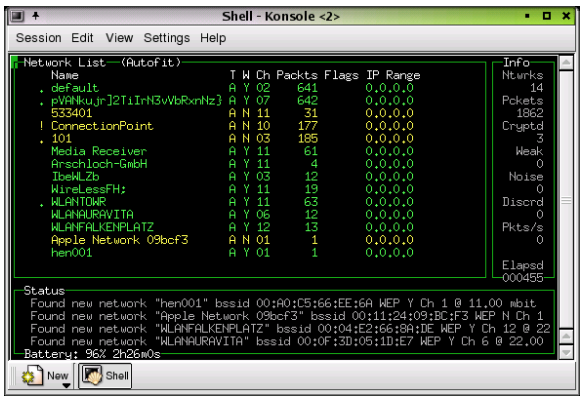
Securing Wireless Networks Reloaded

by Christoph Schnidrig
christoph.schnidrig(at)csnc.ch / christoph.schnidrig(at)gmail.com

Einleitung

Vor knapp zwei Jahren machte Compass Security AG in einem Artikel (Securing Wireless Networks) sowohl auf schwerwiegende Sicherheitslücken in der Konfiguration, als auch in der Verschlüsselung von Wirelessnetzwerken aufmerksam. Aufgrund Erfahrungen und neuen Tools möchte an dieser Stelle nachgegriffen werden. Ein neues Tool erhöht die Geschwindigkeit, mit welcher die WEP-Verschlüsselung gebrochen werden kann massiv. Leider kann aufgrund von Feldtests auch gesagt werden, dass der Sicherheitsproblematik trotz Warnungen in der Presse, wenig Beachtung geschenkt wird.

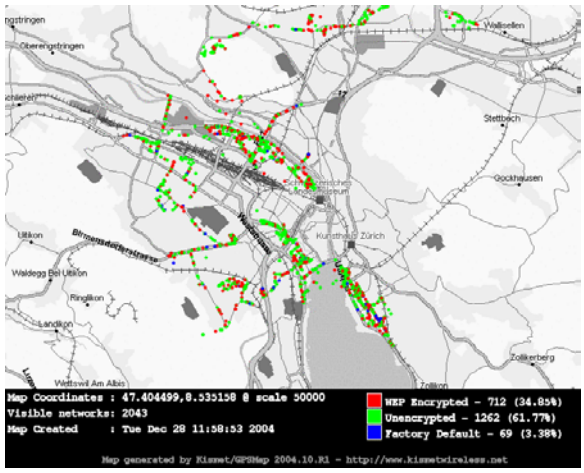
Wardriving – der Fachausdruck für das Entdecken von Funknetzwerken verkommt langsam zum Volkssport. Einfach zu bedienende Tools sind im Internet verfügbar und auf einschlägigen Webseiten können Landkarten mit den detektierten Funknetzwerken gefunden werden.



Wireless Scanner: Kismet

Keine Verschlüsselung

Den Statistiken kann man entnehmen, das zwischen 50 und 70% aller Funknetzwerke unverschlüsselt sind. Dies geschieht sicherlich auch wegen der technischen Unbewandtheit und der Unbekümmertheit von Privatanwendern. Ein Hacker kann diese Gegebenheit nutzen um einerseits heimische Computer anzugreifen und andererseits bösartige Aktivitäten im Internet (z.B. Einspeisung eines Virus) zu kaschieren. Solche Funknetze sind sehr einfach aufzuspüren und können einfach und ohne Passwort benutzt werden. Wie fälschlicherweise oft angenommen wird, bietet die SSID (Netzname) keine, beziehungsweise nur sehr geringe Sicherheit.

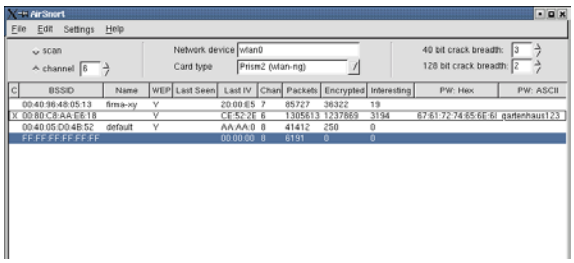


WLAN-Netz Karte von Zürich

Fehlerhafter Produktestandard

Wireless Netze bieten die Möglichkeit die übertragenen Daten zu verschlüsseln (Wired Equivalent Privacy kurz WEP). Leider ist diese Verschlüsselung fehlerhaft implementiert und es gibt frei erhältliche Tools zum Knacken der Keys. Diese sind notwendig um sich in ein WEP-geschütztes Netzwerk einzuklinken.

