6lo
Internet-Draft
Intended status: Standards Track
Expires: September 5, 2015

S. Kumar
Philips Research
P. van der Stok
Consultant

March 4, 2015

Security Bootstrapping over IEEE 802.15.4 in selective order
draft-kumar-6lo-selective-bootstrap-00

Abstract

Low-resource devices in a Low-resource and Lossy Network (LLN) can be based on a mesh network using the IEEE 802.15.4 link standard. Security in these networks MUST be enforced at the link level. Provisioning the devices in a secure manner with keys (often called security bootstrapping) to encrypt and authenticate the link-layer messages is the subject of this specification. This proposal distinguishes itself from other bootstrap proposals by requiring that the devices can be secured in an order determined by the needs of the installation procedure. Other proposals use an "onion model", where first the devices one-hop away from the initial device (often the border router) are secured, followed by the devices that are one-hop away from already secured devices.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 5, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) [RFC4944] on IEEE 802.15.4 [ieee802.15.4] wireless networks is becoming common in many professional domains such as lighting controls. However commissioning of such networks is not easy due to a lack of standardized secure bootstrapping mechanisms for these networks.

The security of IEEE 802.15.4 MAC frames is based on Advanced Encryption Standard (AES) [FIPS.197.2001] in Counter with CBC-MAC Mode (CCM) [CCM] which provides confidentiality and authenticity.

There are different security levels or combinations of authenticated encryption defined in IEEE 802.15.4 as shown in Table 1.

Security Level	Confidentiality	Message Integrity Code (MIC)
0	None	None
1	None	Yes (4 byte MIC)
2	None	Yes (8 byte MIC)
3	None	Yes (16 byte MIC)
4	Yes	None
5	Yes	Yes (4 byte MIC)
6	Yes	Yes (8 byte MIC)
7	Yes	Yes (16 byte MIC)

Table 1: IEEE 802.15.4 supported Security Levels

Although IEEE 802.15.4 defines how security can be enabled between nodes, it does not specify the provisioning and management of the keys. Therefore securing a 6lowpan network with devices from multiple manufacturers with different provisioning techniques is often tedious and time consuming.

Some industry standards have tried to solve the issue by using a mix of other protocols with extensions. For example, Zigbee-IP [ZigbeeIP] uses Protocol for carrying Authentication for Network Access (PANA) [RFC5191] with the additional PANA-Relay [RFC6345] to carry EAP-TLS [RFC5216] packets to the joining node as shown in Figure 1.

```
   +-----------------+
   |    EAP Peer     |    +-------------+
   +-----------------+    |PANA Relay   |
   |PANA Client (PaC)|<-->|Element (PRE)|
   +-----------------+    +------^------+
     Joining Node                |
                                 |
                                 |
                         +-------v-----------+          +-----------+
                         |EAP Authenticator  |          |EAP Server |
                         +-------------------+<--------->+-----------+
                         |PANA Authentication|          |AAA Server |
                         |Agent (PAA)        |          +-----------+
                         +-------------------+
```

Figure 1: EAP over PANA for bootstrapping

The additional protocol stack of PANA and EAP provides for a large amount of flexibility in terms of potential security protocols and cryptographic algorithms that can be used for authentication and key distribution. However this flexibility is often not needed in IoT scenarios or often not wanted for inter-operability reasons (e.g. Zigbee-IP only uses EAP-TLS mode with two possible cryptosuites). DTLS-Relay [I-D.kumar-dice-dtls-relay] as depicted in Figure 2 is an alternative simpler proposal based on trust enrolment [I-D.jennings-core-transitive-trust-enrollment] that provides the same results by reusing the security protocols (like DTLS [RFC6347]) that already exist on IoT devices.

```
   +--------+        +-------+          +-------+
   |  DTLS  |        | DTLS  |          | DTLS  |
   | Client |<------>| Relay |<--------->|Server |
   +--------+        +-------+          +-------+
    Joining                                AAA
     Node                                 Server
```

