论 文 列 表

[1] WANG L, ASHAROV G, PASS R, et al. Blind certificate authorities[C/OL]//2019 2019 IEEE Symposium on Security and Privacy (SP). Los Alamitos, CA, USA: IEEE Computer Society, 2019. https://doi.ieeecomputersociety.org/10.1109/SP.2019.00007.

[2] RUPPRECHT D, KOHLS K, HOLZ T, et al. Breaking lte on layer two[C/OL]//2019 2019 IEEE Symposium on Security and Privacy (SP). Los Alamitos, CA, USA: IEEE Computer Society, 2019. https://doi.ieeecomputersociety.org/10.1109/SP.2019.00006.

[3] RONEN E, GILLHAM R, GENKIN D, et al. The 9 lives of bleichenbacher's cat: New cache attacks on tls implementations[C/OL]//2019 2019 IEEE Symposium on Security and Privacy (SP). Los Alamitos, CA, USA: IEEE Computer Society, 2019. https://doi.ieeecomputersociety.org/10.1109/SP.2019.00062.

[4] MI X, FENG X, LIAO X, et al. Resident evil: Understanding residential ip proxy as a dark service[C/OL]//2019 2019 IEEE Symposium on Security and Privacy (SP). Los Alamitos, CA, USA: IEEE Computer Society, 2019. https://doi.ieeecomputersociety.org/10.1109/SP.2019.00011.

[5] TRAN M, KANG M, HSIAO H, et al. On the feasibility of rerouting-based ddos defenses [C/OL]//2019 2019 IEEE Symposium on Security and Privacy (SP). Los Alamitos, CA, USA: IEEE Computer Society, 2019. https://doi.ieeecomputersociety.org/10.1109/SP.2019.00055.

[6] CALZAVARA S, FOCARDI R, NEMEC M, et al. Postcards from the post-http world: Amplification of https vulnerabilities in the web ecosystem[C/OL]//2019 2019 IEEE Symposium on Security and Privacy (SP). Los Alamitos, CA, USA: IEEE Computer Society, 2019. https://doi.ieeecomputersociety.org/10.1109/SP.2019.00053.

[7] Cheval V, Kremer S, Rakotonirina I. Deepsec: Deciding equivalence properties in security protocols theory and practice[C/OL]//2018 IEEE Symposium on Security and Privacy (SP). 2018: 529-546. DOI: 10.1109/SP.2018.00033.

[8] Borgolte K, Hao S, Fiebig T, et al. Enumerating active ipv6 hosts for large-scale security scans via dnssec-signed reverse zones[C/OL]//2018 IEEE Symposium on Security and Privacy (SP). 2018: 770-784. DOI: 10.1109/SP.2018.00027.

[9] Bhargavan K, Boureanu I, Delignat-Lavaud A, et al. A formal treatment of accountable proxying over tls[C/OL]//2018 IEEE Symposium on Security and Privacy (SP). 2018: 799-816. DOI: 10.1109/SP.2018.00021.

[10] Alrwais S, Liao X, Mi X, et al. Under the shadow of sunshine: Understanding and detecting bulletproof hosting on legitimate service provider networks[C/OL]//2017 IEEE Symposium

on Security and Privacy (SP). 2017: 805-823. DOI: 10.1109/SP.2017.32.

[11] Chau S Y, Chowdhury O, Hoque E, et al. Symcerts: Practical symbolic execution for exposing noncompliance in x.509 certificate validation implementations[C/OL]//2017 IEEE Symposium on Security and Privacy (SP). 2017: 503-520. DOI: 10.1109/SP.2017.40.

[12] Abu-Salma R, Sasse M A, Bonneau J, et al. Obstacles to the adoption of secure communication tools[C/OL]//2017 IEEE Symposium on Security and Privacy (SP). 2017: 137-153. DOI: 10.1109/SP.2017.65.

[13] Cortier V, Drăgan C C, Dupressoir F, et al. Machine-checked proofs of privacy for electronic voting protocols[C/OL]//2017 IEEE Symposium on Security and Privacy (SP). 2017: 993-1008. DOI: 10.1109/SP.2017.28.

[14] Delignat-Lavaud A, Fournet C, Kohlweiss M, et al. Implementing and proving the tls 1.3 record layer[C/OL]//2017 IEEE Symposium on Security and Privacy (SP). 2017: 463-482. DOI: 10.1109/SP.2017.58.

[15] Sivakorn S, Argyros G, Pei K, et al. Hvlearn: Automated black-box analysis of hostname verification in ssl/tls implementations[C/OL]//2017 IEEE Symposium on Security and Privacy (SP). 2017: 521-538. DOI: 10.1109/SP.2017.46.

