Eduroam, providing mobility for roaming users

Licia Florio*, Klaas Wierenga†

*TERENA, the Netherlands
florio@terena.nl

† SURFnet, the Netherlands
Klaas.Wierenga@SURFnet.nl

Abstract

The number of mobile devices within academia has increased significantly over the last couple of years. The majority of laptops sold nowadays have wireless LAN capabilities built-in and users expect to be able to get connectivity everywhere, at home, on the road and at educational institutions. At the same time however, the security of wireless LANs becomes more and more of a concern; due to the increasing number of tools (such as Kismet [1] and Airsnort [2]) compromising security based on Wireless Equivalent Privacy (WEP) security.

The roaming needs of users have led to a number of national and international initiatives to provide network roaming for their constituencies.

In 2003, the TERENA Task Force on Mobility [3] was created to look at WLAN security issues and to formulate requirements to design an international roaming solution that would provide National Research and Educational Networks (NRENs) users with secure Internet access at academic campuses (WLAN and wired) across Europe. The solution proposed was tested and proved to be very successful with more and more institutions joining it. This infrastructure is called Eduroam, which stands for European Roaming.

Keywords: WLAN security, 802.1X, RADIUS, Eduroam.

1 Introduction

The number of mobile devices within academia has increased significantly over the last couple of years. The majority of laptops sold nowadays have wireless LAN capabilities built-in and users expect to be able to get connectivity everywhere, at home, on the road and at educational institutions. At the same time however, a number of tool (such as Kismet and Airsnort) show that the security of wireless LANs based on Wireless Equivalent Privacy (WEP) is not effective at all.

As users are becoming mobile they are expressing the desire to have their familiar environment, services and privileges available whenever they move from one site to another. The number of researchers and students "roaming" between different NREN domains is increasing and so is their demand for these services.

The roaming needs of users have led to a number of national and international initiatives to provide network roaming for their constituencies. Within the TERENA taskforce on Mobility requirements were formulated to develop an international roaming solution that would provide NREN users with secure Internet access at academic campuses (WLAN and wired) across Europe with the following characteristics:

- Minimal administrative overhead (per roaming user)
- Good usability
- Maintaining required security for all partners
- Scalable

TERENA's Mobility task force identified three possible approaches in current use:

- Web-based authentication with RADIUS backend (Finland),
- VPN-based authentication (Germany and Switzerland)
- 802.1 X-based authentication with RADIUS backend (The Netherlands).

Each solution was evaluated and characterised as follows:

- Web: Scalable, Unsafe, already deployed
- VPN: Not Scalable, Safe, already deployed
- 802.1X: Scalable, Safe, New.

Based on these characteristics and on the fact that upcoming security standards like WPA and 802.11i all build on 802.1X, TF-Mobility has concluded that 802.1X authentication with a RADIUS-hierarchy based backend is the method of choice, even though not every institution is able to support it currently because of legacy equipment.

2 The creation of Eduroam

One of the goals of the Mobility task force was to design an inter-NREN roaming infrastructure; having selected 802.1X as the authentication method, it was agreed to set-up a test-bed based on 802.1X and RADIUS servers.

This test-bed has evolved into a pan-European pilot called Eduroam (Education Roaming). The Eduroam service builds on a hierarchical system of RADIUS-servers. TERENA deploys a European top level RADIUS-server to which all European NRENs that participate connect with their national

RADIUS-server. Every institution that wants to participate in Eduroam connects its institutional RADIUS-server to the national server of their NREN.

