Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET)

Sami Keski-Kasari, Karri Huhtanen, Jarmo Harju
Tampere University of Technology
Institute of Communications Engineering
Korkeakoulunkatu 1, 33720 Tampere, Finland
{samikk,karrih,harju}@cs.tut.fi

Keywords
Authentication, Authorisation, Accounting, RADIUS, WLAN, Roaming

Abstract

The increasing amount of wireless and wired public network access areas under the administration of separate instances has driven forward the idea that roaming between these areas should be developed. In the academic world research co-operation and the exchange of students, lecturers and researchers is very common. This increases the need of roaming between related organisations. Several ideas and attempts to standardise WLAN roaming exist but in the combined wireless and wired environment the roaming has not been considered. One idea for roaming is to use RADIUS protocol to carry authentication information. In Finland this idea was first presented for commercial operators by WirLab[1]. With standard RADIUS proxying it is possible to carry authentication, authorisation and accounting information to the RADIUS server of the user's home university. Because the idea is to make the RADIUS servers in different universities to look like a one big RADIUS system there is a need for some kind of hierarchy. This paper describes an application of that idea and an architecture to bring not just WLAN but also general public access roaming into FUNET network and beyond. The hierarchy will be designed also to be interoperable for roaming between other European universities and university networks, for example as a part of TERENA mobility task force.

1 Introduction

The development of the wireless networks and the increasing amount of laptop users have created a demand for setting up public access networks where this kind of mobile users could easily get network access. This kind of instant network access should be easily available for the mobile users even if they are just visitors in some organisation. At the same time the Internet and the organisation's network should be protected from the possibly malicious users. This

[1] WirLab, located in Seinäjoki, Finland, is a research center that studies networking in future real-life application environments.

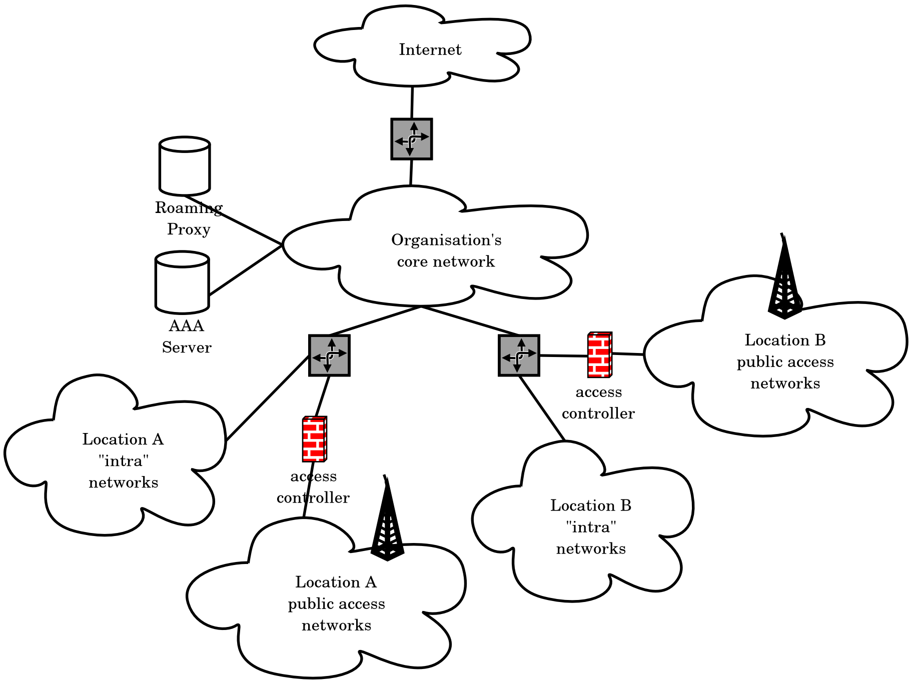
Internet
Roaming Proxy
AAA Server
Organisation's core network
Location B public access networks
access controller
Location A "intra" networks
access controller
Location B "intra" networks
Location A public access networks

Figure 1: Network elements in roaming organisation's network

cannot be done without some kind of access control. The access control cannot be done without organisational authentication infrastructure. When the amount of mobile users moving between organisations increases, the need for transferring authentication information securely between organisations becomes more important. This will not be possible without the roaming infrastructure and means to do public access roaming.

