Roaming Network Access Using Shibboleth

Mikael Linden*, Viljo Viitanen†

* CSC, the Finnish IT Center for Science
mikael.linden@csc.fi

† University of Helsinki
viljo.viitanen@helsinki.fi

Abstract

There are activities aiming at abling users to dock to a wireless or wired network while visiting organisations outside the premises of their usual connection to the network. These activities, known as roaming access to network, are usually based on well-known technologies, such as RADIUS, IEEE 802.1X, VPN or HTTP redirection. On the other hand, there are applications, usually on the web, that are supposed to be accessed across organisational boundaries. The required infrastructure, known as identity federation, takes care of user authentication and authorisation in the participating organisations. Federating software, based, for example, on XML and SOAP, is being developed in the Internet and academic communities.

This research combines the two and implements roaming access to network on Shibboleth, a federating software developed in Internet2. As a result, a unified model was achieved for authentication and authorisation both for network and application access. The architecture makes role-based authorisation easy and provides a single sign-on while preserving the user's privacy. A practical experiment is going on at the University of Helsinki.

Keywords: roaming access, federated identity, Shibboleth

1 Introduction

Network users want using network services to be all the more comfortable. On one hand, this means the users want to have the network connection easily available everywhere while moving around. On the other hand, the users expect applications on the network to be able to provide more personal and tailored services to them. The services, whether they are the applications being accessed or the network connectivity itself, need to be able to recognise the user's authorisation to use the service. Usually, authorisation is based on the user's authenticated identity and the attributes describing her characteristics. The process of keeping track of information system users and their privileges is called user administration.

Typically, the user has one home organisation that she has dealings with and that usually provides most of the services available for her. The home organisation is often the user's employer, school, teleoperator etc. A cross-organisational service means that the service is provided by an organisation other than the user's home organisation. For authentication and authorisation, cross-organisational services need cross-organisational user administration.

Terminology in the area is still young, and varying concepts are being used. In this document, the user's home organisation is called Identity Provider [TFAA04]. The Identity Provider is responsible for authenticating the user and is also the primary source for the user's attributes. The organisation that provides the actual service is called Service Provider. The Service Provider is expected to rely on the authentication done and attributes released by the user's Identity Provider.

Chapter 2 introduces common technologies for a cross-organisational network and application access, which are then compared in Chapter 3. In Chapter 4, the architecture for combining network and application access is introduced. Chapter 5 presents the practical experiments being conducted at the University of Helsinki. Chapter 6 concludes the paper.

2. Cross-organisational Access Technologies

A cross-organisational service may be either network access for roaming users in a visited organisation, or application level access, for example, to a service on the web. Next, technologies to implement cross-organisational network and application access shall be shortly introduced.

2.1. Network Access

Network access is the service that provides a network connection to a user when she is roaming outside her home organisation. A generic architecture is presented in Figure 1. The user can connect to the Service Provider's docking network using either a wireless (WLAN) or a wired link. The Network Access Controller[i] controls the docking network and prevents an unauthenticated user's traffic out of the docking network. In order to authenticate the user, the Network Access Controller consults the user's Identity Provider (i.e.

[i] In [TFMO04], the component is called Access Control Device; here, the word "network" is added to distinguish it from application access.

her home organisation) to deduce if network access should be granted to the user. The Identity Provider has an Authentication Server and a back-end database of its users. Although omitted from the figure, each organisation can typically act both as a home organisation for its local users and a visited organisation for roaming users coming from other organisations.

