CoRE Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 15, 2017

M. Tiloca
SICS Swedish ICT
G. Selander
F. Palombini
Ericsson AB

October 12, 2016

Secure group communication for CoAP
draft-tiloca-core-multicast-oscoap-00

Abstract

This document describes a method for application layer protection of messages exchanged with the Constrained Application Protocol (CoAP) in a group communication context. The proposed approach relies on Object Security of CoAP (OSCOAP) and the CBOR Object Signing and Encryption (COSE) format. All security requirements fulfilled by OSCOAP are maintained for multicast CoAP request messages and related unicast CoAP response messages. Source authentication of all messages exchanged within the group is ensured, by means of digital signatures produced through asymmetric private keys of sender devices and embedded in the protected CoAP messages.

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 April 15, 2017.

Table of Contents

1. Introduction

The Constrained Application Protocol (CoAP) [RFC7252] is a web transfer protocol specifically designed for constrained devices and networks.

[RFC7390] enables group communication for CoAP, addressing use cases where deployed devices benefit from a group communication model for example to limit latencies and improve performance. Use cases include lighting control, integrated building control, software and firmware updates, parameter and configuration updates, commissioning of constrained networks, and emergency broadcasts. [RFC7390] recognizes the importance to introduce a secure mode for CoAP group communication. This specification defines such a mode.

Object Security of CoAP (OSCOAP)[I-D.selander-ace-object-security] describes a security protocol based on the exchange of protected CoAP messages. OSCOAP builds on CBOR Object Signing and Encryption (COSE) [I-D.ietf-cose-msg] and provides end-to-end encryption, integrity, and replay protection across intermediate modes. To this end, a CoAP message is protected by including payload (if any), certain options,

and header fields in a COSE object, which finally replaces the authenticated and encrypted fields in the protected message.

This document describes multicast OSCOAP, providing end-to-end security of CoAP messages exchanged between members of a multicast group. In particular, the described approach defines how OSCOAP should be used in a group communication context, while fulfilling the same security requirements. That is, end-to-end security is assured for multicast CoAP requests sent by broadcaster nodes to the group and for related unicast CoAP responses sent as reply by multiple listener nodes. Multicast OSCOAP provides source authentication of all CoAP messages exchanged within the group, by means of digital signatures produced through asymmetric private keys of sender devices and embedded in the protected CoAP messages. As in OSCOAP, it is still possible to simultaneously rely on DTLS to protect hop-by-hop communication between a broadcaster node and a proxy (and vice versa), and between a proxy and a listener node (and vice versa).

1.1. 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]. These words may also appear in this document in lowercase, absent their normative meanings.

Readers are expected to be familiar with the terms and concepts described in [RFC7252], [RFC7390] and [RFC7641].

Terminology for constrained environments, such as "constrained device", "constrained-node network", is defined in [RFC7228].

Terminology for protection and processing of CoAP messages through OSCOAP, such as "Security Context", "Base Key", "Transaction Identifier", is defined in [I-D.selander-ace-object-security].

This document refers also to the following terminology.

- Keying material: data that is necessary to establish and maintain secure communication among member of a multicast group. This includes, for instance, keys, key pairs, and IVs [RFC4949].

- Group Controller (GC): entity responsible for creating a multicast group, establishing and provisioning security contexts among authorized group members, and managing the joining of new group members. This entity may also be responsible for renewing/ updating security contexts and related keying material. The GC is

not required to be an actual member of the multicast group and to take part in the group communication.

- Broadcaster: member of a multicast group that sends multicast CoAP messagges intended to all members of the group. In a 1-to-N multicast group, only a single broadcaster transmits data to the group; in an M-to-N multicast group (where M and N do not necessarily have the same value), M group members are broadcasters.

- Listener: member of a multicast group that receives multicast CoAP messages when listening to the multicast IPv6 address associated to the multicast group. A listener MAY reply back, by sending a unicast response message to the broadcaster which has sent the multicast message.

- Group request: multicast CoAP request message sent by a broadcaster in the group to all listeners in the group through multicast IPv6.

- Group response: unicast CoAP response message sent back by a listener in the group as a response to a group request received from a broadcaster.

- Source authentication: evidence that a received message in the group originated from a specifically identified group member. This also provides assurances that the message was not tampered with by any other group member or an adversary outside the group.

