MIMI Features with Less Metadata

Comparison: Metadata protection

Baseline

- leaks group id
- leaks epoch
- leaks identity of group members
- leaks identity of senders
- leaks group operations

MIMIMI

- leaks group id
- leaks epoch
- only leaks per-group pseudonyms of members
- only leaks per-group pseudonym of senders
- only leaks pseudonymized group operations

Encrypted HS Messages

- leaks group id
- leaks epoch

Metadata Taxonomy

1. Hub and followers can see everything (baseline)
2. User identities are hidden using per-group pseudonyms (MIMIMI)
3. Same as 2., but messages are encrypted to Hub and group members (MIMIMI + SemiPrivateMessages)
4. Everything but group id and epoch is hidden from Hub and followers (Encrypted HS messages)

Comparison: Functionality

Baseline

- allows both push and pull architectures
- allows server-assisted external join
- allows policy enforcement on Hub

MIMIMI

- allows both push and pull architectures
- allows server-assisted external join (with caveat)
- partially allows policy enforcement on Hub

Encrypted HS Messages

- requires pull architecture
- no server-assisted external join
- no policy enforcement on Hub

Metadata protection comparison

DMA Gatekeeper features

Features taken from [1].

- **Direct invites:** Specific, named users can invite other users
- **Invite codes:** Users can create a code that allows arbitrary users to join
- **3rd party invites:** Users can invite (unnamed) users of another platform to a group
- **Ban:** Users can ban other users s.t. affected users can’t rejoin the group
- **Kick:** Users can kick other users out of a group

[1]: https://docs.google.com/spreadsheets/d/1FiR4yhU5BpLtoeFFda5ORr86qwT33fYZowY_bWDlPas/edit?usp=sharing

DMA Gatekeeper features

Features taken from [1].

- **Limit who can post/send:** Users can mute other users
- **Edit/delete other users' posts:** Self-explanatory
- **Access control:** General access control (e.g. role based)
- **Auditorium rooms:** Users can see/identify only a subset of other group members
- **Limit who can send what types of messages:** Similar to access control

[1]: https://docs.google.com/spreadsheets/d/1FiR4yhU5BpLtoeFFda5ORr86qwT33fYZowY_bWDlPas/edit?usp=sharing

DMA Gatekeeper features

Feature/Approach	MIMIMI	Encrypted HS Messages
Direct invites		
Invite codes		
3rd party invites		
Kick		
Ban		

DMA Gatekeeper features (cont’d)

Feature/Approach	MIMIMI	Encrypted HS Messages
Limit who can post/send		
Edit/delete other users’ posts		
Access control		
Auditorium rooms		
Limit who can send what type of messages		

MIMIMI (pseudonym-based approach)

- **Direct invites:** No issue
- **Invite codes:** Possible (via external join) if invite code contains key material to de-pseudonymize group members
- **3rd party invites:** Could be made possible by providing the hub with the ability to recognize the new user (not sure I understand the feature correctly)
- **Ban:** Depends on the exact specification of the feature, but hard for the DS to enforce due to the use of (per-group unique) pseudonyms
- **Kick:** No issue

MIMIMI (pseudonym-based approach)

- **Limit who can post/send:** Can be enforced by the hub on a per-pseudonym basis
- **Edit/delete other users' posts:** No issue, because mostly independent of the hub
- **Any access control:** No issue, roles and privileges can be assigned to pseudonyms
- **Auditorium rooms:** No issue, because mostly independent of the hub
- **Limit who can send what types of messages:** Can be enforced on a per-pseudonym basis

Encrypted HS Messages

- **Direct invites:** No issue
- **Invite codes:** Would require GroupInfo upload with associated metadata leakage
- **3rd party invites:** Same issue as invite codes
- **Ban:** Depends on the exact specification of the feature, but hard for the DS to enforce based on lack of visibility
- **Kick:** No issue

Encrypted HS Messages

- **Limit who can post/send:** Can’t be enforced by the hub
- **Edit/delete other users’ posts:** No issue, because mostly independent of the hub
- **Any access control:** Only relatively coarse enforcement through epoch keys.
- **Auditorium rooms:** No issue, because mostly independent of the hub
- **Limit who can send what types of messages:** No issue

Summary

- Both approaches limit metadata leakage
  - Encrypted HS messages almost completely
  - MIMIMI to a slightly lesser degree
- Both approaches limit Hub capabilities to enforce policy
  - Encrypted HS messages almost completely
  - MIMIMI because real identities aren’t visible
- Both approaches limit the capability to perform server-assisted external joins
  - Encrypted HS message completely
  - MIMIMI because it requires a secret for new joiners to discover the real identities
- Encrypted HS messages additionally restricts message delivery to a pull/subscribe model

What (other) features are important to us?