

The RADIUS Authentication Fabric: Solving the authentication delivery problem

Michael Helm, Tony Genovese, Roberto Morelli,
Dhivakaran Muruganatham, John Webster
ESnet/LBNL

Stephen Chan, Eli Dart
NERSC

Tom Barron
ORNL

Edwin Menor, Andy Zindel
InfoBlox

Abstract

We propose a *RADIUS authentication fabric* (RAF) to meet the interoperability needs of research sites deploying one-time password (OTP) authentication services. Sites see OTP as an essential countermeasure to widespread hacking, but OTP deployment can also disrupt the numerous (and mission-critical) collaborations between sites and other research institutions. The RAF provides a secure infrastructure for routing authentication traffic, and enables “single token sign-on” for each member of our research community. We have a good foundation for this service, and we have identified what we need to do to advance to a production-quality service for our community.

1 Overview

DOE Lab Computing Facilities Hacked

Security compromises of DOE laboratory research computing facilities in early 2004 caused staff and management to reassess security policies and the level of vulnerability these computing facilities present. While a full assessment is yet incomplete, exploitation of *reusable long-term passwords* was identified as one of the principal methods used by hackers to gain entry to computer facilities, or escalate privileges once initial entry had been gained. Hackers were able to install keyboard sniffers, for example, on vulnerable machines, allowing the hackers to record passwords when used by legitimate users to login with *ssh* to remote systems. The legitimate users’ identities on the remote system were now shared by the hackers, who could use these passwords to login at any time of their choosing.

The hackers exploited many other weaknesses and used a variety of techniques to overcome security measures at various sites. But exploiting the use of long-term, reusable passwords, built-in to UNIX and Windows, and well understood by the user community, allowed the hackers their first access to remote sites. Without that initial help, they would not have been able to exercise other techniques.

Why OTP?

An OTP-based authentication infrastructure would be highly resistant to password attacks. Keyboard sniffers or memory dumps would be useless, since the password is only usable once. There is little reason to think that end user computer systems at colleges, at home, or in public facilities such as kiosks will improve in security over time, unfortunately, so it is reasonable to expect that keyboard sniffing of passwords will be extremely common from now on. OTP is a way of suppressing chain reactions resulting from password theft and illicit logins.

An OTP-based authentication infrastructure presents a number of problems, and vulnerabilities of its own, that must be addressed. A service (a web server, for example) and the end user (who needs to login) have to have some way of agreeing on what the correct password is, without signaling this information to a third party (the hacker). The burden of managing this password information has to be reasonable to both parties. In practice, the service outsources authentication decisions to a back-end service, usually provided by the OTP vendor, and the end user carries an OTP *token*, a small hardware device that generates passwords. Outsourcing the authentication allows the service to focus on its core duty, but introduces the threat of a “man in the middle” between service and OTP source of truth, which might give the service wrong answers. The token simplifies the end user experience to some extent, but it usually requires synchronization with the OTP back-end source of truth. There are also some expected and unexpected threats (early in 2004, someone discovered an RSA token parked in front of a webcam). The token can stop working or be lost or stolen, just like a car key.

NOPS

Service providers and security experts from several affected labs came together to form the NOPS group in March 2004. Initially NOPS discussed methods that could provide more secure access to services, without disrupting cross-site interoperability. The group reviewed work on OTP products, pulling together product reviews and previous work done at other laboratories. Discussion proceeded to clarifying requirements.

- How would a large-scale OTP deployment actually be accomplished?
- What product or products would be used?
- What would happen to the applications and services?

A requirements document ([CHAN2004]) was produced in April 2004 that captured the current thinking of the group (with a Grid focus).

Pursuing a DOE-wide, centrally run OTP deployment was considered, but it was felt by most parties that it would be very difficult to achieve, no matter how desirable. On the other hand, as each institution went its own way, different products would be deployed on different time schedules. Different products, or site-specific authentication, would undoubtedly mean that individuals who had responsibilities at multiple sites would be forced to manage multiple dongles, tokens, key fobs, or other one-time password gadgets. Something needed to be done to head off this problem before implementations imposed it on the research community.

