

Kryptoanaliza stosowana 2025

Lista zadań nr 6a: podatności SSL/TLS (przegląd w postaci seminarium)

Na zajęcia 24 i 26 listopada 2025

Zadanie 1 (3 pkt). Wybierz z poniższej listy jedną z podatności SSL/TLS, zgłoś swój wybór w systemie SKOS i przygotuj 20-minutową prezentację omawiającą tę podatność.

- Sweet32
- SLOTH
- RC4 biases
- Lucky 13, Lucky microseconds
- BEAST
- POODLE, ZombiePoodle, GoldenDoodle
- Cross-protocol attack on DH parameters
- DROWN
- Truncation, Cookie Cutter
- Renegotiation attack
- CRIME, BREACH, HEIST
- Triple-handshake attack
- Selfie
- Frankencerts
- Heartbleed
- Inny, do uzgodnienia

Opis podatności znajdziesz w pracy: Douglas Stebila, *Attacks on TLS*, June 15, 2020, dołączonej do bieżącej listy.

Attacks on TLS

Douglas Stebila

Last updated: June 15, 2020

Target	Attack Name	Year	Reference
Core cryptography			
RSA PKCS#1v1.5 decryption	Side channel – Bleichenbacher	1998*, 2014	[12]*, [38]
DES	Weakness – brute force	1998	[21]
MD5	Weakness – collisions	2005	[33]
RC4	Weakness – biases	2000*, 2013,15	[24, 35]*, [4, 49, 34]
RSA export keys	FREAK	2015	[8]
DH export keys	Logjam	2015	[2]
RSA-MD5 signatures	SLOTH	2016	[11]
Triple-DES	Sweet32	2011*, 2016	[45]*, [10]
Crypto usage in ciphersuites			
CBC mode encryption	BEAST	2002*, 2011	[39]*, [20]
Diffie–Hellman parameters	Cross-protocol attack	1996*, 2012	[51]*, [37]
MAC-encode-encrypt padding	Lucky 13, Lucky microseconds	2013,15	[5, 3]
CBC mode encryption + padding	POODLE, ZombiePoodle, GoldenDoodle	2014,19	[40, ?]
TLS protocol functionality			
Support for old versions	Jager et al., DROWN	2015, 2016	[27, 6]
Negotiation	Downgrade to weak crypto	1996, 2015	[51, 8, 2]
Termination	Truncation, Cookie Cutter	2007,13,14	[7, 46, 9]
Renegotiation	Renegotiation attack	2009	[43]
Compression	CRIME, BREACH, HEIST	2002*, 2012,16	[28]*, [44, 42, 48]
Session resumption	Triple-handshake attack	2014	[9]
Pre-shared keys	Selfie [†]	2019	[19]
Implementation – libraries			
OpenSSL – RSA	Side-channel	2005, 2007	[41, 1]
Debian OpenSSL	Weak RNG	2008	[47]
OpenSSL – elliptic curve	Side-channel	2011–14	[15, 14, 52]
Apple – certificate validation	goto fail;	2014	[32]
OpenSSL – Heartbeat extension	Heartbleed	2014	[16, 17]
Multiple – certificate validation	Frankencerts	2014	[13]
NSS – RSA PKCS#1v1.5 signatures	BERserk (Bleichenbacher)	2006*, 2014	[23]*, [31]
Multiple – state machine	CCS injection, SMACK	2014, 2015	[29, 8]
GnuTLS – session resumption	High-STEKs [†]	2020	[30]
Implementation – HTTP-based applications			
Netscape	Weak RNG	1996	[26]
Multiple – certificate validation	“Most dangerous code”, MalloDroid	2012	[25, 22]
Application-level protocols			
HTTP	SSL stripping	2009	[36]
HTTP server virtual hosts	Virtual host confusion	2014	[18]
IMAP/POP/FTP	STARTTLS command injection	2011	[50]

* denotes theoretical basis for a later practical attack; [†] denotes TLS 1.3-specific attack.