Figure 2: DTLS Relay for bootstrapping

Numerous other recent proposals like [I-D.pritikin-anima-bootstrapping-keyinfra], [I-D.richardson-6tisch--security-6top], [I-D.struik-6tisch-security-considerations], [I-D.ohba-6tisch-security], [I-D.he-iot-security-bootstrapping] discuss network bootstrapping in multi-hop networks and their architectural implications. However an essential aspect of all these

techniques (including the PANA-Relay and DTLS-Relay) is that they rely on an "Onion" topology for bootstrapping: devices which are one-hop wireless from the Border Router (or Commissioning Device) are provisioned first. Devices multiple hops removed from the border router are provisioned by an already provisioned neighbour (an "Onion" layer) until the whole network is bootstrapped.

Such an "Onion" model can be limiting in various professional domains where a large number of devices need to be commissioned (provided with installation information) in an order determined by their physical layout rather than by the wireless network topology. The wireless network topology is often unknown to a commissioner and may vary over time due to environmental conditions (e.g. presence of scaffolding during construction). Therefore, "onion" bootstrapping proposals force a tedious separation of the actual device commissioning done by a domain expert from the security bootstrapping of the devices. The purpose of the bootstrapping proposal of this specification is a simultaneous execution of commissioning and bootstrapping.

In this specification, the bootstrapping order of the nodes can be selected by a commissioner.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Readers are expected to be familiar with all the terms and concepts that are discussed in "neighbour Discovery for IP version 6" [RFC4861], "IPv6 Stateless Address Autoconfiguration" [RFC4862], "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919], "neighbour Discovery Optimization for Low-power and Lossy Networks" [RFC6775] and "Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [RFC4944].

This specification uses the following terms from [RFC6775]:

6LoWPAN link: A wireless link determined by single IP hop reachability of neighbouring nodes. These are considered links with undetermined connectivity properties as in [RFC5889].

6LoWPAN Node (6LN): A 6LoWPAN node is any host or router participating in a LoWPAN. This term is used when referring to situations in which either a host or router can play the role described.

6LoWPAN Router (6LR): An intermediate router in the LoWPAN that is able to send and receive Router Advertisements (RAs) and Router Solicitations (RSs) as well as forward and route IPv6 packets. 6LoWPAN routers are present only in route-over topologies.

6LoWPAN Border Router (6LBR): A border router located at the junction of separate 6LoWPAN networks or between a 6LoWPAN network and another IP network. There may be one or more 6LBRs at the 6LoWPAN network boundary. A 6LBR is the responsible authority for IPv6 prefix propagation for the 6LoWPAN network it is serving. An isolated LoWPAN also contains a 6LBR in the network, which provides the prefix(es) for the isolated network.

Router: Either a 6LR or a 6LBR. Note that nothing in this document precludes a node being a router on some interfaces and a host on other interfaces as allowed by [RFC2460].

This specification uses the following new terms:

Commissioning Tool (CT): A processor that contains keying material, authorizes nodes to join, and communicates the keying material.

6LoWPAN Joining Node (6JN): A 6LoWPAN node that is next to join a secured LoWPAN mesh. This term is used when either the node sends a join request to the CT or the CT sends key material to the node for joining.

6LoWPAN Secured Router (6SR): A 6LoWPAN router that has joint a secured LoWPAN mesh. This term is used when the router has received the key material to join the LoWPAN mesh.

6LoWPAN Un-secured Router (6UR): A 6LoWPAN router that has NOT joint a secured LoWPAN mesh. This term is used when the router has received no key material to join the LoWPAN mesh.

3. Use Case

In lighting controls a major shift is on its way from lighting specific networking standards like [DALI] to Internet networking standards. This shift has a profound influence on the installation and commissioning of the lighting control network. With special purpose networks, the installation of the lighting control and the network were done during the same installation phase.

The choice for the Internet Protocol is motivated by the reduction of costs by separation of concerns, in this case: The separation of the network installation from the lighting control installation and

commissioning. For Internet based installations the following phases are expected in a fair number of installations:

Electric installation: All electric cabling is laid out and connections are validated.

Network installation: All network interfaces are connected and validated.