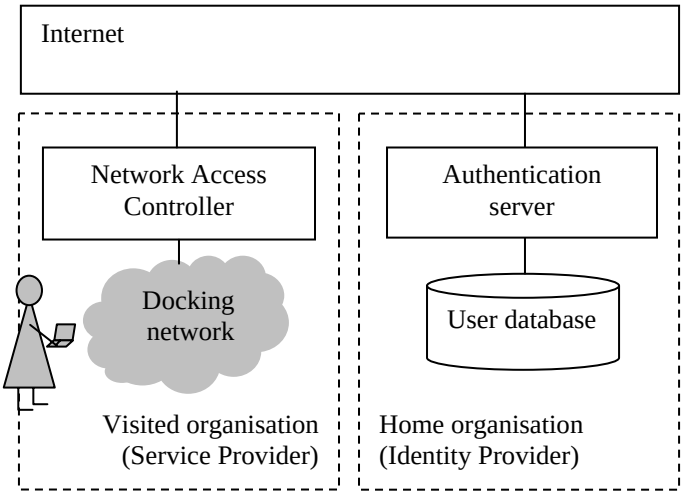

Figure 1. The generic architecture for roaming access to network.

Terena's TF-Mobility group has defined requirements for roaming network access [TFMO04c] and investigated technologies used in academic communities in Europe [TFMO04]. The three most widely used solutions are shortly introduced below.

IEEE 802.1X is a layer 2 authentication protocol that a Network Access Controller uses to authenticate a roaming user. Together with EAP (Extensible Authentication Protocol) and a hierarchy of RADIUS proxy servers, it can be used to validate the user's username and password against her Identity Provider. The user gives her username in the format of *username@domain* and based on the domain name, the RADIUS proxies are used for relaying the authentication request to the correct Identity Provider. The user's credentials (usually the password) are passed to the Identity Provider on EAP. In European higher education, roaming based on 802.1X is used for example in the Netherlands.

Web Redirection is another roaming solution based on a hierarchy of RADIUS proxies. Instead of using 802.1X, the Network Access Controller presents to the user a web dialog, prompting her to enter her username and password, which are then validated against the Identity Provider's RADIUS server. For the user, access from the docking network to the rest of the network is granted only if the Identity Provider responds that the credentials were successfully validated. Web Redirection is used in roaming, for example, in Finnish higher education.

VPN based roaming solution does not require a hierarchy of RADIUS proxies. Instead, the Network Access Controller has a list of all the Identity Providers' VPN gateways, which are the only hosts outside the docking network to which the Network Access Controller allows traffic. It is then up to the VPN gateway in the user's home organisation to authenticate the user and route her traffic to the Internet.

The administrational overhead of the extensive list of VPN gateways can be simplified by attaching all the VPN gateways to a single or a small number of networks, and configuring the address space of the networks to each Network Access Controller. Adding a new Identity Provider would then require no modifications to any of the Network Access Controllers. The solution is known as CASG (Controlled Address Space to Gateways) and described in detail by Terena's TF-Mobility [TFMO04b]. VPN based roaming is used in Swiss higher education.

2.2. Application Access

Accessing cross-organisational applications means using an application level service provided by a Service Provider situated somewhere in the Internet. Typically, applications for a large user base are provided on the web, or may have a web front end for them (such as videoconferencing). Thus, application level access technologies, known as federating softwares[ii], are mostly designed for the web, Kerberos being the most well known exception.

Unlike network access, federating softwares do not have widely deployed protocols on top of which to run. There are implementations utilising web redirects, embedding tickets in the URL fragments, hidden web forms and cookies, but no single standard has emerged. Most prominent technologies, such as SAML (Security Assertion Markup Language), are built on XML and SOAP.

A group of organisations co-operating to administer user access to cross-organisational services is called a federation [TFAA04], which consists both of Identity Providers and Service Providers. To put the co-operation into practice, the federation decides to use some federating software (or develops one of its own).

In academic community, federating software and federations using them are typically aimed at protecting library and e-learning services. The United Kingdom has had the Athens federation [ATHE04] running for years. In Spain and Norway, the national research and education networks have developed the PAPI [PAPI04] and FEIDE [FEID04] systems, respectively. In the Netherlands, Surfnet is promoting A-select [ASEL04] also for cross-organisational transactions.

[ii] From telecommunications perspective, a federating software is a protocol which both the Identity and Service Provider have implemented. From a service developer's point of view, it is a middleware service that provides user authentication and authorisation service to the application.

