Implementation Report on the use of EAP and RADIUS for US eduroam

saag Meeting
IETF 115: London, UK
November 2022
Background

• We worked with Internet2 to implement and deploy new AWS-based US eduroam infrastructure that went live in November 2021
  • FreeRADIUS-based, geographically-redundant, load-balanced deployment
• We have worked with Internet2 to operate, monitor and maintain the US eduroam infrastructure for the past year

The goal of this presentation is to share our EAP and RADIUS implementation and operation experiences with the IETF. Although much of this presentation focuses on need for improvement, our overall experience has been positive and highly successful.
Outline

• Quick review: What is eduroam?
  • Underlying technologies
  • eduroam proxy hierarchy

• Overview of the US eduroam deployment
  • Deployed infrastructure
  • Facts & figures

• Request “routing” in eduroam

• Security challenges

• Operational challenges
What is eduroam?

• A widely-used, international roaming service for higher education and research
  • Now being expanded to K-12, libraries, museums, etc.

• Allows students & staff from education or research institutions to access the Internet at remote eduroam service locations
  • Uses a common SSID: “eduroam”
  • Free, seamless access -- no need for captive portals or new configuration
  • May provide more privileges or better performance than public guest access

• A home institution (IdP) verifies a user’s identity and provides credentials
• eduroam service locations (RPs) proxy authentication requests to the eduroam infrastructure for authentication by the user’s home institution

• Millions of students and staff from thousands of home institutions access eduroam at tens of thousands of service locations throughout the world

• See https://eduroam.org for more information
eduroam authentication overview

A user from “institution.home” uses his Supplicant to access the “eduroam” SSID at “institution.visit”

User: john@institution.home
IdP: institution.home
RP: institution.visit

The request runs through an eduroam Roaming Operator that is peered with both institutions
Underlying technologies

- **RFC 2865**: Remote Dial In User Service (RADIUS)
- **RFC 3748**: Extensible Authentication Protocol (EAP)
- **RFC 3579**: RADIUS Support for EAP
- Various EAP authentication methods, such as:
  - **RFC 5216**: EAP Transport Layer Security (EAP-TLS)
  - **RFC 5281**: EAP Tunneled Transport Layer Security (EAP-TTLS)
  - **RFC 8940**: Protected EAP Protocol
- IEEE 802.11 & IEEE 802.1x
eduroam proxy hierarchy

• Three-tier proxy hierarchy
  • Individual eduroam institutions
  • National-level proxies
  • Top-level eduroam proxies
    • Europe and Asia

• At each level, requests for authentication for unknown realms are forwarded upward
Overview of the US eduroam deployment

• US eduroam is operated by Internet2 InCommon
• US eduroam consists of
  • > 1000 home institutions
  • > 3000 service access points
  • ~2M eligible students and staff members

• See https://incommon.org/eduroam/ for more information
Diagram shows East Coast deployment, duplicated for West Coast
US eduroam facts & figures

• During a typical peak period:
  • Up to 100,000 RADIUS messages received per minute
  • > 12,000 unique authentication requests completed per minute
    • ~65% Access-Accept
    • ~35% Access-Reject
  • ~18% of incoming requests rejected or discarded by our proxy
    • Looping
    • Missing or malformed username or realm
    • Unknown client
    • Invalid authenticator
    • Malformed EAP message
EAP method distribution

- ~75% PEAP
- ~15% EAP-TLS
- ~12% EAP-TTLS

From a report compiled in Q1 2022
Request “routing” in eduroam

• There are two sets of top-level eduroam operators, one in Europe and one in Asia
• There is a National Roaming Operator (NRO) in each country who is responsible for enrolling eduroam institutions and proxying requests between eduroam institutions within their country
• Each NRO provides a JSON-formatted list of their enrolled institutions to their top-level provider (for example, US eduroam provides their list to GEANT in Europe)

• If an institution RADIUS server receives a non-local eduroam request, the request is forwarded to their NRO RADIUS proxy
• If an NRO proxy does not have a matching IDP realm registered, the request will be forwarded to a top-level server
  • If a country code is included in the realm name, the request will be forwarded accordingly
  • Otherwise, a top-level server will be picked in a round robin fashion.
• If the top-level operator does not have a registration entry for the realm, it will be forwarded to the other top-level operator.
An inefficient (but realistic) example

A user from example.com (a Canadian institution) visits a US eduroam service location and attempts to join the "eduroam" SSID.

