considered. The fundamental problem regarding the lack of existing HTTPS deployments was discussed.

Thanks to our project it is possible to simplify the process of HTTPS Everywhere rule generation. This increases the content transmitted exclusively over HTTPS for users of this plugin and makes a small step in the direction of an encrypted Internet.

Acknowledgements

This work has been supported by COMET K1, FFG - Austrian Research Promotion Agency and under grant no. 846028.

7. REFERENCES

[1] Alexa Internet Inc., Top 1,000,000 sites. `http://s3.amazonaws.com/alexa-static/top-1m.csv.zip`.

[2] Amazon Mechanical Turk. `https://www.mturk.com/mturk/welcome`.

[3] Applied Crypto Hardening. Online at `https://bettercrypto.org`, 2015.

[4] 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. Zanella-Béguelin, and P. Zimmermann. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. In *22nd Conference on Computer and Communications Security*. ACM, 2015.

[5] M. Bayer. SQLAlchemy - The database toolkit for python. `http://www.sqlalchemy.org/`.

[6] 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 *Symposium on Security and Privacy*. IEEE, 2015.

[7] J. Clark and P. C. van Oorschot. SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In *Symposium on Security and Privacy*, pages 511–525. IEEE, 2013.

[8] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), Aug. 2008. Updated by RFCs 5746, 5878, 6176.

[9] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, and J. A. Halderman. Neither Snow Nor Rain Nor MITM...: An Empirical Analysis of Email Delivery Security. In *15th Internet Measurement Conference*, pages 27–39. ACM, 2015.

[10] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, et al. The matter of Heartbleed. In *14th Internet Measurement Conference*, pages 475–488. ACM, 2014.

[11] J. Hodges, C. Jackson, and A. Barth. HTTP Strict Transport Security (HSTS). RFC 6797 (Proposed Standard), Nov. 2012.

[12] R. Holz, J. Amann, O. Mehani, M. Wachs, and M. A. Kaafar. TLS in the wild: an Internet-wide analysis of TLS-based protocols for electronic communication. In *Network and Distributed System Security Symposium*. Internet Society, 2016.

[13] R. Holz, T. Riedmaier, N. Kammenhuber, and G. Carle. X. 509 Forensics: Detecting and Localising the SSL/TLS Men-in-the-middle. In *European Symposium on Research in Computer Security*, pages 217–234. Springer, 2012.

[14] M. Huber, M. Mulazzani, and E. Weippl. Who on earth is "Mr. Cypher": automated friend injection attacks on social networking sites. In *Security and Privacy – Silver Linings in the Cloud*, pages 80–89. Springer, 2010.

[15] Internet Security Research Group. Let's Encrypt - Let's Encrypt is a new Certificate Authority. `https://letsencrypt.org/`.

[16] D. Keeler. Preloading HSTS. Mozilla Security Blog - `https://blog.mozilla.org/security/2012/11/01/preloading-hsts`, 2012.

[17] M. Kranch and J. Bonneau. Upgrading HTTPS in Mid-Air: An Empirical Study of Strict Transport Security and Key Pinning. In *Network and Distributed System Security Symposium*. Internet Society, Feb. 2015.

[18] W. Mayer, A. Zauner, M. Schmiedecker, and M. Huber. No Need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large. *arXiv preprint arXiv:1510.08646*, 2015.

[19] J. Prins and B. U. Cybercrime. Diginotar certificate authority breach'operation black tulip', 2011.

[20] A. Ronacher. Flask - web development, one drop at a time. `http://flask.pocoo.org/`.

[21] Y. Sheffel, R. Holz, and P. Saint-Andre. Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS(DTLS). RFC 7457 (Proposed Standard), 2015.

[22] Y. Sheffer, R. Holz, and P. Saint-Andre. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). RFC 7525 (Proposed Standard), 2015.