RADIUS Over DTLS

RADEXT - IETF 75

Alan DeKok
FreeRADIUS

draft-dekok-radext-dtls-02.txt

Major updates

- -00 and -01 were nearly content free
- Major new content in -02

Overview

- No changes to RADIUS☂
  - packet / attribute format / encryption
- Leverages RadSec
  - Gives section by section comparison
  - Details of similarities and differences

☂ Practically perfect in every way.

Changes from RadSec

- Mostly clear-cut changes
  - TCP ➙ UDP, RadSec ➙ RDTLS, TLS ➙ DTLS
- Some differences
  - re-uses RADIUS port
  - retains code ➙ port restrictions

Magic

- RADIUS & DTLS on the same port
  - key: { src (ip, port), dst (ip, port) } -> proto
- proto = DTLS or RADIUS
  - works for live “connections”
- proto is DTLS or RADIUS
  - MUST NOT transport both over same key

More Magic

- What about new sessions?
  - key: { src (ip, port) + dst (ip, port) } -> ???
- Look at packet contents
  - (packet[0] == 22) ? DTLS : RADIUS

Step by Step Guide

- Draft outlines full management algorithm
  - When client is known to support a protocol
- Includes processing of legacy RADIUS
- Outlines management of upgrade path

What it does (not) do

- ✓ Future-proof security via TLS
- ✓ Backwards compatibility
- ✓ Simple migration path
- ✖ Order, reliability, fragmentation

Questions?