Lighting installation: All lighting fixtures are named and other information is loaded into them (commissioning); simultaneously the security bootstrapping of the network is done.

Dependent on the installation company, the proposed network configuration, and the installation contract, these phases and their order may not be respected and a bootstrap protocol may be used different from the one described in this specification.

For an IEEE 802.15.4 network [ieee802.15.4] the specified three phases imply that after the network installation, non-battery powered devices are connected to their electricity supply, and the IEEE802.15.4 layer-2 mesh and the 6LoWPAN IP layer-3 mesh is configured. Also the preferred IP routing protocol must be working to route messages between IEEE 802.15.4 interfaces based on their IP address. During the Lighting installation, devices are selected according to an installation-dependent protocol, named, and layer 2 security keys are loaded into the devices. When all designated devices have received their security keys, the network is closed such that only authorized nodes can route messages in the network, and data packets can only be exchanged between the layer-2 secured devices. The layer-3 routing protocol MUST continue routing messages before, during and after the Lighting installation procedure.

The selection of the devices is executed by an installation engineer using a Commissioning Tool (CT). According to an installation-dependent protocol a device is selected from the set of not yet selected devices, and its identity is communicated to the CT. The CT exchanges messages with the selected device to distribute the keys (see Section 5.4) and other installation specific data. The order of selection is completely installation and installer dependent, is optimized for low cost, and is not aware of network topology.

4. Requirements

This section lists the requirements for the bootstrap solution.

Selection of device: The commissioner is able to select an installed device and commission it without the knowledge of the wireless network topology.

Device authenticity: A commissioner should be able to verify that the credentials of the device being bootstrapped match the credentials of the one selected to commission.

Device authorization: A commissioner should be able to decide if a particular authenticated device can indeed be part of the secure network being created.

Commissioning Tool (CT) authenticity and authorization: The device being commissioned can verify if the CT is allowed to bootstrap the device. Alternatively, the device may allow any CT to bootstrap it provided a mechanism exists, either in-band or out-of-band, to reset it and start over again.

Key Confidentiality: The layer-2 key that is used to secure the network should be encrypted such that only the device being commissioned can decrypt the key.

Key Authenticity: The device should be able to verify that the layer-2 key has not been tampered during transport.

5. Mesh Bootstrap Procedure

The flow of the mesh bootstrap procedure involves a joining node (6JN), a Commissioning Tool (CT) and a path over secured routers (6SR) and unsecured routers (6UR). It is assumed that Neighbour discovery has been executed, and a router protocol supports the routing through the mesh. In the beginning all routers (6LR) are unsecured.

A 6JN announces its presence by sending a join request to the CT. The join request is routed over the mesh involving possibly 6UR and 6LR to the CT. The 6JN MAY be identified by its EUI64 identifier [EUI64]. The identifier MAY be transported in the join request.

In an alternative approach with its own operational constraints, the CT already has a list of all node identifiers, and uses a different bootstrapping protocol. This approach is not the subject of this specification.

The CT on receiving the join request can decide if 6JN is a legitimate device and if it can be part of secure network being commissioned. If positive, then the CT sends the layer-2 key material to the node via a secured channel. The receiving node

installs the key material and passes from unsecured to secured node. The secured node sets up secured links with its 6SR using the received key material. When all nodes are secured, the network is secured, and communication (routing) is only allowed via secured channels.

5.1. Network Layout

The network to be secured consists of a set of wireless nodes interconnected to a mesh network via IEEE 802.15.4 interfaces. The mesh network may be connected to a border router (6LBR) as described in [RFC6775]. The 6LBR may be connected to a backbone. The CT can be connected to the mesh network to be connected in several ways:

CT is connected to an IEEE802.11 interface that communicates with the IEEE802.11 Access Point Located in the 6LBR.

CT is connected to the backbone directly or via a path composed of one or more routers.

It is required that messages can be routed between the CT and each of the candidate devices in the mesh to be secured.

In an alternative network, not considered here, the CT is connected with an IEEE 802.15.4 interface to the mesh network. In this case the 6LBR is not required. A mobile CT can then do one-hop commissioning of the devices.

