Implementing the multi-federation and peer-to-peer roaming on the eduroam federation level

Karri Huhtanen
Department of Communications Engineering, Tampere University of Technology, Korkeakoulunkatu 1, FI-33720 Tampere, Finland and Arch Red Oy, Hermiankatu 8 D, FI-33720 Tampere, Finland
e-mail: karri.huhtanen@{tut.fi|archred.com}

Sami Keski-Kasari
Arch Red Oy, Hermiankatu 8 D, FI-33720 Tampere, Finland
e-mail: sami.keski-kasari@archred.com

Heikki Vatiainen
Arch Red Oy, Hermiankatu 8 D, FI-33720 Tampere, Finland
e-mail: heikki.vatiainen@archred.com

Jarmo Harju
Department of Communications Engineering, Tampere University of Technology, Korkeakoulunkatu 1, FI-33720 Tampere, Finland
e-mail: jarmo.harju@tut.fi

Abstract

As eduroam, other confederations and community networks continue to grow and evolve, the inter-connectivity and roaming issues between these and multiple federations are becoming more important. The current and future needs for multi-community and peer-to-peer roaming must be addressed when developing the federation level eduroam server implementations. Based on the new upgrade developed for the Finnish eduroam top-level server, this paper proposes a design and an implementation to address these issues in a federation level server implementation.

Keywords

Federation inter-connectivity, peer-to-peer roaming, RadSec, eduroam, Finland

Introduction

While the eduroam [1] is clearly the dominating RADIUS [2] based confederation between academic and research organisations, there already exist other federations such as for example commercial community networks, which have similar interests for enabling roaming between their members and academic and research organisation networks. Each of these federations may have their own even contradicting policies for federation member roaming, which means that all roaming relationships cannot be covered within single federation. These commercial federations may also grow more quickly or already cover more areas and organisations than the academic and research federations. Enabling roaming between these federations creates mutual opportunities to extend network coverage without having to invest to the overlapping network infrastructures. Participation to multiple federations on the other hand creates a need to be able to filter and manage the organisation roaming relationships and separate authentication federations. The multiple-federation support in the federation top-level server makes this possible, while providing also functionality for creating ad hoc federations for temporary use such as for example multi-organisational testbeds, technology trials etc.

The Finnish top-level eduroam RADIUS server had already earlier support for two authentication federations: Funet WLAN roaming [3] and eduroam Finland. These two federations were separated because of the eduroam policy to allow only higher education or research organisations, while the Funet WLAN Roaming federation allowed also companies and community networks as members. The authentication traffic was filtered so that organisations willing to roam only with eduroam organisations could roam with eduroam compliant organisations and the non-eduroam compliant organisations could only roam with the organisations belonging to the Funet WLAN Roaming federation. The international roaming was limited to eduroam compliant organisations only.

The key driver for developing multi-federation and peer-to-peer roaming support however, was not the multi-federation requirements but a need for RadSec [4] testing. The utilised Radiator RADIUS server [5] was not capable of getting the

RadSec configuration from the SQL database in the similar fashion it was able to get the RADIUS peer configurations. These limitations led to a design and an implementation, which in addition to being capable of handling fixed RadSec roaming, could also be used as a base for both multi-federation and dynamic RadSec server discovery support [6, pp. 17 – 20]. This paper describes the design and architecture of the solution while considering also implementation issues, advantages and disadvantages of the solution.

Design Targets

One of the first and most important design targets was that the system would support both RADIUS and RadSec protocols and proxy functionality between protocols. The advantage being here that organisations could connect with whichever protocol they had already available and upgrade later easily to a more advanced connection.

The new architecture and implementation were designed from start to support IPv6 for both RADIUS and RadSec clients and servers as well as proxying RADIUS requests from IP version to another between organisation and federation servers. Also in this case, the organisations and federations were to have the option to migrate to the new IP version according to their own capabilities.

As the amount of organisations and supported federations grows in the federation top-level server, the scalability and dynamic configuration become more important issues. The Finnish top-level RADIUS server has supported this for a while providing organisation realm, RADIUS server and client mappings from the SQL database.

