MIMI Room Policy

Rohan Mahy: rohan.iert@gmail.com
IETF 120, 25-July-2024
What is room policy?
Access controls for a room, and properties of a room

- Membership style
  - open
  - members-only
  - fixed-membership (1:1 or Chat DM)
  - parent-dependent

- Types of Roles in the room and their Attributes or Capabilities: Attribute Based Access Control

- Functions required, optional, or forbidden:
  - read receipts/deliver reports
  - history sharing
  - link previews
  - pseudonyms
  - Logging
  - Join links
  - Bot policies
  - MLS Settings
    - Ex: PCS Updates
Strict administrator ABAC policy

Capabilities per role

- **banned**
  - (no capabilities)
- **guest**
  - canSendMessage
  - canReceiveMessage
  - canRemoveSelf
- **ordinary_user**
  - (everything guest can do, plus:)
  - canAddOwnClient
  - canChangeOwnName, Presence, Mood, Avatar
  - canReport
  - canSendLinks
  - canSendImages
  - canSendVideos

- **group_admin**
  - (everything ordinary_user can do, plus:)
  - canSendAttachments
  - canAddParticipant
  - canRemoveParticipant
  - canBanish
  - canUnBanish
  - canKick
  - canChangeRoomName, Subject, Avatar
  - canPromoteRole(from=[ordinary]; to=[group_admin])
  - canDemoteRole([from=[group_admin], to=[ordinary])
  - canDestroyRoom
  - canCreateJoinLink

- **Role levels (low to high capabilities):**
  - **banned**
  - **guest**
  - **ordinary_user**
  - **group_admin**
  - **super_admin**

- **super_admin**
  - (everything group_admin can do, plus:)
  - canPromoteRole(from=[ordinary, group_admin]; to=[super_admin])
  - canDemoteRole(from=[super_admin], to=[ordinary, group_admin])
  - canChangeRoomMembershipStyle

- **Role constraints: must have at least 1 “group_admin”**
Cooperative room ABAC policy

Capabilities per role

• banned
  • (no capabilities)
• ordinary_user
  • canSendMessage
  • canReceiveMessage
  • canRemoveSelf
  • canAddOwnClient
  • canChangeOwnName, Presence, Mood, Avatar
  • canReport
  • canSendLinks
  • canSendImages
  • canSendVideos
  • canSendAttachments
• ordinary_user (continued)
  • canAddParticipant
  • canRemoveParticipant
  • canKick
  • canChangeRoomName, Subject, Avatar
  • canCreateJoinLink
• group_admin
  • (everything ordinary_user can do, plus):
    • canBanish
    • canUnBanish
    • canPromoteRole(from=[ordinary, admin], to=[superadmin])
    • canDemoteRole(from=[superadmin], to=[ordinary, admin])
    • canChangeRoomMembershipStyle
• Role levels (low to high capabilities):
  • banned
  • ordinary_user
  • group_admin
  • super_admin
• super_admin
  • (everything group_admin can do, plus):
    • canPromoteRole(from=[ordinary, admin], to=[superadmin])
    • canDemoteRole(from=[superadmin], to=[ordinary, admin])
    • canChangeRoomMembershipStyle
• Role constraints: must have at least 1 “group_admin”
Moderated room ABAC policy

Capabilities per role

- **banned**
  - (no capabilities)
- **non-participant**
  - canKnock
  - canJoinViaLink
- **guest**
  - canReceiveMessage
  - canRemoveSelf
- **attendee**
  - (everything guest can do, plus:)
  - canAddOwnClient
  - canChangeOwnName, Presence, Mood, Avatar
  - canReport
- **speaker**
  - canSendMessage
  - canChangeRoomName, Subject, Avatar
  - canSendLinks
  - canSendImages
  - canSendVideos
  - canSendAttachments
- **moderator**
  - (everything speaker can do, plus:)
  - canAddParticipant
  - canRemoveParticipant
  - canAcceptKnock
  - canBan
  - canUnBan
  - canKick
  - canPromoteRole(from=[ordinary]; to=[admin])
  - canDemoteRole(from=[admin], to=[ordinary])
  - canCreateJoinLink

• Role levels (low to high capabilities):
  - **banned**
  - **non-participant**
  - **guest**
  - **attendee**
  - **speaker**
  - **moderator**
  - **super_admin**

- **super_admin**
  - (everything group_admin can do, plus:)
  - canDestroyRoom
  - canPromoteRole(from=[ordinary, admin], to=[superadmin])
  - canDemoteRole(from=[superadmin], to=[ordinary, admin])
  - canChangeRoomMembershipStyle

• Role constraints: must have at least 1 "moderator"