There are, however, some technologies that have acquired international use. Shibboleth [SHIB04], the federating software by Internet2, is being used or piloted in the academic world in the United States, Canada, Australia, Switzerland, Finland and the United Kingdom. Outside academic communities, there are commercial organisations developing their federating software, such as Liberty [LIBE04] and WS Federation [WSFE03].

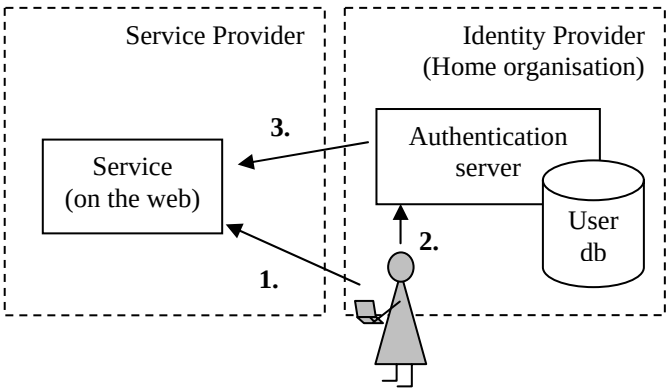

Figure 2. Cross-organisational application access.

Although varying implementations are available, a typical federating software architecture is depicted in Figure 2. The user wants to access a web service outside her home organisation (1. in the figure). At first, the user selects her Identity Provider to whose web server she is then redirected for authentication (2.). Having authenticated the user, the Identity Provider provides the user's attributes to the Service Provider (3.). Based on the attributes, the service decides if the user is authorised to use the service.

Requirements for a federation are listed, for example, in [LIND04]. In addition to a federating software, a federation needs to agree on the syntax and the semantics of the attributes released, on a security infrastructure such as PKI for authenticity and confidentiality of the message exchange and on the arrangements to establish mutual trust between the organisations in the federation. As personal data is processed in the federation, attention should be paid to not compromising the user's privacy when releasing the attributes. For example, the EU directive on data protection [EC95] stipulates that only attributes relevant for the service may be released, and usually only with the user's consent.

3. Comparison of Network and Application Access

Network and application level access have several things in common and some differences as well. In network access, the basic scene is that the user, while roaming outside her home organisation, wants to connect to the network. In application access, the user is perhaps physically in her home organisation, but wants to use services provided by some other organisation. However, nothing prevents a roaming user from accessing remote applications as well.[iii]

Application access technologies typically pay a considerable amount of attention to releasing user attributes properly from the Identity Provider to the Service Provider. In a minimal setup, the only attribute released to the service could be, for example, some role information, such as "the user is a computer science student at the University of Helsinki", that is enough to let her use an article database licensed only for the computer science department. In that case, the identity of the user is hidden from the service, following the EU's data protection directive. A sophisticated service, such as a service for applying as a visiting student to a course in a neighbouring university, probably needs to get a large set of attributes about the applicant and her background in her home organisation (for example: her name, mail address, phone number, target degree, study subject, major, number of credit units so far etc). Unlike application access technology, network access technologies are typically not designed for passing user attributes from the Identity Provider to the Service Provider. On the other hand, if the RADIUS hierarchy is used, the user's identity is, nevertheless, revealed to the Service Provider, because the user's Identity Provider needs to be derived from the username that is in the format of *username@domain*[iv].

Roles are user's attributes that describe her relationship to her home organisation. Role-based authorisation, studied, for example, by Sandhu et al [SAND96, SAND01], relies on the user's role on deciding what services are permitted for her. In a large organisation, such as a university with thousands of users, role-based authorisation is attractive, reducing the complexity of user administration tasks.

