InternetWide Realm Crossover

Rick van Rein
http://internetwide.org
rick+ietf@openfortress.nl

Rewinding the Economy of Scale

- Most users rely on a service provider
  - Originally, low-cost domain hosting providers
  - Increasingly, generic/massive service integrators
- Hosting providers have limited resources
  - When joining forces, each can specialise
  - Identity Providers + [Plugin] Service Providers

Specialised Hosting Providers

- Identity Providers: DNSSEC/DANE, IdP
- Service Providers: XMPP, SIP, aCMS, …

- Service profiles “pulled into” identity provider
  - Like a contract, possibly redirecting payment
- Identity trust: InternetWide Realm Crossover

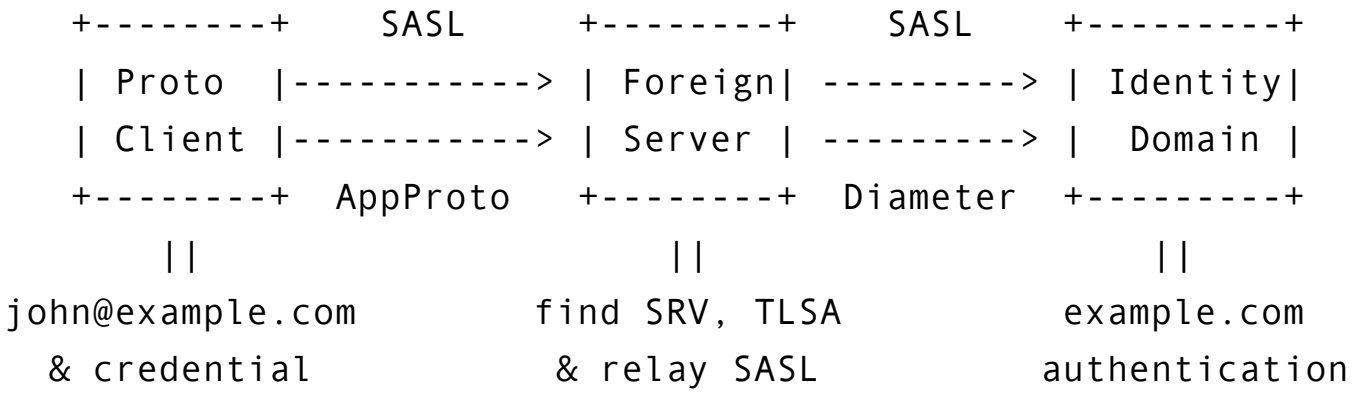
Realm Crossover: Technologies

- for SASL (SMTP, IMAP, XMPP, MQTT, ...)
  - Negotiable from passwords to Kerberos
- for Kerberos (GSS-API protocols)
  - Designed for a dangerous campus network :-)
  - Quantum Proof since ~1993
- for Certificates (TLS, signing, encryption)

Realm Crossover for SASL

- Most protocols exploit SASL authentication
- `SXOVER-PLUS` wraps a plain SASL login
- End-to-end encryption, using channel binding
- Foreign server relays SASL to client domain
- Results in identities like `john@example.com`

Realm Crossover for SASL



Realm Crossover authentication:

Client John authenticates to his own Domain
while using a foreign Server.

Realm Crossover for SASL

- Defined AVPs for SASL over Diameter
- Defined SASL mechanism `SX0VER-PLUS`

- Extra: Added SASL to HTTP
- Extra: Adding SASL to PAM (`sudo`, containers)

Realm Crossover for Kerberos

- Single Sign-on… plus Realm Crossover :-)
- Kerberos offers pre-defined *static key* crossover

- Defined Kerberos host-to-realm map in DNS
- Built Key Exchange based on RFC 5705

Realm Crossover for Certificates

- LDAP found as `_ldap._tcp` in DNS SRV
- Objects `uid=john,…,dc=example,dc=com`
- X.509 certificates and PGP keys: sign, encrypt, …
- Control access, make objects dynamic, ...

- Client DANE could acknowledge a domain CA

Questions?

- EU likes this direction (NGI Pointer)

- *Extra slides: specs, blog and code*

Draft Specifications

- draft-vanrein-internetwide-realm-crossover
- draft-vanrein-diameter-sasl
- draft-vanrein-httpauth-sasl
- draft-vanrein-sipauth-sasl
- https://k5wiki.kerberos.org/wiki/Projects/Realm_Crossover_between_KDCs

Code for [[Quick-]Dia]SASL

- https://gitlab.com/arpa2/Quick-SASL
- https://gitlab.com/arpa2/Quick-SASL/-/blob/master/include/arpa2/quick-diasasl.h
- https://gitlab.com/arpa2/quick-der/-/blob/master/arpa2/Quick-DiaSASL.asn1
- https://gitlab.com/arpa2/freediameter-sasl

Code for HTTP-SASL

- https://gitlab.com/arpa2/apachemod/-/tree/master/arpa2_sasl
- https://gitlab.com/arpa2/apachemod/-/tree/master/arpa2_diasasl
- https://github.com/stef/ngx_http_auth_sasl_module

Blog, Documentation

- http://internetwide.org/tag/identity.html
- http://common.arpa2.net/
- http://quick-sasl.arpa2.net/group__quickdiasasl.html