IETF IMPP WG
Internet draft

G. Klyne, Content Technologies
7 March 2000
Expires: September 2000

Security Framework for Instant Messaging and Presence Protocol

<draft-ietf-impp-security-framework-01.txt>

Status of this memo

Copyright Notice

Abstract

This memo describes the security framework for the Instant Messaging and Presence Protocols. It identifies the entities that use IMPP protocol elements, the trust relationships between them, security threats that are against which defence is to be provided, and the consequent security responsibilities of the active

entities. Specific cryptographic and other security mechanisms are NOT defined here.

NOTE: The security framework for IMPP is inherently bound up with the IMPP protocol design, and this memo is expected to evolve as decisions are made about the protocol design. In its current form, this memo makes some assumptions about the IMPP structure that must be reviewed as design proceeds.

Table of contents

1. Introduction

1.1 Structure of this document

Section 2 identifies the entities that participate in instant messaging and presence applications using the IMPP protocols.

Section 3 describes the communication paths and trust relationships between the participating entities.

Section 4 indicates the threats against which defence is required, and other security requirements.

Section 5 considers the trust model and security requirements to derive security-related responsibilities for each of the participating entities, and identifies the trust boundaries.

1.2 Document terminology and conventions

The acronym IMPP is used for "Instant Messaging and Presence Protocol".

Terminology for IMPP concepts is covered by "A Model for Presence and Instant Messaging" [1].

> NOTE: Comments like this provide additional nonessential information about the rationale behind this document. Such information is not needed for building a conformant implementation, but may help those who wish to understand the design in greater depth.

[[[Editorial comments and questions about outstanding issues are provided in triple brackets like this. These working comments should be resolved and removed prior to final publication.]]]

1.3 Discussion of this document

Discussion of this document should take place on the Instant Messaging and Presence Protocol mailing list. Please send comments regarding this document to:

<impp@iastate.edu>

To subscribe to this list, send a message to "<majordomo@iastate.edu>" containing the command "subscribe impp" in the message body.

To see what has gone on before you subscribed, please see the mailing list archive at:

http://www.imppwg.org

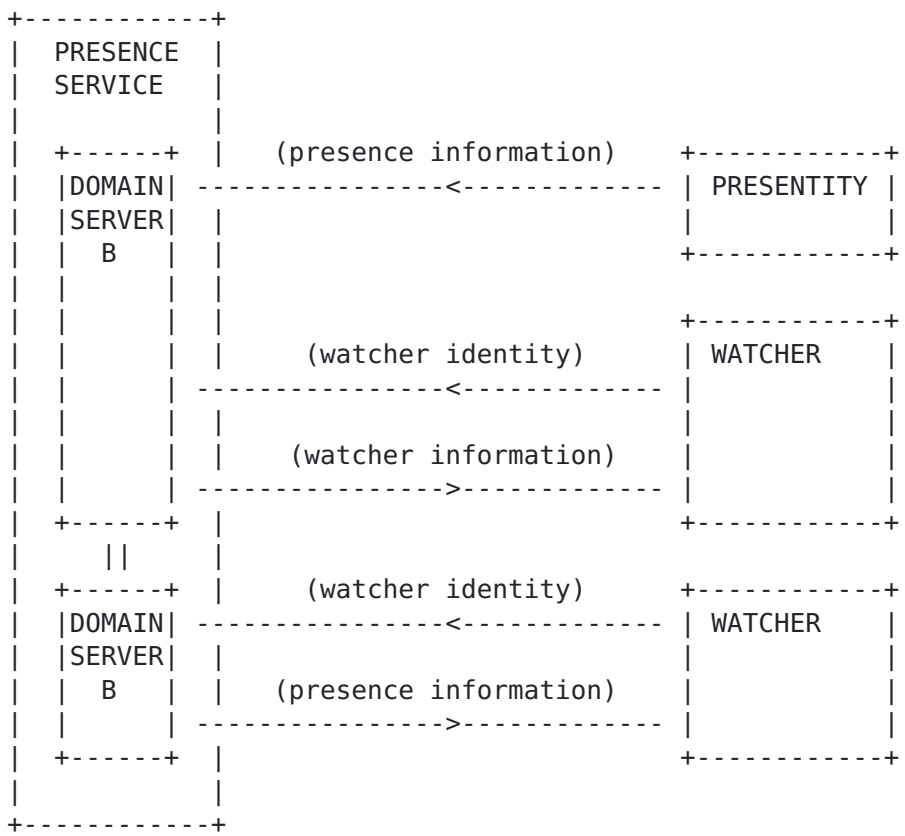
2. Participating entities

2.1 Presence service

PRESENTITY - a client that is the origin of presence information.