• The service location RADIUS server (1) determines that example.com is not a local realm, and forwards the request to one of the US eduroam proxies.

• The US eduroam proxy (2) determines that example.com is not a realm registered in the US, finds no country code in the realm, and forwards the request to an Asian top-level RADIUS proxy.

• The Asian proxy (3) determines that the IDP ream, example.com, is not registered by one of its NROs, so it forwards the request to one of the European top-level servers.

• The European top-level server 4) determines that example.com was registed by the Canadian NRO and forwards the request to one of the Canadian RADIUS proxies.

• The Canadian proxy (5)forwards the request to one of example.com’s RADIUS servers (6).
Cost of “routing” inefficiency

• Successful eduroam authentication requests may traverse up to 6 RADIUS proxies

• Each eduroam authentication requires several request/response exchanges which will follow the same path as the first message
  • Typically 3 to 7 request/response exchanges, depending on the chosen EAP method and credential size

• Cryptographic message authentication is performed for every RADIUS message at every hop, so efficient routing would be highly desirable

• No dynamic routing, and no equivalent of ICMP redirects
• No standard mechanism for loop detection or prevention
Lack of testing/debugging tools

• When a remote EAP/RADIUS request is dropped or rejected, it can be very difficult to figure out why it didn’t work.
  • Many errors result in proxies silently discarding packets
  • Access-Reject messages do not typically contain a useful error code

• Although Status-Server messages provide a way to query the health of a directly-connected server, there is no way to query the health of a more remote server (i.e. no multi-hop ping)

• There is no way to trace the path that a request will take across the proxy fabric (i.e. no traceroute)
Security challenges

• RADIUS message protection is antiquated by today’s standards
• It consists of pairwise shared secrets and and MD5 hash for message authentication
  • The keys are often typed by the administrator into a UI or a plain text file
  • There is no consistently enforced minimum length for the keys, nor is there any requirement for cryptographic generation
  • There is no algorithm agility
Privacy vs. secondary credentials

• User privacy is essential in eduroam, because the risk is exposing the physical location of an end-user

• Secondary credentials (such as certificates) can be valuable to allow password-less authentication, or to protect primary credentials from potential exposure

• PEAP and TTLS allow the use of an anonymous username in the outer method, so that the username is only transmitted over an encrypted tunnel

• EAP-TLS supports secondary credentials, but the username is exposed in plaintext in the unencrypted client certificate

• Support for TLS 1.3 in EAP-TLS and/or wider user of RadSec would meet both requirements if they were fully available and easily deployed

• It would also be desirable to have a non-PKI solution that would support both the privacy and secondary credential requirements.
Operational challenges

• Looping is the most frequent cause of dropped requests
  • Looping is typically caused by misconfiguration of an institution server
  • No standard method for RADIUS loop detection/prevention (we use a vendor attribute)

• Many clients will retry a failed authentication request immediately, with the same credentials
  • No back-off, no apparent limit on the number of retries
  • One example involved 37,000 requests every 5 minutes until manual intervention at the service location

• Long-expired or obsolete credentials often remain configured on user devices
  • There is no way for the IDP to signal the device that the credentials should be invalidated

• Supplicants will try to use obviously bogus credentials
  • Spaces or special characters in usernames or realms, missing realms, expired certs, etc.

• We receive many requests per second with realms of the form wlan.mncNNN.mccNNN.3gppnetwork.org
  • Are we being mistaken for a 3gpp carrier network? How can we make this stop?
Ongoing Progress

• Since I originally offered to make this presentation, work has been proposed in the IETF (in some cases by us) that would address some of the issues we have encountered
  • RADEXT(RA) BOF and rechartering effort
  • EAP-DIE discussion in EMU
Contributors

• Margaret Cullen, Painless Security (mrcullen42@gmail.com)
• Mark Donnelly, Painless Security (mark@painless-security.com)
• Josh Howlett, Federated Solutions (josh@federated-solutions.com)

This presentation contains our own observations and opinions only. It does not represent the views or opinions of Internet2, eduroam.org or any other company or organization.
Questions?