Federating software with fine-tuned means for passing user's attributes to the Service Provider provides comprehensive means for role-based authorisation. Limiting access to a service (such as access to the network or to an article database licensed by a university library) to some smaller subgroup (such as staff and students of one university department) is easy and is up to the Service Provider. However, network access technologies, which have limited support for attribute release, leave authorisation actually to the Identity Provider. The Service Provider grants access, if the Identity Provider validates the user's credentials

[iii] In the case where the authorisation to an application is based on the client's IP address, it is worth noticing that VPN roaming solution is the only one in which the user gets an IP address from her Identity Provider's address space. In academic communities, databases licensed by libraries typically use authorisation based on the client's IP address.

[iv] Tunnelled EAP, such as PEAP or EAP-TTLS, can, however, be used so that the username is passed in a tunnel to the Identity Provider. Outside the tunnel, only the user's domain is visible to the Service Provider for relaying the authentication.

successfully. In fact, authorisation is implicit; the user is authorised to access the network if she has a user account in an Identity Provider.[v]

4. Combining Network and Application Access Technologies

Maintaining two overlapping infrastructures for network and application access is ineffective. A single infrastructure for cross-organisational user administration could serve both network and application level access control. Maintaining and supporting one infrastructure for both network and application access would save work and costs for both Identity Providers and Service Providers. The next part introduces a model on how roaming access to network can be implemented on top of Shibboleth federating software. The model and its benefits and downsides are then compared to the models in Chapter 2.

4.1. Roaming Architecture on Shibboleth

The architecture of roaming access to network on Shibboleth is depicted in Figure 3. Shibboleth is a web based protocol that uses browser redirects to pass the user to her Identity Provider for authentication. After a successful authentication, the Service Provider uses SOAP to retrieve the user's attributes from the Identity Provider. As this paper is not intended to be an in-depth-introduction to Shibboleth, readers are encouraged to refer to Shibboleth architecture [SHIB04c] for description of the protocol and Shibboleth distribution [SHIB04b] for its implementation and deployment.

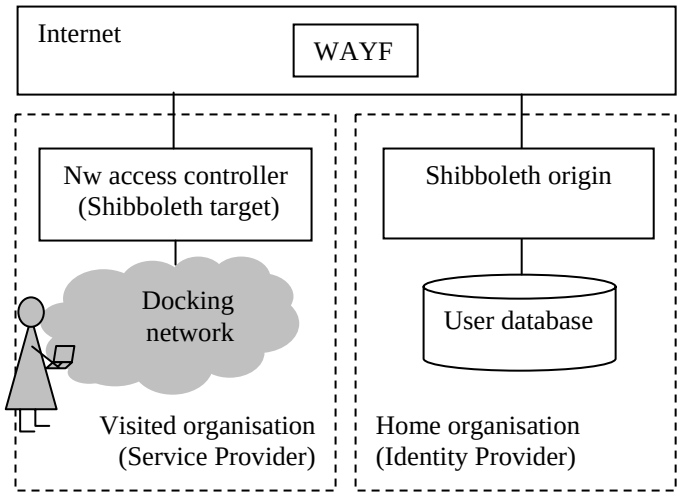

Figure 3. The architecture of roaming access to network on Shibboleth.

[v] TF-Mobility's requirements document [TFMO04c] states that roaming access should be available for all users authorised for Internet access in any home organisation, but visited organisations may want to have more fine-grain authorisation.

The three Shibboleth servers: the Shibboleth origin, the Shibboleth target and the Where Are You From (WAYF) are run on web servers and maintained by the Identity Provider, the Service Provider and the federation, respectively. The Shibboleth origin is the Identity Provider's ordinary Shibboleth server and, from its perspective, network access is just another service for which it provides user authentication and attributes. The Shibboleth origin authenticates the user and communicates with the organisation's user database to supply the Shibboleth target with the user's attributes. The WAYF is the central server that is run by the federation and provides the user a simple drop-down list of all the Identity Providers in the federation.

The actual "shibbolisation" of roaming access to network is done by integrating the Shibboleth target and the Network Access Controller, the component that prevents unauthorised roaming users from accessing the network. The Shibboleth target is the peer of the Shibboleth origin, retrieving attributes of the authenticated user using SAML and SOAP protocol.

