Operating the Infrastructure

Operating the Infrastructure

Regular safety precautions

Everyone is responsible for their own network. It is not in the scope for this document to describe regular network or system security measurements. Local "best current practices" for the network and system design should be followed in any case.

Tracking malicious users

If the requirements of the eduroam policy are followed, it should be possible to provide sufficient evidence to government agencies to allow them to pinpoint a malicious user, thereby protecting the service provider. The requirements are:

- Keeping authentication logs.
- Keeping a DHCP (or even better an ARP) sniffing log.
- Keeping clocks on time with NTP.

The tracing chain is:

1. IP of logged in user that is operating in a malicious manner.
2. IP is linked to MAC address [DHCP or ARP sniffing].
3. Authentication session of this MAC is checked in logs [auth logs].
4. timestamp of authentication and realm is extracted.

From this chain the realm of the offender and the time of login are known. This should be provided to government agencies when required. For example, the information could be: the malicious user is someone from restena.lu who logged in at April 1, 2007, 12:01:45.3221.

Note well: the eduroam service definition document only obliges the Identity Provider and FLR infrastructure to keep logs of all authentications that took place and maintain a synchronised time source. It is in the best interest of a Service Provider to keep sufficient log information themselves though to make sure that the link in steps 3 and 4, above, can be made to trace a user login efficiently. However, even if the SP does not keep the data, it is possible to retrieve the information from FLR logs if need be.

The eduroam operations team can link the realm to a physical point of contact (home federation operator). This federation contact can find the institution, and then in turn the user name of the offender, using the IdP logs with the precise login timestamp that was extracted above.

Note: The User-Name attribute may be obfuscated with an anonymous or even forged outer identity, so it can't be used to reliably identify the individual on the service provider's side. The only reliable User ID is with the IdP.

For the record, the points of the eduroam service definition deliverable DS5.1.1 in question are:

6.2.1: technical contact for federation
6.3.1, Confederation member servers, Bullet 5: logging of authentication attempts
6.3.1, Confederation member servers, Bullet 2: reliable time source
6.3.2, Service Providers, Bullet 2: sufficient layer-2 to layer-3 logging information
6.3.2, Identity Providers, Bullet 4: logging of authentication attempts

Formally, some of these requirements are signed by the federation but affect the institutions, and so should also be re-iterated in the national policies to make them binding for participating institutions. A formal nomination of technical contacts for each institution within a federation is also recommended. For example, Appendix B in DJ5.1.3,2, the national federation policy BCP therefore has sections:

- 4: Logging
- 6.2: Security contact nomination