Proposed Issues: EAP Applicability

Sam Hartman

Painless Security, LLC

IETF 85

November 5, 2012

My Understanding of Scope

- ABFAB Scope: EAP and AAA for application authentication
- Applicability Statement: what applications need to consider when evaluating ABFAB as an authentication approach
- Advice for application security considerations

RETRANSMISSION

- EAP defaults to server-driven retransmits on a timer
- EAP lower layers (applications) MAY indicate they are reliable and set timer to infinite
- Might be needed to fit EAP state machine to application
- Documentation required

Robustness, Retransmission and Discards

- EAP methods can discard a response or request
- Can help improve robustness against attacks when constraints are met
- Interacts with infinite timeouts; documentation required

Re-authentication

- Re-authentication valuable when ending a session is expensive; permits make-before-break for new security parameters
- Network access demonstrates value: avoids disrupting sessions or introducing latency
- Some applications can replace sessions easily

Authorization Lifetime

- EAP keying framework relates MSK lifetime to AAA session lifetime
- Application authorization lifetime is application specific
- Should we document?

QUESTIONS?