Overview[#](https://ldapwiki.com/wiki/TLS%20Compression#section-TLS+Compression-Overview)

TLS Compression as the name implies is Compression within [TLS](https://ldapwiki.com/wiki/TLS).

TLS Compression is [Deprecated](https://ldapwiki.com/wiki/Deprecated) in [TLS 1.3](https://ldapwiki.com/wiki/TLS%201.3)

[RFC 3749](https://ldapwiki.com/wiki/RFC%203749) describes Transport Layer Security Protocol Compression Methods.

[TLS](https://ldapwiki.com/wiki/TLS) has the ability to compress content prior to encryption. Compression does not protect against the [BEAST](https://ldapwiki.com/wiki/BEAST) attack, but it does make it more difficult.

Normally, the bytes sent by the attacker are encrypted and sent over the wire. With compression enabled, the bytes are first compressed, which means that the attacker no longer knows what exactly is encrypted. To make the attack work, the attacker would also have to guess the compressed bytes, which may be very difficult. For this reason, the original [BEAST](https://ldapwiki.com/wiki/BEAST) exploit implemented by Duong and Rizzo could not attack compressed TLS connections.

In some estimates, compression was enabled on about half of all web servers at the time [BEAST](https://ldapwiki.com/wiki/BEAST) was announced. However, client-side support for compression was very weak then and is nonexistent today

TLS Compression has been a target of several [Exploits](https://ldapwiki.com/wiki/Exploit) and generally it is considered that it should be disabled. [CRIME](https://ldapwiki.com/wiki/CRIME) ia a popular [Exploit](https://ldapwiki.com/wiki/Exploit) on TLS Compression and it has been stated that TLS Compression is dead and [CRIME](https://ldapwiki.com/wiki/CRIME) killed it.

More Information[#](https://ldapwiki.com/wiki/TLS%20Compression#section-TLS+Compression-MoreInformation)

There might be more information for this subject on one of the following:

* [CRIME](https://ldapwiki.com/wiki/CRIME)
* [ClientHello](https://ldapwiki.com/wiki/ClientHello)
* [RFC 3749](https://ldapwiki.com/wiki/RFC%203749)
* [Record Protocol](https://ldapwiki.com/wiki/Record%20Protocol)
* [TLS 1.3](https://ldapwiki.com/wiki/TLS%201.3)

CRIME

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/CRIME#mw-head)[Jump to search](https://en.wikipedia.org/wiki/CRIME#searchInput)

*For criminal activity, see*[*Crime*](https://en.wikipedia.org/wiki/Crime)*. For other uses, see*[*Crime (disambiguation)*](https://en.wikipedia.org/wiki/Crime_(disambiguation))*.*

**CRIME** (**Compression Ratio Info-leak Made Easy**) is a [security exploit](https://en.wikipedia.org/wiki/Security_exploit) against secret [web cookies](https://en.wikipedia.org/wiki/Web_cookie) over connections using the [HTTPS](https://en.wikipedia.org/wiki/HTTPS) and [SPDY](https://en.wikipedia.org/wiki/SPDY) protocols that also use [data compression](https://en.wikipedia.org/wiki/Data_compression).[[1]](https://en.wikipedia.org/wiki/CRIME#cite_note-fisher2012-09-13-1) When used to recover the content of secret [authentication cookies](https://en.wikipedia.org/wiki/Authentication_cookie), it allows an attacker to perform [session hijacking](https://en.wikipedia.org/wiki/Session_hijacking) on an authenticated web session, allowing the launching of further attacks. CRIME was assigned [CVE](https://en.wikipedia.org/wiki/CVE_(identifier))-[2012-4929](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4929).[[2]](https://en.wikipedia.org/wiki/CRIME#cite_note-2)



**Contents**

* [1Details](https://en.wikipedia.org/wiki/CRIME#Details)
* [2Prevention](https://en.wikipedia.org/wiki/CRIME#Prevention)
  + [2.1Mitigation](https://en.wikipedia.org/wiki/CRIME#Mitigation)
* [3BREACH](https://en.wikipedia.org/wiki/CRIME#BREACH)
* [4References](https://en.wikipedia.org/wiki/CRIME#References)

Details[[edit](https://en.wikipedia.org/w/index.php?title=CRIME&action=edit&section=1)]

