**ERNW Newsletter 13 / Februar 2007**

Liebe Partner, liebe Kollegen,

willkommen zur dreizehnten Ausgabe des ERNW-Newsletters mit dem Thema:

# WLAN-Security

Version 1.0 vom 31. Januar 2007

von:

Enno Rey (erey@ernw.de)

Der folgende Artikel unternimmt den Versuch einer Bestandsaufnahme des aktuellen Stands von WLAN-Sicherheit. Dazu werden aktuelle Angriffsmethoden, zugehörige Gegenmassnahmen und Entwicklungen beleuchtet.

Die beiden Haupt-Bedrohungen gegen Wireless LANs sind das Mitlesen/Verändern von Verkehr und unautorisierter Netz-Zugang durch einen Angreifer (mit nachfolgenden Attacken gegen Systeme des Netzes).

Im Gegensatz zum kabelgebundenen Netz setzt das Sniffing (Mitlesen) von Netzwerk-Verkehr in WLANs keinen bereits vorhandenen (physischen) Zugang zum Netz voraus. Da die Ausbreitung der Pakete über das Medium (Funk) kaum kontrolliert werden kann, muss stets davon ausgegangen werden, dass ein Angreifer alle per WLAN übertragenen Pakete mitlesen kann (mithilfe einer Karte, die im sog. *RF Monitor Mode* läuft).

Effizienter Schutz kann daher nur durch Verschlüsselung des Verkehrs erfolgen und durch Regelung, welche Stationen „am Netz teilnehmen“ (also Pakete senden) können. Häufig werden jedoch die technologisch vorhandenen Schutzmassnahmen bei WLANs nur unzureichend genutzt und selbst bei Einsatz von Sicherungs-Massnahmen sollte bedacht werden, dass manche davon schlicht mangelhaft (und in Folge mittlerweile mit trivialen Mitteln attackierbar) sind.

Es können in etwa drei „Generationen“ an WLAN Sicherheits-Mechanismen unterschieden werden. Ihre jeweiligen (Protokoll-) Vertreter und Probleme sind in der nachfolgenden Tabelle aufgeführt. Zusammenfassend kann festgehalten werden, dass Technologien der „alten Welt“ nahezu immer erfolgreich attackiert werden können, dies in der „zweiten Generation“ von der konkreten Konfiguration abhängt und in der „modernen Generation“ wiederum als aktuell nicht möglich gilt (vorausgesetzt, es sind keine schwerwiegenden Konfigurations-Fehler unterlaufen).

| Generation | Schutz vor unautorisiertem Zugang | Schutz vor Mitlesen/Veränderung | Bewertung |
|---|---|---|---|
| „alte Welt“ (802.11b) | MAC-Filterung, kein SSID-BC, WEP | WEP (statisch) | leicht angreifbar hinsichtlich Zugang + Entschlüsselung (auch *backward,* d.h. von bereits aufgezeichnetem Traffic). |
| „Zweite Generation“ | Authentifizierung (802.1x) | TKIP/“dynamisches WEP“, MIC | je nach Implementierung angreifbar. Meist jedoch keine *backward*-Analyse möglich. |
| „Moderne Generation“ | Authentifizierung (802.1x mit Zertifikat[en]) | TKIP + MIC, AES-CCMP [WPA2] | Gilt aktuell als nicht mehr auf Zugangs-/Transport-Ebene angreifbar |

Tabelle 1 Generationen WLAN-Security

Typische Angriffe gegen WLANs

Zum Angriffs-Werkzeug gegen WLANs gehören zunächst geeignete Netzwerk-Karten. Diese sollten mittlerweise mindestens 802.11b und 802.11g unterstützen (je nach attackiertem Netz auch 802.11a) und einen von den einschlägigen Tools unterstützen Chipsatz aufweisen (dies ist neben ‚dem Klassiker’ PRISM2 inzwischen in erster Linie der Atheros-Chipsatz, der hinsichtlich Tool-Support dem erstgenannten sogar mittlerweile den Rang abgelaufen hat).

Daneben sind (mind.) ein Anschluss für eine externe Antenne und – falls den Angreifer gesetzliche Vorgaben nicht interessieren – die Sendeleistung der Karte wichtige Kriterien (hierzulande sind nur 100 Milliwatt zulässig, es sind aber über das Internet Karten mit bis zu 300 Mw erhältlich). Eine gute „Allrounder“-Karte ist etwa die Proxim 8470-WD.



