RADIUS + DTLS

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

Alan DeKok
FreeRADIUS

Introduction

- Crypto-agility is required
- *Forward* security is useful
  - We don't want to re-visit RADIUS security
- RADIUS currently has ad-hoc security
  - authentication (MD5 signatures)
  - encryption (MD5 and xor's)
- -00 draft has expired
  - New draft will be issued post-IETF

Datagram TLS

- RFC 4347 (DTLS) has been published
- TLS over UDP (with some minor changes)
- Other WG's are using it
- OpenSSL supports it
  - Implementations of DTLS clients & servers exist
- Does not change RADIUS operational model
  - UDP...

DTLS and Crypto-Agility

- 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

Simple changes to code

- http://crypto.stanford.edu/~nagendra/papers/dtls.pdf

```
int main(int argc, char **argv)
{
        s = socket(...);
        SSL_init()
        ...
        send(s, ...) -> SSL_write(...)
        ...
        recv(s, ...) -> SSL_read(...)
```

RADIUS compatibility

- DTLS and RADIUS packets are orthogonal
  - less than one chance in 2^128 that packets can be confused
- RADIUS + DTLS can re-use the same ports
  - Simplifies deployment
  - No IANA considerations.

Diameter compatibility

- RADIUS + DTLS is a RADIUS transport layer change
- No changes to the RADIUS protocol
  - No messages, attributes, or enumerations
- Therefore no Diameter impact

Discussion?

- No changes to draft from -00
- Slides have been presented at multiple IETF's
- Feedback has been positive
- All known requirements and issues have been addressed with this proposal.