RADIUS Authentication Fabric

ESnet proposed the RADIUS Authentication Fabric (RAF) to support this OTP initiative in April 2004 [GIRAF]. This proposal supported an OTP to Grid bridging effort.

[NCSA](#) was looking at building a PAM module (see [XSSO97] and [PAM2003]) into its popular myProxy credential store ([GridLogon] and [MyProxy2001]), and using RADIUS client capability in PAM to reach the OTP back-ends. RADIUS ([HASSELL2002], [RFC2865]), an [IETF](#) AAA¹ protocol, is widely supported in industry and all major OTP vendors support it. At ESnet, we were experimenting with a RADIUS “appliance” manufactured by [Infoblox](#) ([RADONE]). We realized we could solve the OTP service problem, by creating a RADIUS – based routing service for authentication requests. A customer who needed to run a Grid job at a remote site would login to the local “myProxy” server, which would forward the OTP credentials to the ESnet RADIUS infrastructure. The ESnet RADIUS service would know where all the OTP back-ends were and route appropriately – but how? The end user would use the *RADIUS realm* concept to identify himself and his home site: [user@site](#). The ESnet RADIUS infrastructure would route queries and responses back to the local myProxy service, which would then make the authentication decision.

We proposed a pilot – feasibility study at the April 2004 ESSC, and spent several months working on it in cooperation with members of the NOPS group and Infoblox ([RAFPR]). We have refined the architecture and resolved some basic technical questions about RADIUS and OTP. We have begun development of the federation governing body that would be needed to manage this infrastructure. We have extended the scope of the project to support other important collaborative technologies. We have also begun looking at Kerberos as well as more modern protocols, and discovered a similar initiative underway in Europe. We have the foundation for an important new service for the research community, a new way of delivering and managing authentication information.

2 RAF Architecture

The RADIUS authentication fabric routes authentication traffic between a service and an authentication server.

We will work through a RAF use case (entirely fictitious), in Figure 1 below, to explain the elements of the architecture. Here we see four participating sites, which have federated their OTP-based authentication at the ESnet RAF. Each site provides its own OTP service. Each site provides a public interface to this OTP service – a local RADIUS server.

¹ AAA – Authentication, Authorization, and Accounting. See [SMITH2002].

