OpenRoaming Implementers Meeting 2025-11-12

RadSec testing and updates from the IETF 124

Karri Huhtanen, Heikki Vatiainen (Radiator Software)

Radiator

RadSec implementation testing

- RadSec client (AP) - RadSec server interoperability and best practices (among other things proper server certificate verification configuration)
- RadSec client (RadSec server) - RadSec server interoperability and best practices (Radiator, FreeRADIUS, radsecproxy cooperation in the IETF helps)
- RadSec TLS version interoperability (especially TLSv1.3 and TLSv1.3 session resumption

Experiences in RadSec implementation testing

- Some Wi-Fi APs support only up to TLSv1.2 for RadSec, problems may also occur with operating system TLS stack is stricter than the certificates issued
- Some Wi-Fi AP vendors allow only IP(v4) address configuration (no hostname option, no IPv6) for RadSec connections.
- Certificate detail verification (e.g. SubjectAltName, IP address) is still missing in most of Wi-Fi AP implementations. Most trust to any certificate signed by certain CA root certificate => adversary-in-the-middle (MitM) is easier
- TLSv1.3 support may be broken/incomplete:
  - One vendor Wi-Fi AP tried to connect with TLSv1.3, but broke the connection, when TLSv1.3 session tickets were enabled.
- Some Wi-Fi AP vendor implementations set up separate RadSec TCP connections for authentication and accounting traffic

Operational best practices

- RadSec DNS discovery and connection interoperability and best practices
- RADIUS - RadSec - RADIUS - … proxying, retries, timeouts and failover interoperability and best practices
- RadSec connection lifetime management and best practices. These should be separated into connections between APs and servers and between servers and servers in the roaming federation

Experiences in RadSec in operational use

- RadSec over TCP solves the RADIUS UDP and RadSec DTLS fragmentation problems with EAP and firewalls
- Public DNS service started to give negative answers for NAPTR queries => DNS cache cached those negative answers creating hour long outage for particular realm
- When multiple SRV records with priority and weight fields are received, how the server for RadSec connection is really selected and what happens if the first one on the list fails?
- Mixing UDP RADIUS with RadSec for proxying “is a disaster” waiting to happen
- Timeout for idling connections in the RadSec server caused the server to end Wi-Fi AP connections with no traffic or RadSec or TCP keepalive configured. The Wi-Fi AP did not notice the dropped RadSec connection and failed some of the authentications until it made new connection.
- Keepalives (and/or steady traffic) is needed to keep RadSec connections alive over firewalls, e.g. reverse CoA requires the RadSec connection from Wi-Fi AP server to be working to be able to send it
- But at the same time RadSec connections need to be torn down if idling between roaming brokers / hubs.
- Idle teardown timer of 30 minutes with keepalive configured to be sent every 30 minutes does not work properly as a recommendation or in practice.

Post-quantum encryption testing

- The CNSA 2.0 specification details a set of quantum-resistant cryptographic algorithms for National Security Systems (NSS), replacing vulnerable legacy algorithms like RSA and ECC => affects TLS and RADIUS over TLS (RadSec) as well
- Requires recent enough TLS stack (OpenSSL >=3.5, rustls)
- TLS stack interoperability testing as not all clients and servers use OpenSSL?

Some IETF RFCs and drafts to be tested

- (Datagram) Transport Layer Security ((D)TLS) Encryption for RADIUS (https://datatracker.ietf.org/doc/draft-ietf-radext-radiusdtls-bis/), which updates original RadSec (RFC 6614)
- Operational Considerations for Using TLS Pre-Shared Keys (TLS-PSKs) with RADIUS (https://datatracker.ietf.org/doc/rfc9813/), which covers using TLS-PSK instead of certificates with RadSec
- Reverse Change-of-Authorization (CoA) in RADIUS/(D)TLS (https://datatracker.ietf.org/doc/draft-ietf-radext-reverse-coa/), which enables sending disconnection and other user connection parameters from server to RADIUS client device (such as AP) via existing RadSec tunnel.

Radiator

IETF 124 RadSec and RADIUS update

IETF 124 RadSec and RADIUS updates

- RadSec is the name of RADIUS over (D)TLS now
- Big push to get the RadSec draft finished
- Discussion with QUIC experts
  - RADIUS over QUIC
  - QUIC combines good parts of TLS (solves fragmentation problems) and UDP (has stream multiplexing and no head-of-line-blocking (TCP))?

IETF 124 Hackathon

- Theme: Improving RADIUS Proxy Fabrics

RADIUS has had 30 years of protocol issues. The existing specifications say that servers must discard well-formed, authentic, packets from known clients. There are no provisions for rate limiting packets. In many cases, packets are sent and never see a reply, which contributes to network instability.

We want to add some functionality (current plan is to focus primarily on Protocol-Error) to RADIUS servers (FreeRADIUS, radsecproxy, Radiator)

Radiator

More information…

- Karri Huhtanen: “RADIUS compliance testing” presentation in the OpenRoaming Implementers Meeting, 8th Oct 2025:
  https://radiatorsoftware.com/wp-content/uploads/karri-huhtanen-radius-compliance-testing-2025-10-08.pdf

- Radiator Software presentations and webinars: https://radiatorsoftware.com/webinars/