

Recent Advances in eduroam: RadSec and DAME



APAN 24 Xi'an

28 aug 2007

RadSec

improvements to the RADIUS protocol

DAME

attribute-based authorisation levels



RadSec

A secure, reliable transport profile for
the RADIUS protocol

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, but 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

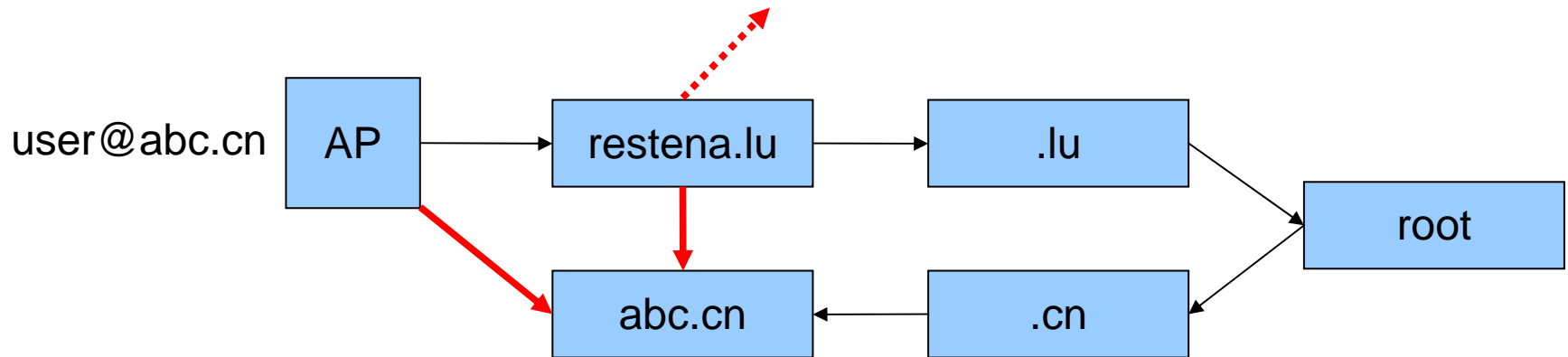


- OSC's "Radiator": popular RADIUS server, has RadSec since several years
 - described in company's whitepaper; RadSec v1
 - v2 narrows the specification
- Stig Venaas' radsecproxy
 - lightweight RADIUS <-> RadSec proxy
 - very small + efficient; embedded and commercial use possible (e.g. OpenWRT package 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



- IETF Internet Draft at <http://www.ietf.org/internet-drafts/draft-winter-radsec-00.txt>
- describes transport profile, two implementations and use case
- Plan: Informational RFC via Independent Submission track



DAMe

augmenting RADIUS authentication
decisions with AAI attribute-based
authorisation decisions
(... a marriage made in heaven?)

eduroam today



- pure EAPoL+RADIUS
- very limited support for attribute exchange
- for roaming visitors: mostly a “yes” or “no” decision
- integrating network-layer authentication with application-layer attribute retrieval and authorisation difficult
- Goal: make possible to request attributes (age, role, ...) during auth process

Possible Solutions (1: push)



- home RADIUS server looks up user's attributes in AAI
- sends AAI attributes in RADIUS attributes
- visited RADIUS picks attributes it needs, determines authorisation level

- **PROBLEM: RADIUS discloses attributes unnecessarily, privacy problem!**

Possible Solutions (2: pull)



- visited RADIUS server signals required attributes during EAP conversation
- home RADIUS sends after successful EAP conversation with Access-Accept
- visited RADIUS evaluates attributes, determines authorisation level
- **PROBLEM:** intermediate RADIUS proxies can read user attributes
(so far, NO trust to intermediates is required
--> would require paradigm change in eduroam)

Possible Solutions (3: DAME)



- RADIUS only for authentication
- visited RADIUS: Access-Accept contains opaque handle + IP of home AAI
- trigger AAI attribute request
- retrieve attributes directly from home AAI (no intermediates)
- make authorisation decision
- user's ARP determines if a particular attribute will be revealed

DAMe and different AAI



- There is more than Shibboleth!
(A-Select, PAPI, Sun Liberty Alliance, ...)
- How does visited RADIUS know what language to use when contacting home AAI?
- eduGAIN comes to the rescue!
- Visited AAI (SP) and home AAI (IdP) can be interconnected via eduGAIN
- choice of AAI on both sides arbitrary (as long as there is an eduGAIN BE)

Further Information



- DAME homepage

<http://dame.inf.um.es>

- current architecture proposal

http://dame.inf.um.es/files/DAME_proposal.pdf

- IETF radiusext working group

<http://www.ietf.org/html.charters/radext-charter.html>

- radsec Internet Draft

<http://www.ietf.org/internet-drafts/draft-winter-radsec-00.txt>



Thank you!

Questions?

Realisation



- use RADIUS servers' Post-Auth hooks (FreeRADIUS: `rlm_perl` in `post-auth { }`, Radiator: `PostAuthHook`)
- on home server side: to add handle
- on visited server side: to trigger AAI attribute request
- Access-Accept stays on hold at visited server side until authorisation decision is made
- eduGAIN can be used to transport attributes over federation borders