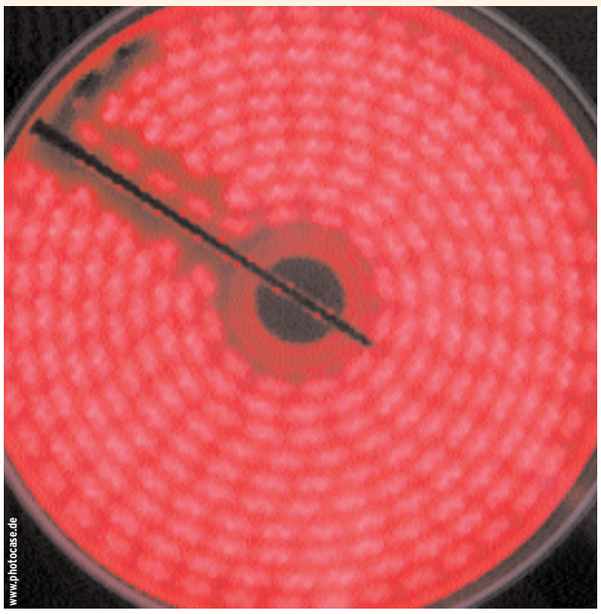
Angriffe auf Wireless-Clients

# Heiße Flecken

Sicherheitsexperten kümmern sich vor allem um die Access Points von WLANs, aber auch der Client bietet Angreifern offene Flanken. Vor allem an öffentlichen Hotspots ist es ganz leicht, Verbindungen automatisch zu übernehmen, wie das Tool Hotspotter zeigt. Max Moser




**Dank moderner,** aufwändiger Schutzmechanismen erscheinen die kabellosen Netzwerke zunehmend als sicher. Authentisierungskonstrukte rund um das EAP-Framework (Extensible Authentication Protocol, **[1]**) versprechen unerwünschte Besucher abzuwimmeln. Das Temporal Key Integrity Protocol (TKIP) **[2]** mit seinen rasch wechselnden WEP-Schlüssel verhindert Replay-Attacken und ein allzu einfaches Brechen der Verschlüsselung. Zudem werden die Keys immer länger.

Mit WPA/WPA2 **[3]** und dem Wechsel zur AES-Verschlüsselung **[4]** scheint also die Sicherheit für die Firmennetze nahezu perfekt zu sein. Als abrundendes Feature bekommen die Access Points V-LAN-Unterstützung, Intrusion-Detection- und Firewall-Systeme spendiert – für meist sehr viel Geld.

Doch die Gefahren lauern auch weit weg vom Firmennetz. Im heutigen, mobilen Zeitalter möchten viele unterwegs arbeiten. Dank der wachsenden Verbreitung von Wireless-Netzwerken und guten Administratoren ist dies heute an sehr vielen Stellen komfortabel möglich: beim Warten auf den Flieger, Im Hotel, im Sitzungszimmer. Der ungebremsten Arbeitswut sind nahezu keine Grenzen mehr gesetzt.

Um die Welt jettende Manager empfinden diese flexible Arbeitsweise als sehr angenehm und lassen sie häufig auch im eigenen Betrieb realisieren. Oft müssen die IT-Abteilungen enormen Sicherungsaufwand betreiben, da viele sensitive Daten übers Netzwerk wandern. Zudem dürfen in der Regel nur privilegierte Personen die firmeninternen Wireless Services offiziell nutzen.

## Manager auf Reisen

Ein typischer Manager, der mit einem WLAN-fähigen Laptop durchs Land reist, hat also mindestens zwei Wireless-Konfigurationen, so genannte Profile, aktiviert. Eins für die Arbeiten am öffentlichen Hotspot, also im Flughafen und Hotel, und eins für den gesicherten Zugang ins geschützte Firmennetzwerk. Im Internet gibt es verschiedene Datenbanken, in denen der nächste Hotspot zu finden ist [5], [6], [7].

Ein kabelloses Netzwerk besteht aus mehreren Komponenten, für die Verständigung untereinander gibt es verschiedenen Arten von Kommunikationspaketen, zum Beispiel Daten, Kontroll- und Management-Pakete. Hier sind vor allem jene fürs Management interessant, die für die Bekanntmachung von Netzwerken und die An- und Abmeldung sowie das Powermanagement eingesetzt werden (siehe Kasten „Wichtige Management-Pakete“).

