Mobile Ad-Hoc Wireless Access in Academia (MAWAA) Project

Towards Seamless Wireless Mobility for UK Academic Networks

Project Summary Report 2: Support for Roaming Access

Editor: Dr T J Chown

School of Electronics and Computer Science,
University of Southampton,
Southampton, SO17 1BJ, United Kingdom
tjc@ecs.soton.ac.uk

Version 1.0

30 June 2004

The MAWAA project was funded by the Joint Information Systems Committee (JISC)

Contents

1 Introduction

The subject matter of wireless networking is one of huge interest for academic (and other) institutions at the time of writing. The 2003 UKERNA Networkshop session on wireless LAN (WLAN) was the most popular session of the event, and that interst was repeated in 2004. A subsequent technical workshop [WAGCONF] filled with over 150 registered attendees in quick time. A recent UCISA "Top Concerns" exercise shows mobile (wireless) access and authentication issues in the top three positions [UCISA-TOP].

In this light, the support from JISC for this investigation into Mobile Ad-Hoc Wireless Access in Academia (MAWAA) has been very timely.

1.1 MAWAA project reports

In this series of three reports we describe the results of a year spent investigating current perceived issues with the deployment of wireless LAN networks in campus environments, with the technology available for such deployments, and with mechanisms that would allow users to roam as seamlessly as possible between such deployments.

The first report "Survey of Wireless LAN Usage and Issues" focuses on the results of formal and informal surveys and interviews with UK academic sites, presenting a summary of the issues that have been raised over the year since the first formal survey was conducted in Q1 2003. It also presents a summary of technical components for wireless LAN deployments and describes specific wireless access authentication methods.

The second report "Support for Roaming Access" explores how the main access control methods are suited to enable user roaming between wireless deployments. This work while undertaken within the scope of MAWAA has also been taken by Southampton into both the UKERNA Wireless Advisory Group [WAG] and also the TERENA Task Force for Mobility [TF-MOBILITY].

The third and final report "Deployment Experience" describes a deployment of wireless LAN made within the School of Electronics and Computer Science at the University of Southampton, using an 802.1x-based solution over a network of some 40 wireless access points.

A glossary of wireless LAN related terms can be found in Deliverable B of the TF-Mobility working group [TF-MOBILITY], and there is a useful resource of WLAN information at the UKERNA Wireless Advisory Group web site [WAG].

1.2 The need for roaming

This report focuses on the delivery of inter-site WLAN roaming, in particular in the academic inter-university context.

As more devices become mobile, staff and students will expect to be able to carry their devices with them, and use them when travelling. Many laptop and PDA devices now come with built-in WLAN. There is an expectation among users that they can use the WLAN resources of another university while visiting that university, be it a researcher at a workshop or a student attending a course.

We can only expect mobility requirements to grow. Thus the delivery of a scalable infrastructure to support inter-site roaming, or “location independent networking” as it is called by UKERNA, would be timely.

In this document we assess the four main access control mechanisms identified in Report 1 for their suitability for inter-site roaming.

2 Roaming Requirements

The first question to ask is what are the requirements for a roaming solution?

Here we present a candidate list of such requirements.

1. The solution should scale to the national and international scale. It should be capable of working between UK and European sites, or UK and Internet 2 sites, for example.

2. It should be easy to use for the roaming user, requiring at most a one-time set-up of client software, or even no client set-up at all

3. It should enable unique user identification.

4. It must clearly scale to support multiple sites and users

5. Authentication and authorisation should be performed by the user’s home institution.

6. Access is granted by the visited institution based on the home institution’s response to an authentication request.

7. It should be transparent to the user, as far as possible.

8. However, it may be desirable to alert the roaming user to local AUP information

9. There should be a low support cost (administrative overhead) for the visited and home institutions.

10. It should be an open standards-based solution

11. The solution should not add significant extra network latency for the roaming user.

12. The solution should be available for all common client platforms (Windows, Linux, BSD, MacOS/X, PocketPC, etc)

13. It should be cheap (or cost-effective) to deploy

14. Ideally it should (re)use existing infrastructure

15. The required security must be maintained for all partners in the process. There should be no spoofing opportunities, for example

16. The system should have accountability and an audit trail for authentication and usage.

17. IP-based authentication should work as intended (a roaming user should ideally not gain access to resources that they should not be entitled to). It should be noted however that IP-based authentication is a very weak system.

18. A site should be able to participate as a home institution or an institution supporting visiting users

19. The solution should be deployable at events such as conferences where there may be no home "institution" as such, but attendees are largely made up of roaming academic users.

20. The solution should also be applicable to wired Ethernet "docking points" at visited institutions.

These goals are in no particular order of importance, but should ideally all be met by the best solution.

2.1 Existing guidelines

The TERENA TF-Mobility [TF-MOBILITY] deliverables, in particular Deliverable G, describe the methods under consideration in the scope of the European National Research and Education Networks (NRENs). The work done under MAWAA fed into Deliverable G (as Southampton was a co-author).

The Wi-Fi Alliance has a document on requirements for roaming for wireless ISPs [WISPR], though there is no specific recommendation made.

GSM Association [GSMA] has a document on WLAN Roaming guidelines; they suggest web-redirection based technology now, moving to 802.1x as it becomes robust and widely supported, and possibly SIM-based EAP (given the GSM context).

There is an Inter-WISP roaming guide by Wirlab [WIRLAB], which focuses on 802.1x.

The work of the TERENA Task Force for Authentication, Authorisation Coordination in Europe is also relevant [TF-AACE].

3 Web-redirection

In this section we consider the appropriateness of the web-redirection based access control method for supporting roaming wireless users.

3.1 Overview

The general principle of web-based redirection access control is that a device cannot access external resources to the WLAN until the user attempts to access any external web page. At this point they are redirected to an authentication page where they must authenticate to then be granted access through the WLAN external gateway (see also Report 1, section 3.5).

The potential for roaming lies with the RADIUS transport used for authentication. If the user is local, authentication may be done against the local authentication back-end. If the user is roaming, the RADIUS request can be referred towards the home institution, either directly, or (for better scalability) via a hierarchy of RADIUS proxies as described in Section 7 below.