Several ideas and attempts to standardise public access roaming exist, but most of them require additional software to be installed in the terminals and/or in the network. Some solutions require even vendor specific hardware or cellular operator network elements to be able to work. Commercial companies offering roaming services also want to charge for the clearing house services, even if the organisations' intent to do roaming is completely uncommercial.

Our solution for the inter-organisation public access roaming introduces a hierarchical architecture which scales from single organisation network to multi-organisation roaming using a common clearing house. The solution does not require any additional software to be installed in the client terminals and also adding network elements is optional if the current organisation authentication infrastructure is already RADIUS-based and public access controllers are used to control the network access.

2 Network architecture

2.1 Introduction

Figure 1 presents an example of the network architecture of a typical roaming organisation using our solution. The public access networks, i.e. the wireless and wired networks available for public users (students, visitors, etc.), are separated from the networks demanding more security by edge routers and dedicated access control devices, the access controllers.

The separation of the public access networks and organisation's internal networks increases the overall network security as breaking through the wireless access points or access controllers does not give instant access to the organisation's intranet. This separation may be customised and enhanced with VLANs, access control and packet filter lists in the routers. Access control devices may also be used to limit users' access to the Internet.

2.2 Network elements

2.2.1 Access controller

The access controller is the network element that controls access from the public access network to the rest of the network and the Internet. It is a common solution used in many commercial WLAN hotspots and there exists several free and commercial implementations of the access control software as well as dedicated network appliances from several vendors like Nokia, Nomadix, Vernier Networks etc.

The operation of the access controller is very simple. Traffic can not pass through it until the user of certain terminal (identified by IP and/or MAC address) has authenticated herself. For authentication process the access controller captures the first HTTP request the terminal sends and redirects the terminal's web browser usually to a HTTPS-secured authentication page where the username and password information is entered. This method is often also called the captive portal. The access controller then checks the validity of the authentication information against some AAA server, for example RADIUS, and opens the access to the network for the authenticated terminal.

The advantage and the main reason for using access controllers and web-based solution is that the terminals only need a web browser to be able to authenticate the user. The web-based solution also remains as the only feasible solution to support the diversity of terminals until some new common authentication technology has penetrated all platforms. For more detailed description of the web-based authentication solution, see Terena Mobility Taskforce's Deliverable F [TMTDelF].

2.2.2 Roaming proxy

The roaming proxy is a network element that forwards the RADIUS [RFC2865] authentication requests and responses to correct destinations. It also provides a layer of abstraction between organisation's AAA server and the roaming network elements. This way the organisation's AAA server does not necessarily have to be modified or reconfigured to support the RADIUS-based roaming hierarchy. Instead a roaming proxy may be added to the network without disturbing the existing authentication infrastructure or opening the organisation's RADIUS server to direct requests from other organisations.

With certain RADIUS-server software (e.g. FreeRADIUS, Radiator) the roaming proxy may be even used to translate the RADIUS authentication requests to LDAP-inquiries in case the organisation's authentication infrastructure is LDAP-based. It may also add a new hierarchy level for authenticating different user groups. For example in the Tampere University of Technology (domain tut.fi) the roaming proxy can separate the authentication requests for tut.fi- and guests.tut.fi-domains to different authentication servers handling the regular and guest users.

Naturally it is also possible for an organisation to integrate roaming proxy configuration into existing RADIUS server eliminating the need for a separate roaming proxy element from the network. This demonstrates the flexibility of this roaming architecture.

2.2.3 AAA server

The AAA server is included in Figure 1 as a separate element to emphasise the possibility of using roaming proxy as an abstraction and security layer or as a translator between authentication systems. For this roaming model it is recommended that the AAA server would be RADIUS-based, but the architecture does not limit the options as long as the roaming proxy knows how to communicate with the AAA server. By separating the functionality needed for roaming hierarchy and authentication to two elements, the organisational AAA server may also be secured more tightly for example behind the organisation's firewall.

