

Mobility Task Force



Deliverable F

Inventory of web-based solution for inter-NREN roaming

Version 1.1

Authors: Sami Keski-Kasari <samikk@cs.tut.fi>, Harri Huhtanen <karrih@cs.tut.fi>

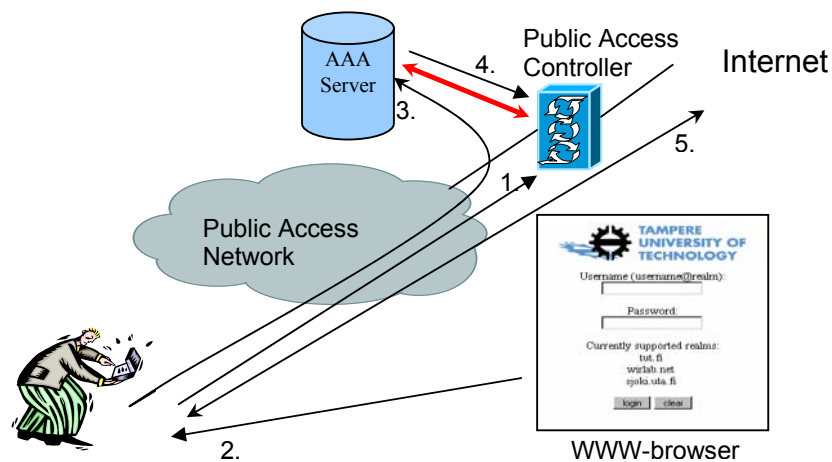
Contributions: James Sankar <J.Sankar@ukerna.ac.uk>

Introduction

In this document we are considering a web-based authentication system as a solution to enable roaming between European research and education networks. This document complies with List of non-Technical Terms [6].

1. Architectural design

The architecture of a web-based authentication system is very simple. It does not need any special functionality to be added to the access points or switches. All functionality is located near the edge of the network. On the edge of the network there is an access control device commonly referred as access control device, which acts as router or bridge to the visited institution network. The access control device denies access to the protected networks by denying the traffic from and to unauthorized hosts. The architecture and functionality can be seen in the picture below.



When visitor users attach to the network that uses web-based authentication they get initial docking IP address via DHCP, but are unable to receive and send traffic outside the network. To gain network access outside of the network, the visitor user must launch their web browsers which will be automatically redirected to an authentication web page (arrow number 1). The access control device manages this process by capturing the HTTP connection and redirects the user's web browser to an authentication page (arrow number 2).

On the authentication page a web form appears so that the visitor user must enter user credentials (e.g. username and password). Then the access control device will authenticate the user based on these credentials (arrow number 3). If the authentication succeeds (arrow number 4) the access control device modifies the firewall rules (arrow number 5) to enable the visitor user to gain access outside of the network. If the authentication fails, an authentication error is returned to the user and the credentials are asked again. The amount of the authentication attempts can be limited.

Detaching the user from the network may be initiated by the user or by the network.

When the user wants to log out, there may be some kind of form or popup windows for sending the logout message. The pop-up window and regular re-registrations via HTTP may be used for ensuring the user's terminal has not left the area without logging out.

Another used method is that the access control device frequently polls user terminal with ARP or ICMP requests to detect if the terminal has left the network. If the user terminal does not answer a specific amount of requests, the terminal is considered detached from the network and the access control device closes the firewall rules to prevent session hijacking.

2. Roaming Issues

Within the area controlled by the same access control device users can roam to other access points or switches without re-authentication. There are some vendor specific protocols which can carry authentication information to other access control devices. In that case the users can roam between areas controlled by different access control devices. Although Mobile-IP support in existing access control devices is almost nonexistent, integrating Mobile-IP to handle IP network roaming into open access control device platform is also possible.

Inter-NREN authentication roaming can be done via RADIUS or LDAP if the access control device and authentication server support those methods. For example in the TUT's self-integrated access control device [1] there are Linux PAM-modules for both protocols. If the authentication is done using RADIUS-protocol then the similar roaming architecture as in the 802.1X case may be used [5]. This may be done so that there is one main RADIUS-server and NREN's RADIUS-servers are attached to that server and organizations' RADIUS servers are attached to those servers. With LDAP-protocol, the hierarchy can be similar but in this case interoperability with 802.1X will not work. For more detailed information about roaming with web-based access control devices information can be found from TUT's web-pages concerning public access roaming. [2]

3. Security Issues

3.1 Securing the user credentials and roaming information

Access control devices use regular web servers to present the authentication form to visitor users. User's credentials are so transferred with HTTP/HTTPS –protocol depending of the access control device. Some commercial access control devices do not even have HTTPS-protocol in the default software version and an additional fee must be paid to get HTTPS-enabled version. Due to this kind of choice of HTTP and HTTPS, HTTPS should be recommended or in the case of intra/inter-NREN –roaming required from the roaming organizations to ensure that some other university doesn't jeopardize other university's user credentials by sending them as clear text. Using HTTPS and SSL/TLS-certificates also provides the possibility of using SSL/TLS - certificates in authenticating the docking networks to users. This way the risk of doing fake docking networks and controllers collecting usernames and password would be harder, but still leaves the responsibility to user to check

the certificate presented by web browser. In practice this would require a PKI-infrastructure to be built inside and between NRENs. The defined PKI-, CA-, etc. policies, practices and the infrastructure would benefit also other projects requiring for example SSL/TLS -certificates valid in different NRENs networks.

