Sedhcpv6
draft-ietf-dhc-sedhcpv6-21

Wednesday, 19 July 2017

13:30-15:00 (CEST)

Athens/Barcelona

Last Edit: 2017-07-17 18:00 CEST (BV)

Bit of history

- Been around for a long time (2007?)
- Went through WGLC in March
  - Several reviews praised the improvement in quality
  - Chairs and some co-authors concerned about lack of implementations
- Primary author disappeared
- Hackathon in Prague planned
- Key signing size limitation discovered
- Stepped back and asked what problem are we trying to solve?

Discussed since IETF'98

- RSA is able to sign up to 2048 (256 bytes):

Generate a 256-bit random keystring K
Encrypt your data with AES-CBC with K
Encrypt K with RSA
Send both to the other side

- elliptic curves
- opportunistic IPsec
- DTLS
- Null auth IPsec
- 802.1x

Discussed in Prague

- Small group met on Sunday (Ted Lemon, Francis Dupont, Tomek, Bernie), went through the use cases and reached a conclusion: dead in its current form
- Discussed with Sec AD afterwards
  - Kathleen suggested to publish as Experimental
  - Kathleen would like to see opportunistic encryption

Use cases

- Corporate network
  - Use 802.1x to protect client-relay and IPsec for relay-server
  - DHCPv6-shield (RFC7610)
- Coffee shop
  - Trust-on-First-Use model, helps a bit with pervasive monitoring, but only if the infrastructure does not participate. Some auth schemes (e.g. sticker with QR code) opening new attack surfaces
- Insider attack in corporate network
  - Fred: one 802.1x authenticated user impersonates another

Next steps

Fix the key signing limitation,
publish as experimental

Rework to JUST do
opportunistic encryption

Work on **problem statement** first,
then restart the work

Drop the work