WLAN Router sicher konfigurieren

Reinhard Tartler

Linux User Group Schwabach
http://lusc.de

21. April 2007

Gliederung

1. Einleitung
   - Bedrohungen
2. Hauptteil
   - Grundlagen
   - Techniken auf Linklayer Ebene
   - Techniken auf Transportebene
3. Fazit

Vorraussetzungen

- Vortrag WLAN Karten und Treiber
- Grundlagen zu Netzwerkprotokollen
- Bitte den Redner bei Unklarheiten sofort Unterbrechen

Vorraussetzungen

- Vortrag WLAN Karten und Treiber
- Grundlagen zu Netzwerkprotokollen
- Bitte den Redner bei Unklarheiten sofort Unterbrechen

Vorraussetzungen

- Vortrag WLAN Karten und Treiber
- Grundlagen zu Netzwerkprotokollen
- Bitte den Redner bei Unklarheiten sofort Unterbrechen

Gliederung

1. Einleitung
   - Bedrohungen
2. Hauptteil
   - Grundlagen
   - Techniken auf Linklayer Ebene
   - Techniken auf Transportebene
3. Fazit

Ausspähung von privaten Daten

- Passwörter zu Online-Diensten
- Zugansdaten (*VPN*) zum Arbeitsplatz
- Homebanking
- Liebesbriefe ...

Ausspähung von privaten Daten

- Passwörter zu Online-Diensten
- Zugansdaten (*VPN*) zum Arbeitsplatz
- Homebanking
- Liebesbriefe ...

Ausspähung von privaten Daten

- Passwörter zu Online-Diensten
- Zugansdaten (*VPN*) zum Arbeitsplatz
- Homebanking
- Liebesbriefe ...

Ausspähung von privaten Daten

- Passwörter zu Online-Diensten
- Zugansdaten (*VPN*) zum Arbeitsplatz
- Homebanking
- Liebesbriefe ...

Weitere mögliche Probleme

- Bandbreitenklau
- Belastung der Telefonrechnung bei volumenbasierten Tarifen
- Angst vor rechtlichen Konsequenzen (*insb. LG Hamburg Urteil vom 26.07.2006, Geschäftsnr.: 308 O 407 / 06*)
- Versenden von Spam (und anderem Unrat)

Weitere mögliche Probleme

- Bandbreitenklau
- Belastung der Telefonrechnung bei volumenbasierten Tarifen
- Angst vor rechtlichen Konsequenzen (*insb. LG Hamburg Urteil vom 26.07.2006, Geschäftsnr.: 308 O 407 / 06*)
- Versenden von Spam (und anderem Unrat)

Weitere mögliche Probleme

- Bandbreitenklau
- Belastung der Telefonrechnung bei volumenbasierten Tarifen
- Angst vor rechtlichen Konsequenzen (*insb. LG Hamburg Urteil vom 26.07.2006, Geschäftsnr.: 308 O 407 / 06*)
- Versenden von Spam (und anderem Unrat)

Weitere mögliche Probleme

- Bandbreitenklau
- Belastung der Telefonrechnung bei volumenbasierten Tarifen
- Angst vor rechtlichen Konsequenzen (*insb. LG Hamburg Urteil vom 26.07.2006, Geschäftsnr.: 308 O 407 / 06*)
- Versenden von Spam (und anderem Unrat)

Gliederung

1. Einleitung
   - Bedrohungen
2. Hauptteil
   - Grundlagen
   - Techniken auf Linklayer Ebene
   - Techniken auf Transportebene
3. Fazit

Schichtenmodel

- Physikalische Schicht (Ethernet)
- Transportschicht (IP)
- Sitzungssicht (TCP/UDP)
- Applikationsebene (HTTP)

Schichtenmodel

- Physikalische Schicht (Ethernet)
- Transportschicht (IP)
- Sitzungssicht (TCP/UDP)
- Applikationsebene (HTTP)

Schichtenmodel

- Physikalische Schicht (Ethernet)
- Transportschicht (IP)
- Sitzungssicht (TCP/UDP)
- Applikationsebene (HTTP)

Schichtenmodel

- Physikalische Schicht (Ethernet)
- Transportschicht (IP)
- Sitzungssicht (TCP/UDP)
- Applikationsebene (HTTP)

Sicherungsansätze

was und wie kann man schützen

- Linklayer Security (WEP/WPA)
- Transportlayer Security (IPSec, openvpn)
- Application Layer Security (SSL/TLS)