2. Use cases

Group Communication for CoAP [RFC7390] provides the necessary background for multicast-based CoAP communication, with particular reference to low-power and lossy networks (LLNs) and resource constrained environments. The interested reader is encouraged to first read [RFC7390] to understand the non-security related details. This section lists a number of possible use cases that benefit from secure group communication. Specific security requirements for these use cases are discussed later in Section 3.

- Lighting control: consider a building equipped with 6LoWPAN [RFC4944][RFC6282] IP-connected lighting devices, switches, and 6LoWPAN border routers. The devices are organized into groups according to their physical location in the building. For instance, lighting devices and switches in a room or corridor can be configured as members of a single multicast group. Switches are then used to control the lighting devices, by sending on/off/dimming commands to all lighting devices in a group. 6LoWPAN

border routers that are connected to an IPv6 network backbone (which is also multicast-enabled) are used to interconnect 6LoWPAN routers in the building. Consequently, this would also enable logical multicast groups to be formed even if devices in the lighting group may be physically in different subnets (e.g. on wired and wireless networks). Group communication enables synchronous operation of a group of 6LoWPAN connected lights, ensuring that the light preset (e.g. dimming level or color) of a large group of luminaires are changed at the same perceived time. This is especially useful for providing a visual synchronicity of light effects to the user. Devices may reply back to the switches that issue on/off/dimming commands, in order to report about the execution of the requested operation (e.g. OK, failure, error) and their current operational status.

- Integrated building control: enabling Building Automation and Control Systems (BACSs) to control multiple heating, ventilation and air-conditioning units to pre-defined presets. Controlled units can be organized into multicast groups in order to reflect their physical position in the building, e.g. devices in the same room can be configured as members of a single multicast group. Furthermore, controlled units are expected to possibly reply back to the BACS issuing control commands, in order to report about the execution of the requested operation (e.g. OK, failure, error) and their current operational status.

- Software and firmware updates: software and firmware updates often comprise quite a large amount of data. Therefore, it can overload a LLN that is otherwise typically used to deal with only small amounts of data, on an infrequent base. Rather than sending software and firmware updates as unicast messages to each individual device, multicasting such updated data to a larger group of devices at once displays a number of benefits. For instance, it can significantly reduce the network load and decrease the overall time latency for propagating this data to all devices. Even if the complete whole update process itself is secured, securing the individual messages is important, in case updates consist of relatively large amounts of data. In fact, checking individual received data piecemeal for tampering avoids that devices store large amounts of partially corrupted data and that they detect tampering hereof only after all data has been received. Devices receiving software and firmware updates are expected to possibly reply back, in order to provide a feedback about the execution of the update operation (e.g. OK, failure, error) and their current operational status.

- Parameter and configuration update: by means of multicast communication, it is possible to update the settings of a group of

similar devices, both simultaneously and efficiently. Possible parameters are related, for instance, to network load management or network access controls. Devices receiving parameter and configuration updates are expected to possibly reply back, to provide a feedback about the execution of the update operation (e.g. OK, failure, error) and their current operational status.

- Commissioning of LLNs systems: a commissioning device is responsible for querying all devices in the local network or a selected subset of them, in order to discover their presence, and be aware of their capabilities, default configuration, and operating conditions. Queried devices displaying similarities in their capabilities and features, or sharing a common physical location can be configured as members of a single multicast group. Queried devices are expected to reply back to the commissioning device, in order to notify their presence, and provide the requested information and their current operational status.

- Emergency broadcast: a particular emergency related information (e.g. natural disaster) is generated and broadcast by an emergency notifier, and relayed to multiple devices. The latters may reply back to the emergency notifier, in order to provide their feedback and local information related to the ongoing emergency.

3. Requirements

The following security requirements are out of the scope of this document and are assumed to be already fulfilled.

- Establishment of a security context: a secure mechanism must be used to distribute keying material, multicast security policies and security parameters to members of a multicast group. A security context must be established among the group members by the Group Controller which manages the multicast group. A 6LoWPAN border router, a device in the 6LoWPAN network, or a remote server outside the 6LoWPAN network, could play the role of the Group Controller. The actual establishment of the security context is out of the scope of this document, and it is anticipated that an activity in IETF dedicated to the design of a generic key management scheme for the LLN will include this feature preferably based on [RFC3740][RFC4046][RFC4535].

