draft-ietf-xmpp-rfc3920bis-03

XMPP WG, IETF 76

Peter Saint-Andre

Overview

- Version at IETF 75 was -00
- Material changes limited to stream negotiation and security improvements
- More reviews needed!

Minor Changes (1)

- Changed “node identifier” to “localpart”
- Corrected whitespace keepalive definition
- Added note about potential unreliability
- Clarified where errors are sent for stream and stanza errors
- Clarified when client is allowed to send outbound stanzas

Minor Changes (2)

- Clarified definition of 'id' attribute, including the meaning of "originating entity"
- Rewrote description of architecture
- Clarified definition of "extended content" to explicitly include XML attributes
- Harmonized text about XML declaration with the XML specification

Minor Changes (3)

- After much list discussion, slightly adjusted text about streams namespace and default namespace
- Added unsupported-feature stream error
- Added IPv6 examples
- Defined feature set for conformance purposes

Stream Negotiation (1)

- In previous versions, the stream negotiation process was underspecified
- Introduced some new terms (e.g., "mandatory-to-negotiate")
- More clearly described stream restarts
- Specified when stream negotiation shall be considered complete

Stream Negotiation (2)

- As a result of these clarifications, defined a state chart for stream negotiation
- Discussed but then rejected common child element to specify whether a feature (1) is mandatory-to-negotiate and (2) requires a stream restart
- Described what stream feature definitions need to include

Stream Negotiation (3)

- Open issues
  - Allow receiving entity to send updated stream features at any point in the session?
  - Allow initiating entity to send stream features?

Security Issues (1)

- Harmonized terminology with RFC 4949 (Internet Security Glossary)
- Added or improved text about hash function agility, JID mimicking, and directory harvesting
- Per new IESG policy, prohibited wildcards in the left-most domain label within certs (e.g., foo*.example.com)

Security Issues (2)

- Added SCRAM as mandatory-to-implement ("MTI") to replace DIGEST-MD5, which is being moved to Historic
- TLS + SASL PLAIN is also MTI
- TLS + SASL EXTERNAL is MTI for servers but *not* for clients

Security Issues (3)

- Public Key Certificates for XMPP entities:
  - MUST conform to RFC 5280
  - The entity MUST NOT be a CA
  - Subject field MUST NOT be null
  - Hashing algorithm SHOULD be SHA-256

Security Issues (4)

- Added profile of draft-ietf-pkix-3281update for attribute certificates
- Added profile of RFC 5280 for issuers of public key certs and attribute certs
- Do we need these in 3920bis?

Security Issues (5)

- TLS re-negotiation attack recently disclosed
- Preliminary analysis indicates that XMPP is not vulnerable because the parties to a stream are required to discard the security context and perform a stream restart after TLS negotiation (or re-negotiation)

Open Issues

- Define fast reconnect logic and "pipelining" of stream negotiation process?
- Internationalized addresses
  - IDNA2003 vs. IDNA2008
  - Stringprep for localpart and resourcepart
- Need more reviews!