The vulnerability exploited is a combination of [chosen plaintext attack](https://en.wikipedia.org/wiki/Chosen_plaintext_attack) and inadvertent [information leakage](https://en.wikipedia.org/wiki/Information_leakage) through data compression similar to that described in 2002 by the cryptographer [John Kelsey](https://en.wikipedia.org/wiki/John_Kelsey_(cryptanalyst)).[[3]](https://en.wikipedia.org/wiki/CRIME#cite_note-3) It relies on the attacker being able to observe the size of the [ciphertext](https://en.wikipedia.org/wiki/Ciphertext) sent by the [browser](https://en.wikipedia.org/wiki/Web_browser) while at the same time inducing the browser to make multiple carefully crafted web connections to the target site. The attacker then observes the change in size of the compressed request payload, which contains both the secret cookie that is sent by the browser only to the target site, and variable content created by the attacker, as the variable content is altered. When the size of the compressed content is reduced, it can be inferred that it is probable that some part of the injected content matches some part of the source, which includes the secret content that the attacker desires to discover. [Divide and conquer](https://en.wikipedia.org/wiki/Divide-and-conquer_algorithm) techniques can then be used to home in on the true secret content in a relatively small number of probe attempts that is a small multiple of the number of secret bytes to be recovered.[[1]](https://en.wikipedia.org/wiki/CRIME#cite_note-fisher2012-09-13-1)[[4]](https://en.wikipedia.org/wiki/CRIME#cite_note-4)

The CRIME exploit was hypothesized by Adam Langley,[[5]](https://en.wikipedia.org/wiki/CRIME#cite_note-5) and first demonstrated by the security researchers Juliano Rizzo and Thai Duong, who also created the [BEAST](https://en.wikipedia.org/wiki/Transport_Layer_Security#BEAST_attack) exploit.[[6]](https://en.wikipedia.org/wiki/CRIME#cite_note-goodin2012-09-13-6) The exploit was due to be revealed in full at the 2012 [ekoparty](https://en.wikipedia.org/wiki/Ekoparty" \o "Ekoparty) security conference.[[7]](https://en.wikipedia.org/wiki/CRIME#cite_note-7) Rizzo and Duong presented CRIME as a general attack that works effectively against a large number of protocols, including but not limited to SPDY (which always compresses request headers), TLS (which may compress records) and HTTP (which may compress responses).

Prevention[[edit](https://en.wikipedia.org/w/index.php?title=CRIME&action=edit&section=2)]

CRIME can be defeated by preventing the use of compression, either at the client end, by the browser disabling the compression of SPDY requests, or by the website preventing the use of data compression on such transactions using the protocol negotiation features of the TLS protocol. As detailed in *The Transport Layer Security (TLS) Protocol Version 1.2*,[[8]](https://en.wikipedia.org/wiki/CRIME#cite_note-8) the client sends a list of compression algorithms in its ClientHello message, and the server picks one of them and sends it back in its ServerHello message. The server can only choose a compression method the client has offered, so if the client only offers 'none' (no compression), the data will not be compressed. Similarly, since 'no compression' must be allowed by all TLS clients, a server can always refuse to use compression.

**Mitigation**[[edit](https://en.wikipedia.org/w/index.php?title=CRIME&action=edit&section=3)]

As of September 2012, the CRIME exploit against SPDY and TLS-level compression was described as mitigated in the then-latest versions of the [Chrome](https://en.wikipedia.org/wiki/Chrome_(web_browser)) and [Firefox](https://en.wikipedia.org/wiki/Firefox) web browsers.[[6]](https://en.wikipedia.org/wiki/CRIME#cite_note-goodin2012-09-13-6) Some websites have applied countermeasures at their end.[[9]](https://en.wikipedia.org/wiki/CRIME#cite_note-9) The [nginx](https://en.wikipedia.org/wiki/Nginx" \o "Nginx) web-server was not vulnerable to CRIME since 1.0.9/1.1.6 (October/November 2011) using [OpenSSL](https://en.wikipedia.org/wiki/OpenSSL) 1.0.0+, and since 1.2.2/1.3.2 (June / July 2012) using all versions of OpenSSL.[[10]](https://en.wikipedia.org/wiki/CRIME#cite_note-10)

Note that as of December 2013 the CRIME exploit against HTTP compression has not been mitigated at all.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Rizzo and Duong have warned that this vulnerability might be even more widespread than SPDY and TLS compression combined.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

BREACH[[edit](https://en.wikipedia.org/w/index.php?title=CRIME&action=edit&section=4)]

*Main article:*[*BREACH (security exploit)*](https://en.wikipedia.org/wiki/BREACH_(security_exploit))