- Multicast data security ciphersuite: all group members MUST agree on a ciphersuite to provide authenticity, integrity and confidentiality of messages in the multicast group. The ciphersuite is specified as part of the security context.

- Backward security: a new device joining the multicast group should not have access to any old security contexts used before its joining. This ensures that a new group member is not able to decrypt confidential data sent before it has joined the group. The adopted key management scheme should ensure that the security context is updated to ensure backward confidentiality. The actual mechanism to update the security context and renew the group keying material upon a group member's joining has to be defined as part of the group key management scheme.

- Forward security: entities that leave the multicast group should not have access to any future security contexts or message exchanged within the group after their leaving. This ensures that a former group member is not able to decrypt confidential data sent within the group anymore. Also, it ensures that a former member is not able to send encrypted and/or integrity protected messages to the group anymore. The actual mechanism to update the security context and renew the group keying material upon a group member's leaving has to be defined as part of the group key management scheme.

The following security requirements need to be fulfilled by the approach described in this document:

- Multicast communication topology: this document considers both 1-to-N (one broadcaster and multiple listeners) and M-to-N (multiple broadcasters and multiple listeners) communication topologies. The 1-to-N communication topology is the simplest group communication scenario that would serve the needs of a typical LLN. For instance, in the lighting control use case, switches are the only entities responsible for sending commands to a group of lighting devices. In more advanced lighting control use cases, a M-to-N communication topology would be required, for instance in case multiple sensors (presence or day-light) are responsible to trigger events to a group of lighting devices.

- Multicast group size: security solutions for group communication SHOULD be able to adequately support different, possibly large, group sizes. Group size is the combination of the number of broadcasters and listeners in a multicast group, with possible overlap (i.e. a broadcaster MAY also be a listener at the same time). In the use cases mentioned in this document, the number of broadcasters (normally the controlling devices) is expected to be much smaller than the number of listeners (i.e. the controlled devices). A security solution for group communication that supports 1 to 50 broadcasters would be able to properly cover the group sizes required for most use cases that are relevant for this document. The total number of group members is expected to be in

the range of 2 to 100 devices. Groups larger than that SHOULD be divided into smaller independent multicast groups, e.g. by grouping lights in a building on a per floor basis.

- Data replay protection: it MUST NOT be possible to replay a group request message or a group response message, which would disrupt the correct communication in the group and the activity of group members.

- Group-level data confidentiality: messages sent within the multicast group SHALL be encrypted. In fact, some control commands and/or associated responses could pose unforeseen security and privacy risks to the system users, when sent as plaintext. In particular, data confidentiality MAY be required if privacy sensitive data is exchanged in the group. This document considers group-level data confidentiality since messages are encrypted at a group level, i.e. in such a way that they can be decrypted by any member of the multicast group, but not by an external adversary or other external entities.

- Source authentication: messages sent within the multicast group SHALL be authenticated. That is, it is essential to ensure that a message is originated by a member of the group in the first place (group authentication), and in particular by a specific member of the group (source authentication). The approach proposed in this document provides both group authentication and source authentication, both for group requests originated by broadcasters and group responses originated by listeners. In order to provide source authentication, outgoing messages are signed by the respective originator group member by means of its own asymmetric private key. The resulting signature is included in the COSE object.

- Message integrity: messages sent within the multicast group SHOULD be integrity protected. That is, it is essential to ensure that a message has not been tampered with by an external adversary or other external entities which are not group members. Message integrity is provided through the same means used to provide source authentication.

4. Scope description

An endpoint joins a multicast group by explicitly interacting with the responsible Group Manager. An endpoint registered as member of a group can behave as a broadcaster and/or as a listener. As a broadcaster, it can transmit multicast request messages to the group. As a listener, it receives multicast request messages from any broadcaster in the group, and possibly replies by transmitting

unicast response messages. Upon joining the group, endpoints are not required to know how many and what endpoints are active in the same group.

An endpoint which is registered as member of a group is identified by an endpoint ID, which is not necessarily related to any protocol-relevant identifiers, such as IP addresses. The Group Manager generates and manages endpoint IDs in order to ensure their uniqueness within a same multicast group. That is, there cannot be multiple endpoints that belong to the same group and are associated to a same endpoint ID.