3.2 Advantages

The web-redirection method has the following advantages:

- It does not require any intelligence in access points or Ethernet switches; thus cheap access points may be used
- The system is already widely deployed by many commercial WISPs.
- Multiple authentication methods may be easily used, e.g. login against database credentials, use of a “scratch card”, or via SMS exchange [WHISPA]
- There is a good range of commercial and open source solutions available, e.g. Bluesocket, Vernier, NoCatAuth, etc.
- The RADIUS backend opens up the possibility for remote RADIUS referrals for roaming support
- The access policy can be fine-tuned on the firewall, depending on the RADIUS response to the user credentials (role-based access)
- Only a web browser is required on the client device
- The web page for the authentication challenge can highlight the local AUP to the visiting user
- A VPN can be run after authentication succeeds, if the local visited site policy allows it

3.3 Disadvantages

The web-redirection method has the following disadvantages:

- The use of DHCP means that spoofed gateway addresses or other IP information may be returned, allowing bogus authentication pages to be presented to the user, from which username and password details might be harvested. Such a weakness may be important where a roaming user is using their home credentials. Most users would not check the SSL certificate on the authentication server. A secure authentication mechanism must provide mutual authentication of both parties. None of the DHCP/WWW based login products provide this at present.
- Any devices without (SSL) web clients cannot gain access (though this would be unusual).
- There can be some problems detecting detachment of devices (this is more of an issue in an environment where network access is charged for).

- The lack of encryption with the basic authentication scheme means that a VPN or other Layer 3 or above encryption method is desirable

- The user appears to be at the visited site; thus IP-based authentication to, for example, bibliographic resources will work when it may not be meant to.

4 Restricted VPNs

In this section we consider the appropriateness of the restricted VPN based access control method for supporting roaming wireless users.

4.1 Overview

In a restricted VPN environment, a user device is granted access to the local WLAN and given IP settings via DHCP. The user cannot access any external infrastructure except for the local site's VPN server; a firewall blocks all other access. Thus the user cannot access external resources until they authenticate to their VPN service (see also Report 1, section 3.4).

To scale this method up to allow inter-site roaming, the WLAN gateway/firewall at each participating site must only allow access to the IP addresses of participating VPN site gateways. This implies the controlling firewall must maintain a (potentially long) list of valid remote VPN gateway IP addresses in its access control list (ACL), and a means to manage and (automatically) update this list is required.

4.2 Advantages

The restricted VPN method has the following advantages:

- It does not require any intelligence in access points or Ethernet switches; thus cheap access points may be used

- Most sites run a VPN service already, so this method reuses existing infrastructure

- The use of VPN gives client device encryption at Layer 3, thus no Layer 2 encryption (WEP) is required

- Laptops built in 2003 or later are capable of encrypting IPsec streams of more than 20 Mbit/s, for example. Typically, bandwidth is thus limited by the wireless network throughput rather than by CPU performance.

- The user's home (external access) security/firewall policy is applied, rather than that of the visited site.

- The user appears to be at their home site; thus IP-based authentication to, for example, bibliographic resources will work.

4.3 Disadvantages

The restricted VPN method has the following disadvantages:

- Client VPN software is needed on the user device. Most devices now ship with such support, including the newer PalmOS PDAs.

- VPN processing on PDAs may be slow.

- The home site VPN server must be able to handle all the traffic of all its concurrent home and roaming wireless users, which may be a significant extra loading. Thus additional VPN servers may need to be deployed, or bandwidth throttling may need to be applied to roaming user sessions. The use of 802.11a/g adds extra bandwidth demands on the home VPN servers.

- Maintaining the VPN “exception” list for participating home VPN gateways is a significant administrative task. It may be possible to use a “controlled address space for gateways” (CASG) such that each NREN allocates VPN addresses from a fixed IPv4 address pool (a /22 would offer 1,024 gateways) such that any given WLAN gateway firewall would only need to have filters for each NREN prefix (perhaps 30 fixed prefixes). Such a solution places complexity in the routing infrastructure however, by adding host routes to the NREN’s network. Alternatively, such VPN gateways could be maintained in the DNS, e.g. such that vpn.ac.uk would only have to contain CNAME pointers to the canonical records, e.g. "universityx.vpn.ac.uk" would first resolve to "staff-vpn.universityx.ac.uk" and then resolve to an IP address (thus institutions could change the network address of their VPN server without informing their NREN).

- Exposing a list of known VPN servers may be a security risk, if some generic flaw is discovered in a common VPN server product.

- All traffic from the roaming user must go via the home VPN server

- Unless a site uses RFC1918 addressing on its WLAN network, it will need one global IP address per potential “docking” device and one VPN IP address per (home or roaming) connecting device.

- Some sites will use NAT, which may cause problems for establishing VPN sessions.

- A fixed firewall limit on which VPN servers may be reached denies a roaming business user (or other non-participating roaming user) from being able to VPN home.

- VPNs often have no security between the roaming node and the home network, thus viruses/worms may spread to the home network if picked up in the remote network (though this is also problem for home users using VPN, where a virus from Hotmail for example may be propagated to the home network).

5 802.1x

In this section we consider the appropriateness of the 802.1x based access control method for supporting roaming wireless users.

5.1 Overview

The 8021.x authentication protocol is designed for Layer 2 port-based authentication. Initially a device will have no Layer 2 access to the network beyond the local access point or Ethernet switch port. A client device (the “supplicant”) initiates an EAP request over 802.1x to the authenticator (usually a wireless access point) which in turn will relay the request via RADIUS to an authentication back-end. If the request is successful, the device will then be admitted for Layer 2 communications by the access point or other authenticator, e.g. by being added to a given VLAN (see Report 1, section 3.6).

As with the web-redirection scheme, the potential for roaming lies with the RADIUS transport used for authentication. If the user is local, authentication may be done against the local authentication back-end. If the user is roaming, the RADIUS request can be referred towards the home institution, either directly, or (for better scalability) via a hierarchy of RADIUS proxies as described in Section 7 below.

5.2 Advantages

The 802.1x method has the following advantages:

- The RADIUS backend opens up the possibility for remote RADIUS referrals for roaming support

- Includes encryption in the wireless access point, which is able to encrypt at the wire(less) speed. There is thus no encryption bottleneck as there may be with a VPN solution.

- A VPN may be initiated once the Layer 2 authentication is completed, if the local visited site policy allows it

- 802.1x support, including for the various popular EAP types (TLS, TTLS, LEAP and PEAP) is now quite widely available in clients (“supplicants”), access points (“authenticators”) and RADIUS servers.

5.3 Disadvantages

The 802.1x method has the following disadvantages:

- It requires 802.1x and appropriate EAP support in clients, access points or Ethernet switches, and the RADIUS server.

- Some clients are currently only available via commercial solutions.

- 802.1x capable access points are expensive, but prices are falling as the technology matures

- 802.1x is still just transitioning from bleeding edge to leading edge at the time of writing

- The user appears to be at the visited site; thus IP-based authentication to, for example, bibliographic resources will work when it may not be meant to.