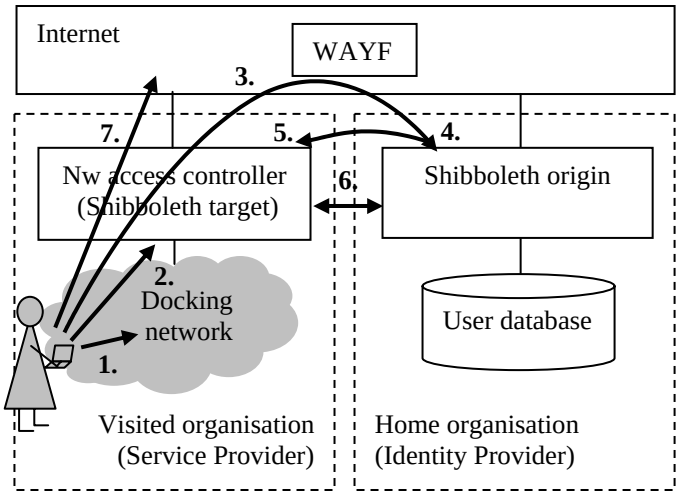

Figure 4. The message exchange in roaming access to network on Shibboleth.

Figure 4 describes the message exchange when a roaming user enters the docking network in a visited organisation.

1. The user activates her client device, connects to the docking network (for example, by activating her WLAN card or by plugging in to an ethernet socket) and gets an IP address via DHCP. However, the Network Access Controller initially blocks all her traffic in and out of the docking network, except the traffic to the TCP port 443 (SSL) of the WAYF and all the Shibboleth origin servers in the federation.
2. The user launches her web browser. The Network Access Controller, which has a web server with Shibboleth target components[vi] in it, captures the user's initial HTTP

[vi] In its current Apache implementation, the Shibboleth target consists of an Apache module and a daemon process running in the same machine.

request. As the web server's main page is protected by Shibboleth, the Shibboleth target is activated and first redirects the user to the WAYF.

3. In the WAYF server the user selects her Identity Provider from a drop-down list. The WAYF server redirects the user to the Shibboleth origin server of her home organisation.
4. The Shibboleth origin authenticates the user, for example, with a username and a password, which are provided to the origin by the user on a web form over HTTPS. The way the authentication takes place is up to the Identity Provider and the federation.
5. After a successful authentication, the Shibboleth origin redirects the user's browser back to the Shibboleth target with a SAML assertion containing a Shibboleth handle.
6. The Shibboleth target uses the handle to acquire the user's attributes from the Shibboleth origin. Communication takes place directly between the Shibboleth target and origin and uses SOAP and SAML.
7. Based on the user's attributes, the Network Access Controller decides if the user is authorised to access the network. If access is granted, it changes the firewall rule so that the traffic can flow between the client and the network.

Roaming access on Shibboleth does not have any specific needs for the client device. A web browser with support for SSL and HTTP redirect, a network interface card and DHCP client is sufficient.

For the visited and the home organisation, roaming access on Shibboleth requires that they are part of a federation which has made necessary agreements for trust establishment, organised the WAYF server etc. In addition, the Identity Providers' Network Access Controllers have to know the IP addresses of the WAYF and the Shibboleth origins in the federation.[vii]

4.2. Comparisons and Remarks

The Shibboleth based roaming architecture and the three roaming architectures presented in Chapter 2 have some common characteristics and also differences, which are summarised in Table 1.

Like the web redirection model, the Shibboleth model relies on capturing the user's HTTP connections in the Network Access Controller. To get access out of the docking network, the user has to open her web browser to initiate the authentication process. However, in Shibboleth, the user's web browser communicates directly on HTTPS with the Identity Provider, whereas in the web redirection model the communication with the Identity Provider is done by the Network Access Controller on top of RADIUS.

Table 1. Comparison of Shibboleth and the three roaming architectures.