## Klartext reden

Sämtliche Management-Pakete innerhalb eines Wireless-Netzwerks werden im Klartext übertragen. Als ob dies nicht schon schlimm genug wäre, erfolgt auch nahezu keine Integritätsprüfung oder eine Sender- und Empfängervalidierung. Ein zweiter Access Point kann die Probe-Request-Pakete eines Clients mit Probe-Responses beantworten und den Client

### Wichtige Management-Pakete

**Beacons:** Werden vom Access Point verschickt, für Timing-Zwecke und zur Verteilung der Netzwerkparameter.

**Probe-Request:** Damit sucht der Client nach verfügbaren Netzwerken, sie enthalten Parameter wie SSID und Frequenz.

**Probe-Response:** Antwort des Access Points auf Probe-Response-Pakete für die Bestätigung oder Verweigerung des weiteren Verlaufs.

**Association Request:** Client gibt bekannt, dass er sich mit einem bestimmten Netzwerk verbinden möchte.

**Association Response:** Der Access Point antwortet, ob einer Verbindung zugestimmt wird oder nicht.

**Disassociation:** Der Access Point weist Client(s) dazu an, die bestehende Verbindung aufzulösen.

**Authentication:** Der Client authentisiert sich für die Netzwerkverbindung.

**Deauthentication:** Der Access Point erzwingt die Aufhebung der Authentisierung.

**Monitor Mode**

**Der Monitor Mode oder auch RFMON Mode genannt, ist ein spezieller Modus, in dem eine Wireless-Karten-Firmware alle empfangenen Pakete an die Treibersoftware weitergibt und nicht nur die Pakete, die für diese Station bestimmt sind – vergleichbar mit Radiohören auf allen Kanälen gleichzeitig.**

dazu auffordern, sich mit ihm zu verbinden. Ein Probe-Response-Paket, wie in Abbildung 2 zu sehen, besteht aus mehreren verschiedenen Teilen. Die wichtigsten sind:

- »Framecontrol (FC)« beinhaltet den Pakettyp (für Management-Pakete »0«) sowie den Subtyp (»5« für Probe-Response) und zusätzlich Flags, die bei einem Probe-Response stets den Wert 0 haben.
- »Destination address« ist die MAC-Adresse des Clients.
- »Source address« ist die MAC-Adresse des Access Points.
- »BSS Id« ist die MAC-Adresse des Access Points.
- »Fixed parameters« enthalten einen Zeitstempel sowie einige Informationen über die Fähigkeiten des Netzwerks.
- »Tagged parameters« beinhalten die SSID, deren Länge sowie den Channel und die unterstützten Übertragungsgeschwindigkeiten.

Hier drängt sich die Frage auf, woran der Benutzer überhaupt erkennt, dass er sich mit einem vertrauenswürdigen, bewusst gewählten Netz verbunden hat und nicht mit einem Netzwerk, das ein Angreifer kontrolliert? Eigentlich kann er dies nicht – und genau darin besteht die Sicherheitslücke.

Bei näherer Betrachtung lässt sich feststellen, dass die folgenden Informationen über ein Netz öffentlich zur Verfügung stehen:

- Logischer Netzwerkname (SSID)
- MAC-Adresse des Access Points
- Konfiguration des Access Points

Die SSID, also den logischen Namen des jeweiligen Netzwerks, kann jeder Access Point benutzen, da dieser Bezeichner frei wählbar ist, keiner Validierung bedarf und auch durchaus doppelt vorhanden sein kann.

Die in jedem Paket enthaltende MAC-Adresse des Access Points kann sich bei Verwendung eines Software-Access-Points ebenfalls duplizieren. Ein doppeltes Vorkommen wird, anders als beim konventionellen Kabelnetzwerk, meist keine Folgen haben. Ein Access Point unterscheidet ohne besondere Vorkehrungen nicht, ob ein versendetes Paket von ihm selbst kommt oder nicht.

