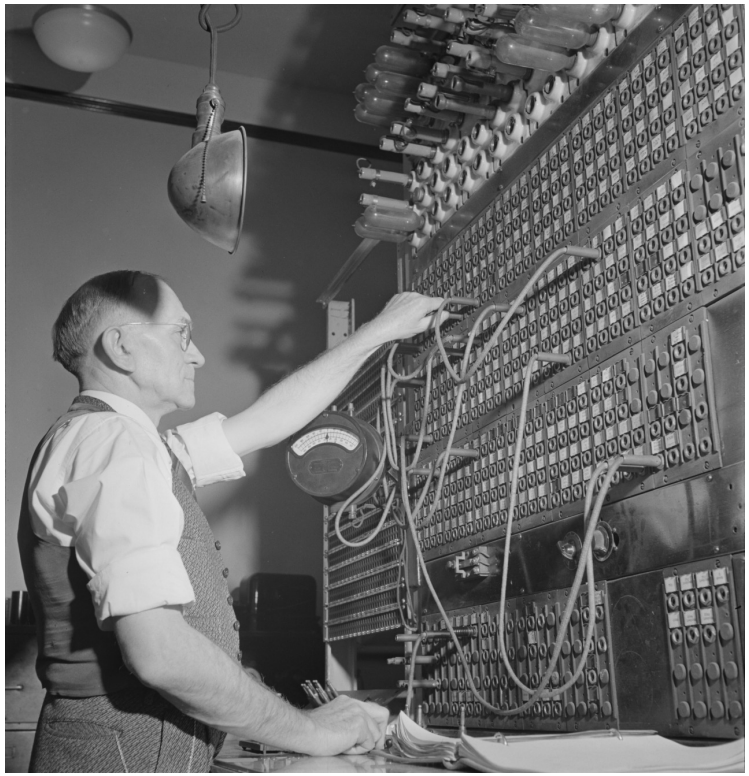
Linux aansluiten op de beveiligde UvA-netwerken (WiFi of bedraad)

Deze tekst legt beknopt uit hoe men op een computer die Linux draait toegang krijgt tot de beveiligde (802.1x) netwerken van de UvA. In sectie 1 bespreken we de WiFi-netten ‘uva’ en ‘eduroam’, sectie 2 gaat over het bedrade beveiligde netwerk (EAPoL).

1 Verbinding opzetten met WiFi-netwerken ‘uva’ en ‘eduroam’

De Universiteit van Amsterdam biedt de medewerkers en studenten in al haar gebouwen toegang tot twee verschillende draadloze netwerken aan genaamd ‘uva’ en ‘eduroam’. Daarnaast is er op elke locatie een publiek netwerk beschikbaar ‘UvA Open Wi-Fi’ genaamd behalve op Science Park waar dit ‘Amsterdam Science Park’ heet. Het publieke netwerk vereist geen authenticatie maar is onbeveiligd, langzaam en staat afgesloten van het intranet. Gebruik het alleen wanneer het niet anders kan. Verbinding maken met het publieke netwerk wijst zichzelf en wordt hier niet besproken.
De procedures om uva en eduroam te configureren zijn identiek. Voor oudere hardware geldt mogelijk dat het nieuwere WiFi-protocol dat op 5 GHz communiceert niet wordt ondersteund. Oude netwerkkaarten werken op 2,4 GHz en zullen het uva-netwerk niet waarnemen maar alleen eduroam (dat op beide frequentiebanden 2,4 GHz en 5 GHz uitzendt). Aangezien, in tegenstelling tot het uva-netwerk, de authenticatie bij eduroam via een externe partij loopt raden we mensen met een UvAnetID aan, waar mogelijk, uva te gebruiken.



1.1 WPA Supplicant

Stel eerst vast dat het pakket wpa_supplicant op uw computer aanwezig is. Op een RPM-gebaseerd systeem (Redhat, SuSE, enz.) kunt u dat doen door bijv. in een terminal het volgende commando te geven:

```
$ sudo rpm -q wpa_supplicant
```

Op APT–gebaseerde systemen (Debian, Ubuntu enz.) luidt het commando:

```
$ sudo dpkg -l wpasupplicant
```

Indien wpa_supplicant ontbreekt dan moet u deze via een alternatieve internetverbinding zien te verkrijgen. Voor de details verwijzen wij u naar de handleiding van uw Linux-distributie.

1.2 Parameters

Alle benodigde parameters voor het verbinding maken met de draadloze netwerken worden in de onderstaande tabel opgesomd.

