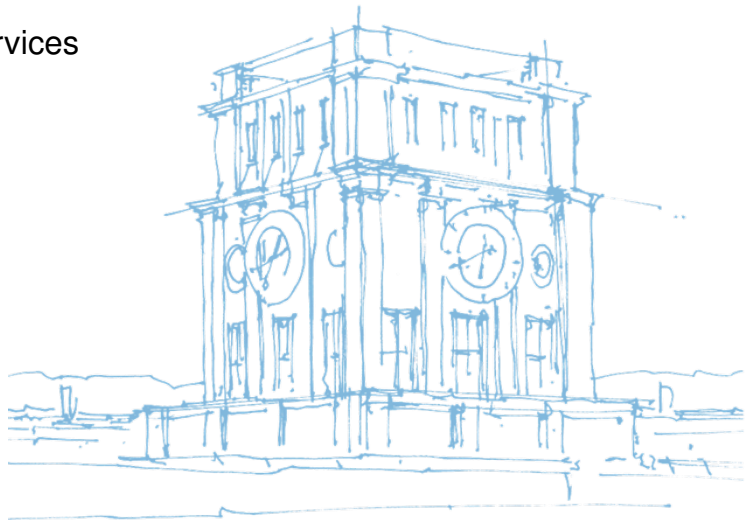
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Measuring Adoption of Security Additions to the HTTPS Ecosystem

Quirin Scheitle

July 16, 2018
Applied Networking Research Workshop (ANRW)
Montreal

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich



Covering Publications

This presentation is based on the following publications:

> Mission Accomplished? HTTPS Security after DigiNotar
> *Johanna Amann*, Oliver Gasser*, Quirin Scheitle*, Lexi Brent, Georg Carle, Ralph Holz*
> Proceedings of the Internet Measurement Conference (IMC 2017), London, UK, Nov. 2017

> A First Look at Certification Authority Authorization (CAA)
> *Quirin Scheitle, Taejoong Chung, Jens Hiller, Oliver Gasser, Johannes Naab, Roland van Rijswijk-Deij, Oliver Hohlfeld, Ralph Holz, Dave Choffnes, Alan Mislove, Georg Carle*
> ACM SIGCOMM Computer Communications Review (CCR), Apr. 2018

Introduction

The HTTPS ecosystem has seen the addition of various security extensions over the past decade, most standardized at IETF.
This body of work aims to assess the *quality* and *quantity* of adoption of these security extensions in the Internet, using active and passive measurements, and controlled experiments.

Highlights in measurements methodology:

- 192M domains scanned from 2 vantage points, using IPv4 and IPv6
  - Large target population avoids bias from, *e.g.*, top lists
- Passive observations on 3 continents, observing 2.4bn TLS connections

Deployment of HTTPS Security Extensions

Mechanism	Standard-ized	Deployment Overall	Deployment Top 10K↓	Effort	Availability Risk
SCSV	2015	49.2M	6789	**none**	**low**
CT-x509	2013	7.0M	1788	**none**	**none**
HSTS	2012	0.9M	349	**low**	**low**
CT-TLS	2013	27,759	171	**high**	**none**
HPKP	2015	6616	156	**high**	**high**
HPKP PL.	2012	479	150	**high**	**high**
HSTS PL.	2012	23,539	144	**medium**	**medium**
CAA	2013	3057	20	**medium**	**low**
TLSA	2012	973	3	**high**	**medium**
CT-OCSP	2013	191	0	**low**	**none**

- High risk and high effort extensions see low deployment
- Highest deployment for technologies without configuration effort: SCSV (software update), CT-x509 (automatically included in certificate)

Deployment of HTTPS Security Extensions

Mechanism	Standard-ized	Deployment Overall	Deployment Top 10K↓	Effort	Availability Risk
SCSV	2015	49.2M	6789	**none**	**low**
CT-x509	2013	7.0M	1788	**none**	**none**
HSTS	2012	0.9M	349	**low**	**low**
CT-TLS	2013	27,759	171	**high**	**none**
HPKP	2015	6616	156	**high**	**high**
HPKP PL.	2012	479	150	**high**	**high**
HSTS PL.	2012	23,539	144	**medium**	**medium**
CAA	2013	3057	20	**medium**	**low**
TLSA	2012	973	3	**high**	**medium**
CT-OCSP	2013	191	0	**low**	**none**

- High risk and high effort extensions see low deployment
- Highest deployment for technologies without configuration effort: SCSV (software update), CT-x509 (automatically included in certificate)

Certification Authority Authorization (CAA) - Introduction

Domain	Type	Flags	Tag	Value
tum.de	CAA	0	issue	"letsencrypt.org"
tum.de	CAA	0	issue	"pki.dfn.de"

Table 1: Exemplary CAA section of DNS zone file

- Controlled Experiment: Assess CA rigor
- Assess Market Adoption
- Role of DNS Providers

Certification Authority Authorization (CAA) - Issuance Experiment

	Configuration	Expected
D1	signed, restrictive	refuse
D2	signed, timeout	refuse
D3	permissive, but critical unknown	refuse
D4	unsigned, timeout	informational
D5	CNAME to D1	refuse
D6	CNAME to NODATA www.D1	informational

Table 3: Test domains and expected CA behavior.

We conduct two rounds of tests, 1 month apart, so CAs have opportunity to fix.