Building the PKI-infrastructure could start inside NREN, where the NREN operator of the NREN would manage the highest CA certificate. This NREN operator would then give organizations inside NREN CA certificates and the organizations could then create SSL/TLS-certificates to be used in the access control devices and other related hosts/devices needed for docking network control and roaming (e.g. for securing the Radius/LDAP-traffic with IPSEC or SSL).

This PKI-infrastructure could also be scaled to even a higher level by introducing a root CA that would issue and certify the NREN CA-certificates. TERENA would be a logical suggestion for this. This practice would then enable a chain of trust where the users would only need this highest certificate installed into their terminals and still be able to verify the certificates of the access control device anywhere on the roaming area.

3.2 Network element security

Both the free and commercial access control devices are usually based on some free UNIX-based operating system and may use common open source software like Apache, PHP, and Perl etc. Because of this, extra attention should be focused in securing these hosts.

Besides access control devices, there are also LDAP/Radius servers and the PKI-infrastructure hosts to be secured. The protocols are encrypting credentials but for example in the hierarchical Radius/LDAP roaming scenarios the user credentials are obtainable in plain text in all RADIUS/LDAP servers and also in the access control device. For that reason in all organizations all these servers must be managed by IT management in the same way to avoid misconfigured servers and leaking of credentials. Roaming policies and requirements could be the place to define the requirements and restrictions in these kinds of issues.

4. Requirements

4.1 Client

Client can be any device that has www-browser that supports HTTPS, network interface card and DHCP client.

4.2 Access Control Device

Access Control Device can be build to any operating system that supports routing and route filtering and has https-server. For example Linux, Windows 2000, etc. TUT's Access Control Device [1] is built on Debian Linux. There is also commercial "ready to use" access control devices like Nomadix, Vernier, etc. For additional security Access Control Device should also support IPsec.

4.3 RADIUS server

Radius server must support RFC 2865 [3] and 2866 [4]. For additional security RADIUS server should support IPsec. There are no other requirements. For example FreeRADIUS, Radiator and Cisco ACS have all required capabilities. FreeRADIUS is available for Unix platforms. Cisco ACS and Radiator are also available for Windows platform. For better performance the authenticating RADIUS server should use an SQL database or LDAP for storing credentials.

5. Scalability

5.1 Access Control Device

Access Control Device is on the edge on network controlling access from docking network to the Internet. Usually one access control device is needed per network. If the operating system or NIC drivers and switches support VLAN assignments or the access control device has more than two NICs, it is possible to serve more networks using one access control device. For networks consisting of several sites/locations additional access control devices may be used when needed.

5.2 RADIUS hierarchy

RADIUS hierarchy can be build by domain names, like in DNS, so it is very scalable. The number of levels in the hierarchy is not limited.

5.3 RADIUS hierarchy

Because all universities have their own CA certificate that is signed with NREN's CA certificate there shouldn't be any scaling problems. Universities can grant their own client certificates, but for example they can't create new CA certificates. If cost is prohibitive, the top level certificate can be self-signed. Then users must once install the top level certificate to their terminals but after that it can be used to verify hosts everywhere inside the roaming community.

6. Interoperability

6.1 802.1X based solution

Access Control Device is not compatible with 802.1X because 802.1X is layer2 solution and Access Control Device is layer3 solution. Web-based solution is still compatible with 802.1X via RADIUS hierarchy. Both techniques can use same RADIUS hierarchy. Only difference is that in 802.1X case user's home institution RADIUS server must support 802.1X.

It is also possible to use both the web-based and the 802.1X authentication methods simultaneously in the wireless environment by using access points, that have the VLAN tagging and multiple network name (ESSID) capabilities. In the wired environment it is possible to get VLAN information from RADIUS to change switch port's VLAN assignment. This way it is possible to assign docking network VLAN id to switch port but the user can choose to authenticate via web-based system or 802.1X. By default the port is in the state that sends traffic to the VLAN controlled by access control device and the scenario is similar to web-based authentication. If the terminal starts 802.1X negotiation, the switch or the access point tries to authenticate the terminal via RADIUS roaming hierarchy. After the successful authentication via 802.1X the switch changes the port's VLAN assignment to a VLAN that allows traffic go through.

6.2 VPN based solution

Access Control Device is fully compatible with VPN solution. Both web-based and VPN solution can co-exist in the same network. Access Control Device must be configured to allow VPN traffic to certain VPN concentrators and all other users authentication is made via web-based system.

7. References

- [1] TUT Public Access, <http://www.atm.tut.fi/tut-public-access/>
- [2] TUT Public Access Roaming, <http://www.atm.tut.fi/public-access-roaming/>
- [3] Remote Authentication Dial in User Service (RADIUS), IETF RFC 2865
- [4] RADIUS Accounting, IETF RFC 2866
- [5] Terena Mobility Taskforce, Deliverable D
- [6] Terena Mobility Taskforce, List of non-Technical Terms