XTLS: End-to-End Encryption for the Extensible Messaging and Presence Protocol (XMPP) Using Transport Layer Security (TLS)

Dirk Meyer and Peter Saint-Andre

Overview

- Use an existing technology like TLS
- Tunnel TLS data over XMPP Base64 encoded
  - XMPP guarantees message ordering required by TLS
- Exchange XML stanzas similar to C2S and S2S
  - Reliable secure transport between clients tunneled through the existing XMPP infrastructure
  - Similar stanza processing on application level

Jingle Security

- Open a transport between clients with TCP characteristics
  - Jingle is mainly used for RTP traffic right now
  - Similar requirements to file transfer
- Define Jingle application for chatting
- Place a security layer between transport and application
  - XTLS: TLS security layer for Jingle

Authentication

- Should work with self-signed certificates
  - Getting a CA-issued certificate is too complex for the average user
- Use TLS-SRP if certificate based authentication fails
  - Simple passwords, shared secret
  - Exchange password over a different channel
- Certificate management
  - When SRP is used, exchange certificates over the secure link for future communication

Open Issues

- TLS-SRP is not widely deployed
  - Integrated into some Open Source TLS stacks
  - Mobile phones and Microsoft Windows have no SRP support
- Maybe rely on SASL for authentication without certificates
  - Mutual authentication with simple password required
  - Maybe with channel bindings to verify the TLS link set up with unknown certificates
- TLS is only one-to-one
- No offline message support