Utilising RadSec, however, created an implementation challenge as the Radiator did not have support for reading RadSec server and client information from the SQL database. Configuring RadSec server and clients to configuration manually would have meant restarting the service causing service breaks and would have been more error-prone in general. Because of this, a design choice was made to utilise Radiator's module DNSROAM for DNS based RadSec server discovery. As a by-product of this choice the implementation gained support for future peer-to-peer RADIUS roaming in addition to the more flexible static configuration of RadSec connections.

There is not a single federation or confederation to cover all the roaming requirements organisations or companies may have, nor it is likely to be any in the future. Even commercial wireless internet service providers have needs to connect to multiple roaming brokers such as iPass, Boingo, Trustive and WeRoam. In Finland there are regional and national community networks, which form their own federations and accept both organisations and companies as members. Some of the organisations are already members in multiple federations and face the challenges of selecting for example the preferred roaming root server for inter-organisation roaming. Each of these federations may have their own policies and requirements for members. Even in academia there exists Funet WLAN Roaming federation for commercial companies and community networks to be able to roam with willing education and research organisations. To be able to support these and the future federation and filtering needs, one of design targets was to develop a fine-grained support for both inter-organisation and inter-federation roaming. In practice this meant supporting the roaming partner selection on both organisation and federation level. For example an organisation might both select the federations it belongs to while still maintaining the opportunity to add roaming partners per organisation basis.

Architecture

Figure 1 presents the architecture of the Finnish eduroam federation-level server implementation containing the multi-federation and peer-to-peer roaming support.

The SQL database contains information about confederation members and their RadSec and RADIUS settings. The settings are maintained with a web based user interface. The web server has only limited access to the SQL database and was in the actual implementation separated to a another virtual host.

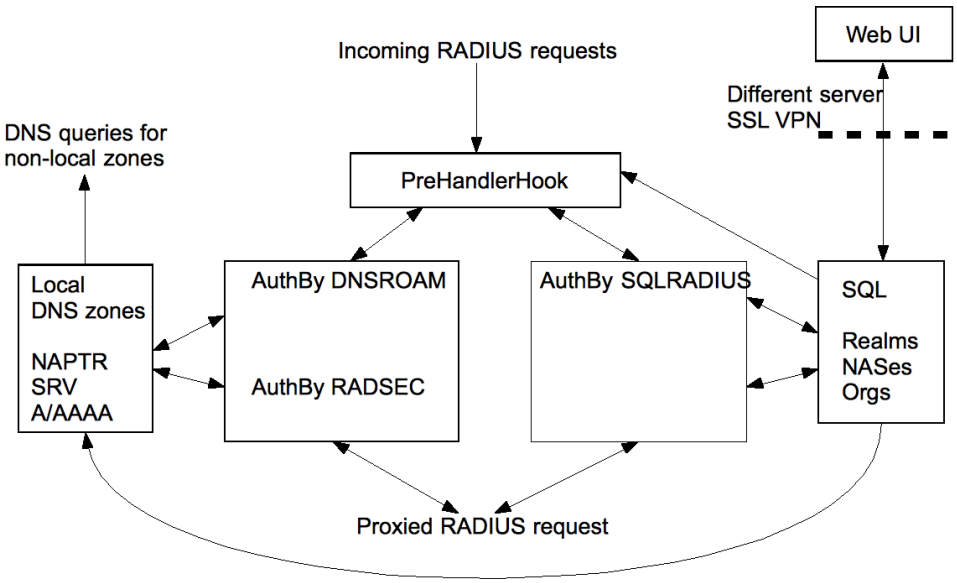

Figure 1: Architecture

Complying authentication and accounting requests enter via a Radiator PreHandlerHook and are proxied forward by either RadSec or RADIUS authentication. Complying requests are the ones that do not try to breach roaming policies, loop back to the sender or have other problems during the processing. The PreHandlerHook hook uses SQL database information to enforce the roaming policies between federation members, chooses and optionally enforces RadSec or RADIUS selection and does loop detection.

Figure 1 shows two handlers, one doing the authentication by DNS roaming based RadSec proxying and the other handler doing authentication by RADIUS proxying. These handlers are called if the roaming policy verdict was successful. Handlers that reject non-compliant requests that should not be forwarded or can not handled e.g., because of database problems are not shown in the figure. These additional handlers return in case of problems Access-Reject messages to callers with informational messages describing the reject reason.

