Security of Messages Exchanged Between Servers and Relay Agents

IETF-96

draft-volz-dhc-relay-server-security-01

Bernie Volz & Yogendra Pal

Last Updated: 07/07/2016 12:02 EDT

Background & Motivation

- IESG raised issues regarding draft-ietf-dhc-access-network-identifier (now RFC7839)

(1) Did the DHC working group consider how this information, when sent without adequate protection between relay and dhcp server, could help in pervasive monitoring? If so, what was the conclusion reached? We have seen http header field information sent between infrastructure nodes being intercepted for that purpose, so this has to be similarly at risk. If the answer is that this is only to be used within a single network operator's setup (or a roaming arrangement) then that needs to be justified (as practical) and, if it can be justified (I'm not sure tbh), also made explicit.

(2) I had a DISCUSS on the draft that became rfc 6757 about protection of this kind of data. In that context I think I was assured that everything (in PMIPv6) was IPsec protected so it was fine. Why, in what we now know is a more threated environment, is it ok to now have weaker protection when I was assured then that IPsec was in fact quite usable in PMIPv6? I think you maybe need to put in a MUST use IPsec requirement for this to be as safe.

(3) section 7: MAY store - this is possibly sensitive information so you ought say that it SHOULD NOT be stored unless needed, and if stored, SHOULD be deleted as soon as possible. Storing sensitive information when not needed just shouldn't be considered acceptable anymore I think - is that reasonable?

Current State of DHCP "Security"

- RFC 2131 (RFC 1542)
  - No security for relay to server communication
- RFC 3315
  - "Use" IPsec (RFC 2401) – Not MUST

```
21.1. Security of Messages Sent Between Servers and Relay Agents

   Relay agents and servers that exchange messages securely use the
   IPsec mechanisms for IPv6 [7].  If a client message is relayed
   through multiple relay agents, each of the relay agents must have
   established independent, pairwise trust relationships.  That is, if
   messages from client C will be relayed by relay agent A to relay
   agent B and then to the server, relay agents A and B must be
   configured to use IPSec for the messages they exchange, and relay
   agent B and the server must be configured to use IPSec for the
   messages they exchange. …
```

Draft Proposes

- Use IPsec for DHCPv6 and DHCPv4 relay <-> relay and relay <-> server communication
  - Already available on most operating systems (Linux, …) for servers
  - Typically also available on routers (relays) & firewalls
- Highly recommended unless other mechanism(s) in place (i.e., VPN)
- Encryption is recommended as relay agents may forward unencrypted client messages as well as include additional sensitive information, such as vendor-specific information (i.e., CableLabs DHCP) and Access-Network-Identifier Options [RFC7839]

IPsec Details

- Mode
  - Relay agents and servers MUST use IPsec in transport mode and Encapsulating Security Payload (ESP)
- Encryption and authentication algorithms
  - Recommend combined mode algorithms for ESP authenticated encryption, ESP encryption algorithms, and ESP authentication algorithms as per section 2.1, 2.2, and 2.3 of [RFC7321] respectively
- Key management
  - Manually configured key management should suffice
    - Relay agents and servers are typically manually configured
    - However, does not provide defense against replayed messages
  - IKE/IKEv2 with pre-shared secrets SHOULD be supported
  - IKE/IKEv2 with public keys MAY be supported

Next steps

- Adopt as WG item?
- Consider alternative security mechanisms?
- Other comments / questions?