        CUSAX: Combined Use of the Session Initiation Protocol (SIP)
          and the Extensible Messaging and Presence Protocol (XMPP)

Abstract

   This document suggests some strategies for the combined use of the
   Session Initiation Protocol (SIP) and the Extensible Messaging and
   Presence Protocol (XMPP) both in user-oriented clients and in
   deployed servers. Such strategies, which mainly consist of
   configuration changes and minimal software modifications to existing
   clients and servers, aim to provide a single, full-featured, real-
   time communication service by using complementary subsets of features
   from SIP and from XMPP. Typically, such subsets consist of telephony
   capabilities from SIP and instant messaging and presence capabilities
   from XMPP. This document does not define any new protocols or syntax
   for either SIP or XMPP and, by intent, does not attempt to
   standardize "best current practices". Instead, it merely aims to
   provide practical guidance to those who are interested in the
   combined use of SIP and XMPP for real-time communication.

Copyright Notice

Table of Contents

1. Introduction

   Historically, SIP [RFC3261] and XMPP [RFC6120] have often been
   implemented and deployed with different purposes: from its very
   start, SIP's primary goal has been to provide a means of conducting
   "Internet telephone calls". On the other hand, XMPP has, from its
   Jabber days, been mostly used for instant messaging, presence
   [RFC6121], and related services such as groupchat rooms [XEP-0045].

For various reasons, these trends have continued through the years,
even after each of the protocols had been equipped to provide the
features it was initially lacking:

o In the context of the SIP for Instant Messaging and Presence
   Leveraging Extensions (SIMPLE) working group, the IETF has defined
   a number of protocols and protocol extensions that not only allow
   for SIP to be used for regular instant messaging and presence but
   that also provide mechanisms for related features such as
   multi-party chat, server-stored contact lists, and file transfer
   [RFC6914].

o Similarly, the XMPP community and the XMPP Standards Foundation
   have worked on defining a number of XMPP Extension Protocols
   (XEPs) that provide XMPP implementations with the means of
   establishing end-to-end sessions. These extensions are often
   jointly referred to as Jingle [XEP-0166], and arguably their most
   popular use case is audio and video calling [XEP-0167].

However, although SIP has been extended for messaging and presence
and XMPP has been extended for voice and video, the reality is that
SIP remains the protocol of choice for telephony-like services, and
XMPP remains the protocol of choice for IM and presence services. As
a result, a number of adopters have found themselves needing features
that are not offered by any single-protocol solution, but ones that
separately exist in SIP and XMPP implementations. The idea of
seamlessly using both protocols together would hence often appeal to
service providers and users. Most often, such a service would employ
SIP exclusively for audio, video, and telephony services and rely on
XMPP for anything else varying from chat, contact-list management,
and presence to whiteboarding and exchanging files. Because these
services and clients involve the combined use of SIP and XMPP, we
label them "CUSAX" for short.

```
            +------------+      +-------------+
            | SIP Server |      | XMPP Server |
            +------------+      +-------------+
                   \              /
            media   \            /  instant messaging,
            signaling \        /   presence, etc.
                     \        /
                +--------------+
                | CUSAX Client |
                +--------------+
```
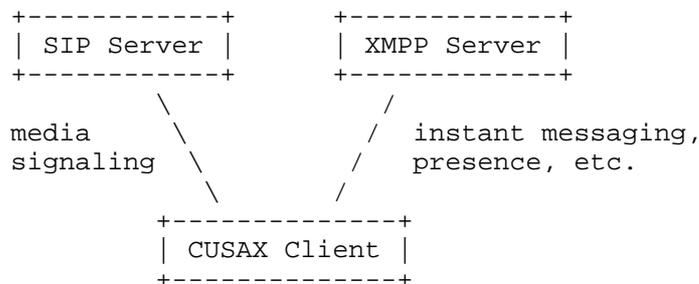
                Figure 1: Division of Responsibilities

This document suggests different configuration options and minimal
modifications to existing software so that clients and servers can
offer these hybrid services while providing an optimal user
experience. It covers server discovery, determining a SIP Address of
Record (AOR) while using XMPP, and determining an XMPP Jabber
Identifier (JID) from incoming SIP requests. Most of the text here
pertains to client behavior, but we also suggest certain server-side
configurations and operational strategies. The document also
discusses significant security considerations that can arise when
offering a dual-protocol solution and provides advice for avoiding
security mismatches that would result in degraded communications
security for end users.