Property	802.1X	Web redirect	VPN	Shibboleth
Uses HTTP connection capture		X		X
Uses RADIUS proxy hierarchy	X	X		
End-to-end security for credentials, e.g., user passwords	X		X	X
User identity not revealed to the visited network	(x)		X	X
The Network Access Controller has to know the Identity Providers' IP addresses (or use CASG)			X	X
All traffic routed through the Identity Provider			X	
Vulnerable to MAC address spoofing		X		X
(x): If tunnelled EAP is used, user identity need not be revealed to the visited network.				

Like in VPN and 802.1X models, the connection for user authentication is an end-to-end connection between the client device and the Identity Provider and, thus, the user's password is never available in cleartext to the visited organisation or any other intermediary, making trust establishment easier. However, in 802.1X and web redirection models, the user's identity is usually revealed to the visited organisation, because the RADIUS hierarchy needs the domain part of the username to route the authentication request to the Identity Provider. In VPN and Shibboleth models, neither the user's identity nor the password need to be revealed to the visited organisation, thus preserving the user's privacy.[viii]

Like the list of gateways in the VPN model, the Network Access Controller must have an extensive list of the Identity Providers' Shibboleth origins and the WAYF's IP addresses to which unauthenticated traffic is allowed in the SSL port 443. The hole in the firewall is required for letting the Shibboleth origin authenticate the user directly. However, once the authentication is done and the Network Access Controller allows the user to access the network, the traffic

[vii] Here it is assumed that the Shibboleth origin authenticates the user by itself. If the Shibboleth origin redirects the user to a separate login server for authentication, its IP address has to be configured to the Network Access Controller as well.

[viii] However, to investigate abuse, logs in the Shibboleth origin and target can be merged to reveal user identity.

need not be routed through any gateway in the Identity Provider. On the other hand, the CASG proposed for the VPN model can be applied for Shibboleth as well.

Like the web redirection model, the Shibboleth model is vulnerable to a MAC address spoofing attack. Neither of the two models provides a link layer traffic encryption or an integrity check, making it possible for an attacker to hijack the MAC and IP address of a legitimate user, for example, right after she has left the wireless network. The attack is made by reconfiguring the victim's MAC address to the attacker's client device, requiring skills and special tools from the attacker [TFMO04, p. 20].

Shibboleth uses WAYF for deducing the user's home organisation. In 802.1X and web redirection, the RADIUS protocol and the hierarchy of RADIUS proxies carry out the task; the user's home organisation is derived from the user's username that is in the format of *username@domain*.

A practical remark is, however, that usually different people are responsible for the network and the applications in an organisation. The network people are not necessarily familiar with application level authentication and authorisation technology. For the network people, it may be easier to deploy a technology, such as RADIUS or VPN, that they are already familiar with.

4.3. Benefits and Downsides

A benefit of the Shibboleth model is that it separates the authentication and the authorisation from each other. Authentication is always done by the Identity Provider, and the Service Provider is not involved in it. What the Service Provider has to do to let authentication happen is just to let the user communicate with her home organisation on SSL. Authorisation, in turn, is solely up to the Service Provider, based on the roles and other attributes released by the Identity Provider. The Service Provider can, for example, decide to prioritise the users with role "staff" in places where there is only a limited amount of network capacity available.

Another benefit of Shibboleth is that it unifies the network and application level access architectures, considering network access as just another shibbolised service. Maintenance and support for overlapping architectures becomes unnecessary. Furthermore, the user is able to enjoy a single sign-on, because the authentication takes place when she accesses the network, and she then has an existing session with her Identity Provider's Shibboleth origin. The existing session makes reauthentication unnecessary if the user later accesses another shibbolised service.

A downside of the Shibboleth model is that the technology is not as widely known and deployed as the other models utilising protocols that have been used for years. Besides Shibboleth, there are also other application level access technologies being used and developed, such as Liberty, whose interoperability may require extra effort. As a technology for fine-grained application level access, Shibboleth also needs a more complex federation with related trust fabrics underneath.

