proxy server extension. IETF TLS Internet-Draft `draft-mcgrew-tls-proxy-server-01`, July 16, 2012.

[43] D. A. McGrew and J. Viega. The Galois/counter mode of operation (GCM), May 31, 2005. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf.

[44] E. Nakashima. Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. The Washington Post, May 20, 2013. https://www.washingtonpost.com/51330428-be34-11e2-89c9-3be8095fe767_story.html.

[45] D. Naylor, K. Schomp, M. Varvello, I. Leontiadis, J. Blackburn, D. R. López, K. Papagiannaki, P. Rodriguez Rodriguez, and P. Steenkiste. Multi-context TLS (mcTLS): Enabling secure in-network functionality in TLS. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, pages 199–212, New York, NY, USA, 2015. ACM.

[46] Y. Nir. A method for sharing record protocol keys with a middlebox in TLS. IETF TLS Working Group Internet-Draft `draft-nir-tls-keyshare-02`, March 26, 2012.

[47] V. Paxson, M. Christodorescu, M. Javed, J. R. Rao, R. Sailer, D. L. Schales, M. P. Stoecklin, K. Thomas, W. Venema, and N. Weaver. Practical comprehensive bounds on surreptitious communication over DNS. In *Proceedings of the 22nd USENIX Security Symposium*, USENIX-SS'17, pages 17–32. USENIX Association, Aug. 2013.

[48] R. Peon. Explicit proxies for HTTP/2.0. IETF Network Working Group Internet-Draft `draft-rpeon-httpbis-exproxy-00`, June 8, 2012.

[49] A. Peterson. How the NSA may be using games to encourage digital snooping. The Washington Post, June 18, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/06/18/how-the-nsa-may-have-used-games-to-encourage-digital-snooping/.

[50] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan. CryptDB: Protecting confidentiality with encrypted query processing. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, SOSP '11, pages 85–100, New York, NY, USA, 2011. ACM.

[51] R. A. Popa, E. Stark, J. Helfer, S. Valdez, N. Zeldovich, M. F. Kaashoek, and H. Balakrishnan. Building web applications on top of encrypted data using Mylar. In *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation*, NSDI'14, pages 157–172, Berkeley, CA, USA, 2014. USENIX Association.

[52] M. W. R. Seggelmann, M. Tuexen. Transport layer security (TLS) and datagram transport layer security (DTLS) heartbeat extension. IETF, 2012. RFC 6520.

[53] E. Rescorla. The transport layer security (TLS) protocol version 1.3. IETF, 2017. draft-ietf-tls-tls13-19.

[54] J. Risen and E. Lichtblau. Bush lets U.S. spy on callers without courts. The New York Times, December 16, 2005. https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

[55] P. Rogaway. The moral character of cryptographic work. Cryptology ePrint Archive, Report 2015/1162, 2015. http://eprint.iacr.org/2015/1162.

[56] E. Ronen, C. O'Flynn, A. Shamir, and A. Weingarten. IoT Goes Nuclear: Creating a ZigBee Chain Reaction, Preliminary Draft Version 0.93, Nov. 2016. http://iotworm.eyalro.net/iotworm.pdf.

[57] J. Salowey, H. Zhou, P. Eronen, and H. Tschofenig. Transport layer security (TLS) session resumption without server-side state. IETF, 2008. RFC 5077.

[58] D. E. Sanger and J. H. Davis. Hacking linked to China exposes millions of U.S. workers. The New York Times, June 4, 2015. https://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html.

[59] S. Schultze. How the Nokia browser decrypts SSL traffic: A "man in the client". Freedom To Tinker Blog, January 11, 2013. https://freedom-to-tinker.com/blog/sjs/how-the-nokia-browser-decrypts-ssl-traffic-a-man-in-the-client/.

[60] G. Shah, A. Molina, and M. Blaze. Keyboards and covert channels. In *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*, USENIX-SS'06, Berkeley, CA, USA, 2006. USENIX Association.

[61] J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy. BlindBox: Deep packet inspection over encrypted traffic. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, pages 213–226, New York, NY, USA, 2015. ACM.

[62] G. R. Simpson. Treasury tracks financial data in secret program. The Wall Street Journal, June 23, 2006. http://www.wsj.com/articles/SB115101988281688182.

[63] R. Singel. Whistle-blower outs NSA spy room. Wired, April 7, 2006. https://archive.wired.com/science/discoveries/news/2006/04/70619.

[64] D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, SP '00, pages 44–55, Washington, DC, USA, 2000. IEEE Computer Society.

[65] Vulnerability note VU#792004. CERT Vulnerability Notes Database. https://www.kb.cert.org/vuls/id/792004.

[66] F. Wang, J. Mickens, N. Zeldovich, and V. Vaikuntanathan. Sieve: Cryptographically enforced access control for user data in untrusted clouds. In *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation*, NSDI'16, pages 611–626, Berkeley, CA, USA, 2016. USENIX Association.

[67] C. Wisniewski. Smart meter hacking can disclose which TV shows and movies you watch. naked security by SOPHOS, Jan. 8, 2012. https://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/.

[68] Z. Zhou and T. Benson. Towards a safe playground for HTTPS and middle boxes with QoS2. In *Proceedings of the 2015 ACM SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization*, HotMiddlebox '15, pages 7–12, New York, NY, USA, 2015. ACM.