Note that this document is focused on coexistence of SIP and XMPP
functionality in end-user-oriented clients. By intent, it does not
define methods for protocol-level mapping between SIP and XMPP, as
might be used within a server-side gateway between a SIP network and
an XMPP network (a separate series of documents has been produced
that defines such mappings). More generally, this document does not
describe service policies for inter-domain communication (often
called "federation") between service providers (e.g., how a service
provider that offers a CUSAX service might communicate with a
SIP-only or XMPP-only service), nor does it describe the reasons why
a service provider might choose SIP or XMPP for various features.

This document concentrates on use cases where the SIP services and
XMPP services are controlled by one and the same provider, since that
assumption greatly simplifies both client implementation and
server-side deployment (e.g., a single service provider can enforce
common or coordinated policies across both the SIP and XMPP aspects
of a CUSAX service, which is not possible if a SIP service is offered
by one provider and an XMPP service is offered by another provider).
Since this document is of an informational nature, it is not
unreasonable for clients to apply some of the guidelines here even in
cases where there is no established relationship between the SIP and
the XMPP services (for example, it is reasonable for a client to
provide a way for its users to easily start a call to a phone number
or SIP URI found in a vCard or obtained from a user directory).
However, the strategies to pursue in such cases are left to
application developers.

This document makes a further simplifying assumption by discussing
only the use of a single client, not use of and coordination among
multiple endpoints controlled by the same user (e.g., user agents
running simultaneously on a laptop computer, tablet, and mobile
phone). Although user agents running on separate endpoints might
themselves be CUSAX clients or might engage in different aspects of
an interaction (e.g., a user might employ her mobile phone for audio

and her tablet for video and text chat), such usage complicates the
guidelines for developers of user agents and therefore is left as a
matter of implementation for now.

It is important to note that this document does not attempt to
standardize "best current practices" in the sense defined in the
Internet Standards Process [RFC2026]. Instead, it collects together
informational documentation about some strategies that might prove
helpful to those who implement and deploy combined SIP/XMPP software
and services. With sufficient use and appropriate modification to
incorporate the lessons of experience, these strategies might someday
form the basis for standardization of best current practices.

2. Client Bootstrap

One of the main problems of using two distinct protocols when
providing one service is the impact on usability. Email services,
for example, have long been affected by the mixed use of SMTP for
outgoing mail and Post Office Protocol version 3 (POP3) or IMAP for
incoming mail. Although standard service discovery methods (such as
the proper DNS records) make it possible for a user agent to locate
the right host(s) for connect purposes, they do not provide the kind
of detailed information that is needed to actually configure the user
agent for use with the service. As a result, it is rather
complicated for inexperienced users to configure a mail client and
start using it with a new service; and as a result, Internet service
providers often need to provide configuration instructions for
various mail clients. Client developers and communication device
manufacturers, on the other hand, often ship with a number of
so-called "wizard" interfaces that enable users to easily configure
accounts with a number of popular email services. Although this may
improve the situation to some extent, the user experience is still
clearly suboptimal.

While it should be possible for CUSAX users to manually configure
their separate SIP and XMPP accounts (often using "wizards"), service
providers offering CUSAX services to users of dual-stack SIP/XMPP
clients ought to provide methods for online provisioning, typically
by means of a web-based service at an HTTPS URL (naturally, single-
purpose SIP services or XMPP services could offer such methods as
well, but they can be especially helpful where the two aspects of the
CUSAX service need to have several configuration options in common).
Although the specifics of such mechanisms are outside the scope of
this document, they should make it possible for a service provider to
remotely configure the clients based on minimal user input (e.g.,
only a user ID and password). As far as the authors are aware, no
open protocol for endpoint configuration is yet available and

adopted; however, application developers are encouraged to explore
the potential for future progress in this space (e.g., perhaps based
on technologies such as WebFinger [RFC7033]).