WATCHER - a client that consumes presence information

PRESENCE SERVICE - a service (e.g. a server or collection of servers) that communicates presence information between PRESENTITYs and WATCHERS, and also gathers and distributes watcher information.



This diagram shows a "typical" arrangement with a PRESENTITY publishing presence information, a WATCHER from a different domain observating that presence information, and a watcher (possibly for the same PRINCIPAL as the original PRESENTITY) observing who is watching PRESENTITIES presence information.

For the purposes of this architecture, watcher information is treated ike another form of presence information, so a agent that observes watcher information is just another WATCHER.

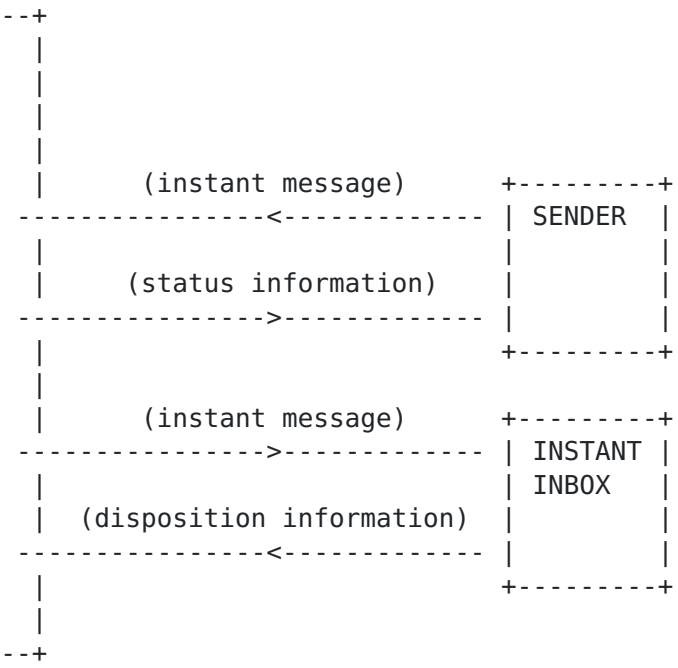
A key element of this architecture is that inter-domain communications are intermediated by a DOMAIN SERVER. This is modelled as a single server, but this is not to preclude distributed server implementatons that are outside the scope of these IMPP specifications.

2.2 Instant Messaging service

SENDER - a client that sends an instant message.

INSTANT INBOX - a client that receives an instant message.

INSTANT MESSAGE SERVICE - a service (e.g. a server or collection of servers) that transfers instant messages between SENDERs and INSTANT INBOXes, and also determines and reports message transfer status information.



This diagram shows a "typical" arrangement with a SENDER sending an instant message, and an INSTANT INBOX receiving that message and returning confirmation back to the sender.

As for presence information, inter-domain communications are intermediated by a DOMAIN SERVER. This is modelled as a single server, but this is not to preclude distributed server implementatons that are outside the scope of these IMPP specifications.

3. Trust model

(T1) The network is not trusted. Information in transit may be subject to snooping or tampering.

3.1 Presence service

[[[This is a strawman, selected for simplicity. Actual trust relationships will need to be determined.]]]

(TP1) PRESENCE SERVICE does not trust PRESENTITY to provide correct identity.

(TP2) PRESENCE SERVICE trusts PRESENTITY to provide correct presence information.

(TP3) PRESENTITY trusts the PRESENCE SERVICE to disclose presence information to authorized parties only.

(TP4) PRESENTITY trusts the PRESENCE SERVICE to distribute presence information uncorrupted.

(TP5) PRESENTITY trusts the PRESENCE SERVICE to provide correct watcher information.

