Network Working Group
Internet-Draft
Intended status: BCP
Expires: March 12, 2014

Y. Sheffer
Porticor

September 8, 2013

Recommendations for Secure Use of TLS and DTLS
draft-sheffer-tls-bcp-00

Abstract

Over the last few years there have been several serious attacks on TLS, including attacks on its most commonly used ciphers and modes of operation. This document offers recommendations on securely using the TLS and DTLS protocols, given existing standards and implementations.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 12, 2014.

Table of Contents

1. Introduction

Over the last few years there have been several major attacks on TLS [RFC5246], including attacks on its most commonly used ciphers and modes of operation. Details are given in Section 2, but suffice it to say that both AES-CBC and RC4, which together make up for most current usage, have been seriously attacked in the context of TLS.

Given these issues, there is need for IETF guidance on how TLS can be used securely. Unlike most IETF documents, this is guidance for deployers rather than for implementers. In fact the recommendations below call for the use of widely implemented algorithms, which are not seeing widespread use today.

This recommendation applies to both TLS and DTLS. TLS 1.3, when it is standardized and deployed in the field, should resolve the current vulnerabilities while providing significantly better functionality, and will very likely obsolete the current document.

1.1. Conventions used in this document

[[Are we normative? This section might go away.]]

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

2. Attacks on TLS

This section lists the attacks that motivated the current recommendation. This is not intended to be an extensive survey of TLS's security.

While there are widely deployed mitigations for some of the attacks listed below, we believe that their root causes necessitate a more systemic solution.

2.1. BEAST

The BEAST attack [BEAST] uses issues with the TLS 1.0 implementation of CBC (that is, predictable IV) to decrypt parts of a packet, and specifically shows how this can be used to decrypt HTTP cookies when run over TLS.

2.2. Lucky Thirteen

A consequence of the MAC-then-encrypt design is the existence of padding oracle attacks [Padding-Oracle]. A recent incarnation of these attacks is the Lucky Thirteen attack [CBC-Attack], a timing side-channel attack that allows the attacker to decrypt arbitrary ciphertext.

2.3. Attacks on RC4

The RC4 algorithm [RC4] has been used with TLS (and previously, SSL) for many years. Attacks have also been known for a long time, e.g. [RC4-Attack-FMS]. But recent attacks [RC4-Attack] have weakened this algorithm even more. See [I-D.popov-tls-prohibiting-rc4] for more details.

2.4. Compression Attacks: CRIME and BREACH

The CRIME attack [CRIME] allows an active attacker to decrypt cyphertext (specifically, cookies) when TLS is used with protocol-level compression. The attack is a consequence of the TLS MAC-then-encrypt approach.

The BREACH attack [BREACH] makes similar use of HTTP-level compression which is much more prevalent than compression at the TLS level, to decrypt secret data passed in the HTTP response.

While the former attack can be mitigated by disabling TLS compression, we are not aware of mitigations at the protocol level to the latter attack, and so application-level mitigations are needed. For example, implementations of HTTP that use CSRF tokens will need to randomize them even when the recommendations of the current document are adopted.

[[Is it possible to affect some length hiding using TLS 1.2 as specified today, i.e. without draft-pironti-tls-length-hiding-01, and using available APIs?]]

3. Selection Criteria

Given the above attacks, we are proposing that deployers opt for a specific ciphersuite when negotiating TLS. We have used the following criteria when framing our recommendations:

- The ciphersuite must be secure in default use, and should not require any additional security measures beyond those defined in the standard.

- The ciphersuite must be widely implemented, i.e. available in a large percentage of popular cryptographic libraries.
- The ciphersuite must have undergone a significant amount of analysis, and the algorithm and mode of operation must both be standardized by relevant organizations.
- We prefer ciphersuites that provide client-side privacy and perfect forward secrecy, i.e. those that use ephemeral Diffie-Hellman.
- When there are multiple key sizes available, we have chosen the current industry standard, 128 bits of strength. Of course deployers are free to opt for a stronger ciphersuite.

4. Recommendations

Based on the criteria above, we recommend using as a preferred ciphersuite the following:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 [RFC5288]

It is noted that the above ciphersuite is an authenticated encryption (AEAD) algorithm [RFC5116], and therefore requires the use of TLS 1.2.

4.1. Details

We recommend that clients include this cipher suite as the first proposal to any server, unless they have prior knowledge that the server cannot respond to a TLS 1.2 client_hello message.

We recommend that servers prefer this ciphersuite (or a similar but stronger one) whenever it is proposed, even if it is not the first proposal.

Note that other profiles of TLS 1.2 exist that use different ciphersuites. For example, [RFC6460] defines a profile that uses the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ciphersuites.

5. Implementation Status

Since this document does not propose a new protocol or a new ciphersuite, we do not provide a full implementation status, as per [RFC6982]. However it is useful to list some known existing implementations of the recommended ciphersuite(s).

Category	Software	As Of Version	Comment
Library	OpenSSL	1.0.1	
	GnuTLS		
	NSS	3.11.1	
Browser	Internet Explorer	IE8 on Windows 7	
	Firefox		TBD
	Chrome		TBD
	Safari		TBD
Web server	Apache (mod_gnutls)	??	
	Apache (mod_ssl)	??	
	Nginx	1.0.9, 1.1.6	With a recent version of OpenSSL

6. Security Considerations

6.1. AES-GCM

Please refer to [RFC5246], Sec. 11 for general security considerations when using TLS 1.2, and to [RFC5288], Sec. 6 for security considerations that apply specifically to AES-GCM when used with TLS.

6.2. Downgrade Attacks

[[Do we need to disallow some protocol variants, e.g. SSL 3.0, so that there are no downgrade attacks possible?]]

7. IANA Considerations

This document requires no IANA actions.

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.

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

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, August 2008.

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.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

[RFC6460] Salter, M. and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 6460, January 2012.

[RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", RFC 6982, July 2013.

[CBC-Attack]
AlFardan, N. and K. Paterson, "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols", IEEE Symposium on Security and Privacy , 2013.

[BEAST] Rizzo, J. and T. Duong, "Browser Exploit Against SSL/TLS", 2011, <http://packetstormsecurity.com/files/105499/Browser-Exploit-Against-SSL-TLS.html>.

[CRIME] Rizzo, J. and T. Duong, "The CRIME Attack", EKOparty Security Conference 2012, 2012.

[BREACH] Prado, A., Harris, N., and Y. Gluck, "The BREACH Attack", 2013, <http://breachattack.com/>.

[RC4] Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Ed.", 1996.

[RC4-Attack-FMS]
Fluhrer, S., Mantin, I., and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Selected Areas in Cryptography , 2001.

[RC4-Attack]

ISOBE, T., OHIGASHI, T., WATANABE, Y., and M. MORII, "Full Plaintext Recovery Attack on Broadcast RC4", International Workshop on Fast Software Encryption , 2013.

[Padding-Oracle]
Vaudenay, S., ""Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS...", EUROCRYPT 2002, 2002, <http://www.iacr.org/cryptodb/archive/2002/EUROCRYPT/2850/2850.pdf>.

Appendix A. Appendix: Change Log

Note to RFC Editor: please remove this section before publication.

A.1. -00

- Initial version.

Author's Address

Yaron Sheffer
Porticor
29 HaHarash St.
Hod HaSharon 4501303
Israel

Email: yaronf.ietf@gmail.com