Project Moonshot update

ABFAB, IETF 80

About Moonshot

- Moonshot is implementing ABFAB
- Developer meeting, 24 March 2011
- Testing event, 25 March 2011
- A big thanks to
  - Luke Howard, Scott Cantor, Daniel Kouril, Michal Prochazka & Linus Nordberg.

Moonshot components

- GSS EAP
- RadSec
- Attribute extraction
- Application integration

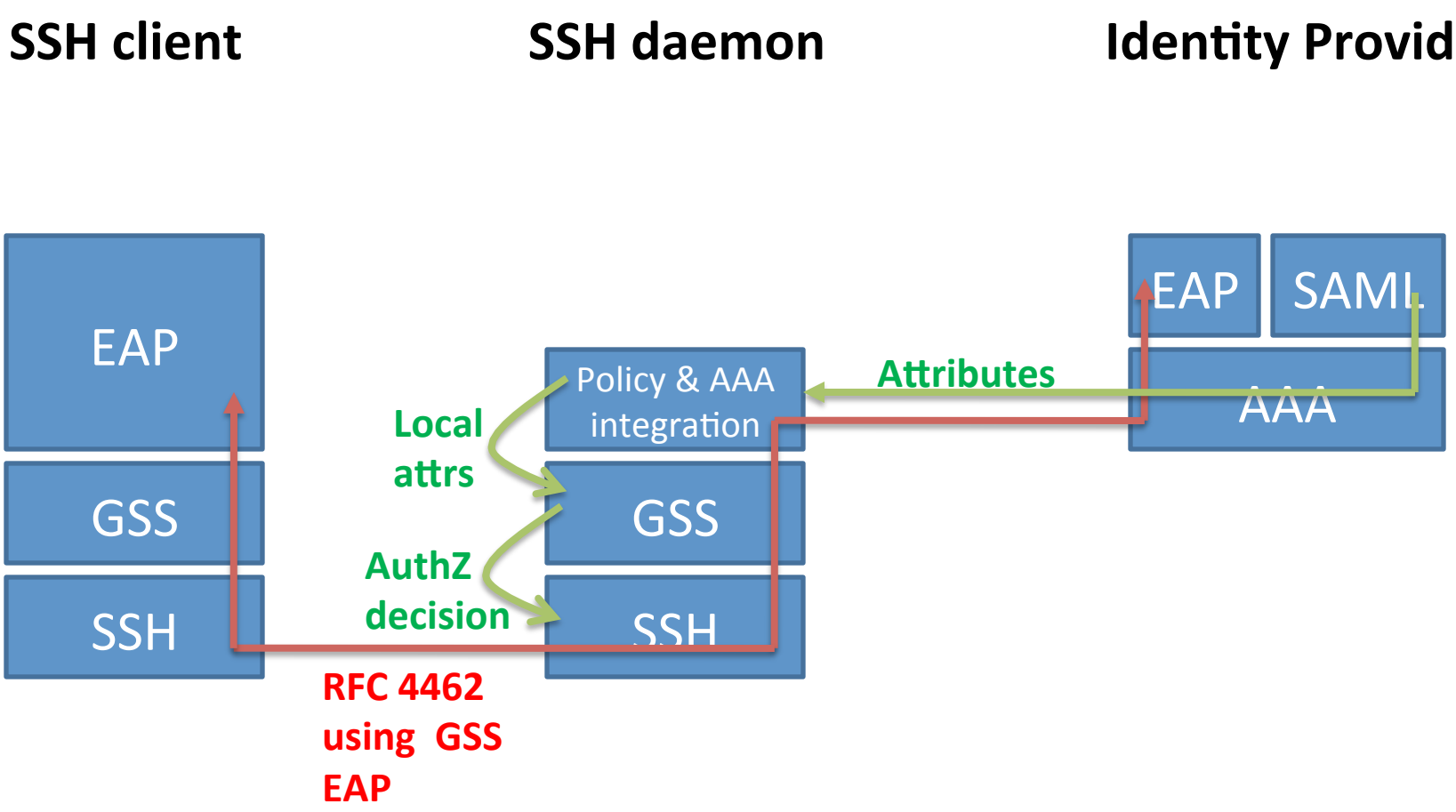
Infrastructure

- GSS library
  - Reasonably complete, all participants were able to demonstrate the mechanism working.
  - No EAP channel binding, yet.
- RadSec
  - Early client support; works with radsecproxy. Not tested directly against a server.
- Attribute extraction & policy layer
  - Support for RADIUS attributes, SAML assertions and attributes: support for local mapping and policy.

Application integration

- Demonstrated with
  - Apache & test HTTP client
  - Prior to test event, demonstrated with
    - openssh
    - Adium
    - Jabberd
  - On-going work for Firefox
- As expected, changes are sometimes required to applications but are minimal.

What's possible with SSH



What's possible with SSH

- RFC 4462 used for GSS EAP authentication
- RADIUS response includes SAML assertion; Identity Provider (IdP) wants to entitle user to log-in.
- Shibboleth policy maps this entitlement from trusted IdPs to mechanism-independent authorisation.
- SSH asks GSS for authorisation decision.
- Core GSS authorises with no knowledge of SAML, EAP or RADIUS.

Usability

- Goal: to select an identity and enter credentials, without modifying applications.
- Better experience when applications are modified.
- Challenges
  - Error handling: when do you record a failure?
  - Authentication description: who are you trying to talk to, and for what?
  - Password handling: when both the application and the library can handle the password, what's the best experience?
  - We need help from Kitten!

Using an IdP with ABFAB

- Conventional Web SSO is here to stay.
- We want to use the same IdP for ABFAB and Web SSO.
- For ABFAB, the RADIUS server typically wants an attribute query; how is the RADIUS server authorised to make that query for anyone?

More information & participation

- http://www.project-moonshot.org
- Developer information:
  - http://www.project-moonshot.org/developers
- Virtual machine for demonstration & testing:
  - http://www.project-moonshot.org/devwiki/vmdk