COMPUTERWOCHE

Die Tricks der Kriminellen

Modernes WLAN-Hacking

Datum: 09.09.2012
Autor(en): Sven Blumenstein
URL: http://www.computerwoche.de/2521564

Funknetze sind angesagt. Kein Smartphone, Tablet, Notebook oder PC wird mehr ohne Wireless-LAN-Schnittstelle ausgeliefert. Auch immer mehr IT-abseitige Alltagsgeräte offerieren einen drahtlosen Netzwerkanschluss. Die Sicherheitsrisiken werden dadurch alles andere als geringer.

In den ersten Jahren nach der Einführung des **WLAN-Standards 802.11**[1] im Jahre 1997 fristete die WLAN-Technik ein eher bescheidenes Dasein im Umfeld der Endanwender. Meistens wurde WLAN in der Industrie eingesetzt um zum Beispiel Systeme zu vernetzen, bei denen eine Verkabelung zu aufwändig oder umständlich war. Die Verbreitung unter den Endanwendern nahm mit der Einführung von schnelleren Breitbandinternetzugängen und der vermehrten Nutzung von Notebooks im privaten Bereich stark zu. Einen Aufschwung erlebte die WLAN-Technik dann im Jahre 2007, als Apple mit der Einführung des ersten iPhones den Boom der Smartphones begründete, der noch bis heute andauert.

Im Markt der mobilen Endgeräte versammelt sich eine Vielzahl von Smartphones, Notebooks, eBook-Readern und Tablets, die in der Regel alle über eine WLAN-Schnittstelle verfügen, damit sich Daten schnell und kabellos übertragen lassen. Bei vielen dieser Endgeräte ist WLAN mittlerweile sogar die exklusive Schnittstelle für einen Netzwerk- und Internetzugang.

Wer das Nokia N900 ein wenig "tunt", kann viel Unsinn damit anstellen...
Foto: cirosec GmbH / Sven Blumenstein

Angetrieben durch die rasche Verbreitung des WLAN-Standards, stand für die Industrie außer Frage, auch andere klassische Elektronik wie Drucker, Fernseher oder Spielekonsolen über WLAN zu vernetzen. Und der Trend geht immer weiter. So gibt es bereits erste Hersteller, die Waschmaschinen, Kühlschränke oder Kaffeemaschinen mit WLAN aufrüsten. In Kombination mit den allgegenwärtigen Smartphone-Apps kann der

Endanwender nun bequem vom Sofa aus den Brühvorgang starten, die Restlaufzeit der Waschmaschine kontrollieren oder das TV-Programm umschalten. Ein Trend, der sich weiter fortführen wird, da die Mehrheit der Endanwender den praktischen Nutzen zu schätzen weiß. Auch im Bereich der Automobilindustrie erfährt das Thema WLAN steigende Beachtung. So wurde erst kürzlich im Rahmen des **"Drive C2X"-Projektes**[2] eine Testphase im Frankfurter Raum gestartet, bei der Autos über WLAN miteinander kommunizieren, um zum Beispiel Verkehrsdaten auszutauschen.

Neue Gefahren

Mit solchen Antennen lassen sich WLANs auch über große Distanzen scannen.
Foto: cirosec GmbH / Sven Blumenstein

Die neue Fülle an mobilen Endgeräten, die nun alle kabellos kommunizieren können, stellt sich schnell die Frage nach der Daten- und Übertragungssicherheit. Einer der größten Nachteile eines WLANs ist es schließlich, dass es nicht über den physikalischen Schutz einer Kabelverbindung verfügt. Ein Funknetz strahlt in der Regel deutlich über die Hauswand oder den Gartenzaun hinaus. Dies eröffnet potenziellen Angreifern viele Möglichkeiten, in sicherer Entfernung zum Ausgangspunkt des WLANs Funkübertragungen auszuspionieren. Bestimmte Angriffsarten sind mit entsprechenden Antennen zudem auf sehr große Distanzen von mehreren hundert Metern bis sogar Kilometern möglich, so dass es quasi unmöglich ist, den Angreifer zu entdecken.