By default, when a CUSAX client is used in concert with SIP and XMPP
accounts that have a CUSAX relationship (see Section 3.4), the client
should disable audio and video calling over XMPP and disable instant
messaging and presence over SIP. (It is a matter of implementation
whether a CUSAX client allows a user to override these defaults in
various ways, e.g., by domain, by individual contact, or by device.)
The main advantage of this approach is that a client would employ the
most relevant features from both SIP and XMPP when used in the
context of a CUSAX service. Note that this default configuration
does not apply to stand-alone SIP accounts or XMPP accounts, for
which other settings are likely to be more appropriate (see
Section 3.4 for details).

Once a client has been provisioned, it needs to independently log
into the SIP account and XMPP account that make up the CUSAX
"service" and then maintain both connections.

In order to improve the user experience, when reporting connection
status, a CUSAX client may wish to present the XMPP connection as an
"instant messaging" or a "chat" account and the SIP connection as a
"Voice and Video" or a "Telephony" connection. The exact naming is
of course entirely up to implementers. The point is that, in cases
where SIP and XMPP are components of a service offered by a single
provider, such presentation could help users better understand why
they are being shown two different connections for what they perceive
as a single service (especially when one of the connections is
disrupted while the other one is still active). Alternatively, the
developers of a CUSAX client or the providers of a CUSAX service
might decide to force a client to completely disconnect unless both
aspects are successfully connected.

Clients may also choose to delay their XMPP connection until they
have been successfully registered on SIP. This would help avoid the
situation where a user appears online to her contacts but calling the
user's client would fail because the user's client is still
connecting to the SIP aspect of the CUSAX service.

3. Operation

Once a CUSAX client has been provisioned and authorized to connect to
the corresponding SIP and XMPP services, it would proceed by
retrieving its XMPP roster.

The client should use XMPP for most forms of communication with the
contacts from this roster, which will occur naturally because they
were retrieved through XMPP. Audio/video features, however, would
typically be disabled in the XMPP stack, so media-related
communication based on these features (e.g., direct calls,
conferences, desktop streaming, etc.) would happen over SIP. The
rest of this section describes deployment, discovery, usability, and
linking semantics that enable CUSAX clients to seamlessly use SIP for
these features.

3.1. Server-Side Setup

In order for CUSAX to function properly, XMPP service administrators
should make sure that at least one of the vCard [RFC6350] "tel"
fields for each contact is properly populated with a SIP URI for the
user's address at the SIP audio/video service provided by the CUSAX
server. There are no limitations as to the form of that number. For
example, while it is desirable to maintain a certain consistency
between SIP AORs and XMPP JIDs, that is by no means required. It is
quite important, however, that the phone number or SIP AOR stored in
the vCard be reachable through the SIP aspect of this CUSAX service.
(The same considerations apply even if the directory storage format
is not vCard storage over XMPP as described by [XEP-0054] or
[XEP-0292].)

Administrators may also choose to include the "video" tel type
defined in [RFC6350] for accounts that would be capable of handling
video communication.

To ensure that the foregoing approach is always respected, service
providers might consider validating the values of vCard "tel" fields
before storing changes. Of course, such validation would be feasible
only in cases where a single provider controls both the XMPP and the
SIP service since such providers would "know" (e.g., based on use of
a common user database for both services) what SIP AOR corresponds to
a given XMPP user.

3.2. Service Management

The task of operating and managing a stand-alone SIP service or XMPP
service is not always easy. Combining the two into a unified service
introduces additional challenges, including:

o The necessity of opening additional ports on the client side if
   SIP functionality is added to an existing XMPP deployment, or vice
   versa.

o The potential for important differences in security posture across
   SIP and XMPP (e.g., SIP servers and XMPP servers might support
   different Transport Layer Security (TLS) ciphersuites).

o The need for, ideally, a common authentication backend and other
   infrastructure that is shared across the SIP and XMPP aspects of
   the combined service.

o Coordinated monitoring and logging of the SIP and XMPP servers to
   enable the correlation of incidents and the pinpointing of
   problems.

o The difficulty of troubleshooting client-side issues, e.g., if the
   client loses connectivity for XMPP but maintains its SIP
   connection.