Es gibt mittlerweile auf einigen Geräten proprietäre Intrusion-Detection-System-Module, die Paketeinspeisungen erkennen sollen. Eine wirkliche Entschärfung des Problems würde aber nur eine Sender-Empfänger-Validierung bringen, wie sie das Open-Source-Projekt Wlsec [11] implementiert. Leider findet dieses Projekt bisher in der kommerziellen Welt wenig Anklang.

## Keine Authentifizierung

Lediglich die Konfiguration der Authentisierung und der Verschlüsselung kann ein anderer Access Point nicht ohne weiteres nachahmen, da diese Informationen nicht öffentlich auslesbar sind. Die Konfigurationsparameter sind jedoch bei Hotspots im Gegensatz zu anderen Access Points vorhersehbar: Beide Schutzmaßnahmen sind ausgeschaltet, da ein Hotspot nur selten authentisiert, geschweige denn verschlüsselt Daten transportiert. Das wäre viel zu umständlich für die Kundschaft.

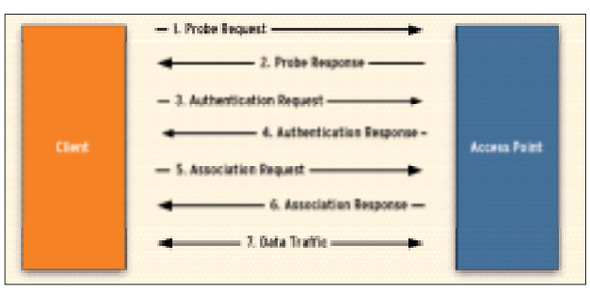



**Abbildung 1: Die Phasen einer Anmeldung am Access Point. Angriffstools nutzen schon die Suche des Clients nach verfügbaren Netzen in Schritt 1 und 2 aus.**

Diese Tatsache erlaubt es dem Angreifer, einem Wireless-Client vorzugaukeln, er habe sich mit einem Netzwerk verbunden, das sein Ver-

trauen verdient, obwohl er sich auf dem Netzwerk eines Angreifers befindet. Mit dem Einsatz von mehreren Wireless-Karten ist sogar ein Man-in-the-middle-Szenario möglich, in dem der gefälschte Access Point die Daten des Clients entführt, auswertet und dann an den richtigen Empfänger weiterleitet.

Dieses Verfahren wurde erstmals mit Airjack **[8]** demonstriert. Die Shmoo Group, durch die Software Airsnort bekannt geworden, erkannte die Problematik ebenfalls und entwickelte das Tool Airsnarf **[9]**, das einen Software-Access-Point mit einer gefälschten Web-Loginseite generiert.

Will sich der Client nicht freiwillig von einer schon bestehenden Verbindung trennen, kann das Tool Void11 Deauthentication-Pakete generieren und damit den Client zwingen, erneut Netze zu suchen.

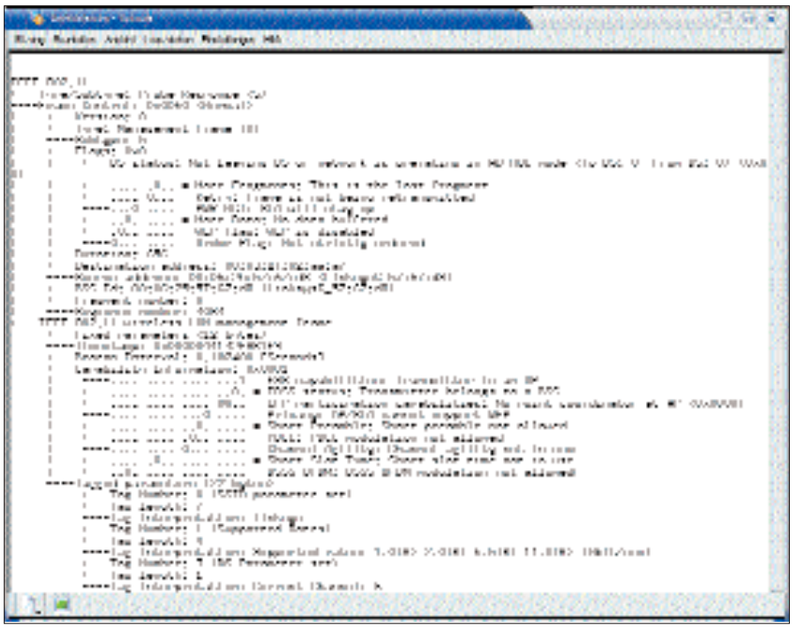


**Abbildung 2: Tools wie Ethereal stellen die Struktur von IEEE802-Paketen übersichtlich dar. Hier ein Probe-Response-Paket, wie es bei dem beschriebenen Angriff Verwendung fand.**

