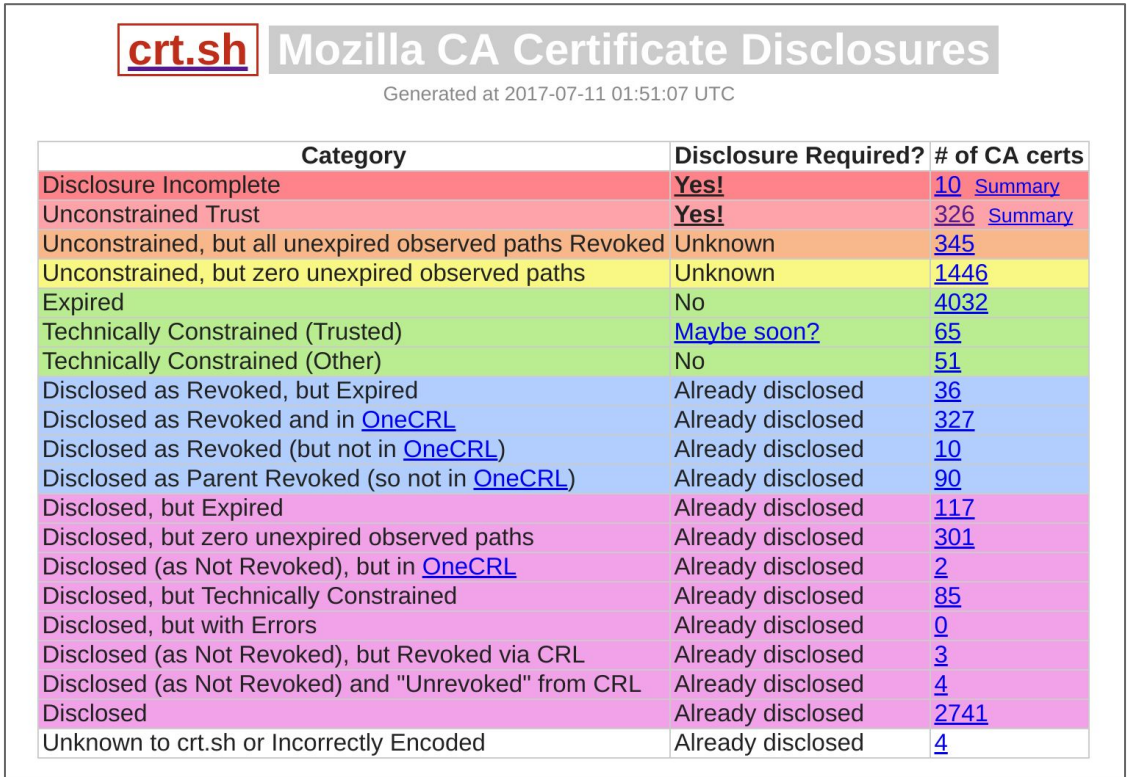
Security and privacy through transparency

Eric Mill, eric.mill@gsa.gov



crt.sh Mozilla CA Certificate Disclosures

Generated at 2017-07-11 01:51:07 UTC

Category	Disclosure Required?	# of CA certs
Disclosure Incomplete	**Yes!**	10 Summary
Unconstrained Trust	**Yes!**	326 Summary
Unconstrained, but all unexpired observed paths Revoked	Unknown	345
Unconstrained, but zero unexpired observed paths	Unknown	1446
Expired	No	4032
Technically Constrained (Trusted)	Maybe soon?	65
Technically Constrained (Other)	No	51
Disclosed as Revoked, but Expired	Already disclosed	36
Disclosed as Revoked and in OneCRL	Already disclosed	327
Disclosed as Revoked (but not in OneCRL)	Already disclosed	10
Disclosed as Parent Revoked (so not in OneCRL)	Already disclosed	90
Disclosed, but Expired	Already disclosed	117
Disclosed, but zero unexpired observed paths	Already disclosed	301
Disclosed (as Not Revoked), but in OneCRL	Already disclosed	2
Disclosed, but Technically Constrained	Already disclosed	85
Disclosed, but with Errors	Already disclosed	0
Disclosed (as Not Revoked), but Revoked via CRL	Already disclosed	3
Disclosed (as Not Revoked) and "Unrevoked" from CRL	Already disclosed	4
Disclosed	Already disclosed	2741
Unknown to crt.sh or Incorrectly Encoded	Already disclosed	4

Secure https://18f.gsa.gov

An official website of the United States government

18F

What we deliver | How we work | About 18F | Blog | Contact

We work with federal agencies to successfully deliver efficient, easy-to-use digital services.

Get in touch

1. We build in the open

18F works in the open from day one of a project, and our resulting code is dedicated fully to the public domain. In addition, any contracts 18F enters into where others will develop software on 18F's behalf ensure that all results are dedicated to the public domain. For our international colleagues, 18F also permanently waives all copyright and related rights worldwide to code created by 18F or its contractors.

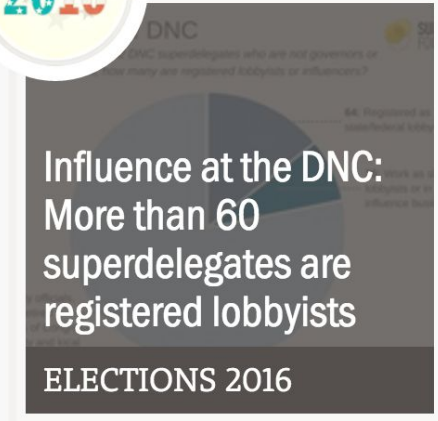
We operate in this way for three reasons:

1. **Operating in the open streamlines communication.** GitHub issues can be used without concern about access permissions and account creation. Access to the project is available regardless of VPN or location, without additional verification requirements. Open source repositories are an easy and accessible location to find source code when pulling in additional experts to check out a problem.
2. **Transparency builds trust with the public**, since everyone's work is accessible to others. Transparency also builds trust within the government, since we can freely pull and cite methods and ideas from existing projects without worrying about possibly revealing something inappropriate.

Making government & politics more accountable & transparent .

2016

SPOTLIGHT



Influence at the DNC: More than 60 superdelegates are registered lobbyists

ELECTIONS 2016

LATEST FROM THE BLOG

AUG. 8, 2016, 3:55 P.M.

A closer look at the problem of open data policy that isn't open

AUG. 8, 2016, 2:06 P.M.

Help us find political dark money in your state

TRANSPARENCY!

Everyone says they love transparency.

TRANSPARENCY!

Everyone says they love transparency.

But then...

Well, we don’t want to give a roadmap to hackers...

But then...

Well, we don’t want to give a roadmap to hackers...

Well, what if it’s somehow PII when it’s connected...

But then...

Well, we don’t want to give a roadmap to hackers...

Well, what if it’s somehow PII when it’s connected...

Well, we don’t want our decisions to be politicized...

But then...

Well, we don’t want to give a roadmap to hackers...

Well, what if it’s somehow PII when it’s connected...

Well, we don’t want our decisions to be politicized...

Well, that’s nice, but we need to just get this done...

But then...

TRANSPARENCY!

Until it feels the least bit uncomfortable!

focus: how transparency can improve privacy and security

Talking about very simple things

- **Data:** Publishing data and information
- **Education:** Explaining concepts to a wider audience
- **Participation:** Easy, open, welcoming processes
- **Defaults**: Assuming open, justifying closed

Can be surprisingly unsimple to ship in practice

The Web PKI

- **Confidentiality.** The visitor's connection is encrypted, obscuring URLs, cookies, and other sensitive metadata.
- **Authenticity.** The visitor is talking to the "real" website, and not to an impersonator or through a "man-in-the-middle".
- **Integrity.** The data sent between the visitor and the website has not been tampered with or modified.

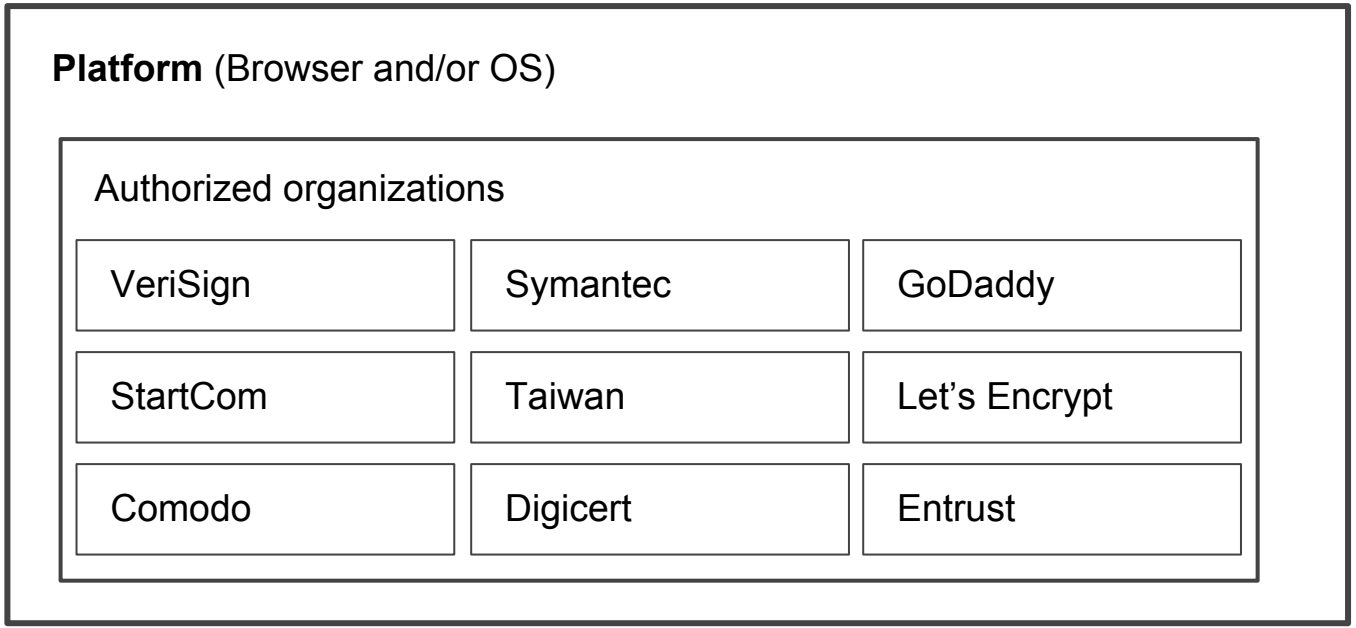
HTTPS has unreasonable requirements

- Requires **zero** user expertise attention to details
- Errors/warnings must be as exceptional as possible
- Can’t gamble TOFU-style for every web service
- Domain owners change hands, keys change
- Needs to allow **everyone** to use encryption

But also: the only widely deployed encryption method that seems to Just Work for regular people

Unreasonable requirements yield unreasonable solutions

corporations trusting other corporations (and governments) on your behalf



Secure | https://blog.mozilla.org/security/2011/08/29/fraudulent-google-com-certificate/

