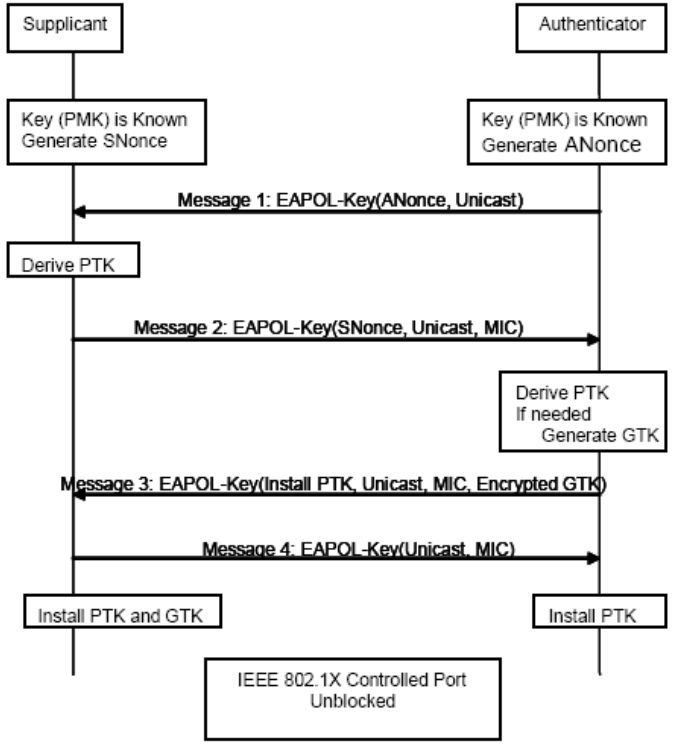


EAP-TTLS/CHAP, Quelle: [Rave09]
(*Anmerkung*: CHAP-Challenge basiert auf TLS-Master Secret)

Beispiel für ein EAP-Protokoll und 4-Way-Handshake



EAP-TTLS/CHAP, Quelle: [Rave09]
(*Anmerkung*: CHAP-Challenge basiert auf TLS-Master Secret)



4-Way-Handshake, Quelle: [802.11i]

