Strengthening Trust in Jabber Technologies

Author: Peter Saint-Andre

Version: 1.0

Date: 2007-01-19

Table of Contents

1.0 Background

Jabber technologies, as formalized in the Extensible Messaging and Presence Protocol (XMPP), are a set of decentralized, open technologies for near-real-time messaging, presence, and streaming XML (now being extended to address multimedia signalling and other advanced use cases). In order to understand how to improve the security and trust characteristics of Jabber technologies, one needs to understand some of their key characteristics:

1. Jabber/XMPP is not a typical open-source project; because the Jabber community is centered on a wire protocol rather than a particular codebase, it consists of many open-source projects, freeware and shareware developers, and commercial software companies. The role of the XMPP Standards Foundation (XSF) is to define protocols through open debate and discussion, then encourage the implementation of those protocols by the many decentralized projects and companies in the Jabber community.

2. Jabber/XMPP technologies are also deployed in a highly decentralized fashion, typically in a client-server architecture that is quite similar to email (but also sometimes in a local mesh or peer-to-peer architecture through the use of zero-configuration networking). As a result, there is a large network of Jabber servers on the Internet, plus many servers operating behind firewalls on organizational intranets. However, few Jabber/XMPP servers are deployed in a high-security fashion (e.g., with non-self-signed certificiates).

3. The core Jabber/XMPP protocols underwent rigorous cross-area and security review within the Internet Engineering Task Force (IETF) in 2002-2004, resulting in a strong security profile through the use of Transport Layer Security (TLS) for channel encryption and Simple Authentication and Security Layer (SASL) for authentication. However, work remains to be done in extending XMPP to include end-to-end encryption, strong identity, server and endpoint reputation, and per-hop reliability.

2.0 Mission

The mission of the XMPP Standards Foundation (XSF) is to build an open, standardized, secure, feature-rich, widely-deployed, decentralized infrastructure for real-time communication and collaboration over the Internet.

For information about specific initiatives the XSF has identified to achieve those goals, refer to the XSF Roadmap.

3.0 Proposal

This proposal concentrates on ways to strengthen the security and trust characteristics of Jabber technologies, the open network of Jabber servers, and communication among Jabber clients. While future proposals may define ways to extend those achievements, baseline security is a higher priority and therefore is the focus of this proposal.

In particular, two projects are described herein:

1. Strengthening server trust by stimulating implementation and deployment of existing Jabber/XMPP protocols for encryption and strong authentication of client-to-server and server-to-server connections.

2. Strengthening endpoint trust by completing development, iteratively improving, and encouraging deployment of strong, easy-to-use end-to-end encryption technologies over the Jabber network.

These projects are described more fully below.

3.1 Channel Encryption and Server Authentication

Objective:

Stimulate implementation and deployment of existing Jabber/XMPP protocols for encryption and strong authentication of client-to-server and server-to-server connections.

Background:

The core Jabber protocols as formalized within the IETF contain support for Transport Layer Security (TLS) and subsequent use of the Simple Authentication and Security Layer (SASL) EXTERNAL mechanism. Several open-source and commercial server implementations conform to RFC 3920 in this regard, but not all server codebases support TLS and SASL. Furthermore, very few server deployments use proper (i.e., non-self-signed) certificates because of the expense of obtaining certificates from traditional certification authorities (for this reason, we have been actively involved in the CAcert project and in Q4 2006 deployed an intermediate certification authority under the auspices of StartCom). These implementation and deployment gaps need to be closed in order to build a more secure Jabber network.

Furthermore, this work will support our efforts to advance XMPP within the Internet Standards Process, since we must demonstrate multiple interoperable implementations in order for our specifications to move forward to Draft Standard. Since TLS and SASL interoperability was not fully demonstrated at the test event in July 2006, more testing is required. However, in-person testing is inconvenient (although productive), which is why the XSF is working to set up a private network for Internet-based interoperability testing. This infrastructure will enable the Jabber/XMPP community to rapidly complete future testing efforts (and eventually also offer compliance certification).

Proposal:

Item	Description	Timing	Cost
Interop testing	Complete full interoperability testing of TLS and SASL between major client and server implementations via the emerging xmpp.org private testing network and at the second XMPP interop event in February 2007 (co-located with FOSDEM 2007), including testing of a wide range of server certificates (e.g., those issued by CAcert and StartCom)	February through April 2007	$1,000
Server implementations	Encourage complete implementation and release of TLS+SASL in major XMPP server implementations, mainly through incentives such as bounties and prizes	February through April 2007	$3,000
Client implementations	Define best practices for client handling of server certificates and encourage implementation of those best practices in major XMPP client implementations, mainly through incentives such as bounties and prizes	February through April 2007	$4,000
Library implementations	Encourage complete implementation and release of TLS+SASL in major XMPP library implementations (preferably at least one library in each popular language), mainly through incentives such as bounties and prizes	February through April 2007	$3,000
Total			$11,000

3.2 End-to-End Encryption

Objective:

Finish development, iteratively improve, and stimulate implementation and deployment of strong, easy-to-use end-to-end encryption technologies over the Jabber network.

