draft-ietf-xmpp-rfc3920bis-05

XMPP WG, IETF 77

Peter Saint-Andre

Overview

- Version at IETF 76 was -03, now at -05
- Clarified several points about XML usage, stream negotiation, and certificate checking
- Open issues regarding (1) mutual auth for s2s streams and (2) i18n addresses
- More reviews still needed!

XML Usage

- Stopped encouraging liberal acceptance of data that is not namespace-well-formed
- Proposed change of SHOULD to MUST:

> - An XMPP server MUST NOT route or deliver data that is not namespace-well-formed, and MUST return a stanza error of <not-acceptable/> or a stream error of <xml-not-well-formed/> in response to the receipt of such data.

Stream Negotiation

- Server SHOULD NOT advertise any stream feature except STARTTLS if TLS is mandatory-to-negotiate
- Server MUST NOT send stream features after stream negotiation is complete (send newly-defined <reset/> stream error instead)

Security Issues (1)

- Recommended improved certificate checking on long-lived streams:
  - Close stream if cert expires
  - Periodically query OCSP responder
- MUST re-auth if cert changes materially between old stream and new stream

Security Issues (2)

- Added reference to `draft-saintandre-tls-server-id-check` for validation of server identity in certificates
- Clarified "simple username" in SASL
  - Default to bare JID or localpart for c2s? (seeming consensus for localpart)

Mutual Auth for s2s (1)

- Spec still requires use of two TCP connections for s2s streams
- This is a legacy of server dialback, but shouldn't be necessary if we have mutual auth (see section 6.3.3.1 of rfc3920bis)
- Can we allow only one TCP connection if mutual auth succeeds?

Mutual Auth for s2s (2)

- Server sends CertificateRequest message
- Peer sends its cert in Certificate message
- If peer cert is acceptable, server offers SASL EXTERNAL
- Peer signals that server cert is acceptable via <auth ... mutual='true'/> during SASL negotiation

Action Items

- Remove hard two-connection rule for s2s
- More completely specify mutual auth
- Make decisions about internationalized JIDs
- Convert XML schema to Relax NG?
- Seek more reviews / interop feedback