DHCPv6 Security
(discussion summary)

draft-ietf-dhc-sedhcp6-08
draft-cui-dhc-dhcpv6-encryption-01
draft-li-dhc-secure-dhcpv6-deployment-01

(Tomek Mrugalski)

IETF'94 Yokohama

A bit of history

- draft-jiang-dhc-secure-dhcpv6-00 published in July 2008
- draft- ietf-dhc-secure-dhcpv6-07, hits IESG in Mar 2013
- Rejected: rewrite without CGA
- Sheng et al. did as requested: draft-ietf-dhc-sedhcpv6
- Adopted, last called, sent to IESG in Jan 2015
- Significant changes requested during AD review:
  - Missing threat analysis
  - Missing use cases/applicability statement
- IESG asked Randy Bush to help and things got interesting…

State couple days ago

- draft-ietf-dhc-sedhcpv6
  - Certs/public keys, TOFU, authentication only
- draft-cui-dhc-dhcpv6-encryption
  - Public keys, encryption only, no authentication
- draft-li-dhc-secure-dhcpv6-deployment-01
  - threat model
  - deployment scenarios

Discussed Issues 1

- Should we include encryption?
  - Pervasive monitoring problem (RFC7258)
  - Opportunistic Encryption: Some protection most of the time (RFC7435)
  - If we don't do this, the vendors will implement authentication only and claim to be secure
  - Without encryption, doing just auth is a huge privacy leak
  - Today encrypted traffic stands out
  - With authentication implemented, encryption is simple
  - Decision: **include encryption**
- Should we combine the auth and encryption drafts?
  - Otherwise the relation between them would be confusing:
    do I need both? Can I do auth only? Enc only? Can do enc if I do auth?
  - Significant overlap (options, key exchanges, etc.)
  - Decision: **combine drafts**

Discussed Issues 2

- TOFU is tricky to get it right
  - Accepted automatically?
  - Excuse for operator to skip necessary setup for security
  - Introduction problem
  - Decision: **out of scope <u>for now</u>**
- Need threat analysis and good use cases description
  - What problems we're trying to solve
  - How to properly use the solution being developed
  - Decision: **rescope and continue working on li-secure-dhcpv6-deployment, adopt when more mature**

Proposal

- The algorithm:
  - if you can, do authentication and encryption
  - if you can’t, just do encryption
- Merge dhc-sedhcpv6 and dhcpv6-encryption
- TOFU out of scope for now
- Companion draft: li-dhc-secure-dhcpv6-deployment
  - Threat analysis (requested by IESG)
  - Use cases (requested by IESG)

drafts presentation

Next Steps

- Ok to drop authenticated-only mode (available options: plain, encrypt, encrypt+auth)?
- Ok for TOFU to be out of scope for now?
- Continue refining draft-li-dhc-secure-dhcpv6-deployment, when ready go with adoption call?