## Hotspotter

Bei Airsnarf ist jedoch eine Automatisierung des Vorgangs nur bedingt möglich, die Netzwerkparameter, zum Beispiel die SSID, müssen schon bekannt sein. Das Tool Hotspotter **[10]** des Autors funktioniert ähnlich wie Airsnarf, reagiert aber selbstständig auf Clients, die nach ungeschützten Netzwerken suchen. Das Programm arbeitet mit jeder Karte zusammen, die mit »iwconfig mode monitor« und mit »iwconfig mode master« angesteuert werden kann, Empfehlenswert sind hier Karten mit dem Prism2-Chipsatz, auch Atheros-basierte Karten funktionierten im Test.

Hotspotter setzt zuerst die Wireless-Karte in den so genannten RFMON oder auch Monitor Mode genannten Modus (siehe Kasten „Monitor Mode“). In diesem Zustand erhält das Programm sämtliche Pakete, die im Empfangsbereich sind, und wertet die Pakete vom Typ Probe-Request weiter aus. Probe-Request-Pakete beinhalten die Informationen, die nötig sind um herauszufinden, nach welchem Netzwerk ein Client gerade sucht (siehe Kasten „Wichtige Management-Pakete“).

Die Suche realisiert der Client durch das Versenden von Probe-Request-Paketen mit dem SSID-Parameter des zu suchenden Netzwerks. Vereinfacht gesagt ruft der Beispiel-Client: Hallo, ist hier das netz »ein_hotspot_betreiber« oder das Netzwerk »mein_sicheres_firmennetz«? Ist eines der Fall, antwortet der Access Point und die Verbindung wird aufgebaut, und zwar mit den in den Profilen des Clients definierten Settings.

Verliert ein Client die Netzwerkverbindung, dann sucht er erneut. Je nach Betriebssystem und Voreinstellungen sucht er entweder automatisch in regelmäßigen Abständen nach den in Profilen vordefinierten Netzwerken oder nur auf Geheiß des Benutzers.

Findet ein Client das gesuchte Netzwerk nicht, sucht er meist automatisch nach dem nächsten in den Profilen definierten Netzwerknamen. Ein Angreifer kann auf diese Weise herausfinden, welcher Client welche Profile definiert hat.

Hotspotter erhält die Bezeichnung des gesuchten Netzwerks und vergleicht sie mit einer Liste von Access Points, die als Hotspots bereits bekannt sind und unchiffriert betrieben werden. Falls eine Übereinstimmung gefunden ist, beendet Hotspotter den Monitor-Modus der Karte und konfiguriert sie automatisch als Software-Access-Point für das gesuchte Netzwerk (siehe Abbildung 3). Das bedeutet vereinfacht gesagt, dass Hotspotter dem Client antwortet: Ja! Hier ist das Netz »ein_hotspot_betreiber«, verbinde dich mit mir.

Der Aufforderung folgt der Client meist allzu gern – damit hat der Angreifer

### Höchste Gefahr bei Windows

Damit die Administration von Clients möglichst einfach funktioniert und auch möglichst jeder Hotspot ohne Konfigurationsänderungen zu benutzen ist, wird oft ein Profil mit »Mein sicheres Netzwerk« erstellt und eins mit der Bezeichnung »ANY«. Letzteres ist ein Spezialfall und enthält alle Netzwerke, unabhängig vom Namen.

Falls ein Angreifer das sichere Netzwerk zu fälschen versucht, könnte der Client sich normalerweise nicht korrekt verbinden, da die Chiffrierungs- oder die Authentication-Settings nicht passen. Bei der beschriebenen Konstellation unter Windows ist dies aber leider nicht der Fall, da das »ANY«-Profil implizit ist. Das bedeutet, dass selbst dann, wenn nur das sichere Profil passt, auch die unsicheren Settings von »ANY« anwendbar sind, da der Netzwerkname »ANY« auf jeden Netzwerknamen passt, also auch auf »Mein sicheres Netzwerk«.