Neben Adaptern gehören Antennen zum Werkzeugkasten von WLAN-Hackern. Typischerweise verfügt ein Angreifer über mehrere Antennen für verschiedene Zwecke.

Der Antenne kommt meist grosse Bedeutung hinsichtlich der passiven und aktiven Erreichbarkeit eines anzugreifenden Netzes zu (weit grössere übrigens als der Leistung der Karte selbst). Dies ist ein Faktor, der auch aus Sicht eines Sicherheits-Beauftragten beachtet werden sollte. Denken Sie nie, dass ein Angreifer Ihre WLANs nicht erreichen kann, nur weil Ihnen selbst das während eines Tests vom Firmenparkplatz aus nicht gelungen ist. „My antenna is bigger than yours“ lautet ein Hacker-Slogan, der dies auf den Punkt bringt.

Bei der Auswahl der Tools und des zugrundeliegenden Betriebssystems ist für WLAN-Angriffe Windows meist eine schlechte Wahl. Viele Tools und vor allem (modifizierte) Kartentreiber sind nur unter BSD oder Linux lauffähig und haben hier traditionell einen gewissen Installations- und Konfigurations-Aufwand erfordert.

Mittlerweile sind Live-CDs verfügbar, die alle Tools mitbringen (bekanntester Vertreter ist die *BackTrack*), so dass sich das notwendige Angreifer-Knowhow auf das Booten einer CD samt Lesen einer Manpage reduzieren lässt.

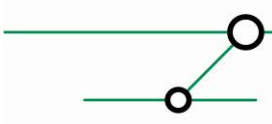
Ein typischer Angriff besteht in etwa aus folgenden Schritten:

- Identifizierung anzugreifender Netze
- Mitlesen des Verkehrs [eingesetztes Tool meist *airodump*]
- Ggf. Injektion von Paketen [*aireplay*]
  - zur De-Authentifizierung von Clients (etwa zum Sniffen eines WPA-Handshakes)
  - zur Erzeugung von Verkehr (zur Ermittlung eines WEP-Schlüssels)
- Bei Vorliegen ausreichender Pakete Knacken des WEP-Keys, WPA-PSK [*aircrack*] oder LEAP-Passworts [*asleap*]
- Ggf. Entschlüsselung des bereits aufgezeichneten Verkehrs [*airdecap*]
- Teilnahme am WLAN und Angriffe gegen weitere Netzteilnehmer oder Netzwerk-Verkehr

Vorab ist festzuhalten, dass statisches WEP so gut wie immer knackbar ist, wenn es dem Angreifer gelingt, Pakete mit ca. 500.000 (bei 64Bit WEP) bis 1000.000 (128Bit) unterschiedlichen sogenanten Initialisierungs-Vektoren (IVs) aufzuzeichnen. Dies dauert (ohne zusätzliche Angriffe, siehe dazu unten) in einem WLAN mit mehreren aktiven Stationen und typischem User-Verhalten (Fileserver-Zugriffe, Mail, Surfen) meist nur einige Stunden. Das Knacken selbst ist danach in wenigen Minuten erledigt.

Angriffe gegen WPA mit *Preshared Key* (WPA-PSK) und LEAP basieren hingegen auf Bruteforce-Verfahren oder Wörterbuch-Attacken und sind daher von der Güte der eingesetzten Kennwörter abhängig.





WEP ist (erstaunlicherweise?) noch immer in etwa 20-30% der Unternehmensnetze anzutreffen; eine ähnliche Verteilung gilt für Privathaushalte. Vom Arbeitszimmer eines der Autoren aus sind etwa folgende Netze sichtbar (Tool: *airodump*):