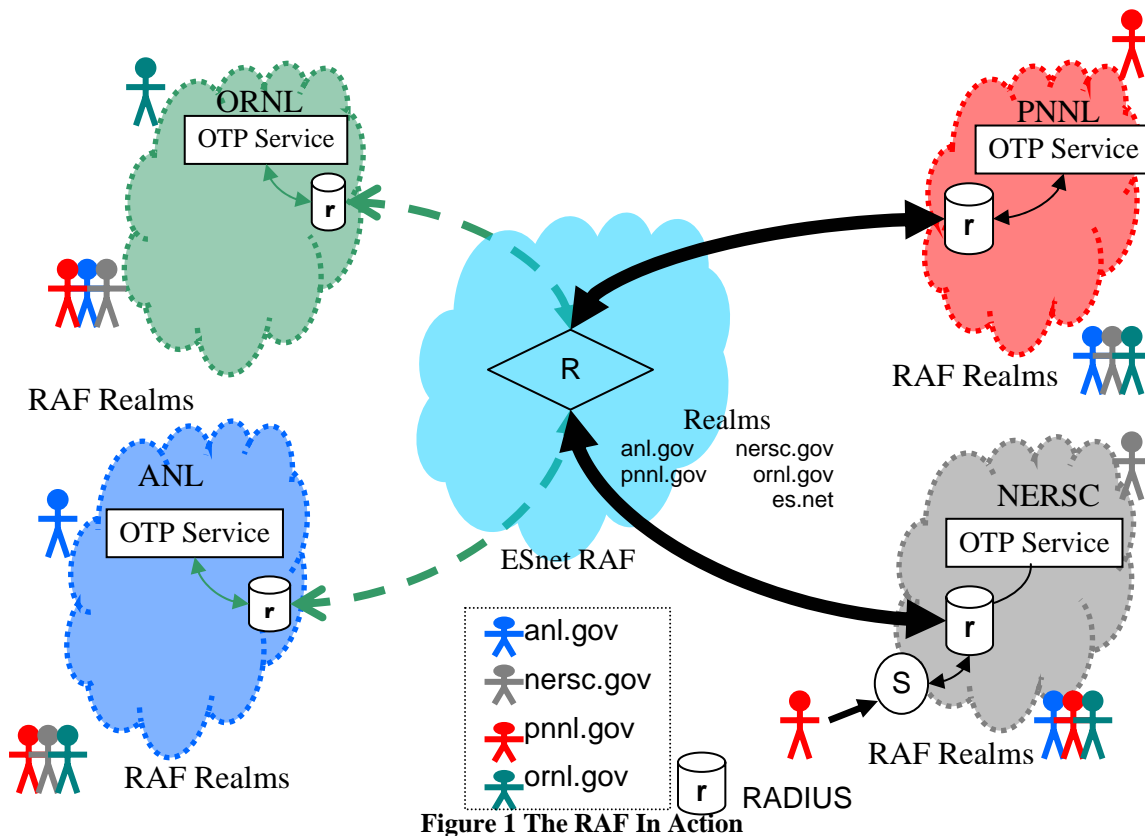


Figure 1 The RAF In Action

A scientist from PNNL wants to use a service at NERSC (lower right). The scientist is prompted for a user name and password from the service (“S” bubble in the figure). Our scientist user provides his RAF identity *johndoe@pnnl.gov* and a password generated by the OTP token that PNNL issued to him. This login dialogue is passed on to the local RADIUS server at NERSC (little “r”), which recognizes *johndoe@pnnl.gov* as a RAF realm identity, not a local identity. It forwards this login request to the ESnet RAF (“R” in the diamond in the center), through RADIUS proxy. The RAF knows where the authoritative authentication server for “pnnl.gov” is, and forwards to the PNNL RADIUS server (upper right little “r”). Both of these RAF RADIUS proxy connections are over a VPN established between the RAF and each site server. The PNNL local RADIUS server routes this authentication query to the PNNL OTP server, which verifies or rejects the authentication. The results are returned over the same path to the NERSC service application. On successful authentication, the application then makes an access decision (authorization).

The core of the RAF is a set of RADIUS appliances operated by ESnet. These appliances run only the RADIUS protocol, and some administrative and back-end functions; they are not general purpose computers. The appliances are configured in a “highly available” (HA) configuration pair, and each pair constitutes a single node. Several nodes are deployed around the ESnet core and at critical sites. Each node presents identical information. The nodes themselves are not visible to the sites or the end users, and the failure of a single node will not disable the RAF or a site (uncompleted authentication transactions would be lost).

Each site presents a RADIUS service to the RAF, and to local services that authenticate both local and remote users. The local RADIUS service *must* support RADIUS proxy. Sites provide an OTP service of their choosing, and configure their local RADIUS service to route authentication requests to the OTP vendor's back-end authentication database. Services that need to support remote users are configured to use the local RADIUS service for authentication.

Sites federate at the ESnet RAF. The ESnet RAF federation addresses:

- A *formal agreement* between the site and the other partners about OTP management.
- A *naming convention* for RADIUS realms, based on sites' DNS domain names;
- A *shared secret* between a site and ESnet RAF, unique per site;
- A *VPN* between the ESnet RAF and site RADIUS servers.

Only RADIUS node information is federated; decisions about authorizations, services, and management of RADIUS clients are site decisions. Sites are free to limit their participation in the federation: they may restrict locally the list of other realms that may authenticate, and they may limit the participation of their OTP service in the federation.

One-Time Password Technology

One-time passwords (OTP) ([SMITH2002]) replace static, long-term, re-usable passwords with a single-use password based on an algorithm². While the account stays constant, each login requires a different password. The security experts in the NOPS group argue that re-usable passwords give hackers an enormous advantage, direct access to vulnerable systems thru stolen passwords. Eliminating re-usable passwords will reduce exposure (see [CHAN2004]).

End users will have OTP tokens. The NOPS group argues for a hardware token, a small device that generates an appropriate password for the end user to whom it is issued. The token is synchronized to an OTP back-end authentication server.