Für "Interessierte" gibt es Stab- und Richtfunkantennen in allen Größen. Unser Bild im vorangegangenen Absatz zeigt von unten nach oben:

- PCMCIA Karte mit integrierter Antenne, Reichweite bis 50 Meter (360 Grad Abstrahlwinkel)
- 5 dBi Stab-Antenne, Reichweite bis 100 Meter (360 Grad Abstrahlwinkel)
- 9 dBi Stab-Antenne, Reichweite bis 200 Meter (360 Grad Abstrahlwinkel)
- 6 dBi Richtfunk-Antenne, Reichweite bis 350 Meter (45 Grad Abstrahlwinkel)
- 20 dBi Richtfunk-Antenne, Reichweite bis 3000 Meter (25 Grad Abstrahlwinkel)

Der Feind in der Waschmaschine

Eine weitere Gefahr ergibt sich durch die Ausstattung bisher autarker Endgeräte mit WLAN-Technik. So wird nun nicht nur der Laptop oder das Smartphone angreifbar, sondern auch der Fernseher, die Waschmaschine oder das Auto. Viele Endanwender sind sich den drohenden Gefahren nicht bewusst: Forschern des "Centers for Automotive Embedded Systems Security" (CAESS) ist es beispielsweise gelungen, per WLAN **Zugriff auf die Fahrzeugelektronik zu erlangen**[3]. Das ermöglichte ihnen nicht nur, die Türen zu öffnen oder die Wegfahrsperre zu entfernen, sondern auch die Fahrzeugbremsen zu deaktivieren.

Die Angreifbarkeit bisher sicherer Endgeräte stellt also nicht nur eine Gefahr für die Integrität von Daten oder die Verfügbarkeit dieser Geräte dar, sondern kann unter Umständen auch eine Gefahr für Leib und Leben bedeuten.