| # | BSSID | ESSID | Encryption |
|---|---|---|---|
| 1 | 00:30:F1:EC:5C:F6 | engelbert | WPA (0 handshake) |
| 2 | 00:0E:2E:33:C7:2F | 01050501 | WEP (112 IVs) |
| 4 | 00:12:BF:4E:56:E7 | WLAN | WPA (0 handshake) |
| 5 | 00:09:5B:2C:59:DC | ZEN | None (192.168.0.3) |
| 6 | 00:03:C9:B6:9A:99 | WLARS | No data - WEP or WPA |
| 7 | 00:30:F1:D4:90:DD | Elchland2 | WPA (0 handshake) |
| 8 | 00:04:0E:36:17:8E | | No data - WEP or WPA |
| 9 | 00:04:0E:2B:B8:13 | Fritz!Box SL WLAN | No data - WEP or WPA |
| 10 | 00:04:0E:62:35:8F | KLAAS | WEP (1380 IVs) |
| 11 | 00:13:49:15:7D:5C | ArcorWirelessLANxc7R | WEP (58 IVs) |
| 12 | 00:09:5B:41:B9:54 | Sinead_OConnor | No data - WEP or WPA |
| 13 | 00:30:F1:EB:7C:CE | | No data - WEP or WPA |
| 14 | 00:09:B7:55:27:7C | AP1 | No data - WEP or WPA |
| 15 | 00:03:C9:B9:CC:DD | bar*2=a! | No data - WEP or WPA |
| 16 | 02:7C:CA:C7:0E:85 | PSP_AUCES00001_L_ | None (0.0.0.0) |
| 17 | 00:14:6C:7D:07:5C | Unknown | |
| 18 | 00:15:0C:2E:B2:2A | SimmiPetraTina | WPA (0 handshake) |
| 19 | 00:15:E9:06:83:AA | wireless | No data - WEP or WPA |
| 20 | 00:40:96:52:FC:8E | r2a | No data - WEP or WPA |
| 21 | 00:14:6C:7D:07:82 | HANSOLO | No data - WEP or WPA |



Inmitten einer deutschen Großstadt sieht ein zufälliger Snapshot so aus:

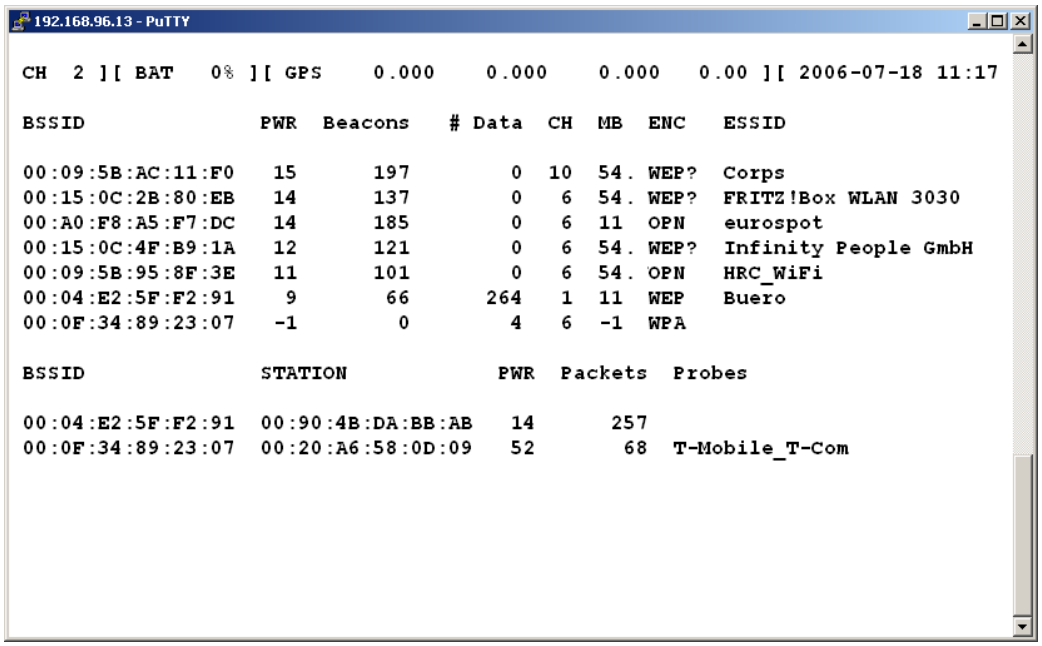



Abb. 1 Zufälliger Snapshot erreichbarer WLANs in einer Grosstadt

Anhand der Spalte „Data“ wird ersichtlich, in welchen Netzen am meisten ‚interessante’ Pakete übertragen werden, weshalb ein Angreifer seine Aufmerksamkeit jetzt speziell dem Netz mit SSID „Buero“ zuwenden könnte (oder einem der anderen Netze, wenn es sich um einen zielgerichtete Attacke handelt):

