MLS

Raphael Robert, Britta Hale, Richard Barnes, Konrad Kohbrok, Rohan Mahy, Anh Pham, Marta Mularczyk, Joel Alwen

IETF 121, Dublin

Agenda

- Overview of drafts
- Changes in mls-extensions
- Discussion about mechanics of extensions
- Additional wire formats (draft-pham-mls-additional-wire-formats)

Overview of current drafts

- draft-hale-mls-combiner
- draft-mahy-mls-xwing
- draft-barnes-mls-appsync
- draft-kohbrok-mls-associated-parties
- draft-mahy-mls-semiprivatemessage
- draft-kiefer-mls-light
- draft-mularczyk-mls-splitcommit
- draft-pham-mls-additional-wire-formats

Overview of other drafts

- Paired MLS - PCS in Limited Modes
  draft-fondevik-mls-pairedmls
  Status: on hold because of virtual clients
- A membership proof extensions for the Messaging Layer Security (MLS) Protocol
  draft-mahy-mls-member-proof
  Status: retracted

Changes in mls-extensions

draft-05

- Include definition of ExtensionState extension
- Add safe use of AAD to Safe Extensions framework
- Clarify how capabilities negotiation works in Safe Extensions framework

WIP

- PR: Additional credentials
- PR: Group context extension encryption
- Issues: Either editorial or minor mechanical changes

Discussion about mechanics of exts

- The word “extension” is overloaded
- The MLS protocol is extensible in predefined ways
- We have a Safe Extension Framework
- Capability negotiation is not complete (i.e. wire formats)
- It’s an ongoing discussion that will likely be continued at an interim meeting

draft-pham-mls-additional-wire-formats

Additional wire formats

Status quo:

- Both PrivateMessgae & PublicMessage have an AAD field
- AAD = additional authenticated data
- That data is always sent in plaintext
- There is no way to directly authenticate data that is not part of a message

Additional wire formats

Main idea:

- “BYOAAD” = bring your own AAD
- Redefine both PrivateMessage & PublicMessage
- Drop the AAD, but keep all other fields
- The application provides the AAD when incoming messages are processed

Additional wire formats

Alternatives considered:

- Define a safe extension that puts a hash in the current AAD.
  Downside: Unnecessary payload is transmitted.
- Use GCE.
  Downside: Not fine-grained, only covers Commits.

Additional wire formats

Open questions:

- Should this replace existing MLS messages (both private & public) or be used alongside them?