6 Roamnode

In this section we consider the appropriateness of the Roamnode based access control method for supporting roaming wireless users.

6.1 Overview

The Roamnode system was developed at the University of Bristol [ROAMNODE]. Its basic principle is that the physical and logical connectivity to the network are split. A client device authenticates to a local roamnode on the WLAN by using PPPoE which invokes a RADIUS referral to the home roamnode and its user authentication backend. If successful, a temporary IP-in-IP tunnel is established back from the local roamnode to the home roamnode, over which a subsequent PPTP VPN session may be established.

As with the web-redirection and 802.1x schemes, the potential for roaming lies with the RADIUS transport used for authentication. If the user is local, authentication may be done against the local (home) roamnode's authentication back-end. If the user is roaming, the RADIUS request can be referred towards the user's home roamnode, either directly, or (for better scalability) via a hierarchy of RADIUS proxies as described in Section 7 below.

6.2 Advantages

The Roamnode method has the following advantages:

- It does not require any intelligence in access points or Ethernet switches; thus cheap access points may be used

- The RADIUS backend opens up the possibility for remote RADIUS referrals for roaming support

- The access mechanism abstracts physical connectivity from logical connectivity

- Users are protected from each other by encryption; PPPoE creates PPP sessions that separate clients into separate Layer 2 interfaces, forcing all traffic to go through the PPP gateway. The client device may also not need to posses an addressable IP interface (instead a virtual interface can be used).

- It has support for bandwidth management per user via RADIUS attributes, if required to throttle the VPN load, and prioritisation for local over remote users.

- Because they are using a VPN, the user appears to be at their home site; thus IP-based authentication to, for example, bibliographic resources will work.

- PPPoE relieves the problems of DHCP spoofing. Only a cryptographic hash of the user's password is passed to the local roamnode, and not the password itself. Therefore, it is not possible to acquire credentials of users by sniffing the network, or by a malicious third party masquerading as a trusted authenticator. The local roamnode also authenticates itself to the client device by passing it a second hash returned from the user's authentication server. The client device will not establish the connection to the local roamnode unless the hash is correct. Thus trust is established in both directions (unlike the weaker web-redirection method).

- An 802.1x or web-redirection user may also set up a VPN to their home site, but may have problems if NATs or other restrictions prevent that (e.g. firewall filters). A roamnode user however must set up a VPN back to their home site's roamnode.

- The use of VPN gives client device encryption at Layer 3, thus no Layer 2 encryption (WEP) is required

- Laptops built in 2003 or later are capable of encrypting IPsec streams of more than 20 Mbit/s, for example. Typically, bandwidth is thus limited by the wireless network throughput rather than by CPU performance.

- The user's home (external access) security/firewall policy is applied, rather than that of the visited site.

6.3 Disadvantages

The Roamnode method has the following disadvantages:

- All traffic from the roaming user must go via the home VPN server

- Roamnode sites must coordinate their allocations of RFC1918 address space

- A PPPoE client is required on client devices. Vendors have to date only implemented PPPoE in desktop/laptop operating systems. There are not, at the time of writing, any PPPoE clients for wireless PDA devices, although Bristol recently announced that a development deal for such a client had been secured.

- A PPTP VPN client is required on client devices. Most devices now ship with such support, including the newer PalmOS PDAs.

- VPNs often have no security between the roaming node and the home network, thus viruses/worms may spread to the home network if picked up in the remote network (though this is also problem for home users using VPN, where a virus from Hotmail for example may be propagated to the home network).

- The architecture requires an IP-in-IP tunnel over which a VPN (a second layer of tunnelling) is run.

It should also be noted that the support for Roamnode depends on a small, dedicated team at the University of Bristol. However, there are several examples of other uch successful projects, e.g. the Radiator development, or Mailscanner.

7 Towards a roaming solution

In this section we review the ongoing activities towards wireless roaming, and suggest potential avenues to move forward towards an international solution.

7.1 UKERNA Wireless Advisory Group

The UKERNA Wireless Advisory Group [WAG] is studying a range of issues related to wireless networking, some outside the scope of 802.11a,b,g. However, some work is being done in roaming architectures.

At the time of writing the 802.1x and Roamnode solutions seem to be favoured, both sharing a common RADIUS authentication transport back-end.

The results of the MAWAA work are now being taken on board in the UKERNA Location Independent Networking trial [LIN], which is prototyping a scalable RADIUS referral infrastructure during the second half of 2004.

7.2 TERENA TF-Mobility Working Group

The TF-Mobility WG has produced many deliverables [TF-MOBILITY]. It also has brought together many European NRENs with a diverse set of already-deployed access mechanisms that have some consideration for scalable roaming support.

SURFnet has deployed an 802.1x [SURFNET] trial between half a dozen Dutch sites. To date the trial has been successful, although some teething issues still remain with particular 802.1x clients. A mixture of EAP-TLS (for administrative staff) and EAP-TTLS (for other users) has been deployed.

SURFnet has also set up the infrastructure to test hierarchical RADIUS referrals, as illustrated below in Figure 7-1. This testbed includes the University of Southampton. The proposal for a common RADIUS hierarchy between European NRENs is expanded in a later section below.

