Network Working Group   P. Saint-Andre
Internet-Draft   &yet
Updates: 6120 (if approved)   T. Alkemade
Intended status: Standards Track
Expires: October 16, 2015   April 14, 2015

Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)
draft-ietf-uta-xmpp-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, this document provides stronger recommendations.

In particular, this document updates [RFC6120] by specifying that XMPP implementations and deployments MUST follow the best current practices documented in the "Recommendations for Secure Use of TLS and DTLS" [I-D.ietf-uta-tls-bcp]. This includes stronger recommendations regarding SSL/TLS protocol versions, fallback to lower versions, TLS-layer compression, TLS session resumption, cipher suites, public key lengths, forward secrecy, and other aspects of using TLS with XMPP.

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. Recommendations

The best current practices documented in the "Recommendations for Secure Use of TLS and DTLS" [I-D.ietf-uta-tls-bcp] are included here by reference. Instead of repeating those recommendations here, this document mostly provides supplementary information regarding secure implementation and deployment of XMPP technologies.

3.1. 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].

The server (i.e., the XMPP receiving entity) to which a client or peer server (i.e., the XMPP initiating entity) connects might not offer a stream feature of <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>. Although in general this stream feature indicates that the server supports XMPP 1.0 and therefore supports TLS, that this stream feature might be stripped out by an attacker (see Section 2.1 of [RFC7457]). Similarly, the <required/> child element of the <starttls/> stream feature is used to indicate that negotiation of TLS is mandatory, but could also be stripped out by an attacker. Therefore, the initiating entity MUST NOT be deterred from attempting TLS negotiation even if the receiving entity does not advertise support for TLS. Instead, the initiating entity SHOULD (based on local policy) proceed with the stream negotiation and attempt to negotiate TLS.

3.2. Compression

XMPP supports an application-layer compression technology [XEP-0138]. Although this XMPP extension might have slightly stronger security properties than TLS-layer compression (since it is enabled after SASL authentication, as described in [XEP-0170]), this document neither encourages nor discourages use of XMPP-layer compression.

3.3. Session Resumption

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

3.4. 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 (e.g., it does

not modify the recommendations in [RFC6120] regarding the Subject Alternative Names or other certificate details that need to be supported for authentication of XMPP connections using PKIX certificates).

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 and servers MUST authenticate clients.

This document does not mandate that servers need to authenticate peer servers, although such authentication is strongly preferred and servers SHOULD authenticate each other. Unfortunately, in multi-tenanted environments it can be extremely difficult to obtain and deploy PKIX certificates with the proper Subject Alternative Names (see [I-D.ietf-xmpp-dna] and [I-D.ietf-xmpp-posh] for details). To overcome that difficulty, the Domain Name Associations (DNA) specification [I-D.ietf-xmpp-dna] describes a framework for XMPP server authentication methods, which include not only PKIX but also DNS-Based Authentication of Named Entities (DANE) as defined in [I-D.ietf-dane-srv] and PKIX over Secure HTTP (POSH) as defined in [I-D.ietf-xmpp-posh]. These methods can provide a basis for server identity verification when appropriate PKIX certificates cannot be obtained and deployed.

Given the pervasiveness of eavesdropping [RFC7258], even an unauthenticated connection might be better than an unencrypted connection in these scenarios (this is similar to the "better than nothing security" approach for IPsec [RFC5386]). Unauthenticated connections include connections negotiated using anonymous Diffie-Hellman mechanisms or using self-signed certificates, among others. In particular for XMPP server-to-server interactions, it can be reasonable for XMPP server implementations to accept unauthenticated but encrypted connections when Server Dialback keys [XEP-0220] are used; such keys on their own provide only weak identity verification (made stronger through the use of DNSSEC [RFC4033]), but this at least enables encryption of server-to-server connections. The DNA prooftypes described above are intended to mitigate the residual need for unauthenticated connections in these scenarios.

3.5. 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].

3.6. Human Factors

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

- o Determine if a given incoming or outgoing XML stream is encrypted using TLS.
- o Determine the version of TLS used for encryption of a given stream.
- o If authenticated encryption is used, determine how the connection was authenticated or verified (e.g., via PKI, DANE, POSH, or Server Dialback).
- 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.

4. IANA Considerations

This document requests no actions of the IANA.

5. Security Considerations

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 (sender's 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 and related actions to strengthen the security of the XMPP network are based on the assumption that XMPP servers and

clients have not been subject to widespread compromise. If this assumption is valid, then 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.

This document covers only communication over the XMPP network and does not take into account gateways to non-XMPP networks. As an example, for security considerations related to gateways between XMPP and the Session Initiation Protocol (SIP) see [RFC7247] and [I-D.ietf-stox-im].

6. References

6.1. Normative References

[I-D.ietf-uta-tls-bcp]
Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of TLS and DTLS", draft-ietf-uta-tls-bcp-11 (work in progress), February 2015.

[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.

[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.

6.2. 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-12 (work in progress), March 2015.

[I-D.ietf-stox-im]
Saint-Andre, P., Houri, A., and J. Hildebrand, "Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Instant Messaging", draft-ietf-stox-im-13 (work in progress), March 2015.

[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-10 (work in progress), March 2015.

[I-D.ietf-xmpp-posh]
Miller, M. and P. Saint-Andre, "PKIX over Secure HTTP (POSH)", draft-ietf-xmpp-posh-04 (work in progress), February 2015.

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

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[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.

[RFC7247] Saint-Andre, P., Houri, A., and J. Hildebrand, "Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Architecture, Addresses, and Error Handling", RFC 7247, May 2014.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, May 2014.

[RFC7457] Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", RFC 7457, February 2015.

[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.

Appendix A. 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.

Appendix B. Acknowledgements

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

Roni Even caught several important issues in his review on behalf of the General Area Review Team.

Thanks to Leif Johansson and Orit Levin as chairs of the UTA WG, Ben Campbell and Joe Hildebrand as chairs of the XMPP WG, and Stephen Farrell as the sponsoring Area Director.

Authors' Addresses

Peter Saint-Andre
&yet

Email: peter@andyet.com
URI: https://andyet.com/

Thijs Alkemade

Email: me@thijsalkema.de