Although separation of functionality (SIP for media and XMPP for IM
and presence) can help to ease the operational burden to some extent,
service providers are urged to address the foregoing challenges and
similar issues when preparing to launch a CUSAX service.

Beyond the issues listed above, service providers might want to be
aware of more subtle operational issues that can arise. For example,
if a service provider uses different network operators for the SIP
service and the XMPP service, end-to-end connectivity might be more
reliable or consistent in one service than in the other service.
Similar issues can arise when the media path and the signaling path
go over different networks, even in stand-alone SIP or XMPP services.
Providers of CUSAX services are advised to consider the potential for
such topologies to cause operational challenges.

3.3. Client-Side Discovery and Usability

When rendering the roster for a particular XMPP account, CUSAX
clients should make sure that users are presented with a "Call"
option for each roster entry that has a properly set "tel" field.
This is the case even if calling features have been disabled for that
particular XMPP account, as advised by this document. The usefulness
of such a feature is not limited to CUSAX. After all, numbers are
entered in vCards or stored in directories in order to be dialed and
called. Hence, as long as an XMPP client has any means of conducting
a call, it may wish to make it possible for the user to easily dial
any numbers that it learned through whatever means.

Clients that have separate triggers (e.g., buttons) for audio calls
and video calls may choose to use the presence or absence of the
"video" tel type defined in [RFC6350] as the basis for choosing

whether to enable or disable the possibility for starting video calls
(i.e., if there is no "video" tel type for a particular contact, the
client could disable the "video call" button for that contact).

In addition to discovering phone numbers from vCards or user
directories, clients may also check for alternative communication
methods as advertised in XMPP presence broadcasts and Personal
Eventing Protocol nodes as described in "XEP-0152: Reachability
Addresses" [XEP-0152]. However, these indications are merely hints,
and a receiving client ought not associate a SIP address and an XMPP
address unless it has some way to verify the relationship (e.g., the
vCard of the XMPP account lists the SIP address and the vCard of the
SIP account lists the XMPP address, or the relationship is made
explicit in a record provided by a trusted directory).
Alternatively, or in cases where vCard or directory data is not
available, a CUSAX client could take the user's own address book as
the canonical source for contact addresses.

3.4. Indicating a Relationship between SIP and XMPP Accounts

In order to improve usability, in cases where clients are provisioned
with only a single telephony-capable account they ought to initiate
calls immediately upon user request without asking users to indicate
an account that the call should go through. This way, CUSAX users
(whose only account with calling capabilities is usually the SIP part
of their service) would have a better experience, since from the
user's perspective calls "just work at the click of a button".

In some cases, however, clients will be configured with more than the
two XMPP and SIP accounts provisioned by the CUSAX provider. Users
are likely to add additional stand-alone XMPP or SIP accounts (or
accounts for other communications protocols), any of which might have
both telephony and instant messaging capabilities. Such situations
can introduce additional ambiguity since all of the telephony-capable
accounts could be used for calling the numbers the client has learned
from vCards or directories.

To avoid such confusion, client implementers and CUSAX service
providers may choose to indicate the existence of a special
relationship between the SIP and XMPP accounts of a CUSAX service.
For example, let's say that Alice's service provider has opened both
an XMPP account and a SIP account for her. During or after
provisioning, her client could indicate that alice@xmpp.example.com
has a CUSAX relationship to alice@sip.example.com (i.e., that they
are two aspects of the same service). This way, whenever Alice
triggers a call to a contact in her XMPP roster, the client would
preferentially initiate this call through her example.com SIP account
even if other possibilities exist (such as the XMPP account where the

vCard was obtained or a SIP account with another provider).
Similarly, the client would preferentially initiate textual chat
sessions using her XMPP account.