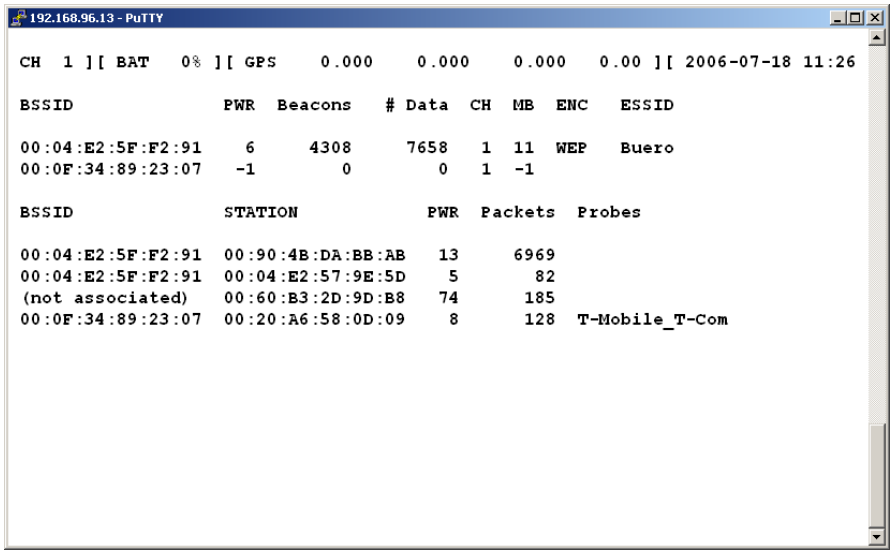



Abb. 2 Fokussierung auf ein Netz

Dadurch werden dann noch mehr verwertbare Pakete aufgezeichnet (also solche, die – bei Angriffen gegen WEP – interessante Initialisierungsvektoren enthalten).

Wird dann eine leistungsfähige Antenne angeschlossen, kann die Empfangsleistung erheblich erhöht werden:

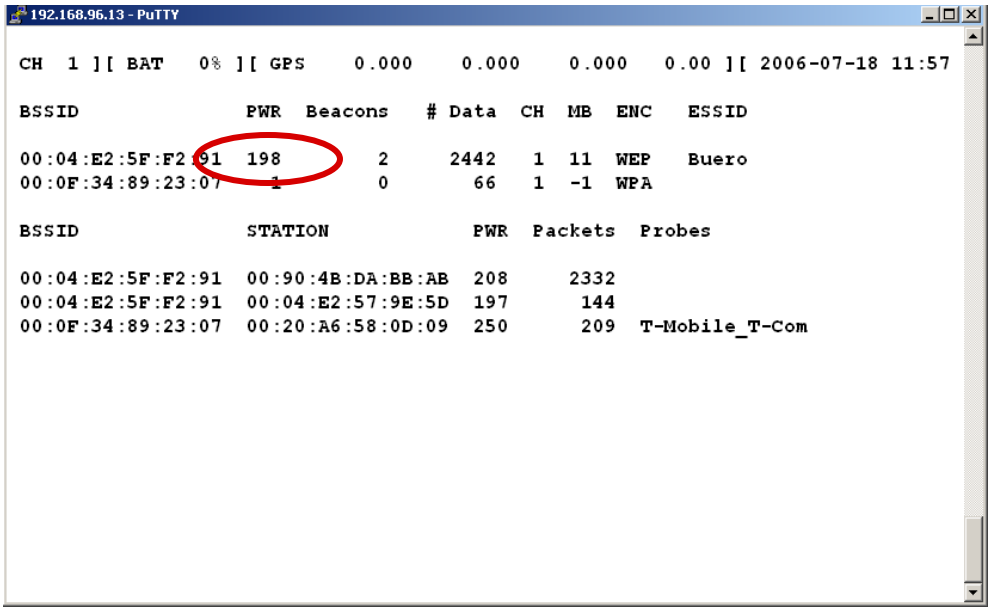



Abb. 3 Verbesserung der Empfangsleistung durch Anschluss einer Antenne

Da nur eine zwei assoziierte Stationen sichtbar sind, von denen auch nur eine Netzwerk-aktiv ist, wäre es jetzt möglich, dem Angreifer-Glück durch die Injektion von Pakete nachzuhelfen. Hier werden nicht nur passiv Pakete mitgelesen, sondern aktiv Pakete in das Netz eingebracht.