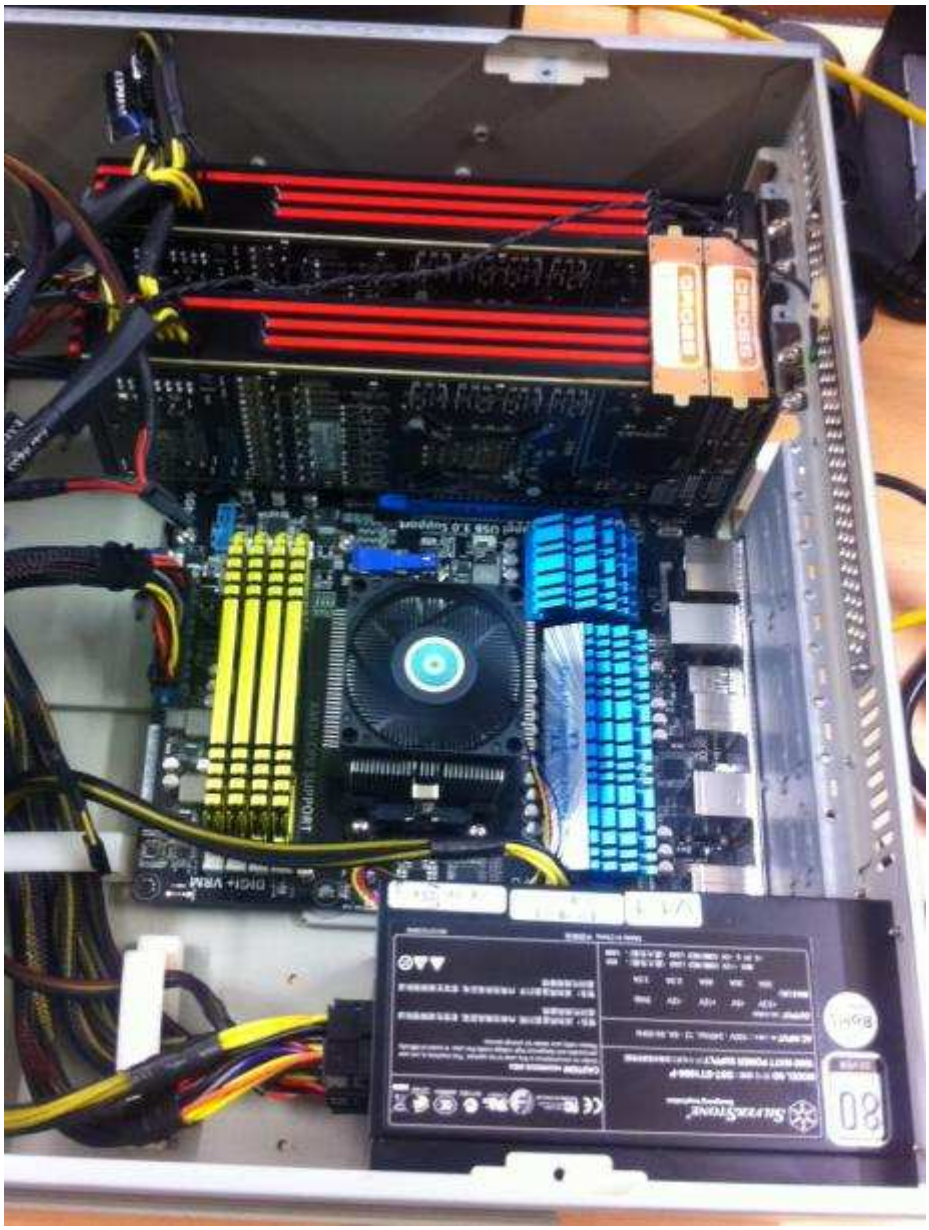
Unsichtbare Sicherheit

Die Frage, die sich zwangsläufig stellt, ist die: "Wie sichert man etwas, das man nicht sieht?" Diese Problematik ist im Bereich der Absicherung von kabellosen Netzwerken allgegenwärtig. Im Rahmen von zahlreichen WLAN-Sicherheitsüberprüfungen der cirosec GmbH aus Heilbronn zeigten sich große Defizite bei der Absicherung von WLANs in Unternehmen. So wurde in vielen Fällen der bereits erwähnte Nachteil der weitläufigen Abstrahlung von WLANs unterschätzt, durch die ein Angreifer auch von außerhalb der Unternehmensgrenze agieren kann. Des Weiteren zeigten sich deutliche Mängel bei den über WLAN bereitgestellten Endanwendungen. So war es beispielsweise **im Rahmen der Sicherheitsüberprüfung eines Hotels möglich,**[4] über das öffentliche Hotel-WLAN auf die persönlichen Daten aller Hotelgäste zuzugreifen, sowie unverschlüsselt übertragene Kreditkartendaten mitzulesen.

WEP, WPA, WPA2 - und was jetzt?

Doch welche Sicherheitsfunktionen stehen zur Verfügung? Im Laufe der Jahre wurde der Standard 802.11 um mehrere Verschlüsselungstechniken erweitert, welche die Integrität der Daten gewährleisten und Angreifer aussperren sollten. Die 1997 mit der Verabschiedung von 802.11 eingeführte Verschlüsselung "Wired Equivalent Privacy" (WEP) wurde 2001 für "gebrochen" erklärt. Während die ersten erfolgreichen Angriffe damals noch einen enormen Zeitaufwand erforderten, wurden die Angriffstechniken auf WEP derart weiterentwickelt, dass ein Angriff heutzutage keine Frage der Zeit mehr ist. Eine WEP-Verschlüsselung lässt sich inzwischen innerhalb weniger Minuten, oft sogar Sekunden knacken. Der 2003 eingeführte Nachfolger von WEP namens "Wi-Fi Protected Access" (WPA) wurde bereits ein Jahr später (2004) das erste Mal erfolgreich angegriffen. Ebenfalls 2004 wurde WPA2 eingeführt, was sich bis heute als relativ sicher darstellt. Relativ deshalb, da es auch hier Angriffstechniken gibt, die aber im Gegensatz zu WEP und WPA nicht auf Schwachstellen in der Implementierung der Verschlüsselung beruhen.

So ist das schwächste Glied in der Sicherheit von WPA2 bis heute das für die Verschlüsselung verwendete Passwort. In der Regel wird bei WPA2 von einem "Passphrase" ("Passwortsatz") gesprochen, um zum Ausdruck zu bringen, dass ein einzelnes Wort keine ausreichende Sicherheit bietet. Dennoch verwenden viele Endanwender trotzdem leicht zu merkende Passwörter. Der Grund dafür liegt nicht nur in der noch oft verbreitenden Sorglosigkeit, sondern teilweise in der mangelnden Usability von mobilen Endgeräten wie Smartphones, Tablets und eBook-Readern. Denn auf einer Touchscreen-Tastatur lässt sich das Passwort "meinwlan123" natürlich deutlich einfacher eintippen als Beispielsweise "m3!N?{wL4N}*123$%". Dieser Umstand erleichtert es einem Angreifer, verschiedene Attacken auf WPA2-geschützte WLANs vorzunehmen.



