[13] M. Belshe and R. Peon, "The SPDY protocol," IETF draft-mbelshe-httpbis-spdy-00, 2012.

[14] Akamai Technologies, "Visualizing akamai," akamai.com/html/technology/dataviz3.html, 2014.

[15] J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When HTTPS meets CDN: A case of authentication in delegated service," in *IEEE S&P*, 2014.

[16] I. Sysoev and B. Mercer, "How nginx processes requests," nginx.org/docs/http/request_processing.html, 2012.

[17] Apache Foundation, "Virtual host documentation," http://httpd.apache.org/docs/current/vhosts/, 2014.

[18] S. Stamm, B. Sterne, and G. Markham, "Reining in the web with content security policy," in *WWW*, 2010.

[19] E. Hammer-Lahav, D. Recordon, and D. Hardt, "The OAuth 2.0 Authorization Protocol," IETF Draft, 2011.

[20] A. Barth, C. Jackson, and J. C. Mitchell, "Robust defenses for cross-site request forgery," in *CCS*, 2008.

[21] A. Bortz, A. Barth, and A. Czeskis, "Origin cookies: session integrity for web applications," in *W2SP*, 2011.

[22] R. Hansen and J. Sokol, "MitM DNS rebinding SSL wildcards and XSS," http://goo.gl/23Yt9l, 2010.

[23] M. Schloesser, B. Gamble, J. Nickel, C. Guarnieri, and H. D. Moore, "Project sonar: IPv4 SSL certificates," https://scans.io/study/sonar.ssl, 2013.

[24] Alexa Internet Inc., "Top 1,000,000 sites (updated daily)," http://goo.gl/OZdT6p, 2014.

[25] S. Pai, Y. Sharma, S. Kumar, R. M. Pai, and S. Singh, "Formal verification of oauth 2.0 using alloy framework," in *CSNT*. IEEE, 2011.

[26] S.-T. Sun and K. Beznosov, "The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems," in *CCS*. ACM, 2012.

[27] C. Bansal, K. Bhargavan, and S. Maffeis, "Discovering concrete attacks on website authorization by formal analysis," in *CSF*. IEEE, 2012.

[28] D. Akhawe, A. Barth, P. Lam, J. Mitchell, and D. Song, "Towards a formal foundation of web security," in *CSF*, 2010, pp. 290–304.

[29] M. Belshe, R. Peon, and M. Thomson, "Hypertext transfer protocol version 2," 2012. [Online]. Available: http://tools.ietf.org/html/draft-ietf-httpbis-http2-14

[30] A. Parsovs, "Practical issues with TLS client certificate authentication," in *NDSS*, 2014.

[31] M. Dietz, A. Czeskis, D. Balfanz, and D. S. Wallach, "Origin-bound certificates: a fresh approach to strong client authentication," in *Usenix Security*, 2012.

[32] 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 *IEEE S&P*. IEEE, 2014.

[33] C. Evans and C. Palmer, "Certificate pinning extension for HSTS," 2011. [Online]. Available: http://tools.ietf.org/html/draft-evans-palmer-hsts-pinning-00

[34] C. Meyer and J. Schwenk, "SoK: Lessons learned from SSL/TLS attacks," in *Information Security Applications*, ser. LNCS. Springer, 2014, pp. 189–209.

[35] J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When HTTPS meets CDN: A case of authentication in delegated service," in *IEEE Symposium on Security & Privacy 2014 (Oakland'14)*. IEEE, 2014.

[36] B. Moeller and A. Langley, "TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks," Internet Draft (v.01), 2014.

[37] R. Wang, S. Chen, and X. Wang, "Signing me onto your accounts through Facebook and Google: A traffic-guided security study of commercially deployed single-sign-on web services," in *IEEE S&P*, 2012.

[38] D. Fett, R. Kusters, and G. Schmitz, "An expressive model for the web infrastructure: definition and application to the BrowserID SSO system," in *IEEE S&P*, 2014.

[39] K. Bhargavan, A. Delignat-Lavaud, and S. Maffeis, "Language-based defenses against untrusted browser origins," in *Usenix Security*, 2013.

[40] C. Bansal, K. Bhargavan, and S. Maffeis, "Discovering concrete attacks on website authorization by formal analysis," in *CSF*, 2012.

[41] M. Marlinspike, "More tricks for defeating SSL in practice," *Black Hat USA*, 2009.

[42] J. Hodges, C. Jackson, and A. Barth, "HTTP Strict Transport Security (HSTS)," IETF RFC 6797, 2012.

[43] J. Selvi, "Bypassing http strict transport security."

[44] C. Jackson, A. Barth, A. Bortz, W. Shao, and D. Boneh, "Protecting browsers from DNS rebinding attacks," *TWEB*, vol. 3, no. 1, 2009.

[45] S. Son and V. Shmatikov, "The hitchhiker's guide to DNS cache poisoning," in *SecureComm*, 2010.

[46] D. Dagon, M. Antonakakis, P. Vixie, T. Jinmei, and W. Lee, "Increased DNS forgery resistance by 0x20-bit encoding: security via leet queries," in *CCS*, 2008.

[47] N. Karapanos and S. Capkun, "On the effective prevention of TLS man-in-the-middle attacks in web applications," in *Usenix Security*, 2014.

[48] C. Soghoian and S. Stamm, "Certified lies: setecting and defeating government interception attacks against SSL," in *FC*, 2012.

[49] C. Karlof, U. Shankar, J. D. Tygar, and D. Wagner, "Dynamic pharming attacks and locked same-origin policies for web browsers," in *CCS*, 2007.

[50] 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 *ACM CCS*, 2012.

[51] D. Akhawe, B. Amann, M. Vallentin, and R. Sommer, "Here's my cert, so trust me, maybe? understanding TLS errors on the web," in *WWW*, 2013.

[52] T. Duong and J. Rizzo, "Here come the XOR ninjas," *White paper, Netifera*, 2011.

[53] J. Rizzo and T. Duong, "The CRIME attack," in *EKOparty Security Conference*, vol. 2012, 2012.

[54] B. Beurdouche, K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and J. K. Zinzindohoue, "A messy state of the union: taming the composite state machines of TLS," in *IEEE S&P*, 2015.

[55] B. Laurie, "Certificate transparency," *Commun. ACM*, vol. 57, no. 10, 2014.

[56] D. Basin, C. Cremers, T. H.-J. Kim, A. Perrig, R. Sasse, and P. Szalachowski, "ARPKI: Attack resilient public-key infrastructure," in *CCS*, 2014.