Dies ist für bestimmte Pakete auch ohne Kenntnis des WEP-Keys möglich, der ja gerade erst noch ermittelt werden soll. So werden etwa sog. Management-Frames gar nicht verschlüsselt und andere Pakete sind anhand ihres immergleichen (Header-) Aufbaus auch ohne Entschlüsselung identifizierbar. Dies gilt z.B. für ARP-Requests.

Einen solchen kann dann der Angreifer nach Aufzeichnung erneut in das Netz einbringen und entsprechende ARP-Antworten (Responses) hervorrufen, die jeweils mit eigenen IVs verschlüsselt sind und damit die Anzahl interessanter, aufzeichenbarer Pakete vergrössern:

Das eingesetzte Tool heisst *aireplay*:

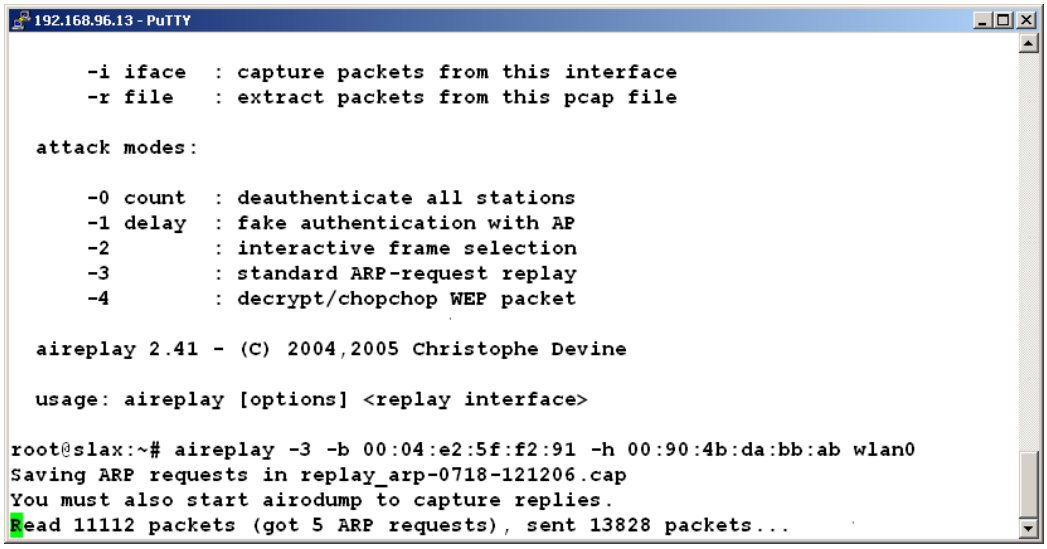
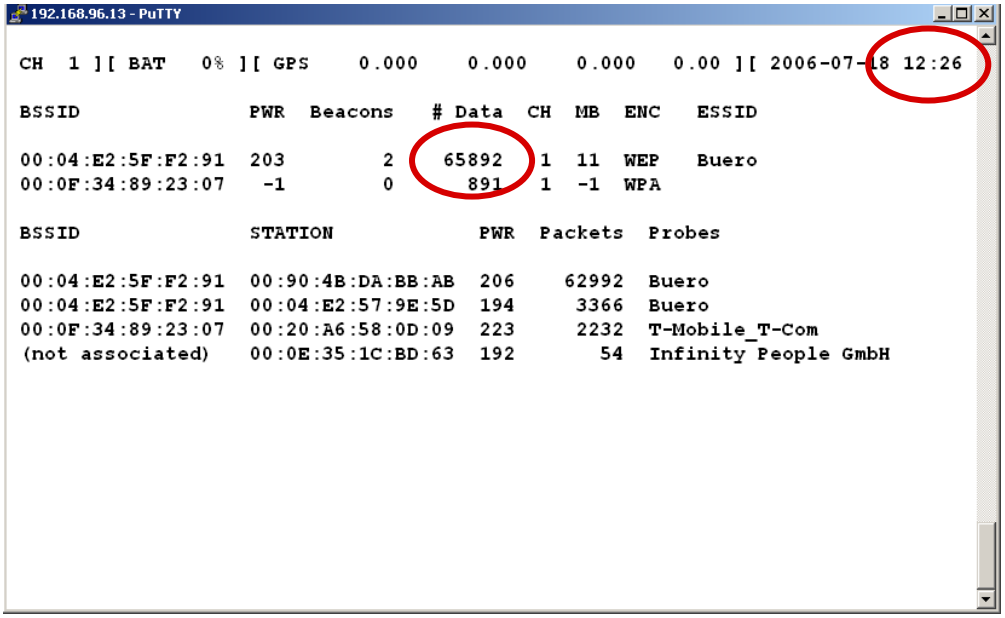



