Ephemeral keying for ABFAB

Linus Nordberg, NORDUnet

March 6, 2014

Goals for today

- Lure you to think about ephemeral keys
- Should we do this?

The problem at hand

An observer on the path between the ABFAB client and the RP will see things like

- NAI
- acceptor name (i.e. the service requested)

and possibly

- EAP MSK (when AAA w/o confidentiality)
- IdP x509 certificates

Suggested solution

- Extend RFC 7055 to allow for (or require) the GSS-API initiator and acceptor to perform a Diffie-Hellman key exchange before any other traffic is sent.
- This DH key is then used to derive a symmetric key used to encrypt context tokens.

Changes -00 to -01

- Why this should not be done in the application tunnel.
- TLS session resumption may make the client fingerprintable (thanks Jim Schaad).
- Change two false statements (thanks to Jim, again).

Open questions

- The meat, obviously :)
- Costs
  - Implementation
  - Complexity
  - Computation
  - Round trips
- Should we detect bid down attacks? Prevent them too?
- Should this be optional or not? Note complexity and bid down.