Mozilla Security Blog

AUG
29
2011

Fraudulent *.google.com Certificate

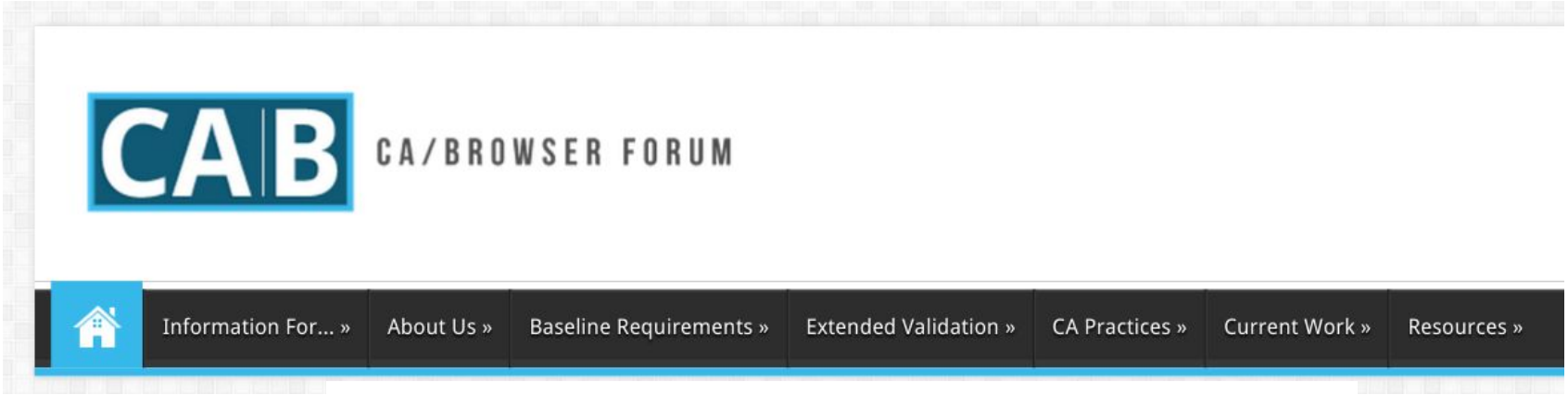

Johnathan Nightingale

65 responses

Update (Sept. 6, 2011 @10:37 a.m. PT):

New security updates for Firefox are now available.

CA / Browser Governance



Baseline Requirements
for the
Issuance and Management
of
Publicly-Trusted Certificates, v.1.2.5

(Current through adoption of Ballot 148 on 2 April 2015)

Microsoft Trusted Root Certificate: Program Requirements

1. Introduction

The Microsoft Trusted Root Certificate Program (“Program”) supports the distribution of qualifying root certificates in Microsoft Windows and other Microsoft Products and Services. This page describes the Program’s general and technical requirements, including information about how a Certificate Authority (CA) can contact Microsoft to request inclusion into the Program.

This document lists the details and requirements for the Program. Certification Authorities ("CAs") that are current members of the Program are listed at http://support.microsoft.com/kb/931125.

How Root Certificate Distribution Works

Starting with the release of Windows Vista, root certificates are updated on Windows automatically. When a user visits a secure Web site (by using HTTPS SSL), reads a secure email (S/MIME), or downloads an ActiveX control that is signed (code signing) and encounters a new root certificate, the Windows certificate chain verification software checks the appropriate Microsoft Update location for the root certificate. If it finds it, it downloads it to the system. To the user, the experience is seamless. The user does not see any security dialog boxes or warnings. The download happens automatically, behind the scenes.

2. Certificate Authority Intake Process

In order to begin the process to be included in the Program, a CA must fill out the application located at http://aka.ms/rootcertapply and email the completed form to trustcert@microsoft.com. This will begin the onboarding process, outlined below:

1. Microsoft will review the application, and may request additional documentation from the CA to determine if the CA meets the Program requirements and whether, in Microsoft’s judgment, the CA’s inclusion into the program will benefit Microsoft’s customers

Apple Root Certificate Program

Program Requirements

Apple uses public key infrastructure (PKI) to secure and enhance the experience for Apple users. Apple products, including our web browser Safari and Mail.app, use a common store for root certificates. Apple requires root certification authorities to meet certain criteria, which include:

- Certification Authority (CA) providers must complete a WebTrust Principles and Criteria for Certification Authorities audit or equivalent.
- Transport Layer Security (TLS) CA providers must complete a WebTrust SSL Baseline Requirements Audit Criteria for Certification Authorities audit or equivalent and maintain compliance with the CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.
- Extended Validation (EV) CA providers must complete a WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL audit or equivalent and maintain compliance with the CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates.
- CA providers must strictly limit the number of roots per CA provider.
- A root certificate must provide broad value to Apple's users.
- CA providers must demonstrate equivalence if submitting a non-WebTrust audit.
- CA providers must notify Apple if they anticipate a change in control. Do not assume trust is transferable.

Submission Process

To begin the submission process, e-mail certificate-authority-program@apple.com requesting inclusion of your root certificate. CA providers will be contacted if any additional information is required, and when consideration of the inclusion request is complete.

Root Acceptance

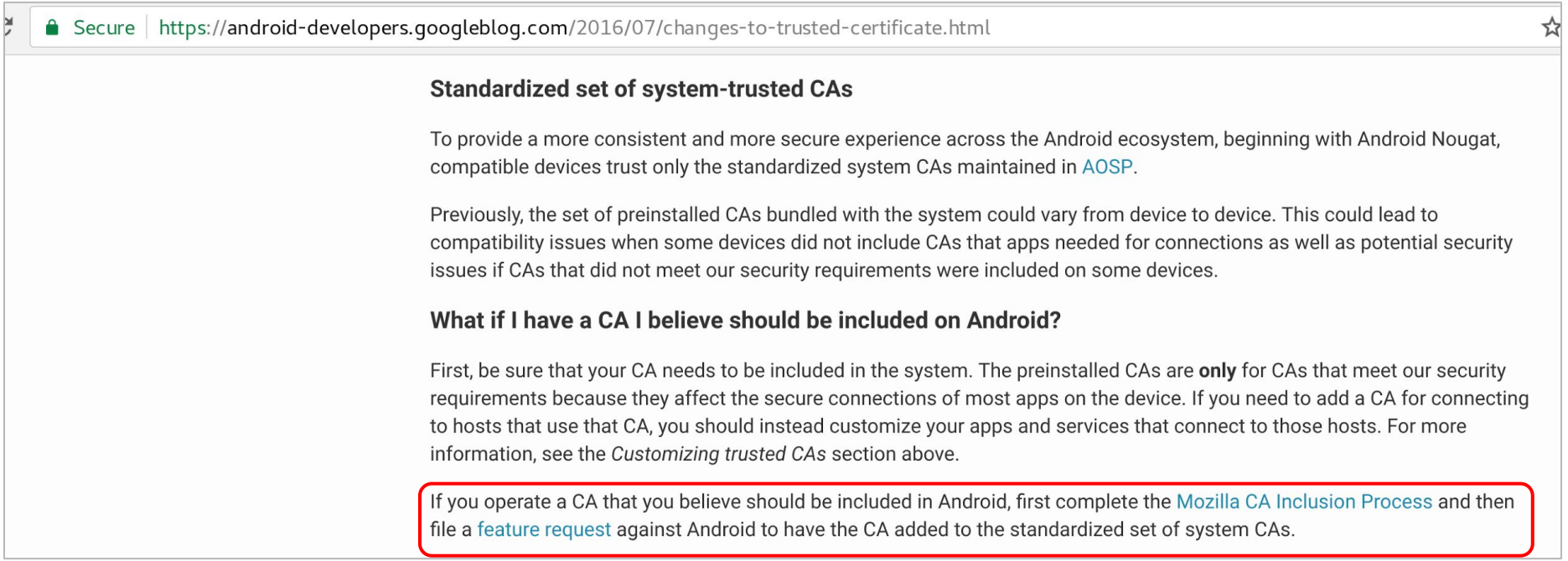
Apple accepts and removes root certificates as it deems appropriate in its sole discretion.

Mozilla Root Store Policy

7.1 Inclusions

We will determine which CA certificates are included in Mozilla's root program based on the benefits and risks of such inclusion to typical users of our products. We will consider adding additional CA certificates to the default certificate set upon request only by an authorized representative of the subject CA. We will make such decisions through a public process, based on objective and verifiable criteria.

Google generally relies on Mozilla



Groups

NEW TOPIC | Mark all as read | Filters

My groups
Home
Starred

Favorites

Click on a group's star icon to add it to your favorites

Recently viewed
Digital44
mozilla.dev.security
certificate-transpa…
Third-Thursday-dc
mozilla.dev.securi…

Recent searches
mozilla phishing (i…
let's encrypt phish…
cnnic (in mozilla.d…

mozilla.dev.security.policy

Shared publicly

30 of 1051 topics (99+ unread)

GlobalSign BR violation (1)
By Roland Bracewell Shoemaker - 1 post - 19 views

Incapsula via GlobalSign issued[ing] a certificate for non-existing domain (testslsslfeb20.me) (2)
By Itzhak Daniel - 2 posts - 45 views

Misissued/Suspicious Symantec Certificates (13)
By Andrew Ayer - 59 posts - 2985 views

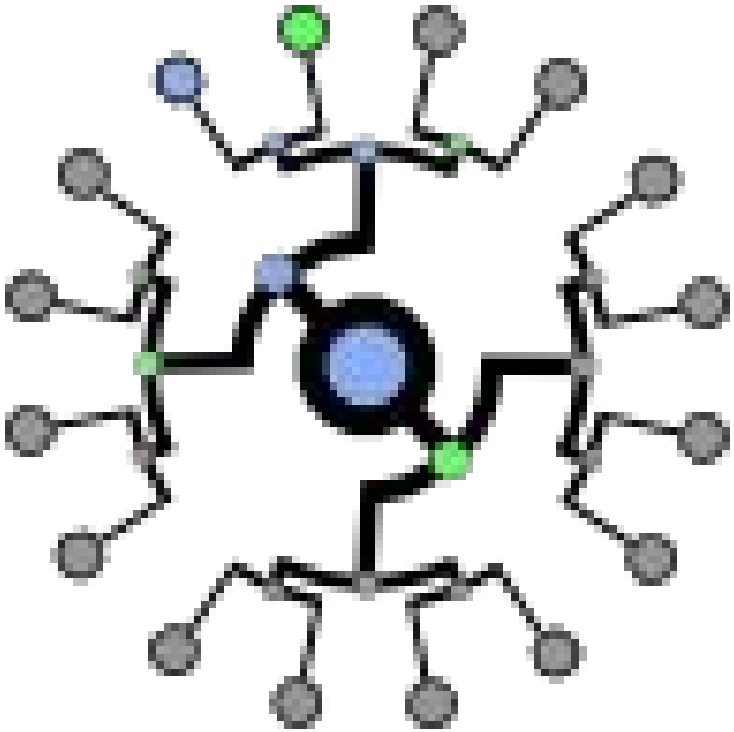
SHA-1 serverAuth cert issued by Trustis in November 2016 (12)
By Rob Stradling - 12 posts - 345 views