Abb. 4 Optionen und Einsatz eines Injektions-Tools

und der angestrebte Effekt ist unmittelbar sichtbar:




Verfügt der Angreifer dann nach einiger Zeit (hier ca. 60 Minuten) über ausreichend Pakete, ist das Knacken des Schlüssels nur noch Formsache:

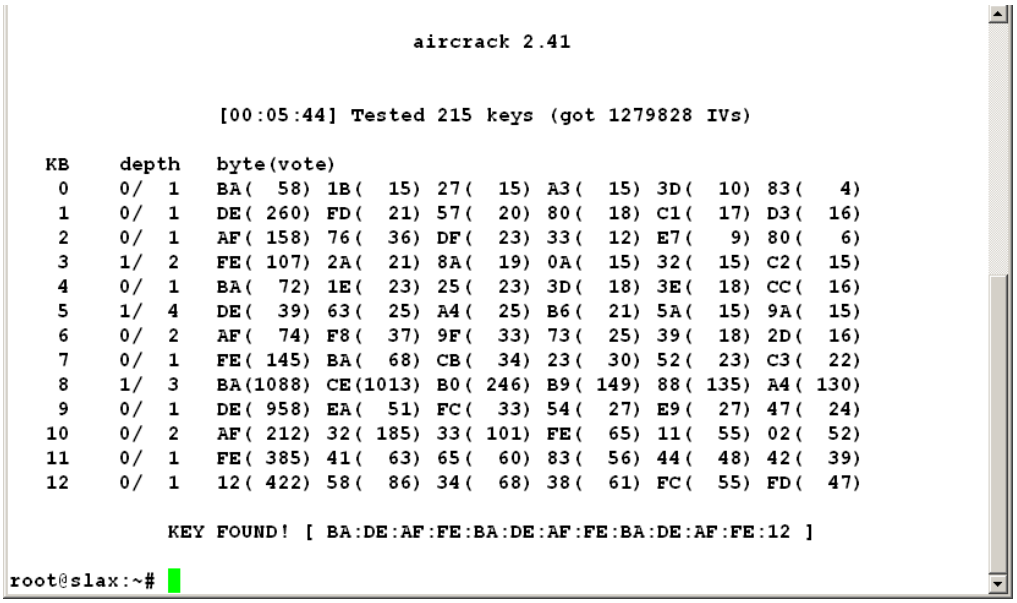



Abb. 6 Knacken eines WEP-Keys inkl. benötigter Zeit

Hätte es sich um ein Netz gehandelt, das mit einem (schwachen) WPA-PSK „geschützt“ wäre, sähe der Knackvorgang etwa so aus

