Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 13, 2014

P. Saint-Andre
Cisco Systems, Inc.

September 9, 2013

Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP) draft-saintandre-xmpp-tls-00

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.

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. Given the evolving threat model on the Internet today (see, for example, [I-D.trammell-perpass-ppa]), it is necessary to provide 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 <https://www.ietf.org/mailman/listinfo/xmpp>.

4. Recommendations

4.1. Protocol Versions

XMPP implementations MUST NOT negotiate SSL version 2 [RFC6176].

XMPP implementations MUST NOT negotiate SSL version 3.

XMPP implementations MUST support, and prefer to negotiate, TLS version 1.2 [RFC5246].

XMPP implementations MAY negotiate TLS version 1.1 [RFC4346].

XMPP implementations MAY negotiate TLS version 1.0 [RFC2246].

4.2. Ciphersuites

XMPP implementations MUST NOT negotiate RC4 ciphersuites [I-D.popov-tls-prohibiting-rc4].

XMPP implementations MUST NOT negotiate ciphersuites that use so-called "export-level" encryption (including 40-bit and 56-bit algorithms).

XMPP implementations MUST NOT negotiate ciphersuites that use less than 128-bit algorithms.

XMPP implementations SHOULD prefer ciphersuites that use 256-bit algorithms or higher.

XMPP implementations MUST support, and SHOULD prefer to negotiate, ciphersuites that offer perfect forward secrecy, such as those in the "EDH", "DHE", and "ECDH" families.

5. Open Issues

This document has the following open issues:

- Add information about the rationale for each recommendation, perhaps in an appendix.
- Recommend a specific ciphersuite or a small number of ciphersuites?
- Provide recommendations regarding key lengths?
- Discuss TLS compression vs. application-layer compression?

6. IANA Considerations

This document requests no actions of the IANA.

7. Security Considerations

This entire document discusses security.

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.

[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.

[RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, March 2011.

8.2. Informative References

[I-D.popov-tls-prohibiting-rc4]
Popov, A., "Prohibiting RC4 Cipher Suites", draft-popov-tls-prohibiting-rc4-00 (work in progress), August 2013.

[I-D.sheffer-tls-bcp]
Sheffer, Y., "Recommendations for Secure Use of TLS and DTLS", draft-sheffer-tls-bcp-00 (work in progress), September 2013.

[I-D.trammell-perpass-ppa]
Trammell, B., "The Perfect Passive Adversary: A Threat Model for the Evaluation of Protocols under Pervasive Surveillance", draft-trammell-perpass-ppa-00 (work in progress), September 2013.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

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

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

Author's Address

Peter Saint-Andre
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
USA

Phone: +1-303-308-3282
Email: psaintan@cisco.com