A service relying on OTP will act much like an existing service: it will engage the end user in a login dialogue requesting an account name and a password. The end user provides the appropriate password from his OTP token. The login name and password are forwarded by the service to the OTP back-end service for verification. If the OTP back-end approves the authentication, the service proceeds to an authorization decision.

RADIUS

RADIUS (see [RFC2865]) is an Internet standard protocol, designed to carry authentication information between a service and a shared authentication server. It is an ideal transport protocol for supporting OTP – based infrastructure. It is widely supported in industry: major OTP vendors support RADIUS access to their back-end authentication service. It is widely supported in services, e.g. firewall products, PAM RADIUS client support for login and *sshd*, web server authentication, and many others.

The RADIUS authentication model is a generalization of the OTP authentication model above. Authentication information is forwarded from a RADIUS client (such as a web server) to a RADIUS server, for verification. The RADIUS server can forward the authentication query to other RADIUS servers (using RADIUS proxy), or an external

² Algorithm - designed to return a *non-guessable* password. An example of how this is done is found in the [S/Key RFC](#).

service (using a plug-in interface). Transactions involving passwords are secured and encrypted using a shared secret between RADIUS client and server. RADIUS can support a wide variety of authentication technologies and special service requirements. RADIUS can support referrals and chaining through RADIUS proxy and RADIUS realms, allowing different communities and different technologies to be served simultaneously.

RADIUS Naming Convention

A naming convention is essential to the RAF. In a simple RADIUS environment for a small work group, every user could be assigned to a single authentication database. The RADIUS standard provides the concept of a RADIUS *realm*, to allow authentication and authorization decisions to be grouped and dispersed, but does not define realm in depth. In the RAF, the realm determines where the authentication query will be routed. Our naming convention:

- Realms are site top level domain names
- Local names are site decisions

Names then look like “mike@es.net” or “John.Q.Public@biglab.org”. Names must be unique across the RAF (only one OTP server can speak for “mike@es.net”), and this meets this requirement. We allow for growth with subdomains, and we provide a naming convention that will be familiar to most users. RADIUS names (and realm names) are case-sensitive (RADIUS vendors may limit this feature). Site help desk personnel will have to be made aware of this, and the RAF federation should moderate naming practices where possible.

3 Applications and Services

Broadly, the RAF is designed to support collaborations among communities of researchers requiring a common authentication solution. The RAF is focused on the requirements identified by the NOPS group ([CHAN2004]). Our experiences developing and deploying our services are documented extensively in ([RAFPR]). But the RAF must support real applications too. We have tested some important applications that are likely to use the RAF, and begun design work on others.

OTP

OTP products from at least three vendors are in use at several DOE laboratory sites, and we have experience with two of them: [RSA SecurID](#), and [CryptoCard](#). ESnet has worked on SecurID integration and has a small test server and deployment in-house. Oak Ridge (ORNL) also has a separate SecureID deployment on the RAF. NERSC has a CryptoCard deployment on the RAF.

Applications Area

We are integrating some important collaboration services with RADIUS and OTP. All of these services use a RADIUS client embedded in a pluggable authentication module (PAM). PAM provides a widely used login service on modern UNIX platforms. The typical system administrator is likely to be more familiar with PAM than RADIUS, or other authentication technology. PAM presents some challenges. It is a layered API, providing the capability to call out to modules that manage authentication, access control,

session, and password management, plus a policy language to hold it all together. We have had positive experiences with PAM-RADIUS integration, but we are just beginning. Working directly with the applications is important. The boundary between the application and the RAF (or any other authentication infrastructure) is often somewhat fuzzy. Names are important. The RAF requires each customer to have a RAF-unique name, such as mike@es.net, to route the request properly. But an application such as *sshd* may need a different style of name or a local name. A Grid application may need an X.509 – style name or a handle into a policy database for an access control decision. We have looked at some typical applications to make sure we can engineer the RADIUS infrastructure properly, and identify what steps need to be taken in PAM or the RADIUS client to complete the integration process.

There are numerous applications that might benefit from OTP, but may not be appropriate for the RAF: financial services, site-based IMAP mail services, and the like. We are looking at applications that matter to cross-site collaborations, where the RAF can add value by minimizing the number of tokens end users need, by minimizing system administrator burden, and simplifying the relationships between sites.