DNS information is used by Radiator's RadSec module to resolve addresses of peer servers that receive the outgoing proxied requests. Depending on the confederation policy or the members' own wishes, all RadSec related DNS information can be completely local, partly local or always looked up over the Internet. Local DNS information is created based on the member settings in the SQL database.

Periodic cron jobs are used to update firewall information based on changes of RadSec and RADIUS client information in the database.

Implementation

The implementation uses hooks offered by Radiator for custom request processing, PostgreSQL database [7] for storing the dynamically updated configuration information and logging information and BIND 9 DNS server [8] for dynamic and optionally distributed request destination configuration.

Radiator PreHandlerHook

Radiator's PreHandlerHook is used to execute custom code implemented for this server. The code runs before the processing of RADIUS requests is started. The hook uses SQL database for functionality such as loop detection, RADIUS and RadSec selection, roaming policy enforcement and decision.

The hook adds vendor specific RADIUS attributes to the requests for affecting the selection of proper authentication handlers. Choosing the correct authentication handler (AuthBy DNSROAM + Authby RADSEC or AuthBy SQLRADIUS) relies completely on the attributes the PreHandlerHook adds to requests.

The RADIUS attributes are also used to trigger Access-Reject messages when loops are detected or the packet can not be forwarded for some other reason. All these vendor specific attributes are for internal use only and are removed before the request is proxied forward.

SQL database

PostgreSQL database is used by Radiator to periodically refresh RadSec and RADIUS client information. The database is populated by a web based user interface running on a separate web server. The web server access to the database server has been limited for security reasons. The contents of the database are also used to periodically update the DNS zone and configuration when changes are detected.

The database contains the organisation, realm, roaming and federation relationship information as well as information about the organisations' RADIUS RadSec servers and clients. The information in SQL database combined with the PreHandlerHook policy decision and enforcement makes it possible for the implementation to support multi-federation roaming with organisation level roaming partner granularity. The granularity is achieved by doing to roaming policy lookup both on the confederation and organisation level.

An example of this kind of multi-level lookup is: Can users from University of Helsinki roam with Arch Red Oy? The former is an eduroam member and the latter is a Funet WLAN roaming member. On the confederation level their confederations do not have roaming agreements, but an organisation level roaming agreement exists between the two. This bilateral agreement can be configured via the web based user interface.

The simplified database model is shown in figure 2.

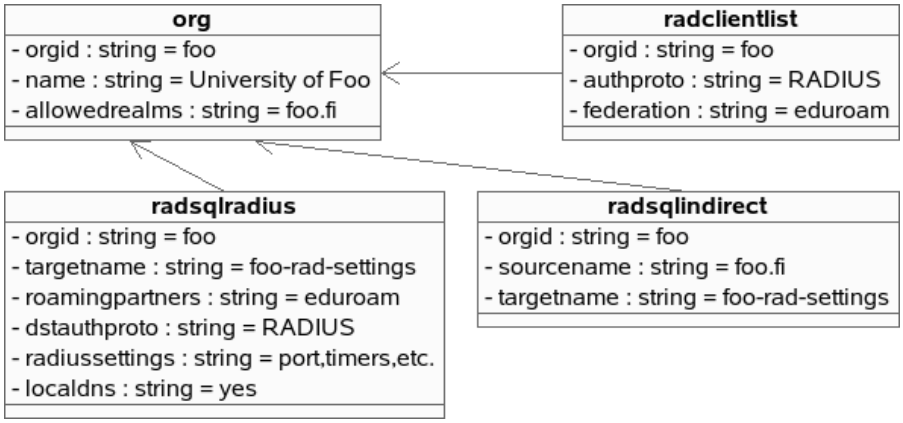

Figure 2: Simplified database structure with example values

The senders, network access servers (NASes) in RADIUS terminology, are modelled by the radclientlist table. The proxying destination is resolved by realm, such as foo.fi, to a radsqlradius entry via the radsqlindirect table. The tables for one federation member are linked with orgid attribute.

For the incoming requests the PreHandlerHook uses federation information from the sender to determine sender's federation. The federation and orgid can be specified as allowed roaming partners by the receivers in the radsqlradius table. The radsqlradius table also contains the information that is used to select RadSec or RADIUS according to the destination organisation's settings.