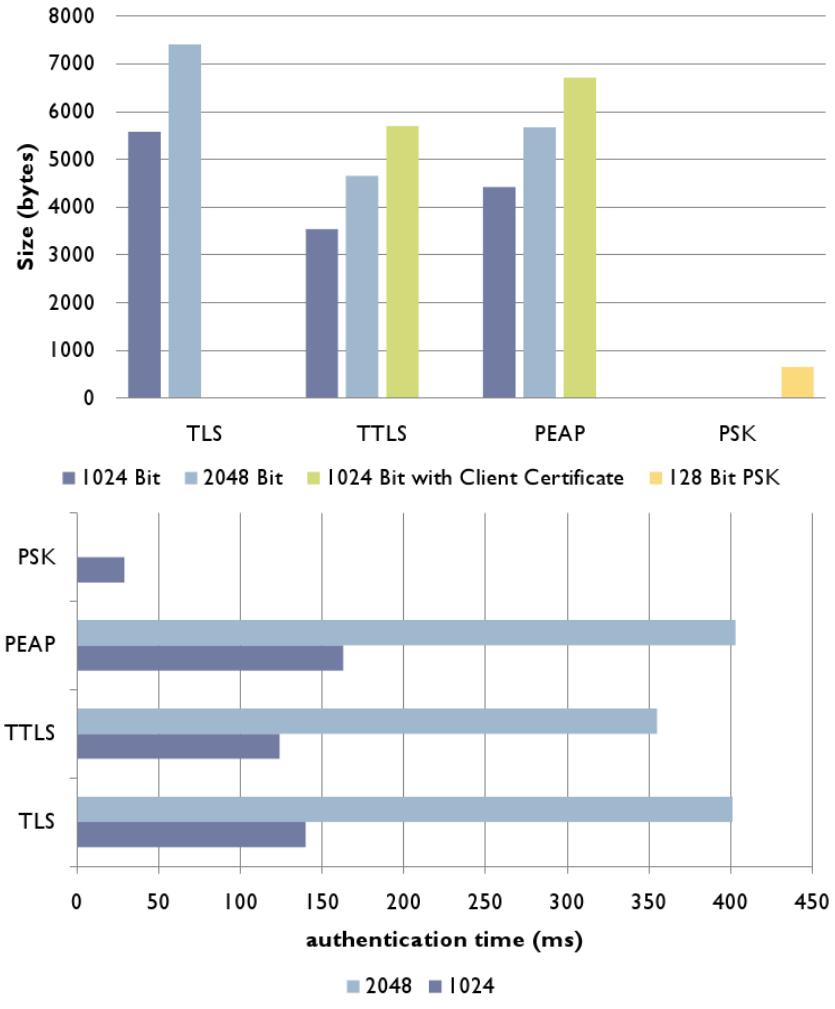
Sicherheit der EAP Protokolle

- Analyse von verschiedenen Angriffen auf EAP Protokolle [Noack07]
- Bewertung:
  - Angriff erfolgreich (- -)
  - Angriff unter besonderen Bedingungen erfolgreich (-, o)
  - Angriff nicht erfolgreich (+)

	EAP-PSK	EAP-TLS	EAP-TTLS	EAP-PEAP	LEAP	EAP-FAST	EAP-IKEv2
Dictionary Attack	+	+	+	+	- -	-	+
Bruteforce	+	+	+	+	-	+	o
Cryptanalysis	+	+	+	+	+	+	+
Replay Attack	o	+	+	+	+	o	+
Cert. Manipulation	+	o	o	o	+	+	+
Identity Spoofing	o	+	-	-	- -	-	o
Session Hijacking	-	-	-	-	-	-	-
Typing Attack	-	+	+	+	+	o	+
Downgrading Attack	+	+	+	+	+	+	+
Algebraic Attack	+	+	+	+	+	+	+

Performanz der EAP Protokolle

- EAP-TLS überträgt Client- *und* Server-Zertifikat
- EAP-TTLS und EAP-PEAP übertragen nur Server-Zertifikat, danach PAP/CHAP/MSCHAPv2/...
- Innere Authentifizierung von EAP-TTLS benötigt *keinen* EAP-Overhead!
- EAP-PSK authentifiziert mit Shared-Secret



Quelle: [Rave09]

Entscheidung der Ruhr-Universität für ein EAP-Protokoll

Die Ruhr-Universität Bochum setzt EAP-TTLS/PAP mit einem 2048 Bit großen Serverzertifikat ein

- Eines der sichersten Verfahren!
- Das schnellste der sichersten Verfahren!
- PAP übermittelt die Clientzugangsdaten im Klartext, **aber** Klartext-Kommunikation ist durch TLS-Tunnel geschützt.

weitere Entwicklung

- Leider nicht überall unterstützt

Betriebssystem	EAP-TTLS-PAP ?
Linux	Ja
MacOS X	Ja
Windows	3rdParty
iPhone/iPod touch	Ja
Nokia Telefone (Symbian)	Nein

Fazit & Ausblick

- Ausbau Funknetz (Botanischer Garten)
- WPA2

Fragen?

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

Literatur


IEEE 802.11 Working Group.
IEEE Standard for Information technology – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications/Amendment 6: Medium Access Control (MAC) Security Enhancements.
IEEE 802.11i, IEEE Computer Society, Juni 2004.


Andreas Noack.
Sicherheitsanalyse von EAP-Protokollen.
Masterthesis, Ruhr-Universität Bochum, Embigence GmbH, September 2007.


Johannes Rave.
Efficiency of EAP-Protocols.
Seminar Netz- und Datensicherheit WS08/09, 2009.