Another downside of Shibboleth is the scalability and security issue raised by the maintenance of the extensive list of Shibboleth origins in the federation. It can be, however, partially overcome with CASG.

5. Practical Experiments

To get practical experience, the Shibboleth based roaming architecture has been implemented and piloting started in the University of Helsinki. The shibbolised Network Access Controller was connected to the HAKA pilot federation, the federation of Finnish higher education that uses Shibboleth as the federating software. However, there were no modifications to Shibboleth implementation as the federation in use is just a configuration issue for the Shibboleth target. The architecture should be easily adapted to other Shibboleth federations as well.

5.1. Background Information of the University of Helsinki

The University of Helsinki is the largest university in Finland, with 39 000 users. The university has four campuses in Helsinki, the main one located in the centre of the city. There are also 6 other universities and several polytechnics in Helsinki.

HUPnet, Helsinki University Public network, has been available for the staff and the students of the University of Helsinki since 2001. Currently, HUPnet covers about a third of the university buildings in Helsinki, and the coverage is increasing as more base stations are installed. HUPnet also has ethernet sockets available for wired use. On an average day, there are about 50 different users connecting to HUPnet.

Situated in the heart of Helsinki, the university has been deliberate to open HUPnet for roaming users. There have been concerns that there would be considerably more roaming users coming in than going out, causing the cost to accumulate to the university. However, the university could open HUPnet to some limited user group, for example, to the staff and the faculties of other universities. Allowing access for staff and denying it from students requires role based authorisation, which is not supported by the web redirection roaming model. As the University of Helsinki has been active on Shibboleth deployment, it has now been integrated to roaming access as well.

5.2. Implementation

In the implementation, the Network Access Controller runs in a Debian Linux machine (Figure 5). When a user enters the docking network, a DHCP server gives her an IP address that belongs to a virtual LAN that the Network Access Controller separates from the Internet. Initially, the Iptables configuration of the Network Access Controller is configured

to block all traffic from the user's IP address to the Internet, except the TCP traffic in port 443 to the Shibboleth origins in the federation.

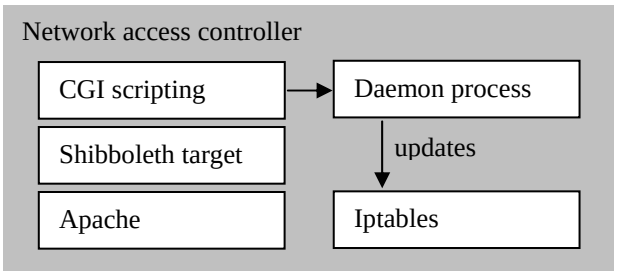

Figure 5. The shibbolised network access controller of HUPnet.

There are Shibboleth target components installed in an Apache web server that runs on the Network Access Controller. When the user opens her web browser, the Network Access Controller captures the web browser's initial HTTP request and provides the initial front page of HUPnet as the HTTP response. The user is asked if she is a local user (and to be authenticated against the local user database of the University of Helsinki) or a user from another university (and to be authenticated on Shibboleth).

To initiate Shibboleth authentication, the user enters a directory in the web server that is protected by Shibboleth in the web server configuration. The Shibboleth authentication and attribute exchange take place, and if the user has attributes required in the server authorisation configuration (that is, eduPersonAffiliation value ‘employee’), she is allowed to run a Perl script in the directory. The Perl script calls a daemon process running in the same machine and provides it with the IP address of the user. The daemon process, running with root privileges, makes necessary modifications to the Iptables configuration file of the Network Access Controller in order to let the user access the Internet.

In HUPnet, user authentication is valid for two hours at a time, after which it has to be renewed. A user can also initiate an explicit logout from HUPnet by calling another CGI script that restores the Iptables configuration.