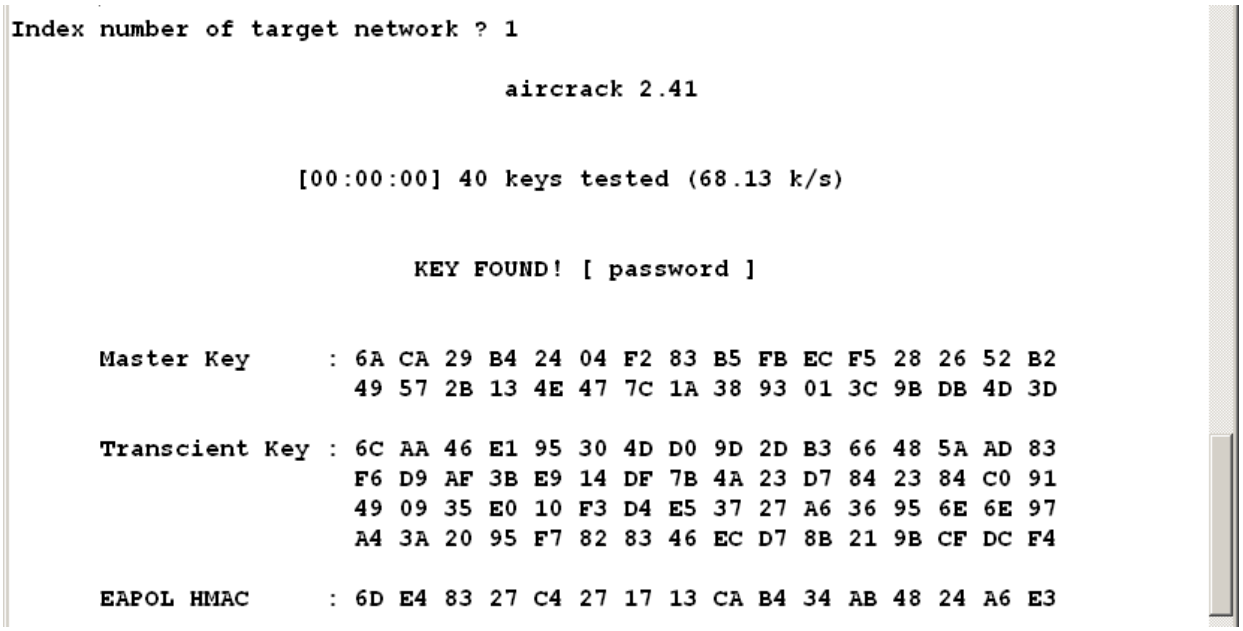



Abb. 6 Knacken eines WPA-PSK

Da WPA-PSK aber nur durch Bruteforce- oder Wörterbuch-Angriffe erfolgreich attackiert werden kann, ist ein langer, komplexer Schlüssel zur Abwehr von Angriffen sicher hilfreich (zumal die zugrundeliegenden Einzelschritte beim Knacken durchaus aufwendig im Sinne von erforderlichen CPU-Zyklen sind).

Es sollte jedoch bedacht werden, dass ein motivierter, gut ausgerüsteter Angreifer einen Teil der notwendigen Rechenarbeiten schon im Vorfeld erledigen kann bzw. inzwischen auf sog. pre-computed tables oder spezielle Hardware zurückgreifen kann und damit die zum Knacken notwendige Zeit erheblich verkürzen kann [1].

Sollten also im Organisations-Kontext Sicherungs-Mechanismen der „zweiten Generation“ (dies sind in erster Linie WPA-PSK und LEAP) zum Einsatz kommen, ist eine Risiko-Analyse erforderlich, die u.a. den Schutzbedarf der übertragenen Daten und mögliche Angreifertypen berücksichtigt.

In der Praxis kann nämlich oft der „reinen Lehre“ der WLAN-Sicherheit, die im Grunde 802.1x-basierte Authentifizierung mit Zertifikaten (mindestens auf Infrastruktur-Seite) als alleinig sichere Lösung ansieht, häufig nicht entsprochen werden.

Gründe hierfür können sein:

- Der Implementierungs-Aufwand, insbesondere die Bereitstellung einer PKI.
- Nicht alle Wireless-Clients unterstützen Zertifikats-basierte Verfahren (dies gilt etwa Drucker, Mobile Datenerfassungsgeräte, manche Unix-basierten Stationen).
- Betriebs-Erfordernisse können dem entgegenstehen, etwa wenn an kleinen Remote-Standorten die Netz-Teilnahme nicht von stabilen Verbindungen zum Haupt-Standort abhängen soll und kein administratives Personal vor Ort ist.

Neben der Auswahl einzusetzender Technologien und Protokolle ist die Gesamt-Sicherheit von WLANs jedoch auch von Design-Aspekten und organisatorischen Prozessen abhängig. Dazu zählen etwa:

- Netzwerk-Design und Segmentierung
- Die Rolle von Access Points (Fähigkeiten und ihre Verwaltung)
- Intrusion Detection

Netzwerk-Segmentierung, die die Sicherheit unterstützt, basiert immer auf „Security-Leveln“ im Netz. Diese richten sich idealerweise nach dem Schutzbedarf der transportierten Daten/der enthaltenen Knoten („Server mit Personaldaten gehören in ein dediziertes Segment“) oder nach dem Bedrohungs-Potential („Clients, die aufgrund bestimmter Faktoren nicht gepatcht werden können, gehören in eigene Segmente“).

