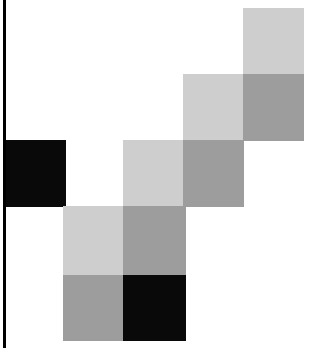


Extensible Messaging and Presence Protocol (XMPP)

Mikko Laukkanen

Contents

Introduction

- Instant messaging (IM) is a service, where communicating parties – typically end-users – send messages in one-to-one or one-to-many fashion in near real-time.
- Presence is a ”state” of the communicating party
- The XMPP (Extensible Messaging and Presence Protocol) is targeted at delivering instant messages and presence information.
- XMPP is an open and XML-based protocol, which has evolved through an open development within the Jabber open-source community
  - Jabber protocol was submitted twice; the second resulted in the creation of XMPP WG

Introduction, cont’d

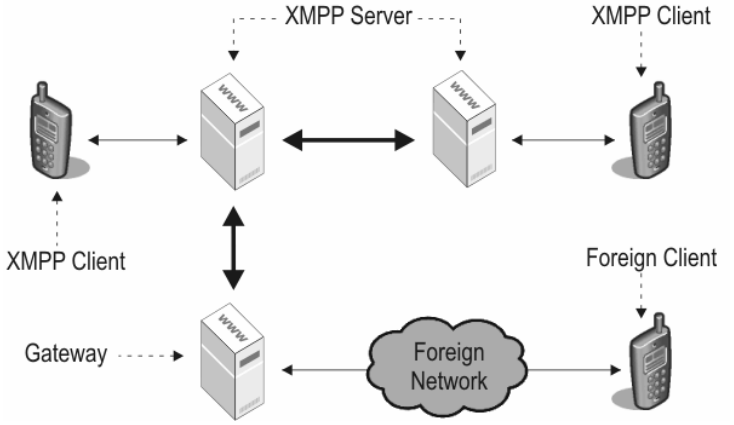
- Within the IETF specification work, the main extensions to the XMPP are
  - Security
  - Authentication
  - Privacy, and
  - Access control
- Other features: localization and internationalization
- XMPP aims at compliance with the RFC2778 and RFC2779

XMPP Internet Drafts and Status of Work

- Internet Drafts
  - XMPP Core
  - XMPP Instant Messaging and Presence
  - Mapping the XMPP to Common Presence and Instant Messaging (CPIM)
  - End-to-End Object Encryption in the XMPP
- Core and IM&Presence approved as proposed standards, but not yet as RFCs
- No progress on XMPP Mapping and E2E Security during the last months

XMPP Core

XMPP Core, Architecture

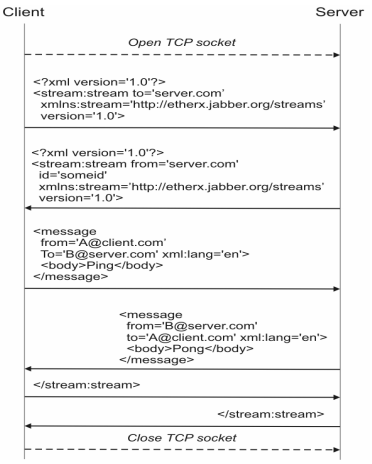


XMPP Core, Addressing

- Addressing
  - JID (Jabber Identifier)
  - Composed of *node*, *domain*, and *resource*
  - Mikko@foo.com/client1, chatroom1@bar.com

XMPP Core, XML Streams

- Instead of delivering separate XML documents on a single connection, a persistent connection is used for delivering the XML data elements



XMPP Core, XML Stanzas

- Message, presence, and IQ
- The message stanza is used a push mechanism from one entity to another
- Presence stanza is the notification part of the basic publish-subscribe mechanism; it is used to deliver information from one entity to multiple recipients
- IQ (Info/Query) is a request-response interaction, with which an entity is able to request some information from another entity

XMPP Instant Messaging and Presence

XMPP Instant Messaging and Presence, IM Stanzas

- Extensions to the XMPP Core in terms of basic instant messaging and presence management
- The message stanza is extended to cover types and elements specific to the instant messaging and presence: *chat, groupchat, headline, normal*, or *error*

