

Nutzung der Wireless-LAN-Umgebung in der Hochschule mit Linux



Braunschweig University of Art
Hochschule für Bildende Künste Braunschweig

ZKI
Zentrale Einrichtung für Kommunikationstechnik &
Informationsverarbeitung

Autor: Sebastian Fromhage
Datum: 18.10.2005

Nutzung der Wireless-LAN-Umgebung in der Hochschule mit Linux

Das Funknetz der HBK ist in die Netzwerk-Infrastruktur integriert.

Informationen für den WLAN Zugang unter Linux.

Für Linux gibt es zwei Programme, mit deren Hilfe Sie sich Zugang zu dem 802.1x WLAN der FH verschaffen können:

- Xsupplicant
- wpa-supplicant

Beide unterstützen verschiedene IEEE802.1X-Methoden und unterschiedliche Netzwerkkarten. Die Methode EAP – TTLS (PAP) die im HBK-WLAN verwendet wird, wird von beiden unterstützt. Welcher Supplicant nun von den beiden verwendet werden soll, muß man von der verwendeten WLAN-Karten abhängig machen, da beide Clients unterschiedliche Karten verwenden können.

Vom Xsupplicant verwenden Sie bitte nicht die Version 1.2pre sondern die Version 1.0.1.

<http://www.open1x.org>

Die aktuelle Version 0.3.9 vom wpa-supplicant

http://hostap.epitest.fi/wpa_supplicant/

Beide benötigen OpenSSL:

<http://www.openssl.org/>

Das erforderliche Root Certificat **ca.crt** erhalten Sie im PWA:

<https://pwa.fh-wolfenbuettel.de/ca/index.jsp>

Speichern Sie das Zertifikat im Verzeichnis /etc als **ca.crt** ab.

Nach dem Kompilieren können Sie eine der beiden Beispielkonfigurationen nutzen, in dem Sie die entsprechenden Stellen in den Konfigurationsdateien ersetzen. **Fett** geschriebenes ist durch eigene Parameter zu ersetzen.

Sie können die Dateien auch herunterladen.

Xsupplicant

Startscript:

```
#!/bin/sh
```

```
iwconfig wlaninterface enc 0000000000
```

```
xsupplicant -c /etc/xsupplicant.conf -i wlaninterface -d A
```

/etc/xsupplicant.conf

```
network_list = 802.1x
default_netname = 802.1x
logfile = /var/log/xsupplicant.log
allow_interfaces = wlaninterface #z.B. ath0
deny_interfaces = interface      #Netzwerkanschlüsse, die nicht erfasst werden
                                #sollen z.B. eth1
first_auth_command = <BEGIN_COMMAND>dhclient wlaninterface<END_COMMAND>
802.1x
{
    allow_types = eap-ttls
    identity = <BEGIN_ID>anonymous<END_ID>
    eap-ttls
    {
        root_cert = /etc/ca.crt
        chunk_size = 1398
        random_file = /dev/urandom
        phase2_type = pap
        pap
        {
            username = <BEGIN_UNAME>HBK-LOGIN<END_UNAME>
            password = <BEGIN_PASS>PASSWD<END_PASS>
        }
    }
}
```

WPA - Supplicant

Startscript:

```
#!/bin/sh

pkill wpa_supplicant
pkill dhclient

rm -fr /var/run/wpa_supplicant

ifconfig wlaninterface 0.0.0.0 down
ifconfig ethernetinterface 0.0.0.0 down

iwconfig wlaninterface mode Managed
iwconfig wlaninterface key 000000000 key open
iwconfig wlaninterface essid 802.1x

( /usr/sbin/wpa_supplicant -iwlaninterface -c/etc/wpa_supplicant.conf
-Dwlaninterface -B ) > /tmp/wpa_supplicant.log 2>&1 < /dev/null
sleep 5
dhclient wlaninterface
```

/etc/wpa_supplicant.conf:

...

```
# Catch all example that allows more or less all configuration modes
network={
    mode=0
    ssid="802.1x"
    scan_ssid=1
    key_mgmt=IEEE8021X
    eap=TTLS
        anonymous_identity="anonymous"

    identity="HBK-LOGIN"
    password="PASSWD"

    ca_cert="/etc/ca.crt"

    subject_match="/C=DE/ST=Niedersachsen/L=Braunschweig/O=HBK-
BS/OU=ZKI/CN=wlan.hbk-bs.de/emailAddress=wlan-admin@hbk-bs.de"

    phase2="auth=PAP"
}
```