GPU Password Cracking: Mit leistungsstarken Grafikkarten lassen sich Bruteforce-Attacken in sehr kurzer Zeit erfolgreich bewerkstelligen.
Foto: cirosec GmbH / Sven Blumenstein

Der gängigste Angriffsvektor sind die "Brute-Force"- oder "Dictionary"-Attacken. Während bei ersterem alle Kombinationen eines definierten Zeichensatzes ausprobiert werden, geht es bei letzterem um die "Abarbeitung" einer Liste mit gängigen Passwörtern. Diese Art des Passwort-Knackens hat sich in jüngster Zeit deutlich weiterentwickelt. Während früher die entsprechenden Berechnungen noch auf einzelnen Systemen liefen, kann heutzutage auf Mehrkern-Systeme, verteiltes Rechnen über mehrere Systeme hinweg oder auf sogenanntes "GPU Password Cracking" zurückgegriffen werden. Zumeist benutzen die Angreifer den Grafikprozessor (GPU, Graphical Processing Unit) einer Grafikkarte für die mathematischen Berechnungen. Die erzielte Geschwindigkeit liegt hier deutlich über der durch die reine Verwendung klassischer Prozessoren (CPU) erreichten.

WPS - ein Schlag ins Wasser

Ein sicheres Passwort allein reicht aber nicht aus, wie die jüngste Weiterentwicklung des WPA2-Standards zeigt: Der Nachteil, komplexe WPA2-Schlüssel auf mobilen Endgeräten manuell eintippen zu müssen, führte zur Entwicklung des sogenannten WPS ("Wi-Fi Protected Setup"). Hierbei wurden mehrere Methoden implementiert, um einen WPA2-Schlüssel auf ein mobiles Endgerät zu übertragen, ohne dass der Endanwender diesen eintippen muss. Eine Methode ist die "PIN-Methode", bei der eine numerische PIN auf dem Endgerät eingegeben wird. Anschließend transferiert der Access Point den WPA2-Schlüssel zum Endgerät, dieses trägt ihn automatisch in der WLAN Konfiguration ein. Diese Methode führte Ende 2011 zur **Entdeckung einer massiven Sicherheitslücke**[5], da es mit nur wenigen Tausend Versuchen möglich war, Zugriff auf jedes WPA2-Netzwerk mit aktiviertem WPS und PIN-Methode **zu erlangen**[6]. Hier wurde also ein eigentlich sicherer Standard zu Gunsten des Komforts unsicher gemacht.

[Hinweis auf Bildergalerie:] gal1

Luftlöcher hacken

Will ein Angreifer in ein WLAN einbrechen, ist die Vorgehensweise vergleichbar zu dem klassischen Einbruch in ein Gebäude. Nachdem das Ziel ausgewählt wurde, wird es eine Zeit lang beobachtet, bevor der eigentliche Einbruch vonstatten geht. Der größte Unterschied zwischen dem klassischen und dem digitalen Einbruch besteht in den verwendeten Werkzeugen. Anstatt Brecheisen und Bohrmaschine kommen bei Angriffen auf WLANs Software-Werkzeuge wie die Aircrack-NG Suite, Kismet oder MDK3 zum Einsatz.

Mit den richtigen Tools lässt sich jedes WLAN aufspüren und auslesen. Hier eine Eigenbaukonstruktion aus 2-Watt-Alfa-Antenne (in Deutschland sind im praktischen Einsatz maximal 100 Milliwatt erlaubt), verbunden mit einem Nokia N900.
Foto: cirosec GmbH / Sven Blumenstein

Der Ablauf eines solchen Angriffs folgt dabei oft demselben Schema: Zuerst wird der Datenverkehr des als Ziel ausgewählten WLANs mitgelesen ("sniffing"). Dabei unterstützen Designschwächen im 802.11 Standard den Angreifer deutlich, da die Steuerpakete die von WLAN-Geräten ausgesendet werden - sogenannte Beacon-Frames und Probe-Requests - unabhängig von der verwendeten Verschlüsselung immer unverschlüsselt übertragen werden. Neben der verwendeten Verschlüsselungstechnik und dem Namen des Netzwerkes (SSID, Service Set Identifier) enthalten diese Steuerpakete noch eine Vielzahl weiterer Informationen über das gesuchte oder angebotene WLAN. Ein Angreifer kann also sehr leicht erkennen, welche Netzwerke in seiner Umgebung existieren und welche Endgeräte sich zu welchem Netzwerk verbinden wollen. Dadurch sind gezielte Angriffe möglich. Neben dem eigentlichen Cracken des verwendeten Passwortes für die Verschlüsselung sind auch Angriffe möglich, die das WLAN einfach nur stören oder blockieren. Dabei können entweder Endgeräte von den Access Points getrennt werden ("Deauthentication/Disassociation Attack"), oder Access Points durch eine Vielzahl von Anfragen überlastet werden ("Authentication DoS"). Da diese Angriffe die Designschwächen des Protokolls ausnutzen, hilft dagegen auch keine eingesetzte Verschlüsselung.