Sicherungsansätze
was und wie kann man schützen

- Linklayer Security (WEP/WPA)
- Transportlayer Security (IPSec, openvpn)
- Application Layer Security (SSL/TLS)

Sicherungsansätze
was und wie kann man schützen

- Linklayer Security (WEP/WPA)
- Transportlayer Security (IPSec, openvpn)
- Application Layer Security (SSL/TLS)

Gliederung

1. Einleitung
   - Bedrohungen
2. Hauptteil
   - Grundlagen
   - Techniken auf Linklayer Ebene
   - Techniken auf Transportebene
3. Fazit

Unverschlüsselt

- einfache Einrichtung
- sehr bedingter Überblick über verbundene Hardware
- Filterung von Hardwareadressen *(MAC)* als einzige Sicherung

Unverschlüsselt

- einfache Einrichtung
- sehr bedingter Überblick über verbundene Hardware
- Filterung von Hardwareadressen *(MAC)* als einzige Sicherung

Unverschlüsselt

- einfache Einrichtung
- sehr bedingter Überblick über verbundene Hardware
- Filterung von Hardwareadressen *(MAC)* als einzige Sicherung

WEP40/128

- *wired equivalent privacy*
- Verschlüsslungsverfahren RC4 gilt immernoch als *sicher*
- Implementierung fragwürdig
- 802.11a/b/g (WiFi) Standard vorgeschrieben

WEP40/128

- *wired equivalent privacy*
- Verschlüsslungsverfahren RC4 gilt immernoch als *sicher*
- Implementierung fragwürdig
- 802.11a/b/g (WiFi) Standard vorgeschrieben

WEP40/128

- *wired equivalent privacy*
- Verschlüsslungsverfahren RC4 gilt immernoch als *sicher*
- Implementierung fragwürdig
- 802.11a/b/g (WiFi) Standard vorgeschrieben

WEP40/128

- *wired equivalent privacy*
- Verschlüsslungsverfahren RC4 gilt immernoch als *sicher*
- Implementierung fragwürdig
- 802.11a/b/g (WiFi) Standard vorgeschrieben

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

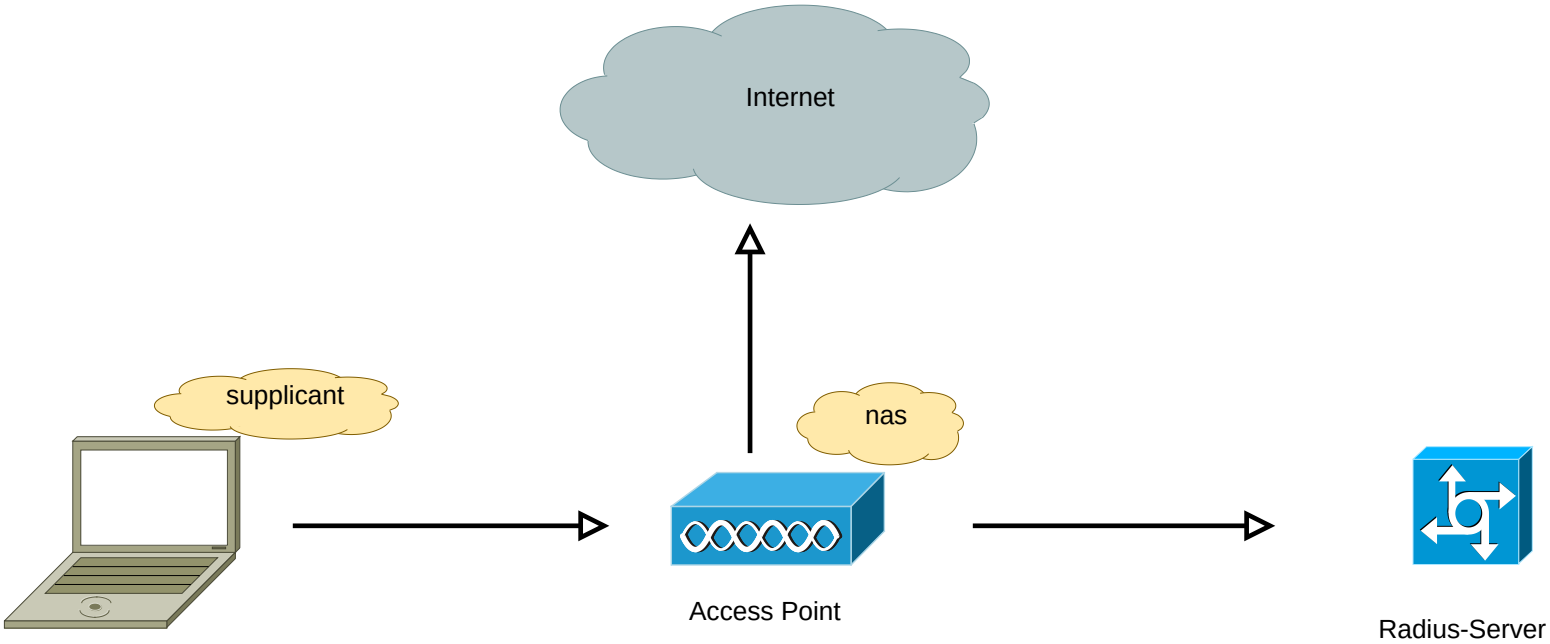
WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