5.2. Commissioning Tool discovery

The discovery of the Commissioning Tool (CT) by the 6LR is outside the scope of this specification. The CT can be discovered in several ways dependent on the infrastructure, for example:

Mesh connected to backbone: In this case the CT can announce its presence in DNS using DNS-SD [RFC6763]. The 6JN can query DNS for the address of the nodes supporting the CT service.

Resource Directory present: When a Resource Directory (RD) [I-D.ietf-core-resource-directory] is present, the CT can store the presence of its service in the RD. The 6JN can query the RD for the address of the nodes supporting the CT service.

Stand alone mesh: The 6JN can send a multicast to /.well-known/core querying the existence of the CT service.

5.3. Bootstrap security layer

The purpose of this document is to specify a so-called "bootstrap-layer" between layer-2 and layer-3 to satisfy the use case of Section 3. In the text the "joining node" (6JN) is the unsecured router (6UR) that is selected to be the next 6LR to be secured. The following considerations have led to the definitions of the bootstrap layer:

Messages MUST be routed between CT and the 6JN.

The route between CT and 6JN may pass through the 6LBR.

The route between CT and 6JN may pass through secured routers (6SR) and unsecured routers (6UR).

The last consideration follows directly from the installation-dependent order of 6JN selection. The last consideration also means that a 6SR has to communicate over secured and unsecured links.

Every 6LR maintains in the bootstrap-layer:

A list of its neighbours. (This list can be shared with neighbour discovery, or with other protocols).

A Boolean variable, ALL_SECURED, which initially is false.

These two items constitute the bootstrap state of a 6LR.

The neighbour list of the node contains information whether a link between itself and the neighbour is secured. Dependent on the value of the bootstrap state, packets are refused, encrypted, decrypted, and passed on between layer-2 and layer-3.

5.3.1. ICMP messages

The protocol uses one ICMP message transporting two bootstrap requests:

Join Secure Request (JSR): This is an unsecured message that is sent from an 6UR to the CT with the request to be secured.

Set Secure Request (SSR): this is a secured message that is sent from a 6SR to signal its secured state to a neighbour 6LR

The layout of the ICMP messages is:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |     Code      |          Checksum             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Status     |   Reserved    |     Registration Lifetime     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                            EUI-64                             +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: ICMP message layout

IP fields:

IPv6 source: In a JSR this the non link-local address of the sending 6UR; in a SSR this is the link-local address of the sending 6SR.

IPv6 destination: In a JSR this is non link-local address of the CT; in a SSR this is the link-local address of a neighbour 6LR.

Hop Limit: Set to MULTIHOP_HOPLIMIT on transmit. MUST be ignored on receipt.

ICMP Fields:

Type: TBD for JSR and for SSR

Code: Set to one for JSR and set to two for SSR.

Checksum: The ICMP checksum. See [RFC4443].

Status: 8-bit unsigned integer. Indicates the status of a registration in the CT. MUST be set to 0 in JSR. See Table 2.

Reserved: This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Registration Lifetime: 16-bit unsigned integer. The amount of time in a unit of 60 seconds that the 6LR should retain the secure state in the Neighbor entry for the sender of the SSR.

EUI-64:   64 bits. This field is used to uniquely identify the
               interface of the registered address by including the
               EUI-64 identifier [EUI64] assigned to it unmodified.

The Status values used in JSR and SSR are (to be done/ eventually removed):

Status	Description
0	Success
1	Duplicate Address
2	Impossible
3-255	Allocated using Standards Action [RFC5226]