In order to participate in the secure group communication, an endpoint needs to maintain additional pieces of information, stored in its own security context. Those include keying material used to protect and verify group messages, as well as the public keys of other endpoints in the groups, in order to verify digital signatures of secure messages and ensure their source authenticity. These pieces of information are provided by the Group Manager through out-of-band means or other pre-established secure channels. Further details about establishment, revocation and renewal of the security context and keying material is out of the scope of this document.

According to [RFC7390], any possible proxy entity is supposed to know about the broadcasters in the group and to not perform aggregation of response messages. Also, every broadcaster expects and is able to handle multiple unicast response messages associated to a same multicast request message.

5. Security context

To support multicast communication secured with OSCOAP, each endpoint registered as member of a multicast group maintains a security context as defined in Section 3 of [I-D.selander-ace-object-security]. In particular, each endpoint in a group stores:

1. one Common Context, received upon joining the multicast group and shared by all the endpoints in the group. The Common Context contains the Context Identifier, the COSE AEAD algorithm and the Base Key used to derive endpoint-based keying material (Section 3.2 of [I-D.selander-ace-object-security]);

2. one Sender Context, used to secure outgoing messages. In particular, the Sender Context is initialized according to Section 3 of [I-D.selander-ace-object-security], once the endpoint has joined the multicast group. Besides, in addition to what defined in [I-D.selander-ace-object-security], the Sender

Context stores also the endpoint's asymmetric public-private key pair;

3. one Recipient Context for each different endpoint from which messages are received, used to process such incoming secure messages. The endpoint creates a new Recipient Context upon receiving an incoming message from another endpoint in the group for the first time. Besides, in addition to what defined in [I-D.selander-ace-object-security], each Recipient Context stores also the public key of the associated other endpoint from which secure messages are received.

The Sender Key/IV stored in the Sender Context and the Recipient Keys/IVs stored in the Recipient Contexts are derived according to the same scheme defined in Section 3.2 of [I-D.selander-ace-object-security].

6. Message exchange

Each multicast/unicast message is protected and processed as described in [I-D.selander-ace-object-security], with the following modification: the Sender ID of the endpoint transmitting the message MUST be sent explicitely. That is, the Sender ID MUST be included in the header of the COSE object, as defined in Section 5 of [I-D.selander-ace-object-security]).

The processing for securing multicast request messages and unicast response messages with OSCOAP is the same as in non-multicast communication, with the following two modifications.

1. Upon receiving a secure CoAP message, the recipient endpoint retrieves the Sender ID from the header of the COSE object. Then, the Sender ID is used to retrieve the correct Recipient Context associated to the sender endpoint and used to process the received message. When receiving a secure CoAP message from that sender endpoint for the first time, the recipient node creates a new Recipient Context, initializes it according to Section 3 of [I-D.selander-ace-object-security], and includes the sender endpoint's public key.

2. Before transmitting a secure CoAP message, the sender endpoint uses its own private key to create a counter signature of the COSE_Encrypt0 object (Appendix C.4 of [I-D.ietf-cose-msg]). Then, the counter signature is included in the Header of the COSE object in its "unprotected" field. The recipient endpoint retrieves the corresponding public key of the sender endpoint from the associated Recipient Context and uses it to verify the

counter signature, before proceeding with the verification and decryption of the secure message.

The mapping between unicast response messages from listener endpoints and the associated multicast request message from a broadcaster endpoint relies on the same principle adopted in [I-D.selander-ace-object-security]. That is, it is based on the Transaction Identifier (Tid) associated to the secure multicast request message, which is considered by listener endpoints as part of the Additional Authenticated Data when protecting their own response message.

7. Security considerations

Specific security aspects to be taken into account are discussded below.

7.1. Group-level security

The approach described in this document relies on commonly shared group keying material to protect communication within a multicast group. This requires that all group members are trusted, i.e. they do not forward the content of group messages to entities that are not registered as members of the group. However, in many use cases, the devices in the multicast group belong to a common authority and are configured by a commissioner. For instance, in a professional lighting scenario, the roles of broadcaster and listener are configured by the lighting commissioner, and devices strictly follow those roles.

Furthermore, the presented approach SHOULD take into consideration the risk of compromise of group members. Such a risk is reduced when multicast groups are deployed in physically secured locations, like lighting inside office buildings. The adoption of key management schemes for secure revocation and renewal of security contexts group keying material SHOULD be considered.

