

1st TF-Mobility Meeting

Date: 10 February 2003

Venue: Terena offices, Amsterdam

Attendees

Bormann, Carsten - Universitaet Bremen TZI

Sankar, James - UKERNA

Pollem, Niels - Universitaet Bremen TZI

Kienholz, Ueli - SWITCH

Keski-Kasari, Sami - TUT

Strømdal, Magnus - UNINETT

Leira, Jardar - UNINETT

Rauschenbach, Juergen - DFN-Verein

Kaskina, Baiba - TERENA

Chown, Tim - University of Southampton

Saywell, Mike - University of Southampton

Venaas, Stig - UNINETT

Wierenga, Klaas - SURFnet

Florio, Licia - TERENA

James Sankar - UKERNA

Apologies

Roland Staring - SURFnet (Roland is no longer part of the taskforce).

Erik Dobbstein - SURFnet

Introduction

Carsten Bormann chaired, together with James Sankar. The agenda was reviewed and it was agreed to reschedule the discussion section sequentially instead than in parallel. The approved agenda is appended below:

Agenda

10:00 – 10:10 Agenda bashing

10:10 – 10:20 Charter bashing, if any

10:20 – 11:45 **Short** reports

y10:20 – 10:40 UKERNA Survey (Mike Saywell)

y10:40 – 10:55 User Experience with Wbone (Niels Pollem)

y10:55 – 11:15 .CH update (Ueli Kienholz)

y11:15 – 11:25 .NL update (Klaas Wierenga)

y11:15 – 11:50 (open, coffee break)

11:50 – 11:55 Deliverable B: discussion

11:55 – 12:25 Deliverable C: overview, discussion

Lunch

13:30 – 16:30 Next Deliverables (D, E, F)

y13:30 – 14:15 Deliverable F: discussion

y14:15 – 15:15 Deliverable E: discussion

.15:15– 15:30 coffee break

y15:30 – 16:30 Deliverable D: discussion
y16:30 – 16:45 so what does this mean for G?
16:45 Wrapup, items J, K, L; next meeting
17:00 – open (Small editing groups)

Key points from the meeting

1.0 Final charter discussion and comments

The charter was reviewed, followed by a short discussion on the deliverables and timescales. All TF members agreed the following

- Deliverable G should state “Preliminary Architecture for Inter-NREN roaming” rather than “Preliminary selection for inter-NREN roaming”.
- Deliverable I should include “the implementation and evaluation of the recommended technical document for inter-NREN roaming”.
- Deliverables J, K and L are not dependent on Deliverable I, and a first draft of each deliverables should commence as soon as is practically possible.

2.0 Short reports:

2.1 Overview about UKERNA/ University of Southampton survey (Tim Chown)

Tim presented preliminary results of the UKERNA / University of Southampton Wireless LAN survey, whose aim was to provide the UK scenario regarding mobile technologies and their use. Most Wireless LAN users have adopted 802.11a or 802.11b followed by mesh radio and Wireless DSL. Most security implementations were based on MAC filtering (32%), followed by WEP (30%), followed by traditional Firewall / VPN (27%) and 802.1x / Dynamic WEP (11%). Six detailed site surveys are scheduled for February 2003.

The survey revealed some positive points, there were few interoperability issues (however cheap access points were problematic) and there were many VPN solutions available that could be used in both wired and wireless environments.

The negative points were that there was little confidence in WEP, whilst VPN, Bluesocket and 802.1x options were perceived as complex.

2.2 User Experience on the Wbone (Niels Pollem)

Five universities in Bremen have a shared Wbone using local VPN solutions (“deep security”) connected to a single router. Staff and students can roam across the five universities without changes to user configuration. 1500 users are registered; registration takes place at the home institution. A VPN gateway is required to gain access to/from the Wbone.

2.3 Update about the mobility project in Switzerland (Ueli Kienholz)

As a result of a SWITCH mobile survey (www.switch.ch/mobile/mobilesurvey.pdf) and a workshop, a draft architecture document was written to enable unrestricted access to VPN gateways so that Internet Access could be authenticated at the home network. All access is via VPN tunnels, the advantages and disadvantages are listed below

Advantages – Access to the Internet from home with the use of home resources, encryption, accountability and minimal administration costs.