Web based user interface

Web based user interface is used for managing organisations and their RADIUS and RadSec related information. The configuration information is stored in the SQL database and the information is used for Radiator to periodically refresh the client information. The web user interfaces removes also the need for editing configuration files by hand.

The user interface has two-level hierarchy, where roaming level administrators can add and manage organisations and define allowed realms for the organisations. The organisation level administrators can administer their own organisation's settings such as RADIUS/RadSec server IP addresses, shared secrets and manage organisation realms and subrealms. Organisation administrators can utilise this, for example, for creating a subrealm for RadSec testing without interfering with organisation's other roaming settings.

Local DNS service

Local DNS server is used for RadSec dynamic configuration because Radiator does not yet have a similar kind of handler for RadSec as it does for RADIUS (AuthBy SQLRADIUS). DNS zone information is generated locally from

the SQL database for organisations marked capable for RadSec authentication. The DNS record types are NAPTR, SRV, A and AAAA as specified by the dynamic peer discovery draft [9]. The RadSec related information can be configured in the SQL database via the web based user interface.

The federation members can also maintain their own DNS data to facilitate peer-to-peer roaming. If the members maintain their own DNS data, the local DNS server forwards the queries generated by Radiator over the Internet.

The implementation also supports a hybrid model where some of the organisations have their information in the federation top-level server's local DNS and the others publish their own authentication server information via public DNS servers. This hybrid model makes it possible to migrate gradually from hierarchical roaming model to a DNS based RadSec service discovery architecture in the future.

The decision to generating local DNS data or relying on Internet lookup is recorded in the radsqlradius table's localdns column. The local DNS service is only used internally and does not answer to queries over the Internet.

Periodic jobs and statistics

Cron utility runs periodic jobs that maintain firewall rules, update DNS zone information and push configuration settings to the duplicated server. Periodic jobs also run statistics which create reports on roaming activity and can use the database for collecting information about RadSec and IPv6 usage.

Future directions

Since the initial development and deployment of the upgraded Finnish federation top-level server, the server has been duplicated for enhanced availability and reliability. Both servers are currently (April 2010) connected to the European top-level servers via IPv4 RadSec. First organisation has also migrated to RadSec and several others have been encouraged to do so, but getting organisations to first configure the second top-level server has been a priority.

In the near future getting more organisations to migrate from Radius to RadSec is one of the major objectives as well as getting them to switch from IPv4 connections to IPv6. In a farther future are the DNS based RadSec peer-to-peer roaming tests and utilisation of the hybrid model, which in the even farther future may lead to a completely peer-to-peer multi-federation architectures where the federation selection can be made based on the certificates suggested by the authentication servers.

As the dynamic discovery advances, firewalling the organisation and federation level server becomes more challenging. The main reason is that access to the authentication servers must be opened for arbitrary hosts around the Internet for peer-to-peer connections to work properly. Utilising RadSec and federation signed certificates to control the permission to connect to authentication servers is one option to authenticate and authorise these connections, but the security and usability of these should be tested and piloted in an actual environment. Other additional future research topics are also the ways to survive denial-of-service attacks against organisation level authentication servers as these would now be open to the Internet.

Summary

Designing and implementing a multi-federation and peer-to-peer functionality on the eduroam federation level is already possible and feasible. This paper presented one way to design and implement those utilising Radiator RADIUS server. As a result of the design choices made in this case, the actual implementation is able to support multiple federations and DNS based RadSec service discovery in a way that enables a gradual migration paths for organisations to utilise the new technologies. Organisations and even the top-level server administrators do not need to make drastic changes to their federation connections before they are ready to do so. Even then the various architectures can be used in parallel in a hybrid model. The fine-grained organisation and federation level roaming control also offers new opportunities to conduct roaming research without disrupting the actual production service. One of this kind of roaming research topics could be for example replacing the Radius/RadSec hierarchy with a completely DNS service discovery based peer-to-peer roaming architecture and service.

