

uta
Internet-Draft
Intended status: Informational
Expires: December 26, 2014

Y. Sheffer
Porticor
R. Holz
TUM
P. Saint-Andre
&yet
June 24, 2014

Summarizing Current Attacks on TLS and DTLS
draft-ietf-uta-tls-attacks-01

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

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 December 26, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

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	2
2.	Attacks on TLS	3
2.1.	SSL Stripping	3
2.2.	BEAST	3
2.3.	Lucky Thirteen	3
2.4.	Attacks on RC4	3
2.5.	Compression Attacks: CRIME and BREACH	4
2.6.	Certificate Attacks	4
2.7.	Diffe-Hellman Parameters	4
2.8.	Denial of Service	4
3.	Security Considerations	5
4.	IANA Considerations	5
5.	Acknowledgements	5
6.	References	5
6.1.	Normative References	5
6.2.	Informative References	5
Appendix A.	Appendix: Change Log	7
A.1.	draft-ietf-uta-tls-bcp-01	7
A.2.	draft-ietf-uta-tls-bcp-00	7
A.3.	draft-sheffer-uta-tls-bcp-00	7
	Authors' Addresses	8

[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](#)].

[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.](#) SSL Stripping

Various attacks attempt to remove the use of SSL/TLS altogether, by modifying HTTP traffic and HTML pages as they pass on the wire. These attacks are known collectively as SSL Stripping, and were first introduced by Moxie Marlinspike [[SSL-Stripping](#)]. In the context of Web traffic, these attacks are only effective if the client accesses a Web server using a mixture of HTTP and HTTPS.

[2.2.](#) 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 to decrypt HTTP cookies when HTTP is run over TLS.

[2.3.](#) 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.

[2.4.](#) Attacks on RC4

The RC4 algorithm [[RC4](#)] has been used with TLS (and previously, SSL) for many years. RC4 has long been known to have a variety of cryptographic weaknesses, e.g. [[RC4-Attack-Pau](#)], [[RC4-Attack-Man](#)], [[RC4-Attack-FMS](#)]. Recent cryptanalysis results [[RC4-Attack-ALF](#)] exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts.

These recent results are on the verge of becoming practically exploitable; currently they require 2^{26} sessions or 13×2^{30} encryptions. As a result, RC4 can no longer be seen as providing a sufficient level of security for TLS sessions.

[2.5.](#) Compression Attacks: CRIME and BREACH

The CRIME attack [[CRIME](#)] allows an active attacker to decrypt ciphertext (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 [[I-D.ietf-uta-tls-bcp](#)] are adopted.

[2.6.](#) Certificate Attacks

There have been several practical attacks on TLS when used with RSA certificates (the most common use case). These include [[Bleichenbacher98](#)] and [[Klima03](#)]. While the Bleichenbacher attack has been mitigated in TLS 1.0, the Klima attack that relies on a version-check oracle is only mitigated by TLS 1.1.

The use of RSA certificates often involves exploitable timing issues [[Brumley03](#)], unless the implementation takes care to explicitly eliminate them.

[2.7.](#) Diffie-Hellman Parameters

TLS allows to define ephemeral Diffie-Hellman and Elliptic Curve Diffie-Hellman parameters in its respective key exchange modes. This results in an outstanding attack, detailed in [[Cross-Protocol](#)]. In addition, clients that do not properly verify the received parameters are exposed to MITM attacks. Unfortunately the TLS protocol does not require this verification, see [[RFC6989](#)] for the IPsec analogy.

[2.8.](#) Denial of Service

Server CPU power has progressed over the years so that TLS can now be turned on by default. However the risk of malicious clients and coordinated groups of clients ("botnets") mounting denial of service attacks is still very real. TLS adds another vector for computational attacks, since a client can easily (with little computational effort) force the server to expend relatively large

computational work. It is known that such attacks have in fact been mounted.

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

This document requires no IANA actions.

5. Acknowledgements

We would like to thank Stephen Farrell, Simon Josefsson, Yoav Nir, Kenny Paterson, Patrick Pelletier, Tom Ritter and Rich Salz for their review of this document. We thank Andrei Popov for contributing text on RC4.

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

6. References

6.1. Normative References

[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.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-00](#) (work in progress), March 2014.
- [RFC6989] Sheffer, Y. and S. Fluhrer, "Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 6989](#), 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/>>.
- [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-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>>.
- [Cross-Protocol]
Mavrogiannopoulos, N., Vercauteren, F., Velichkov, V., and B. Preneel, "A cross-protocol attack on the TLS protocol", 2012, <<http://doi.acm.org/10.1145/2382196.2382206>>.

[RC4-Attack-Pau]

Paul, G. and S. Maitra, "Permutation after RC4 key scheduling reveals the secret key.", 2007, <<http://dblp.uni-trier.de/db/conf/sacrypt/sacrypt2007.html#PaulM07>>.

[RC4-Attack-Man]

Mantin, I. and A. Shamir, "A practical attack on broadcast RC4", 2001.

[SSL-Stripping]

Marlinspike, M., "SSL Stripping", February 2009, <<http://www.thoughtcrime.org/software/sslstrip/>>.

[Bleichenbacher98]

Bleichenbacher, D., "Chosen ciphertext attacks against protocols based on the RSA encryption standard pkcs1", 1998.

[Klima03] Klima, V., Pokorny, O., and T. Rosa, "Attacking RSA-based sessions in SSL/TLS", 2003.

[Brumley03]

Brumley, D. and D. Boneh, "Remote timing attacks are practical", 2003.

Appendix A. Appendix: Change Log

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

A.1. draft-ietf-uta-tls-bcp-01

- o Added SSL Stripping, attacks related to certificates, Diffie Hellman parameters and denial of service.
- o Expanded on RC4 attacks, thanks to Andrei Popov.

A.2. draft-ietf-uta-tls-bcp-00

- o Initial WG version, with only updated references.

A.3. draft-sheffer-uta-tls-bcp-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

