Measuring Adoption of Security Additions to the HTTPS Ecosystem

Quirin Scheitle
Technical University of Munich (TUM)
scheitle@net.in.tum.de

Taejoong Chung
Northeastern University

Johanna Amann
ICSI

Oliver Gasser
Technical University of Munich (TUM)

Lexi Brent
The University of Sydney

Georg Carle
Technical University of Munich (TUM)

Ralph Holz
The University of Sydney

Jens Hiller
RWTH Aachen

Johannes Naab
Technical University of Munich (TUM)

Roland van Rijswijk-Deij
University of Twente and SURFnet

Oliver Hohlfeld
RWTH Aachen

Dave Choffnes
Northeastern University

Alan Mislove
Northeastern University

ABSTRACT

Web security has been and remains a highly relevant field of security research, which has seen many additional features standardiazed at IETF over the past years.

This talk covers two papers, which in sum provide a conprehensive survey of quantity and quality of adoption of such new security extensions by HTTPS web servers.

The protocols covered are Certificate Transparency (CT) at the PKI/certificate level, HTTP Strict Transport Security (HSTS) and HTTP Public Key Pinning (HPKP) at the HTTP level, Downgrade-Preventing Signaling Cipyher Suite Value (SCSV) at the TLS level, and Certification Authority Authorization (CAA) and TLSA record types. For all these security extensions, we conduct extensive active scans from 2 continents, using IPv4 and IPv6, as well as passive observations from 3 continents. We extensively analyze our results, and discuss adoption of these security extensions by deployment risk, deployment effort, and their relative age, finding low-risk, low-effort extensions deployed the most wide-spread. We consider this a lesson learned for future standardization.

In a subsequent deep-dive in the second paper, we exhaustively analyze the effectiveness of CAA after its effectiveness on Sep 8, 2017. We assess quality and quantity of CAA adoption by servers through holistic active scans, deployment by DNS operators through test domains, and conduct an extensive issuance experiment to scrutinize the rigor of implementation by Certification Authorities (CAs).

Based on [1] and [2].

[1] Johanna Amann, *Oliver Gasser*, Quirin Scheitle*, Lexi Brent, Georg Carle, and Ralph Holz. 2017. Mission accomplished?: HTTPS security after diginotar. In Proceedings of the 2017 Internet Measurement Conference (IMC '17). ACM, New York, NY, USA, 325-340. DOI: https://doi.org/10.1145/3131365.31314

[2] Quirin Scheitle, Taejoong Chung, Jens Hiller, Oliver Gasser, Johannes Naab, Roland van Rijswijk-Deij, Oliver Hohlfeld, Ralph Holz, Dave Choffnes, Alan Mislove, and Georg Carle. 2018. A First Look at Certification Authority Authorization (CAA). SIGCOMM Comput. Commun. Rev. 48, 2 (May 2018), 10-23. DOI: https://doi.org/10.1145/3213232.3213235

ANRW '18, July 16, 2018, Montreal, QC, Canada

ACM ISBN 978-1-4503-5585-8/18/07.
https://doi.org/10.1145/3232755.3232756

CCS CONCEPTS

• **Security and privacy** → **Network security**;

KEYWORDS

HTTPS; TLS; SCSV; Certificate Transparency; SCSV; CAA; TLSA.

ACM Reference Format:
Quirin Scheitle, Taejoong Chung, Johanna Amann, Oliver Gasser, Lexi Brent, Georg Carle, Ralph Holz, Jens Hiller, Johannes Naab, Roland van Rijswijk-Deij, Oliver Hohlfeld, Dave Choffnes, and Alan Mislove. 2018. Measuring Adoption of Security Additions to the HTTPS Ecosystem. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3232755.3232756