References

- [1] O. Aciicmez, S. Gueron, and J.-P. Seifert. New branch prediction vulnerabilities in OpenSSL and necessary software countermeasures. In S. D. Galbraith, editor, *Cryptography and Coding*, volume 4887 of *LNCS*, pages 185–203. Springer, 2007.
- [2] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Z. Béguelin, and P. Zimmermann. Imperfect forward secrecy: How Diffie–Hellman fails in practice. In I. Ray, N. Li, and C. Kruegel, editors, *22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 5–17. ACM, 2015.
- [3] M. Albrecht and K. G. Paterson. Lucky microseconds: A timing attack on Amazon’s s2n implementation of TLS. In M. Fischlin and J.-S. Coron, editors, *Advances in Cryptology – Proc. Eurocrypt 2016*, volume 9665 of *LNCS*, pages 622–643. Springer, 2016.
- [4] N. J. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, and J. C. N. Schuldt. On the security of RC4 in TLS. In S. T. King, editor, *22th USENIX Security Symposium*, pages 305–320. USENIX Association, 2013.
- [5] N. J. AlFardan and K. G. Paterson. Lucky thirteen: Breaking the TLS and DTLS record protocols. In *34th IEEE Symposium on Security and Privacy*, pages 526–540. IEEE Computer Society, 2013.
- [6] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Käasper, S. Cohney, S. Engels, C. Paar, , and Y. Shavitt. DROWN: Breaking TLS using SSLv2. In *Proc. 25th USENIX Security Symposium*, 2016.
- [7] D. Berbecaru and A. Lioy. On the robustness of applications based on the SSL and TLS security protocols. In J. Lopez, P. Samarati, and J. L. Ferrer, editors, *4th European PKI Workshop (EUROPKI)*, volume 4582 of *Lecture Notes in Computer Science*, pages 248–264. Springer, 2007.
- [8] B. Beurdouche, K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, A. Pironti, P. Strub, and J. K. Zinzindohoue. A messy state of the union: Taming the composite state machines of TLS. In *36th IEEE Symposium on Security and Privacy*, pages 535–552. IEEE Computer Society, 2015.
- [9] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Pironti, and P.-Y. Strub. Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. In *35th IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2014. <https://secure-resumption.com/>.
- [10] K. Bhargavan and G. Leurent. On the practical (in-)security of 64-bit block ciphers – collision attacks on HTTP over TLS and OpenVPN. In *23rd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016.
- [11] K. Bhargavan and G. Leurent. Transcript collision attacks: Breaking authentication in TLS, IKE, and SSH. In *Network and Distributed System Security Symposium*. Internet Society, February 2016. <http://www.isoc.org/isoc/conferences/ndss/2016/proceedings/>.
- [12] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In H. Krawczyk, editor, *Advances in Cryptology – Proc. CRYPTO ’98*, volume 1462 of *LNCS*, pages 1–12. Springer, 1998.
- [13] C. Brubaker, S. Jana, B. Ray, S. Khurshid, and V. Shmatikov. Using Frankencerts for automated adversarial testing of certificate validation in SSL/TLS implementations. In *35th IEEE Symposium on Security and Privacy*, pages 114–129. IEEE Computer Society, 2014.
- [14] B. B. Brumley, M. Barbosa, D. Page, and F. Vercauteren. Practical realisation and elimination of an ECC-related software bug attack. In O. Dunkelman, editor, *Topics in Cryptology – CT-RSA 2012*, volume 7178 of *LNCS*, pages 171–186. Springer, 2012.
- [15] B. B. Brumley and N. Tuveri. Remote timing attacks are still practical. In V. Atluri and C. Diaz, editors, *Proc. 16th European Symposium on Research in Computer Security (ESORICS) 2011*, volume 6879 of *LNCS*, pages 355–371. Springer, 2011.
- [16] Codenomicon. Heartbleed bug, April 2014. <http://heartbleed.com/>.

- [17] M. J. Cox, April 2014. <https://plus.google.com/+MarkJCox/posts/TmCbp3BhJma>.
- [18] A. Delignat-Lavaud and K. Bhargavan. Virtual host confusion: Weaknesses and exploits. In *Black Hat 2014*, 2014. https://bh.ht.vc/vhost_confusion.pdf.
- [19] N. Drucker and S. Gueron. Selfie: reflections on TLS 1.3 with PSK. Cryptology ePrint Archive, Report 2019/347, 2019. <https://eprint.iacr.org/2019/347>.
- [20] T. Duong. BEAST, September 2011. <http://vnhacker.blogspot.com.au/2011/09/beast.html>.
- [21] Electronic Frontier Foundation. Frequently asked questions (FAQ) about the Electronic Frontier Foundation’s “DES cracker” machine, July 1998. https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html.
- [22] S. Fahl, M. Harbach, T. Muders, L. Baumgärtner, B. Freisleben, and M. Smith. Why Eve and Mallory love Android: An analysis of Android SSL (in)security. In *Proc. 2012 ACM Conference on Computer and Communications Security (CCS)*, pages 50–61. ACM, 2012.
- [23] H. Finney. Bleichenbacher’s RSA signature forgery based on implementation error, August 2006. <https://www.ietf.org/mail-archive/web/openpgp/current/msg00999.html>.
- [24] S. R. Fluhrer and D. A. McGrew. Statistical analysis of the alleged RC4 keystream generator. In B. Schneier, editor, *Fast Software Encryption, 7th International Workshop*, volume 1978 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 2000.
- [25] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov. The most dangerous code in the world: validating SSL certificates in non-browser software. In T. Yu, G. Danezis, and V. D. Gligor, editors, *19th ACM SIGSAC Conference on Computer and Communications Security*, pages 38–49. ACM, 2012.
- [26] I. Goldberg and D. Wagner. Randomness and the Netscape browser: How secure is the World Wide Web? *Dr. Dobb’s Journal*, January 1996. <http://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html>.
- [27] T. Jager, J. Schwenk, and J. Somorovsky. On the security of TLS 1.3 and QUIC against weaknesses in PKCS#1 v1.5 Encryption. In *22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015.
- [28] J. Kelsey. Compression and information leakage of plaintext. In *Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers*, volume 2365 of *Lecture Notes in Computer Science*, pages 263–276. Springer, 2002.
- [29] M. Kikuchi. How I discovered CCS injection vulnerability (CVE-2014-0224), June 2014. <http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/>.
- [30] F. Klute. CVE-2020-13777: TLS 1.3 session resumption works without master key, allowing MITM, June 2020. <https://gitlab.com/gnutls/gnutls/-/issues/1011>, <https://capsule8.com/blog/high-steks-on-path-attacks-in-gnutls-cve-2020-13777/>.
- [31] A. Langley. PKCS#1 signature validation, September 2014. <https://www.imperialviolet.org/2014/09/26/pkcs1.html>.
- [32] A. G. Langley. Apple’s SSL/TLS bug, February 2014. <https://www.imperialviolet.org/2014/02/22/applebug.html>.
- [33] A. K. Lenstra and B. de Weger. On the possibility of constructing meaningful hash collisions for public keys. In C. Boyd and J. M. G. Nieto, editors, *Information Security and Privacy, 10th Australasian Conference*, volume 3574 of *Lecture Notes in Computer Science*, pages 267–279. Springer, 2005.
- [34] I. Mantin. Attacking SSL when using RC4: Breaking SSL with a 13-year-old RC4 weakness. In *Black Hat Asia*, March 2015. https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf.
- [35] I. Mantin and A. Shamir. A practical attack on broadcast RC4. In M. Matsui, editor, *Fast Software Encryption, 8th International Workshop*, volume 2355 of *Lecture Notes in Computer Science*, pages 152–164. Springer, 2001.

