# RadSec version 2
# IETF 69 - opsawg 24 july 2007

## RadSec

## A secure, reliable transport profile for the RADIUS protocol

Stefan Winter (stefan.winter@restena.lu)

# RadSec on one slide

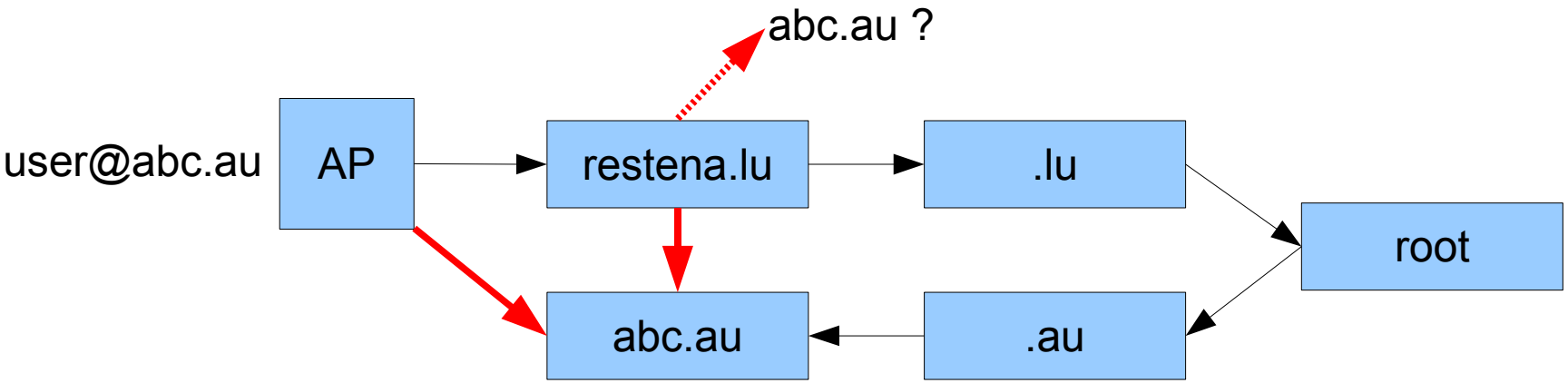
- wraps RADIUS payloads in new transport profile
- transport packet payload with TCP
  - UDP made sense when one packet per auth was sufficient, bot not any more with EAP conversations
  - peer's “alive” status does not rely on guessing any more
- authenticate peers and encrypt traffic with TLS
  - obsoletes (weak) shared secrets and static IP bindings
- independence of shared secrets and IP bindings enables dynamic peer discovery

# Implementations

- OSC's “Radiator”: popular RADIUS server, has RadSec since several years
  - described in company's whitepaper; RadSec v1
  - v2 narrows the specification
- Stig Venaas' radsecproxy
  - lightweight RADIUS <-> RadSec proxy
  - very small + efficient; embedded and commercial use possible (e.g. OpenWRT package exists)
- two implementations exist and interoperate -> description of the protocol in use should benefit community

# Merits of peer discovery

- use arbitrary method to find peer
- can shorten paths in large proxy environments
- one such example: eduroam



# Merits of IP/shared secret independence

- deployment of NASes possible in
  - NATted networks
  - changing IPs (e.g. DSL with forced re-dial)
  - UDP-unfriendly networks
- Example: OpenWRT Access Point
  - WPA2-Enterprise, RADIUS server = localhost:1812
  - radsecproxy on localhost:1812, preconfigured to contact tld1.eduroam.lu on boot
  - -> access control with WPA2-Enterprise with **no** run-time config (only needs DHCP LAN uplink)

# Why not Diameter?

- lack of usable implementations
  - no real open source solution
  - most Diameter servers focus on validating EAP-TLS and EAP-SIM
- RadSec's simple measures achieve large portion of the merits of Diameter
- largely deployed RADIUS installations (easy to leverage to RadSec)
- no WLAN NAS support for Diameter
- IPR situation concerning Diameter

# State of the draft

- I-D at http://www.ietf.org/internet-drafts/draft-winter-radsec-00.txt
- describes transport profile, two implementations and use case
- submitted independently
  - does not interfere with radiusext business (out-of-charter)
  - creates no new interop problems with Diameter
- Plan: Informational RFC via Independent Submission track

# Questions?

- What do you think?
- Does it fit into OPS & Mgmt?
- Course of action (Independent Submission to RFC Editor) appropriate?