RFC 3489bis

Jonathan Rosenberg
Cisco

My Apologies

- Work issues prevented me from properly handling this
- -06 is barely different from -05 and has tons of comments left to address, some as old as November 06
- I chose to focus on ICE rather than STUN for what cycles I had for this topic
- Suggest providing a deadline and if it is missed, help is brought in to finish editing
  - 2 weeks

Reviews studied-to-be-integrated

- Magnus Westerlund
- Eric Rescorla
- Marc Petit-Huguenin
- Magnus Westerlund
- Francois Audet

Issues from Mails

- Ekr: Why do we need all three authentication techniques
  - Need to motivate a bit more the rationale
- Ekr: Require hash agility in MESSAGE-INTEGRITY
  - Proposal: document an agility plan. Would define a new attribute with a signaled hash algorithm, require inclusion of this AND message-integrity for some years and then deprecate message-integrity in a revision
- Ekr: short term credential recommended for Binding usage?
  - Yes, as in RFC 3489

Issues from Mails

- Lennox1: Need to define binding indications used in ICE
  - Yes!
- Johns1: How long to remember a response to discard subsequent ones?
  - When you receive a response you discard transaction, if you get a response without a transaction you discard
- Johns2: Lot more normative statements
  - No – clutters it up

Issues from Mails

- Westerlund1: Need to say more on STUN and TCP with framing
  - From sip-outbound decision, we now have a case that all STUN usages with TCP use a shim framing (TURN has one, ICE has another). Should now require that.
- Westerlund2: Need to discuss the redirection attack
  - DDoS
  - Overload someone elses servers
  - Conclusion: these are not significant attacks

Issues from Mails

- Audet1: What is the meaning of a v4 host getting a v5 mapped-address and vice-versa?
  - Case was v6 network natted into v4 and vice-versa
  - In this case a single stack v4 could learn v6 and could use it in an offer or answer in the case of ICE for example
- Matthews1: Uniqueness of transaction ID
  - Randomly generated providing high probabiliyt of global uniqueness