Cross-organisational roaming on wireless LANs based on the 802.1X framework

Author:

Klaas Wierenga
SURFnet bv
P.O. Box 19035
3501 DA Utrecht
The Netherlands

e-mail: Klaas.Wierenga@SURFnet.nl

Keywords:

Mobility, authentication, 802.1X, Wireless LAN

Abstract:

Introduction

Most institutions within the SURFnet constituency are deploying or have concrete plans to deploy wireless LAN (WLAN) services for their students and employees. At the same time there is an increasing awareness of the risks involved in deploying these kinds of services. SURFnet, in turn, has the ambition to provide an infrastructure for cross-institutional (both nationally and internationally) roaming for wireless networks. This has led to a project at the University of Twente in which a secure solution for access to WLANs has been developed. It builds on the 802.1X standard for port based authentication for wired and wireless networks and allows for guest access to the WLAN. These activities are carried out in conjunction with the nationwide wireless testbed in the Freeband project and within the TERENA Taskforce on mobility.

Requirements

In order to select the best possible solution the following requirements were formulated:

- Identify users uniquely at the edge of the network.
- Session (identity) takeover is impossible
- Easy to install and use for the end-user
- Per-institution user subscription management

- Low maintenance
- Easy to use for guests
- The home institution of a guest performs the authentication
- Use various authentication-mechanisms
- Support for common operating systems
- The solution is vendor independent
- Guaranteed interworking with the existing RADIUS based infrastructure SURFnet deploys for dial-in and ADSL access
- Traffic separation (for instance based on VLAN assignment) support

Please note that these requirements reflect the fact that the resource to protect is the access to the network, not the data streams that ensue. The latter should be implemented as an end-to-end secure path from the device to the home network, for instance using a secure tunnel at the application layer. For the same reason encryption of the wireless path has not high priority.

Various solutions

There are a number of solutions for providing a wireless access infrastructure. The following have been investigated prior to selecting 802.1X: open network access, WEP-based, MAC-based, VPN-gateway and web-gateway based. They were dropped for reasons of low security or bad scalability.

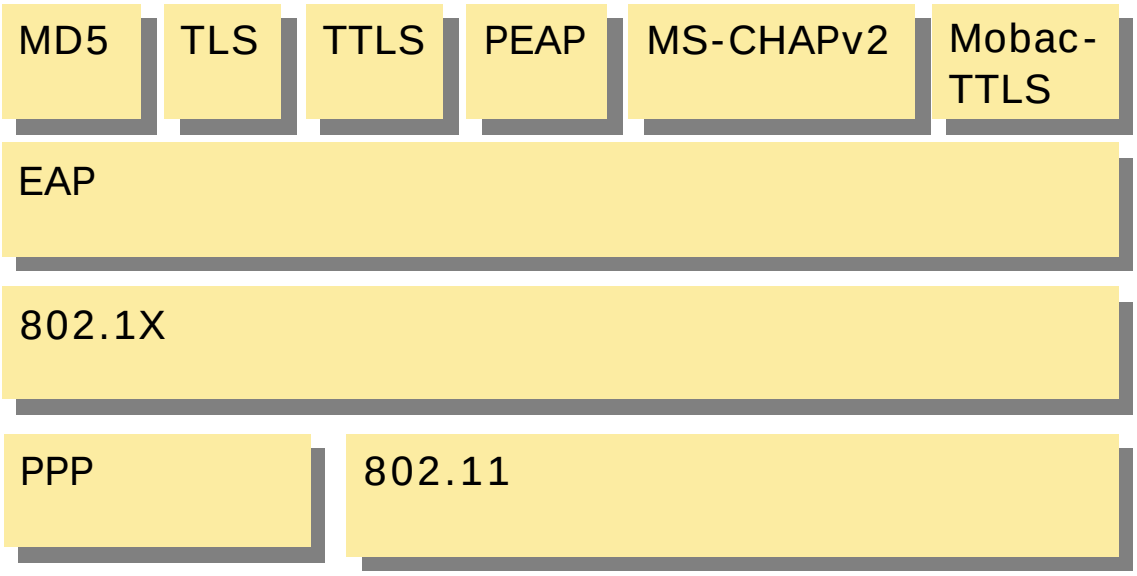
- IEEE 802.1X

The IEEE 802.1X standard for port based authentication is a layer 2 solution between client and wireless access point or switch. In the 802.1X framework authentication information is carried using the Extensible Authentication Protocol (EAP, RFC 2284), a protocol that enables the use of several authentication methods, currently MD5, TLS, TTLS, MS-CHAPv2, PEAP and SIM-card based.
The communication between client and access point is encrypted using dynamic keys and uses a RADIUS backend, thereby making it both secure and scalable. The disadvantage of this solution is the relative novelty and the fact that (currently) client software is necessary on most platforms.
Based on the possibility for secure guest access, scalability and the fact that 802.1X is also deployed in a number of wired pilots in the SURFnet constituency this solution was selected to pursue.