Let's Encrypt appears to issue a certificate for a domain that doesn't exist (30)
By Tony Zhaocheng Tan - 30 posts - 213 views

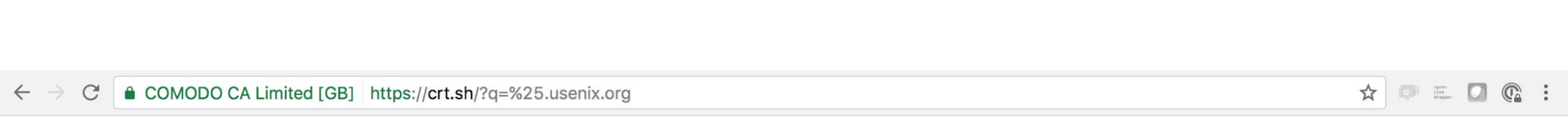
SHA-1 collision (4)
By Adrian R. - 4 posts - 141 views

Audit Reminder Email Summary (4)
By Kathleen Wilson - 4 posts - 221 views

Google Trust Services roots (15)
By Peter Bowen - 15 posts - 376 views



Certificate Transparency



crt.sh Identity Search

Group by Issuer

Criteria	Identity LIKE '%.usenix.org'

Certificates

crt.sh ID	Logged At	Not Before	Identity	Issuer Name
38800445	2016-10-02	2014-03-11	lisa14submissions.usenix.org	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO SSL CA
38800445	2016-10-02	2014-03-11	www.lisa14submissions.usenix.org	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO SSL CA
38505349	2016-10-01	2011-07-26	papers.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
38352912	2016-10-01	2011-09-15	webmail.usenix.org	C=US, O="Thawte, Inc.", OU=Domain Validated SSL, CN=Thawte DV SSL CA
37588460	2016-10-01	2011-05-10	jobs.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
33261433	2016-09-20	2010-03-01	db.usenix.org	C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA, emailAddress=premium-server@thawte.com
33070709	2016-09-20	2010-05-11	jobs.usenix.org	C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA, emailAddress=premium-server@thawte.com
33044686	2016-09-20	2010-07-26	papers.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
9938103	2015-10-07	2015-10-05	*.usenix.org	C=US, O="thawte, Inc.", CN=thawte SHA256 SSL CA
8933375	2015-08-20	2015-08-16	enigma.usenix.org	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
5914630	2014-12-17	2014-03-18	lisa14submissions.usenix.org	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO Extended Validation Secure Server CA
5914630	2014-12-17	2014-03-18	www.lisa14submissions.usenix.org	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO Extended Validation Secure Server CA
5618728	2014-11-16	2014-11-14	www.usenix.org	C=US, O="thawte, Inc.", CN=thawte SHA256 SSL CA
4796811	2014-08-15	2014-07-29	papers.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
4284119	2014-06-07	2014-06-05	www.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
3391130	2014-02-01	2014-01-24	www.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
3346589	2014-01-25	2014-01-24	www.usenix.org	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=EssentialSSL CA
2430373	2013-08-01	2013-07-31	papers.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
2375722	2013-07-22	2011-04-11	r1.usenix.org	O=Root CA, OU=http://www.cacert.org, CN=CA Cert Signing Authority, emailAddress=support@cacert.org
2001872	2013-05-22	2013-05-11	papers.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
1892627	2013-05-10	2011-02-28	db.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
1891053	2013-05-10	2012-07-23	papers.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
1657880	2013-04-26	2012-01-26	www.usenix.org	C=US, O="Thawte, Inc.", CN=Thawte SSL CA

Discovery of unexpected fb.com certificates

Earlier this year, our Certificate Transparency monitoring service alerted us to an important opportunity to better align internal certificate policies. Specifically, we learned that the Let's Encrypt CA issued two TLS certificates for multiple `fb.com` subdomains.

These two certificates raised red flags for our team because they:

- were not issued by our primary CA vendor
- were not authorized by our security team
- were shared with multiple domains that we do not own or control

We determined that these certificates were requested by the hosting vendor managing these domains for several of our microsites. The vendor had authorization from another Facebook team to use Let's Encrypt, but that detail was not communicated to our security team. The investigation was completed in a matter of hours and the certificates were revoked. We found no indications that these certificates were ever controlled by unauthorized parties, and we were able to respond before they had been deployed on the production hosts.

crt.sh Mozilla CA Certificate Disclosures

Generated at 2017-07-13 07:41:08 UTC

Category	Disclosure Required?	# of CA certs
Disclosure Incomplete	**Yes!**	17 Summary
Unconstrained Trust	**Yes!**	314 Summary
Unconstrained, but all unexpired observed paths Revoked	Unknown	345
Unconstrained, but zero unexpired observed paths	Unknown	1436
Expired	No	4033
Technically Constrained (Trusted)	Maybe soon?	64
Technically Constrained (Other)	No	51
Disclosed as Revoked, but Expired	Already disclosed	36
Disclosed as Revoked and in OneCRL	Already disclosed	327
Disclosed as Revoked (but not in OneCRL)	Already disclosed	14
Disclosed as Parent Revoked (so not in OneCRL)	Already disclosed	90
Disclosed, but Expired	Already disclosed	117
Disclosed, but zero unexpired observed paths	Already disclosed	309
Disclosed (as Not Revoked), but in OneCRL	Already disclosed	2
Disclosed, but Technically Constrained	Already disclosed	86
Disclosed, but with Errors	Already disclosed	0
Disclosed (as Not Revoked), but Revoked via CRL	Already disclosed	3
Disclosed (as Not Revoked) and "Unrevoked" from CRL	Already disclosed	4
Disclosed	Already disclosed	2749
Unknown to crt.sh or Incorrectly Encoded	Already disclosed	8

Sustaining Digital Certificate Security

October 28, 2015

Posted by Ryan Sleevi, Software Engineer

This post updates our previous notification of a misissued certificate for google.com

Following our notification, Symantec published a report in response to our inquiries and disclosed that 23 test certificates had been issued without the domain owner's knowledge covering five organizations, including Google and Opera.

However, we were still able to find several more questionable certificates using only the Certificate Transparency logs and a few minutes of work. We shared these results with other root store operators on October 6th, to allow them to independently assess and verify our research.

Symantec performed another audit and, on October 12th, announced that they had found an additional 164 certificates over 76 domains and 2,458 certificates issued for domains that were never registered.

OCT
24
2016

Distrusting New WoSign and StartCom Certificates

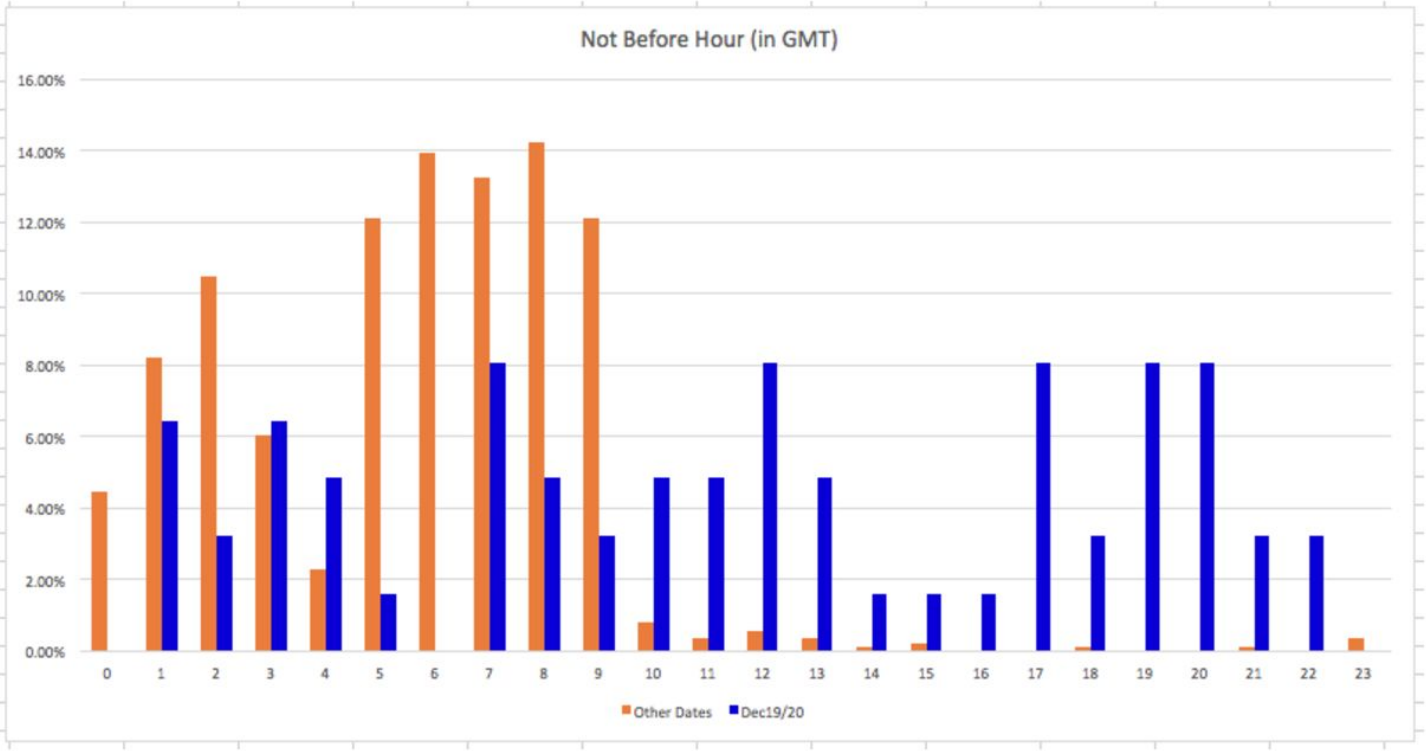
Kathleen Wilson

Mozilla has discovered that a Certificate Authority (CA) called WoSign has had a number of technical and management failures. Most seriously, we discovered they were backdating SSL certificates in order to get around the deadline that CAs stop issuing SHA-1 SSL certificates by January 1, 2016. Additionally, Mozilla discovered that WoSign had acquired full ownership of another CA called StartCom and failed to disclose this, as required by Mozilla policy. The representatives of WoSign and StartCom denied and continued to deny both of these allegations until sufficient data was collected to demonstrate that both allegations were correct. The levels of deception demonstrated by representatives of the combined company have led to Mozilla's decision to distrust future certificates chaining up to the currently-included WoSign and StartCom root certificates.

WoSign and StartCom

This document contains additional information, and Mozilla's proposed conclusion for community discussion, regarding the matter of WoSign and StartCom.

