Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 4, 2016

A. Biggs
S. Cooley
Cisco Systems
July 03, 2015

Primitives for Confidential Group Communications
draft-abiggs-saag-primitives-for-confidential-groups-00

Abstract

Insert pithy abstract here.

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 January 4, 2016.

Table of Contents

1. Introduction

This specification defines application agnostic primitives for use in establishing authorization and end-to-end confidentiality in multiparty communications. These primitives address three essential elements of secure group communications:

- Authentication
- Group Membership
- Secure Key Exchange

Authentication is based on the identification of interoperating entities by acct URI and proof of possession of the private counterpart of a public key discoverable through a key discovery service [I-D.miller-saag-key-discovery] available from a well-known URL.

Authorization is based on the group membership classification of authenticated entities, as represented in the form of a Group Membership Block Chain (GMBC) structure defined by this specification. Critical properties of the GMBC are tamper-resistance, efficient mutability, deployability, and suitability for decentralized management.

The secure exchange of keys is based on existing key wrapping standards which allow for secure multicast of key material to authenticated recipients. This strategy builds on the GMBC based

authorization model by taking advantage of reliable group membership classification when addressing wrapped keys to other members.

This specification takes particular care to define these primitives in such a way as they may be suitable for both centralized and decentralized deployment patterns. It is also a goal of this document to describe these primitives in terms of accepted and modern standards in cryptographic technology and infrastructure.

A non-goal of this specification is to define the means by which these primitives are exchanged among interoperating entities involved in group communications. Rather these are building blocks for extending group confidentiality to both new and existing communications and content sharing protocols. With that in mind, however, this specification does advance the notion of recognizing two general classes of deployment for these primitives: "moderated" and "unmoderated".

Another non-goal of this specification is the authentication of sender identity for encrypted data exchanged over a confidential group communications resource supported by the primitives described here. Care is taken to ensure that only authenticated members of a group may decipher secured communications, however the means by which group members may reliably identify the sender of some communications data is out of scope for this specification.

1.1. Terminology

entity

An entity is a user or automated agent that is uniquely identifiable by an acct URI [RFC7565] and for which there exists a key discovery service [I-D.miller-saag-key-discovery] through which public keys may be obtained for that URI.

group

A group is a set of entities whose membership wish to engage in secure and authenticated multiparty communications over some group communications resource.

group communications resource

A group communications resource is any uniquely identifiable streamed or discrete data path that represents an exchange of personal communications between two or more entities.

group membership block chain (GMBC)

A group membership block chain is a primitive defined by this specification for the purpose of providing an effective means for defining, updating, sharing, and verifying the membership of a group.

group key (GK)

A group key is an encrypted object containing symmetric key material and associated metadata secured by the public key(s) of other group members.

This document uses the terminology from [RFC7515], [RFC7516], [RFC7517], and [RFC7518] when discussing JOSE technologies. Most security-related terms in this document are to be understood in the sense defined in [RFC4949].

1.2. Notational Conventions

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Overview

2.1. Authentication by Public Key Discovery

In the context of this specification, entity authentication is defined as the demonstration of possession of the private component of an asymmetric key pair. Specifically, an entity uniquely identified by an acct URI [RFC7565] may be authenticated by demonstrating possession of the private counterpart of one or more public keys as may be discovered using that acct URI and the mechanisms described in [I-D.miller-saag-key-discovery].

2.2. Authorization by Group Membership Block Chain

In the context of this specification, authorization is defined as the classification of any given entity as either a "member" or "non-member" with respect to the group. A member of the group is by definition authorized to receive keying material used to encrypt group communications, and likewise a non-member is not. A member may also be endowed with privileges to alter the membership of the group. The means by which group membership classification established, updated, and validated is through operations on a Group Membership Block Chain (GMBC).

A GMBC is an ordered list of data blocks representing a tamper-resistent chronological account of group membership updates. The first block in the GMBC defines the initial set of group members and each subsequent block represents an addition/removal of one or more other entities to/from the group.

Each block consists of a JSON object signed (as a JWS [RFC7515]) with the private key of the entity that created that block within the chain. That JSON object includes attributes representing the following:

- the acct URI [RFC7565] of the entity that created the block,
- an array of group membership update operations, and
- a hash of the preceding block in the membership chain (if any).

A group membership update operation is a JSON object with two fields:

- a tag indicating the operation type ("add" or "remove"), and
- the acct URI of the entity being either added to or removed from the group.

In addition to the above attributes, the first block of the chain, referred to here as the genesis block, also includes the following attributes:

- a URI that uniquely identifies the group communications resource,
- the acct URI [RFC7565] of the group moderator (optional), and
- a nonce.