3 Roaming architecture

3.1 Introduction

Figure 2 illustrates one possibility of building a RADIUS-based roaming infrastructure. In this, so far fictional, scenario an additional RADIUS hierarchy level and a roaming proxy is added to handle roaming inside a region. In the example, the region consists of organisations located in one city, Tampere, Vaasa or Oulu.

In the example NREN (National Research and Education Network) roaming root server has the knowledge of which fi-domains are handled by which roaming proxy. For example the roaming root server knows that tut.fi, uta.fi and tpu.fi are handled by the Tampere area roaming proxy and similarly which domains are handled by the Vaasa's or Oulu's roaming proxy. It may also know where to forward top-level domains it doesn't recognise extending the architecture to support also the inter-NREN roaming.

The added hierachy level in the example also demonstrates how easily extra fault-tolerance can be added to the roaming infrastructure. Now even if the roaming root server fails or is unreachable, the roaming inside a region still works as the roaming proxies inside the region use the regional roaming proxy as their default RADIUS server.

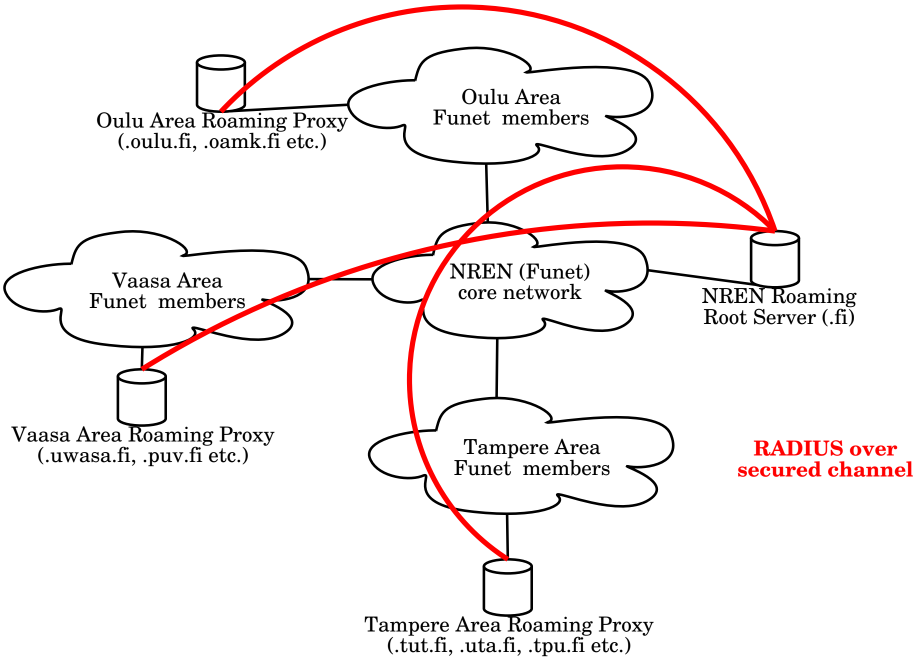

Figure 2: Roaming hierarchy example

3.2 Roaming infrastructure elements

3.2.1 NREN roaming root server

Section 3.1 already revealed that the NREN roaming root server is the roaming element that knows all the domains and the IP addresses of the roaming proxy servers handling them. It is the default RADIUS server for the regional roaming proxies. This means that when a regional RADIUS server does not recognise the domain in the authentication request it received, the regional roaming radius proxy forwards the request directly to NREN roaming root server. Because the NREN roaming root server knows all fi-domains, it is also the server that will connect to other NREN root servers for inter-NREN roaming.

3.2.2 Regional roaming proxy

The regional roaming proxy, Area Roaming Proxy in Figure 2, is also optional like the roaming proxy in the organisation's network. The roaming proxies or even the organisational AAA servers may connect directly to the roaming root server if less hierarchy is preferred. In practice the NREN roaming root servers, regional roaming proxies and organisational roaming proxies are in this roaming architecture simply RADIUS servers configured differently according to their roles and position in the roaming infrastructure. Additional servers may be added or removed freely according to the scalabilty, security and fault-tolerance requirements.

