Message Recall

draft-leiba-morg-message-recall

Barry Leiba
Huawei Technologies

What & Why

- Proprietary systems often allow users to recall sent messages.
- This is often requested for Internet-standard messages.
- Often.
- Very often.

Why not?

- Lots of complications
  - Authorization across domains
  - What if the recipient has seen it?
  - What about multiple recipients?
    - Recall from *all* or *none*?
    - Recall as best we can?
  - What attacks are possible?
    - From *both* sides

Protocol

- Each message has a “secret code”
- Hash of code included in message
- Recall request includes original code (no longer secret)
- Hash the original for authentication
- Domain policies still apply

Protocol

- Two-stage hold/recall available
  - "hold" is optional
  - Allows "all or none" to be implemented
  - Hold can be rescinded by "release"
  - Timeouts recommended here
- Recalled message MUST NOT be made available to recipient
  - Open to attack by lying

Looking for input/discussion

- Asking the MORG WG to allow discussion there.
- Perhaps have MORG adopt it?
- If not…
  - Another WG (existing or new)?
  - Individual submission? (skeptical)