

Combining RADIUS with Secure DNS for Dynamic Trust Establishment between Domains

Henk Eertink[†] Arjan Peddemors[†] Roy Arends[†] Klaas Wierenga[‡]

[†]INCA Group, Telematica Instituut, Postbus 589, Enschede, The Netherlands
{ Henk.Eertink, Arjan.Peddemors, Roy.Arends }@telin.nl

[‡]SURFnet, Postbus 19035, Utrecht, The Netherlands
Klaas.Wierenga@SURFnet.nl

Keywords Network Roaming, Authentication Infrastructure, Dynamic Trust Establishment, RADIUS, Secure Domain Name System

Extended Abstract

Current solutions for the authentication of users in roaming situations, where users move between the networks managed by different authorities, are most often based on RADIUS [4]. One example of such a roaming domain is the *EduRoam* [3] initiative, which establishes a European RADIUS authentication hierarchy. The trust establishment between the RADIUS entities in these domains is accomplished using a static shared secret for each peer, where authentication requests are passed on from one entity to the other until the request reaches the authenticating server. This mechanism has a number of disadvantages, namely (1) the traffic generated for authentication must travel through a chain of RADIUS proxies, while the authentication itself is only of interest to the RADIUS entities at the edges of the chain (the one that needs to authenticate a user and the one that checks the user credentials), (2) intermediate proxies may inspect the RADIUS payload which places extra requirements on the type of authentication, i.e. in practice only EAP-TLS or tunneled EAP types are used, (3) having a fixed chain of proxies is quite error-prone, as failure of one of the servers in the chain can easily result in denial of service to roaming users, (4) a shared secret must be agreed upon and exchanged out-of-band for secure communication between RADIUS peers, and (5) it is not easy for participating entities in a roaming agreement to obtain an overview of all other partners in the agreement.

In this paper we propose a solution that is compatible with existing RADIUS deployments, while able to setup peer-to-peer trust relationships between RADIUS proxies in a dynamic fashion. This means that we need to define a mechanism through which RADIUS shared secrets can be established dynamically after both entities are confident that they share a common policy, implemented through a roaming agreement. Hence, the solution consists of two components:

1. a mechanism that is used to derive whether two parties are part of the same roaming infrastructure, and to discover the proper authentication server of each other
2. a mechanism to establish a shared secret for secure RADIUS interactions between these authentication servers.

For the first problem we use DNSsec [1], and adding a simple key-establishment protocol alongside the RADIUS protocol solves the second problem.

The authentication process for this scenario is depicted in figure 1. The following actions take place:

1. A RADIUS client, such as an 802.11 WLAN access points, needs to authenticate a user and sends the user credentials, including the user realm/domain, to the local RADIUS server.
2. (and 3, 4, 5) The RADIUS server in the visiting domain notices that this user is not part of the own domain and decides to setup a direct connection to the RADIUS server that is capable of executing the authentication. It looks up, through Secure DNS, the IP address and certificate of the RADIUS server of the home domain *as part of the roaming domain DNS tree*. The roaming domain administrator manages this tree, effectively deciding which parties cooperate in a

roaming agreement. Secure DNS makes sure that the answers are correct and trustworthy. Every RADIUS server has its own public and private key pair and has its public key published in the form of a certificate in the roaming domain DNS tree. These certificates can be self-signed and do not need to be part of a Public Key Infrastructure (PKI).

6. Using the IP address and the certificate of the home RADIUS server, the visiting RADIUS server establishes a TLS connection to the home RADIUS server to negotiate a shared secret. We call this the RADIUS Key Exchange (RKE) protocol. The server in the home domain executes similar checks as the proxy in the visiting domain, e.g. checks – through DNS – that the incoming request for key exchange is from a party that is part of the roaming domain (not depicted).
7. (and 8) The shared secret now is used to setup a normal RADIUS connection between the peers in order to perform a straightforward user authentication over RADIUS.