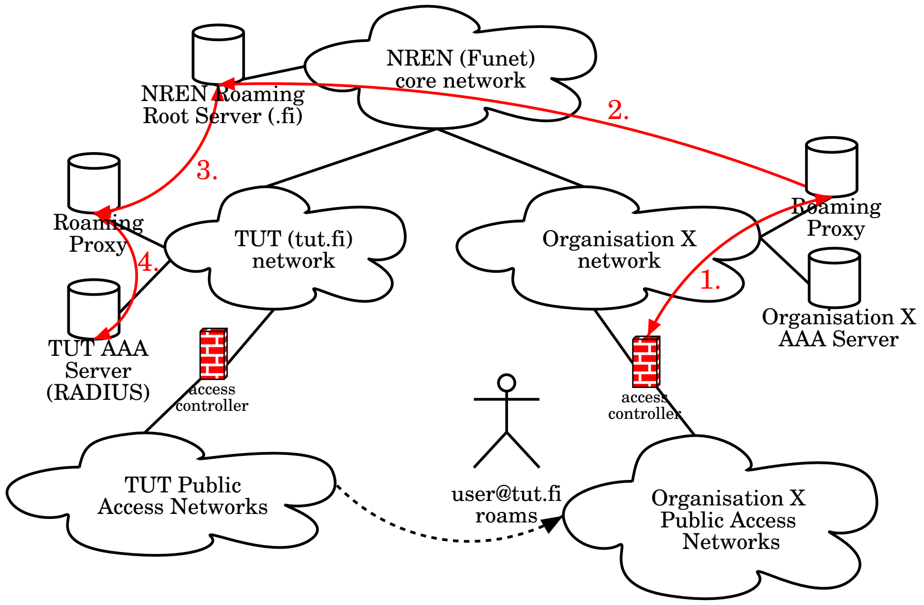

Figure 3: Inter-organisation roaming example

3.3 Inter-organisation roaming in practice

An example of the inter-organisation roaming is presented in Figure 3. The scenario begins from the situation where a visiting user from Tampere University of Technology (TUT, tut.fi) has entered organisation X's public access network. Because this example is based on captive portal solution, the user has already received an IP address from the public access network for the user terminal. The user has started a WWW browser, received the authentication page and entered username (in form user@tut.fi) and password in the web form. The user now submits the web form and the authentication process for roaming begins:

1. The access controller sends a RADIUS authentication request containing the username and password to the roaming proxy in its home network.

2. The roaming proxy in organisation X's network does not recognise the tut.fi-domain in the username (user@tut.fi) and forwards the RADIUS authentication request to its default RADIUS server, which in this case is configured to be Funet's NREN roaming root rerver.

3. The NREN roaming root server has the knowledge of all fi-domain roaming proxy IP addresses and the respective domains they are handling. This way the roaming root server is able to forward the RADIUS authentication request to the roaming proxy in the Tampere University of Technology (TUT) network.

4. The roaming proxy in the TUT network forwards the RADIUS request to the TUT AAA server, which makes the final decision of accepting

the username-password pair. The TUT AAA server informs the roaming proxy about its decision with RADIUS response message, which is forwarded through the same chain of servers back to the access controller.

Depending on the RADIUS response the access controller now informs the user about accepting or denying of the network access. If the access is accepted, access controller opens firewall rules for the user terminal and the user now gains an access to the network beyond the access controller.

4 Security issues

4.1 Connections between network and roaming elements

The access controllers use regular web servers to present the authentication form to the user. User's credentials are transferred with HTTP/HTTPS -protocol depending on the configuration of the access controller. Some commercial access controllers do not even have HTTPS-protocol in the default software version and an additional fee must be paid to get HTTPS-enabled version. Due to security reasons, HTTPS should be recommended or in the case of inter-NREN -roaming required from the roaming organisations.

Using HTTPS and SSL/TLS-certificates also provides the possibility of using SSL/TLS-certificates in authenticating the public access networks to users. This way the risk of doing fake public access networks and controllers collecting usernames and password would be harder, but still leaves the responsibility to the user to check the certificate presented by the web browser. In practice this would require a PKI-infrastructure to be built inside and between NRENs.