7.2. Late joining endpoints

Upon joining the multicast group when the system is fully operative, listeners are not aware of the current sequence number values used by different broadcasters to transmit multicast request messages. This means that, when such listeners receive a secure multicast message from a broadcaster, they are not able to verify if that message is fresh and has not been replayed.

In order to address this issue, upon receiving a multicast message from a particular broadcaster for the first time, late joining

listeners can initialize their last-seen sequence number in their Recipient Context associated to that broadcaster. However, after that they drop the message, without delivering it to the application layer. This provides a reference point to identify if future multicast messages from the same broadcaster are fresher than the last one seen. As an alternative, a late joining listener can directly contact the broadcaster, and explicitly request a confirmation of the sequence number in the first received multicast message.

A possible different approach considers the GC as an additional listener in the multicast group. Then, the GC can maintain the sequence number values of each broadcaster in the group. When late joiners send a request to the GC to join the group, the GC can provide them with the list of sequence number values to be stored in the Recipient Contexts associated to the appropriate broadcasters.

7.3. Provisioning of public keys

Upon receiving a secure CoAP message, a recipient endpoint relies on the sender endpoint's public key, in order to verify the counter signature conveyed in the COSE Object.

If not already stored in the Recipient Context associated to the sender endpoint, the recipient endpoint retrieves the public key from a trusted key repository. In such a case, the correct binding between the sender endpoint and the retrieved public key MUST be assured, for instance by means of public key certificates. Further details about how this requirement can be fulfilled are out of the scope of this document.

Alternatively, the Group Manager can be configured to store public keys of group members and provide them upon request. In such a case, upon joining a multicast group, an endpoint provides the Group Manager with its own public key, by means of the same secure channel used to carry out the join procedure. After that, the Group Manager MUST perform a proof-of-possession challenge-response with the joining endpoint, in order to verify that it actually owns the associated private key. In case of success, the Group Manager stores the received public key as associated to the joining endpoint and its endpoint ID. From then on, that public key will be available for secure and trusted delivery to other endpoints in the multicast group.

Note that in simple, less dynamic, multicast groups, it can be convenient for the Group Manager to provide an endpoint upon its joining with the public keys associated to all endpoints currently present in the group.

8. IANA Considerations

This document has no actions for IANA.

9. References

9.1. Normative References

[I-D.ietf-cose-msg]
Schaad, J., "CBOR Object Signing and Encryption (COSE)", draft-ietf-cose-msg-20 (work in progress), October 2016.

[I-D.selander-ace-object-security]
Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security of CoAP (OSCOAP)", draft-selander-ace-object-security-06 (work in progress), October 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <http://www.rfc-editor.org/info/rfc7252>.

[RFC7641] Hartke, K., "Observing Resources in the Constrained Application Protocol (CoAP)", RFC 7641, DOI 10.17487/RFC7641, September 2015, <http://www.rfc-editor.org/info/rfc7641>.

9.2. Informative References

[RFC3740] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, DOI 10.17487/RFC3740, March 2004, <http://www.rfc-editor.org/info/rfc3740>.

[RFC4046] Baugher, M., Canetti, R., Dondeti, L., and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture", RFC 4046, DOI 10.17487/RFC4046, April 2005, <http://www.rfc-editor.org/info/rfc4046>.

[RFC4535] Harney, H., Meth, U., Colegrove, A., and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol", RFC 4535, DOI 10.17487/RFC4535, June 2006, <http://www.rfc-editor.org/info/rfc4535>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <http://www.rfc-editor.org/info/rfc6282>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <http://www.rfc-editor.org/info/rfc7228>.

[RFC7390] Rahman, A., Ed. and E. Dijk, Ed., "Group Communication for the Constrained Application Protocol (CoAP)", RFC 7390, DOI 10.17487/RFC7390, October 2014, <http://www.rfc-editor.org/info/rfc7390>.

Authors' Addresses

Marco Tiloca
SICS Swedish ICT
Isafjordsgatan 22
Kista SE-16440 Stockholm
Sweden

Email: marco@sics.se

Goeran Selander
Ericsson AB
Farogatan 6
Kista SE-16480 Stockholm
Sweden

Email: goran.selander@ericsson.com

Francesca Palombini
Ericsson AB
Farogatan 6
Kista SE-16480 Stockholm
Sweden

Email: francesca.palombini@ericsson.com