Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 17, 2014
P. Saint-Andre
&yet
T. Alkemade
February 13, 2014

STRINT Workshop Position Paper: Strengthening the Extensible Messaging and Presence Protocol (XMPP)
draft-saintandre-strint-workshop-xmpp-02

Abstract

This document describes existing and potential future efforts at strengthening the Extensible Messaging and Presence Protocol (XMPP), for discussion at the W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Extensible Messaging and Presence Protocol (XMPP) [RFC6120] (along with its precursor, the so-called "Jabber protocol") has been used since 1999 for instant messaging(IM), presence, and other forms of near-real-time communication.

XMPP has a distributed client-server architecture, with one hop from a client to a server and one hop between any two servers, for a total of at most three hops on the communication path from a given client to another client. Although XMPP has supported per-hop channel encryption using Transport Layer Security (TLS) [RFC5246] since 2004 through a STARTTLS upgrade mechanism on the standard XMPP ports (with a hardcoded TLS-only port for the client-to-server hop since 1999), in practice TLS has not been universally deployed for operational reasons. In the last few months, operators of XMPP services have been working to deploy TLS more widely, and those efforts are summarized in this document.

Given the client-server architecture of XMPP, per-hop encryption using TLS does not protect messages inside the application servers that are used for routing. Therefore, various efforts have been made to provide end-to-end object encryption for the payloads of XMPP "stanzas". To put it mildly, these efforts have been less than completely successful. This document also summarizes the state of end-to-end encryption for XMPP.

2. Terminology

Various security-related terms are to be understood in the sense defined in [RFC4949].

3. Per-Hop Encryption

As mentioned, XMPP includes the ability to protect each hop in a communication path using Transport Layer Security (TLS). Although per-hop encryption does not protect XMPP payloads from attacks against XMPP servers (since absent end-to-end encryption the payloads would still be cleartext within the servers), it does protect against eavesdropping on the relevant XML streams. Because eavesdropping on unprotected XML streams would reveal personally identifying information such as a user's contact list (which in XMPP is stored on the server) and the intended recipients of a user's messages, protecting all the hops in a communication path is critically important for maintaining the privacy and security of XMPP-based interactions.

Until recently, client-to-server streams were widely protected on the XMPP network, but server-to-server streams were not. This state of affairs has had many causes:

- The lack of TLS protection was not as visible to end users or server administrators.

- Several major XMPP services did not offer or negotiate TLS over server-to-server streams.

- Deployment of proper certificates for authenticated encryption is operationally impossible in multi-tenanted environments.

The last item deserves some explanation. Many instant messaging clients "hardcode" the connection hosts for multi-tenanted domains. For example, if the XMPP service for example.com is serviced by hosting.example.net (and example.net is a large enough service provider), many IM clients will provide a "wizard" interface that enables the end user to choose "example.net" as a service type or provider when configuring an account. As a result, the client software will hide the security details of the connection to example.com and override identity mismatches of the kind otherwise forbidden by the security considerations of the core XMPP specification [RFC6120] and the "CertID" specification [RFC6125]. However, because these overrides are not applied on server-to-server streams, many existing implementations and deployments do not even attempt TLS negotiation for server-to-server streams.

Although a technology like DANE/DNSSEC (see [I-D.ietf-dane-srv]) or POSH/HTTPS (see [I-D.ietf-xmpp-posh] and [I-D.ietf-xmpp-dna]) would provide means to overcome the operational limitations of authenticated encryption, neither is yet widely deployed. Thus, in practice, when server-to-server streams are being protected often the technology used is unauthenticated encryption via TLS and the XMPP Server Dialback extension [XEP-0220].

In late 2013, a number of service operators in the XMPP community committed to mandating encryption on all hops under their control, and a number of software developers committed to supporting the features needed to make such encryption possible. The goal is to enable such encryption permanently on May 19, 2014. So far, one test day has been held (on January 4, 2014) and another test day will be held (on February 22, 2014) before the date of the STRINT workshop. The test day revealed bugs in several XMPP software implementations and prompted security improvements at a number of deployed services.

Also helpful has been the "IM Observatory" site at [1]. Most IM clients allow end users to inspect their connection to determine whether it is encrypted or not. However, users cannot easily determine the status of the other hops on the path to a user on a different server. Thus the IM Observatory has multiple goals: to give end users a tool with which they can examine the security of the entire end-to-end path, to give service operators information about improvements they can make to their servers' security, and to give all XMPP developers helpful statistics about the entire network.

4. End-to-End Encryption

The XMPP community has experimented with a significant number of end-to-end encryption technologies, including OpenPGP [XEP-0027], S/MIME [RFC3923], SIGMA [XEP-0116], end-to-end TLS [I-D.meyer-xmpp-e2e-encryption], XML encryption (never publicly documented), CMS with JOSE formats [I-D.miller-xmpp-e2e], and Off-the-Record (OTR) Messaging [2]. Unfortunately, none of these technologies has been formalized through a standards development organization. However OTR is the most widely implemented.

5. IANA Considerations

This document requests no actions of the IANA.

6. Security Considerations

This entire document discusses security.

7. References

7.1. Normative References

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

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

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

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

7.2. Informative References

[I-D.ietf-dane-srv] Finch, T., Miller, M., and P. Saint-Andre, "Using DNS-Based Authentication of Named Entities (DANE) TLSA records with SRV and MX records.", draft-ietf-dane-srv-04 (work in progress), February 2014.

[I-D.ietf-xmpp-dna] Saint-Andre, P. and M. Miller, "Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)", draft-ietf-xmpp-dna-05 (work in progress), February 2014.

[I-D.ietf-xmpp-posh] Miller, M. and P. Saint-Andre, "PKIX over Secure HTTP (POSH)", draft-ietf-xmpp-posh-00 (work in progress), February 2014.

[I-D.meyer-xmpp-e2e-encryption] Meyer, D. and P. Saint-Andre, "XTLS: End-to-End Encryption for the Extensible Messaging and Presence Protocol (XMPP) Using Transport Layer Security (TLS)", draft-meyer-xmpp-e2e-encryption-02 (work in progress), June 2009.

[I-D.miller-xmpp-e2e]
Miller, M., "End-to-End Object Encryption and Signatures for the Extensible Messaging and Presence Protocol (XMPP)", draft-miller-xmpp-e2e-06 (work in progress), June 2013.

[RFC3923] Saint-Andre, P., "End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)", RFC 3923, October 2004.

[XEP-0027]
Muldowney, T., "Current Jabber OpenPGP Usage", XSF XEP 0027, November 2006.

[XEP-0116]
Paterson, I., Saint-Andre, P., and D. Smith, "Encrypted Session Negotiation", XSF XEP 0116, May 2007.

[XEP-0220]
Miller, J., Saint-Andre, P., and P. Hancke, "Server Dialback", XSF XEP 0220, September 2013.

7.3. URIs

[1] https://xmpp.net/

[2] https://otr.cypherpunks.ca/

Authors' Addresses

Peter Saint-Andre
&yet

Email: ietf@stpeter.im

Thijs Alkemade

Email: me@thijsalkema.de