If, on the other hand, no relationship has been configured or
discovered between a SIP account and an XMPP account, and the client
is aware of multiple telephony-capable accounts, it ought to present
the user with the option of using XMPP Jingle as one method for
engaging in audio and video interactions with a contact who has an
XMPP address. This can help to ensure that a CUSAX user can complete
audio and video calls with XMPP users who are not part of a CUSAX
deployment.

3.5. Matching Incoming SIP Calls to XMPP JIDs

When receiving a SIP call, a CUSAX client may wish to determine the
identity of the caller and a corresponding XMPP roster entry so that
the receiving user could revert to chatting or other forms of
communication that require XMPP. To do so, a CUSAX client could
search the user's roster for an entry whose vCard has a "tel" field
matching the originator of the call. In addition, in order to avoid
the effort of iterating over the entire roster of the user and
retrieving vCards for all of the user's contacts, the receiving
client may guess at the identity of the caller based a SIP Call-Info
header whose 'purpose' header field parameter has a value of "impp"
as described in [RFC6993]. To enable this usage, a sending client
would need to include such a Call-Info header in the SIP messages
that it sends when initiating a call. An example follows.

Call-Info: <xmpp:alice@xmpp.example.com> ;purpose=impp

Note that the information from the Call-Info header should only be
used as a cue: the actual AOR-to-JID binding would still need to be
confirmed by the vCard of a contact in the receiving user's roster or
through some other trusted means (such as an enterprise directory).
If this confirmation succeeds, the client would not need to search
the entire roster and retrieve all vCards. Not performing the check
might enable any caller (including malicious ones) to employ someone
else's identity and perform various scams or Man-in-the-Middle
attacks.

However, although an AOR-to-JID binding can be a helpful hint to the
user, nothing in the foregoing paragraph ought to be construed as
necessarily discouraging users, clients, or service providers from
accepting calls originated by entities that are not established
contacts of the user (e.g., as reflected in the user's roster); that
is a policy matter for the user, client, or service provider.

It is also worth noting that callers preferring to remain anonymous
as per [RFC3325] would not provide Call-Info information.

4. Multi-Party Interactions

CUSAX clients that support the SIP conferencing framework [RFC4353]
can detect when a call they are participating in is actually a
conference and can then subscribe to conference state updates as per
[RFC4575]. A regular SIP user agent might also use the same
conference URI for text communication with the Message Session Relay
Protocol (MSRP). However, given that SIP's instant messaging
capabilities would normally be disabled (or simply not supported) in
CUSAX deployments, an XMPP Multi-User Chat (MUC) room [XEP-0045]
associated with the conference can be announced/discovered through
<service-uris> bearing the "grouptextchat" purpose [GROUPTEXTCHAT].
Similarly, an XMPP MUC room can advertise the SIP URI of an
associated service for audio/video interactions using the
'audio-video-uri' field of the "muc#roominfo" data form [XEP-0004] to
include extended information [XEP-0128] about the MUC room within
XMPP service discovery [XEP-0030]; see [XEP-0045] for an example.
These methods would enable a CUSAX-aware SIP conference server to
advertise the existence of an associated XMPP chat room and for a
CUSAX-aware XMPP chat room to advertise the existence of an
associated SIP conference server.

If a CUSAX client joins the MUC room associated with a particular
call, it should not rely on any synchronization between the two.
Both the SIP conference and the XMPP MUC room would function
independently, each issuing and delivering its own state updates.
Hence, it is possible that certain peers would temporarily or
permanently be reachable in only one of the two conferences. This
would typically be the case with single-stack clients that have only
joined the SIP call or the XMPP MUC room. It is therefore important
for CUSAX clients to provide a clear indication to users as to the
level of involvement of the various participants: i.e., a user needs
to be able to easily understand whether a certain participant can
receive text messages, audio/video, or both.

At the level of the CUSAX service, it is also possible to enforce
tighter integration between the XMPP MUC room and the SIP conference.
Permissions, roles, kicks, and bans that are granted and performed in
the MUC room can easily be imitated by the conference focus/mixer
into the SIP call. If, for example, a certain MUC member is muted,
the conference mixer can choose to also apply the mute on the media
stream corresponding to that participant. However, the details and
exact level of such integration are entirely up to implementers and
service providers.