At the August 2013 [Black Hat](https://en.wikipedia.org/wiki/Black_Hat_Briefings) conference, researchers Gluck, Harris and Prado announced a variant of the CRIME exploit against HTTP compression called [BREACH](https://en.wikipedia.org/wiki/BREACH_(security_exploit)) (short for Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext). It uncovers HTTPS secrets by attacking the inbuilt HTTP data compression used by webservers to reduce network traffic.[[11]](https://en.wikipedia.org/wiki/CRIME#cite_note-11)

References[[edit](https://en.wikipedia.org/w/index.php?title=CRIME&action=edit&section=5)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/CRIME#cite_ref-fisher2012-09-13_1-0) [***b***](https://en.wikipedia.org/wiki/CRIME#cite_ref-fisher2012-09-13_1-1) *Fisher, Dennis (September 13, 2012).*[*"CRIME Attack Uses Compression Ratio of TLS Requests as Side Channel to Hijack Secure Sessions"*](https://threatpost.com/crime-attack-uses-compression-ratio-tls-requests-side-channel-hijack-secure-sessions-091312/)*. ThreatPost. Retrieved September 13, 2012.*
  2. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-2) [*"CVE-2012-4929"*](https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2012-4929)*. [Mitre Corporation](https://en.wikipedia.org/wiki/Mitre_Corporation" \o "Mitre Corporation).*
  3. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-3) *Kelsey, J. (2002). "Compression and Information Leakage of Plaintext".*[*Fast Software Encryption*](https://www.iacr.org/cryptodb/data/paper.php?pubkey=3091)*. Lecture Notes in Computer Science.****2365****. pp. 263–276.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1007/3-540-45661-9\_21*](https://doi.org/10.1007%2F3-540-45661-9_21)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-3-540-44009-3*](https://en.wikipedia.org/wiki/Special:BookSources/978-3-540-44009-3)*.*
  4. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-4) [*"CRIME - How to beat the BEAST successor?"*](http://security.stackexchange.com/questions/19911/crime-how-to-beat-the-beast-successor/19914)*. StackExchange.com. September 8, 2012. Retrieved September 13,2012.*
  5. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-5) *Langley, Adam (August 16, 2011).*[*"Re: Compression contexts and privacy considerations"*](https://groups.google.com/d/msg/spdy-dev/B_ulCnBjSug/rcU-SIFtTKoJ)*. spdy-dev (Mailing list).*
  6. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/CRIME#cite_ref-goodin2012-09-13_6-0) [***b***](https://en.wikipedia.org/wiki/CRIME#cite_ref-goodin2012-09-13_6-1) *Goodin, Dan (September 13, 2012).*[*"Crack in Internet's foundation of trust allows HTTPS session hijacking"*](https://arstechnica.com/security/2012/09/crime-hijacks-https-sessions/)*. Ars Technica. Retrieved September 13, 2012.*
  7. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-7) *Rizzo, Juliano; Duong, Thai.*[*"The CRIME attack"*](https://docs.google.com/presentation/d/11eBmGiHbYcHR9gL5nDyZChu_-lCa2GizeuOfaLU2HOU/edit)*. Ekoparty. Retrieved September 21, 2012 – via Google Docs.*
  8. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-8) *Dierks, T.; Resorla, E. (August 2008).*[*"The Transport Layer Security (TLS) Protocol Version 1.2 - Appendix A.4.1 (Hello messages)"*](http://tools.ietf.org/html/rfc5246#appendix-A.4.1)*.*[*IETF*](https://en.wikipedia.org/wiki/IETF)*. Retrieved July 10, 2013.*
  9. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-9) *Leyden, John (September 14, 2012).*[*"The perfect CRIME? New HTTPS web hijack attack explained"*](https://www.theregister.co.uk/2012/09/14/crime_tls_attack/)*. The Register. Retrieved September 16, 2012.*
  10. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-10) *Sysoev, Igor (September 26, 2012).*[*"Nginx mailing list: crime tls attack"*](http://mailman.nginx.org/pipermail/nginx/2012-September/035600.html)*. nginx.org. Retrieved July 11, 2013.*
  11. [**^**](https://en.wikipedia.org/wiki/CRIME#cite_ref-11) *Goodin, Dan (August 1, 2013).*[*"Gone in 30 seconds: New attack plucks secrets from HTTPS-protected pages"*](https://arstechnica.com/security/2013/08/gone-in-30-seconds-new-attack-plucks-secrets-from-https-protected-pages/)*.*