For some weeks now, Mozilla has been investigating a list of potential incidents relating to the CA WoSign. Some of those turned out, in Mozilla's view, to be not WoSign's fault (e.g. Issue T, a mis-issuance for the domain alicdn.com, which got temporarily taken over by an attacker) or only minor (e.g. Issue F, a lack of proper locking); others acknowledged by WoSign are very serious, such as including arbitrary unvalidated domain names in certificates. The most serious from a trust perspective are those that WoSign has denied but where credible evidence exists of the truth of the allegation. One of these was the suggestion (Issue S) that WoSign has been intentionally back-dating certificates to avoid blocks on SHA-1 issuance in browsers, having qualified audits and/or being caught violating the CAB Forum Baseline Requirements. This document gives more information on that allegation; the involvement of StartCom will become clearer as the story unfolds.



For all other Type Y issuances (orange), the notBefore time is almost always during the working day, China time (UTC +0800) - you can even detect the presence of a lunch break. This is further proof that these certificates are manually issued. By contrast, for the Macau certificates (blue), the times are distributed, perhaps randomly, throughout the entire 24 hour period.

Tyro

So what's the connection between all of these different pieces of information?

Tyro is an Australian payments processor, who have historically been customers of GeoTrust (owned by Symantec) and Comodo. You will recall from earlier that the payment processing industry is one of those industries which is having particular difficulty with the SHA-1 transition.

If we look in crt.sh, we can see a number of certificates issued for the DNS name "*.tyro.com" by different CAs. These are wildcard certs, able to be used by any number of hosts inside the tyro.com domain. Ordering them by age, we can construct a picture which looks like this:

Feb 3rd 2010	GeoTrust issues a SHA-1 certificate for *.tyro.com from their Equifax root, valid until May 6th 2013.
Apr 6th 2013	A month before their old cert expires, GeoTrust issues a replacement SHA-1 certificate for *.tyro.com from a GeoTrust root, valid until June 7th 2016. A simple roll-over replacement.
Jan 1st 2016	SHA-1 issuance ban comes into effect.
May 24th 2016	A month before their old cert expires, GeoTrust issues a **SHA-256** certificate for *.tyro.com from a GeoTrust root, valid until June 23rd 2019.

Merchant security is Tyro's priority

Sascha Hess 27/09/2016

This morning my team brought a paper from the Mozilla foundation to my attention which questions the practice of a group of Certificate Authorities.

It uses one of Tyro's current certificates as an example for a "mis-issued certificate" by the relevant Certificate Authority. Tyro welcomes the efforts of the Mozilla foundation to ensure we can continue to trust the internet.

Before delving into the details, let me assure our customers that this issue does not affect the security of your transactions in any way. Tyro is committed to security and protecting customer data at all times. Transparency is one of our core values and as such it comes natural to us to share the details of our SHA-2 journey so far.

During routine security maintenance which included an upgrade (from SHA-1 to SHA-2), we learned that there is a subset of Tyro merchants using out-of-date and unsupported operating systems. The SHA-2 upgrade unexpectedly prevented their POS from connecting to us.

In wanting to do the right thing by our merchants, we made a decision to implement a temporary workaround to allow our small and medium-sized merchants to continue to transact. We reached out in good faith to certificate authorities to provide a few months runway to resolve this big challenge in a way that had minimal impact on merchants. While our internal processes

Kathle. .. dracen. (100)	mozilla-security	**Remediation Plan for WoSign and StartCom** - I think that the steps against StartCom are too extreme	11/2/16
Gervase .. Percy, Han (69)	mozilla-security	**WoSign: updated report and discussion** - 在 2016年11月1日星期二 UTC+8下午6:43:53，Gervase Mar	11/1/16
Peter Kurrasch	mozilla-security	**Deception (was: WoSign: updated report and discussion)** - evidence that WoSign engaged in a delibe	10/11/16
Rob .. Gervase, Peter (89)	mozilla-security	**Re: Incidents involving the CA WoSign** - the CA WoSign On 07/10/16 04:21, Peter Gutmann wrote: >	10/11/16
Gervase .. Eddy (16)	mozilla-security	**WoSign and StartCom: next steps** - attend. WoSign already provided its incident report which includes	10/9/16
Gervase .. Han, Nick (45)	mozilla-security	**WoSign and StartCom** - believes that WoSign mis-behaved in ways that a competent auditor should h	10/7/16
Kyle .. Andrew, Tom (9)	mozilla-security	**Deficiencies in the Web PKI and Mozilla's shepherding thereof, exposed by the WoSign af...** - On 4 Oc	10/5/16
certificate-authority-pr.	mozilla-security	**Apple's response to the WoSign incidents** - Trust for WoSign CA Free SSL Certificate G2 Certificate A	10/1/16
Jakob, Hanno (2)	mozilla-security	**WoSign and StartCom situation possible misreporting by Feist Duck** - misreport the WoSign/StartCom	9/30/16
Peter Kurrasch	mozilla-security	**New Roots? (was: WoSign and StartCom)** - Re: WoSign and StartCom > > Should StartCom/WoSign	9/29/16
Kurt, Rob, Gervase (5)	mozilla-security	**WoSign and duplicate serial numbers** - On 26/09/16 23:45, Kurt Roeckx wrote: > Looking at other cas	9/27/16
Peter .. Richard, Eddy (9)	mozilla-security	**WoSign and StartCom audit reports** - On 09/23/2016 10:11 PM, Peter Bowen wrote: > On Fri, Sep 23,	9/26/16
Jakob .. Florian (21)	mozilla-security	**WoSign Issue L and port 8080** - On 17/09/2016 16:30, Florian Weimer wrote: > * Nick Lamb: > >> On	9/19/16
Gervase .. Percy, Han (12)	mozilla-security	**WoSign's Ownership of StartCom** - reports that WoSign and StartCom may > have failed to comply wi	9/11/16
Richard .. Kurt, Percy (100)	mozilla-security	**RE: Incidents involving the CA WoSign** - sorry that WoSign don't notify all browsers after the incident I	9/7/16
Gervase .. Richard (100)	mozilla-security	**Incidents involving the CA WoSign** - On 31/08/16 19:13, Ryan Sleevi wrote: > A) Remove the CA. Use	9/2/16

Apple's response to the WoSign incidents

mozilla-security x

certificate-authority-program@group.apple.com certificate-authority-program@group.appl 9/30/16

to dev-security-p.

Blocking Trust for WoSign CA Free SSL Certificate G2

Certificate Authority WoSign experienced multiple control failures in their certificate issuance processes for the WoSign CA Free SSL Certificate G2 intermediate CA. Although no WoSign root is in the list of Apple trusted roots, this intermediate CA used cross-signed certificate relationships with StartCom and Comodo to establish trust on Apple products.

In light of these findings, we are taking action to protect users in an upcoming security update. Apple products will no longer trust the WoSign CA Free SSL Certificate G2 intermediate CA.

To avoid disruption to existing WoSign certificate holders and to allow their transition to trusted roots, Apple products will trust individual existing certificates issued from this intermediate CA and published to public Certificate Transparency log servers by 2016-09-19. They will continue to be trusted until they expire, are revoked, or are untrusted at Apple's discretion.

As the investigation progresses, we will take further action on WoSign/StartCom trust anchors in Apple products as needed to protect users.

Regards,

Apple Root Certificate Program

blink-dev ›

Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates

103 posts by 49 authors

Previous Page 1 Next

Ryan Sleevi Mar 23

Other recipients: awha...@chromium.org

Note: Historically, the Google Chrome team has not used the Blink Process for Certificate Authority-related security issues, of which there have been a number over the years. However, we are interested in exploring using this process for such changes, as it provides a greater degree of transparency and public participation. Based on the level of participation and feedback we receive, we may consider using this for the future. However, as CA-related security incidents may require immediate response to protect users, this should not be seen as a guarantee that this process can be used in future incident responses.

Primary eng (and PM) emails:
rsleevi@chromium.org awhalley@chromium.org

Summary
Since January 19, the Google Chrome team has been investigating a series of failures by Symantec Corporation to properly validate certificates. Over the course of this investigation, the explanations provided by Symantec have revealed a continually increasing scope of misissuance with each set of questions from members of the Google Chrome team; an initial set of reportedly 127 certificates has expanded to include at least 30,000 certificates, issued over a period spanning several years. This is also coupled with a series of failures following the previous set of misissued certificates from Symantec, causing us to no longer have confidence in the certificate issuance policies and practices of Symantec over the past several years. To restore confidence and security of our users, we propose the following steps:

- A reduction in the accepted validity period of newly issued Symantec-issued certificates to nine months or less, in order to minimize any impact to Google Chrome users from any further misissuances that may arise.
- An incremental distrust, spanning a series of Google Chrome releases, of all currently-trusted Symantec-issued certificates, requiring they be revalidated and replaced.
- Removal of recognition of the Extended Validation status of Symantec issued certificates, until such a time as the community can be assured in the policies and practices of Symantec, but no sooner than one year.

About 25,900,000 results (0.45 seconds)

Symantec CA Response to Google Proposal and Community ...
https://www.symantec.com/connect/blogs/symantec-ca-proposal
Apr 26, 2017 - On March 23, **Google** posted a blog outlining a proposal to change how **Symantec's** SSL/TLS certificates are recognized in Chrome.

Symantec's Response to Google's subCA Proposal | Symantec ...
https://www.symantec.com/connect/.../symantec-s-response-google-s-subca-proposal
Jun 1, 2017 - **Google** shared this new proposal for **Symantec's** CA with the community on May 15. We have since been reviewing this proposal and weighing ...

Top stories

Symantec explores selling web certificates business: sources

Reuters · 1 day ago

Symantec Considering Sale of a Billion Dollar Business

TheStreet.com · 19 hours ago

Symantec looks to divest web certification unit for $1b, reshifting focus

Tech Wire Asia · 1 day ago

mozilla.dev.security.policy ›

Misissued/Suspicious Symantec Certificates

64 posts by 17 authors G+1

Andrew Ayer

Other recipients: mozilla-dev-s...@lists.mozilla.org

I. Misissued certificates for example.com

On 2016-07-14, Symantec misissued the following certificates for example.com:

https://crt.sh/?sha256=A8F14F52CC1282D7153A13316E7DA39E6AE37B1A10C16288B9024A9B9DC3C4C6
https://crt.sh/?sha256=8B5956C57FDCF720B6907A4B1BC8CA2E46CD90EAD5C061A426CF48A6117BFBFA
https://crt.sh/?sha256=94482136A1400BC3A1136FECA3E79D4D200E03DD20B245D19F0E78B5679EAF48
https://crt.sh/?sha256=C69AB04C1B20E6FC7861C67476CADDA1DAE7A8DCF6E23E15311C2D2794BFCD11

I confirmed with ICANN, the owner of example.com, that they did not authorize these certificates. These certificates were already revoked at the time I found them.