GIRAF

The Grid-Integrated RADIUS Authentication Fabric ([GIRAF]) extends the RAF to support access to Grid proxy certificates (see [RFC3820]). There are two proposed variants of this service. One relies on the NCSA GridLogon (an extension of the myProxy service; see [GridLogon]). The myProxy service issues a certificate on successful OTP authentication, signed by the long-term key it holds on behalf of the account owner. NCSA has developed a PAM module for myProxy and begun experimentation. Another variant, the ESnet SIPS service (see [ESOTP], slides 28-30), is still in the design phase. The Site Integrated Proxy Server (SIPS) dispenses with the long-term credential store, and issues a certificate on successful OTP login. The SIPS is a trusted subordinate certificate authority (CA). The profile for this type of CA is being developed in the Global Grid Forum.

In either case, the GIRAF provides a gateway between the OTP authentication and Grid security services. For Grid applications, Grid proxy certificates are provided, and no changes to applications need to be made. But these short-lifetime proxy certificates are only provided to end users who can authenticate with a token to a trusted OTP infrastructure through the RAF.

Sshd

ESnet has deployed an *sshd* gateway service based on an *openssl* server and PAM – based authentication. This is based on a standard distribution of *openssl*.

Apache

ESnet and ORNL have deployed Apache-based web servers that require client authentication. These servers are configured to allow OTP authentication from any of the NOPS partners to succeed, and deny authentication from other parties. NERSC has been developing a more sophisticated Apache web server that maps RAF names to local account names.

4 Outstanding Engineering Issues

The feasibility study has concluded, but the pilot phase of the RAF has just begun. We have identified a number of issues that need to be explored. Not all of these are strictly RADIUS or RAF problems; for example the applications and PAM present certain problems, and OTP products have limitations. The pilot phase will explore these problems (or a subset) and develop solutions and recommendations.

RAF Core

How can we provide a reliable and consistent interface to the RAF core? The core needs to present a consistent interface to the RADIUS servers at the edge (the sites). The sites should not need to be aware of internal structure or specific configurations of ESnet servers. ESnet needs to develop a replication strategy that allows multiple, redundant servers to be deployed around the ESnet core, while presenting the same interface to the edge RADIUS servers through DNS. In the long run, we need to develop a comprehensive, wide-area high availability solution. We anticipate that we will need to have multi-master replication in the future, as our RADIUS data management grows more sophisticated.

How can we provide reliable and consistent service at the RAF edge? We need to develop a simple referral and configuration service for RADIUS at the client, so that changes to the RAF do not cause perturbations at the local site. We need to develop a “catch-all” proxy referral with our RADIUS vendor, and explore this capability in other RADIUS servers.

We need to understand quality control and problem isolation issues better. The failure of an individual node in the RAF will cause an authentication to time out or fail; we need to make sure this failure information gets routed to the end user properly so that he can react, not become confused.

RADIUS Operations and Security

Compromise of RADIUS servers, whether in the ESnet core or at sites, has grave potential for system compromises. For services, a RADIUS compromise represents a man-in-the-middle threat, since a compromised RADIUS server can hand back an illegitimate “successful authentication” response to a local service. This threat is especially serious in the ESnet core, since these RADIUS routers return responses to all members of the federation. RADIUS servers connecting to the RAF must present as few opportunities for compromise as possible. The ESnet core will deploy a RADIUS appliance, which presents no services for compromise, and will manage these servers through a VPN or IPSEC connection. We will discuss enhancements and security auditing features with Infoblox in the next phase of the project, as part of the replication and wide-area HA work. While we cannot mandate our deployment at every RAF site, the RAF federation will take on the work of publishing security practices and creating a policy for site RADIUS servers on the RAF.

RADIUS, despite being a very mature protocol, presents us with a great many research opportunities. RADIUS security (see [HASSELL2002], p. 131-138) is adequate to the task, but only just. RADIUS provides no data confidentiality except for password data on the wire, and little data integrity protection. We will deploy VPN or IPSEC ([RFC2411]) between RAF Core and edge servers. This will minimize the possibility of a man-in-the-middle attack on the RAF. RADIUS traffic will also have to traverse

firewalls, both at ESnet and local sites. These closely linked issues require careful study.