Dass dies möglich ist, ist schon seit bald 4 Jahren bekannt. Die Tools dazu sind auch beinahe so lange verfügbar (z.B. Airsnort).



WEP Cracker: AirSnort

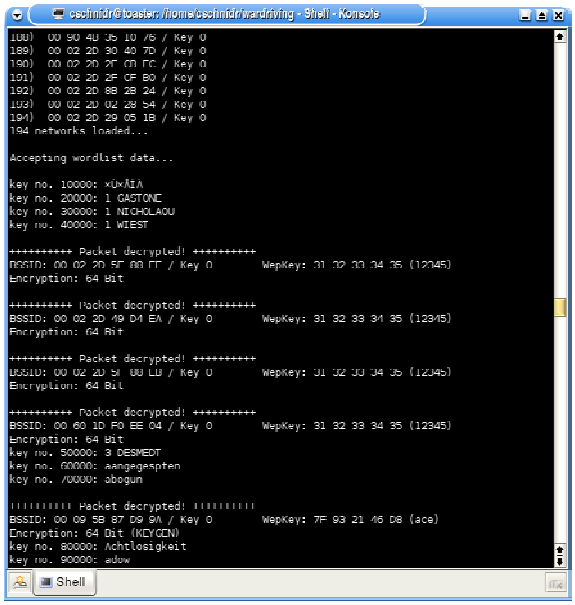
Airsnort nutzt als Angriffspunkt die relativ kurzen Initialisierungsvektoren (IV) - es

by Christoph Schnidrig
christoph.schnidrig(at)csnc.ch / christoph.schnidrig(at)gmail.com

werden ca. 3000 bis 5000 schwache Pakete für das Brechen des WEP-Keys benötigt. Dazu muss der gesamte WLAN-Verkehr über mehrere Stunden resp. Tage oder gar Wochen aufgezeichnet werden. Je nach Netzwerkbelastung und der verwendeten Komponenten ist das sehr aufwendig. Nach dem Bekanntwerden dieser Schwäche begannen Hersteller diese schwachen IVs zu filtern dieser Schwäche entgegen zu wirken.

Schwache WEP-Keys

Zu der eben erläuterten WEP Problematik kommt, dass viele Administratoren zu schwache WEP Keys wählen. Das Tool wepattack versucht diese Gegebenheit auszunutzen und implementiert eine Wörterbuchattacke auf WEP. Mittels geschickter Ausnutzung von Gegebenheiten, bei WEP Paketen sind die ersten 6 Bytes immer gleich (known plaintext), kann das Tool mehrere Tausend Keys pro Sekunde prüfen. Dazu wird lediglich ein einziges verschlüsseltes WLAN-Paket benötigt. Bei einem Feldversuch, wurden verschlüsselte Pakete von 192 Netzen aufgefangen. Nachdem wepattack 3 Tage lang auf die Pakete angesetzt worden war, waren 10% aller WEP Keys gebrochen!

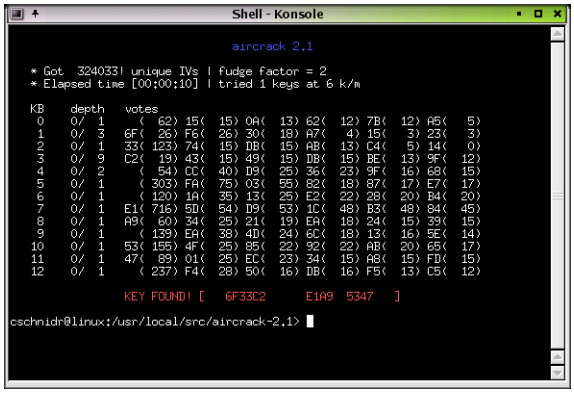


Wepattack – Wörterbuchattacke gegen WEP

Dies ist nur möglich, weil normale Wörter als WEP-Key benutzt werden. Leider sind auch einige in Wireless-Software eingebauten Key-Generatoren sehr schwach und nutzen nur einen kleinen Bereich des zur Verfügung stehenden Zeichenraums (key space).