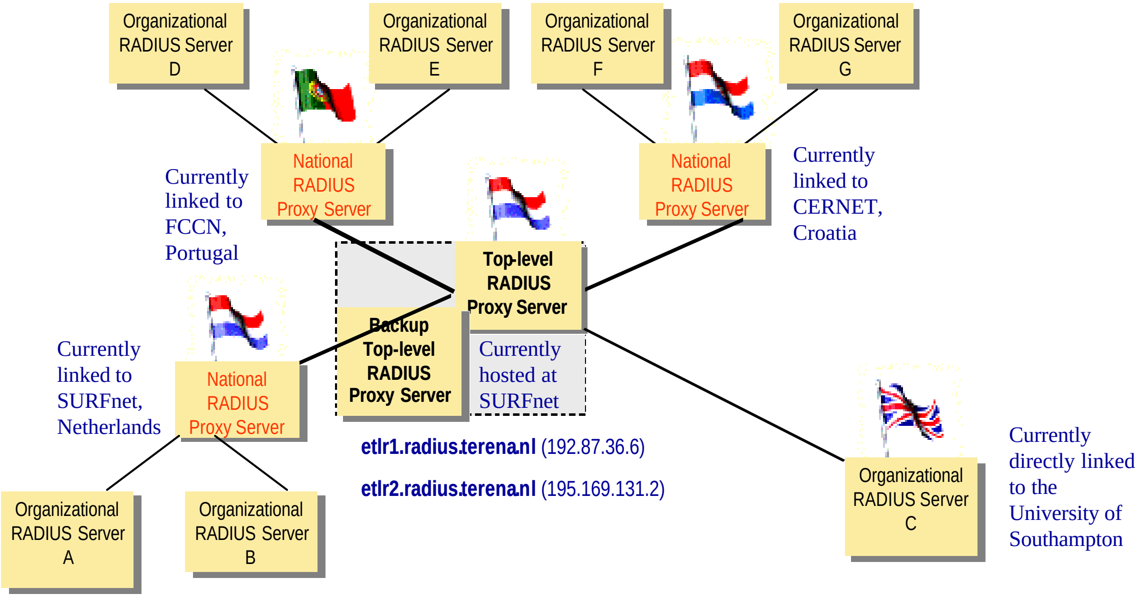
Organizational RADIUS Server D
Organizational RADIUS Server E
Organizational RADIUS Server F
Organizational RADIUS Server G
Currently linked to FCCN, Portugal
National RADIUS Proxy Server
National RADIUS Proxy Server
Currently linked to CERNET, Croatia
Top-level RADIUS Proxy Server
Backup Top-level RADIUS Proxy Server
Currently hosted at SURFnet
Currently linked to SURFnet, Netherlands
National RADIUS Proxy Server
etlr1.radius.terena.nl (192.87.36.6)
etlr2.radius.terena.nl (195.169.131.2)
Organizational RADIUS Server C
Currently directly linked to the University of Southampton
Organizational RADIUS Server A
Organizational RADIUS Server B

Figure 7-1: RADIUS hierarchy under test within TF-Mobility WG

The Swiss NREN SWITCH has set up the SWITCHMobile [SWITCH] roaming testbed, between (the small number of) Swiss universities. This is a classic restricted VPN deployment, where each WLAN gateway device contains a manually configured ACL with the addresses of the other participating SWITCHmobile VPN servers, as shown for two sites in Figure 7-2.

The system uses DHCP for local address assignment, the same 802.11b SSID everywhere, has no mandatory use of layer 2 protocols (like WEP) and no local authentication required as long as a user solely wants to establish a VPN connection with the VPN gateway at their home site.

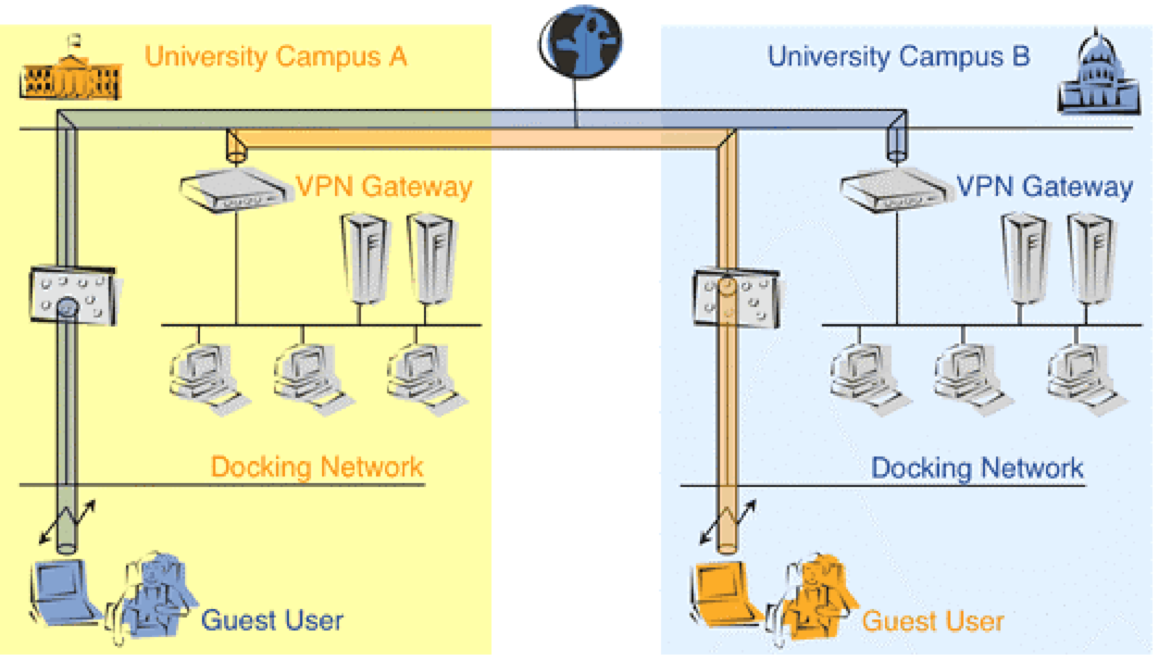

Figure 7-2: SWITCHmobile

The public access roaming system in Finland [FUNET] uses web-redirection. The Finns have tried a number of open source web-redirection systems. Roaming has been tested using RADIUS referrals between the Wirlab and TUT sites. The trials have been reported in a TNC2003 paper [TNC-ROAM].

The solution in Bremen, Germany is the Wbone [WBONE]. Here, the docking networks of five universities are given private RFC1918 IP address space and are interconnected by permanent IP-in-IP tunnels across the German research network, a mesh that forms the Wbone. A node docking in any site WLAN can access their home VPN gateway via the Wbone.

The Wbone is not a particularly elegant or scalable solution. The alternative use of CASG (controlled address space for gateways) for restricted VPN deployments has been suggested, whereby each VPN gateway in an NREN network takes its IP address from a pool allocated by the NREN for its own universities' VPN gateways. Such allocations mean that WLAN gateways only need the prefix ranges of 30 (or so) NREN prefixes in their ACLs, rather than one IP address per VPN gateway. This solution however has impacts on NREN networks, forcing the use of host routes.

The Portuguese NREN, FCCN, has implemented a small IPsec VPN pilot with both client and server certificates [FCCN]. The use of client certificates is often problematic due to the deployment and management problems of a full PKI. In this deployment, short-lived, non-signing certificates are used. The testing is in its early stages.

The overall feeling in the TF-Mobility WG is that the common usage of RADIUS for authentication transport by 802.1x, web-redirection and Roamnode suggests that the creation of a pan-European RADIUS referral hierarchy may be a useful infrastructure initiative to support user roaming. In parallel, work should be undertaken on understanding how the restricted VPN solution can be made to scale. This plan is illustrated in Figure 7-3.

