New TEAP Stuff? Looking at BRSKI

EMU

Eliot Lear, and others

March, 2018
I’m new at EAP...

Soprano

Mary had a little lamb, little lamb, little lamb, Mary had a

S.  

little lamb whose fleece was white as snow.
802.11 onboarding problem: provision access

Prerequisite to send: network access

http/tls get [...]/.well-known/est/requestvoucher

- Potential Solutions
  - 802.11u ANQP extension
  - Use of a new TEAP method
  - Extend Wifi Alliance Device Provisioning Protocol (DPP)
- Different forms of results needed (PSK, EAP-TLS, username/password, etc...)

Network B
A Quick TEAP Review

• Has outer TLS – with the ability to defer cert validation
  • ANIMA BRSKI has something similar known as “provisional trust”

• Allows for inner methods

• Has EST-like enrollment mechanism (PKCS#10)

• Has Trusted-Server-Root and PKCS#7 TLVs for trust anchor installment

• **LACKS** means to do trusted introduction
  (this is what ANIMA BRSKI is for)
A Quick ANIMA/BRSKI Review

- Extends EST to make a trusted introduction between device and local deployment
- Authentication Server. = Registrar
- Registrar passes a voucher request to Manufacturer who returns a voucher
- This allows for trust of the registrar
- Registrar can then be used to seed trust anchors in client
- Client can also request a deployment cert
Extending TEAP to have BRSKI: choices

• Create a new EAP method
  • Seems pretty clear as to how to generate an intermediate result
  • Might be misused if it doesn’t rewrap in TLS (e.g., not to be used as native EAP method without TEAP)

• Create new TEAP TLVs
  • Guarantees that can only be used with TEAP (with outer TLS)
  • Need to confirm how best to create both intermediate and eap-success.
Sample (incomplete flow)

Can do EAP-Success here if we recognize local cert

Can skip BRSKI and go right to enroll if we need to re-enroll
We’re just beginning...

• draft-friel-brski-over-802dot11 is a problem statement that looks also at various approaches

• We’re seeing discussion about which methods are the best way forward

• Is EAP-TEAP the correct way to do this? We’re not sure.

• Is EAP the right mechanism to use? We’re not sure.

• For re-enroll, should registrar be identified somehow by IP address?
  • Do we need an EST discovery mechanism?
  • Should a method provide that?

• Best approach for channel binding?