Neue WEP-Attacke

Im Sommer 2004 wurde eine weitere WEP-Attacke, die auf statistischer Kryptoanalyse basiert, bekannt. Das Tool (chopper) war ein sogenannter proof-of-concept und wurde sicher auch deshalb von anderen neu implementiert. Da die neue Art WEP zu knacken nicht mehr auf schwachen IVs basiert, ist es nicht mehr nötig Millionen von Wireless-Paketen zu sniffen. Wenige hunderttausend Pakete reichen aus, um den WEP-Key statistisch zu erheben.



Ab 300'000 verschlüsselten WLAN-Paketen knackt aircrack den verwendeten WEP-Key!

Sind die Pakete einmal gesammelt geht die Kryptoanalyse sehr schnell von statten. Aircrack benötigt dazu nur wenige Minuten.

Diese Attacke rüttelte die IT-Sicherheitswelt auf. Das ohnehin schon angekratzte Image der Wireless-Sicherheit ist nun ganz dahin. Die Lösungen zur Behebung dieser Sicherheitsmängel sind schon lange diskutiert. Entweder man lässt die Finger vom Funknetzwerken, benutzt neuere Technologien oder verschlüsselt den Datenverkehr zusätzlich mit einem VPN, welche oftmals schon vorhanden ist.

by Christoph Schnidrig
christoph.schnidrig(at)csnc.ch / christoph.schnidrig(at)gmail.com

WEP ist Vergangenheit, WPA Zukunft

„WEP dead again" lautet der treffende Titel eines lesenswerten Artikels auf securityfocus.com. Auch die zuvor aufgezeigten Sicherheitsprobleme von WEP zeigen, dass WEP wirklich tot ist resp. sein müsste. Im Sommer 2004 wurde ein neuer Standard (802.11i) verabschiedet, der die WLAN-Sicherheit von Grund auf neu definiert. Da schon lange grosser Druck auf den Herstellern lastete, wurde ein Subset aus dem neuen Standard genommen und ein Quasistandard Wi-Fi Protected Access (WPA) definiert. WPA bietet denn auch stark verbesserte Sicherheit:

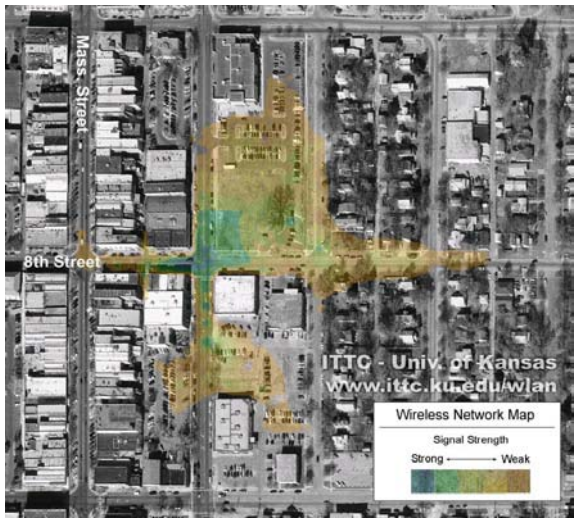
- ❑ WEP wurde durch TKIP und Michael ersetzt. Hiermit werden auch dynamische Keys eingeführt, welche alle paar Minuten gewechselt werden.
- ❑ Zur Ermittlung der Sitzungsschlüssel wurde ein Handshake-Verfahren zwischen Client und AP entwickelt (EAP). EAP authentisiert zum einen den Client und verteilt auch die Schlüssel.
- ❑ Ein vereinfachtes Verfahren mittels PSK (pre-shared key), bei welchem kein Radiusserver benötigt wird, wird auch bereitgestellt. Hier gilt es zu beachten, dass lange und zufällige Keys gewählt werden. Es gibt bereits Tools die auf den WPA PSK Wörterbuchattacken durchführen können!
- ❑ Aushandlung des Verschlüsselungsverfahrens zwischen Client und AP. Gemischte WEP/WPA Netze werden dabei auch zu gelassen, davor wird aber ausdrücklich abgeraten.