II. Suspicious certificates for domains containing the word "test"

On 2016-11-15 and 2016-10-26, Symantec issued certificates for various domains containing the word "test" which I strongly suspect were misissued:

https://crt.sh/?sha256=b81f339b971eb763cfc686adbac5c164b89ad03f8afb55da9604fd0d416bbd21
https://crt.sh/?sha256=f45d090e1bf24738a8e86734aa7acf7c9e65b619eb19660b1f73c9973f11b841
https://crt.sh/?sha256=bcbc26c9e06c4fe1c9e4d55fa27a501c504ea84e23e114b8ac004f7c0776cd0b

Gervase Markham via d. (4)	mozilla-security	**Symantec meeting and status** - Re: Symantec meeting and status Hi Peter, I note you have copied in	Jul 3
Gervase Markham via . (19)	mozilla-security	**Symantec response to Google proposal** - On 20/06/2017 08:08, Gervase Markham wrote: > On 20/06	Jun 20
Gervase Markham via . (11)	mozilla-security	**Mozilla requirements of Symantec** - On 20/06/2017 09:05, Ryan Sleevi wrote: > On Mon, Jun 19, 201	Jun 20
Peter Kurrasch via de. (5)	mozilla-security	**An alternate perspective on Symantec** - care about Symantec or even website security because my li	Jun 8
Gervase Markham via . (26)	mozilla-security	**Google Plan for Symantec posted** - require of Symantec. * Mozilla would wish, after 2017-08-08, to alt	May 25
Gervase Markham via . (27)	mozilla-security	**Symantec: Update** - default, Symantec shall issue certificates with embedded SCTs > (soft-fail for failu	May 22
Gervase Markham via . (14)	mozilla-security	**Draft further questions for Symantec** - m aware Symantec was required to upload certificates to CT or	May 19
Gervase, Eric (38)	mozilla-security	**Symantec: Draft Proposal** - Symantec logs TLS server certificates that are intended to be trusted by C	May 15
Gervase, Eric, Lee (29)	mozilla-security	**Symantec Conclusions and Next Steps** - steve_medin=symantec.com@lists.mozilla.org] On Behalf O	May 15
Gervase Markham via dev-.	mozilla-security	**Questions for Symantec (2)** - program requesting Symantec's answers to the following questions by cl	May 11
Ryan Sleevi via dev-s. (2)	mozilla-security	**Google's past discussions with Symantec** - one thing Symantec has not decided to obey Google on is	Apr 27
Gervase Markham via . (11)	mozilla-security	**Questions for Symantec** - do. Symantec noted that they are path length > constrained > > in their resp	Apr 27
Steve, Gervase, Eric (23)	mozilla-security	**Symantec Response L** - I probably need some additional information to see if my partners can effectiv	Apr 19
Steve Medin via dev-. (12)	mozilla-security	**Symantec Response B** - improperly included Symantec's BR-compliance OID. If > the cert wasn't a BI	Apr 17
Gervase Markham via d. (7)	mozilla-security	**Symantec Issues doc updated** - Browser and Symantec sides > of the process) are likely to be unavai	Apr 12
Steve Medin via dev-s. (9)	mozilla-security	**Symantec Response X** - The only Symantec RAs capable of authorizing and issuing publicly trusted S	Apr 11

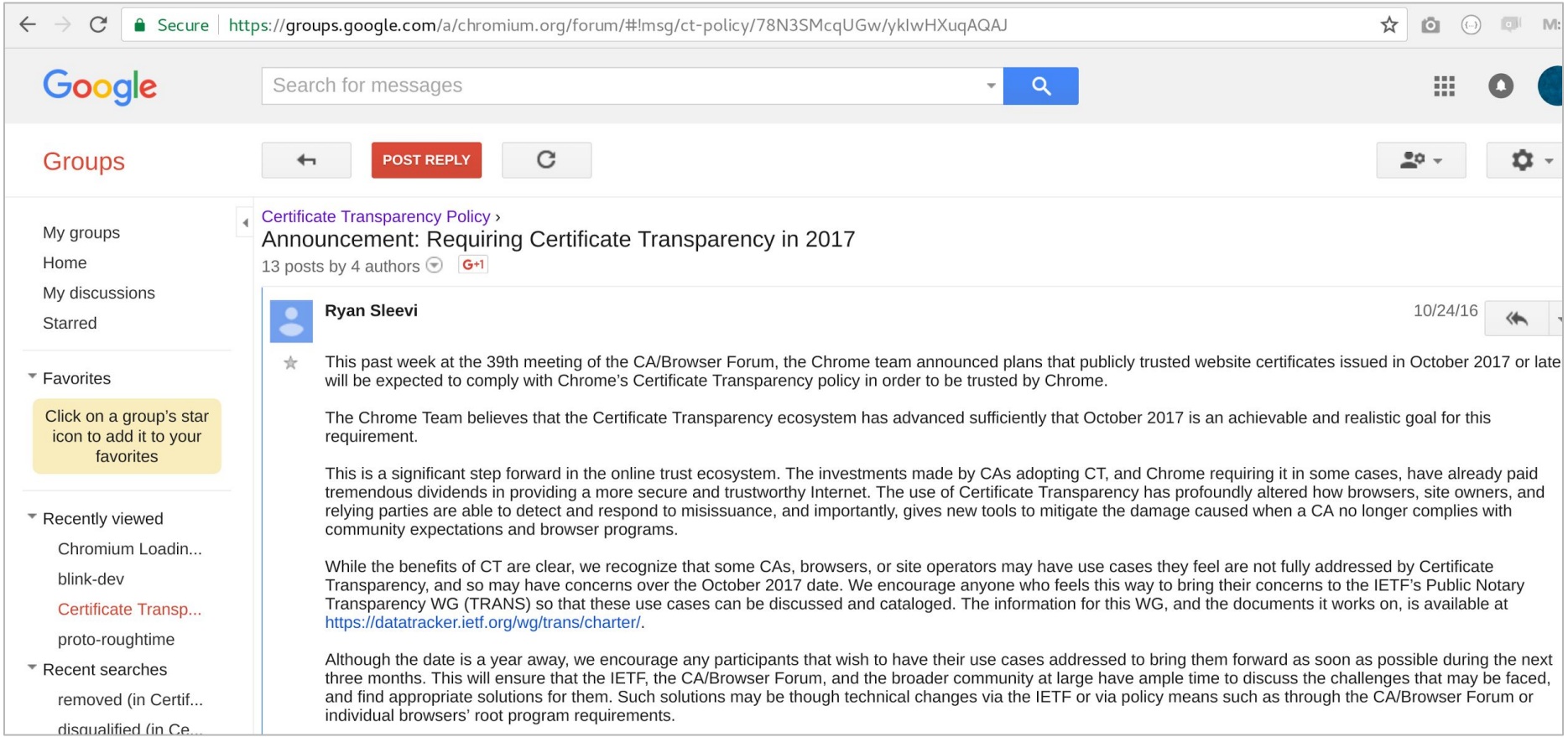
Mozilla Proposal re: Symantec

Gervase Markham
v1.0 - 2017-05-23

Recently, Mozilla has been conducting an investigation into the Certificate Authority Symantec, and the various issues that have been raised over the past 2-3 years with their PKI, certificate issuance processes and infrastructure. Mozilla, as a public benefit organization, takes its role as a root store operator and protector of the integrity of the security system of the Web very seriously. We run our root program in an open and transparent fashion in order to help retain the confidence of the public in the security of the web.

Having considered the list of issues, Symantec have now posted their proposal for a set of actions they propose to take to attempt to restore trust. This document you are reading represents a proposed response from Mozilla to the issues we discovered and Symantec's proposal. It is open for discussion and comment in mozilla.dev.security.policy, and so may change in small or large ways. The final decision-maker on what action to take will be Kathleen Wilson, module owner of the CA Certificates module.

Certificate Transparency can be *technically enforced* by clients


Secure https://groups.google.com/a/chromium.org/forum/#!msg/ct-policy/78N3SMcqUGw/ykIwHXuqAQAJ
Google
Search for messages
Groups
POST REPLY
My groups
Home
My discussions
Starred
Favorites
Click on a group's star icon to add it to your favorites
Recently viewed
Chromium Loadin...
blink-dev
Certificate Transp...
proto-roughtime
Recent searches
removed (in Certif...
disqualified (in Ce...
Certificate Transparency Policy ›
Announcement: Requiring Certificate Transparency in 2017
13 posts by 4 authors
G+1
Ryan Sleevi
10/24/16
This past week at the 39th meeting of the CA/Browser Forum, the Chrome team announced plans that publicly trusted website certificates issued in October 2017 or late will be expected to comply with Chrome's Certificate Transparency policy in order to be trusted by Chrome.
The Chrome Team believes that the Certificate Transparency ecosystem has advanced sufficiently that October 2017 is an achievable and realistic goal for this requirement.
This is a significant step forward in the online trust ecosystem. The investments made by CAs adopting CT, and Chrome requiring it in some cases, have already paid tremendous dividends in providing a more secure and trustworthy Internet. The use of Certificate Transparency has profoundly altered how browsers, site owners, and relying parties are able to detect and respond to misissuance, and importantly, gives new tools to mitigate the damage caused when a CA no longer complies with community expectations and browser programs.
While the benefits of CT are clear, we recognize that some CAs, browsers, or site operators may have use cases they feel are not fully addressed by Certificate Transparency, and so may have concerns over the October 2017 date. We encourage anyone who feels this way to bring their concerns to the IETF's Public Notary Transparency WG (TRANS) so that these use cases can be discussed and cataloged. The information for this WG, and the documents it works on, is available at https://datatracker.ietf.org/wg/trans/charter/.
Although the date is a year away, we encourage any participants that wish to have their use cases addressed to bring them forward as soon as possible during the next three months. This will ensure that the IETF, the CA/Browser Forum, and the broader community at large have ample time to discuss the challenges that may be faced, and find appropriate solutions for them. Such solutions may be though technical changes via the IETF or via policy means such as through the CA/Browser Forum or individual browsers' root program requirements.

For certificates to validate, they'll need to have been logged

Meaningfully detects and deters phishing, fraud, and other attacks

Data transparency

+

Process transparency

HTTPS in the U.S. Government

Executive policy: HTTPS + HSTS everywhere

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 8, 2015

M-15-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Tony Scott
Federal Chief Information Officer

SUBJECT: **Policy to Require Secure Connections across Federal Websites and Web Services**

This Memorandum requires that all publicly accessible Federal websites and web services[1] only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).

USG can be a difficult environment to make new encryption-related policies

Why we use HTTPS for every .gov we make

By **Eric Mill**

November 13, 2014

security | best practices | https

The `.gov` in government websites carries a lot of weight. Citizens expect government websites to be secure, trustworthy, and reliable. Citizens expect anything they read on a `.gov` website to be official, and they expect any information they submit to that website — especially if they're submitting personal information — to be sent safely and only to the government.