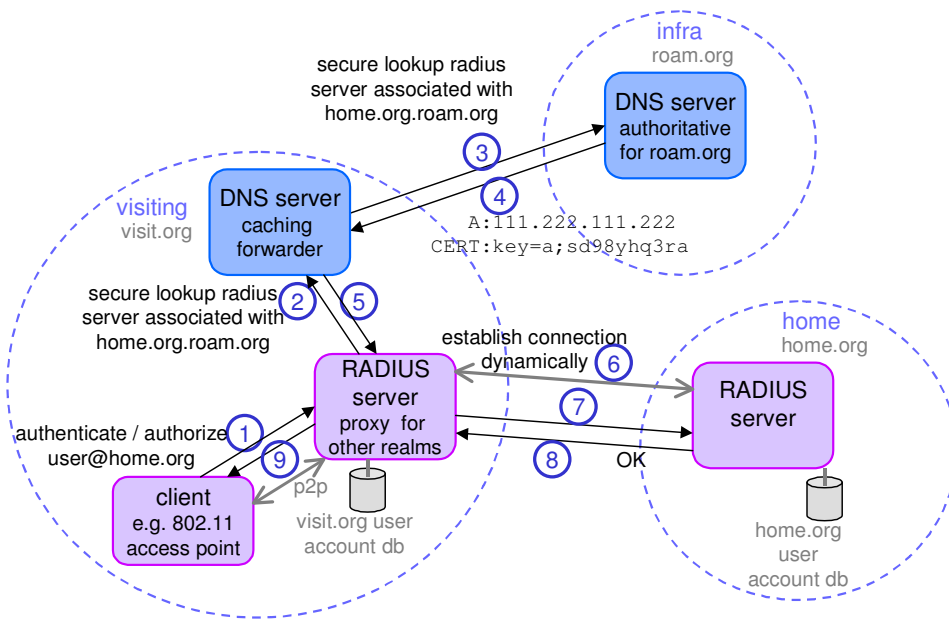


Fig. 1. : RADIUS-DNSSEC distributed authentication for a user accessing resources in a visiting domain. The numbers indicate the steps taken to authenticate the user at his RADIUS server in his home domain.

We believe that this solution stays close to configurations currently in wide use, thereby allowing for easy migration, while at the same time tackling a number of existing problems. The only requirement for deployment is that RADIUS servers that support dynamic trust-establishment also support this key-establishment protocol, and that a DNSsec enabled zone is used to administer the parties in the roaming agreement. This solution has been implemented as an extension to RADIATOR.

Other protocols and mechanisms exist that can be applied to address the problems identified above. The Diameter protocol [2], as projected replacement for RADIUS, has explicit support for network roaming situations, but has so far not seen widespread deployment. Also, a solution based on RADIUS in combination with a Public Key Infrastructure, where PKI is replacing the DNSsec functionality, may be used.

References

- [1] Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "DNS Security Introduction and Requirements", draft-ietf-dnsext-dnssec-intro-10 (work in progress), May 2004.
- [2] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "*Diameter Base Protocol*", IETF RFC 3588, Sept. 2003
- [3] EduRoam, <http://www.eduroam.org/>
- [4] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "*Remote Authentication Dial In User Service (RADIUS)*", IETF RFC 2865, June 2000

Vitae

Henk Eertink is a senior researcher at Telematica Instituut. He leads a group that is focused on security issues, mobility management and context awareness.

Arjan Peddemors is a research engineer at the Telematica Instituut. His interests are in the area of mobile and pervasive computing, with a specific focus on mobility management and network resource awareness for mobile applications. He is currently working towards his PhD.

Roy Arends is a network engineer at Telematica Instituut, and an active member in the DNSsec working groups of the IETF.

Klaas Wierenga is manager of Middleware Services at SURFnet. He is co-chair of the TERENA taskforce on Mobility (TF-Mobility) and active member of the Internet2 working group on network authentication (SALSA NetAuth). Furthermore, he is leader of the Roaming task within GN2 "Roaming and Authorisation" activity (JRA5)