Disadvantages – It is not an efficient method on the backbone, local resources at the guest network cannot be used, VPN equipment is expensive and the architecture is not good for supporting multicast.

There are scaling issues to overcome in updating Access Control Lists (ACL), SWITCH has tried to make the process more manageable by listing the details of approved administrators that manage VPN gateways so that any ACL requests can be made and updated. The alternative is to develop a PERL script to automate ACLs as can be done for Cisco routers with automatic email alerts to notify System Administrators. The issue is whether an automated approach will result in a loss of network access control.

2.4 SURFnet Update (Klaas Wierenga)

Activity 1 – SURFnet is using 802.1x with a TTLS module developed by a small commercial company to SMS message a one-time password to guest users for a limited duration. The University of Twente is rolling out a 600-access point wireless network with 802.1x with its 802.1x client for Win XP and Win 2000 (with latest service pack) and meetinghouse client for MAC and UNIX users. Amsterdam Polytechnic is using the same programme and is operational.

Activity 2 – A 1million Euro funded procurement exercise ends 10.02.03 to procure an 802.11b and 802.1x service to cover the Netherlands.

Activity 3 – A separate activity looking at WEP with 802.11b access to cater for non 802.1x users or other NRENs that use other authentication methods such as SSID or Orinoco APs with a webserver behind for granting access.

3.0 Discussion on deliverable B: Glossary of Terms (Carsten Bormann)

The glossary will be updated by Carsten Bormann and will include comments from the group. Licia Florio will take responsibility from Roland Staring to manage requested changes to the glossary. The update draft will be posted on 13th of February.

4.0 Discussion about deliverable C: Inter NREN roaming requirements (Carsten Bormann)

Carsten Bormann presented the first draft for this deliverable. All TF members agreed that a glossary of the common terms such as guest/visitor/foreign network should be standardised and defined to ensure all deliverables are written in a consistent way.

Key talking points included the following

1. What are the regulatory and legal issues that need to be addressed for WLAN Roaming (eg. National and European law, NRENs Acceptable Use Policies and Civil issues such as determining user accountability)? It may be best to principally abide by the home institution AUP where the access is granted by the home access, but this would restrict access to local resources on the “guest” network. One suggestion was to draw up a European NREN AUP.
2. Accountability is key to promptly stop abuse and identify the abuser. Both 802.1x and VPN require the support of Administrators to update tables.
 - a. Restricted Access using VPN – VPN can identify the home IP address but would have to deny access to that home VPN Gateway, restricting access to all these particular home users trying to access home from the guest network until the abuser issue is resolved.
 - b. Restricted Access using 802.1x – 802.1x can identify the guest IP address and match this with a home IP address by using an administrator table to match IP address and/or NAI in RADIUS if rules are followed to find a “person”.
3. The use of NAT should be discouraged, but as there are many people that use NAT, then the proposed solution should be able to allow them to plug in.
4. Carsten Bormann will update the Deliverable C draft with the TF comments and submit to the group for further comment.

5.0 Discussion about deliverable F: Inventory for a web-based solution to Inter NREN roaming (Sami Keski-Kasari)

Sami proposed the use of a LINUX box to deny non-local traffic and point to a http based web server for “guests” to enter a username and password to either a local or remote RADIUS server to authenticate the “guest” and allocate an IP address for accounting purposes. Dynamic WEP keys have low-level encryption and because the access is through Web browser there is no way to transfer WEP keys to the client as it is not defined neither in RADIUS, nor LDAP, nor HTTP protocol specifications. The restriction of this approach is then not the scalability, which is foreseen in the protocol specification, but it is in the method of authentication and protocols used for that, which implies that no guarantee can be provided to encrypt the user traffic. This means that with this solution it is possible to do authentication over HTTPS, so authentication information is encrypted but after successful authentication users must

encrypt their traffic by themselves if they want encrypted traffic (for example set up VPN tunnel or use ssh, https, imaps, etc.)