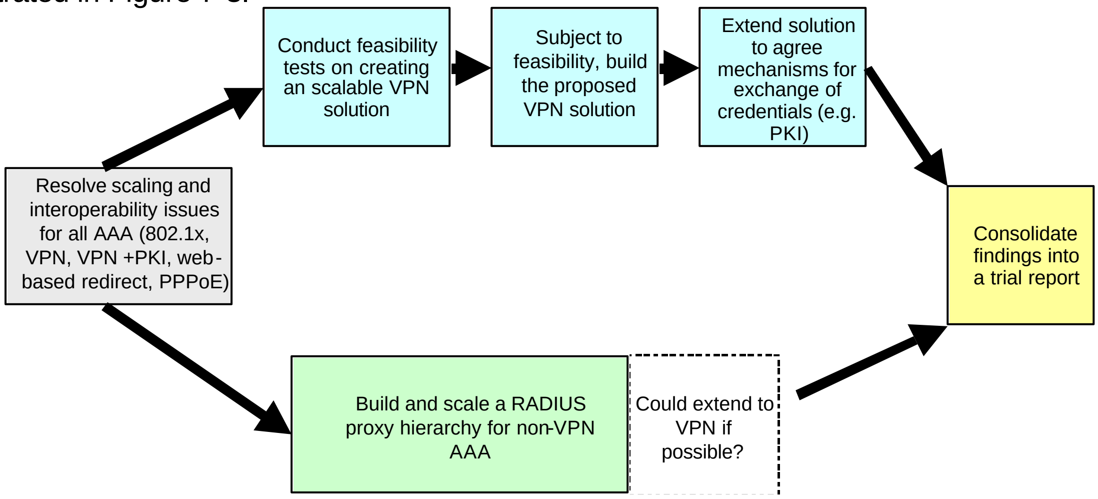
Resolve scaling and interoperability issues for all AAA (802.1x, VPN, VPN +PKI, web-based redirect, PPPoE)
Conduct feasibility tests on creating an scalable VPN solution
Subject to feasibility, build the proposed VPN solution
Extend solution to agree mechanisms for exchange of credentials (e.g. PKI)
Consolidate findings into a trial report
Build and scale a RADIUS proxy hierarchy for non-VPN AAA
Could extend to VPN if possible?

Figure 7-3: Future workflow for TF-Mobility WG

7.3 Comparison of methods

Here we begin by assessing each of the four main solutions for scalable roaming against the criteria cited in the first section of this report.

Requirement	Web	VPN	802.1x	Roamnode
The solution should scale to the national and international scale.	Y	?	Y	Y
It should be easy to use for the roaming user, requiring at most a one-time set-up of client software, or even no client set-up at all	Y	Y	Y	Y
It should enable unique user identification.	Y	Y	Y	Y
It must clearly scale to support multiple sites and users	Y	?	Y	Y
Authentication and authorisation should be performed by the user's home institution.	Y	Y	Y	Y
Access is granted by the visited institution based on the home institution's response to an authentication request.	Y	Y	Y	Y
It should be transparent to the user, as far as possible.	Y	Y	Y	Y
it may be desirable to alert the roaming user to local AUP information	Y	N	?	N

There should be a low support cost (administrative overhead) for the visited and home institutions.	Y	Y	Y	Y
It should be an open standards-based solution	Y	Y	Y	?
The solution should not add significant extra network latency for the roaming user.	Y	N	Y	N
The solution should be available for all common client platforms (Windows, Linux, BSD, MacOS/X, PocketPC, etc)	Y	Y	Y	N
It should be cheap (or cost-effective) to deploy	Y	Y	?	Y
Ideally it should (re)use existing infrastructure	N	Y	N	N
The required security must be maintained for all partners in the process. There should be no spoofing opportunities, for example.	?	Y	Y	Y
The system should have accountability and an audit trail for authentication and usage.	Y	Y	Y	Y
IP-based authentication should work as intended (a roaming user should ideally not gain access to resources that they should not be entitled to).	N	Y	N	Y
A site should be able to participate as a home institution or an institution supporting visiting users	Y	Y	Y	Y
The solution should be deployable at events such as conferences.	?	?	?	?
The solution should also be applicable to wired Ethernet “docking points” at visited institutions.	Y	Y	Y	Y
Clear “Yes” count	16	15	15	14

The chart suggests that there is no clear winner when we compare the functionality against the original requirements list. However, some features, like “must provide the required security” has many aspects, and not all requirements are equal (and there may be no consensus on which requirements are the most important for any given site).

If we look at the list of advantages and disadvantages per method, then the Roamnode solution appears to have the most advantages, but is not without its drawbacks, including the requirement for all VPN traffic to route via the homenode, the need to establish IP-in-IP tunnels and manage a pool of RFC1918 address space, and not least the current lack of PPPoE support in PDAs (though this looks set to be addressed in the future). The development team is small, but there is no reason to believe it cannot continue to support the project well.

The 802.1x solution appears to have good potential, but is still just arguably not quite ready for prime time. It is not far away though, and is worthy of pursuit. With the use of EAP-TLS, 802.1x is very secure, though EAP-TTLS is a better compromise between security and convenience, while still being secure enough. We comment on our 802.1x deployment experiences in Report 3.

The web-redirection system is perhaps simplest, but does have a potentially big security concern over the reliance on DHCP as part of the authentication scheme. It has the advantage of early widespread hotspot deployment, as well as a growing foothold in the academic market.

The restricted VPN solution is able to reuse existing VPN services, but has some challenges to overcome before it can be shown to be demonstrably scalable (e.g. through trials of the CASG concept). As with Roamnode, users may wish to use VPN to access their home networks anyway, but may be less happy to have other traffic routed via the home network too.

7.4 A RADIUS hierarchy for roaming support

The common feature of the web-redirection, 802.1x and Roamnode solutions for roaming support is the use of a RADIUS transport for the authentication exchange and associated credentials and responses.

Most sites will already have a RADIUS server deployed, e.g. to support dialup (which was the original purpose of the RADIUS protocol). However, such servers may not support all desired EAP types (e.g. MS IAS does not have the same breadth of feature support that Radiator does).

This suggests that a RADIUS referral relationship between the participating sites supporting a roaming infrastructure would be beneficial, such that non-local authentication requests (for users outside the local realm) can be referred to the user's home site RADIUS server for processing.

The question then is how to structure these referrals. One possibility is for each participating site to have a RADIUS trust relationship with each other site that it wishes to share roaming capability with. In a more commercial setting, such a selective relationship may be appropriate. However in an academic setting, where each university falls under the auspices of a NREN, and universities have a mutual interest in collaboration, it would seem appropriate to refer RADIUS requests to a national (NREN managed) "clearing house" from which referrals could be directed to the home sites. Thus each university would have a RADIUS relationship with its NREN, and any referral between two universities would pass through the NREN's RADIUS proxy.