Hacker's Paradise

Wurde ein mobiles Endgerät einmal mit einem WLAN verbunden, sucht dieses Gerät auch Tage später permanent mit den bereits erwähnten Probe-Requests nach dem entsprechenden WLAN. Das Werkzeug Airbase-NG aus der Aircrack-NG Suite bietet die Möglichkeit, auf solche Probe-Requests zu antworten und automatisch die passenden Beacon-Frames mit dem gesuchten Netzwerknamen zu erzeugen. Dadurch wird das gesuchte Netzwerk aus Sicht des Endgerätes verfügbar. Versucht das Endgerät, sich anschließend zu diesem gefälschtem Netzwerk zu verbinden, zeichnet Airbase-NG den Verbindungsversuch auf ("Handshake"). Wurde ein WPA2-geschütztes WLAN emuliert, reichen die aufgezeichneten Informationen, um die bereits beschriebenen Angriffe auf den WPA2-Schlüssel vorzunehmen *(siehe auch Code-Appendix auf der folgenden Seite)*.

Auch dieser gebräuchliche Linksys-

Router WRT54 lässt sich zu einem praktischen Hacking-Werkzeug "umrüsten".
Foto: cirosec GmbH / Sven Blumenstein

Schützt ein Unternehmen sein WLAN mit einer Verschlüsselung, muss ein Angreifer also nicht in der Nähe des Netzwerkes sein, um die Verschlüsselung anzugreifen. Jeder Mitarbeiter trägt die notwendigen Informationen dafür durch die mobilen Endgeräte schließlich mit sich herum. Sei es nun daheim, in der Freizeit, am Flughafen, in Hotels oder an anderen Orten, an denen sich der Mitarbeiter mit im Unternehmen genutzten Endgeräten aufhält.

Empfehlungen

Wie lassen sich WLANs wirklich gegen Angreifer schützen? Eines vorweg: Aufgrund der angesprochenen Designschwächen im Protokoll kann es keine vollständige Sicherheit geben - zumindest was die Verfügbarkeit eines WLANs angeht. Jeder WLAN-Betreiber sollte sich im Klaren darüber sein, dass ein Angreifer das Funknetz jederzeit lahm legen könnte. Die Vernetzung von geschäftskritischen Systemen per WLAN sollte deshalb gründlich durchdacht sein. Bei den verwendeten Verschlüsselungsverfahren ist eine Lösung auf Basis von 802.1X und Zertifikaten dem klassischen WPA2 mit einem Passwort vorzuziehen. Ist dies aufgrund der verwendeten Endgeräte oder anderen Gründen nicht möglich, sollte das verwendete Passwort den gängigen Passwortrichtlinien entsprechen, um Brute-Force- oder Dictionary-Angriffe zu erschweren.

Derzeit wird bei Generierung von WPA2-Passwörtern eine Länge von mindestens 14 Zeichen unter Verwendung von Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen empfohlen. In jedem Fall sollte darauf geachtet werden, dass die Unterstützung für WPS deaktiviert ist. Des Weiteren sind sprechende SSIDs wie beispielsweise "WLAN-FirmaXYZ" tabu, da dies einem Angreifer nicht nur die Auswahl des anzugreifenden WLANs erleichtert, sondern auch dafür sorgt, dass sich die Endgeräte permanent als Client dieses Netzwerkes zu erkennen geben. Das könnte auch zum gezielten Diebstahl eines solchen Gerätes, zum Beispiel in einem Restaurant oder Zug führen (Stichwort **Wirtschaftsspionage**[7]). Falls technisch möglich, wird empfohlen, die automatische Netzwerksuche und die automatische Verbindung zu WLANs auf den Endgeräten zu unterbinden - das verhindert das Senden von Probe-Requests. Noch besser ist es natürlich, die WLAN-Schnittstelle nur bei Bedarf zu aktivieren.