The approach above describes one relatively lightweight possibility
of combining SIP and XMPP multi-party interaction semantics without
requiring tight integration between the two. As with the rest of
this document, this approach is by no means normative.
Implementations and future documents may define other methods or
provide other suggestions for improving the unified communications
user experience in cases of multi-user chats and conference calling.

5. Federation

   In theory, there are no technical reasons why federation (i.e.,
   inter-domain communication) would require special behavior from CUSAX
   clients. However, it is worth noting that differences in
   administration policies may sometimes lead to potentially confusing
   user experiences.

   For example, let's say atlanta.example.com observes the CUSAX
   policies described in this document. All XMPP users at
   atlanta.example.com are hence configured to have vCards that match
   their SIP identities. Alice is therefore used to making free, high-
   quality SIP calls to all the people in her roster. Alice can also
   make calls to the Public Switched Telephone Network (PSTN) by simply
   dialing numbers. She may even be used to these calls being billed to
   her online account, so she would be careful about how long they last.
   This is not a problem for her since she can easily distinguish
   between a free SIP call (one that she made by calling one of her
   roster entries) from a paid PSTN call that she dialed as a number.

   Then, Alice adds xmpp:bob@biloxi.example.com. The Biloxi domain only
   has an XMPP service. There is no SIP server and Bob uses an
   XMPP-only client. However, Bob has added his mobile number to his
   vCard in order to make it easily accessible to his contacts. Alice's
   client would pick up this number and make it possible for Alice to
   start a call to Bob's mobile phone number.

   This could be a problem because, other than the fact that Bob's
   address is from a different domain, Alice would have no obvious and
   straightforward cues telling her that this is in fact a call to the
   PSTN. In addition to the potentially lower audio quality, Alice may
   also end up incurring unexpected charges for such calls.

   In order to avoid such issues, providers maintaining a CUSAX service
   for the users in their domain may choose to provide additional cues
   (e.g., a service-generated signal that triggers a user-interface
   warning in a CUSAX client, an auditory tone, or a spoken message)
   indicating that a call would incur unexpected charges.

Another scenario arises when a SIP service allows communication only
with intra-domain numbers; here, Alice might be prevented from
establishing a call with Bob's mobile phone. Providers should
therefore make sure that calls to inter-domain numbers are flagged
with an appropriate audio or textual warning.

6. Summary of Suggested Strategies

The following strategies are suggested for CUSAX user agents:

1. By default, prefer SIP for audio and video and XMPP for
    messaging and presence.

2. Use XMPP for all forms of communication with the contacts from
    the XMPP roster, with the exception of features that are based
    on establishing real-time sessions (e.g., audio/video calls) for
    which SIP should be used.

3. Provide online provisioning options for providers to remotely
    set up SIP and XMPP accounts so that users wouldn't need to go
    through a multi-step configuration process.

4. Provide online provisioning options for providers to completely
    disable features for an account associated with a given protocol
    (SIP or XMPP) if the features are preferred in another protocol
    (XMPP or SIP).

5. Present a "Call" option for each roster entry that has a
    properly set "tel" field in the vCard or equivalent.

6. If the client is provisioned with only a single telephony-
    capable account, initiate calls immediately upon user request
    without asking users to indicate an account that the call should
    go through.

7. If no relationship has been configured or discovered between a
    SIP account and an XMPP account, and the client is aware of
    multiple telephony-capable accounts, present the user with the
    choice of reaching the contact through any of those accounts.

8. If known, indicate the existence of a special relationship
    between the SIP and XMPP accounts of a CUSAX service.

9. Optionally, present the XMPP connection as an "instant
    messaging" or a "chat" account and the SIP connection as a
    "Voice and Video" or a "Telephony" account.

10. Optionally, determine the identity of the audio/video caller and
    a corresponding XMPP roster entry so that the user could use
    textual chatting or other forms of communication that require
    XMPP.

11. Optionally, delay the XMPP connection until after a SIP
    connection has been successfully registered.

12. Optionally, check for alternative communication methods (SIP
    addresses advertised over XMPP and XMPP addresses advertised
    over SIP).

