Network Working Group
Internet-Draft
Updates: 6120 (if approved)
Intended status: Standards Track
Expires: September 5, 2014

P. Saint-Andre
&yet
T. Alkemade

March 4, 2014

Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)

draft-saintandre-xmpp-tls-06

Abstract

This document provides recommendations for the use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP). This document updates RFC 6120.

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 used Transport Layer Security (TLS) [RFC5246] (along with its precursor, Secure Sockets Layer or SSL) since 1999. Both [RFC6120] and its predecessor [RFC3920] provided recommendations regarding the use of TLS in XMPP. In order to address the evolving threat model on the Internet today (see, for example, [I-D.trammell-perpass-ppa]), this document provides stronger recommendations (see also [I-D.sheffer-tls-bcp]). This document updates [RFC6120].

2. Terminology

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

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Discussion Venue

The discussion venue for this document is the mailing list of the XMPP Working Group, for which archives and subscription information can be found at [1]. Discussion might also occur on the mailing list of the UTA Working Group, for which archives and subscription information can be found at [2].

4. Recommendations

4.1. Support for TLS

Support for TLS (specifically, the XMPP profile of STARTTLS) is mandatory for XMPP implementations, as already specified in [RFC6120] and its predecessor [RFC3920].

If the server to which an XMPP client or peer server connects does not offer a stream feature of <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/> (thus indicating that it is an XMPP 1.0 server that supports TLS), the initiating entity MUST NOT proceed with the stream negotiation and MUST instead abort the connection attempt. Although XMPP servers SHOULD include the <required/> child element to indicate that negotiation of TLS is mandatory, clients and peer servers MUST NOT depend on receiving the <required/> flag in determining whether TLS will be enforced for the stream.

4.2. Protocol Versions

Implementations MUST follow the recommendations in [I-D.sheffer-tls-bcp] as to supporting various TLS versions and avoiding fallback to SSL.

4.3. Cipher Suites

Implementations MUST follow the recommendations in [I-D.sheffer-tls-bcp].

4.4. Public Key Length

Implementations MUST follow the recommendations in [I-D.sheffer-tls-bcp].

4.5. Compression

Implementations MUST follow the recommendations in [I-D.sheffer-tls-bcp].

XMPP supports an application-layer compression technology [XEP-0138], which might have slightly stronger security properties than TLS (at least because it is enabled after SASL authentication, as described in [XEP-0170]).

4.6. Session Resumption

Implementations MUST follow the recommendations in [I-D.sheffer-tls-bcp].

Use of session IDs [RFC5246] is RECOMMENDED instead of session tickets [RFC5077], since XMPP does not in general use state management technologies such as tickets or "cookies" [RFC6265].

Note that, in XMPP, TLS session resumption can be used in concert with the XMPP Stream Management extension; see [XEP-0198] for further details.

4.7. Authenticated Connections

Both the core XMPP specification [RFC6120] and the "CertID" specification [RFC6125] provide recommendations and requirements for certificate validation in the context of authenticated connections. This document does not supersede those specifications. Wherever possible, it is best to prefer authenticated connections (along with SASL [RFC4422]), as already stated in the core XMPP specification [RFC6120]. In particular, clients MUST authenticate servers.

4.8. Unauthenticated Connections

Given the pervasiveness of passive eavesdropping, even an unauthenticated connection might be better than an unencrypted connection (this is similar to the "better than nothing security" approach for IPsec [RFC5386]). In particular, because of current deployment challenges for authenticated connections between XMPP servers (see [I-D.ietf-xmpp-dna] for details), it might be reasonable for XMPP server implementations to accept unauthenticated connections when the Server Dialback protocol [XEP-0220] is used for weak identity verification; this will at least enable encryption of server-to-server connections. Unauthenticated connections include connections negotiated using anonymous Diffie-Hellman algorithms or using self-signed certificates, among other scenarios.