Background:

The protocols developed in the early Jabber open-source community included a PGP-based extension for end-to-end encryption (XEP-0027), which contains some security holes and in any case was not widely deployed since few normal users have OpenPGP keys. When the IETF formalized the core Jabber protocols, the IETF's security reviewers requested definition of an end-to-end object encryption method based on S/MIME (RFC 3923). Unfortunately, this S/MIME technology is deeply unpopular among XMPP developers since it is not very "Jabberish" (it is the only XMPP protocol that uses MIME and it also requires a CPIM parser, none of which exist) and in fact has not been implemented in any Jabber client. Both the OpenPGP and S/MIME approaches require key or certificate management (which is difficult for end users), are based on an assumption of object encryption (which is appropriate for email but which does not take advantage of the real-time nature of XMPP), and do not ensure perfect forward secrecy (as does, for example, Off-the-Record Messaging or "OTR").

In order to move all of the XMPP RFCs forward, we need to demonstrate a widely implemented and interoperable method of end-to-end encryption. To ensure the security of XMPP communications, we need an end-to-end encryption technology that is actually deployable and preferably easy to use, so that an end user can simply click a button and have it set up between the clients with no end user interaction. This means using client-generated RSA keys and opportunistic in-stream negotiation (à la SSH), as is done in OTR. Unfortunately, OTR as defined and deployed in Gaim and Adium encrypts only the plaintext message body and does not enable encryption of full XMPP stanzas, which is essential for full end-to-end encryption of, say, Jingle signalling traffic. The Encrypted Sessions protocol (XEP-0116 and related specifications) appears to be the approach most likely to succeed, but we will not know unless we implement it, test it, and have it reviewed by a knowledgeable security expert. Therefore, finalization, security review, implementation, testing, and deployment of the Encrypted Sessions technology will be a high priority for the XMPP Standards Foundation over the next 12 months.

Proposal:

Item	Description	Timing	Cost
Protocol development	Complete initial stable version of Encrypted Sessions specifications	January through February 2007	$2,000
Security review	Sponsor an independent security review of Encryption Sessions specifications	February through March 2007	$8,000
Client implementations	Encourage implementation of initial stable protocol version in major XMPP client implementations, mainly through incentives such as bounties and prizes	February through through June 2007	$8,000
Library implementations	Encourage implementation of initial stable protocol version in major XMPP library implementations, mainly through incentives such as bounties and prizes	February through June 2007	$6,000
Initial interop testing	Complete initial interoperability testing of encrypted sessions between major client implementations via online testing	June through August 2007	$2,000
Iterations	Based on results of interop testing and security review, iteratively improve speficiations and sponsor modifications to implementations	August through September 2007	$3,000
Final interop testing	Complete final interoperability testing of encrypted sessions between major client implementations	October 2007	$2,000
Total			$31,000

4.0 Oversight and Reporting

The XMPP Standards Foundation (XSF) shall report its progress on a monthly basis and shall maintain a public status page for each project. Overall project management shall be directed by Peter Saint-Andre (Executive Director of the XSF) and shall be run under the oversight of the XSF's Board of Directors, which currently consists of Alexander Gnauck, Mickaël Rémond, and Matt Tucker (Chair).

5.0 Cost Summary

Item	Cost
Cost of projects	$42,000
XSF administration/oversight (10%)	$4,200
Total	$46,200

6.0 Major Open-Source Implementations

Appendix A: Server Implementations

For purposes of this document, "major open-source server implementations" are stipulated to be the following:

- ejabberd
- jabberd 1.4
- Wildfire

Additional server implementations may be added to the foregoing list, and unlisted projects still may be eligible for incentives.

Appendix B: Client Implementations

For purposes of this document, "major open-source client implementations" are stipulated to be the following:

- Adium
- Coccinella
- Exodus
- Gaim
- Gajim
- Gossip
- Kopete
- Psi

Additional client implementations may be added to the foregoing list, and unlisted projects still may be eligible for incentives.

Appendix C: Library Implementations

For purposes of this document, "major open-source library implementations" are stipulated to be the following:

- gloox (C++)
- iksemel (C)
- Jabber-Net (C#)
- JSO (Java)
- libstrophe (C)
- Loudmouth (C)
- Net::XMPP (Perl)
- PyXMPP (Python)
- Smack (Java)
- Twisted Words (Python)
- xmpppy (Python)

Additional library implementations may be added to the foregoing list, and unlisted projects still may be eligible for incentives.

END