XMPP Instant Messaging and Presence, IM Example

```
<message
   to='B@server.com'
   from='A@client.com'
   type='chat'
   xml:lang='en'>
  <subject>Hello user B!</subject>
  <subject xml:lang='fi'>Moi käyttäjä B!</subject>
  <body>Can you send me your picture?</body>
  <body xml:lang='fi'>Lähetä minulle kuvasi?</body>
  <thread>thread-xx-yy</thread>
</message>
```


XMPP Instant Messaging and Presence, Presence Stanzas

- May have one of the following type: *unavailable*, *subscribe*, *subscribed*, *unsubscribe*, *unsubscribed*, *probe*, or *error*
  - Example:

```
<presence to='A@client.com' type='subscribe'/>
<presence to='B@client.com' type='subscribed'/>
```

- Supports the following child elements: *show*, *status*, and *priority*
- The *show*-element is meant for machine processing, whereas the *status* is for human end-users
  - Example:

```
<presence xml:lang='en'>
  <show>dnd</show>
  <status>Having a coffee break</status>
  <status xml:lang='fi'>Kahvitauolla</status>
  <priority>1</priority>
</presence>
```

XMPP Instant Messaging and Presence, IQ Stanzas

- Main usage: subscriptions and roster (contact list) management
- Possible message types: *set, get, result, error*

```
<iq from='A@client.com' type='get' id='r1'>
  <query xmlns='jabber:iq:roster'/>
</iq>

<iq to='A@client.com' type='result' id='r1'>
  <query xmlns='jabber:iq:roster'>
    <item jid='Mikko@foo.com/client1'
          name='Mikko'
          subscription='both'>
      <group>Relatives</group>
    </item>
    <item jid='chatroom1@bar.com'
          name='ChatRoom1'
          subscription='from'>
      <group>ChatRooms</group>
    </item>
  </query>
</iq>
```


XMPP to CPIM Mapping

- IMPP WG specified an abstract interoperable framework for instant messaging called Common Presence and Instant Messaging (CPIM)
- To be interoperable with each other, the different IM and presence specifications, such as XMPP, may define mappings to the CPIM
- For XMPP, these mappings are specified in Mapping the XMPP to Common Presence and Instant Messaging (CPIM) Interned Draft
- The CPIM mapping is also used in E2E signing and encryption

XMPP to CPIM Mapping, Example

- XMPP XML stanza:

```
<message from='A@client.com' to='B@server.com'>
  <subject>Hi!</subject>
  <subject xml:lang='fi'>Moi!</subject>
  <body>Hello World!</body>
</message>
```

- CPIM MIME headers and content:

```
Content-type: text/plain; charset=utf-8
Content-ID: <xyz@client.com>
From: A <im:A@client.com>
To: B <im:B@server.com>
Subject: Hi!
Subject:;lang=fi Moi!

Hello World!
```


SASL and TLS in XMPP

- Simple Authentication and Security Layer (SASL) for authentication (RFC2222)
- Transport Layer Security (TLS) for secure channels (RFC2246)
- General steps in TLS/SASL negotiation
  1. XML streams are opened and TLS is negotiated
  2. A new stream is opened, and SASL is negotiated
  3. Assuming both steps are successful, a new stream is opened for the application-domain specific communications

Related Technologies

- Jabber
  - Differencies in encryption, authentication, error handling, internationalization, session establishment, and privacy
  - Implementations (based on Jabber) are or will be XMPP Core / IM&Presence compliant
- SIMPLE
  - Differencies in architecture
  - Requires more bandwidth than XMPP; however, this may vary based on the implementations...
- Commercial products
  - AIM, ICQ, MSN Messenger, Yahoo IM
  - Gateways are possible, but may not be practically easy to implement
- Possible interoperability by using mappings to common specifications and/or using gateways between different technologies

Discussion and Future

- XMPP and mobile (wireless) environments?
  - XMPP suits well for (slow) wireless environments in terms of using persistent TCP connections
  - Extra optimization by using (compressed) binary XML?
- XMPP does not suffer from the problems of NAT
- Several other and different IM/Presence technologies are available, and the interoperability will be very important issue
- Some overlap with the XCON WG (multi-chat); discussion about cooperation is going on

Thank you!

Questions & Comments?

BACKUP SLIDES

From Jabber to XMPP...

- Aug 1999, J. Miller on behalf of Jabber community approached IETF
- June 2000 Jabber community submitted the Jabber protocol to the IETF ? no success...
- 2002 another submission, and this time a successful one ? XMPP WG was formed

XMPP E2E Signing/Encryption

1. Generate a CPIM MIME object out of the XMPP stanza.
2. Encrypt and/or sign the headers and the content of the generated CPIM object.
3. Put the resulting encrypted object inside e2e child element of a message stanza in XMPP