Durch geschicktes Timing beim Einsatz von Deauthentication-Paketen lassen sich auf diese Weise auch Clients unbemerkt vom bestehenden sicheren Netzwerk entführen. Es gibt kommerzielle Clientsoftware, die dieses Verhalten nicht zeigt. Hier ist der Odyssey-Client [12] zu empfehlen.

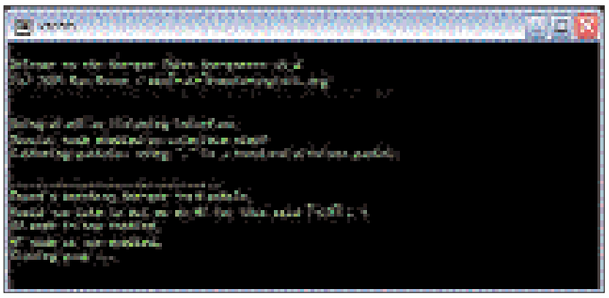


**Abbildung 3: Hotspotter in Aktion, jeder Punkt zeigt ein empfangenes Netzwerkpaket.**

die Netzwerkverbindung unter seiner Kontrolle.

## Angriff auf Knopfdruck

Erhält Hotspotter einen der Parameter »-r« oder »-e« zusammen mit dem gewünschten Bash-Skript, wird alles automatisch ausgeführt. Bei »-r« geschieht dies, bevor in den Access-Point-Modus gewechselt wird, bei »-e« erst, nachdem die Wireless-Karte des Angreifers bereits als Access Point konfiguriert ist.

Welche Aktionen das übergebene Bash-Skript ausführt, ist ganz und gar der Phantasie des Angreifers überlassen. Beispiele sind die automatische Vergabe einer IP-Adresse und die Namensauflösung an den anzugreifenden Client mittels DHCP und DNS, ein automatisches Portscannen bis hin zum automatischen Datenklau oder der kompletten Systemübernahme mit Hilfe eines neuen Exploit oder Trojaners. Ebenfalls kann der Client mit gefälschten Loginseiten konfrontiert werden.

## Fazit

Wer bedenkt, dass viele Laptops bereits eingebaute Wireless-Adapter haben und gerade jene Personen mit kritischen Daten oft wenig über die Bedienung ihrer Geräte wissen, sollte sich klar darüber sein, dass kabelloses Arbeiten in Zügen, auf Flughäfen oder Messen ein ernstes Problem sein kann: Vorbei an den teuren Sicherungsmitteln ist es durch die Hintertür leicht, Trojaner zu installieren oder Informationen zu entwenden, um später über andere Wege Zugang zum gesicherten Firmennetz zu erhalten. *(uwo)* ■

**Infos**


**[1]** EAP: [http://www.faqs.org/rfcs/rfc3871.html]

**[2]** TKIP: [http://www.cisco.com]

**[3]** WPA: [http://wwww.wi-fi.org]

**[4]** AES: [http://www.faqs.org/rfcs/rfc3565.html]

**[5]** Deutsches Hotspot-Verzeichnis: [http://gamefiles.giga.de/hotspot/liste.php]

**[6]** Schweizer Hotspot-Verzeichnis: [http://www.swisshotspots.ch]

**[7]** Internationales Hotspot-Verzeichnis: [http://mobile.yahoo.com/wifi]

**[8]** Airjack: [http://sourceforge.net/projects/airjack]

**[9]** Airsnarf: [http://airsnarf.shmoo.com]

**[10]** Hotspotter: [http://wwww.remote-exploit.org]

**[11]** WLSecProjekt: [http://wlsec.net]

**[12]** Odyssey-Client für Windows: [http://www.funk.com/radius/wlan/lan_c_radius.asp]

**[13]** Liste mit 500 SSIDs von Hotspots und unverschlüsselten Netzen auf der Heft-CD: »/opt/auditor/full/share/hot«