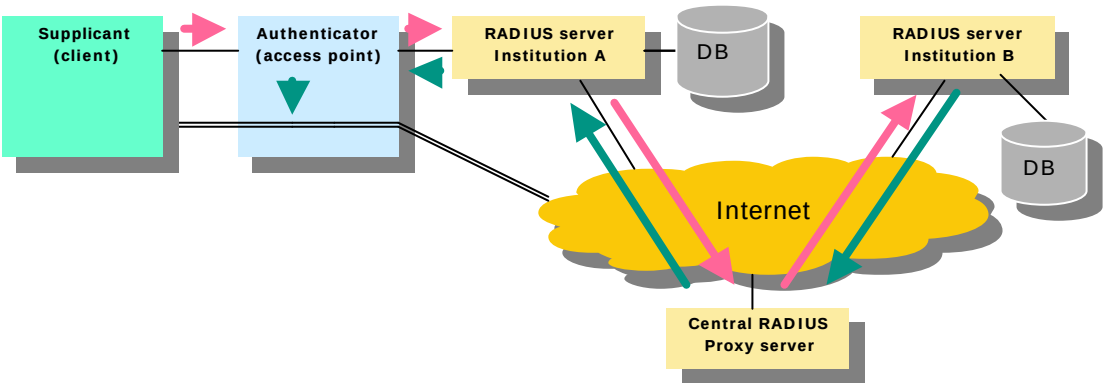
The pilot

The figure below shows the protocol stack of the 802.1X framework. Please note that on top of EAP the desired authentication method needs to be selected. Since username/password is considered to be weak authentication, the choice was between TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) en PEAP (Protected EAP). At the time of selection PEAP, the protocol proposed by

Cisco and Microsoft, was not yet available. For this reason TLS and TTLS were chosen. Additional tests were done with authentication based on one time passwords sent by SMS, in combination with TTLS.
TLS and TTLS both set up a TLS connection between client and access point, TLS using both client and server certificates, TTLS only server certificates.



At the backend the existing RADIUS infrastructure of SURFnet has been used. The complete infrastructure looks as follows:



When a user connects to the network he provides his credentials to the authenticator (the access point) that verifies this using the RADIUS backend. If the user is properly authenticated the access point lets the user traffic through. In case of guest use the RADIUS proxying mechanism makes sure that the EAP encapsulated credentials get transported towards the home RADIUS server, whether it is located nationally or internationally, where the user gets authenticated against the user database.

Results

- Clients

In order for the client (supplicant in 802.1X terminology) to use 802.1X based authentication, the client OS needs to support EAP and the required authentication method. For the pilot EAP-TLS and EAP-TTLS were selected. TTLS because it doesn't require a PKI with end-user certificates and TLS for the case where such a PKI does exist.
Currently the windows XP operating system supports EAP and TLS. For earlier windows versions EAP support is announced. In the project a TTLS module developed for SURFnet was distributed. Apart from this module there exist commercial clients that include both an EAP and TTLS or TLS stack. In the pilot Funk and Meetinghouse clients have been tested. For Apple systems commercial clients exist and for various Unix flavors there are public domain implementations.

- Access Points

Most modern Access Points support 802.1X authentication or have announced this. In the pilot products from Cisco (350 and 1200) and Orinoco (AP2000) have been tested successfully.

- RADIUS servers

The intermediate RADIUS server must be able to handle EAP messages and the final RADIUS server must also support the requested authentication method. In the pilot Radiator 3.3.1 was used. In cooperation with the creator of Radiator some bugs in the EAP implementation have been resolved.. Other RADIUS servers that support TTLS and TLS include Meetinghouse, FUNK Steel-Belted and FreeRADIUS (the latter just TLS).

- Switches

In the project VLAN assignment at the University of Twente HP switches based on the provided credentials was successfully demonstrated.

- Usability

One of the design criteria was the ease of use for the end-users. The pilot has shown that, once the user has installed the 802.1X client, use of the wireless network is handled seamless and transparent. In fact, it was found that there need to be stronger visual clues as to the nature of the connection, secure or insecure.
The installation of the client-software is a bottleneck.The fact that Cisco and Microsoft have announced native PEAP-support promises ease of use for a large percentage of the users and suggests moving from TTLS to PEAP.

Security

Security of Wireless LANs is a hot item. The ongoing stories about wardriving, WEP-key cracking and man-in-the-middle attacks have given a lot of system operators cold feet. The pilot shows that as long as a strong EAP capable protocol is used 802.1X provides a framework that gives a sufficient level of security for the intended purpose, i.e. access control to the network. For data integrity or privacy issues a number of wireless security extensions (WPA, TKIP, 802.11i etc.) have been proposed, that also build on the 802.1X framework.

Conclusion

The piloted solution is both scalable and seamless. With the proper EAP authentication protocol the solution is also secure for the intended purpose. SURFnet will require use of 802.1X authentication in the nation-wide wireless testbed that will be established in the Freeband project, thus stimulating the use of this technology instead of less secure (web-based) or less scalable (VPN) solutions.
Apart from providing institutions a sufficiently secure and easy to deploy solution the large added benefit of this solution is the ease in deploying a nationally and even internationally solution for inter-institutional roaming.

Acknowledgements:

This abstract is based on information provided by the participants in the project: Sander Smit of the University of Twente, Tom Rixom of Alfa&Ariss and Erik Dobbelsteijn of SURFnet Innovation Management.

Vitae:

Klaas Wierenga has worked for 7 years at SURFnet. In his capacity as Innovation Manager he is responsible for a number of projects in the wireless and mobility area. He participates in the TERENA taskforce on mobility.

References:

More information about the project, including links to external sources of information can be found at the SURFnet 802.1X page: http://www.surfnet.nl/innovatie/wlan/