(TP6) PRESENCE SERVICE does not trust WATCHER to provide correct identity.

(TP7) PRESENCE SERVICE does not trust WATCHER to respect confidentiality and privacy concerns.

(TP8) WATCHER trusts PRESENCE SERVICE to provide correct presence information.

(TP9) WATCHER trusts the PRESENCE SERVICE to disclose watcher information to authorized parties only.

(TP10) WATCHER trusts PRESENCE SERVICE to provide correct watcher information.

3.2 Instant Messaging service

[[[This, too, is a strawman, selected for simplicity. Actual trust relationships will need to be determined.]]]

(TM1) INSTANT MESSAGE SERVICE does not trust SENDER to provide correct identity.

(TM2) SENDER trusts the INSTANT MESSAGE SERVICE to disclose instant message and associated information to authorized parties only.

(TM3) SENDER trusts the INSTANT MESSAGE SERVICE to distribute instant message uncorrupted.

(TM4) SENDER trusts the INSTANT MESSAGE SERVICE to provide correct message status information.

(TM5) INSTANT MESSAGE SERVICE does not trust INSTANT INBOX to provide correct identity. [[[How does INSTANT MESSAGE SERVICE get information about INSTANT INBOX?]]]

(TM6) INSTANT MESSAGE SERVICE does not trust INSTANT INBOX to respect confidentiality and privacy constraints.

(TM7) INSTANT INBOX trusts INSTANT MESSAGE SERVICE to provide correct instant message information.

(TM8) INSTANT INBOX trusts the INSTANT MESSAGE SERVICE to disclose message disposition and status information to the sender only (and other authorized parties?).

(TM9) INSTANT INBOX trusts INSTANT MESSAGE SERVICE to deliver messages only from authorized senders.

4. Security threats and requirements

[[[Some general goals and threats not covered explicitly by the requirements document...]]]

(R1) Privacy: protections should exist against unauthorized disclosure of personal information.

(R2) Authenticity: identities of the participating PRINCIPALs should be verified. This implies that protocol handling agents must provide information to allow the origin of information or requests to be authenticated.

(R3) Denial of service: possibilities for external parties to impair the service to legitimate participants should be minimized. [[[Need to identify specific DoS attacks?]]]

(R4) Denial of participation, fair play: participants should be required to meet all protocol participation requirements, or not be permitted to participate. [[[Is this really relevant for this application?]]]

4.1 Presence service

[[[From [2], section 5.3...]]]

(RP1) PRESENTITY must be able to control disclosure of its presence information. [2, sections 5.3.1-3]

(RP2) The PRINCIPAL controlling a PRESENTITY determines which other PRINCIPALs may update the presence information. Access control decisions are made independently of the presence of a PRESENTITY [[[Is this really in scope? It describes UA rather than protocol behaviour.]]]

[[[From [2], section 5.5...]]]

(RP3) Capability to protect PRESENCE INFORMATION against tampering or corruption.

(RP4) Capability to protect PRESENCE INFORMATION against replay by a third party.

(RP5) Capability to protect confidentiality of PRESENCE INFORMATION.

[[[Watcher information -- seems not to be covered by reqs?]]]

4.2 Instant Messaging service

[[[From [2], section 5.3...]]]

(RM1) PRINCIPAL controlling an INSTANT INBOX determines who can send messages to it. This implies that protocol handling agents must record access control information and provide for testing of authenticated message identifies.

(RM2) The PRINCIPAL controlling an INSTANT INBOX determines which other PRINCIPALs may read messages from it. [[[Is this really in scope? It describes UA rather than protocol behaviour.]]]

[[[From [2], section 5.5...]]]

(RM3) Capability to protect INSTANT MESSAGE against tampering or corruption.

(RM4) Capability to protect INSTANT MESSAGE against replay by a third party.

(RM5) Capability to protect confidentiality of INSTANT MESSAGE.

5. Trust boundaries and security responsibilities

The parts of the PRESENCE SERVICE that interface with PRESENTITYs and/or WATCHERs span trust boundaries.

Similarly, the parts of the INSTANT MESSAGE SERVICE that interface with SENDERs and/or INSTANT INBOXes span trust boundaries.

