WLAN Sicherheit

by Commander1024

Gliederung

- WLAN Sicherheit
- Verbreitete Verschlüsselungstechnologien
- Angriffsszenario WEP
- Angriffsszenario WPA
- WPA Attack airocrack/airolib
- Fortgeschrittene Sicherungsmaßnahmen
- WPA2-Enterprise mit freeradius

Verbreitete Technologien

- WEP (traurig aber wahr)
- WPA-PSK (TKIP)
- WPA2-PSK (AES)
- Open System (der Königsweg? ;-))

Angriffsszenario WEP

- Lächerlich kleine Zahl an IV Paketen benötigt
  - deauth: deauthenticate 1 or all stations
  - fakeauth: fake authentication with AP
  - interactive: interactive frame selection
  - arpreplay: standard ARP-request replay
  - chopchop: decrypt/chopchop WEP packet
  - fragment: generates valid keystream
  - caffe-latte: query a client for new IVs
  - cfrag: fragments against a client
- Nun nur noch ein paar Sekunden CPU Kraft ;-)

Angriffsszenario WPA

- Verschlüsselung nicht ganz so trivial
- WPA Handshake wird benötigt (deauth attack)
- Bruteforce mit CPU sehr zeitintensiv
- Dictionary Attack (plain oder preprocessed)
- GPU Bruteforce (aircrack-ng-cuda, pyrit, diverse kommerzielle/closed source tools)

WPA Attack airocrack/airolib

Video – Präsentation

(by rdirect)

Fortgeschrittene Sicherungsmaßnahmen

- Auf WLAN (und DECT) komplett verzichten.
- Offenes WLAN an einem dedizierten Ethernet Port für OpenVPN, Stronswan, etc. (Rest komplett firewalled)
- WPA2-”Enterprise” (leider viele verschiedene Implementierungen)
  - Tool der Wahl: freeradius
  - Windows 2003 eingeschränkt, W2k8 und höher wurde der RADIUS Server fallen gelassen

WPA2-Enterprise mit freeradius

- AP mit der Möglichkeit, einen externen RADIUS Server für Auth zu nutzen.
- Kommunikation AP<->freeradius verschlüsselt mit Shared Secret
- Clients überprüfen, die Echtheit des Servers via OpenSSL Zertifikatskette
- Clients authentifizieren sich mit Zertifikat oder eigener Passphrase
- Zugänge können zeitlich eingeschränkt, temporär ausgestellt und widerrufen werden

Ende

Vielen Dank für die Aufmerksamkeit.

Technische Details zum freeradius Setup:
http://www.commander1024.de/wordpress/2010/10/wlan-wpa2-enterprise-eap-tls-und-co/