

WLAN an der Ruhr-Universität Bochum

Andreas Jobs

25. November 2009

Rechenzentrum - Abtl. Rechnernetz

- ca. 42.580 Switchports
- ca. 31.930 Netzwerkanschlüsse
- ca. 9700 aktive Anschlüsse (mittags)
- 1.820 Netzwerkkomponenten
- 356 Standorte

Rechenzentrum - Abtl. Rechnernetz

- ca. 42.580 Switchports
- ca. 31.930 Netzwerkanschlüsse
- ca. 9700 aktive Anschlüsse (mittags)
- 1.820 Netzwerkkomponenten
- 356 Standorte
- 172 Accesspoints

Rechenzentrum - Abtl. Rechnernetz

- ca. 42.580 Switchports
- ca. 31.930 Netzwerkanschlüsse
- ca. 9700 aktive Anschlüsse (mittags)
- 1.820 Netzwerkkomponenten
- 356 Standorte
- 172 Accesspoints
- 6 Personen (5,5 Stellen)

Warum ein Funknetz?

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

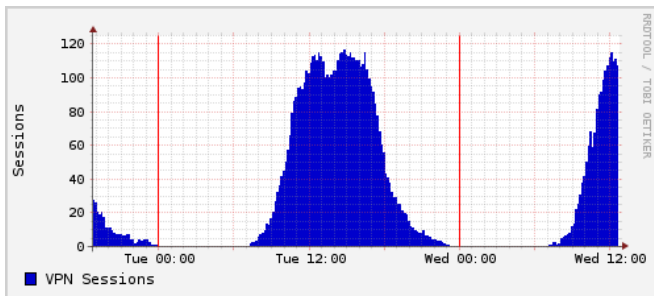
- Ähnliche Sicherheit wie im Kabelnetz
- Authentifizierung erforderlich, da öffentlicher Port
- Geschützte Klartextauthentifizierung benötigt.

- 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)

- 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

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

- 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

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)
 - ...

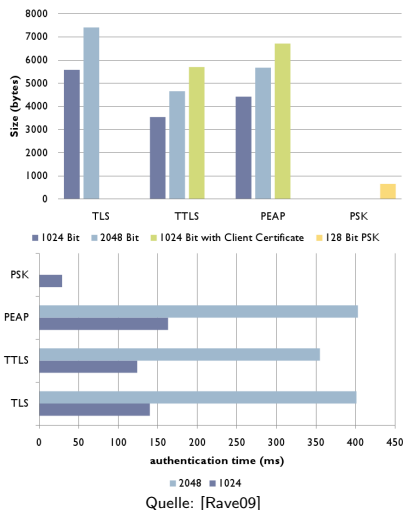
Sicherheit der EAP Protokolle

- 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



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.

- Leider nicht überall unterstützt

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

- Ausbau Funknetz (Botanischer Garten)
- WPA2

Fragen?

Fragen?

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!



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.