Acknowledgements

The authors have developed Funet WLAN Roaming and eduroam in Finland since 2002 in cooperation with CSC – IT Center for Science Oy while working in various roles at Tampere University of Technology and Arch Red Oy. In this particular case the authors want to thank Ms. Wenche Backman and Mr. Jari Miettinen from CSC as well as CSC in general for supporting this RadSec development, which led to a design and implementation of a multi-federation and peer-to-peer roaming functionality on the Finnish top-level server.

References

[1] Wierenga, K. and Florio, L. (2005), “Eduroam, past, present and future”, Proceedings of the TERENA Networking Conference 2005, Poznan, Poland, 6 - 9 June 2005.

[2] C. Rigney, S. Williams, A. Rubens, W. Simpson: Remote Authentication Dial In User Service (RADIUS), RFC2865, IETF Standards Track, June 2000.

[3] Keski-Kasari, S., Huhtanen, K. and Harju, J. (2003), “Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET)”, Proceedings of the TERENA Networking Conference 2003, Zagreb, Croatia, May 19 – 22, 2003, (CD-ROM).

[4] Winter S., McCauley M., Venaas S., Wierenga K., TLS encryption for RADIUS over TCP (RadSec). RADIUS Extensions Working Group, Internet-Draft, March 5 2010. Expires September 6, 2010. http://tools.ietf.org/html/draft-ietf-radext-radsec-06 Accessed 15th of April 2010.

[5] Open System Consultants, Radiator RADIUS server, http://www.open.com.au/radiator/ Accessed 15th of April 2010.

[6] T. Lenggenhager (SWITCH), S. Winter (RESTENA), T. Wolniewicz (UMK), D. Lopez (RedIRIS), S. Neinert (USTUTT), J. Rauschenbach (DFN), A. Solberg (UNINETT), I. Thomson (DANTE), JRA5, “DJ5.4.1,2 Advanced Technologies Overview, Second Edition”. February 2009. http://www.eduroam.org/downloads/docs/GN2-08-243-DJ5-4-1-2_Advanced_Technologies_Overview_Second_Edition_20090204080004.pdf Accessed 30th of November 2009.

[7] PostgreSQL, open source object-relational database system, http://www.postgresql.org/ Accessed 15th of April 2010.

[8] Bind 9, domain name server software, http://www.isc.org/software/bind. Accessed 15th of April 2010.

[9] Winter S., McCauley M., NAI-based Dynamic Peer Discovery for RADIUS over TLS and DTLS. RADIUS Extensions Working Group, Internet-Draft, March 5 2010. Expires September 6, 2010. http://tools.ietf.org/html/draft-ietf-radext-dynamic-discovery-02 Accessed 15th of April 2010.

Vitae

Karri Huhtanen (MSc) is a researcher at the Department of Communications Engineering at Tampere University of Technology, researching community network architectures as a part of his PhD studies. He has earlier worked in the wireless communications industry in the research and development departments of equipment vendors and wireless/internet service providers and now leads an Internet services company, Arch Red Oy, concentrating on wireless and wired Internet technologies, services and architectures.

Sami Keski-Kasari (MSc), works currently as a network designer for the Finnish Defence Forces and as a part-time network specialist for Arch Red Oy concentrating especially in the RADIUS authentication systems and architectures. As a part of his postgraduate studies and work as a researcher at the Tampere University of Technology Sami participated earlier in the work of Terena's Mobility Taskforce developing eduroam both on the national and international level.

Heikki Vatiainen (MSc), in addition to his work as a network and security architect in Arch Red Oy, has worked within networks and protocol research in the Department of Communications Engineering at the Tampere University of Technology as a researcher since 1996 and since 2003 as a laboratory engineer. Heikki also held a part-time position of an IT security specialist at TUT. During his studies Heikki has participated in the development of Linux ATM-support, MCOP multicast control protocol and its reference implementation as well as in the development of open source software like the Ethereal network protocol analyser.

Jarmo Harju received his MSc from Helsinki University of Technology in 1979 and PhD in mathematics from the University of Helsinki in 1984. From 1985 - 89 he was a senior researcher at the Telecommunications Laboratory of the Technical Research Centre of Finland, working with the development of protocol software. From 1989 - 95 he was professor of data communications at Lappeenranta University of Technology. Since 1996, he has been professor of telecommunications in the Department of Communications Engineering at Tampere University of Technology, Finland, where he is leading a research group concentrating on network architectures and QoS issues.