5.1 Privacy

From (R1), (T1), (TP3), (TP7), (TM1), (TM8).

PRESENTITY may disclose presence information to authenticated PRESENCE SERVICE.

PRESENCE SERVICE must enforce disclosure of presence information to only authorized, authenticated WATCHERs.

PRESENCE SERVICE must enforce disclosure of watcher information to only authorized, authenticated PRESENTITYs and WATCHERs.

SENDER may disclose instant message to authenticated INSTANT MESSAGE SERVICE.

INSTANT MESSAGE SERVICE must enforce disclosure of instant message information to only authorized, authenticated INSTANT INBOXes.

INSTANT INBOX may disclose instant message disposition information to authenticated INSTANT MESSAGE SERVICE.

Privacy-sensitive information should (optionally) be encrypted for network transfers. (But note that traffic analysis may still uncover the identity of an active PRESENTITY, WATCHER, SENDER or INSTANT INBOX.)

5.2 Authenticity

From (R2), (T1), (TP1), (TP3), (TP6), (TM1), (TM2), (TM5)

PRESENTITY must provide proof of identity to PRESENCE SERVICE.

WATCHER must provide proof of identity to PRESENCE SERVICE.

PRESENTITY or WATCHER must authenticate PRESENCE SERVICE before accepting presence or watcher information.

SENDER must provide proof of identity to INSTANT MESSAGE SERVICE.

INSTANT INBOX must provide proof of identity to INSTANT MESSAGE SERVICE.

INSTANT INBOX must authenticate INSTANT MESSAGE SERVICE before accepting instant message information.

SENDER must authenticate INSTANT MESSAGE SERVICE before accepting message status information.

5.3 Denial of service

PRESENTITY may restrict WATCHERs who are FETCHERs differently from WATCHERs who are SUBSCRIBERs. (A high rate of fetches may constitute a denial of service attack.)

[[[Need more ideas about DoS attack modes]]]

5.4 Cheating

From (R4).

[[[This refers to security threats where a party participates in a protocol to obtain value without fulfilling its own obligations for participation. For example, a payment protocol that allowed goods to be delivered before an untrusted party made irrevocable commitment to payment would be somewhat flawed.]]]

There are currently no identified cheat modes.

5.5 Authorization to disclose presence information

From (RP1), (T1), (TP1), (TP3)

PRESENTITY must provide proof of identity to PRESENCE SERVICE.

The PRESENCE SERVICE accepts changes for presence disclosure permissions only from the corresponding authenticated PRESENTITY.

The PRESENCE SERVICE must store presence disclosure permissions in a tamper-proof fashion, and disclose presence information only to authenticated WATCHERs in accordance with the corresponding permissions.

5.6 Authorization to update presence information

From (RP2), (T1), (TP1), (TP2)

PRESENTITY must provide proof of identity to PRESENCE SERVICE.

The PRESENCE SERVICE accepts changes for presence update permissions only from the corresponding authenticated PRESENTITY.

The PRESENCE SERVICE must store presence update permissions in a tamper-proof fashion, and accept presence update information only from authenticated PRESENTITYs in accordance with the corresponding permissions.

5.7 Integrity of presence information

From (RP3), (T1), (TP2), (TP4)

PRESENTITY must provide presence information to PRESENCE SERVICE in integrity-protected fashion.

PRESENCE SERVICE must provide presence information to WATCHER in integrity-protected fashion.

> NOTE: because the entities here effectively trust each other to provide correct information, the integrity protection here does not need to be a full-blown authenticated integrity check. For example, a randomly generated signing key generated by the sender of the information, or a checksum and randomly generated encrypting key generated by the receiver might be adequate.
>
> In some environments, a physically protected network might be considered adequate for this purpose.

5.8 No replay of presence information

From (RP4), (T1), (TP3)

PRESENTITY and PRESENCE SERVICE should implement mechanisms to prevent presence information from being recorded and replayed at a later date.

PRESENCE SERVICE and PRESENTITY should implement mechanisms to prevent presence information from being recorded and replayed at a later date.