OTP

RSA SecurID needs to be solidly supported. The one-time passwords are time-based: the token and the back-end server must be synchronized, and each new password has only a sixty-second lifetime. We need to study issues of network latency and node failure. We need to make sure that the quality of the RADIUS services and the network itself cause few problems, and when problems occur, the problem is obvious to the end user and local administrators.

The SecurID back-end server is configured to defend against multiple uses of the same password inside the sixty-second validity period (replay attack). In other words, the end user cannot login to more than one service in one validity period, and a failure, or even accidental replay, may result in the back-end server locking out the user as a defense. This needs to be studied in-depth. In particular applications and end user expectations need to be studied. Replicated SecurID backends need careful management; replicas that are out of contact with each other for some time may each return an authentication approval for the same password. Other OTP technology may have similar quirks; this lore should be captured in a community best practices document. Other OTP technologies are capable of supporting challenge-response as part of the authentication dialogue. Initial reports from NOPS partners suggest this will not be a popular configuration as it is too difficult for end users. However, it is popular with security officers. Understanding challenge-response OTP better will benefit the community.

Applications

Each application influences the RAF architecture, sometimes subtly, often overtly. The applications that we have studied are not adapted completely to RAF usage, and some development, particularly PAM development, will be required.

Secure, Extensible, Token Authentication

NERSC has proposed (see [SETA2004]) a comprehensive, Kerberos-based service for sites. Supercomputer customers need to run batch jobs; this is an essential capability. This proposal will link techniques to enable Kerberos support of batch jobs, to previous work supporting OTP authentication to Kerberos, and use the ESnet RAF to provide this service to NERSC customer base.

Grid Integrated RADIUS Authentication Fabric

The most interesting application, and the one that needs the most development, is the Grid Integrated RADIUS Authentication Fabric or GIRAF. NCSA code has become available recently for a test deployment of the myProxy-based service. We need to develop the SIPS design and produce a demonstration service. SIPS is a direct gateway between the RAF and Grid services. A RADIUS authentication results in a grid proxy certificate, which is then used to run Grid jobs.

Web server client authentication

Each page on a secure web server can require authentication. Often this is hidden from us when we use such sites, but navigation around a web site or multiple web sites using

OTP authentication can be very annoying. Each page can require a new password from the token, and replays from the browser can cause security lockouts. There are solutions for this problem from the OTP industry, and we need to explore these for suitability. GIRAF (see above) might also help, by substituting X.509 client certificate login for OTP login.

Ssh

RADIUS realm names, and UNIX account names are significantly different, but the *openssh* PAM module does not do any mapping. This must be improved. General features and expectations about *ssh* usage in a gateway are not fully understood. Lawrence Berkeley National Laboratory in particular has been studying this problem in-depth (to be published).

Large scale file transfers

There are only a few customers who require extraordinarily large file transfers – but they are very important. The network bandwidth and data store requirements are severe, and a caching gateway service is probably not adequate in most cases. What can we do for the source and endpoints of these transactions? Will a supported Grid service meet this need?

Firewalls and VPNs

Many sites will require their customers to authenticate to a firewall or acquire a VPN for access to some services. RADIUS support for firewalls and VPN products is well supported in industry by all parties, but an engineering demonstration of this is needed. Both ESnet and ORNL have begun this work.

Client security

RADIUS secures the connection between an application, like a firewall authentication daemon, and the RADIUS service, as well as any back-end the RADIUS server itself uses to verify authentication. It has little to offer the client. We need to provide full end-to-end security to the client. This remains a research problem, but for the immediate future we will support EAP-TLS ([RFC2716]), which ESnet is already investigating for an internal use.

5 Federation

The RAF links multiple OTP authentication services from independent DOE laboratory sites. Each site has its own OTP policies and practices. Before a site will join the RAF it must develop a level of trust in the other members. To set up an environment of trust, we are developing a common set of policy and practices in the RAF federation document (see [RAFFED04]). The federation document charters our OTP federation, and describes how we will manage existing and future issues. This federation uses a new federation template which is currently being reviewed by the Global Grid Forum. Before they join the RAF federation, each member will review the policies and practices to determine how they fit with local policies. If some issues of the RAF federation do not meet local requirements, they can work with the RAF Federation for potential changes. Any organization that joins the RAF agrees to abide by the RAF federation policies and practices.

