WLAN Sicherheit gestern und heute

Referent: Michael Schwab

Zu meiner Person

- Umfassendes Interesse für Funk Datenübertragung
- Einsatz verschiedener Funktechniken (DECT / WLAN)
- Beschäftigung mit IT Sicherheit
- Beschäftigung mit Cryptographie

Sicherheit gestern (vor ca 2 Jahren)

- etwa 30 - 50% der WLANs verschlüsselt
- Einfache Tools zum finden des Schlüssels
  Nutzung schwacher IVs (WEPCRACK)
- Nur WEP als Verschlüsselung verfügbar
- 11 MBit Übertragungsrate

Sicherheit heute

- etwa 70 - 90% der WLANs verschlüsselt
  davon 5-10% mit WPA
- Leistungsfähige Tools zum finden des Schlüssels
- Nutzung verschiedenster Schwachstellen
- WEP und WPA als Verschlüsselung verfügbar
- 54 MBit Übertragungsrate
- Viele APs senden keine schwachen IVs mehr

Statistik

- Sicherheit:
  10% Offen - 80% WEP - 10% WPA
- Geschwindigkeit:
  10% 11 Mbit - 2% 22 Mbit - 88% 54 Mbit
- SSID:
  30% WLAN - 10% Fritz* - 5% NETGEAR - 4% ConnectionPoint

Einführung in WLAN Verschlüsselung (RC4)

- Ein Schlüssel erzeugt eine Zufallszahlenfolge
- Jedes Paket hat einen neuen Schlüssel
- 24 Bit werden mitgeschickt (dynamischer IV)
  40 / 104 Bit sind geheim (statischer Schlüssel)
- Zufallszahlengenerator ist nicht perfekt
  Zufallszahlen lassen Rückschluss auf Schlüssel zu
- RC4 ist SEHR PERFORMANT

Die Sicherheit von WEP

- WEP gilt seit jeher als unsicher
- Leistungsfähige Tools verfügbar
- AIRCRACK - eines der besten Tools
  um zu sehen wie unsicher WEP wirklich ist

Die Sicherheit von WPA

- WPA und insbesondere WPA2 gelten als sicher
- Für einen Angriff
  Benötigt man die Daten eines Handshakes
- RC4 und AES als Verschlüsselung verfügbar
- Sicherheit hängt vom Netzpasswort ab
- Schnelle Dictionary Attack
- Verfügbare Rechenleistung ist entscheidend

Passive Cryptoanalyse mit Aircrack

- Mitlesen von Initialisierungsvektoren
- Benötigte Mindestmenge (+/- 70%)
  350000 IVs für 64 Bit
  650000 IVs für 128 Bit
- Tools:
  airodump, tcpdump, aircrack

Erfahrungen mit Aircrack

- Menge gesammelter IVs ist entscheidend
- Brachiale Rechenleistung nicht so wichtig
- airodump sammelt nur IVs -> kleine Datei
- tcpdump sammelt Pakete ->
  viel Information nach Entschlüsselung

Vorführung mit einem AP im Saal

- Erklärung der Bildschirmausgabe von Aircrack
- Ermitteln eines 64 Bit Schlüssels

Vor- und Nachteile eines passiven Angiffs

- Vorteile:
  Der Angreifer bleibt unerkannt
  Monitormodus genügt
  Hardwareanforderungen sind gering

- Nachteile:
  Lange Zeit des Sammelns von IVs

Aktiver Angriff

- Künstliches Erzeugen von Traffic - sammeln von IVs
- Replay Attacke
- Sammeln von Paketen die ein ARP-Request sein könnten
- Wiederaussenden eines ARP-Requests
- Tool: aireplay

Vor- und Nachteile eines aktiven Angiffs

- Vorteile:
  man ist relaiv schnell am Ziel

- Nachteile:
  Kompliziert - Treiber - Hardware
  Angemeldete Clients, Reichweite
  Auffällig - IDS

Fazit

- Trotz moderner APs sind etwa 90% der WLANs nur mit WEP gesichert
- 90% der WLANs haben sehr wenig Traffic
- WEP Schlüssel können leicht ermittelt werden
- Verbesserung der Sicherheit notwendig
- WLANs ohne Traffic sind recht sicher

Danke für Ihre Aufmerksamkeit

weitere Fragen