RADSEC CLIENT SECURITY

KARRI HUHTANEN
RADIATOR SOFTWARE OY

Radiator

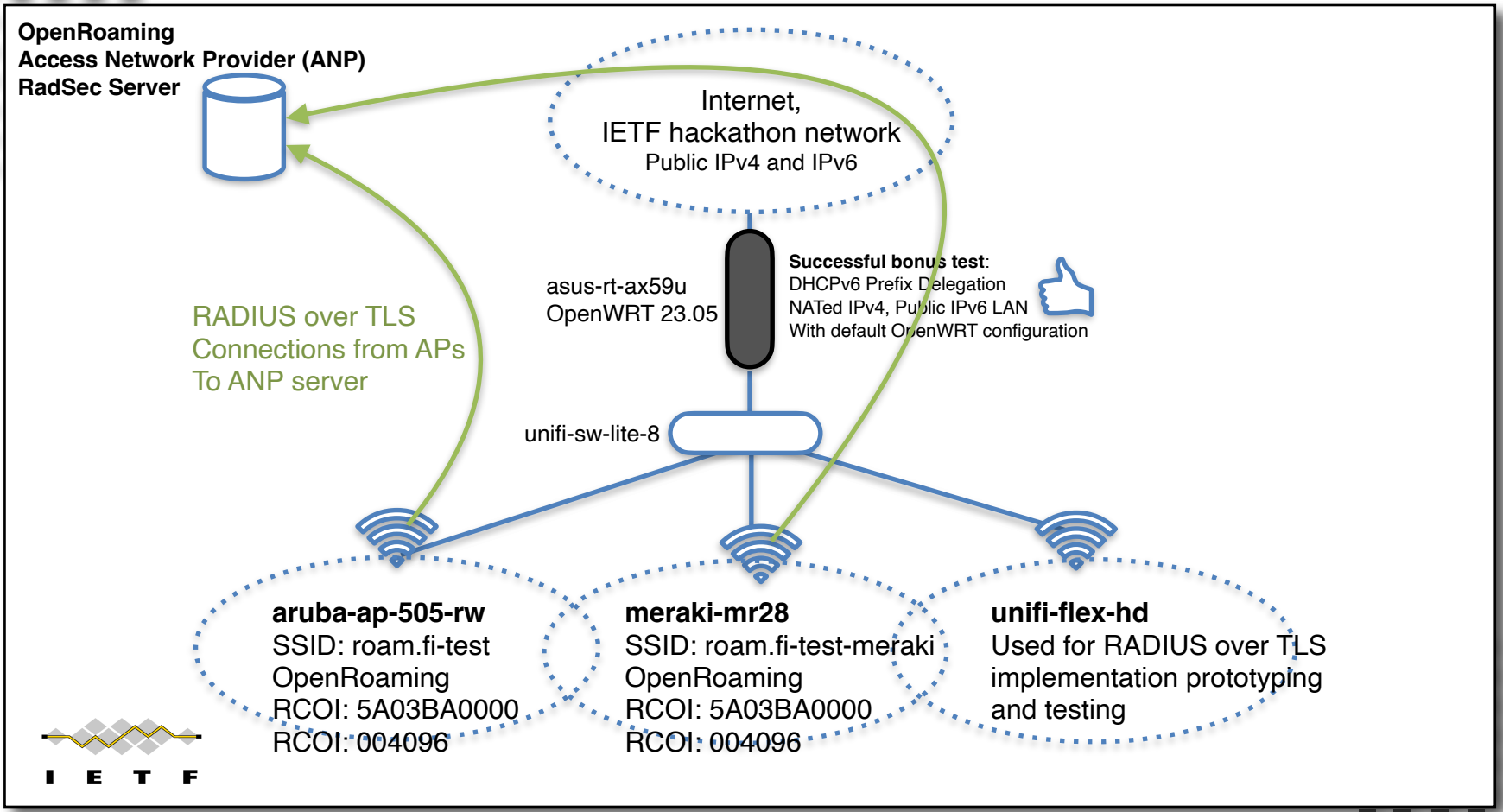
IETF Hackathon: EAPRAD

IETF 121
2–3 November 2024
Dublin, Ireland

https://datatracker.ietf.org/meeting/121/materials/slides-121-hackathon-sessd-ietf121-eaprad-hackathon-group-presentation-00

Hackathon Plan

- EAP-FIDO implementation work
  - emu working group: https://datatracker.ietf.org/wg/emu/about/
  - https://datatracker.ietf.org/doc/draft-ietf-emu-eap-fido/
- Discussing RADIUS drafts currently in the radext working group, trialling and testing implementations
  - radext working group: https://datatracker.ietf.org/wg/radext/about/
  - RADIUS over TLS (RadSec) update: https://datatracker.ietf.org/doc/draft-ietf-radext-radiusdtls-bis/
  - RADIUS and TLS-PSK: https://datatracker.ietf.org/doc/draft-ietf-radext-tls-psk/
  - Deprecating Insecure Practices in RADIUS: https://datatracker.ietf.org/doc/draft-ietf-radext-deprecating-radius/
- RADIUS over TLS (RadSec) interoperability testing with Aruba, Meraki and Ubiquiti hardware focusing on the configuration of the RADIUS over TLS details, certificate validation, TLSv1.3 support
- OpenRoaming roaming test network setup utilizing RADIUS over TLS (RadSec) connections and multiple IdP profiles including SIM authentication with dynamic 3GPP realm/IdP discovery


OpenRoaming
Access Network Provider (ANP)
RadSec Server
Internet,
IETF hackathon network
Public IPv4 and IPv6
asus-rt-ax59u
OpenWRT 23.05
Successful bonus test:
DHCPv6 Prefix Delegation
NATed IPv4, Public IPv6 LAN
With default OpenWRT configuration
RADIUS over TLS
Connections from APs
To ANP server
unifi-sw-lite-8
aruba-ap-505-rw
SSID: roam.fi-test
OpenRoaming
RCOI: 5A03BA0000
RCOI: 004096
meraki-mr28
SSID: roam.fi-test-meraki
OpenRoaming
RCOI: 5A03BA0000
RCOI: 004096
unifi-flex-hd
Used for RADIUS over TLS
implementation prototyping
and testing
I E T F

AP RadSec implementation testing

	Ubiquiti FlexHD	Meraki MR28	Aruba APIN0505
Configuration interface			
Server address	Literal IPv4 only	Literal IPv4/6, or FQDN	Literal IPv4/6, FQDN
Shared secret	No default	No default	Default per RFC
Certificates	User provided	Server CA: user provided Client CA: given by Meraki	User provided
TLS connection			
TLS version support	1.3	1.2	1.2
Server identity validation			

*actual connections only tested over IPv4

OpenRoaming IdP tests

- Successful roaming with at least 5 different OpenRoaming IdPs
- Successful roaming with SIM authentication utilizing DNS discovery for finding IdP server based on the mnc.mcc.3gppnetwork.org realm

What we learned

- RADIUS over TLSv1.3 support is not yet at least these tested access point with the latest stable and beta software.
- Certificate installation, handling, validation and configuration needs improvements in all of the tested access points.
- Comments about drafts will be presented in the respective working groups.

Wrap Up

Team members:

Jan-Frederik Rieckers

Karri Huhtanen

Heikki Vatiainen

Fabian Mauchle

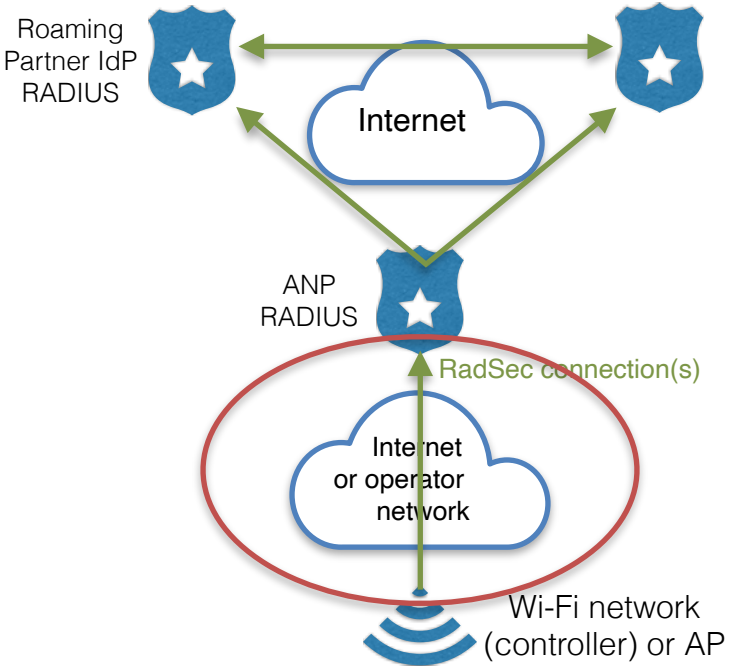
Alex Clouter

Subir Das

Alan DeKok

SO WHY IS RADSEC CERTIFICATE VALIDATION IMPORTANT?

RadSec connections from network devices to ANP RADIUS server



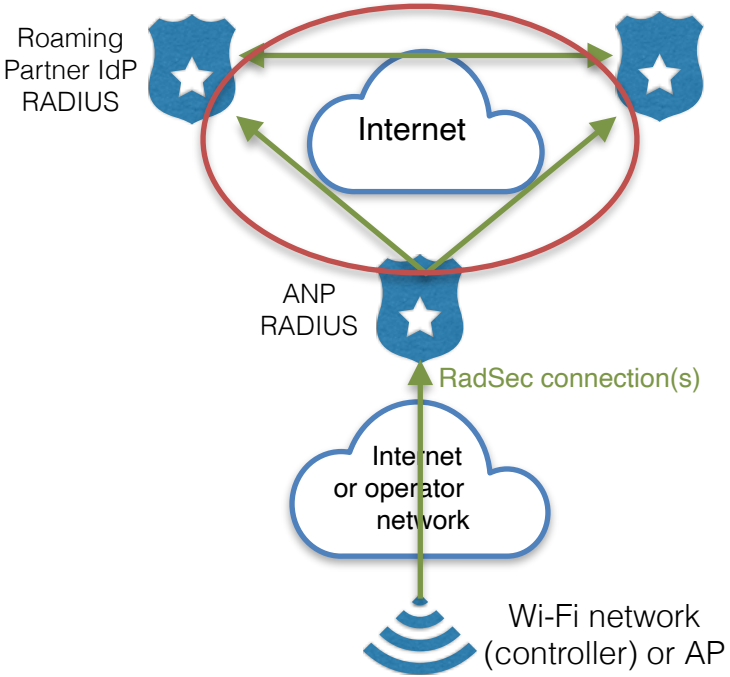
- If Wi-Fi controller or AP does not verify the ANP RADIUS server certificate anyone with access to the network between it and ANP RADIUS server can perform man-in-the-middle attack undetected.
- If Wi-Fi controller or AP only verifies that server certificate is issued by certain CA and not the certificate details (e.g. CN, SubjectAltName, certificate type (client/server)), anyone with a key and certificate from the same CA can perform man-in-the-middle attack undetected.
- The risk grows larger and/or more public the network between AP/controller and ANP RADIUS is.

AP RadSec implementation testing

	Ubiquiti FlexHD	Meraki MR28	Aruba APIN0505
Configuration interface			
Server address	Literal IPv4 only	Literal IPv4/6, or FQDN	Literal IPv4/6, FQDN
Shared secret	No default	No default	Default per RFC
Certificates	User provided	Server CA: user provided Client CA: given by Meraki	User provided
TLS connection			
TLS version support	1.3	1.2	1.2
Server identity validation			

*actual connections only tested over IPv4

RadSec connections between ANPs and IdPs



- If the RadSec client does not verify the RadSec server certificate details (CN, SubjectAltName, certificate type (client/server)), **anyone with WBA OpenRoaming certificate and able to get between roaming connection** may perform man-in-the-middle attack undetected.
- For example DNS poisoning, BGP highjacking could be used to get the roaming authentication traffic rerouted.
- Compared to the network equipment RADIUS servers can be configured properly to check certificate details mitigating the risk.
- **WBA WRIX, PKI and IETF specifications have already requirements to cover these connections.**

Summary

- The RadSec certificate verification implemented in the network equipment is too often incomplete and insecure.
- To ensure that the security and configuration of the network devices is implemented properly, the proper certificate verification should be covered and required in the security requirements documents.
- Some the network device improvements could be done by adding more comprehensive and strict RadSec configuration options in the user interface, some may need to update the RadSec implementing components.
- In the RADIUS servers the certificate verification is already implemented comprehensively and there the issue is more that the certificates contain suitable information for DNS discovery and certificate validation based on it.