RAF Federation issues

The OTP federation document addresses the following issues (common to most federations).

1. General introduction and statement of goals
2. Description of the federation - membership
3. General architecture of the federation
4. Operational requirements for equipment and personnel
5. A statement on liability
6. A statement on the financial responsibilities of the members and the federation in general
7. How will the federation handle audits and conformance
8. A statement on member and customers' privacy and confidentiality.
9. How the federation will handle compromise and disaster recovery
10. How the federation will manage itself

Some specific issues that the RAF federation must address in the federation charter:

1. Types of authentication permitted
2. VPN or IPSec management
3. Token management – replacement, resynchronization, etc
4. Radius shared secret management
5. RADIUS configurations
6. RADIUS replication
7. Realm naming practices

Trust starts with an understanding of how each member operates his OTP and RADIUS systems and software. This transparency gives other members a level of trust in the operations environments of each member. ESnet as operator of the RAF will have its policy and procedures developed and reviewed by the RAF membership. ESnet, because it will control the RADIUS backbone servers, has great responsibility for the integrity and viability of the RAF. How do we verify that all parties stick to their agreements? Independent audits are the traditional means, but are difficult. We will begin with self-auditing and publishing of members' operations and policies. The federation membership may wish to develop a more rigorous auditing strategy as required.

6 Future Work

Is the RADIUS authentication fabric the last word in authentication in the research scientific community? There are a number of other opportunities in view now, and no doubt others will emerge. We will describe two of them.

Eduroam and SALSA Netauth

In late September 2004 we were made aware of a parallel effort in Europe. [Eduroam](#) ([EDUROAM]), sponsored by [TERENA](#), is a hierarchical RADIUS architecture supporting *roaming*. Its primary customer is the researcher temporarily located at a member institution, who needs to gain access to the local wireless network for his laptop in a secure fashion.

Eduroam offers multiple levels of RADIUS proxying and delegation, and appears to have advanced filtering techniques that would greatly improve the RAF. Eduroam has also begun exploring other advanced authentication technology. Eduroam offers us the opportunity to extend the reach of the RAF to Europe (and vice-versa).

Eduroam is an independent proof of concept of the RAF architecture. The [Internet2 SALSANetauth](#) working group, in the “Federated Wireless Network Authentication” (FWNA) sub group, has recently started exploring the possibility of developing a service similar to Eduroam for the US research and higher education communities. Supporting this work could greatly enhance the utility of the RAF in the US research and academic communities.

Beyond RADIUS – the “*” Authentication Fabric

We need to look beyond RADIUS. We need to provide full end-to-end security for both service and end user; RADIUS must be extended to meet this requirement. EAP-TLS is a good first step. New protocols such as AuthA ([AUTHA04]) should be investigated. *Kerberos* (see RFC1510[]) is important in the research community. Unfortunately, it is neither ubiquitous, nor interoperable with RADIUS. The development of an EAP-KERBEROS or equivalent should be considered.

The IETF has developed DIAMETER ([RFC3588]), an advanced protocol to replace RADIUS. DIAMETER addresses some of the security and reliability issues in RADIUS. Eduroam (see above) is tracking this standard.

7 Conclusion

We now have a solid technical basis for the RADIUS authentication fabric. We will continue the RAF into a pilot phase, where we will extend the depth of the RAF by working on the engineering issues we identified in the feasibility study, and the breadth by strengthening support for selected applications and developing working governance in the RAF federation. Prospects for a successful RAF production service are very bright. The RAF will significantly improve the capabilities for secure collaboration in DOE Office of Science programs. We will also collaborate with similar initiatives such as Eduroam and I2 SALSANetauth to extend the reach and capability of the RAF.