Table 2

5.3.2. Joining a 6LR to the secured mesh

```
   +------+   +------+    +------+   +------+    +------+    +------+
   |      |   |      |    |      |   |      |    |      |    |      |
   |  CT  |   | 6LBR |    | 6SR  |   | 6UR  |    | 6JN  |    | 6SR  |
   +------+   +------+    +------+   +------+    +------+    +------+
      |          |           |           |           |           |
      |          | (secured) |(unsecured)|(unsecured)|(unsecured)|
      |          |           |           |           |           |
      |          |           |           | <--(1)----|           |
      |          |           | <---(2)---|    JSR    |           |
      |          |<---(3)--- |           |           |           |
      | <--(4)-- |           |           |           |           |
      |          |           |           |           |           |
      |=================(5)=========================>|           |
      |          |   (many packets    DTLS           |           |
      |          |           |           |           |           |
      |          |           |           | <--(6)----| ---(7)--->|
      |          |           |           |    SSR    |    SSR    |
      |          |           |           |           |           |
      |          |           |           |           |<---(8)----|
      |          |           |           |           |    SSR    |
      |          |           |           |           |           |
      |          | (secured) |(unsecured)|(unsecured)| (secured) |
      |          |           |           |           |           |
```

Figure 4: Message flow diagram of bootstrap protocol

Figure 4 is a message flow diagram representing the bootstrapping protocol message exchange. The diagram is quite close to the message flow diagram of [I-D.richardson-6tisch--security-6top]. It is assumed that the neighbours have discovered each other at layer-2 with the IEEE802.15.4 beacons. Also it is assumed that all NS, RS, RA, and DAD messages have been exchanged with Neighbour Discovery. Also the routing protocol has started.

Assume, that at some point during the security bootstrap protocol, the 6LBR interface and the two 6SR interfaces have been secured. Before the bootstrap protocol starts the variable ALL_SECURED is set to false in all nodes.

The 6JN sends at (1) a JSR over an unsecured channel containing its EUI64 identifier. At (2) the message is routed on over an unsecure channel, and at (3) it is routed to the 6LBR over a secure channel. At (4) the unsecured request is passed on to the CT. After reception, the CT sets up a secure end-to-end DTLS link with 6JN (described further in Section 5.4) and securely transfers the keys over this DTLS session at (5). The secure DTLS packets are routed over secure and unsecure layer-2 channels in the mesh. Once the keys are installed, the 6JN sends a SSR to both neighbours at (6) and (7). At (8) the 6SR neighbour returns a SSR to 6JN. Afterwards the link between 6JN and 6SR is secured.

When all designated 6LR have become 6SR, the CT sends a network close messages to all designated 6SR. On reception, the 6SR nodes set their variable ALL_SECURED to true.

5.3.3. Packet handling

Dependent on the bootstrap state of the 6LR, the following rules are followed by the bootstrap layer for the communication with a neighbouring 6LR, called N. The packet handling is specified under 3 conditions:

Condition 1: The link with N is signalled secure in the neighbour list:

- An unsecured packet arriving from N is refused.

- A secured, authenticated packet arriving from N is decrypted and if authentication is verified, passed on to layer 3.

Condition 2: The link with N is signalled NOT secure in the neighbour list, and ALL_SECURED is false:

- When the receiving node is secured, a secured packet arriving from N is decrypted and if authentication is verified, passed on to layer-3. This is needed for the SSR packet at step (8) in Figure 4.

- When the receiving node is not secured, a secured packet from N is refused.

- An unsecured packet from N is passed on to layer-3.

Condition 3: ALL_SECURED is true:

- All unsecured packets are refused.

Packets coming from layer-3 with destination N are sent according to the rules:

- When the link with N is signalled secure in the neighbour list, the packet is encrypted and authenticated.

- When the link with N is signalled unsecure in the neighbour list, the packet is sent without encryption or authentication.

5.3.4. Securing a channel

After termination of the secure key transfer (see Section 5.4, the node fills the ACL table maintained at layer-2 [ieee802.15.4]. The next stage is to determine whether the neighbours are also equipped with the keys. Once the neighbour of a secured node is secured, the link between the two MUST be declared secure in the list of both neighbours. The determination of a secure link is done by exchanging SSR messages, according to the following protocol:

> A node that has set its keys in the ACL table sends a secured SSR message to all its neighbours.
>
> On reception of a secured SSR from node N, and the link of node N is not secured in the list of neighbours, and the receiving node is secured, the receiving node sends a secured SSR to node N; consecutively, the receiving node sets the link of neighbour N to secured in the list of neighbours.
>
> On reception of a secured SSR from node N and the receiving node is NOT secured, the receiving node rejects the message.

