OP IMP EXP

OPERATIONAL AND IMPLEMENTATION EXPERIENCE

ALAN DEKOK IETF 115
OPERATIONAL AND IMPLEMENTATION EXPERIENCE

‣ Review of what we have versus what we want

‣ Concentrating on Open Source and Eduroam
  ‣ This information is widely available.
  ‣ Harder to find information about commercial products

‣ With some public information on commercial vendors
  ‣ More participation from commercial vendors would help a lot
RADIUS/TLS

- Not as widely used as it could be. Why?
  - radsecproxy has a limit of one connection per home server
  - FreeRADIUS had issues (recently fixed) with blocking
  - Radiator, Cisco, Nokia implement it, NPS does not
- Supported in some NAS equipment
  - Cisco, Aruba, Aerohive, ...
RADIUS/DTLS

- Much less used
  - radsecproxy has the single connection issue
  - FreeRADIUS does not implement it
  - Cisco ISE, others are unknown
- Supported in some NAS equipment
  - Cisco switches, others are unknown
TLS OPERATION

- Much of roaming is still RADIUS/UDP
- TLS-PSK is essentially unused
- TLS certificates are hard to get
  - Misleading CAs is wide-spread practice
- TLS certificates are hard to manage
  - How did we renew them last time? What’s the process?
ROAMING IS OFTEN STILL UDP

› Much of Eduroam is still UDP

› See previous comments on TLS / DTLS implementations

› OpenRoaming uses TLS, and RFC 7585 dynamic discovery.

› Many roaming providers use IPSec.

› “RADIUS in the cloud” providers are almost entirely UDP

› Most roaming uses TLS-based EAP methods, but anything else is “in the clear”
TLS-PSK

- Essentially not implemented
- RFC 6614 or RFC 7360 suggest it, but say nothing about identities
  - It looks like NAS vendors went “We don’t know what to do, and the specs don’t give guidance, so we’ll just ignore TLS-PSK”
- Implementation?
  - FreeRADIUS. Not radsecproxy
  - Commercial vendors ???
TLS CERTIFICATES AND MANAGING THE CA

- The CA forum is the CA / Browser forum
  - Web-specific
  - Essentially impossible to get certificates with non-WWW OIDs
  - RADIUS admins just say “yes, this is for a web server”
- Private CAs are hard to manage
- No one has $1B to create a new global CA for RADIUS / EAP / …
TLS CERTIFICATES ARE HARD TO MANAGE

‣ It’s hard enough to get shared secrets correct:
  ‣ Log says “Please check shared secret”. *What could that possibly mean?*

‣ Certificates expire
  ‣ Who requested it last time? From where?

‣ Configuring supplicants is hard, too
  ‣ Many of them just ignore the server certificate and often the CA
HOW TO FIX THESE PROBLEMS?

‣ Mandate good behavior
‣ Describe how to do it
‣ Implement missing functionality