

Mobility Workshop
TERENA, Amsterdam
March 06, 2002

Meeting report by: Licia FLORIO, TERENA
March 12, 2002

Participants List

Carsten Bormann	Universität Bremen TZI
Valentino Cavalli	TERENA
Martin Dunmore	Lancaster University
Francis Dupont	ENST Bretagne
John DYER	TERENA
Licia Florio	TERENA
Avgust Jauk	ARNES
Ueli Kienholz	SWITCH
Jardar Leira	UNINETT
Marcin Michalak	University of Brussels
Saverio Niccolini	University of Pisa
Loutfi Nuaymi	ENST Bretagne
Juergen Rauschenbach	DFN-Verein
Steffen Rothkugel	RESTENA
James Sankar	UKERNA
Piotr Sasiedzki	Silesian University of Technology (POL-34)
Roland Staring	SURFnet
Magnus Strømdal	UNINETT
Egon Verharen	SURFnet
Klaas Wierenga	SURFnet

Introduction

Licia Florio of TERENA (who chaired) opened the meeting. She briefly described the TERENA interest in the mobility fields and the objective of the day.

The aim of the workshop was to explore what is going on in different NRENs and a possible cooperation at European level.

A possible way of cooperation could be cross-testing of the technology used in one NREN in other NRENs.

Presentation section

SWITCH by Ueli Kienholz

Ueli reported the results of a questionnaire sent to all the institutions in Switzerland, about the WLAN usage and their network set-up.

The questionnaire wanted to evaluate how the students can connect to the network on a guest campus with notebook/mobile device and how they can use their network services remotely and the local ones as well.

The main results of the questionnaire are:

- typically, separate network segments are built especially for access for mobile users,
- almost every university have fixed “publicly” accessible workstation,
- wireless access and pilot applications are almost at every place, but big areas are not covered yet,
- universities have plans to expand the coverage by 2002,
- technology is always 802.11b.

About the authentication and authorization of mobile users many concepts are in place at the individual universities, such as: SSH sessions, Session Intercept, IPSec (in this last case VPN connections must be set up from the wireless clients).

The universities are afraid of providing any services without authentication; but there is not a common solution for this, yet.

Questions:

1. How are the email services managed?

There are several possibilities to read own e-mails from another locations, e.g. web access with SSL.

2. What about the wireless LAN regulations in Switzerland?

It is allowed to use it outdoor, there is no special restriction, different from the French situation, where because of the strict laws, the wireless LAN use is not allowed outdoor.

In the Netherlands outdoor usage will be liberalized in a few months, in accordance with EU regulations.

Presentation available at:

<http://www.switch.ch/docs/mobilesurvey.pdf>

UNINETT by Jardar Leira

UNINETT have been working a lot on mobility technology, establishing a ‘PDA community’ (it is a working group) to cooperate and exchange ideas. The working group has been doing tests on Linux, mobility, GPS and VoIP.

UNINETT tested the WLAN and the vendors that can provide this technology as well. The tests were about performance, features, ease of use, security, compatibility and scalability.

The report will be available in English for the mobility community.

UNINETT have been working on some interesting projects. Some are best practice such as Security on WLANs, others are about PDA using, such as KOKOSNETT and a registration system for teachers on a PDA.

In the near future UNINETT would like to get proper working IP telephony (with live pictures and voice), a better IPv6 support and a wider use of the PDA systems (for instance they could be used as authentication for physical access).

A demonstration of the work that is being carried out in UNINETT, was the Jardar presentation through iPAQ with VGA adapter.

Presentation available at:

http://www.terena.nl/mobility/meet/UNINETT_Mobility_TERENA2002.ppt

SURFnet by Klaas Wierenga

Klaas briefly described the list of the current projects in SURFnet.

SURFnet have already an operational dial-in telephone network with which all students in the Netherlands can dial-in for local tariff to the SURFnet network.

The system is implemented with three steps of RADIUS-servers, one from the dial-in provider, another is a top-level server by SURFnet and another is present at each institution (an institution RADIUS-server).

The institution does the subscriber management.

SURFnet are working in order to extend this model using Wireless LANs. The idea is to have a similar system with Wireless LANs, meaning that when the users are at some SURFnet institution, regardless what institution they are coming from, they can use the wireless LAN for free.

Another option is to combine this wireless LAN structure with GPRS. The idea is that in the whole country a user could use paid GPRS, but as soon as there is a wireless LAN connection, the user could use this wireless LAN.

SURFnet is keen to provide the details in English. They would like to explore the possibility of having the dial-in and WLAN setup in other countries, so that a user could use local dial in-networks if he is in the country of another NREN and vice versa

Klaas asked for the Wireless network details in the other institutions to check how and where the test could be realized.

Questions:

1. Is RADIUS secure enough for the authentication? Wouldn't Diameter be better for this purpose?

Klaas answered that Diameter is still hardly deployed, because of complexity of configuration.

Presentation available at:

<http://www.terena.nl/mobility/meet/mobility-workshop.ppt>

University of Bremen, by Carsten Bormann

In Germany they are working on an inter-institution roaming infrastructure that would allow users from participating institutions to work at any other location, using their home access account.

Carsten presented the W-Bone project to interconnect the WLAN-VLANs present almost in every institution, to allow the users to get registered with the host institution, using their home account.

The insecure area is represented in this case by the WLAN access, but in this area the users can't access any local resources. Instead, the user has to use the VPN gateway at its home institution to access any resources outside the insecure WLAN-VLAN, including local resources at the visited location. This can guarantee a good security level.