Der Standard IEEE 802.11i unterstützt weitere Sicherheitsfunktionen, wie zum Beispiel AES-Verschlüsselung. Es ist zu erwarten, dass die Anbieter diese Funktionen auch in ihre Produkte integrieren werden. Diejenigen Produkte die den neuen Standard voll unterstützen tragen das Label WPA2.

Checkliste

Wer trotz allen Ausführungen noch Wireless einsetzen möchte oder muss, sollte folgende Punkte beachten. (Die Reihenfolge stellt keine Priorisierung dar!)

- ❑ Guter Standort für den AP auswählen
  Access Point wenn möglich nicht an ein Fenster sondern eher in die Gebäudemitte stellen.



Wegen der grossen Abstrahlung können viele andere den WLAN-Verkehr empfangen.

- ❑ WPA benutzen
  Neuere Produkte unterstützen sogenannte Pairwise Keys (eigene Keys pro WLAN-Verbindung).
- ❑ Benutzung von EAP-TLS
  Im Zusammenspiel mit einem Radiusserver kann die Authentisierung und die Schlüsselverteilung implementiert werden.
- ❑ Falls trotzdem PSK eingesetzt wird
  Unbedingt starke und lange Keys wählen. Siehe Keygenerator unter Tools. Den eingebauten Keygenerator nicht verwenden.
- ❑ Neutraler Netznamen (SSID) wählen
  Nicht den Firmennamen oder andere Angaben, die Rückschluss auf den Betreiber erlauben.

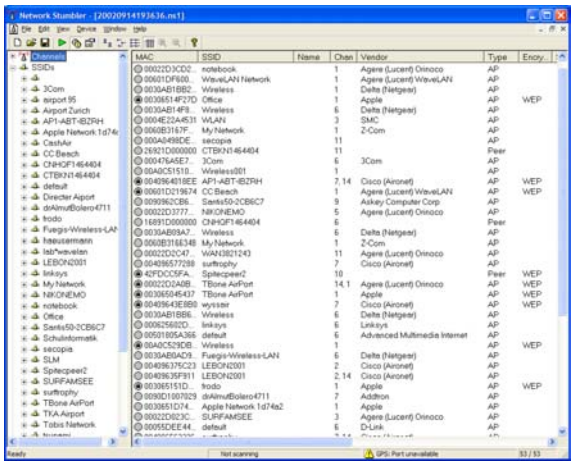
by Christoph Schnidrig
christoph.schnidrig(at)csnc.ch / christoph.schnidrig(at)gmail.com

- ❑ SSID Broadcasts wenn möglich abstellen
  Dies verhindert das „ausposaunen" des Netznamens. Ist bei den meisten Accesspoints möglich.
- ❑ Admin Interfaces des AP schützen
  Starke Passwörter wählen und alle Dienste die nicht benötigt werden ausschalten: SNMP, Telnet, HTTP...
- ❑ Schalten Sie ihren Accesspoint bei nicht Gebrauch aus. Dies könnte mit einer Zeitschaltuhr automatisiert werden.
- ❑ Für sensitive Netze empfehlen wir zusätzlich die Installation eines VPN's. Kann ein Angreifer die WPA Verschlüsselung knacken, sieht er trotzdem nur verschlüsselte Daten.
- ❑ Da die statischen WPA PSK auf dem Client Computer gespeichert werden, muss auch auf diese geachtet werden. Wir empfehlen den Patchlevel und die Virendefinitionen auf den Clients aktuell zu halten.
- ❑ Zweckmässiges Konfigurieren und regelmässige Kontrolle der Logs auf dem Access Point.
- ❑ Selbst regelmässige Scans durchführen um sicherzustellen, dass keine Accesspoints von Mitarbeitern installiert worden sind.
- ❑ Behalten Sie die Security-Advisories ihres Funkkomponenten Herstellers im Auge und aktualisieren Sie wenn nötig die Firmware der eingesetzten Geräte.
- ❑ Erkundigen Sie sich vor dem Kauf über die verschiedenen Sicherheits-Features der Produkte.