The first .gov domains hardcoded into your browser as all-HTTPS

By **Eric Mill**

February 9, 2015

https security best practices

```
1778.    { "name": "uspsoig.gov", "include_subdomains": true, "mode": "force-https" },
1779.    { "name": "notalone.gov", "include_subdomains": true, "mode": "force-https" },
1780.    { "name": "aids.gov", "include_subdomains": true, "mode": "force-https" },
1781.    { "name": "itdashboard.gov", "include_subdomains": true, "mode": "force-https" },
1782.    { "name": "paymentaccuracy.gov", "include_subdomains": true, "mode": "force-https" },
1783.    { "name": "cao.gov", "include_subdomains": true, "mode": "force-https" },
1784.    { "name": "cfo.gov", "include_subdomains": true, "mode": "force-https" },
1785.    { "name": "cio.gov", "include_subdomains": true, "mode": "force-https" },
```

Every `.gov` website, no matter how small, should give its visitors a secure, private connection. Plain HTTP (`http://`) connections are neither secure nor private, and can be easily intercepted and impersonated. In today's web browsers, the best and easiest way to fix that is to use HTTPS

FTC.gov is now HTTPS by default

By: Ashkan Soltani, Chief Technologist | Mar 6, 2015 11:00AM

In another step to enhance the FTC's website, I'm pleased to announce that our agency has enabled encryption by default (HTTPS) for ftc.gov, our primary public domain, and home of the Tech@FTC blog. Ironically, as I was preparing this post, the entire internet has been FREAKing out about another vulnerability in SSL.

While we have long provided secure transport for FTC domains that handle sensitive consumer data, such as complaint data and email subscriptions, consumers will now browse our entire site more privately, and their browsers will automatically verify the identity of the website to which they're connecting – an important step to mitigate attempts to impersonate the FTC.

March 2015: Released for 30 days of public comment

The HTTPS-Only Standard

- Home
- Why Everything?
- FAQ
- Server Name Indication
- Strict Transport Security
- Mixed Content
- Migrating APIs
- Other Technical Concepts
- Resources

The HTTPS-Only Standard

The American people expect government websites to be secure and their interactions with those websites to be private. Hypertext Transfer Protocol Secure (HTTPS) offers the strongest privacy protection available for public web connections with today's internet technology. The use of HTTPS reduces the risk of interception or modification of user interactions with government online services

This proposed initiative, "The HTTPS-Only Standard," would require the use of HTTPS on all publicly accessible Federal websites and web services.

We encourage your feedback and suggestions.

Goal

All publicly accessible Federal websites and web services [1] only provide service over a secure

+1 on behalf of Google Chrome Public Comment
#104 by asirap was closed on Jun 8, 2015

OTI Public Comment: OTI Supports the Proposed HTTPS-Only Standard Public Comment
#103 by natmey was closed on Jun 8, 2015

Very excited to see this proposal Public Comment
#101 by adrifelt was closed on Jun 8, 2015

Secure-to-origin for CDNs Public Comment
#100 by jsha was closed on Jun 8, 2015

Advise secure cookies Public Comment
#99 by jsha was closed on Jun 8, 2015

EFF public comment: HTTPS-Only is necessary and overdue Public Comment
#98 by jsha was closed on Jun 8, 2015

Changes per IETF IAB comments ✓ Public Comment
#97 by josephlhall was closed on Jun 8, 2015

A much-needed bar-raising Public Comment 1
#96 by svitka was closed on Jun 8, 2015

+1 from X-Lab. Public Comment
#95 by saschameinrath was closed on Jun 8, 2015

+1 from the W3C TAG Public Comment 1
#94 by torgo was closed on Jun 8, 2015

Finalizing the HTTPS-Only Standard as formal policy #108

Merged **konklone** merged 15 commits into `master` from `changes` on Jun 8, 2015

Conversation 0 | Commits 15 | Files changed 5

Below are some details on the changes we've made since the original proposal. I've mapped some to commits, but some are lumped in to others.

- `725b141` - Emphasize that high-priority websites should begin the HTTPS migration process immediately, and set a specific deadline of **December 31, 2016**.
- `7f0836c` - Elaborate on planning for change, mention cipher/protocol choices and forward secrecy explicitly.
- `6cb9a30` and `eee26c9` - Incorporate the IETF's suggested revisions on integrity in #97, and then make further edits to relevant areas to clarify mixed content and SNI. Thanks to **@josephlhall** for the detailed pull request.
- `e2061fe` - A number of non-substantive copy changes, and rewording to reflect the transition from proposal to policy.

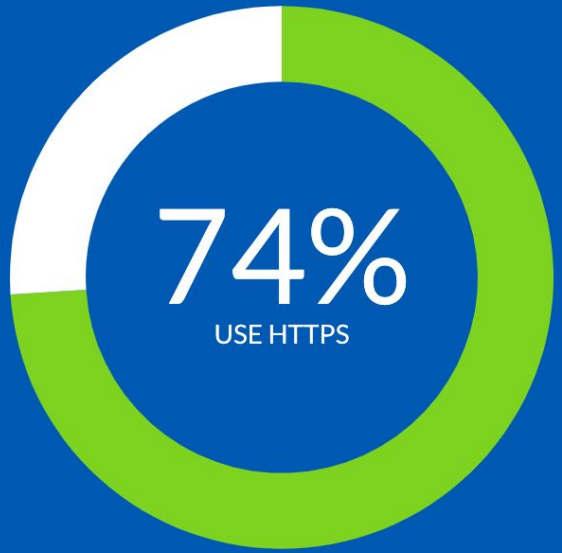
Thank you again to everyone who participated!

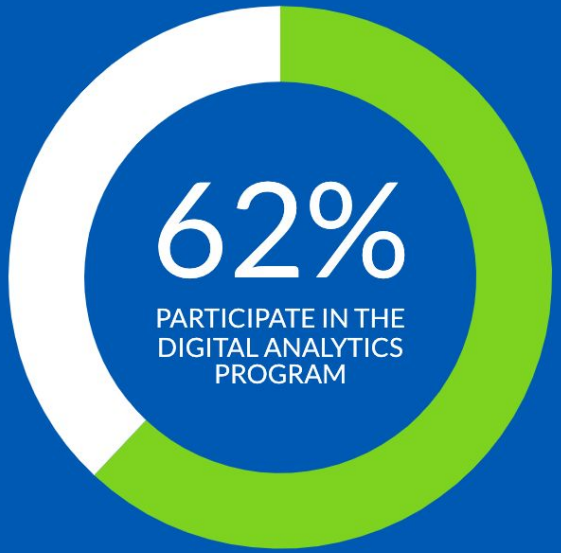
Fixes #78, fixes #79, fixes #80, fixes #81, fixes #83, fixes #84, fixes #86, fixes #87, fixes #88, fixes #89, fixes #92, fixes #93, fixes #94, fixes #95, fixes #96, fixes #97, fixes #98, fixes #99, fixes #100, fixes #101, fixes #103, fixes #104, fixes #105, fixes #106, and fixes #107.

Public comments helped immensely in finalizing a strong policy

Pulse

How federal government domains are meeting best practices on the web.





Domain	Uses HTTPS	Enforces HTTPS	Strict Transport Security (HSTS)	Preloaded (recommended)
acquisition.gov	Yes	Yes	Yes	
HTTPS enforced. Consider preloading this domain to enforce HTTPS across the entire zone. No public subdomains found. Consider preloading.				
ahrq.gov	Yes	Yes	Yes	
HTTPS enforced. Consider preloading this domain to enforce HTTPS across the entire zone. **Known public subdomains:** **66%** of 88 public sites known to Censys enforce HTTPS. **77%** of 26 public sites known to the Digital Analytics Program enforce HTTPS. For more details, read our methodology, or download subdomain data for this agency.				
americathebeautifulquarters.gov	Yes	Yes	Yes	Ready
Almost there! Domain is ready to be submitted to the HSTS preload list. All subdomains will be protected when preloading is complete.				

https://https.cio.gov/guide/

- Compliance FAQ
  - What protocols are covered by M-15-13?
  - Do I need to shut off port 80?
  - What about network services that don't actually serve web content?
  - What does "all Federal agency domains or subdomains" include?
  - What about domains that are only used to redirect visitors to other websites?
  - Do domains that redirect to other external domains need to redirect internally to HTTPS before redirecting externally?
  - What about domains that are technically public, but in practice are only used internally?
  - What happens to visitors using browsers that don't support HSTS, like older versions of Internet Explorer?
  - This site redirects users to HTTPS – why is Pulse saying it doesn't enforce HTTPS?
  - Are federally operated certificate revocation services (CRL, OCSP) also required to move to HTTPS?

Tracking the U.S. government's progress on moving to HTTPS

- The White House policy generated significant HTTPS adoption in the U.S. government, to the point that **the government now outpaces the private sector on HTTPS**.
- HTTPS has gone from **a clear minority to a clear majority** of support across executive branch .gov domains since the release of the policy.
- Web traffic data suggests that **HTTPS is now used for most web requests** to executive branch .gov web services.
- In 2017, agencies should focus on closing gaps through the use of **inexpensive and free certificates**, and by **preloading their domains** wherever possible.

from https://18f.gsa.gov/2017/01/04/tracking-the-us-governments-progress-on-moving-https/

Second order effects

National Cybersecurity Assessments & Technical Services Team (DHS)

We hack governments (and others) to improve 'cyber hygiene'.

The Internet https://www.dhs.gov/cy... ncats_info@hq.dhs.gov

README.md

Services

We are the National Cybersecurity Assessments and Technical Services (NCATS) team, a division of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). All NCATS services are provided at no cost.

README.md

Pushing HTTPS 🔒

`pshtt` (*"pushed"*) is a tool to scan domains for HTTPS best practices. It saves its results to a CSV (or JSON).

`pshtt` was developed to *push* organizations— especially large ones like the US Federal Government 🇺🇸 — to adopt HTTPS across the enterprise. Federal .gov domains must comply with M-15-13, a 2015 memorandum from the White House Office of Management and Budget that requires federal agencies to enforce HTTPS on their web sites and services by the end of 2016. Much has been done, and still more yet to do.

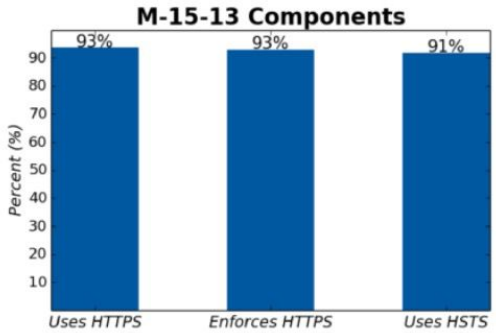
`pshtt` is a collaboration between the Department of Homeland Security's National Cybersecurity Assessments and Technical Services (NCATS) team and the General Service Administration's 18F team, with contributions from NASA and various non-governmental organizations.

Getting Started

`pshtt` can be installed as a module, or run directly from the repository.