A hierarchy adds an extra referral and also an extra point of failure, but makes scalability much easier to deliver. Each site only needs to set up one trust relationship to its NREN, and is then capable of supporting roaming to all other national universities under its NREN. This architecture means that all universities would implicitly trust all other universities. If a university chooses not to "peer" with a specific other university, it can then opt to not forward RADIUS requests for that realm to the NREN proxy.

This hierarchy can be scaled internationally, by having a European RADIUS "clearing house" proxy service between NRENs. This enables roaming between users at different universities in different countries.

This hierarchy does not support the restricted VPN roaming solution. This implies that a separate avenue is required to enable restricted VPN scaling; the Roamnode is one such path, the exploration of deployment of CASG is another.

The RADIUS proxies would need to support RFC2865 and RFC2866, and be able to forward the desired EAP types. As described in Report 1, most RADIUS servers, with the exception of MS IAS, would be able to perform this role. In the SURFnet trials, Radiator [RADIATOR] was selected based on its feature set, open (Perl) code and pricing.

The establishment of such a RADIUS hierarchy may also enable other services to be shared, outside the WLAN roaming scope, where RADIUS lookup is available.

TERENA TF-Mobility [TF-MOBILITY] Deliverable G specifies the requirements on RADIUS functionality for site servers, and for NREN and European proxy servers.

7.5 RADIUS usernames and realms

One property of the hierarchy is a requirement to have a common, but generalised, realm naming scheme. E-mail style realms could be used, e.g. universityx.ac.uk could be the common realm format in the UK, or universityx.nl for Dutch universities. Username formats would be a per-site issue.

Thus the username part can have any format, the realm fragment should sit within the home site's DNS namespace.

The RADIUS reply would allow a querying site to distinguish between users who authenticate locally or remotely, and based on that property place the user into an appropriate VLAN (e.g. one more trusted for internal users, or with greater external connectivity restrictions for visitors).

7.6 Securing RADIUS communications

There are a number of documents that suggest best practice to secure RADIUS communications, e.g. the O'Reilly RADIUS text [OREILLY], including.:

- Configure RADIUS clients and servers to use IPSec with ESP with 3DES;
- Use computer-generated shared secrets consisting of a random sequence of at least 32 hex digits or 22 printable characters;
- Use a different shared secret for each RADIUS client-server pair;
- Require the use of the message-authenticator attribute for all access-request messages, with cryptographically strong values;
- Lock out an account at the home authenticator after a set number of failed authentications (though this has a DoS implication).

The use of IPsec may be excessive, as any sensitive attributes, including the password, should already be encrypted by use of appropriate shared secrets. There is some literature that suggests IPsec in this context can help prevent DoS attacks, but such attacks against academic services are rare.

Another issue here is that access points do not generally support IPsec, so the IPsec could only be applied between universities and NRENs, which is usually running over a reasonably secure infrastructure path (compared to the access point to university RADIUS server path). End-to-end IPsec can thus only be considered when the access point vendors support the functionality, and IPsec vendor interoperability is well proven.

Existing RADIUS deployments use a shared secret, and are not widely reported to be problematic. However, it seems prudent to study possible attacks on the shared secret. One suggestion here is that a deployment ensures that RADIUS clients and proxies use genuinely random Request Authenticators and that RADIUS proxies and servers enforce the use of Message Authenticators. Using unique, randomly generated secrets for each university-NREN RADIUS “peering” is a sensible measure. Such secrets could also be replaced or changed periodically.

The bottom line is perhaps that it is impossible to guarantee that an authentication request is coming from the genuine owner of the credentials. This would be the motivation for account lock-out after a number of failed requests, but that would have to be balanced against the DoS implication.

7.7 RADIUS accounting

Accounting messages should always be sent to the home RADIUS server. The proxies can also store that information, but if they do so the data protection implications must be followed.

RFC2866 describes the accounting statistics that can be gathered, which include username, IP address, session duration and volume of data transferred (in or out).

8 Roaming Policy Issues

In this section we discuss the responsibilities for the various parties in the roaming hierarchy. This work is being pursued now in the context of the UKERNA WAG [WAG] activities.

Ultimately if the trust relationships breakdown there are sanctions that can be applied; a visited site can block referrals on a per-site basis, or the NREN proxy could revoke roaming rights on a per-site basis. A home site could block authentication on a per user basis.

An interesting issue is whether a common SSID should be used across all sites supporting roaming. While this may be good for publicity and user awareness of an available roaming infrastructure, it raises the possibility for rogue access points to easily be set up to trick users into potentially giving credentials to an attacker. Some consideration is required for how best to alert a user to the genuine presence of a roaming service.

8.1 Users

Users should abide by the AUPs of the visited site, their home site (if the roaming method relies on connectivity back to that site) and the JANET and any regional network AUPs.

A problem for a roaming user is how they are alerted to, or can discover, the AUP of the visited site. If the roaming authentication is 100% seamless, the policy cannot be highlighted (e.g. as it might be on the authentication web page of a web-redirection service).

It may be the case that most universities have similar AUPs, but some may be influenced by local limitations, e.g. an FE college with a 2Mbit/s leased line will be more bandwidth conscious than a university with a 1Gbit/s uplink.

A VPN solution will mean that the user is in effect connecting to external sites via their home site, and thus their home AUP applies. However, if the local site has bandwidth related AUP conditions, these will also apply, so the AUP is never a solely home site issue for VPN users (i.e. for the restricted VPN or Roamnode solutions).

The user should also act immediately on requests by administrative staff from the visited or home organisation, and must be responsible for the use of their credentials. Users should not offer their credentials for use by other users, for example.

8.2 Sites

The home site should make its users (home and visitors) aware of its AUP and roaming conditions, and ensure the AUP is adhered to.

The home site should provide support for its users, e.g. installing one-time software for roaming capability such as 802.1x clients where required. It is also responsible for the actions of users it authenticates, whether local or remote.

A site should liaise with the NREN for RADIUS proxy trust set-up and ongoing maintenance.

Sites must log accounting information, in particular the assignment of IP addresses and authenticated user credentials, and visited sites should make these and related logs (e.g. web proxy accesses) available to the home site when requested to do so, subject to the provisions of the Data Protection Act and RIPA.

Any reports of misuse at the visited site should be forwarded promptly to the home site.

A site supporting roaming should ensure that roaming systems are configured, maintained and operated securely, so as not to put the security of other sites or their users at risk.

8.3 Central (national) RADIUS server

The national (NREN) RADIUS proxy should configure its trust relationships with each participating site in a secure manner (see Section 7 above). It must protect the security of participating sites and the system as a whole.

