XMPP BOSH
AppArea Meeting
IETF 74

Jack Moffitt &
Peter Saint-Andre

Design Decisions

- Goal: emulate bidirectional TCP binding
- Constraints: HTTP/1.0, don't force polling (but support it for limited clients), work with proxies/NATs/gateways, consume minimal bandwidth, provide in-order delivery, don't rely on HTTP headers / cookies / status codes

How It Works

- Basic method: client sends HTTP POST with <body/> element + payload, server returns error or 200 OK with <body/> + optional payload
- Typically use 2 request-response pairs at a time (server replies to first request so that one request is outstanding)
- Payloads are XML

Reliability & Security

- Supports pings (empty <body/>) and acks
- Should use HTTPS or HTTP over TLS
- Session-IDs and Request-IDs provide protection against a blind attacker
- Optional key sequencing method protects against passive attacks

Deployment

- Fairly significant deployment on XMPP network, mostly for instant messaging (IM)
- Support in various XMPP servers, standalone connection managers, and web clients
- Some non-IM use (e.g., drop.io)

Open Issues

- Addition of connection manager between client and (XMPP) server introduces new security concerns
- Two models: (1) dedicated connection manager for single domain or (2) proxy to any domain
- Application of single origin policy to BOSH