Overview

We measure the presence and enforcement of HTTPS for your agency's publicly-accessible .gov domains. **This report includes all agency-registered domains and known subdomains** (see the Methodology section for a description of how these domains are collected). Domains which do nothing but redirect to other websites *are* measured.



- **325** domains (93.9%) have HTTPS enabled
- **322** domains (93.1%) default to HTTPS
- **318** domains (91.9%) use HSTS
- **314** domains compliant with M-15-13

Office of Personnel Management owns 24 second-level .gov domains and NCATS discovered 449 subdomains. **Of these, 20 second-level domains and 326 subdomains responded to HTTP/HTTPS requests over the public Internet**. Domains that did not respond to these requests are marked 'non-web' and are removed from the above compliance figures. See the Results section for a list of non-web domains.

Blog

Open source collaboration across agencies to improve HTTPS deployment

By **Cameron Dixon**

January 6, 2017

https security open source

NASA

GitHub, Inc. [US] https://github.com/dhs-ncats/pshtt/pull/65

This repository Search Pull requests Issues Marketplace Gist

dhs-ncats / pshtt

Unwatch 30

Code Issues 22 Pull requests 0 Projects 0 Wiki Insights

Debug logging in main pshtt exception cases #65

Merged h-m-f-t merged 1 commit into dhs-ncats:master from unknown repository on Mar 24

Conversation 2 Commits 1 Files changed 2

egyptiankarim commented on Mar 21 • edited Contributor

A slightly more thought out attempt at pull request #62. I did a bit of copy-editing to the existing warning messages throughout the main exception cases and added a debug level logging line for the actual exception messages.

Debug logging in main pshtt exception cases ✓ 1169aef

konklone reviewed on Mar 22 View changes

From launch to landing: How NASA took control of its HTTPS mission

By **Karim Said**

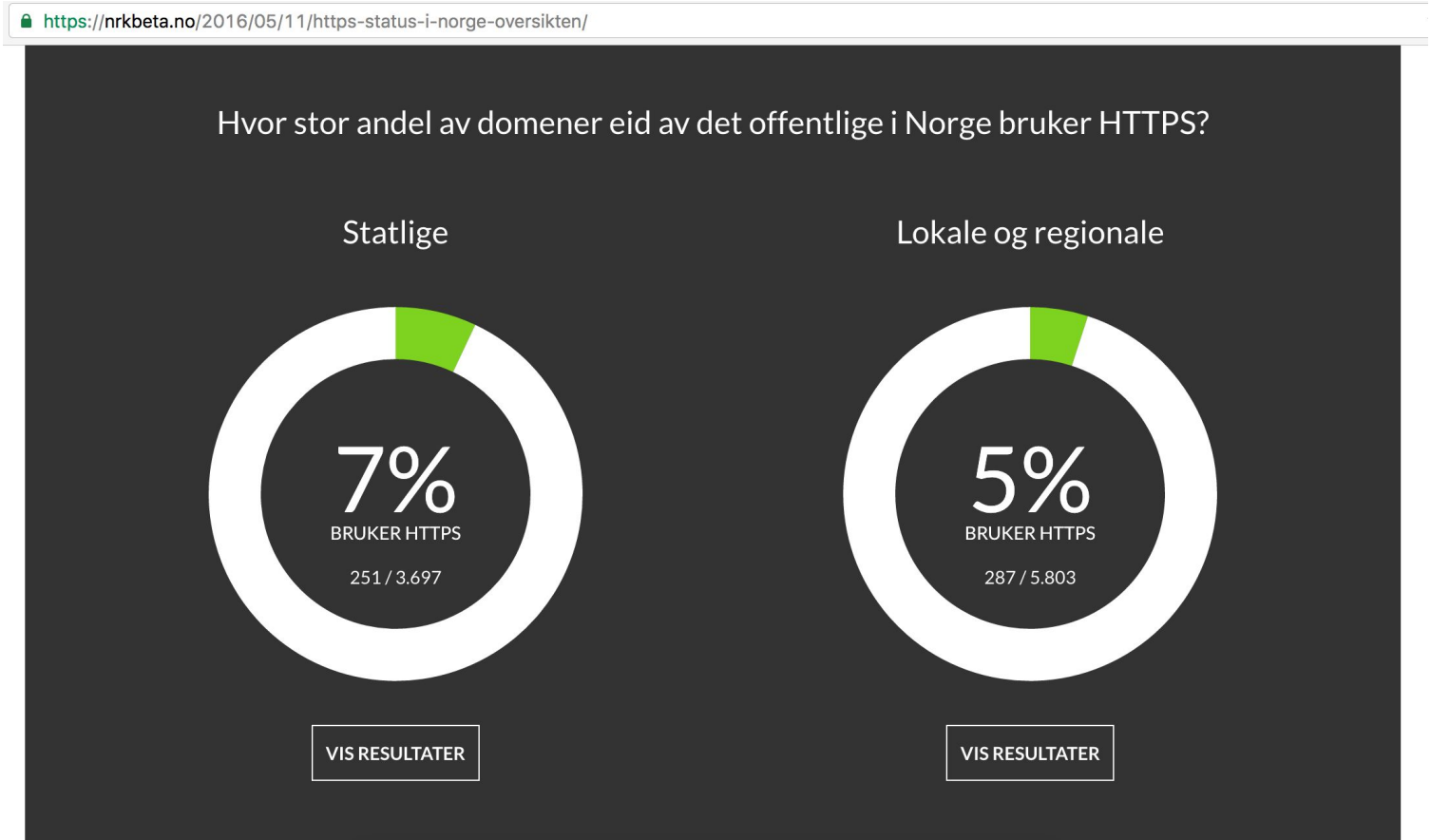
May 25, 2017

https security

Editor's note: This is a guest post by Karim Said of NASA. Karim was instrumental in NASA's successful HTTPS and HSTS migration, and we're happy to help Karim share the lessons NASA learned from that process.

In 2015, the White House Office of Management and Budget released M-15-13, a "Policy to Require Secure Connections across Federal Websites and Web Services". The memorandum emphasizes the importance of protecting the privacy and security of the public's browsing activities on the web, and sets a goal to bring all federal websites and services to a consistent standard of enforcing HTTPS and HSTS.

Forked by a Norwegian newspaper



Action by the Norwegian government

Oppdrag NSM - sikker tilkobling; HTTPS

Nasjonal sikkerhetsmyndighet viser til brev fra Justis- og beredskapsdepartementet av 1. april 2016 der NSM bes å vurdere bruk av sikker tilkobling for statlige webtjenester innen 6. mai 2016 (med innvilget fristutsettelse til 31. mai 2016). NSM vil i dette brevet vurdere hensiktsmessigheten av å innføre krav om sikker tilkobling for statlige webtjenester ved bruk av *Hypertext Transfer Protocol Secure* (HTTPS). Brevet omtaler også de nasjoner NSM er kjent med som har innført tilsvarende krav eller anbefalinger.

NSM har utarbeidet en rapport om bruk av HTTPS i for offentlige tjenester. Rapporten er vedlagt dette svaret i sin helhet og utdyper emnet ytterligere.

Vurdering av hensiktsmessigheten av å innføre krav om sikker tilkobling til statlige webtjenester

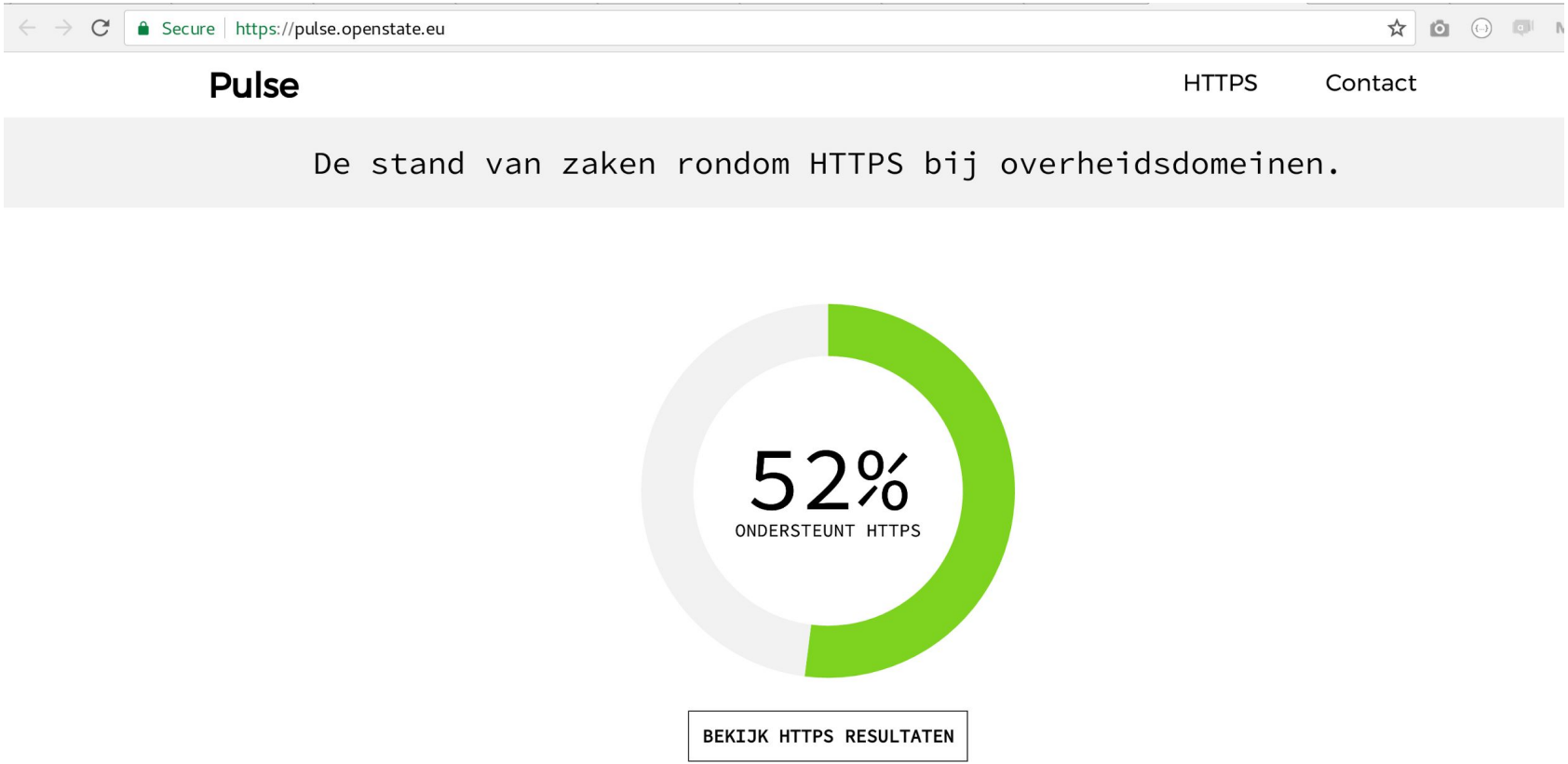
NSMs anbefaling

NSM mener at alle offentlige tjenester på web alltid skal benytte HTTPS. Dette vil gi både

Tilsvarende anbefalinger fra andre nasjoner

NSM er kjent med at amerikanske og tyske myndigheter har innført krav om bruk av HTTPS i offentlig forvaltning. I USA kravstilte Office of Management and Budget i memorandum av 8.