Von diesen Grundgedanken ausgehend sollte jede Organisation im Rahmen eines formalisierten Prozesses entscheiden, ob und welche WLANs in segmentierten Netz-Einheiten (etwa IP-Subnetzen) realisiert werden. Gelangt man etwa zum Ergebnis, dass das Bedrohungspotential in WLANs und kabelgebundenen Netzen unterschiedlich ist, sollten diese nicht in gemeinsamen IP-Subnetzen implementiert werden.

Darüber hinaus unterstützen viele moderne Access Points die Bildung von VLANs (mit jeweils eigenen SSIDs und zugehörigen Authentifizierungs-/Verschlüsselungs-Methoden). Solche Fähigkeiten sollten weitestmöglich genutzt werden, insbesondere wenn die Landschaft der assoziierten Stationen hinsichtlich ihrer Security-Fähigkeiten heterogen ist.



Eine immer grössere Rolle kommt der Sicherheit der Access Points selbst zu. Je nach Erfordernissen und Management-Strukturen kann es sinnvoll sein, „thin“ oder „dumb“ Access Points einzusetzen, die über kaum eigene Intelligenz verfügen und deren Steuerung und Verwaltung über nachgelagerte Switches oder „WLAN Controller“ stattfindet. Die Vor- und Nachteile solcher Lösungen werden in einem nachfolgenden Artikel diskutiert.

Wenn „autonome“ Access Points mit eigener Intelligenz eingesetzt werden, müssen diese vor Diebstahl angemessen geschützt werden (Umfragen zufolge sind mind. 10% der auf ebay angebotenen Access Points gestohlene Geräte) und sie müssen als Infrastruktur-Devices gegen unautorisierten Zugriff geschützt werden. Dazu zählen typische Hardening-Mechanismen wie die Auswahl sicherer Management-Methoden (SSH statt Telnet, HTTPS statt HTTP), die Restriktion zulässiger IP-Adressen beim Zugriff und die Konfiguration guter Authentifzierungs-Mechanismen (Userverwaltung, Kennwörter). Eine Checkliste für Cisco-basierte Access-Points kann von den Autoren bezogen werden [2].

Sicherheit umfasst jedoch nicht nur Prävention, sondern immer auch funktionierende Kontroll- und Detektions-Mechanismen. Zur WLAN-Sicherheit sollten daher auch Intrusion Detection Fähigkeiten gehören, die ermöglichen, unzulässige Netzteilnehmer (Stationen oder sog. *Rogue Access Points*) zu erkennen und ggf. orten oder nachverfolgen zu können.

Dies kann über die Korrelation und Auswertung von Logfiles geschehen oder über dedizierte Technologien. Leider existieren hier bisher keine Hersteller-übergreifenden Standards, sondern nur proprietäre Lösungen (etwa Ciscos WLSE-Appliance, die in erster Linie zentrale Management-Aufgaben übernimmt).



Zusammenfassend kann festgehalten werden, dass WLANs je nach eingesetzter Technologie vergleichsweise einfach attackiert werden können (oder eben nicht). Die Wahl einer Technology wird von diversen Faktoren bestimmt und sollte Gegenstand einer Risiko-Analyse sein. WLAN Sicherheit umfasst daneben auch geeignetes Netzwerk-Design und Betriebs-Prozesse. Der Fokus von WLAN-Angriffen wird sich zukünftig verlagern; Angriffsfläche bieten dann etwa die Web-Interfaces von Access Points oder Hersteller-proprietäre Protokolle (z.B. Ciscos WLCCP).

Links:
[1] http://www.layerone.info/2006/presentations/Cracking_WiFi_Faster-LayerOne-Church_of_WiFi.pdf
[2] www.ernw.de/publikationen/hard_cisco_aps.pdf

Mit freundlichen Grüßen,

Enno Rey
CISSP, ISSAP, CISA

Kontakt:
Roland Fiege
Kaufm. Geschäftsführer
ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 151 16 22 7557
rfiege@ernw.de
www.ernw.de