SelfLinux-0.13.1

WLAN unter Linux

Autor: Robin Haunschild (*H@unschild.de*)
Formatierung: Robin Haunschild (*H@unschild.de*)

Inhaltsverzeichnis

1 Einleitung

Dieses Kapitel von SelfLinux erklärt Schritt für Schritt, wie man seine Funknetzwerkschnittstelle unter Linux einrichtet. Dabei wird auch das Thema Verschlüsselung angesprochen. Lange Zeit war es ein großes Problem, seine Netzwerkkarte unter Linux zum Funken zu bewegen. Mit der Zeit werden aber immer mehr WLAN-Chips direkt vom Linux-Kernel unterstützt. Der Rest kann - zumindest auf 32-Bit-Linux-Systemen - mit dem Ndiswrapper und dem Windows-Treiber verwendet werden.

2 Treiber

Generell sollte man zwischen WLAN-Chipsätzen, für die es native Linux-Treiber gibt, und denen für die es nur Windows-Treiber gibt unterscheiden. Im letzteren Fall wird der Windows-Treiber mit dem Programm Ndiswrapper geladen. Bei den nativ von Linux unterstützten Chipsätzen ist der Treiber entweder bereits im Linux-Kernel enthalten oder man muß das Modul für den WLAN-Chipsatz selbst kompilieren und laden. Beim selbst kompilieren benötigt man die Header-Dateien des installierten Linux-Kernels. Je nach benötigtem/verwendetem Treiber unterscheiden sich die Gerätenamen für die WLAN-Verbindung. Bei Chipsätzen, die per Ndiswrapper angesteuert werden, heißt das Gerät wlanX, andere Treiber hingegen bevorzugen meist die ethX-Nomenklatur. In diesem Kapitel wird als Gerätename für das Netzwerkgerät wlan0 verwendet.

3 Die Wireless-Tools

Die wichtigsten Programme zur Konfiguration drahtloser Netzwerkkarten unter Linux sind iwconfig und iwlist. Bei Debian sind sie im Paket wireless-tools zusammen mit weiteren Programmen enthalten. Als Alternative zu den Programmen iwlist und iwconfig existieren einige grafische Anwendungen zur Konfiguration von drahtlosen Netzwerken. Jedoch versagen sie beim Einrichten mancher Funknetzwerkschnittstellen.

3.1 iwlist

Die wichtigste Verwendung von iwlist, ist das Auffinden von Hotspots (offenen Funknetzwerken) und das scannen nach dem eigenen Netzwerk. Ein Beispiel zeigt das folgende Listing:

```
# iwlist wlan0 scan
wlan0     Scan completed :
          Cell 01 - Address: 00:02:2D:39:9B:1A
                    ESSID:"<hidden>"
                    Protocol:IEEE 802.11b
                    Mode:Master
                    Channel:11
                    Encryption key:off
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
                    Quality=100/100  Signal level=-201 dBm
                    Extra: Last beacon: 172ms ago
          Cell 02 - Address: 00:15:0C:4C:13:F1
                    ESSID:"FRITZ!Box Fon WLAN 7170"
                    Protocol:IEEE 802.11bg
                    Mode:Master
                    Channel:6
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s
                              48 Mb/s; 54 Mb/s
                    Quality=100/100  Signal level=-206 dBm
```

```
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (1) : TKIP
                        Authentication Suites (1) : PSK
                    Extra: Last beacon: 204ms ago
```

Bei diesem Scan wurden zwei Funknetzwerke gefunden: Ein unverschlüsseltes mit versteckter Session-ID (Cell 01) und ein mit WPA verschlüsseltes Funknetzwerk mit sichtbarer ESSID (Cell 02). Beide Konfigurationen sollte man vermeiden. Allerdings ist das Netzwerk Cell 02 deutlich sicherer konfiguriert als das Netzwerk Cell 01.

3.2 iwconfig

Die Eingabe von iwconfig gibt für jede Netzwerkschnittstelle des Systems aus, ob sie drahtlos ist oder nicht. Wurden keine drahtlosen Schnittstellen erkannt, so könnte die Ausgabe wie folgt aussehen:

```
lo        no wireless extensions.

eth0      no wireless extensions.
```

Dabei stellt lo die loopback-Schnittstelle und eth0 das kabelgebundene Netzwerkgerät dar. Ein Beispiel für die Ausgabe, wenn eine drahtlose und eine kabelgebundene Schnittstelle vorhanden sind könnte etwa so aussehen:

```
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11b/g  ESSID:off/any  Nickname:"Broadcom 4306"
          Mode:Managed  Frequency=2.484 GHz  Access Point: Invalid
          Bit Rate=1 Mb/s   Tx-Power=15 dBm
          RTS thr:off   Fragment thr:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Die wichtigsten Schritte, um sich mit einer Funkstation ohne Verschlüsselung anzumelden sind die Folgenden:

```
root@linux /root/ # iwconfig wlan0 mode Managed
root@linux /root/ # iwconfig wlan0 essid "ESSID"
```

Der erste Befehl sorgt dafür, daß der WLAN-Chip in den verwalteten Modus versetzt wird. Alternativ kann man durch den Parameter "Ad-Hoc" ein sogenanntes "Point-to-Point"-Netzwerk zwischen zwei Funknetzwerkkarten aufbauen. Der zweite Befehl setzt die Session-ID auf den Wert ESSID. Mit der ESSID "*" kann man jedem beliebigen offenen Netzwerk beitreten.

Nach dieser Konfiguration kann man, wenn sich im Funknetzwerk ein DHCP-Server befindet (meist die Funkstation) die konfigurierte Funknetzwerkschnittstelle mit

```
root@linux /root/ # ifup wlan0
```

in Betrieb nehmen. Es wird an dieser Stelle jedoch explizit davor gewarnt, Funknetzwerke ohne Verschlüsselung zu betreiben. Dies birgt nicht nur Sicherheitsrisiken, sondern kann auch juristische Folgen nach sich ziehen. Weitere Bemerkungen dazu folgen in den Schlußbemerkungen zu diesem Kapitel.

4 Verschlüsselung

Aus den Gründen, die in den Schlußbemerkungen angesprochen werden, wird an dieser Stelle lediglich die Verschlüsselung per WPA (Wi-Fi Protected Access) besprochen.

Unter Linux ermöglichen die Zusatzprogramme xsupplicant und wpasupplicant die Möglichkeit, den Funkverkehr zu verschlüsseln. Von beiden Programmen gibt es wahrscheinlich auch Pakete Ihrer Linux-Distribution. Im Folgenden wird die Einrichtung der WPA-Verschlüsselung mit wpasupplicant beschrieben.

4.1 WPASupplicant

Nach der Installation von WPASupplicant trennen Sie nur noch die Konfiguration und das WPA-Zertifikat vom Betrieb Ihres "sicheren" Funknetzwerkes. Das WPA-Zertifikat erhält man vom Betreiber des Funknetzwerkes und sollte es im Linux-Dateisystem ablegen.

Ein Beispiel für eine Konfigurationsdatei, die ebenfalls an einer beliebigen Stelle im Dateisystem liegen kann (/etc bietet sich für Konfigurationsdateien an) zeigt das folgende Listing:

Beispiel einer WPASupplicant-Konfigurationsdatei

```
network={
        pairwise=TKIP
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=TTLS
        phase2="auth=PAP"

        # Passende ESSID
        ssid="ESSID"

        # Login Daten
        identity="username"
        password="password"

        # Pfad zum Zertifikat
        ca_cert="PFAD_ZUM_ZERTIFIKAT"
}
```

Selbstverständlich müssen die Werte von ssid, identity, password und ca_cert ersetzt werden. Ggf. verwenden Sie auch andere Authentifikationsmethoden dazu sollten Sie den Administrator des betreffenden Funknetzwerkes oder das Handbuch Ihrer Funkstation konsultieren.

Der Befehl

```
root@linux /root/ # wpa_supplicant -i wlan0 -c /etc/wpasupplicant.conf -D
ndiswrapper &
```

startet den WPASupplicant-Dienst wenn Ihre Konfigurationsdatei wpasupplicant.conf heißt und unter /etc liegt und Sie den ndiswrapper zum Betrieb Ihres WLAN-Chips nutzen. Andernfalls gilt es, auch diese Werte zu ersetzen. Verfügbare Werte für den verwendeten Linuxtreiber zeigt die folgende Tabelle.

Anschließend kann das Funknetzwerk, wenn ein DHCP-Server darin vorhanden ist, mit dem bekannten Befehl "ifup wlan0" aktiviert werden.

5 Schlußbemerkungen

Es dürfte bekannt sein, daß es wenig hilft, ein Netzwerk mit WEP (Wired Equivalent Privacy) zu verschlüsseln. Lauscht ein versierter Angreifer wenige Minuten im verschlüsselten Netzwerkverkehr ist ihm aufgrund der Schwäche des Verschlüsselungsalgorithmus von WEP der ehemals geheime Schlüssel bekannt. Allein das Verstecken der ESSID bietet auch keinen ausreichenden Schutz. Am Besten verwendet man eine WPA-Verschlüsselung und versteckt die ESSID/SSID. Ansonsten ist nicht nur die Sicherheit des eigenen Funknetzwerkes in Gefahr, sondern man hat mit juristischen Kosequenzen zu rechnen, wenn jemand über ein nicht ausreichend geschütztes Funknetzwerk illegale Aktivitäten betreibt. Der Betreiber des Funknetzwerkes ist über den Provider und die vergebene öffentliche IP-Adresse ausfindig zu machen, aber selbst bei intensivem Protokollieren des Netzwerkverkehrs ist es nahezu unmöglich den WLAN-Hacker zu lokalisieren.

Wie immer freut sich der Autor über konstruktive Kritik, gefundene Fehler, Anregungen, etc.