Any logged accounting information should be made available to home or visited sites as appropriate.

9 Conclusions

In this report we have reviewed the main four available solutions for WLAN site authentication and access control for their appropriateness for deployment in an inter-site wireless user roaming context. Those access control methods are:

- Restricted VPN
- Web-redirection

- 802.1x
- Roamnode

We have proposed a set of general criteria for evaluating the appropriateness of these available mechanisms.

However, it is not clear from the review which of the methods has a distinct advantage. Each has relative strengths and weaknesses. The web-redirection method has the advantage of an early deployment foothold, if only in the single site (non-roaming) scenario.

The clear commonality between the methods is the use of a RADIUS transport for authentication by the 802.1x, Roamnode, and web-redirection methods. This strongly suggests that rather than favouring a single solution, a RADIUS infrastructure should be deployed between participating roaming sites to enable trust (peering) relationships.

The most scalable way to deliver the RADIUS referrals between sites is via a hierarchy with national (and European) proxies brokering trust between the universities and NRENS (and between the NRENs via a central European RADIUS proxy service).

In Report 3 we describe the results of experiments with such a RADIUS hierarchy, conducted between Southampton and other sites including SURFnet.

The deployment of a pan-European restricted VPN roaming solution is problematic, because the nice scaling property of the RADIUS hierarchy is not available, and the requirement to maintain lists of participating home VPN server IP addresses in each participating home site WLAN gateway firewall ACL is problematic. While there are proposals to reduce the scale of this problem, e.g. by use of controlled address space for gateways (CASG), it is a not insignificant challenge.

The two thrusts for the roaming support are thus the deployment of a RADIUS hierarchy, and the exploration of scalable VPN gateway solutions. The RADIUS solution appears the more promising solution at this time.

In terms of specific methods, the web-redirection system probably has the deployment head start, but has some disadvantages, including potential security exploits due to DHCP and gateway spoofing (although reports of such exploits are yet to emerge).

The longer term solution, and cleanest solution, seems to be 802.1x, once the vendor support (in particular built-in to operating systems as it is now with MacOS/X) is hardened and access point prices fall. However, the Roamnode solution is also attractive, although certain aspects may be lacking elegance. Parallel studies of 802.1x and Roamnode would thus seem appropriate. In Report 3, we focus on deployment experience of the 802.1x solution.

The establishment of such a RADIUS hierarchy may also enable other services to be shared, outside the WLAN roaming scope, where RADIUS lookup is available.

There are other challenges to study, e.g. best practice in protecting the shared secret between RADIUS servers, and how to advertise to users that a site supports WLAN roaming (without use of a common SSID) and what the specific AUP of the site is.

10 References

[6NET] The 6NET Project,
http://www.6net.org/

[802.11] IEEE 802.11 protocols
http://grouper.ieee.org/groups/802/11/

[802.1q] 802.1q VLANs
http://www.ieee802.org/1/pages/802.1Q.html

[8021X] IEEE 802.1x
http://standards.ieee.org/getieee802/

[8021XWS] TERENA 802.1x Workshop, March 2004
http://www.terena.nl/tech/task-forces/tf-mobility/1x/

[ABOBA] Unofficial 802.11 Security Page
http://www.drizzle.com/~aboba/IEEE/

[AEGIS] Meetinghouse AEGIS client and server
http://www.mtghouse.com/

[AIRMAGNET] AirMagnet
http://www.airmagnet.com/

[AIRSNORT] AirSnort
http://airsnort.shmoo.com/

[ALFA] Alfa-Ariss freeware 802.1x client for Windows
http://www.alfa-ariss.com/

[APSNIFF] ApSniff
http://www.bretmounet.com/ApSniff/

[BLUESOCKET] Bluesocket Wireless Gateway
http://www.bluesocket.com/

[CAPWAP] IETF CAPWAP WG
http://www.ietf.org/html.charters/capwap-charter.html

[CISCO] Cisco WLAN Security in Depth
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

[CONSUME] Consume.net
[DELLWP] Dell White Paper on Wireless Security
http://www.dell.com/downloads/global/vectors/wireless_security.pdf

[DHC] IETF dhc Working Group,
http://www.ietf.org/html.charters/dhc-charter.html

[EDIN] Bluesocket case study at Edinburgh
http://www.bluesocket.com/customers/UoE-1.pdf

[EAP-TTLS] EAP Tunnelled TLS Authentication Protocol (IETF Draft)
http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-03.txt

[FACTSHEET] JANET Wireless Security factsheet
http://www.ja.net/documents/factsheets/wireless-security.pdf

[FCCN] VPN Roaming using Client Certificates
http://www.fccn.pt/projectos/campusvirtuais/Testes/index_ongoing

[FLURER] Weaknesses in the Ket Scheduling Algorithm of RC4
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[FREERADIUS] FreeRADIUS
http://www.freeradius.org/

[FREESWAN] FreeS/WAN
http://www.freeswan.org/

[FUNET] Public Access Roaming in Finland
http://www.atm.tut.fi/public-access-roaming/

[GSMA] GSM Association WLAN Roaming Guidelines
http://www.gsmworld.com/documents/wlan/ir61.pdf

[HIPERLAN2] Hiperlan 2
http://www.hiperlan2.com/

[HPI] High Plains Internet wireless AAA
http://www.hpi.net/whitepapers/warta/

[HUPNET] NUPNet (non-English)
http://www.helsinki.fi/~vviitane/hupnet/

[IAS2003] MS Internet Authentication Service for Windows 2003 server
http://www.microsoft.com/windowsserver2003/technologies/ias/default.mspx

[IETF] The Internet Engineering Task Force,
http://www.ietf.org/

[INTERNET2] Internet 2
http://www.internet2.edu

[IPv6FORUM] IPv6 Forum
http://www.ipv6forum.com

[JANETAUP] JANET Acceptable Use Policy
http://www.ja.net/documents/use.html

[JANETSEC] JANET Security Policy
http://www.ja.net/documents/JANET_security_policy.html

[JANET-CERT] JANET CERT
http://www.ja.net/CERT/cert.html

[JISC] The Joint Information Systems Committee
http://www.jisc.ac.uk

[JISC-BRIEF] JISC Briefing Papers
http://www.jisc.ac.uk/index.cfm?name=publications

[JISC-WLAN] Potential Role of WLANs in Education
http://www.jisc.ac.uk/index.cfm?name=pub_ibsmwireless (senior management)
http://www.jisc.ac.uk/index.cfm?name=pub_ibwireless (for others)