[16] Larisch J, Choffnes D, Levin D, et al. Crlite: A scalable system for pushing all tls revocations to all browsers[C/OL]//2017 IEEE Symposium on Security and Privacy (SP). 2017: 539-556. DOI: 10.1109/SP.2017.17.

[17] RONEN E, PATERSON K G, SHAMIR A. Pseudo constant time implementations of TLS are only pseudo secure[C/OL]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. 2018: 1397-1414. https://doi.org/10.1145/3243734.3243775.

[18] PATTON C, SHRIMPTON T. Partially specified channels: The TLS 1.3 record layer without elision[C/OL]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. 2018: 1415-1428. https://doi.org/10.1145/3243734.3243789.

[19] HOANG V T, TESSARO S, THIRUVENGADAM A. The multi-user security of gcm, revisited: Tight bounds for nonce randomization[C/OL]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. 2018: 1429-1440. https://doi.org/10.1145/3243734.3243816.

[20] ACER M E, STARK E, FELT A P, et al. Where the wild warnings are: Root causes of chrome https certificate errors[C/OL]//CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2017: 1407-1420. http://doi.acm.org/10.1145/3133956.3134007.

[21] THOMAS K, LI F, ZAND A, et al. Data breaches, phishing, or malware?: Understanding the risks of stolen credentials[C/OL]//CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2017: 1421-1434. http://doi.acm.org/10.1145/3133956.3134067.

[22] VANHOEF M, PIESSENS F. Key reinstallation attacks: Forcing nonce reuse in wpa2[C/OL]//CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2017: 1313-1328. http://doi.acm.org/10.1145/3133956.3134027.

[23] CREMERS C, HORVAT M, HOYLAND J, et al. A comprehensive symbolic analysis of tls 1.3[C/OL]//CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2017: 1773-1788. http://doi.acm.org/10.1145/3133956.3134063.

[24] XIAO Y, LI M, CHEN S, et al. Stacco: Differentially analyzing side-channel traces for detecting ssl/tls vulnerabilities in secure enclaves[C/OL]//CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2017: 859-874. http://doi.acm.org/10.1145/3133956.3134016.

[25] FELSCH D, GROTHE M, SCHWENK J, et al. The dangers of key reuse: Practical attacks on ipsec IKE[C/OL]//27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018: 567-583. https://www.usenix.org/conference/usenixsecurity18/presentation/felsch.

[26] PODDEBNIAK D, DRESEN C, MÜLLER J, et al. Efail: Breaking s/mime and openpgp email encryption using exfiltration channels[C/OL]//27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018: 549-566. https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak.

[27] KIM D, KWON B J, KOZÁK K, et al. The broken shield: Measuring revocation effectiveness in the windows code-signing PKI[C/OL]//27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018: 851-868. https://www.usenix.org/conference/usenixsecurity18/presentation/kim.

[28] BIRGE-LEE H, SUN Y, EDMUNDSON A, et al. Bamboozling certificate authorities with BGP[C/OL]//27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018: 833-849. https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee.

[29] LIU B, LU C, DUAN H, et al. Who is answering my queries: Understanding and characterizing interception of the DNS resolution path[C/OL]//27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018: 1113-1128. https://www.usenix.o

rg/conference/usenixsecurity18/presentation/liu-baojun.

[30] O'NEILL M, HEIDBRINK S, WHITEHEAD J, et al. The secure socket API: TLS as an operating system service[C/OL]//27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018: 799-816. https://www.usenix.org/conference/usenixsecurity18/presentation/oneill.

[31] O'NEILL M, HEIDBRINK S, RUOTI S, et al. Trustbase: An architecture to repair and strengthen certificate-based authentication[C/OL]//26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association, 2017: 609-624. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/oneill.

[32] JERO S, KOCH W, SKOWYRA R, et al. Identifier binding attacks and defenses in software-defined networks[C/OL]//26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association, 2017: 415-432. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/jero.

[33] XU L, HUANG J, HONG S, et al. Attacking the brain: Races in the SDN control plane [C/OL]//26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association, 2017: 451-468. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/xu-lei.

[34] SIVAKORN S, JEE K, SUN Y, et al. Countering malicious processes with process-dns association[C/OL]//Network and Distributed System Security Symposium (NDSS). 2019. https://www.ndss-symposium.org/ndss-paper/countering-malicious-processes-with-process-dns-association/.

[35] KLEIN A, PINKAS B. Dns cache-based user tracking[C/OL]//Network and Distributed System Security Symposium (NDSS). 2019. https://www.ndss-symposium.org/ndss-paper/dns-cache-based-user-tracking/.

[36] APOSTOLAKI M, MARTI G, MÜLLER J, et al. Sabre: Protecting bitcoin against routing attacks[C/OL]//Network and Distributed System Security Symposium (NDSS). 2019. https://www.ndss-symposium.org/ndss-paper/sabre-protecting-bitcoin-against-routing-attacks/.