The defined PKI-, CA-, etc. policies, practices and the infrastructure would benefit also other projects requiring for example SSL/TLS-certificates that are valid in different NRENs networks. An example of this are the connections between the roaming root servers, proxies and even access controllers; for additional security IPSEC tunnels and certificates can be used to secure the traffic between roaming infrastructure elements and to authenticate the hosts allowed to connect to each other.

4.2 Yet another PKI needed

To make the certificate system work and at the same time be scalable there's no other option than building a yet another public key infrastructure (PKI). Building it could start inside NREN, where the NREN operator would manage the highest CA certificate. This NREN operator would then give organisations inside NREN CA certificates and the organisations could then create SSL/TLS-certificates to be used in the access controllers and other related hosts and devices needed for public access control and roaming.

This PKI-infrastructure could also be scaled to even a higher level by introducing a root CA that would issue and certify the NREN CA-certificates. This practice would then enable a chain of trust where the users would only need this highest certificate installed into their terminals and still be able to verify the certificates of the access controllers anywhere in the roaming area.

4.3 The network and roaming element security

Both the free and commercial access controllers are usually based on some free UNIX-based operating system and may use common open source software like Apache, PHP, and Perl etc. Because of this, extra attention should be focused in securing these hosts and to ensure that security upgrades are installed regularly.

In addition to the access controllers, there are also LDAP/Radius servers and the PKI-infrastructure hosts to be secured. For example in the hierarchical Radius/LDAP roaming scenarios the user credentials are obtainable in plain text in all RADIUS/LDAP servers and also in the access controller. Compromising roaming proxy or root server would in theory compromise all the user accounts and passwords on AAA servers below it in the roaming hierarchy.

Because of this, consistent recommendations, requirements and policies to configure, secure and maintain hosts are needed. Only this way the roaming organisations are able to trust each other enough so that the building of the roaming relationships is possible.

4.4 Unauthorised use of the user credentials

When considering inter-NREN-roaming the security of user credentials arises an important issue. The information management of roaming organisations must be able to detect if the credentials of a certain user have been leaked and used for example at the same time in two different countries.

In the RADIUS hierarchy based roaming model it is possible to disable user account in user's home university RADIUS server if it's known that the user credentials have been leaked. More problematic issue is how the user or administration would know that user's credentials are in the wrong hands. One solution for detecting and preventing this is to use RADIUS accounting features [RFC2866] and specify, that the user can be logged in only once and from one place at the time. That doesn't solve the original problem of how the credentials have leaked but helps to recognise unauthorised usage. By using RADIUS accounting and analysing logs it is possible to build automatic detection systems for detecting unauthorised usage.

4.5 Political and privacy issues

In the roaming architecture there are several elements gathering information about the user and the user terminal so that the system administration of each organisation is able to track potential malicious use back to a certain user. This is expected and people are used to trust their system administration.

Combining the logs and the information from several sources becomes an important issue. Who are allowed to do it and for what purpose? The legislation of the different countries may have different views on the issue without even mentioning the system administration of the different organisations.

Even if these clearly are important issues, starting to define them without an experimental system may be slow and may even not be possible. It's important that the solutions to these issues are based on the real usage scenarios and existing architecture so that they will have their basis in the reality. This can be only achieved if the roaming infrastructure development is allowed to continue and it does not need to wait for the policies to be formed before implementations.

5 Future development

5.1 From captive portals to 802.1X

In the presented roaming architecture it is possible to use any authentication method that uses RADIUS for transporting the AAA messages. The architecture that was first based on web-based authentication system can be replaced in the future with the 802.1X-based [8021X] solution when there is enough client software available, or more precisely, integrated to the user terminals.

It is also possible to use both the web-based and the 802.1X authentication methods simultaneously in the wireless environment by using access points that have the VLAN tagging and multiple network name (ESSID) capabilities. In the wired environment it is possible to get VLAN information from RADIUS to change switchport's VLAN assignment. This way it is possible to assign public access VLAN id to switchport but the user can choose to authenticate via web-based system or 802.1X. By default the port is in the state that sends traffic to the VLAN controlled by the access controller and the scenario is similar to web-based authentication. If the terminal starts 802.1X negotiation, the switch or the access point tries to authenticate the terminal via RADIUS roaming hierarchy. After the successful authentication via 802.1X the switch changes the port's VLAN assignment to a VLAN that allows traffic go through.