The following strategies are suggested for CUSAX services:

1. Use online provisioning and configuration of accounts so that
   users won't need to set up two separate accounts for the CUSAX
   service.

2. Use online provisioning so that calling features are disabled for
   all XMPP accounts.

3. Ensure that at least one of the vCard "tel" fields for each XMPP
   user is properly populated with a SIP URI that is reachable
   through the SIP service.

4. Optionally, include the "video" tel type for accounts that are
   capable of handling video communication.

5. Optionally, provision clients with information indicating that
   specific SIP and XMPP accounts are related in a CUSAX service.

6. Optionally, attach a "Call-Info" header with an "impp" purpose to
   all SIP INVITE messages, so that clients can more rapidly
   associate a caller with a roster entry and display a "Caller ID".

7. Security Considerations

   Use of the same user agent with two different accounts providing
   complementary features introduces the possibility of mismatches
   between the security profiles of those accounts or features. Two
   security mismatches of particular concern are:

   o The SIP aspect and XMPP aspect of a CUSAX service might offer
     different authentication options (e.g., digest authentication for
     SIP as specified in [RFC3261] and Salted Challenge Response
     Authentication Mechanism (SCRAM) authentication [RFC5802] for XMPP
     as specified in [RFC6120]). Because SIP uses a password-based
     method (digest) and XMPP uses a pluggable framework for

      authentication via the Simple Authentication and Security Layer
      (SASL) technology [RFC4422], it is also possible that the XMPP
      connection could be authenticated using a password-free method
      such as client certificates with SASL EXTERNAL, even though a
      username and password is used for the SIP connection.

   o The Transport Layer Security (TLS) [RFC5246] ciphersuites offered
      or negotiated on the XMPP side might be different from those on
      the SIP side because of implementation or configuration
      differences between the SIP server and the XMPP server. Even more
      seriously, a CUSAX client might successfully negotiate TLS when
      connecting to the XMPP aspect of the service but not when
      connecting to the SIP aspect, or vice versa. In this situation,
      an end user might think that the combined CUSAX session with the
      service is protected by TLS, even though only one aspect is
      protected.

   Security mismatches such as these (as well as others related to end-
   to-end encryption of messages or media) introduce the possibility of
   downgrade attacks, eavesdropping, information leakage, and other
   security vulnerabilities. User agent developers and service
   providers must ensure that such mismatches are avoided as much as
   possible (e.g., by enforcing common and strong security
   configurations and policies across protocols). Specifically, if both
   protocols are not safeguarded by similar levels of cryptographic
   protection, the user must be informed of that fact and given the
   opportunity to bring both up to the same level.

   Section 5 discusses potential issues that may arise due to a mismatch
   between client capabilities, such as calls being initiated with costs
   that are not expected by the end user. Such issues could be
   triggered maliciously, as well as by accident. Implementers
   therefore need to provide necessary cues to raise user awareness as
   suggested in Section 5.

   Refer to the specifications for the relevant SIP and XMPP features
   for detailed security considerations applying to each "stack" in a
   CUSAX client.

8. References

8.1. Normative References

   [RFC3261]   Rosenberg, J., Schulzrinne, H., Camarillo, G.,
                      Johnston, A., Peterson, J., Sparks, R., Handley, M.,
                      and E. Schooler, "SIP: Session Initiation Protocol",
                      RFC 3261, June 2002.

   [RFC6120]   Saint-Andre, P., "Extensible Messaging and Presence
                      Protocol (XMPP): Core", RFC 6120, March 2011.

   [RFC6121]   Saint-Andre, P., "Extensible Messaging and Presence
                      Protocol (XMPP): Instant Messaging and Presence",
                      RFC 6121, March 2011.

8.2. Informative References

   [GROUPTEXTCHAT]   Ivov, E., "A Group Text Chat Purpose for Conference
                      and Service URIs in the Session Initiation Protocol
                      (SIP) Event Package for Conference State", Work
                      in Progress, June 2013.

   [RFC2026]   Bradner, S., "The Internet Standards Process --
                      Revision 3", BCP 9, RFC 2026, October 1996.