[37] FROLOV S, WUSTROW E. The use of tls in censorship circumvention[C/OL]//Network and Distributed System Security Symposium (NDSS). 2019. https://www.ndss-symposium.org/ndss-paper/the-use-of-tls-in-censorship-circumvention/.

[38] LEE H, SMITH Z, LIM J, et al. matls: How to make tls middlebox-aware?[C/OL]//Network and Distributed System Security Symposium (NDSS). 2019. https://www.ndss-symposium.org/ndss-paper/matls-how-to-make-tls-middlebox-aware/.

[39] LEE J, WALLACH D S. Removing secrets from android's tls[C]//Network and Distributed System Security Symposium. 2018.

[40] JERO S, HOQUE E, CHOFFNES D, et al. Automated attack discovery in tcp congestion control using a model-guided approach[C]//Proc. of Network and Distributed System Security Symp., San Diego, CA, USA. 2018: 1-15.

[41] HUSSAIN S, CHOWDHURY O, MEHNAZ S, et al. Lteinspector: A systematic approach for adversarial testing of 4g lte[C]//Network and Distributed Systems Security (NDSS) Symposium 2018. 2018.

[42] BORGOLTE K, FIEBIG T, HAO S, et al. Cloud strife: mitigating the security risks of domain-validated certificates[C]//Proc. Internet Society Symposium on Network and Distributed System Security (NDSS). 2018.

[43] TSIRANTONAKIS G, ILIA P, IOANNIDIS S, et al. A large-scale analysis of content modification by open http proxies[C]//Network and Distributed System Security Symposium (NDSS). 2018.

[44] RITZDORF H, WÜST K, GERVAIS A, et al. Tls-n: Non-repudiation over tls enabling ubiquitous content signing[C]//Network and Distributed System Security Symposium (NDSS). 2018.

[45] DURUMERIC Z, MA Z, SPRINGALL D, et al. The security impact of https interception.[C]//Network and Distributed System Security Symposium (NDSS). 2017.

[46] DOREY K, CHANG-FONG N, ESSEX A. Indiscreet logs: Diffie-hellman backdoors in tls. [C]//NDSS. 2017.

[47] GILAD Y, COHEN A, HERZBERG A, et al. Are we there yet? on rpki's deployment and security.[C]//NDSS. 2017.

[48] MCMAHON STONE C, CHOTHIA T, DE RUITER J. Extending automated protocol state learning for the 802.11 4-way handshake[C]//LOPEZ J, ZHOU J, SORIANO M. Computer Security. Cham: Springer International Publishing, 2018: 325-345.

[49] KIM S, LEE S, CHO G, et al. Preventing dns amplification attacks using the history of dns queries with sdn[C]//FOLEY S N, GOLLMANN D, SNEKKENES E. Computer Security – ESORICS 2017. Cham: Springer International Publishing, 2017: 135-152.

[50] HAN D, CHEN Y, LI T, et al. Proximity-proof: Secure and usable mobile two-factor authentication[C/OL]//MobiCom '18: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking. New York, NY, USA: ACM, 2018: 401-415. http://doi.acm.org/10.1145/3241539.3241574.

[51] Bu K, Yang Y, Guo Z, et al. Flowcloak: Defeating middlebox-bypass attacks in software-defined networking[C/OL]//IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. 2018: 396-404. DOI: 10.1109/INFOCOM.2018.8486230.

[52] Yang Z, Järvinen K. The death and rebirth of privacy-preserving wifi fingerprint localization with paillier encryption[C/OL]//IEEE INFOCOM 2018 - IEEE Conference on Computer

Communications. 2018: 1223-1231. DOI: 10.1109/INFOCOM.2018.8486221.

[53] Chen J, Yao S, Yuan Q, et al. Certchain: Public and efficient certificate audit based on blockchain for tls connections[C/OL]//IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. 2018: 2060-2068. DOI: 10.1109/INFOCOM.2018.8486344.

[54] Zhang X, Knockel J, Crandall J R. Onis: Inferring tcp/ip-based trust relationships completely off-path[C/OL]//IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. 2018: 2069-2077. DOI: 10.1109/INFOCOM.2018.8486426.

[55] Liu C, Cui Y, Tan K, et al. Building generic scalable middlebox services over encrypted protocols[C/OL]//IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. 2018: 2195-2203. DOI: 10.1109/INFOCOM.2018.8485861.

[56] Li J, Ma X, Guodong L, et al. Can we learn what people are doing from raw dns queries? [C/OL]//IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. 2018: 2240-2248. DOI: 10.1109/INFOCOM.2018.8486210.