Network Working Group	E. Ivov
Internet-Draft	SIP Communicator
Intended status: Informational	E. Marocco
Expires: September 3, 2010	Telecom Italia
	March 02, 2010

TOC

Problem Statement and Possible Best Practices for Authentication of SIP+XMPP Clients
draft-ivov-sipxmpp-auth-01

Abstract

This document discusses several mechanisms for simplifying authentication of dual-stack SIP+XMPP clients against the corresponding SIP and XMPP services. The text is not attempt to define a complex credential sharing protocol but rather to determine and eventually encourage use of a simple mechanism that would allow service providers to host a SIP+XMPP solution appearing as a single service to their users. In other words, the goal here is to agree on a set of recommendations that would encourage client developers to implement simple UIs that would only require users to provide an ID and a password when configuring their SIP+XMPP account for the first time (as opposed to having to do so separately for SIP and XMPP).

Status of this Memo

Table of Contents

---

1. Introduction

TOC

[TODO:ref-to-charter] and [TODO:ref-to-draft] define the requirements and the semantics for combined use of SIP and XMPP servers. Among other things, the combination allows providers to easily use SIP server products with audio/video capabilities together with IM/presence XMPP ones when building platforms that provide all these features in a single service. Both, the proposed charter, and the draft solution make it clear that server side components should be barely if at all modified and that the effort of making both protocols function as one should be delegated to client-side applications
The issue discussed in this problem statement is related to how such client-side applications would be able to determine that a SIP and an XMPP server operate together and that (or if) it would be able to reuse the same set of user credentials (e.g. a user ID and a password) when connecting to both of them. The purpose of this document is to enumerate a ways that would allow this and discuss their various pros and cons.

The document does not attempt to open the way for new protocol extensions. The ideal result of this work would be a section in a related specification, that defines a set of assumptions, which clients would be able to make when discovering and connecting to SIP+XMPP networks, or a separate Best Practices document.

1.1. Why it is important to have a common authentication mechanism.

TOC

During a previous discussion which took place on the DISPATCH mailing list, various individuals expressed the opinion that the issue at hand need not be explicitly stated in an IETF document.
The Internet has already seen an example of a similar situation that was left without a solution. The SMTP [TODO:reference] protocol is often used in conjunction with either POP3 [TODO:reference] or IMAP [TODO:reference] without any explicitly defined relation. As a result, most e-mail clients require users to configure separately their inbound and outbound mail accounts. The concept is often quite confusing to inexperienced users. Some clients have therefore started proposing per-provider account creation wizards which only require users to fill in a user name and a password and then "fill in" the rest according to the setup of the specific provider.
The above workaround is of course non-existent for average and small size providers, and it requires an extra effort from application developers that is clearly avoidable.
The following sections of this document briefly discuss simple ways of addressing the issue.

---

2. Simply stating it ...

TOC

One relatively simple way of making sure that a URI and a password would be enough to connect to a SIP+XMPP service would consist in allowing clients to make the following assumptions:

- after applying the standard XMPP and SIP discovery mechanisms using the supplied URI (i.e. looking up the corresponding SRV DNS records), the client would discover the XMPP and SIP servers that should be used for the newly configured XMPP+SIP account.

- The supplied URI and password could be used as authentication credentials for both the XMPP and the SIP service.

Needless to say, clients may provide mechanisms (e.g. an "Advanced Configuration" form) that allow users to override the above assumptions

and explicitly specify different connection points with different sets of credentials.
The mechanism has the advantage of being relatively simple and require no other modifications to server side products other than making sure that user credentials would be valid for both the SIP and XMPP deployments. In many cases however, this would be resolvable through database synchronization and scripting, and hence be applicable to existing server-side implementations.

---

3. Using the domain in the auth header in SIP or XMPP

TOC

Participants in the related discussions on the DISPATCH mailing list also suggested using the "domain" parameter of the 'WWW-Authenticate' headers used in SIP authentication challenges. If present such a "domain" parameter may be used as an indication that the target URI would allow XMPP connections with the same credentials.
The main advantage of this mechanism is the fact that it allows for a discovery phase that is completely decoupled from the one used by regular SIP and XMPP. This means that service providers could use one set of servers to handle standard SIP and XMPP and then direct users to different addresses for their SIP+XMPP services.
Contrary to the DNS-based mechanism however, relying on domain parameters is more likely to require implementation changes since it relies on the parameter being configurable. It hence represents more of a contradiction with the requirements that XMPP+SIP work was chartered with.
Other issues worth noting, are the reliance of this mechanism on authentication methods that support the domain parameter, and the fact that it adds a sequential dependency between the SIP and XMPP authentication procedures.

---

4. Security Considerations

TOC

1. PENDING

---

5. IANA Considerations

TOC

None.

---

6. Acknowledgments

TOC

Simo Veikkolainen, Markus Isomaki, Peter St. Andre, Roni Even, Scott Lawrence, Spencer Dawkins, and several others provided helpful feedback in the related discussion that took place on the DISPATCH mailing list.

---

7. Informative References

TOC

[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 (TXT).

Authors' Addresses

TOC

	Emil Ivov
	SIP Communicator
	Strasbourg 67000
	France
Email:	emcho@sip-communicator.org
	Enrico Marocco
	Telecom Italia
	Via G. Reiss Romoli, 274
	Turin 10148
	Italy
Email:	enrico.marocco@telecomitalia.it