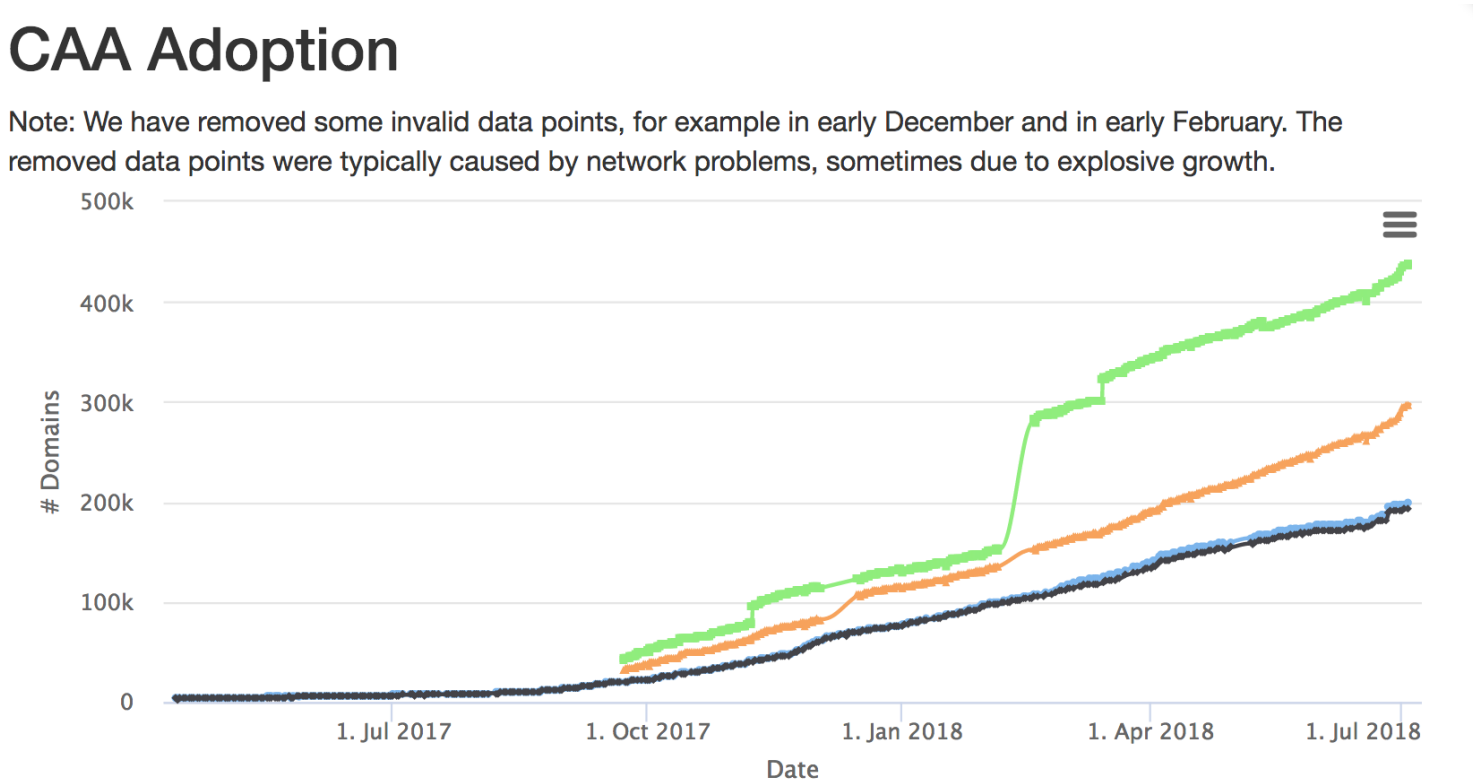
Certification Authority Authorization (CAA) - Issuance Experiment

CA ↓	D1	D2	D3	D4	D5	D6
Expected →	R	R	R	*	R	*
RapidSSL	RR	R[I]	RR	RI	-R	-I
Comodo	[I]R	[I][I]	[I]R	II	-R	-I
Let's Encrypt	RR	RR	RR	RR	-R	-I
GoDaddy	RR	RR	RR	II	-R	-I
StartCom	RR	[I][I]	RR	RI	-[I]	-I
Buypass	RR	[I]R	RR	CI	-R	-R
Certum	RR	[I]R	R[I]	II	-[I]	-I
DigiCert	RR	-R	-R	-I	-R	-I
AlphaSSL	-R	-R	-R	-I	-R	-I
SSL.com	-[I]	-[I]	-R	-I	-R	-I
Symantec	-R	-R	-R	-I	-R	-I
GeoTrust	-R	-[I]	-R	-I	-R	-I

Certification Authority Authorization (CAA) - Market Adoption

Large-Scale Active DNS Scans, configurable live view:

`https://caastudy.github.io`



Certification Authority Authorization (CAA) - DNS Provider Support

DNS Operator	CAA Support	% Domains
T1: GoDaddy, Amazon, Google, Cloudflare *T2:* 1&1, OVH	✓	49.4%
Alibaba, Network Solutions, eNom, Bluehost, NameCheap, WIX, HostGator, NameBright, register.com, 123-reg, WordPress, Xinnet, DreamHost, Yahoo, Rightside, DNSPod	✗	29.6%
Parking Services	–	21.0%

Table 8: CAA configurable at 6 of the top 31 DNS operators as of February 16, 2018 (T2), up from 4 on November 18, 2017 (T1).

These top 31 DNS providers covered 54% of the com/net/org domains.

Summary

- HTTPS security extensions differ vastly in scope and deployment
- Low risk and effort technologies are much more widely deployed
- CAA: Mixed CA rigor, encouraging market adoption, DNS provider support as a critical factor
- Data, software, and tools are publicly available:
  `https://github.com/tumi8/imc17-missionaccomplished`
  `https://caastudy.github.io`