Looking into the Future: Exploring Enhancements to eduroam Infrastructure

Authors

Stefan Winter <stefan.winter@restena.lu>
+352 424409 1
Fondation RESTENA
6, rue Richard Coudenhove-Kalergi
1359 Luxembourg
LUXEMBOURG

Chris Phillips <chris.phillips@canarie.ca>
CANARIE
45 O'Connor St., Suite 500
Ottawa, ON, K1P 1A4.
CANADA

Keywords

eduroam, network infrastructures, federations, DNSSEC, DANE

Abstract

Over the past decade, the eduroam™ wireless roaming consortium has grown enormously in popularity by connecting thousands of independent participating institutions worldwide to allow easy and secure access to wireless internet for mobile institutional users. At the inception of eduroam, the RADIUS[1] protocol was only a few years old but was deemed the most applicable. A decade, and many large-scale RADIUS deployments later, the eduroam team has appreciated the durability of the RADIUS protocol but has experienced it's fair share of challenges. Most of these challenges are invisible to end users as they are infrastructure improvements behind the scenes by the eduroam Regional Operators. However, it will be these improvements that enable the eduroam infrastructure to continue to scale as end users behaviour converges on always being connected regardless where they are, with their multiple devices refreshing to the latest technology more frequently than ever.

The eduroam team is evaluating new technologies and approaches with an eye to maintaining the qualities that eduroam is known for while leveraging the infrastructure investments of the eduroam Regional Operators around the globe.

This presentation will highlight some of the technologies and express an opinion on their impact and value to the eduroam service. As well, this presentation will highlight key challenges, emerging requirements, and explore options to upgrade with little to no service interruption. A course of action will be presented for discussion to solicit feedback and insight. While much of the content is technical in nature exploring the implications to policy, procedures, and business models will also be incorporated. What follows is a brief outline of the presentation.

- **Challenges**
- Some of the challenges encountered with the classic RADIUS approach are:
- static server-to-server connections
- manual reconfiguration needed for new participants
- aggregation of traffic into single points of failure
- unreliability of the RADIUS UDP transport.
- determining where to route traffic by Top Level Domains (TLDs) works well, but not so well for .com,.net,.edu, .eu domains that many eduroam end users have.

Over the operational period of eduroam the RADIUS core has remained the same but the transport has had incremental improvements(RADIUS/TLS[2]) which help address the aforementioned challenges.

RADIUS/TLS solves some of these challenges, but in itself does not provide our sought after flexibility for server-to-server interconnections. This flexibility can be added by operating RADIUS/TLS with a dynamic discovery fabric. Several options exist each of which have benefits and drawbacks. Choosing a path forward needs to strike a balance between them as the eduroam infrastructure goes into the next decade.

- **Options explored in this presentation:**
- **Dynamic Server Discovery with DNS** [3]. Due to its wide deployment there is a wealth of information on it's challenges and benefits that help set the stage for comparisons to other approaches. As DNS provides no cryptographic protection, the Public Key Infrastructure (PKI) needs will be discussed in this model as well.

- **Dynamic Server Discovery with DNSSEC.** There is an IETF specification[3] that also covers this advanced discovery option. It's pros and cons are very similar to the first option, but has some unique characteristics of its own with PKI elements available via DNS.

- **Use of DNSSEC in combination with DANE[4] records for dynamic server discovery.** In this option, both the name resolution and the authorisation checks are stored in the Domain Name System and can use self-signed certificates. One of the two aspects is under control of the federation administrator, the other one under control of the participant. The challenge around the TLDs that do not necessarily align with regions will also be discussed.

- **Moonshot Trust Router model.** Is a new protocol[5] that is being incubated alongside the RADIUS community and will be briefly touched on.

Acknowledgements

References

[1] http://tools.ietf.org/html/rfc2865
[2] http://tools.ietf.org/html/rfc6614
[3] https://datatracker.ietf.org/doc/draft-ietf-radext-dynamic-discovery/
[4] http://tools.ietf.org/html/rfc6698
[5] http://tools.ietf.org/html/draft-mrw-abfab-trust-router-01

Author Biographies

Stefan Winter graduated in Computer Science at the University of Karlsruhe, Germany, in September 2004, with a specialisation in telematics and foundations of Computer Science. Since then he is working as R&D Engineer for the Luxembourg Research and Education Network RESTENA, where network roaming and identity federations are in the focus of his activities. He led the R&D work for eduroam during the second half of the GN2 project, and is now continuing these efforts as Roaming task leader in GN3. He is also member of the Global eduroam Governance Committee and an active IETF participant.

Chris Phillips is the Technical Architect for CANARIE's Canadian Access Federation, an access federation operating the eduroam and SAML trust fabrics in Canada. Chris has a BSc in Computing from Queen's University in Kingston (1995) and has worked previously in the private sector through multiple acquisitions followed by just under a decade with Queen's working on internet scale systems for directory, mail, single sign on, and identity management systems that interact with Peoplesoft. Chris is also a member of the Global eduroam Governance Committee, participates with IETF activities, and is an active participant in Internet2 working groups.