WPA

- grundsätzliche Unterteilung:
  - WPA1 (TKIP) (RC4)
  - WPA2 (CCMP) (AES)
  - (viele) weitere Subvarianten durch Kombination und unteschiedliche unterliegende Protokolle
    - “Enterprise” EAP-TLS,TTLS,PEAP,LEAP
    - “Personal” PSK
- Stellt höhere Anforderungen:
  - Hardware (firmware)
  - Software (supplicant)
  - Access Point (nas)

Aufbau einer WPA Infrastruktur



Gliederung

1 Einleitung
- Bedrohungen

2 Hauptteil
- Grundlagen
- Techniken auf Linklayer Ebene
- Techniken auf Transportebene

3 Fazit

IPSec

- Bewährtes Sicherungsverfahren für Internetverbindungen
- Standardisiert: Viele Hardware Router implementieren IPSec
- viele verschiedene Varianten
- Linux support sehr fragwürdig in Version 2.4
- Besserung in Linux 2.6

IPSec

- Bewährtes Sicherungsverfahren für Internetverbindungen
- Standardisiert: Viele Hardware Router implementieren IPSec
- viele verschiedene Varianten
- Linux support sehr fragwürdig in Version 2.4
- Besserung in Linux 2.6

IPSec

- Bewährtes Sicherungsverfahren für Internetverbindungen
- Standardisiert: Viele Hardware Router implementieren IPSec
- viele verschiedene Varianten
- Linux support sehr fragwürdig in Version 2.4
- Besserung in Linux 2.6

IPSec

- Bewährtes Sicherungsverfahren für Internetverbindungen
- Standardisiert: Viele Hardware Router implementieren IPSec
- viele verschiedene Varianten
- Linux support sehr fragwürdig in Version 2.4
- Besserung in Linux 2.6

IPSec

- Bewährtes Sicherungsverfahren für Internetverbindungen
- Standardisiert: Viele Hardware Router implementieren IPSec
- viele verschiedene Varianten
- Linux support sehr fragwürdig in Version 2.4
- Besserung in Linux 2.6

openvpn

- Reine Softwareimplementierung
- nicht standardisiert
- unterstützt sowohl Zertifikats als auch PSK
- einfach einzurichten

openvpn

- Reine Softwareimplementierung
- nicht standardisiert
- unterstützt sowohl Zertifikats als auch PSK
- einfach einzurichten

openvpn

- Reine Softwareimplementierung
- nicht standardisiert
- unterstützt sowohl Zertifikats als auch PSK
- einfach einzurichten

openvpn

- Reine Softwareimplementierung
- nicht standardisiert
- unterstützt sowohl Zertifikats als auch PSK
- einfach einzurichten

Bewertung

- Unverschlüsselt/WEP ungenügend
- WPA derzeit das einzige einigermaßen brauchbare Verfahren auf Link-Layer
- Alternativen zu WPA
  - OpenVPN
  - IPSec

Bewertung

- Unverschlüsselt/WEP ungenügend
- WPA derzeit das einzige einigermaßen brauchbare Verfahren auf Link-Layer
- Alternativen zu WPA
  - OpenVPN
  - IPSec

Bewertung

- Unverschlüsselt/WEP ungenügend
- WPA derzeit das einzige einigermaßen brauchbare Verfahren auf Link-Layer
- Alternativen zu WPA
  - OpenVPN
  - IPSec

Bewertung

- Unverschlüsselt/WEP ungenügend
- WPA derzeit das einzige einigermaßen brauchbare Verfahren auf Link-Layer
- Alternativen zu WPA
  - OpenVPN
  - IPSec

Bewertung

- Unverschlüsselt/WEP ungenügend
- WPA derzeit das einzige einigermaßen brauchbare Verfahren auf Link-Layer
- Alternativen zu WPA
  - OpenVPN
  - IPSec