DHCP Relay / Server Communication and Pervasive Monitoring

IETF-95

Bernie Volz

Last Updated: 03/22/2016 15:00 EDT

Background & Motivation

- IESG raised issues regarding draft-ietf-dhc-access-network-identifier

(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 “Security”

- RFC 2131 (RFC 1542)
  - No security for relay to server communication
- RFC 3315
  - “Use” IPsec (RFC 2401) – Not MUST. Is it used?

```
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. …
```

So, do we need to “fix” this?

- Is there a real problem?
- Does the WG want to work on this?
- What tools do we have?
  - IPsec sufficient? (Could also be used for v4)
  - Use seDHCPv6? (Pre-shared keys SHOULD be OK)
  - Consider TLS (either over UDP or TCP)?
  - What else …
- Must work Relay <-> Relay & Relay <-> Server

Next steps

- Should we work on this?
- If so …
  - Who wants to work on this?
  - Create a design team or discuss on ML?

(RFC 2418) 6.5. Design teams
It is often useful, and perhaps inevitable, for a sub-group of a working group to develop a proposal to solve a particular problem. Such a sub-group is called a design team. In order for a design team to remain small and agile, it is acceptable to have closed membership and private meetings. Design teams may range from an informal chat between people in a hallway to a formal set of expert volunteers that the WG chair or AD appoints to attack a controversial problem. The output of a design team is always subject to approval, rejection or modification by the WG as a whole.