uta   Y. Sheffer
Internet-Draft   Porticor
Intended status: Informational   R. Holz
Expires: August 11, 2014   TUM
                                                        P. Saint-Andre
                                                                  &yet
                                                      February 7, 2014

Summarizing Current Attacks on TLS and DTLS
draft-sheffer-uta-tls-attacks-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 summarizes these attacks, with the goal of
   motivating generic and protocol-specific recommendations on the usage
   of TLS and DTLS.

Status of this Memo

Copyright Notice

include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

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.

   This situation motivated the creation of the UTA working group, which
   is tasked with the creation of generic and protocol-specific
   recommendation for the use of TLS and DTLS.

   "Attacks always get better; they never get worse" (ironically, this
   saying is attributed to the NSA). This list of attacks describes our
   knowledge as of this writing. It seems likely that new attacks will
   be invented in the future.

   For a more detailed discussion of the attacks listed here, the
   interested reader is referred to [Attacks-iSec].

1.1. Conventions used in this document

   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
   recommendations. 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, the predictable initialization vector) 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 in all current versions
   of TLS 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], [RC4-Attack-AlF]) 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 TIME attack [TIME] and the later BREACH attack [BREACH] both make similar use of HTTP-level compression to decrypt secret data passed in the HTTP response. We note that compression of the HTTP message body is much more prevalent than compression at the TLS level.

The former attack can be mitigated by disabling TLS compression, as recommended below. We are not aware of mitigations at the protocol level to the latter attack, and so application-level mitigations are needed (see [BREACH]). For example, implementations of HTTP that use CSRF tokens will need to randomize them even when the recommendations of [TBD] are adopted.

3. Security Considerations

This document describes protocol attacks in an informational manner, and in itself does not have any security implications. Its companion documents certainly do.

4. IANA Considerations

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

This document requires no IANA actions.

5. Acknowledgements

We would like to thank Stephen Farrell, Simon Josefsson, Yoav Nir,

Kenny Paterson, Patrick Pelletier, and Rich Salz for their review of
a previous version of this document.

The document was prepared using the lyx2rfc tool, created by Nico
Williams.

6. References

6.1. 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.

6.2. Informative References

   [I-D.popov-tls-prohibiting-rc4]
              Popov, A., "Prohibiting RC4 Cipher Suites",
              draft-popov-tls-prohibiting-rc4-01 (work in progress),
              October 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/>.

   [TIME]   Be'ery, T. and A. Shulman, "A Perfect CRIME? Only TIME
              Will Tell", Black Hat Europe 2013, 2013, <https://
              media.blackhat.com/eu-13/briefings/Beery/
              bh-eu-13-a-perfect-crime-beery-wp.pdf>.

   [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.

   [RC4-Attack-AlF]
             AlFardan, N., Bernstein, D., Paterson, K., Poettering, B.,
             and J. Schuldt, "On the Security of RC4 in TLS", Usenix
             Security Symposium 2013, 2013, <https://www.usenix.org/
             conference/usenixsecurity13/security-rc4-tls>.

   [Attacks-iSec]
             Sarkar, P. and S. Fitzgerald, "Attacks on SSL, a
             comprehensive study of BEAST, CRIME, TIME, BREACH, Lucky13
             and RC4 biases", 8 2013, <https://www.isecpartners.com/
             media/106031/ssl_attacks_survey.pdf>.

   [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

   o Initial version, extracted from draft-sheffer-tls-bcp-01.

Authors' Addresses

   Yaron Sheffer
   Porticor
   29 HaHarash St.
   Hod HaSharon 4501303
   Israel

   Email: yaronf.ietf@gmail.com

Ralph Holz
Technische Universitaet Muenchen
Boltzmannstr. 3
Garching 85748
Germany

Email: holz@net.in.tum.de

Peter Saint-Andre
&yet

Email: ietf@stpeter.im