RESTENA

Foro de Movilidad RedIRIS 21 oct 2010

Evolution of eduroam
a new operational model, and new developments in the IETF

Stefan Winter <stefan.winter@restena.lu>

Introduction

- Stefan Winter <stefan.winter@restena.lu>
  - RESTENA Foundation (“Luxembourg's RedIRIS”)
  - Task Leader of GN3 “Multi-Domain User Applications Research – Roaming”
  - Operating the national RADIUS proxy servers (“Luxembourg's José-Manuel”)

Topics for today

- eduroam status update
- eduroam's proposed new operational model
  - RADIUS/TLS
  - dynamic server discovery
- IETF developments
  - Identifying hotspots
  - Recognising users
  - secure authentication without a server cert

Status Update

- >1000 hotspots
  - Between 1 and 1200 Access Points each
  - Google map available
- >1 million users
- International Monitoring
- Eduroam database (contact details)

RADIUS/TLS with dynamic discovery

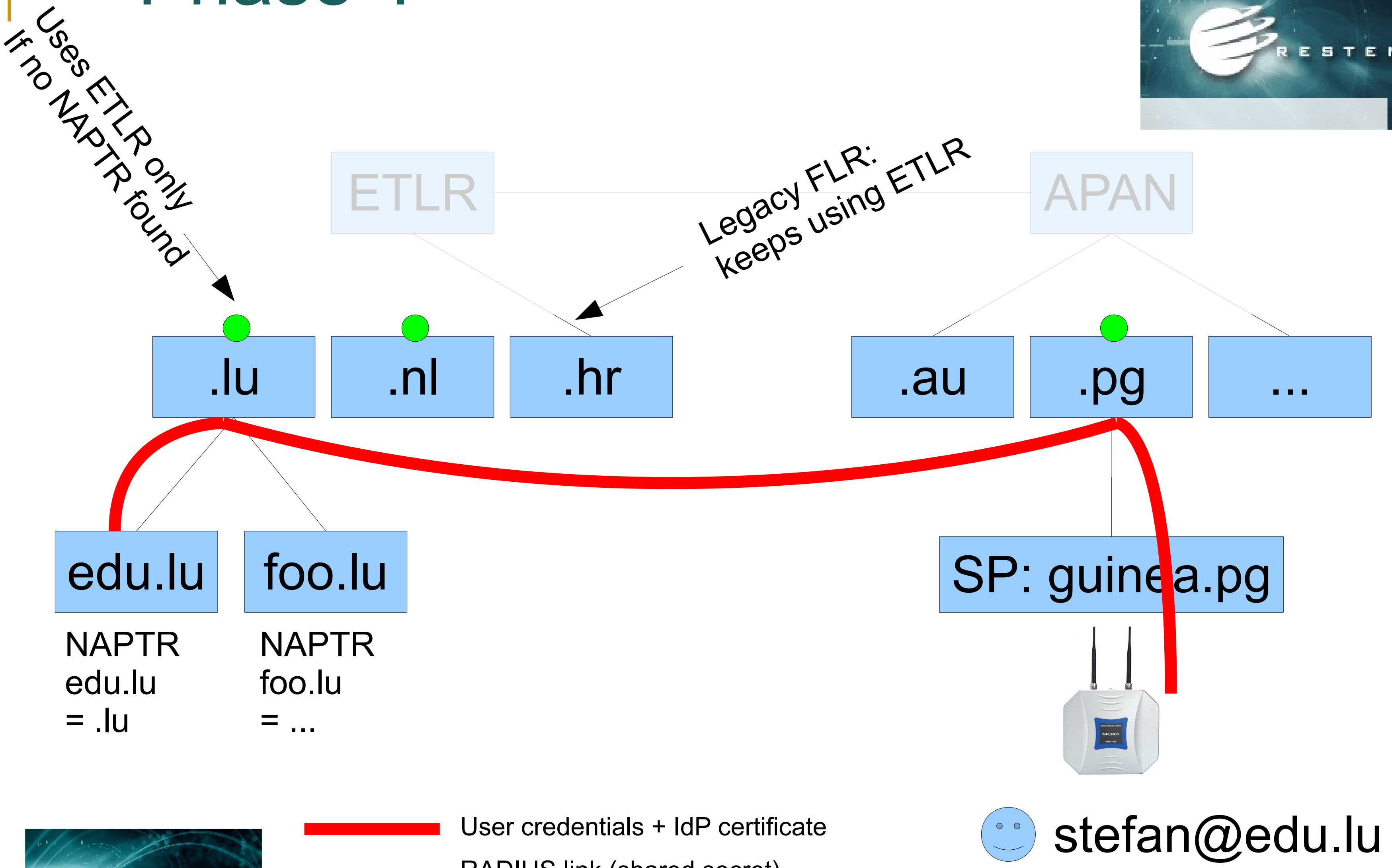
- Goal: overcome eduroam's long-standing problem: How to route “realm.edu”?
- Federation-level server model not flexible enough
- “routing” information needs to go elsewhere
  - DNS (with or without SEC)
  - Accredited servers only → certificates (eduPKI) and RADIUS/TLS
- No “big switch” day