   [RFC3325]   Jennings, C., Peterson, J., and M. Watson, "Private
                      Extensions to the Session Initiation Protocol (SIP)
                      for Asserted Identity within Trusted Networks",
                      RFC 3325, November 2002.

   [RFC4353]   Rosenberg, J., "A Framework for Conferencing with
                      the Session Initiation Protocol (SIP)", RFC 4353,
                      February 2006.

   [RFC4422]   Melnikov, A. and K. Zeilenga, "Simple Authentication
                      and Security Layer (SASL)", RFC 4422, June 2006.

   [RFC4575]   Rosenberg, J., Schulzrinne, H., and O. Levin, "A
                      Session Initiation Protocol (SIP) Event Package for
                      Conference State", RFC 4575, August 2006.

   [RFC5246]   Dierks, T. and E. Rescorla, "The Transport Layer
                      Security (TLS) Protocol Version 1.2", RFC 5246,
                      August 2008.

   [RFC5802]   Newman, C., Menon-Sen, A., Melnikov, A., and N.
                      Williams, "Salted Challenge Response Authentication
                      Mechanism (SCRAM) SASL and GSS-API Mechanisms",
                      RFC 5802, July 2010.

   [RFC6350]   Perreault, S., "vCard Format Specification",
                      RFC 6350, August 2011.

   [RFC6914]   Rosenberg, J., "SIMPLE Made Simple: An Overview of
                   the IETF Specifications for Instant Messaging and
                   Presence Using the Session Initiation Protocol
                   (SIP)", RFC 6914, April 2013.

   [RFC6993]   Saint-Andre, P., "Instant Messaging and Presence
                   Purpose for the Call-Info Header Field in the
                   Session Initiation Protocol (SIP)", RFC 6993,
                   July 2013.

   [RFC7033]   Jones, P., Salgueiro, G., Jones, M., and J. Smarr,
                   "WebFinger", RFC 7033, September 2013.

   [XEP-0004]   Eatmon, R., Hildebrand, J., Miller, J., Muldowney,
                   T., and P. Saint-Andre, "Data Forms", XSF XEP 0004,
                   August 2007.

   [XEP-0030]   Hildebrand, J., Millard, P., Eatmon, R., and P.
                   Saint-Andre, "Service Discovery", XSF XEP 0030,
                   June 2008.

   [XEP-0045]   Saint-Andre, P., "Multi-User Chat", XSF XEP 0045,
                   February 2012.

   [XEP-0054]   Saint-Andre, P., "vcard-temp", XSF XEP 0054,
                   July 2008.

   [XEP-0128]   Saint-Andre, P., "Service Discovery Extensions", XSF
                   XEP 0128, October 2004.

   [XEP-0152]   Hildebrand, J. and P. Saint-Andre, "XEP-0152:
                   Reachability Addresses", XEP XEP-0152,
                   September 2013.

   [XEP-0166]   Ludwig, S., Beda, J., Saint-Andre, P., McQueen, R.,
                   Egan, S., and J. Hildebrand, "Jingle", XSF XEP 0166,
                   December 2009.

   [XEP-0167]   Ludwig, S., Saint-Andre, P., Egan, S., McQueen, R.,
                   and D. Cionoiu, "Jingle RTP Sessions", XSF XEP 0167,
                   December 2009.

   [XEP-0292]   Saint-Andre, P. and S. Mizzi, "vCard4 Over XMPP",
                   XSF XEP 0292, September 2013.

Appendix A. Acknowledgements

Authors' Addresses

    Emil Ivov
    Jitsi
    Strasbourg 67000
    France

    Phone: +33-177-624-330
    EMail: emcho@jitsi.org

    Peter Saint-Andre
    Cisco Systems, Inc.
    1899 Wynkoop Street, Suite 600
    Denver, CO 80202
    USA

    Phone: +1-303-308-3282
    EMail: psaintan@cisco.com

    Enrico Marocco
    Telecom Italia
    Via G. Reiss Romoli, 274
    Turin 10148
    Italy

    EMail: enrico.marocco@telecomitalia.it