Requirements for End-to-End Encryption in the Extensible Messaging and Presence Protocol (XMPP)

Peter Saint-Andre

Introduction

- Several attempts for end-to-end secure communication
  - Little to no deployment: OpenPGP, S/MIME, ESessions
  - New approach: TLS

- Scope
  - One-to-one communication sessions (main focus)
  - One-to-one offline messages
  - One-to-many information broadcast
  - Many-to-many communication sessions

Threat Analysis

A client only knows about its connection to the server

- Is the peer connected to its server using TLS?
- Is the server-to-server link secure?
- Can the peer's server be trusted for authentication?
- Can the servers involved be trusted?

- We need end-to-end encryption to protect traffic between clients

Security Requirements

- Confidentiality
- Integrity
- Replay Protection
- Perfect Forward Secrecy
- PKI Independence
- Authentication
- Identity Protection
- Robustness
- Upgradability

Application Requirements

- Generality
- Implementability
- Usability
- Efficiency
- Flexibility
- Offline messages