802.1X Workshop

30-31 March 2004,

Amsterdam, TERENA Offices

Introduction

The workshop, organised by SURFnet and TERENA, was attended by about 20 people per day, coming from different countries, like Germany, the Netherlands, Hungary and the UK. Most of the participants were Dutch and there were a lot of representatives of the universities. Many universities in the Netherlands (like university of Twente) have already set up 802.1X.
The workshop aimed at providing an overview of 802.1X technology, and providing a practical introduction into setting up an 802.1X based infrastructure.

Why 802.1X: Klaas Wierenga, SURFnet

The morning of the workshop was dedicated to the theoretical foundations. The meeting was opened by Klaas Wierenga, who gave a general overview of the technology and explained why SURFnet adopted made a choice for 802.1X.

The first part of the presentation was dedicated to the requirements for a secure, scalable solution for access to (wireless) networks:

- identify users uniquely at the edge of the network
- allow for guest usage (users sometimes have already problems roaming between faculties inside the same university, let alone beyond that)
- scalability, meant that the solution must be easy to implement, even when scaling to possibly hundreds of thousands of users.
- easy to install and use
- operating system independent
- secure
- after the proper authentication there should be open connectivity (preferably no NAT, no firewall)

The second part of the presentation evaluated several authentication solutions against these criteria:

1) Open network = this solution is the easiest to implement and of course is the most insecure. There is no possibility for tracing the users.

2) Open network with MAC address filtering = MAC addresses provides some protection but can be spoofed and still it is hard tracing the users. Administratively a nightmare when scaling up.
3) WEP = This method is based on sharing a secret within a community. For small communities it works, but for large community it is hard to manage. The WEP key can also be cracked and changing the key (which would make the solution more secure) is hard as the new key should be distributed again among many users.
4) Open network + web gateway = This solution is quite scalable being based on web browser therefore no client software is required. It is hard to secure as packets can be sniffed, session could be intercepted to gather credentials unless a SSL is established to secure transfer of credentials, supported by a RADIUS backend, thus scalable.
5) Open network and VPN gateway = VPN is secure. The traffic is encrypted for each exchange of data, users need a VPN client and it is hard to scale with a large number of users. It requires VPN concentrators that can be expensive.

The third part of the presentation was dedicated to 802.1X, a solution that combines the security of the VPN-based approach with the scalability of the web-based approach.

802.1X is a layer 2 port based solution (it works for both wired and wireless networks) that authenticates over Ethernet between the client and the wireless access point / SWITCH. It uses EAP (Extensible Authentication Protocol) as the mechanism to carry credentials. Users do not get IP-connectivity until they have successfully authenticated.

The element that makes 802.1X attractive is the fact that several authentication mechanisms can be used with EAP. The backend used so far is RADIUS based, so there it is possible to use existing infrastructure. RADIUS communication is based on shared secrets, but other backends are being explored in the TF-Mobility task force (http://www.terena.nl/tech/task-forces/tf-mobility).

Because most of the security attacks work on layer 3 (IP layer) and 802.1X knows the users MAC address (layer 2) some work is needed to connect layer 2 and layer 3. Despite this 802.1X proves to be the best "future proof" of the network access methods described above.
At the moment Windows XP and 2000 and MacOS X have 802.1X built in. For most other platforms there are clients available.

A look inside 802.1X technology: Tom Rixom, ALFA & ARISS

Tom described the way 802.1X works in particular on the Windows platform. ALFA & ARISS developed an EAP-TTLS client for SURFnet.

Windows uses an EAP-API which installs in the system some DLLs to handle different authentication methods. EAP itself provides only a way to carry users 'credentials, but it doesn't provide any security. 802.1X controls port access at layer 2 by only allowing the sending and receiving of EAP messages via unauthenticated ports and passing them onto an authentication server.
EAP works in combination with various authentication methods which go from less secure like MD5 (username and password, no man-in-the-middle attack prevention) to TLS (based on client/servers PKI certificates, but it is hard to be used due to the difficulties of PKI). The most used method at the moment are TTLS and PEAP, which both use a TLS tunnel (built on layer 2) between the client and the server (RADIUS) and it is used to carry securely the users' credentials to the server. The RADIUS server uses a certificate to authenticate itself to the client; the client authenticates itself to the server by providing the credentials, thus not requiring a client certificate.
The RADIUS answer is sent to the access point.
The software developed by Alfa & Ariss, called SecureW2 uses the windows certificate trust hierarchy and the chain of certificates of the authentication server must be installed on the local computer (the software controls the user interaction via a pop up box in Win XP) prior to user authorization.

The server side of 802.1X: Paul Dekkers - SURFnet

Paul talked about the server side of 802.1X and in particular focused the start of his talk on the mutual authentication needed to have a secure solution.
Paul also talked about Wi-Fi clients and issues related to particular vendors and operating systems that have increased the complexity and support required for Wireless LANs.
Paul briefly ran through the step-by-step process for setting up a secure connection between client and access point by creating dynamic WEP-keys and the setup that ensures a secure tunnel from client to authentication server.
Paul then discussed the hands on session explaining the equipment, concepts and exercises that would be taking place in the afternoon.

Hands on workshop

In the hands on workshop there were five groups, each had a Radiator RADIUS server, a Cisco switch, a Cisco access point (the latter two provided by Cisco Systems) and a laptop and wireless card. The exercises were as follows:

1. Connect laptop to switch and configure VLAN.
2. Set up and configure RADIUS.
3. Configure access point and switch to use RADIUS.
4. Enable 802.1X on access point and switch.
5. Configure laptop with 802.1X client.

6. Enable trunking on access point and switch.
7. Configure VLAN assignment.
8. Configure RADIUS proxying.
9. Create a non –1X guest VLAN.

The hands on section was considered successful and instructive by the participants, who recommended more events like this.

Presentations, exercises and the streaming of the theoretical parts are available on-line at: http://www.terena.nl/tech/task-forces/tf-mobility/1x/