In this roaming architecture the same RADIUS hierarchy can be used both for the web-based authentication and 802.1X based authentication without modifications to the roaming infrastructure. The only requirement is that the RADIUS server software used supports the chosen 802.1X authentication protocol. This makes the migration path from captive portals to 802.1X very easy.

5.2 From user mobility to seamless mobility

Currently the architecture and the used network elements do not support seamless mobility as it has not been yet an important feature for the users. It might however become more important as the features of the mobile terminals and mobile phones are constantly developing.

Even in this case the architecture is not the limiting factor. New services, new authentication methods, new network technologies may be added to the infrastructure if they are open enough to be available on the platforms used in building the network. For example if there is a need for introducing Mobile-IPv4/IPv6 to the network, this can easily be implemented by adding Mobile-IPv4/IPv6 stack in the Linux-based access controller. If the network is built with commercial components this may be a lot harder.

6 Conclusion

By combining the web-based captive portal authentication solution and RADIUS-based roaming hierarchy it is possible to realise a public access roaming infrastructure, which supports the widest range of user terminals, has the fewest limitations for using third party software and hardware both in the network and in the terminals and which is scalable and extensible regarding its security, fault-tolerance and development features.

The benefits of this architecture may even be enhanced by using open software and network elements so that adding new services and technologies is possible without waiting them to appear in the regular vendors' roadmaps. The open architecture, network elements and software provides the chance for infrastructure to evolve one step at the time instead of replacing the whole system with a new one every second year.

The migration and future development possibilities of this presented architecture clearly demonstrate that this architecture is capable to evolve when the requirements and technologies continue to develop further.

Acknowledgements

The authors would like to thank people working for WirLab, especially Juha Heinänen, Jouni Vuorela and Mika Mustikkamäki, about publishing the idea of RADIUS-based roaming [WirLRoam] and for co-operation in the public access roaming research and implementation work. Authors would like to thank also IT management of Tampere University of Technology for positive attitude to this research and implementation work.

References

[TMTDelF] Sami Keski-Kasari, Karri Huhtanen: *Terena Mobility Taskforce, Deliverable F: Inventory of web-based solution for inter-NREN roaming*, (http://www.atm.tut.fi/public-access-roaming/theory/tf-mobility-del-f.pdf) June 2003.

[RFC2865] Rigney, Willens, Rubens, Simpson: *RFC 2865: Remote Authentication Dial In User Services (RADIUS)*, June 2000.

[RFC2866] Rigney: *RFC 2866: RADIUS Accounting*, March 2002.

[WirLRoam] Mika Mustikkamäki: *Inter WISP WLAN roaming* (http://www.wirlab.net/wirlab_wlan_roaming.ppt), September 2002.

[8021X] IEEE 802.1 Working Group: *IEEE Std 802.1X-2001: Port-Based Network Access Control*, June 2001.

Vitae

Sami Keski-Kasari received his M.Sc. in telecommunications at Tampere University of Technology in 2002. He is doing his post-graduate studies in telecommunications at Tampere University of Technology. Since 2000 he has been researcher of telecommunications at Tampere University of Technology in the Institute of Communications Engineering.

Karri Huhtanen, currently finishing his M.Sc studies and researching WLAN hotspot and public access architecture at Tampere University of Technology, has already worked within wireless communications industry in the R&D departments of an equipment vendor like Nokia and wireless/internet service providers like Jippii Group Oyj and Wireless Network Services Oy. His job descriptions have varied from the design engineer trainee to a research & development manager, responsible of the development of system architecture for both regional and hotspot WLAN networks.

Prof. Jarmo Harju received his M.Sc. from the Helsinki University of Technology in 1979 and Ph.D. in mathematics from the University of Helsinki in 1984. During 1985 - 89 he was a senior researcher at the Telecommunications Laboratory of the Technical Research Center of Finland, working with the development of protocol software. In 1989 - 95 he was professor of data communications at Lappeenranta University of Technology. Since 1996 he has been professor of telecommunications at Tampere University of Technology in the Institute of Communications Engineering, where he is leading the "Networks and Protocols" group.