WiFi-netwerken	
SSID:	uva *of* eduroam
Mode:	Infrastructure
IPv4 Settings:	Automatic (DHCP)
Wireless security:	WPA & WPA2 Enterprise
Authentication:	Protected EAP (PEAP)
Anonymous identity:	`anonymous@uva.nl`
Domain:	`uva.nl` *(zie onderstaande toelichting)*
CA certificate:	*(zie onderstaande toelichting)*
Inner authentication:	MSCHAPv2
Username:	*UvAnetID*`@uva.nl`
Password:	*wachtwoord van uw UvAnetID*

Toelichting:

- Voer uw UvAnetID in kleine letters in.
- Het domein van uw gebruikersaccount (`@uva.nl`) dient vermeld te worden, dan wel in een apart veld, of als achtervoegsel van uw UvAnetID gescheiden door een apestaart (`@`), d.w.z. *UvAnetID*`@uva.nl`
- Authenticatie met externe Eduroam-accounts (bijv. VUnetID) werkt ook, maar uitsluiten op het `eduroam`-netwerk. Het domein moet overeenkomen met de beheerder van het account.
- Voor studenten geldt dat het UvAnetID gelijk is aan hun collegekaartnummer.
- Het veld '**CA certificate**' vraagt om een kleine file met informatie waarmee uw computer de authenticiteit van een desbetreffend netwerk kan verifiëren. Hiermee voorkomt u een zg. *man-in-the-middle attack*, de situatie waarin een derde partij zich valselijk voordoet als de authentieke server. U dient het certificaat natuurlijk op te halen via een ander kanaal, ofwel downloaden na eerst verbinding te maken met het publieke netwerk (`UvA Open Wi-Fi` of `Amsterdam Science Park`) of vanaf een andere computer. U vindt het certificaat door op pagina `http://wifiportal.uva.nl` onder "Select your device:" de optie "Non-specific OS" te selecteren (let op: *niet* "Linux"). Download de file `usertrustrsaca [jdk].cer` vanaf de bovenste link USERTrust RSA Certification Authority (Jan 18 2038). U kunt het certificaat in uw home-directory laten en de configuratie ernaar laten verwijzen, maar we raden aan het op te slaan in de centrale "trust store" van uw systeem en deze op te nemen in de configuratie.

Het gedownloade UvA-certificaat installeren in de trust-store gaat voor de verschillende Linux-distributies een beetje anders. Open een commando-venster zoals **Terminal**.

Bij de Redhat-familie zijn de commando's als volgt:

```
$ sudo cp usertrustrsaca\ [jdk].cer /etc/pki/ca-trust/source/anchors/
$ sudo update-ca-trust extract
```

Bij op Debian gebaseerde distributies gaat het zo:

```
$ openssl x509 -in usertrustrsaca\ [jdk].cer -outform PEM -out usertrustrsaca\ [jdk].crt
$ sudo cp usertrustrsaca\ [jdk].crt /usr/local/share/ca-certificates/
$ sudo update-ca-trust
```

Bij SuSE zo:

```
$ openssl x509 -in usertrustrsaca\ [jdk].cer -outform PEM -out usertrustrsaca\ [jdk].crt
$ sudo cp usertrustrsaca\ [jdk].crt /etc/pki/trust/anchors/
$ sudo update-ca-certificates
```

Voor andere Linux-versies verwijzen wij u naar de desbetreffende documentatie.

Na afloop kunt u de `.cer`- en `.crt`-bestanden in uw home weggooien. In het veld '**CA certificate**' vult u nu de het pad van de trust store in. Voor de Redhat-familie is dit `/etc/pki/ca-trust/extracted/pem/directory-hash/ca-certificates.crt`. Bij de Debian-familie gebruike men `/etc/ssl/certs/ca-certificates.crt`.

2 Verbinding opzetten met een bedraad 802.1x-netwerk (EAPoL)

[1] Net als bij de WiFi-netwerken moet de gebruiker zich bij de bedrade LANs (i.e. VLANs 315x) eerst authenticeren met zijn of haar UvAnetID voordat de verbinding bruikbaar wordt. Alle benodigde parameters voor het verbinding maken worden in de onderstaande tabel opgesomd:

802.1x-netwerk	
IPv4 Settings:	Automatic (DHCP)
802.1x Security:	*Aan*
Authentication:	Protected EAP (PEAP)
PEAP version:	Automatic
Anonymous identity:	`anonymous@uva.nl`
CA certificate:	*niet verplicht*
Inner authentication:	MSCHAPv2
Username:	*UvAnetID*`@uva.nl`
Password:	*wachtwoord van uw UvAnetID*

Toelichting:

- De in te vullen gebruikersnaam (**Username**) is uw UvAnetID (in kleine letters) gevolgd door "`@uva.nl`". Dit achtervoegsel wordt vaak vergeten. Bedenk ook dat het hier niet uw e-mailadres betreft.
- Het veld '**CA certificate**' vraagt om een kleine file met informatie waarmee uw computer de authenticiteit van een desbetreffend netwerk kan verifiëren. Hiermee voorkomt u een zg. *man-in-the-middle attack*, de situatie waarin een derde partij zich valselijk voordoet als de authentieke UvA-server. Dit is voor WiFi erg belangrijk, maar voor bedrade netwerken minder relevant. Wij kiezen er hier voor het veld blanco te laten. Zie evt. de uitleg onder sectie 1.

[1] Tot 2024 bood de UvA twee aparte netwerken aan voor eigen-beheerde computers, VLAN 256 en VLAN 18. Sindsdien is een nieuwe groep beveiligde VLAN's gecreëerd (VLAN 315x) waar alle zelf beheerde en centraal beheerde computers op aangesloten kunnen worden. Voor de configuratie van de netwerkverbinding is afgezien hiervan weinig veranderd.