QoS2 in a number of ways. First, by exploring techniques to disambiguate between stale checksums and attacks on the HTTP channel. Our current approach conflates both and reacts in a heavy handed manner. Second, by implementing checksum verification in the browser. Third, by enhancing the nginx and Apache platforms to support QoS2. Finally, we hope to evaluate QoS2 under a variety of workloads, to understand how the benefits of QoS2 are impacted by the choices made by content-providers.

8. ACKNOWLEDGEMENTS

We thank our anonymous reviewers for their thoughtful comments and feedback. This work was supported by NSF Award CSR-1409426.

9. REFERENCES

[1] Ball, James and Borger, Julian and Greenwald, Glenn. Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security. *The Guardian*, 6, 2013.

[2] Tim Dierks. The transport layer security (TLS) protocol version 1.2. 2008.

[3] David Naylor, Alessandro Finamore, Ilias Leontiadis, Yan Grunenberger, Marco Mellia, Maurizio Munafò, Konstantina Papagiannaki, and Peter Steenkiste. The Cost of the "S" in HTTPS. In *Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies*, CoNEXT '14, pages 133–140, New York, NY, USA, 2014. ACM.

[4] Xing Xu, Yurong Jiang, Tobias Flach, Ethan Katz-Bassett, David Choffnes, and Ramesh Govindan. Investigating Transparent Web Proxies in Cellular Networks. *Passive and Active Measurement Conference*, 2015.

[5] Jeffrey Erman, Alexandre Gerber, Mohammad T. Hajiaghayi, Dan Pei, and Oliver Spatscheck. Network-aware Forward Caching. In *Proceedings of the 18th International Conference on World Wide Web*, WWW '09, pages 291–300, New York, NY, USA, 2009. ACM.

[6] Jeffrey Erman, Alexandre Gerber, Mohammad Hajiaghayi, Dan Pei, Subhabrata Sen, and Oliver Spatscheck. To Cache or not to Cache: The 3G case. *Internet Computing, IEEE*, 15(2):27–34, 2011.

[7] S. Loreto, J. Mattsson, R. Skog, H. Spaak, G. Gus, D. Druta and M. Hafeez. Explicit Trusted Proxy in HTTP/2.0. *IETF Internet-Draft*, 2014.

[8] Hodges, Jeff and Jackson, Collin and Barth, Adam. HTTP Strict Transport Security (HSTS). *IETF Internet-Draft*, 2012.

[9] Michael Kranch and Joseph Bonneau. Upgrading HTTPS in mid-air: An empirical study of strict transport security and key pinning. *Network and Distributed System Security (NDSS) Symposium*, 2015.

[10] Qi Huang, Ken Birman, Robbert van Renesse, Wyatt Lloyd, Sanjeev Kumar, and Harry C. Li. An Analysis of Facebook Photo Caching. In *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles*, SOSP '13, pages 167–181, New York, NY, USA, 2013. ACM.

[11] Michael Butkiewicz, Harsha V. Madhyastha, and Vyas Sekar. Understanding Website Complexity: Measurements, Metrics, and Implications. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, IMC '11, pages 313–328, New York, NY, USA, 2011. ACM.

[12] Ping Chen, Nick Nikiforakis, Lieven Desmet, and Christophe Huygens. A Dangerous Mix: Large-scale analysis of mixed-content websites. In *Proceedings of the 16th Information Security Conference (ISC)*, 2013.

[13] Xin Jin, Li Erran Li, Laurent Vanbever, and Jennifer Rexford. SoftCell: Scalable and Flexible Cellular Core Network Architecture. In *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*, CoNEXT '13, pages 163–174, New York, NY, USA, 2013. ACM.

[14] S. Loreto, J. Mattsson, R. Skog, H. Spaak, G. Bourg, D. Druta and M. Hafeez. Explicitly authenticated proxy in HTTP/2.0. *IETF Internet-Draft*, July 2014.

[15] D. McGrew, D. Wing, Y. Nir and P. Gladstone. TLS Proxy Server Extension. *IETF Internet-Draft*, July 2012.

[16] Thomas Fossati, Vijay K. Gurbani and Vladimir Kolesnikov. Love all, trust few: On trusting intermediaries in HTTP. In *ACM SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization*. ACM, 2015.

[17] Andrea Bittau, Michael Hamburg, Mark Handley, David Mazières, and Dan Boneh. The case for ubiquitous transport-level encryption. In *Proceedings of the 19th USENIX Conference on Security*, USENIX Security'10, pages 26–26, Berkeley, CA, USA, 2010. USENIX Association.

[18] A. Bittau, D. Boneh, M. Hamburg, M. Handley, D. Mazieres and Q. Slack. Cryptographic protection of TCP streams. *IETF Internet-Draft*, July 2014.

[19] Sneha Kasera, Semyon Mizikovsky, Ganapathy S. Sundaram, and Thomas Y. C. Woo. On Securely Enabling Intermediary-based Services and Performance Enhancements for Wireless Mobile Users. In *Proceedings of the 2Nd ACM Workshop on Wireless Security*, WiSe '03, pages 61–68, New York, NY, USA, 2003. ACM.

[20] Yongguang Zhang and Bikramjit Singh. A Multi-Layer IPSEC Protocol. In *USENIX Security Symposium*, volume 9, 2000.

[21] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. BlindBox: Deep Packet Inspection over Encrypted Traffic. In *Proceedings of the 2015 ACM SIGCOMM Conference*, 2015.

[22] Ziv Bar-Yossef and Sridhar Rajagopalan. Template Detection via Data Mining and Its Applications. In *Proceedings of the 11th International Conference on World Wide Web*, WWW '02, pages 580–591, New York, NY, USA, 2002. ACM.

[23] Bert Hubert. TC–Linux man page. http://lartc.org/manpages/tc.txt, 2010.

[24] Ashish Vulimiri, Philip Brighten Godfrey, Radhika Mittal, Justine Sherry, Sylvia Ratnasamy, and Scott Shenker. Low Latency via Redundancy. In *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*, CoNEXT '13, pages 283–294, New York, NY, USA, 2013. ACM.