8 RAF Team

ESnet: Tony Genovese, Michael Helm, Roberto Morelli, Dhivakaran Muruganatham, John Webster

InfoBlox: Edwin Menor, Andy Zindel

LBNL: Olivier Chevassut

NERSC: Stephen Chan, Eli Dart

ORNL: Tom Barron, Sue Willoughby

ANL: Remy Evard, Gene Rakow, Craig Stacey; Frank Siebenlist (Globus)

PNNL: Craig Gorenson

NCSA: Jim Basney, Von Welch

9 References

[AUTHA04] Abdalla, M &al. “One-time Verifier-based Encrypted Key Exchange”. Submitted to PKC’05. Aug 2004

- [CHAN2004] Chan, S., Lau, S., Srinivasan, J., and A.Wong. "One Time Password Authentication for Open High Performance Computing Environments". *NOPS* group, April 2004. <http://www.doe grids.org/CA/Research/OTP-final.pdf>
- [EDUROAM] Sankar, James and Klaas Wierenga, "Inter-NREN Roaming: Final Report". TERENA Technical Report. TF-MOBILITY. 2004. <http://www.terena.nl/tech/task-forces/tf-mobility/firsttofdels/TF-MobilityfinalReport.pdf>
- [ESOTP] Helm, M & al. "ESnet PKI One Time Password Support". ESSC slides, 27 Apr 2004
- [GIRAF] Helm &al, "Grid Integrated RADIUS Authentication Fabric." ESnet ATF team, June 2004. <http://www.doe grids.org/CA/Research/GIRAF.pdf>
- [GridLogon] Basney, J., Welch, V., and F. Siebenlist, "A Roadmap for Integration of Grid Security with One-Time Passwords". NCSA and Globus. <http://www.ncsa.uiuc.edu/~jbasney/grid-otp.pdf>
- [HASSELL2002] Hassell, Jonathan, *RADIUS*, O'Reilly, 2002
- [MyProxy2001] Novotny, J., Tuecke, S., and Von Welch, "[An online credential repository for the Grid: MyProxy](#)". In *Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10)*. IEEE Computer Society Press, 2001. <http://www.globus.org/research/papers/myproxy.pdf>
- [PAM2003] Smorgrav, Dag-Erling. "Pluggable Authentication Modules." FreeBSD, 2003. http://www.freebsd.org/doc/en_US.ISO8859-1/articles/pam/
- [PMA04] Cowles, R &al. "Policy Management Authority Model Charter". GGF. Feb 2004. https://forge.gridforum.org/projects/caops-wg/document/Grid_PMA_model_charter/en/1
- [RADONE] "RADIUS One Network Appliance". Infoblox, 2004. http://www.infoblox.com/products/radiusone_overview.cfm
- [RAFPR] Muruganantham, D., &al, "ESnet RAF Progress Report". Work in progress. 2004
- [RAFFED04] Genovese, T. &al. "DOE One Time Password Federation". Work in progress. 2004
- [SETA2004] Andrews, M., Chan, S., and Stephen Lau, "Secure, Extensible, Token Authentication for Department of Energy High Performance Computing". NERSC. Draft project proposal. 2004.
- [SMITH2002] Smith, Richard E, *Authentication: From Passwords to Public Keys*, Addison-Wesley, 2002
- [RFC1510] Kohl, J and C Neumann, "The Kerberos Network Authentication Service (V5)". RFC 1510. IETF, September 1993. <http://www.ietf.org/rfc/rfc1510.txt>
- [RFC2411] Thayer, R &al, "IP Security Document Roadmap". RFC 2411. IETF, November 1998. <http://www.ietf.org/rfc/rfc2411.txt>
- [RFC2716] Aboba, B. and D Simon, "PPP EAP TLS Authentication Protocol". RFC 2716. IETF, October 1999. <http://www.ietf.org/rfc/rfc2716.txt>

[RFC2865] Rigney, C. &al, "Remote Authentication Dial In User Service (RADIUS)". RFC 2865. IETF, June 2000. <http://www.ietf.org/rfc/rfc2865.txt>

[RFC3588] Calhoun, P. &al, "Diameter Base Protocol". RFC 3588. IETF, September 2003. <http://www.ietf.org/rfc/rfc3588.txt>

[RFC3820], Tuecke, S. &al, "Proxy Certificate Profile". RFC 3820. IETF, June 2004. <http://www.ietf.org/rfc/rfc3820.txt>

[XSSO97] X/Open Single Sign-On Service (XSSO) Pluggable Authentication Modules. The Open Group, 1999