DHCPv6/DHCP options for LWM2M bootstrap information

draft-ietf-dhc-dhcpv6-lwm2m-bootstrap-options-00

Srinivasa Rao Nalluri Ericsson

Context

- **draft-ietf-dhc-dhcpv6-lwm2m-bootstrap-options-00**
  - Replaces **draft-nalluri-dhc-dhcpv6-lwm2m-bootstrap-options-03**
  - Presented in IETF-99
  - Adopted by WG

WG Review

- Important WG comments

[Francis Dupont]

- as IKEv2 is over UDP too this problem is addressed in RFC 7296 by allowing many different "encodings" (currently 15 in the IANA registry).

So I am afraid authors just took a good text about certificate transport (BTW I'd pick the same one so my concern is not about the choice) but missed to add an additional statement about application.

I propose:

- add something about the encoding byte so nobody will forget to read RFC 7296 and for instance put a X.509 certificate as the whole content

[Srinivas] Section 4 added to describe details on certificate encoding

WG Review

[Bernie Volz]
In section 3.2 and 3.4, the option-len field is described incorrectly:
option-len: Length of the 'LWM2M-server-certificate' field in octets
It should be ?1 + length of the 'LWM2M-server-certificate' field in octets? (to account for the cert-encoding octet).

And, also in 3.4:

LWM2M-server-certificate: Digital certificate of LWM2M server
encoded accoring to cert-encodeing. See Section 4<https://tools.ietf.org/html/draft-nalluri-dhc-dhcpv6-lwm2m-bootstrap-options-03#section-4> for details

I think the table added in the 03 version in section 4 has a column heading missing to indicate what unspecified/deprecated means? And, not sure why those numbers with document references weren?t included? Also, it isn?t clear why some entries were eliminated? I would either suggest removing the table completely, or reproducing it as it is fully (I understand the reserved values (0 and 5) were removed, but it causes someone to wonder why they aren?t there). Ah ? I see that the table was copied from RFC 7296 and not from IANA?s pages. I still think the IANA pages would be better or not to reproduce the table?

WG Review

[Srinivas]

- Option length corrected
- Certificate encoding types tables is corrected by picking correct values from IANA
- Mistyped words are corrected

IoT Expert review

- WG insisted on expert review
- Requested T2TRG for review
- Reviewers assigned for review by T2TRG chair (Ari Keränen)
  - Hannes Tschofenig
  - Carsten Bormann

IoT expert review comment

[Hannes Tschofenig] How do you prevent that an attacker sets up a DHCP server and points to his or her LwM2M bootstrap server and thereby takes full control of the IoT device?

[Srinivas]

- Make sure there is L2 switch between DHCP client and server(maybe on or close to access node) and DHCP snooping function running on it. Make sure DHCP server(s) is reachable through one trusted switch port. Use firewall to filter all DHCP server messages on all other ports.

-Install DHCP relay agent (or proxy) on access node so that broad cast messages are terminated and unicast request are sent to preconfigured DHCP servers.

As these DHCP servers which are reachable through above means are controlled by service provider I don’t see any significant risk. These mechanisms are today implemented in network gateways (For example, PGW in 4G core and Broadband Network Gateway in fixed access)

I did not mention above text in draft considering it as deployment explanation. If you think it make sense we can include this in security section of draft.

IoT expert review comment

I think the challenge is to design something that is independent of some other security mechanisms outside the device. Currently, there is no solution in the document that provide this and I fear that in practice this security will not work since those who deploy the solution are not necessarily aware of the tradeoffs.

I fear that your proposal right now causes more security problems then it solves. I will think about can be done about this.

Next Steps

- WG opinion on expert comment
- Discuss further with IoT expert to Close comment

Thank you