Metadata Privacy

Proposal: Protection Levels

Metadata such as room policies / participant lists are exposed to...

1. ~~Clients, hub server, and non-hub servers~~ ← unnecessarily over-sharing
2. **Clients and hub server** ← **Baseline**
3. **Clients and hub server (pseudonymously)** ← **Opt-in**
4. ~~Clients~~ ← too much functionality loss

Pseudonyms are an extra layer

MIMI works the same way regardless of what the identifiers identify

The protocol doesn't care whether the identities are real

In the pseudonymous case, you need a little more mechanism to achieve the same results as in the non-pseudonymous case

- How does a user get pseudonyms?
- How does Bob get a per–group pseudonym for Alice to add her?
- How do abuse reports get associated with the abuser's real identity?

Since multiple parties are involved, need a spec and capability negotiation

Proposal: Baseline + Opt-In

In the base protocol document:

- Use SemiPrivateMessage to deny any information to follower servers
- Make sure the protocol is actually agnostic as to pseudonymity
- Provide enough negotiation hooks to allow opt-in to pseudonymity

In a pseudonymity extension document:

- Define the additional machinery to make pseudonyms work

As these docs mature, we can revisit whether to upgrade the baseline