4.9. Server Name Indication

Although there is no harm in supporting the TLS Server Name Indication (SNI) extension [RFC6066], this is not necessary since the same function is served in XMPP by the 'to' address of the initial stream header as explained in Section 4.7.2 of [RFC6120].

4.10. Human Factors

It is RECOMMENDED that XMPP clients provide ways for end users (and that XMPP servers provide ways for administators) to complete the following tasks:

- o Determine if a client-to-server or server-to-server connection is encrypted and authenticated.
- o Determine the version of TLS used for a client-to-server or server-to-server connection.
- o Inspect the certificate offered by an XMPP server.
- o Determine the cipher suite used to encrypt a connection.
- o Be warned if the certificate changes for a given server.

5. Implementation Notes

Some governments enforce legislation prohibiting the export of strong cryptographic technologies. Nothing in this document ought to be taken as advice to violate such prohibitions.

6. IANA Considerations

This document requests no actions of the IANA.

7. Security Considerations

As noted in "A Threat Model for Pervasive Passive Surveillance" [I-D.trammell-perpass-ppa]), the use of TLS can help limit the information available for correlation to the network and transport layer headers as opposed to the application layer. As typically deployed, XMPP technologies do not leave application-layer routing data (such as XMPP 'to' and 'from' addresses) at rest on intermediate systems, since there is only one hop between any two given XMPP servers. As a result, encrypting all hops (sending client to sender's server, sender's server to recipient's server, recipient's server to recipient's client) can help to limit the amount of "metadata" that might leak.

It is possible that XMPP servers themselves might be compromised. In that case, per-hop encryption would not protect XMPP communications, and even end-to-end encryption of (parts of) XMPP stanza payloads would leave addressing information and XMPP roster data in the clear. By the same token, it is possible that XMPP clients (or the end-user devices on which such clients are installed) could also be compromised, leaving users utterly at the mercy of an adversary.

This document, along with actions currently being taken to strenthen the security of the XMPP network, do not assume widespread compromise of XMPP servers and clients or their underlying operating systems or hardware. Thus it is assumed that ubiquitous use of per-hop TLS channel encryption and more significant deployment of end-to-end object encryption technologies will serve to protect XMPP communications to a measurable degree, compared to the alternatives.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, January 2008.

[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.

8.2. Informative References

[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.sheffer-tls-bcp]
Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of TLS and DTLS", draft-sheffer-tls-bcp-02 (work in progress), February 2014.

[I-D.trammell-perpass-ppa]
Trammell, B., Borkmann, D., and C. Huitema, "A Threat Model for Pervasive Passive Surveillance", draft-trammell-perpass-ppa-01 (work in progress), November 2013.

[RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, October 2004.

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

[RFC5386] Williams, N. and M. Richardson, "Better-Than-Nothing Security: An Unauthenticated Mode of IPsec", RFC 5386, November 2008.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, April 2011.

[XEP-0138]
Hildebrand, J. and P. Saint-Andre, "Stream Compression", XSF XEP 0138, May 2009.

[XEP-0170]
Saint-Andre, P., "Recommended Order of Stream Feature Negotiation", XSF XEP 0170, January 2007.

[XEP-0198]
Karneges, J., Saint-Andre, P., Hildebrand, J., Forno, F., Cridland, D., and M. Wild, "Stream Management", XSF XEP 0198, June 2011.

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

8.3. URIs

[1] https://www.ietf.org/mailman/listinfo/xmpp

[2] https://www.ietf.org/mailman/listinfo/uta

Appendix A. Acknowledgements

Thanks to the following individuals for their input: Dave Cridland, Philipp Hancke, Olle Johansson, Steve Kille, Tobias Markmann, Matt Miller, and Rene Treffer.

Authors' Addresses

Peter Saint-Andre
&yet

Email: ietf@stpeter.im

Thijs Alkemade

Email: me@thijsalkema.de