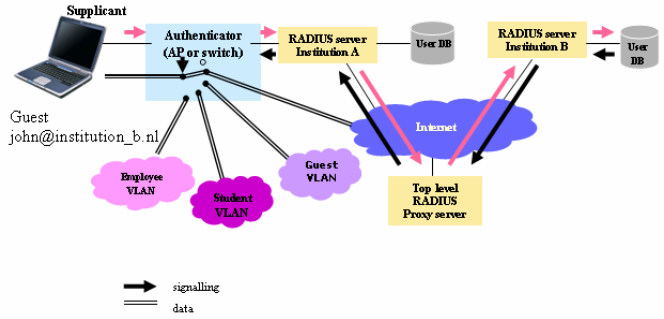

Figure 1: Eduroam basic set-up (© SURFnet)

Figure 1 shows the typical operation based on 802.1X for a guest user at an Eduroam participant site in the Netherlands. The user, belonging to the institution called **institution b**, provides his credentials; the RADIUS-server of **institution a** discovers that it is not responsible for the **institution_b.nl realm** and proxies it to the national RADIUS-proxy server (that in turn might proxy it to the European server in case the user is coming from another country).

This national server forwards the credentials to the home-institution of the user where they are verified. The 'acknowledge' of a successful authentication travels back over the proxy-hierarchy to the visited institution and the user is granted access.

Because the user credentials travel via a number of intermediate servers, not under control by the home-institution of the user, it is important that the credentials are protected for privacy reasons. This requirement limits the types of authentication methods that can be used. Basically there are two categories of useful authentication methods, those that use credentials in the form of some **public key** mechanism with certificates (EAP-TLS, EAP-SIM) or those that use the so-called **tunneled authentication** (EAP-TTLS, PEAP). Authentication using both server and end-user certificates requires the roll-out of a public key infrastructure (PKI) with end-user certificates which has proven difficult in most NRENs. Most institutions therefore use a **tunneled authentication** method that only requires server-certificates.

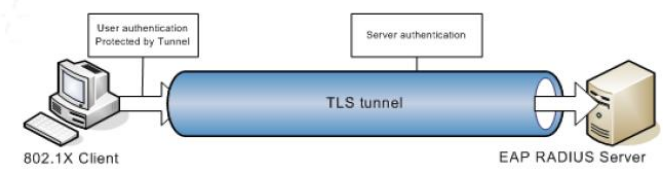

Figure 2: Tunneled authentication (© Alfa&Ariss)

3 Current Situation

At the time of writing (April 2005) more than 350 institutions in 18 countries participate in Eduroam.

Figure 3: Current Eduroam Paretcipants

Most countries that participate in Eduroam are setting up a web page showing which institutes are participating in Eduroam. In the United States of America the Internet2 working group SALSA-NetAuth [4] has started an initiative to create a RADIUS-hierarchy for higher education and to become Eduroam participants. Also in the Australian-Pacific region an Eduroam initiative has started.

Assisted by various members of the European Eduroam federation, AARnet[5] and GRANGEnet [6] have set up Eduroam Australia that is connected to the European Eduroam federation and also a first pilot connection with the US has been established.

3 Conclusion

Eduroam has proven itself as a scalable, secure and successful pilot service. This is proven by the fact that more and more countries and institutions participate, also beyond Europe, thus making it more and more beneficial for the participants.

Within the 6th framework project GÉANT2 [7] the aim is to expand the existing infrastructure into a pan-European full service for Roaming and Authentication/Authoristion. This will result in a service that is more robust and suitable for new categories of use, in particular federated access to applications. Foreseen improvements of the infrastructure concentrate on the 'backplane' of the service, while keeping intact the institutional set-up. This combined with the fact that new security standards like WPA and 802.11i are built upon the 802.1X framework ensure that an investment in Eduroam participation is justified.

It is TERENA's intention to expand the Eduroam service to encompass as much of the academic community as possible. It should be noted that since the system requires a national level RADIUS server this implies that the NREN in these countries need to be involved.

Acknowledgements

This paper is based on information provided by Klaas Wierenga (SURFnet), co-chair of TERENA TF-Mobility and by all people who contributed to the mobility task-force.

References

[1] Kismet (http://www.kismetwireless.net/) 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.

[2] Airsnort (http://airsnort.shmoo.com/), WLAN system to recover encryption keys.

[3] TERENA Task Force on Mobility, http://www.terena.nl/tech/task-forces/tf-mobility

[4] SALSA-NetAuth, http://security.internet2.edu/netauth/

[5] http://www.aarnet.edu.au/

[6] http://www.grangenet.net/index.html

[7] http://www.geant2.net/