The process proposed is as follows (1) The Linux box at the guest network identifies a non- local user and brings up an authentication interface web page, (2) the user inputs the authentication details (note if this information is passed between RADIUS servers, this information is passed as clear text). (3) The username, password, IP address and MAC address is transferred.

This solution is easy to implement and requires no client software, however, it is not completely secure. This solution requires a LINUX box at all roaming locations. It may be possible to use SMS messaging to deliver a one-time password for guest use for a limited duration to overcome security concerns.

Other options include

- Establishing a SSH RADIUS authorisation connection
- Establishing a IPsec RADIUS AAA connection
- Access Controller links to VPN Gateways only for “guest” users; however there would be a scaling issue in managing and updating the ACL.

6.0 Discussion of deliverable E: Inventory for a VPN based solution to Inter NREN roaming (Ueli Kienholz)

Ueli has written a first draft based on the SWITCH model, differences identified in the Bremen VPN model and SURFNet 802.1x model will be included. TF members agreed that there were several approaches to solving the issues of deliverable E, either at the Access Controller Level (Access Point); the router or client software level. It was agreed that all options should be explored and the amount of effort and other trade offs should be identified and compared.

Building trust relationships between institutions and/or NRENs and getting administrators to update ACLs are key issues that may determine the success of WLAN roaming. The TF members acknowledged this is a hard task to achieve and the answer maybe either (1) travelling users unable to gain access due to outdated ACL information are pressured by these users to update the ACL or (2) A RADIUS server at the NREN level offers a national service and administers centrally on behalf of the institutions.

Ueli welcomes any ideas of how to update ACLs automatically.

Ueli would like details of any VPN based intercampus roaming examples in Europe.

7.0 Discussion of deliverable D: Inventory for an 802.1x based solution to Inter NREN roaming (Klaas Wierenga)

Klaas presented the deliverable on Erik's behalf that could not attend the meeting. Klaas will amend the TNC abstract to include the issues raised at this meeting by the 28.02.03.

Klaas will focus on TLS solutions using client and server based certificates and TTLS solution on server based certificates only.

Klaas is also looking at PEAP and MOBACS TTLS (an enhancement of TTLS using SMS messages for one-time only passwords).

There is an issue of where to have 802.1x, should it be on the Access Point or the switch behind it? If on the former Access Point costs are high. Security is only concerned with the Access control. Institutions or users have the option to enhance security end-to-end themselves. Example 802.1x configurations are available on the SURFnet website.

8.0 Discussion on deliverable G: Preliminary architecture for inter NREN roaming (James Sankar).

There are several options for AAA, the key areas are web-based, 802.1x or VPN / RADIUS. Each has different levels of security, cost, manageability etc. Any preliminary architecture must meet the needs of these options and the requirements as set out in deliverable C. Dual infrastructure is not an acceptable alternative.

9.0 Discussion on deliverable J (Jardar Leira)

A first draft of the WLAN product matrix will be ready by 03.03.03

10.0 Discussion on deliverables K (Jardar Leira)

A first draft of the WLAN product-testing document will be ready by 03.03.03

11.0 Discussion on deliverables L (Tim Chown)

Tim Chown will act as a channel between the mobility taskforce and IPv6 / MobileIP group and will update each group as appropriate.

Tim Chown and possibly Chris Edwards will produce an inventory of IPv6 / Mobile IP issues by August 2003.

12.0 Next meeting

The next meeting will take place at the Terena Networking Conference in Zagreb, Croatia on Sunday 18 May, from 10 a.m till 12.30

Summary of Actions:

Action		Deadline
3.1	CB will circulate the revised version of Deliverable B	13 Feb 03
3.2	LF will collect comments and will put it on-line	14 Feb 03
4.1	CB will circulate a draft for Del C	End of Feb 03
9.1	JL will circulate a draft for deliverable J	3 March 03
10.1	JL will circulate a draft for deliverable J	3 March 03
11.1	TC will circulate a draft fro Del L	August 03

Key:

CB= Carsten Bormann

LF= Licia Florio

JL = Jarda Leira

TC= Tim Chown