Eine weitere Schutzmöglichkeit für die Integrität der übertragenen Daten wäre die Verwendung einer zusätzlichen Verschlüsselungsebene wie beispielsweise ein **VPN mit IPSec**[8]. Um bestimmte Angriffe zu erkennen und teilweise auch zu verhindern, bieten einige Hersteller so genannte "RF Monitoring Systeme" an. Erkennt ein solches System Angriffe auf das WLAN, schlägt es Alarm und leitet auf Wunsch Gegenmaßnahmen ein. Das kann neben dem gezielten Blockieren von bestimmten Verbindungen oder Access Points auch die Lokalisierung von Endgeräten über Triangulation sein.

Fazit

WLANs sind vor allem aufgrund des Booms mobiler Endgeräte präsenter denn je. Die Verbreitung steigt stetig

und auch die Netzbetreiber beginnen vermehrt, den steigenden mobilen Datentransfer in WLAN-Hotspots auszulagern. Viele Firmen, die jahrelang ohne WLAN ausgekommen sind, werden durch die steigende Verbreitung mobiler Arbeitsgeräte zum Aufbau eines Funknetzwerkes gezwungen. Geräte, die bisher keine WLAN-Schnittstellen hatten, werden nun entsprechend angreifbar. Betrachtet man die Entwicklung der Endgeräte im Vergleich mit der Entwicklung der Sicherheitsfunktionen in 802.11, zeigen sich deutliche Defizite in den Sicherheitsstandards. Während Angriffe durch neue Techniken immer effizienter werden, hat sich in den letzten Jahren in Bezug auf die Sicherheitsfunktionen nur sehr wenig getan. Unternehmen und Endanwender sollten also kritisch bewerten ob und in welchem Umfang sie WLANs tatsächlich brauchen und die Verwendung unter Umsetzung möglichst vieler der beschriebenen Sicherheitsmaßnahmen abwägen. (sh)

Beispielhafte Probe-Requests

Wir zeigen eine Beispiel-Ausgabe eines Angriffs auf Endgeräte mit Airbase-NG durch die Emulation gesuchter WLANs. In der Ausgabe sind die verschiedenen Probe-Requests von zwei Clients zu sehen. Die hervorgehobenen Zeilen zeigen Aufzeichnungen von WPA2-Handshakes, die für Angriffe auf den WPA2-Schlüssel verwendet werden können.

```
# airbase-ng -vv -c 8 -Z 4 -W 1 -F capture mon0

16:36:30 Created tap interface at0

16:36:30 Trying to set MTU on at0 to 1500

16:36:30 Access Point with BSSID 00:C0:CA:4F:FF:FF started.

16:36:32 Got directed probe request from 10:0B:A9:76:FF:FF - "Kloster Hotel"

16:36:35 Got directed probe request from 10:0B:A9:50:FF:FF - "AndroidTether"

16:36:41 Got directed probe request from 10:0B:A9:76:FF:FF - "katze"

16:36:42 Got directed probe request from 10:0B:A9:76:FF:FF - "cirobank"

16:36:42 Got directed probe request from 10:0B:A9:76:FF:FF - "lachsfisch"
```

16:36:42 Got an auth request from 10:0B:A9:76:FF:FF (open system)

16:36:42 Client 10:0B:A9:76:FF:FF associated (WPA2;CCMP) to ESSID: "lachsfisch"

```
16:36:51 Got directed probe request from DC:2B:61:B3:FF:DD - "cirobank"
```

```
16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "Familie Schmidt"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "RUB-WLAN"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "Boingo Hotspot"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "WLAN FirmaXYZ"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "3A1"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "RUB-WLAN"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "2e2training"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "Hotelinternet"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "maxspot (FREE)"

16:36:52 Got directed probe request from DC:2B:61:B3:FF:DD - "evil"
```

16:36:57 Got an auth request from DC:2B:61:B3:FF:DD (open system)

16:36:57 Client DC:2B:61:B3:FF:DD associated (WPA2;CCMP) to ESSID: "evil"

Links im Artikel:

[1] **http://de.wikipedia.org/wiki/IEEE_802.11**
[2] **http://www.drive-c2x.eu/frankfurt-facts**
[3] **http://www.autosec.org/publications.html**
[4] **https://www.cirosec.de/deutsch/aktuelles/pressemeldungen/pressemeldung/2011/07/13/gravierende-datenschutzmaengel-in-zahlreichen-hotels.html**
[5] **http://www.computerwoche.de/security/2502803/**
[6] **http://www.kb.cert.org/vuls/id/723755**
[7] **http://www.computerwoche.de/security/2500724/**
[8] **http://www.computerwoche.de/security/2356264/index2.html**

Bildergalerien im Artikel: