



# Report from IETF-73

Stefan Winter <[stefan.winter@restena.lu](mailto:stefan.winter@restena.lu)>

# Overview



- radext wg (RadSec, i18n)
- proxy meeting (draft-proxythreat)
- emu wg (channel bindings, tunnel-reqs)
- nea wg (endpoint security vs. snooping)
- dime wg (CER vulnerability)
- capwap wg (live and let die)
- other (XP Supplicant, 802.1X-rev,dhcp-auth)

# RADIUS Extensions (radext) RadSec



- Draft is in “WG Last Call”
- Couple of comments outstanding
- Will issue rev -03 ASAP
  
- TCP transport part has a few challenges
  - Reserve ID for Status-Server?
  - Useful without TLS encryption?

# RADIUS Extensions (radext) i18n issues



(also in EMU, Diameter and Security Area meetings)

- “You are doomed!”
- Alan DeKok presented overview of the mess
- Problem not so pressing if in local control
  - e.g. 1-domain enterprise deployments
  - eduroam will suffer, due to realm interpreting
- No volunteer in IETF yet to fix the numerous RFC errata
- Reports about int'l roaming environments with a need to get this fixed

# Proxies Interest Group draft-hoeper-proxythreat



- Document tries to evaluate how evil AAA proxies are
- So far, a lot of duplication of security-related information in older RFCs
- Scope of document to be widened
  - Explain why proxies are sometimes necessary or desired
  - Describe currently deployed problem mitigations: EAP (eduroam), OTPs (Cisco) ...
  - ... any why all those workarounds are imperfect

# EAP Method Updates (emu)



- Channel bindings
  - Two major goals
    - tie inner and outer EAP method together (to detect inner-forwarding)
    - To enable EAP peer communication (i.e. supplicant to IdP)
  - Use case of “Am I Roaming or Not” explicitly in document → useful for dense eduroam hotspots
- EAP Tunnel requirements
  - Progressing nicely

# Network Endpoint Assessment (NEA)



- Standardisation process coming along okay, but...
- Concrete vendor implementations have some disturbing features
  - e.g. allow NEA server to query for arbitrary registry keys
  - Or CPU speed
- Unclear why this is related to security
- “Foot in the door” concept
- User consent?

# Diameter Maintenance and Extensions (dime)



- After request on dyn discovery algorithm
  - (NAPTR → A): declared broken, and nobody used it anyway.
  - Will change to RadSec behaviour
- Security vulnerability on connection setup (CER / CEA handshake) (see next)
  - Concept: either out of band security (IPSec) or negotiate inband security
  - Negotiation is not protected in any way!
  - wg trying to figure out alternative ways (STARTTLS, alternate TCP port)

# Diameter: TLS negotiation



Initiating Peer

Contacted Peer

(establish TCP/SCTP)

“I can do TLS”

(Capability Exchange Request  
Inband-Security = TLS)

“I can do TLS, too”

(Capability Exchange Announce  
Inband-Security = TLS)

“Let's do TLS”

(TLS handshake)

# Diameter: Attack scenario (intermediate bad guy)



Initiating Peer

Contacted Peer

(establish TCP/SCTP) ~~"I can do TLS"~~ **No idea about TLS.**

→  
(Capability Exchange Request  
~~Inband-Security = TLS~~)

~~"I can do TLS, too"~~ **Me neither.**

←  
(Capability Exchange Announce  
~~Inband-Security = TLS~~)

~~"Let's do TLS"~~ (peers rely on OOB)

→  
(~~TLS handshake~~) (if IPSec  
unconfigured, may communicate  
in clear)

# Control and Provisioning of Wireless Access Points (capwap)



- Base specification finished, awaiting implementation
- Very few activity in the meeting
- Nobody raised hand as for implementing or planning to implement
- But apparently, several implementations are ongoing anyway

# Other



- Contacted MS person with knowledge about built-in supplicant
  - ❑ Default PEAP settings are made for Domain logon
  - ❑ Other use cases somewhat neglected
  - ❑ 802.1X perceived as not widely deployed
  - ❑ eduroam may well be largest known **wired** 802.1X deployment world-wide
  - ❑ PEAP has privacy as “uncommitted feature”
  - ❑ Invited to send paper describing deployment size and weak points in built-in supplicant

# More Other



- Got advice to look into 802.1X-rev
  - e.g. SSID-like beacon on wired ports
  - Rumor has it: better error reporting to client (“Network Status Notification”)
- Authenticated DHCP (Stig's work) is picked up by dhc working group

# The End