The genesis block must also include at least one "add" operation, though it need not necessarily represent the addition of the entity that created it (i.e. entities may create new groups within which they are not themselves members).

The membership of the group is implicit and may be determined by processing the GMBC in chronological order. At any given point in time the membership of the group is defined as that set of entities for each of which there exists a block containing an "add" operation and for which there does not exist a subsequent block containing a "remove" operation.

To protect against unauthorized tampering the GMBC is validated by verifying the signatures of each block, verifying that each non-

genesis block contains a valid hash of the preceding block, and verifying that each block is created by an entity that is among the group's membership as determined by the segment of chain preceding that block. Block signature verification is made possible through the knowledge of each member's acct URI and through the employment of key discovery mechanisms defined in [I-D.miller-saag-key-discovery].

2.3. Key Distribution by Group Keys

A Group Key (GK) is composed of a symmetric encryption key with associated metadata that has been created for the purpose of encrypting confidential communications intended for the exclusive consumption by group members. This exclusivity of access to the key material is secured by defining the GK as the encryption of this symmetric key and metadata using the public entity key(s) of the other group members.

More specifically, the cleartext content of a group key is a JSON object including attributes representing the following:

- a URI that uniquely identifies the group key,
- the acct URI [RFC7565] of the entity that created the group key,
- a hash of the genesis node of the GMBC to which the key belongs,
- a JWK [RFC7517] that represents the symmetric key material, and
- a timestamp indicating a time beyond which the key should not be used for encryption.

This JSON object is encrypted in a JWE [RFC7516] JSON serialization with one or more recipients. In unmoderated groups the resulting JSON serialization must include each other member of the group as determined by the most recently available and validated GMBC. In moderated groups the resulting JSON serialization need only include the moderator as the recipient.

Group keys may be created by members and non-members alike. A non-member may generate a group key as described above and use it to encrypt its own communications to the group. This can be a useful property as it provides for "write only" capability to the confidential channel. Note that the authentication of origin of encrypted data shared over the group communications resource is expressly out of scope for this specification.

A group may have any number of group keys associated with it. Each member of a group must use its own group key for purposes of

encryption and shares this group key with the remainder of the group for purposes of decryption. A member must not re-use a group key created by another entity, as that other entity may not itself be a member (as mentioned above).

It is recommended that all entities that share encrypted content over the group communications resource rotate their group keys regularly so as to mitigate against vulnerabilities that are exacerbated by the extended use of individual keys.

3. Deployment Patterns

The preceding sections describe structural primitives for authenticating and authorizing entities by virtue of their group membership as defined by a GMBC, and for the exclusive sharing of encryption key material among members through an associated set of GKs. While these provide the building blocks for establishing confidential group communications, the means by which these objects are exchanged among members has not been discussed and is generally regarded as out of scope for this specification. With that said, it remains worthwhile to discuss two general patterns of deployment and to describe their practical structure. These patterns may be described as "moderated groups" and "unmoderated groups".

3.1. Unmoderated

An unmoderated group is characterized by the absence of a moderator attribute in the GMBC genesis block and therefore the absence of a privileged member within the group through which GMBC and GK objects may be brokered. In an unmoderated group these objects may instead be exchanged through the group communications resource either in-band with these communications themselves or through in-band references to external repositories. Both the GMBC and GK objects are designed to be hardened against tampering and exposure of sensitive data, and as such may be reasonably exchange through either public or private channels.

3.2. Moderated

A moderated group is characterized by the presence of a moderator attribute in the GMBC genesis block. The entity represented by the acct URI [RFC7565] given in the moderator attribute is regarded as a member and furthermore cannot be removed from the group.

The moderator serves as a facilitator for the exchange of GMBC and GK objects. In particular it supports the following interactions with other members of the group:

- a moderator will accept new GMBC blocks from other members
- a moderator will accept requests for GMBC updates from other members
- a moderator will accept new GKs from other members
- a moderator will accept requests for GKs from other members

The protocol through which a moderator services these requests is out of scope for this specification.

4. Mandatory-to-Implement

5. Security Considerations

6. Appendix A. Acknowledgments

7. Appendix B. Document History

-00

- Initial draft.

8. Normative References

[I-D.miller-saag-key-discovery] Miller, M. and S. Nandakumar, "Key Discovery Service", draft-miller-saag-key-discovery-00 (work in progress), July 2015.

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

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, May 2015.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, May 2015.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, May 2015.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, May 2015.

[RFC7565] Saint-Andre, P., "The 'acct' URI Scheme", RFC 7565, May 2015.

Authors' Addresses

Andrew Biggs
Cisco Systems

Email: adb@cisco.com

Shaun Cooley
Cisco Systems

Email: shcooley@cisco.com