Referenzen

Tools

- ❑ NetStumbler (Network Discovery / Win32)
  http://www.netstumbler.org/



Wireless Scanner: NetStumbler

- ❑ Kismet (Network Discovery, Sniffer / Linux)
  http://www.kismetwireless.net/
- ❑ AirSnort (WEP Cracker / Linux)
  http://airsnort.shmoo.com/
- ❑ WEPAttack (WEP Wörterlisten Attacke / Linux)
  http://wepattack.sourceforge.net/
- ❑ aircrack (Statistische Kryptoanalyse / Linux und Win32)
  http://www.cr0.net:8040/code/network/
- ❑ Keygenerator für zufällige Keys
  http://www.csnc.ch/static/download/download_tools.html

Eigenbau Antennen

- ❑ Pringels Antenne
  http://www.oreillynet.com/lpt/wlg/448
- ❑ Omnidirectional Antenne
  http://www.tux.org/~bball/antenna/
- ❑ Antennen Anschluss Umbau (DWL 650)
  http://c0rtex.com/~will/antenna/

by Christoph Schnidrig
christoph.schnidrig(at)csnc.ch / christoph.schnidrig(at)gmail.com

Technische Dokumentation

- Weaknesses in the Key Scheduling Algorithm of RC4 (Ursprung der WEP Attacken)
  http://downloads.securityfocus.com/library/rc4_ksaproc.pdf
- WEP: Dead Again, Part 1
  http://www.securityfocus.com/infocus/1814
- Statistische Kryptoanalyse bei WEP: KoreK
  http://forums.netstumbler.com/showthread.php?t=12489
- heise.de: Angriffe auf WPA
  http://www.heise.de/security/artikel/53014
- heise.de: Jenseits von WEP
  http://www.heise.de/kiosk/archiv/ct/2004/21/214

Weitere Infos

- Gute Quelle mit vielen Securitythemen
  http://www.sans.org/rr/wireless/
- Schweizer Wardriving Portal
  http://www.wardriving.ch/
- Wireless Network Visualisation Project
  http://www.ittc.ku.edu/wlan/
- 802.11 Community
  http://nocat.net/
- WiFi Konsortium (WPA)
  http://www.wifi.org

Über den Autor

Nach der Informatik TS arbeitete ich 3 Jahre als System Engineer bei Comline AG. Anfangs 2001 wechselte ich zu Compass Security und nahm die Tätigkeit als Security Analyst auf. Ende 2001 schloss ich ein Nachdiplomstudium in Wirtschaft ab.

Mit grosser Freude habe ich die Projekte und Arbeiten bei Compass Security erledigt. Mit vielen guten Erinnerungen nehme ich nun Abschied von Compass und deren Mitarbeitern und werde mich neuen Aufgaben zuwenden. An dieser Stelle möchte ich meinen Arbeitskollegen und den Kunden für die angenehme Zusammenarbeit danken.

Compass Security AG

Wir sind ein Schweizer Unternehmen aus Rapperswil SG und führen professionelle IT Sicherheitsüberprüfungen durch. Mit Whitehat oder Blackhat Approach untersuchen wir IT-Infrastrukturen und Webapplikationen der Kunden. Sei es im Rahmen eines Produkte Sign-off, oder in regelmässigen Abständen - Compass ist Ihr Partner für die Identifikation von Schwachstellen und Sicherheitslücken. Nationale und internationale Unternehmen im In- und Ausland vertrauen auf unsere Kompetenz, wenn es um die Beurteilung von IT-Risiken geht.

Wir verbessern die eingesetzten Assessment Methoden ständig. Schwerpunkt wird auch auf die Schulung gelegt. Aus diesem Grund bieten wir regelmässig Kurse an. Dieses Jahr haben wie den Evidence Lab Kurs in das Programm aufgenommen. Dabei wird auf die praktische Spurensuche in Computer Systemen eingegangen.

Weiteres siehe: http://www.csnc.ch

11. Februar 2005, V1.0