dynamic discovery: soft migration

- Migration plan in 2 phases
  - Phase 1: deploy on FLR servers (keep IdP and SP untouched)
  - Phase 2: move IdPs and SPs at their own pace
  - Phase 2 doesn't have to be done at all
- Phase 1 changes:
  - IdPs publish a DNS record (RR NAPTR); basically states “my eduroam service is handled by RedIRIS”

<my realm> NAPTR x-eduroam:radius.tls <my FLR>

Phase 1



Uses ETLR only
If no NAPTR found

Legacy FLR:
keeps using ETLR

ETLR

APAN

.lu

.nl

.hr

.au

.pg

...

edu.lu

foo.lu

SP: guinea.pg

NAPTR
edu.lu
= .lu

NAPTR
foo.lu
= ...

stefan@edu.lu

━ User credentials + IdP certificate

— RADIUS link (shared secret)

● TLS interface (eduPKI(*) certificate)

Dynamic Discovery

- “realm.edu” problem solved as soon as all .edu domains have NAPTR entry (and their FLRs can handle incoming traffic)
- Phase 2 gives certificates directly to IdPs and SPs – this makes federation servers obsolete at a technical level

Identifying hotspots

- Problem:
  RADIUS hierarchy makes SP “anonymous”
- For IdP, knowing the location of user may be helpful for debugging
- Enter: RFC5580
  - Operator-Name attribute (#126 – string)
  - Operator-Name = “1foo.bar”
- Deployment a bit more difficult than usual
  - Ascend and U.S. Robotics hijacked 126 a long time ago and made it an Integer
  - Some RADIUS still use wrong dictionary entry