5.4. Secure key transfer

The layer-2 keys are distributed to the devices over a secure DTLS session as indicated in message (5) in Figure 4. This DTLS session is created using a trust anchor that is deployed in the devices during manufacturing. The trust anchor can be for e.g. one of these listed below:

- Pre-shared key: The manufacturer of the device can embed a pre-shared key as a trust anchor during the personalization of the device in the factory. The key along with EUI-64 of the device is then shared with authorized commissioners such that a secure DTLS channel based on [RFC4279] can be established between the CT and 6JN. It is recommended to use the cipher suite TLS_PSK_WITH_AES_128_CCM_8 [RFC6655] which is the mandatory to implement cipher suite for use with shared secret based DTLS in Constrained Application Protocol (CoAP) [RFC7252].

- Raw public key: The manufacturer of the device can embed a {pubic-key, private-key} pair of an asymmetric cryptographic algorithm as a trust anchor during the personalization of the device in the factory. The public-key (or a hash of the public-key) is available out-of-band (for e.g. printed on the device) to the commissioner to enable authentication and authorization of the selected device over a secure DTLS channel based on [RFC7250]. It is recommended to use the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 [RFC7251] which is the recommended cipher suite for raw-public key based DTLS in CoAP.

- Certificates: The manufacturer of the device can embed a {public-key, private-key} pair along with a certificate (signed by the manufacturer or a trusted third party) linking the public-key to an identity in the device. This could be for example an IEEE 802.1AR certificate [IDevID] which links the public-key to the EUI-64 of the device. The DTLS session is then established between the CT and JN based on the trust in the certificate. It is recommended to use the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 which is recommended for certificate based DTLS in CoAP.

It is important to note that only the pre-shared key option above provides mutual authentication of the DTLS channel. For raw public key and certificate option, an additional root public key needs to be provisioned in the device for authenticating the CT with a mutually authenticated DTLS handshake.

6. Setting layer-2 key values

Once the DTLS session is established (using any of the trust anchors mentioned above), the layer-2 keys can be transported within the secure session. The setting of the values in the device can be achieved using a CoAP request on a well-defined CoAP resource which is used for configuring the MAC layer keys, in analogy to the multicast address setting in [RFC7390].

Another solution is using a YANG file that specifies configurable key entries, the values of which can be set with for example CoMI [I-D.vanderstok-core-comi].

CoAP endpoints implementing the layer-2 key setting RESTful interface MUST support the CoAP Internet Media Type "application/coap-group+json".

A resource offering this representation can be annotated for direct discovery [RFC6690] using the Resource Type (rt=) Link Target Attribute "core.ky", where "ky" is shorthand for "layer-2 key values". An authorized client uses this media type to query/ manage layer-2 key values of a CoAP endpoint as defined in the following subsections.

TODO: specify payload format and resource name "/coap-key2"

7. IANA Considerations

The document registers one new ICMPv6 "type" number under the subregistry "ICMPv6 "type" Numbers":

- Bootstrap Request (xxx)

8. Security Considerations

- During the commissioning period, rogue nodes can use the network and send requests to 6LR and thus compromise the nodes. It is recommended that during the period from network start up till the end of the secure bootstrapping, no resources can be accessed in the 6LR. Consequently, the nodes can only exchange ICMP messages. In this case the routing tables and the neighbour tables of the 6LR can be corrupted. Such corruption will be detrimental to the bootstrap process and can be detected, after which the installer SHOULD take measures to remove the rogue nodes.

- After all nodes in the network have been commissioned, the network needs to be finally secured by setting ALL_SECURED to true for all nodes. This final message needs to be securely sent by the CT

either in unicast or multicast to all the nodes in the network. If additional nodes need to be added to the network at a later point in time, a new secure message needs to be sent by the CT with ALL_SECURED set to false. This message can either be sent to the whole network or (if known) only to the neighbours of the joining node. Both messages that change the ALL_SECURED state should be authenticated by the CT and not re-playable.