The university of Helsinki is aware of the architecture's vulnerability to the MAC address spoofing attack and has accepted the risk of a successful attack, because all the attacker gains is just unauthorised access to the Internet. If Internet access is what the attacker wants, it can be obtained freely from the many public Internet "hotspots" at the university and there is little need to hack the university’s wireless network. On the other hand, as the attack requires special skills and tools, it is expected that the present architecture is sufficient to prevent ordinary users from getting unauthorised access, and the small number of attackers skilled enough is tolerable.

However, if MAC address spoofing becomes a problem, a sketch has been made of an improvement of making the web browser in the client device poll the Network Access Controller regularly on SSL. As the communication on SSL relies on a shared secret between the web browser and the server, the attacker replacing a client device in the docking network can be recognised and detached from the network. A downside of the improved architecture is that a temporary interference in the wireless network may block the polling and detach the user from the network.

5.3. Current Status and Future Plans

The shibbolised HUPnet has been launched for pilot use. Staff and faculty members are able to roam at the University of Helsinki if their home organisation belongs to the HAKA pilot federation. The source code of HUPnet has been made public and available for other institutions and federations for free as open source in SourceForge [HUPN04].

6. Conclusions

This paper presented an architecture that turns network access into just another service that can be used across organisational boundaries like application level services in a federation. Piloting the implementation that utilises Shibboleth federating software has started.

Combining network and application level access technologies reduces overlapping infrastructure and brings application level features, such as role-based authorisation and single sign-on, available also for network access. As a downside, application level access technologies are not yet so mature as network level access technologies. The architecture has to allow an unauthenticated user’s traffic to a small set of hosts in the Internet, making the maintenance of the service more difficult.

Acknowledgements

We want to acknowledge Sami Keski-Kasari for comments on the architecture and Carsten Borrman for the idea of introducing CASG also to the roaming architecture on Shibboleth. Acknowledgements also to Switch, which has provided lots of high-quality documentation on Shibboleth, and to Internet2 for the Shibboleth software itself.

References

ASEL04 The A-Select Authentication System. Alfa & Ariss b.v. http://www.a-select.org/

ATHE04 The Athens Access Management System. Eduserv. http://www.athens.ac.uk/

EC95 European Communities. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

FEID04 Felles elektronisk identitet. Uninett. http://www.feide.no/

HUPN04 The HUPnet - Helsinki University Public network. University of Helsinki. http://hupnet.sourceforge.net/

LIBE04 Liberty alliance project. http://www.projectliberty.org/

LIND04 Linden M. 2003. Towards Cross-Organisational User Administration. Informatica 27, 3, 353–359

PAPI04 The PAPI AA Framework. RedIRIS. http://papi.rediris.es/

SAND01 PARK J. S., Sandhu R. 2001. Role-based Access Control on the Web. ACM Transactions on Information and System Security. 4, 1, 37–71.

SAND96 Sandhu R., Coyne E. J., Feinstein H. L.,Youman C. E. 1996. Role-based Access Control Models. IEEE Computer 29, 2, 38–47.

SHIB04 The Shibboleth project. Internet2. http://shibboleth.internet2.edu/

SHIB04b The Shibboleth test and software distribution site. Internet2. http://shibboleth.internet2.edu/release/shib-download.html

SHIB04c The Shibboleth architecture, working draft 01, 25 May 2004. Internet2.

TFAA04 Trans-European Research and Education Networking Association, Task Force Authentication and Authorisation coordination for Europe. Deliverable B.2: AAI Terminology ver 1.0.

TFMO04 Trans-European Research and Education Networking Association, Task Force Mobility. Deliverable G: Preliminary selection for inter-NREN roaming.

TFMO04b Trans-European Research and Education Networking Association, Task Force Mobility. Deliverable E: Inventory of VPN-based Solutions for Inter-NREN Roaming.

TFMO04c Trans-European Research and Education Networking Association, Task Force Mobility. Deliverable C: Requirements definition for inter-NREN roaming. Version 1.4.

WSFE03 Web Services Federation Language. IBM, Microsoft, VeriSign. 2003.