Recognising Users

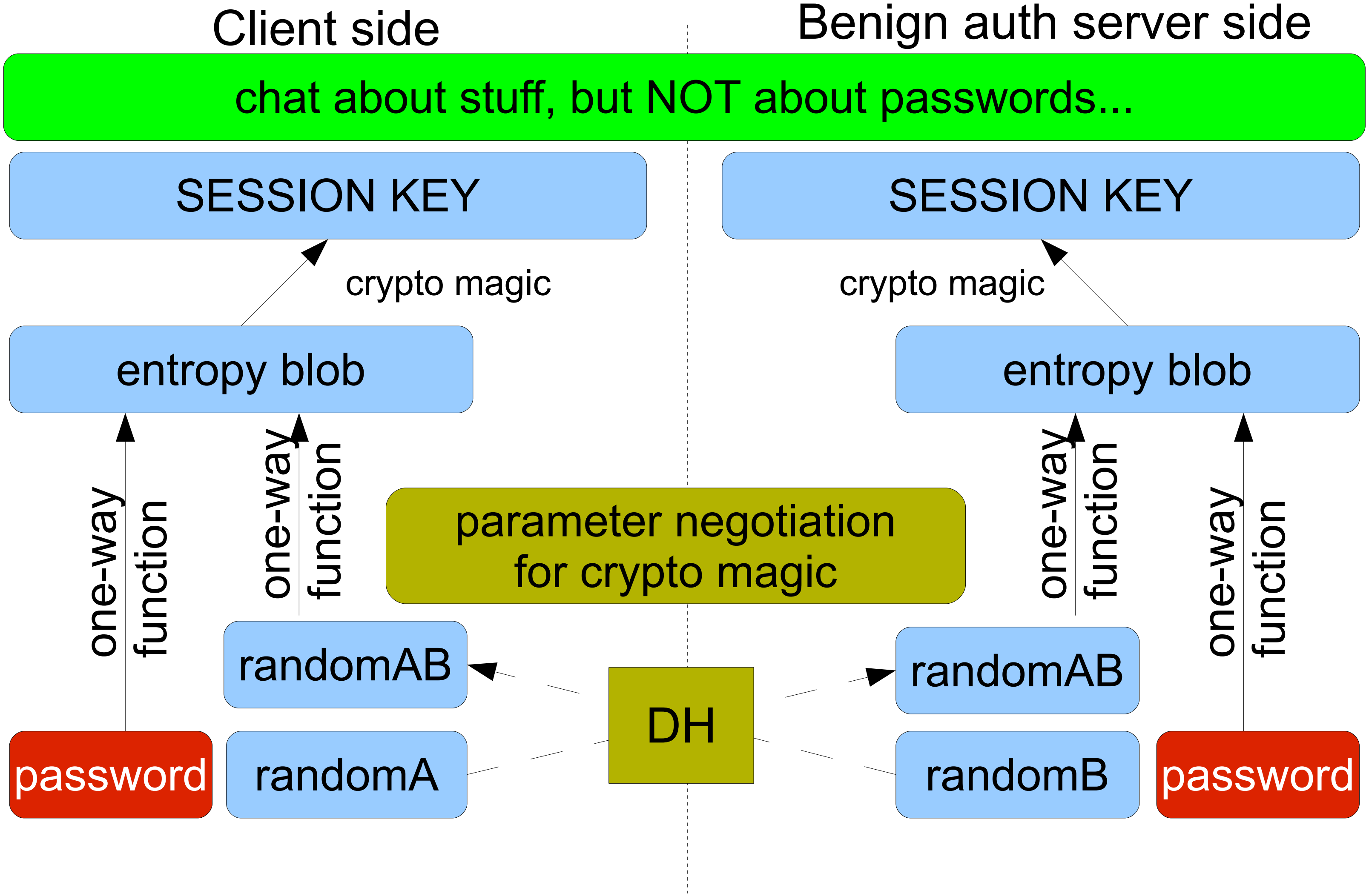
- Problem:
  Users can disguise (outer identity, MAC)
- Operator may want to blacklist a “bad guy”
- Needs persistent handle
- Enter: RFC4372
  - Chargeable-User-Identity (#89, string)
  - Based on inner identity …
  - … and is per Operator-Name
- This is eduPersonTargetedID!

Secure authentication without a server certificate

- EAP-EKE: “Encrypted Key Exchange”
- Allows
  - mutual authentication
  - With only a (weak) user password
  - In particular: no PKI, no server certificate, no CA!
  - derivation of crypto keys
  - not susceptible against MITM attacks

“Everything we've ever dreamt of”(*)

Now how is that supposed to work?



New requirements in Operations

- Move to mandatory WPA2/AES support
  - Technically, long overdue
  - Deployment-wise, daunting costs for some
  - Reduces problems for users!
- 11b is dead, long live 11g, 11n
  - Policy still requires 11b support
  - Not enforced any more

Thank you for your attention!