> NOTE: as the PRESENCE SERVICE is generally trusted by the other parties, authentication by the PRESENTITY and WATCHER are sufficient to realize these requirements.

5.9 Confidentiality of presence information

From (RP5), (T1)

PRESENTITY should send presence information only after authenticating the PRESENCE SERVICE.

PRESENTITY should encrypt presence information sent to the PRESENCE SERVICE.

PRESENCE SERVICE should send presence information only after authenticating the WATCHER.

PRESENCE SERVICE should encrypt presence information sent to the WATCHER.

5.10 Authorization to send to inbox

From (RM1), (TM1), (TM10).

INSTANT INBOX (or PRINCIPAL) must provide proof of identity to INSTANT MESSAGE SERVICE.

The INSTANT MESSAGE SERVICE accepts changes for inbox delivery permissions only from the corresponding authenticated INSTANT INBOX (or PRINCIPAL).

The PRESENCE SERVICE must store instant message delivery permissions in a tamper-proof fashion, and deliver instant messages only from authenticated SENDERs in accordance with the corresponding permissions.

5.11 Authorization to receive inbox message

From (RM2), ...

[[[Need to clarify role of PRINCIPAL here.]]]

5.12 Integrity of instant message

From (RM3), (T1), (TM3), (TM7)

SENDER must provide instant message to INSTANT MESSAGE SERVICE in integrity-protected fashion.

INSTANT MESSAGE SERVICE must deliver instant message to INSTANT INBOX in integrity-protected fashion.

> NOTE: because the entities here effectively trust each other to provide correct information, the integrity protection here does not need to be a full-blown authenticated integrity check. See section 5.7.

5.13 No replay of instant message

From (RM4), (T1), (TM2), (TM7).

SENDER and INSTANT MESSAGE SERVICE should implement mechanisms to prevent an instant message from being recorded and replayed at a later date.

INSTANT MESSAGE SERVICE and INSTANT INBOX should implement mechanisms to prevent an instant message from being recorded and replayed at a later date.

> NOTE: as the INSTANT MESSAGE SERVICE is generally trusted by the other parties, authentication by the SENDER and INSTANT INBOX are sufficient to realize these requirements.

5.14 Confidentiality of inbox message

From (RM5), (T1).

SENDER should send instant message only after authenticating the INSTANT MESSAGING SERVICE.

SENDER should encrypt instant message sent to the INSTANT MESSAGING SERVICE.

INSTANT MESSAGING SERVICE should deliver instant message only after authenticating the INSTANT INBOX.

INSTANT MESSAGING SERVICE should encrypt instant message delivered to the INSTANT INBOX.

6. Security considerations

This entire document is about security considerations.

[[[Additional points?]]]

7. Acknowledgements

Harald Alvestrand provided initial guidance regarding concepts needing to be covered by this security framework. Christophe Vermeulen provided initial diagrams showing component interactions across domains.

8. References

[1] "A Model for Presence and Instant Messaging"
Mark Day, Lotus
Jonathan Rosenberg, Bell Labs
Hiroyasu Sugano, Fujitsu
Internet draft: <draft-ietf-impp-model-03.txt>
Work in progress, August 1999

[2] "Instant Messaging / Presence Protocol Requirements"
Mark Day, Lotus
Sonu Aggarwal, Microsoft
Gordon Mohr, Activerse
Jesse Vincent, Arepa
Internet draft: <draft-ietf-impp-reqts-03.txt>
Work in progress, August 1999

8. Author's address

Graham Klyne (editor)
Content Technologies Ltd.
1220 Parkview,
Arlington Business Park
Theale
Reading, RG7 4SA
United Kingdom.
Telephone: +44 118 930 1300
Facsimile: +44 118 930 1301
E-mail: GK@ACM.ORG

Appendix A: Amendment history

00a 11-Nov-1999 Memo initially created.

01a	07-Mar-2000	Incorporate initial review comments, mostly editorial. Extend description of participating entities to show the role of domain servers in handling inter-domain communications.

TODO

+ Review component intereactions (section 2)

+ Update trust model (section 3)

+ Review security threats and requirements (section 4)

+ Update security responsibilities (section 5)

+ Say more about security considerations (section 6)?

Full copyright statement