

Generalversammlung SGRP Rahmenprogramm Live Hacking eines Access Points

Roland Portmann, dipl. Ing. ETH



GV SGRP 2005

30. September 2005

Übersicht

- Ziel:
 - Wichtigsten Probleme beim Einsatz von WLAN's kennen
- Programm:
 - Footprinting: Wo sind welche Access Points ?
 - Access Points ohne Verschlüsselung
 - Es geht nicht ohne!!
 - Risiken
 - Eine Lösung
 - Access Points mit Verschlüsselung
 - Einige Angriffe: theoretisch und praktisch

Begriffe

- SSID: Service Set IDentification
 - Wird benötigt für die Anmeldung am Access Point
 - Ein AP sendet i.d.R Beacon Frames mit diesem Namen aus
- BSS ID: Basic Service Set Identifier
 - Zuordnung einer Verbindung zu AP
 - Form einer MAC-Adresse
- Funkkanal
 - 1-13 (je nach Protokoll weitere)
- MAC-Adressen wie bei Ethernetkarten

Unverschlüsselte AP: Gibt es das noch?

- Hotspots
 - In Bahnhöfen
 - In Hotels
 - In Konferenzräumen
 - In Zügen
 - Überall
- Jedermann kann zuschauen !!!!
- Lösung:
 - VPN Verbindungen

Was nützt es, wenn man:

- SSID unterdrückt:
 - Man sieht SSID nur noch beim Verbindungsaufbau
 - Falls WEP eingesetzt wird, sieht man während des Verbindungsaufbaus auch die SSID
 - Der Access Point wird immer noch entdeckt!
- Mac Filter einsetzt:
 - Mac Filter kann umgangen werden
 - Demo Eigenschaft-Seite auf IBM Notebook

Akt 1: unsichere Verschlüsselung WEP

- Man versucht die WLAN mit Verschlüsselung zu sichern
- Ein Teil des Schlüssels ist in Klartext (IV)
- Nach 2^{24} Pakete kommt es zu Kollisionen:
 - Mittels XOR Funktionen kann der Inhalt entschlüsselt werden
 - Kein Angriff auf Schlüssel
 - Vertraulichkeit nicht gewährleistet
 - Keine bekannte Hacker-Tools

Akt 2: Attacke auf Schlüssel

- Seit Sommer 2001 ist die Fluhrer-Mantin-Shamir Attacke bekannt:
 - 3 Bytes des Schlüssels werden immer im Klartext gesendet (IV = Initialvektor)
 - Einzelne IV's sind schwach
 - Wenn ein Teil des Klartextes bekannt ist, kann der Wert eines Schlüsselbytes mit einer Wahrscheinlichkeit von 5% berechnet werden
 - Header Informationen werden auch verschlüsselt → einzelne Byte sind konstant (= Klartext)
 - Wenn man ca. 10'000'000 Pakete gesniff hat, kann mit Programmen (airsnort) der Schlüssel mit hoher Wahrscheinlichkeit berechnet werden.
- Probleme für Hacker:
 - 10'000'000 Pakete → 10 Stunden dranbleiben
 - Moderne WLAN-Devices vermeiden weak IV Vectors.

Akt 3: Die KoreK-Attacke

- Im Sommer 2004 veröffentlichte ein Hacker namens KoreK ein Tool mit dem Namen „chopper“
 - Das Tool basiert auf einer statistischen Kryptoanalyse
 - [Genaue Informationen sind schwer zu finden](#)
 - Gemäss seinen Angaben
 - Bei 256'000 Pakete → 99% Knackwahrscheinlichkeit
 - Bei 128'000 Pakete → 75% Knackwahrscheinlichkeit
 - Allgemeine Tests:
 - Bei 64 Bit Keys → 250'000 Pakete
 - Bei 128 Bit Keys → 500'000 Pakete
 - Unabhängig von Weak Vectors!!
- Aktuelle Tools
 - Aircrack
 - WepLab

Akt 3: Die KoreK-Attacke

- I got this half-baked cracker, which sometimes can crack wep with less 100,000 IVs. There was a post quite while on netstumbler with a reference to 13% cases. Reinjection greatly speeds up the process (if the users are not using p2p). WEP is really bad. It's just that the tools haven't been made/released. Let's say 200000 IVs are necessary + injection tool (500 packet/s, packets are 100byte long): less than 7minutes/20Megs.

Two flaws I have never seen discussed:

Chopping:

- Take a WEP packet. Chop off the last byte. The CRC/ICV is broken. Now if the last byte was 0, you xor last the last 4 bytes with a certain value and the CRC will become valid again. Retransmit the packet. Does it get through? If not, then if the last byte is 1...
- What FMS conveniently forgot to say/Demo of other statistical flaws of WEP:

Gehts mit noch weniger sniffing?

- Ich habe nur ein einziges Paket? Hoffnungslos?
 - Ein Teil des Schlüssels ist bekannt
 - 3 Bytes des verschlüsselten Teils sind konstant (und bekannt)
 - Trottel am Werk?
- Problem:
 - Schlüsselraum auch bei 40 Bit sehr gross (Supercomputer oder viiiiiiiiiiiiiiiiiiiiiiel Zeit)
 - Viele Devices unterstützen eine Klartexteingabe des Schlüssels
 - Schlüssel ist häufig ein MD5 Hash des Klartextes
 - Vielleicht könnte doch eine Dictionary Attacke funktionieren?
 - Tools WepAttack und WepLab

Aktive Tools für WEP-Attacken

- Bis jetzt wurde nur brav gesniff
- Gibt es nicht Methoden mit denen man aktiv eingreifen kann?
 - Problem mit AirCrack: Man braucht 200'000 Pakete und niemand arbeitet
 - Das Airoplay Tool bringt einen AP dazu in einigen Minuten diese Menge Pakete auszusenden (ARP-Pakete)
- Was machen, wenn der WEP Key wirklich nicht zu knacken ist?
 - Replay Attacken mit dem Tool chopchop
 - Ein gesniffes Packet wird einem AP zurückgeschickt. Dabei wird jeweils ein Byte geändert.
 - Man wartet aus, ob der AP das Packet akzeptiert oder nicht und kann damit den Inhalt entschlüsseln.

Tools?

- Linux PC mit Auditor Knoppix
- Alle Tools sind in der neuesten Version vorhanden.
- <http://remote-exploit.org/?page=auditor>