- The large number of messages exchanged between the joining node and CT can be misused by a rogue node to create a Denial-of-Service (DoS) at nodes closer to the 6LBR, 6LBR itself or at the CT. This can be limited by ensuring that the DTLS handshake is only performed by the CT with a node that the commissioner has presently chosen to bootstrap. Thus the rogue messages are only limited to ICMP "Bootstrap Request" messages.

9. Acknowledgements

The authors would like to thank Peter Lenoir and Dee Denteneer for the valuable discussions that helped in shaping the solution.

10. Change log

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, August 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

11.2. Informative References

[CCM] National Institute of Standards and Technology, , "SP 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", May 2004.

[DALI] IEC, , "Digital Addressable Lighting Interface, IEC 62386", June 2009.

[EUI64] IEEE, "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>.

[FIPS.197.2001] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[I-D.he-iot-security-bootstrapping] ana.hedanping@huawei.com, a., "Security Bootstrapping of IEEE 802.15.4 based Internet of Things", draft-he-iot-security-bootstrapping-00 (work in progress), January 2015.

[I-D.ietf-core-resource-directory]
Shelby, Z. and C. Bormann, "CoRE Resource Directory", draft-ietf-core-resource-directory-02 (work in progress), November 2014.

[I-D.jennings-core-transitive-trust-enrollment]
Jennings, C., "Transitive Trust Enrollment for Constrained Devices", draft-jennings-core-transitive-trust-enrollment-01 (work in progress), October 2012.

[I-D.kumar-dice-dtls-relay]
Kumar, S., Keoh, S., and O. Garcia-Morchon, "DTLS Relay for Constrained Environments", draft-kumar-dice-dtls-relay-02 (work in progress), October 2014.

[I-D.ohba-6tisch-security]
Chasko, S., Das, S., Lopez, R., Ohba, Y., Thubert, P., and A. Yegin, "Security Framework and Key Management Protocol Requirements for 6TiSCH", draft-ohba-6tisch-security-01 (work in progress), March 2014.

[I-D.pritikin-anima-bootstrapping-keyinfra]
Pritikin, M., Behringer, M., and S. Bjarnason, "Bootstrapping Key Infrastructures", draft-pritikin-anima-bootstrapping-keyinfra-01 (work in progress), February 2015.

[I-D.richardson-6tisch--security-6top]
Richardson, M., "6tisch secure join using 6top", draft-richardson-6tisch--security-6top-04 (work in progress), November 2014.

[I-D.struik-6tisch-security-considerations]
Struik, R., "6TiSCH Security Architectural Considerations", draft-struik-6tisch-security-considerations-01 (work in progress), January 2015.

[I-D.vanderstok-core-comi]
Stok, P., Greevenbosch, B., Bierman, A., Schoenwaelder, J., and A. Sehgal, "CoAP Management Interface", draft-vanderstok-core-comi-06 (work in progress), February 2015.

[IDevID] IEEE Standard, , "IEEE 802.1AR Secure Device Identifier", December 2009, <http://standards.ieee.org/findstds/standard/802.1AR-2009.html>.

[RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, March 2008.

[RFC6345] Duffy, P., Chakrabarti, S., Cragie, R., Ohba, Y., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA) Relay Element", RFC 6345, August 2011.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, July 2012.

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link Format", RFC 6690, August 2012.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

[RFC7250] Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, June 2014.

[RFC7251] McGrew, D., Bailey, D., Campagna, M., and R. Dugal, "AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS", RFC 7251, June 2014.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

[RFC7390] Rahman, A. and E. Dijk, "Group Communication for the Constrained Application Protocol (CoAP)", RFC 7390, October 2014.

[ZigbeeIP]
ZigBee Alliance, , ""ZigBee IP Specification"", .

[ieee802.15.4]
Institute of Electrical and Electronics Engineers, , "IEEE Standard 802.15.4-2006", 2006.

Authors' Addresses

Sandeep S. Kumar
Philips Research
High Tech Campus 34
Eindhoven 5656 AE
NL

Email: ietf.author@sandeep-kumar.org

Peter van der Stok
Consultant

Email: consultancy@vanderstok.org