- [36] M. Marlinspike. New tricks for defeating SSL in practice. In *Black Hat DC*, February 2009. <https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>, <http://www.thoughtcrime.org/software/sslstrip/>.
- [37] N. Mavrogiannopoulos, F. Vercauteren, V. Velichkov, and B. Preneel. A cross-protocol attack on the TLS protocol. In *Proc. 2012 ACM Conference on Computer and Communications Security (CCS)*, pages 62–72. ACM, 2012.
- [38] C. Meyer, J. Somorovsky, E. Weiss, J. Schwenk, S. Schinzel, and E. Tews. Revisiting SSL/TLS implementations: New Bleichenbacher side channels and attacks. In *23rd USENIX Security Symposium*, pages 733–748. USENIX Association, 2014.
- [39] B. Möller. Security of CBC ciphersuites in SSL/TLS: Problems and countermeasures, 2002. <https://www.openssl.org/~bodo/tls-cbc.txt>.
- [40] B. Möller, T. Duong, and K. Kotowicz. This POODLE bites: Exploiting the SSL 3.0 fallback, September 2014. <https://www.openssl.org/~bodo/ssl-poodle.pdf>.
- [41] C. Percival. Cache missing for fun and profit, May 2005. <http://www.daemonology.net/papers/htt.pdf>.
- [42] A. Prado, N. Harris, and Y. Gluck. SSL, gone in 30 seconds: A BREACH beyond CRIME. In *Black Hat USA 2013*, August 2013. <https://www.blackhat.com/us-13/archives.html#Prado>.
- [43] M. Ray and S. Dispensa. Renegotiating TLS, November 2009.
- [44] J. Rizzo and T. Duong. The CRIME attack, 2012. Presented at ekoparty '12. <http://goo.gl/mlw1X1>.
- [45] P. Rogaway. Evaluation of some blockcipher modes of operation. Technical report, Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, February 2011. <http://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf>.
- [46] B. Smyth and A. Pironti. Truncating TLS connections to violate beliefs in web applications. In *Black Hat USA*, July 2013. <http://www.bensmyth.com/files/Smyth13-truncation-attacks-to-violate-beliefs.pdf>.
- [47] The Debian Project. Debian Security Advisory DSA-1571-1 openssl – predictable random number generator, May 2008. <http://www.debian.org/security/2008/dsa-1571>.
- [48] M. Vanhoef and T. V. Goethem. HEIST: HTTP encrypted information can be stolen through TCP-windows. In *Black Hat USA*, August 2016. https://tom.vg/papers/heist_blackhat2016.pdf.
- [49] M. Vanhoef and F. Piessens. All your biases belong to us: Breaking RC4 in WPA-TKIP and TLS. In *24th USENIX Security Symposium*. USENIX Association, 2015.
- [50] W. Venema and M. Orlando. Vulnerability note VU#555316: STARTTLS plaintext command injection vulnerability, March 2011. <http://www.kb.cert.org/vuls/id/555316>.
- [51] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. In *Second USENIX Workshop on Electronic Commerce*, November 1996. <http://www.usenix.org/publications/library/proceedings/ec96/index.html>.
- [52] Y. Yarom and N. Benger. Recovering OpenSSL ECDSA nonces using the FLUSH+RELOAD cache side-channel attack, 2014. Cryptology ePrint Archive, Report 2014/140.