[JNUG] JNUG Report on Wireless Security
http://www.jnug.ac.uk/reports/wlsec.html

[KISMET] Wireless detector
http://www.kismetwireless.net/

[LIN] UKERNA Location Independent Networking
http://lin.bristol.ac.uk/

[LINUXWPA] Linux WPA Supplicant
http://hostap.epitest.fi/wpa_supplicant/

[MISHRA] An initial security analysis of the IEEE 802.1x standard
http://www.cs.umd.edu/~waa/1x.pdf

[MOBBRIS] Mobile Bristol
http://www.mobilebristol.com

[MOBILEIP] IETF mobileip Working Group,
http://www.ietf.org/html.charters/mobileip-charter.html

[MSDEPLOY] Deploying secure 802.11 networks using Microsoft Windows
http://www.microsoft.com/WindowsXP/pro/techinfo/deployment/wireless/

[MUDD] Wireless Network Structure
http://www.wl0.org/~sjmudd/wireless/network-structure/english/article.pdf

[NAT] Traditional IP Network Address Translator, RFC3022.
http://www.ietf.org/rfc/rfc3022.txt

[NGTRANS] IETF ngtrans Working Group,
http://www.ietf.org/html.charters/ngtrans-charter.html

[NOCATNET] NoCatNet
http://nocat.net/

[NOMADIX] Nomadix Wireless Gateway
http://www.nomadix.com/applications/wifi-hotspots.asp

[OASIS] OASIS from StockholmOpen.net
http://software.stockholmopen.net/index.shtml

[ODYSSEY] Funk 802.1x Solution
http://www.funk.com/radius/wlan/wlan_suite.asp

[OPEN1X] Open Source 802.1x Implementation
http://www.open1x.org/

[OREILLY] O'Reilly RADIUS book
http://www.oreilly.com/catalog/radius/

[PANA] IETF pana WG
http://www.potaroo.net/ietf/ids-wg-pana.html

[PATERNO] Using PPPoE in WLANs, IETF Internet Draft
http://www.ietf.org/internet-drafts/draft-gpaterno-wireless-pppoe-13.txt

[POPTOP] PPTP Server for Linux
http://www.poptop.org/

[PPP-RADIUS] RADIUS plugin for pppd
http://www.chelcom.ru/~anton/projects/pppd-tacacs+radius/

[RADIATOR] Radiator RADIUS server
http://www.open.com.au/radiator/

[REGISTER1] WLAN hot spots get hotter
http://www.theregister.co.uk/content/69/29683.html

[RFC2607] Proxy Chaining and Policy Implementation in Roaming
http://www.ietf.org/rfc/rfc2607.txt

[ROAMNODE] The Nomadic Network Service
http://www.nomadic.bristol.ac.uk/

[SHIBBOLETH] Shibboleth
http://shibboleth.internet2.edu/

[SJ4] The SuperJANET4 Network
http://www.superjanet4.net/

[SOWN] Southampton Open Wireless Network
http://www.sown.org.uk/

[STUMBLER] NetStumbler
http://www.stumbler.net/

[SURFNET] SURFnet 802.1x Authentication and Authorisation
http://www.surfnet.nl/innovatie/wlan/

[SURVEY-RES] Survey Results
http://www.ja.net/development/network_access/wireless/uk_activities/

[SWITCH] SWITCH Mobile
http://www.switch.ch/mobile/

[SYNTEGRA] Wired vs Wireless deployment costs, case study
http://www.us.syntegra.com/acrobat/208986.pdf

[TF-AACE] TERENA TF-AACE WG

http://www.terena.nl/tech/task-forces/tf-aace/

[TF-MOBILITY] TERENA TF-Mobility WG
http://www.terena.nl/tech/task-forces/tf-mobility/

[THRU] 802.11a/b/g Throughput
http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html

[TINO] Tino Is Not Oasis
http://www.cc.puv.fi/~teu/tino/

[TMOB] T-Mobile to Bring 802.1x to the Masses
http://www.wi-fiplanet.com/news/article.php/3091051

[TNC-ROAM] RADIUS-based Public Access Roaming in FUNET
http://www.atm.tut.fi/public-access-roaming/theory/applied-radius-roaming.pdf

[UCISA-CASE] UCISA Wireless case studies
http://www.ucisa.ac.uk/groups/ng/docs/report_wireless_casestudies.html

[UCISA-EXP] Exploiting and Protecting the Network
http://www.ucisa.ac.uk/groups/ng/expl/expl-00.htm

[UCISA-TOP] UCISA Top Concerns 2004
http://www.ucisa.ac.uk/activities/surveys/tc/2004

[UKBBTF] UK Broadband Task Force
http://www.broadband.gov.uk/html/ukbroadband_task_force/publications.html

[UKERNA] The United Kingdom Education & Research Networking Association
http://www.ukerna.ac.uk/

[UNINETT] UNINETT WLAN Information
http://www.uninett.no/wlan/

[USERAUTH] JANET User Authentication factsheet
http://www.ja.net/documents/factsheets/041-User-Authentication.pdf

[USPATENT] US patentclaim on web redirection
http://wifinetnews.com/archives/002848.html

[USPOL] US university AP policies
http://listserv.educause.edu/cgi-bin/wa.exe?A2=ind0308&L=cio&P=R10719&I=-3&m=4211

[UTAH] AEGIS 802.1x 128-bit wireless card support
http://www.laptop.lib.utah.edu/cgi-bin/dot1x/dot1xCompatibility.pl

[VERNIER] Vernier Networks WLAN Gateway
http://www.verniernetworks.com/

[WAG] UKERNA Wireless Advisory Group (WAG)
http://www.ja.net/development/network_access/wireless/

[WAGCONF] UKERNA Wireless Conference, February 2004 http://www.ja.net/conferences/wireless/feb-04/prog.html

[WBONE] The WBONE
http://www.wbone.org/

[WEPBUGS] Security of the WEP algorithm
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[WEPBUGS2] WEP concepts and vulnerability
http://www.wi-fiplanet.com/tutorials/article.php/1368661

[WEPCRACK] WEPCrack
http://wepcrack.sourceforge.net/

[WHISPA] Wireless access by SMS
http://www.roke.co.uk/itu/technology.asp

[WI-FIA] Wi-fi Alliance
http://www.wi-fi.org/

[WIRE1X] 802.1x supplicant
http://wire.cs.nthu.edu.tw/wire1x

[WIRLAB] Inter-WISP Roaming: A service concept
http://www.wirlab.net/wirlab_wlan_roaming.ppt

[WISPR] Best Current Practice for WISP Roaming
http://www.wi-fi.org/opensection/wispr.asp

[WLANA] The Wireless LAN Association
http://www.wlana.org/