The W-Bone project uses the WLAN Roaming exchange (WRX), an exchange point that maintains information for tunnel management and address/routing coordination.

W-Bone based roaming works in this way: before traveling the users registers their MAC addresses (one-time effort), and look up the SSID used by the destination network. An SSID is an identifier attached to the packets sent over the wireless LAN that can be used as a "password" for joining a particular radio network (BSS). All radios and access points within the same BSS must use the same SSID, or they can't talk. At the destination the users must configure their local services.

Question and remarks:

1. The solution seems good, but it is not scalable at European level and it's seems difficult to find an integration with other systems. The system is based on its own address management and it assumes the participating institutions organize a separate routing domain for the W-Bone.

Moreover such a model assumes that all the participating campus have to adopt the same solution. Carsten said that this solution tends to be called "standard architecture" in Germany because the institutions are increasingly adopting it. It would be worthwhile just to interconnect the "standard architecture" systems.

2. Do you use PKI for the authentication?

Carsten said that each institution will have a database that contains the users name and their passwords (the passwords are encrypted). So no PKI is needed on a global basis, each institution is free to do what they want.

3. SSID can't be used as an authorization method. It is not unique and can be easily figured out. It is a way of grouping wireless users so they access the same access point. Carsten said that SSID is used for legal reasons only: If closed 802.11b networks are used, you have to explicitly set your card to the SSID of a W-Bone participant; this constitutes a deliberate break-in in many national computer law systems. Other institutions use MAC addresses for this purpose, this creates the unfortunate requirement to collect them in the WRX.

Presentation available at:

<http://www.terena.nl/mobility/meet/wlan-2002-03-05-en.pdf>

Discussion session

The general discussion started trying to define what the mobility activity could be and what area could be deeper explored.

The group agreed on defining mobility as a way to have access anywhere at anytime (it could be either a service supposed to get suspended and to get restarted in other locations or a service continuously provided), with the support of mobility technology.

All wireless networks have two common security problems, authentication and privacy, that are still hard to solve.

Up to now the IPv6 protocol is still considered a research protocol. Some upper level applications are necessary to implement the authentication and authorization mechanisms for the users access.

The security problem is very serious and the WLAN security was discussed. The insecurity of WLAN plays an important role in the cross-institutional experiments. Some institutions like SURFnet, taking into account that this aspect is a serious problem, try to design architecture or a model based on WLANs that allows to add a stronger security policy, when requested.

Other institutions prefer to wait until the WLANs security will be improved and others, like Germany, prefer to use something else (instead of WLAN).

In a first moment the idea of designing a common architecture seemed to get consensus, but at the end the group agreed for a first documentation exchange.

Possible identified scenarios about the user access are:

1. Being around the world and get Internet access and then have access to services on own local network
2. Traveling around and getting access to the own information via a WLAN unsafe connection and then the user asks to be authenticated in his own network – not sure there is a solution for each case
3. Another problem is related to the way the information is presented; a user could work with laptop or PDA in another environments. It would be interesting having a sort of metadata, in order to adapt the information the devices.
4. It is not possible to move from GPRS to WLAN Ethernet without mobile IP. Many GPRS operators use the NAT addresses, and this creates communication problems. Many GSM operators will deploy NAT addresses to allow the communication between GSM and GPRS.

The common scenario is described below:

(1) Client	(2) policy enforcement point/	(3) policy decision point
Student-A	PEP-B	PDP-A

Here a student from university A (Student-A) wants to get access to the Internet at university B. University B restricts access at the Policy Enforcement Point (PEP-B) based on the credentials supplied by the clients. In order to get cross-organizational access the decision to let Student-A use the Internet, based on the credentials showing that Student-A is from university A, should be taken at the Policy Decision Point of University A. The university B in this case provides only the Internet access, but not the local resources access.

There are two main steps in this scheme, the connection from the client to the PEP and the connection between the PEP and the PDP:

- Client-A from university A requests access to the Internet at PEP-B, so the first problem is how to make this communication secure and what protocol should be used. WEP is not secure enough.
- PEP (installed on B) -> PDP (installed on A). The communication between PEP-B and PDP-A could be in a secure environment. Radius seems to be a possible candidate for this solution; turning it into a TRUST network. This solution has already successfully been deployed by SURFnet in their dial-in network, the Fibre-to-the-dormitory project and the GPRS-pilot.

Klaas thinks that university A should decide how much secure the authentication of student-A should be, as they are the only ones with a contractual relation with student-A.

Conclusions and action lists

- Cookbook about the set-up of a trust WLAN network. The cookbook should provide recommendations and set up things in order to avoid security problems and other pitfalls (in NL are deploying WLAN and many organizations ask SURFnet how to do it). SURFnet would provide the cookbook, by the **first week of June**.
- TERENA will maintain a web page with pointers to activities and information
- SURFnet and UNINETT will provide some basic documents to initiate a common activity, trying to identify the possible basic blocks in order to define later on a common architecture. The document will be available the **first week of June**.
- All the participants will provide the English documentation, describing their mobility projects as described:
SURFnet will provide the documentation in English about their GPRS project (**first week of June**)
SWITCH will provide documentation in English about their activities in the mobility area, by **first week of June**,
UNINETT are working on making a secure system. They will provide English documentation about this by **first week of June**,
POLAND (Piotr Sasiedzki) has plans about a countrywide access to research network. They will provide their local documentation in English, by **first week of June**.
- All the other participants are welcome to provide documents and URL.

The next Mobility meeting will be in Limerick on 2nd of June, 10.00 a.m.