RADIUS + DTLS

http://www.ietf.org/internet-drafts/draft-dekok-radext-dtls-00.txt

Alan DeKok
FreeRADIUS

Introduction

- Crypto-agility is required for RADIUS
- The security of RADIUS is “inventive”
- Suffers from any number of attacks
  - Replay
  - Simplistic “encryption” schemes
  - Complete lack of packet verification
  - No privacy (or ad-hoc privacy)
- We can do better...

Proposal: use TLS

- TLS would appear to solve all crypto-agility requirements
  - Strong integrity checks
  - Strong encryption
  - Cryptographic negotiation
  - Designed by people who understand crypto
- Re-inventing crypto work is dangerous

More on TLS

- TLS is good
  - Everyone uses it, including...
  - Radiator has been using “RADSEC” for a while
  - The “proof is in the pudding”
- TLS is bad
  - Due to using TCP
  - RFC 3539 notes problems with AAA & TCP
- Recent developments help

Datagram TLS

- RFC 4347 was recently issued
- TLS over UDP (with some minor changes)
- Other WG's are using it
- OpenSSL supports it
  - Toy implementation of DTLS client & server exists
- Preliminary investigations
  - DTLS to RADIUS gateway is harder than it looks

Problems with DTLS

- It requires more from RADIUS servers
  - Ordered delivery requirements
  - Per-originator connection handling
  - i.e. UDP + accept() + sequence #'s =~ TCP
- Requires DTLS servers to re-implement much of TCP
- Oops..
  - Traded off one problem for another.

Benefits of DTLS

- Solves crypto-agility for once, and forever
- Maybe we don't need shared secrets any more?
  - Sound of many hands clapping
- Section 3 of the draft addresses the crypto-agility requirements

Diameter compatibility

- RADIUS + DTLS is mostly a RADIUS transport layer change
- Proposal for new Service-Type = DTLS
  - Mandates that this never reaches a Diameter server
- Therefore no Diameter impact

Discussion?

- Is DTLS too “heavy”?
- Is session tracking is a problem?
  - How do others (e.g. SIP) do it?
- DTLS to RADIUS gateways?
- Do we need another port?

Relevant drafts

- http://www.ietf.org/internet-drafts/draft-mcgrew-tls-srtp-02.txt
  - Covers multi-session DTLS issues
  - RADIUS Identifier limitations may require multiple DTLS connections
  - We may want to extend the RADIUS Identifier space..
- http://tools.ietf.org/wg/sip/draft-jennings-sip-dtls-03.txt
  - SIP & DTLS