Forked by a Dutch civil society organization



Action by the Dutch government

Secure | https://www.forumstandaardisatie.nl/standaard/https-en-hsts

Forum Standaardisatie

Home | Lijst open standaarden | Toetsen van standaarden | Thema's | Vergaderingen | FAQ | Zoek naar... | Zo

Home » Lijst open standaarden

HTTPS en HSTS

Over de standaard

Beschrijving	Beveiligde webcommunicatie
Lijst status	Aanbevolen

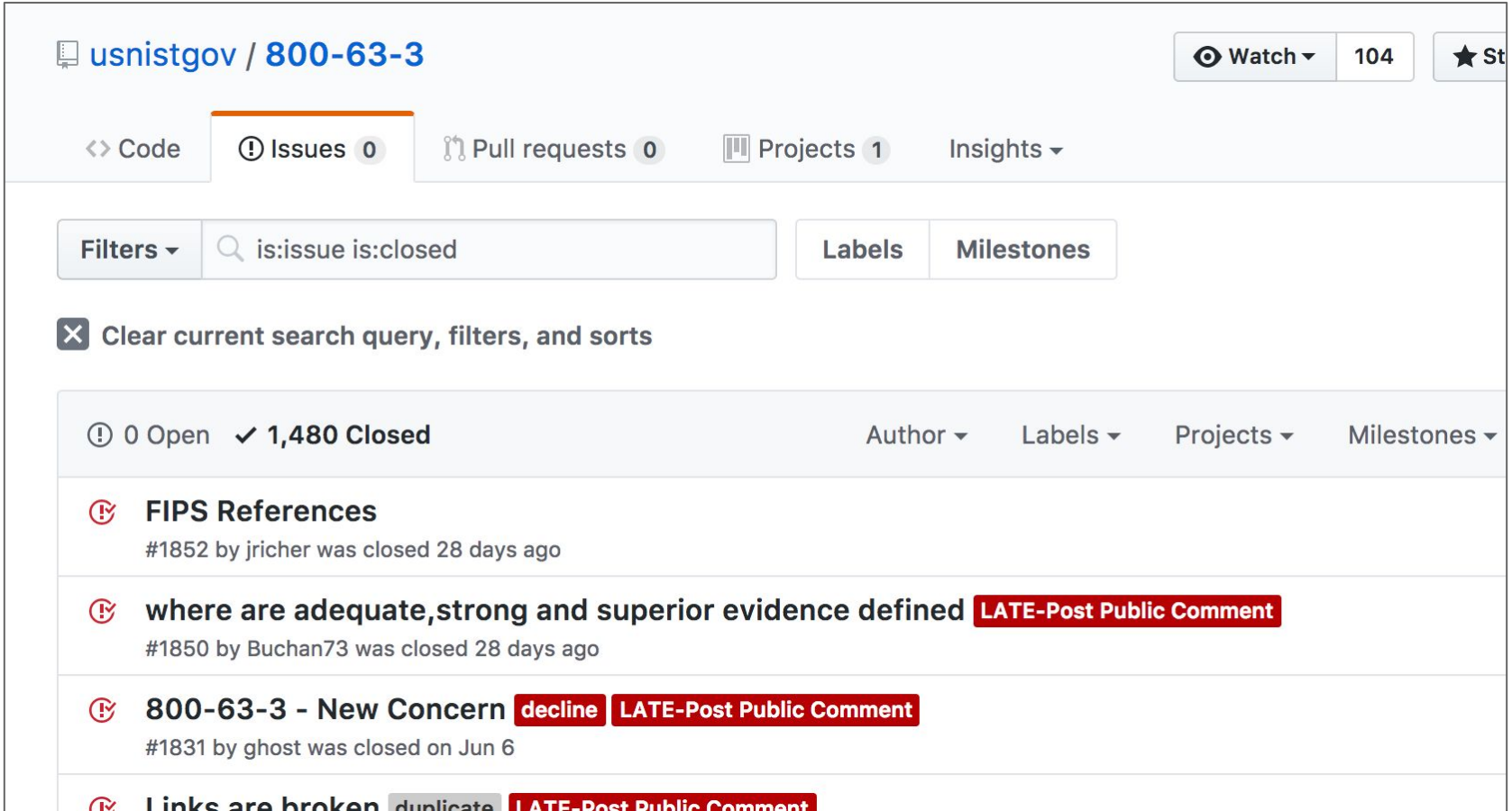
Uitleg

Nut	HTTPS, is een uitbreiding op het HTTP-protocol met als doel een veilige uitwisseling van gegevens. Bij gebruik van HTTPS worden

Bart Knubben

Adviseur internet- en beveiligingsstandaarden

NIST now doing public comment in the same way



Came out of a public comment on GitHub

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

require the subscriber to choose a different value.

Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret. This is particularly important following the rejection of a memorized secret on the above list as it discourages trivial modification of listed (and likely very weak) memorized secrets [Blacklists].

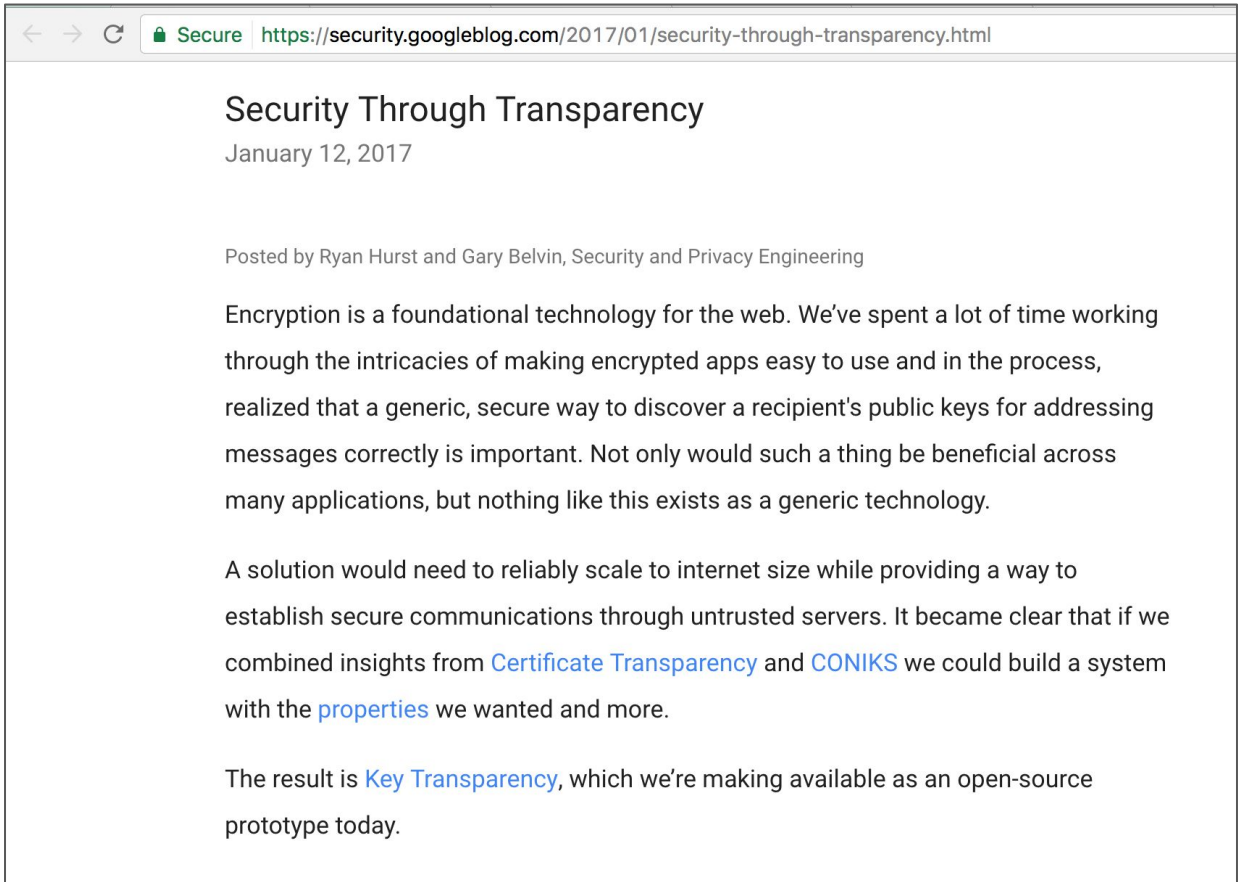
Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in Section 5.2.2.

Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

Verifiers SHOULD permit claimants to use "paste" functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets.

Frontiers

Building on the success of Certificate Transparency



README.md

Trillian: General Transparency

Secure https://play.google.com/store/apps/details?id=party.davidsherenowitsa.transparensbee

Apps

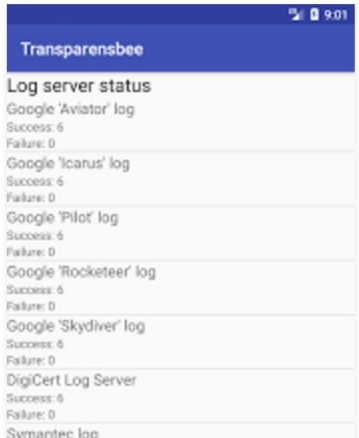
Categories | Home | Top Charts | New Releases

Transparensbee

David Cook **Tools**

Everyone

Installed



Third party services

```
<script src="//ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js"></script>

 <link href='https://fonts.googleapis.com/css?family=Lato:300,400,700'

  <script src="https://platform.twitter.com/widgets.js"></script>

       <script src="//use.typekit.net/wde1aof.js"></script>

href="https://cdn-static-1.medium.com/_/fp/css/main-base.17jbVAZmSSr6Xqu8XxlkdQ.css">


<!-- Google Analytics -->
<script>
  (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
  (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
  m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
  })(window,document,'script','https://www.google-analytics.com/analytics.js','ga');
  ga('create', 'UA-48605964-1', 'gsa.gov');
```

Eric Mill
@konklone

Ran my phantomas-based 3rd party scanner (github.com/18F/domain-sca…) on NYT homepage. Causes visitors' browsers to ping 73 distinct hostnames.


```
"offenders": {
  "domains": [
    "static01.nyt.com: 94 request(s)",
    "a1.nyt.com: 21 request(s)",
    "tpc.googlesyndication.com: 19 request(s)",
    "px.moatads.com: 15 request(s)",
    "typeface.nyt.com: 14 request(s)",
    "securepubads.g.doubleclick.net: 13 request(s)",
    "beacon.krxd.net: 10 request(s)",
    "www.facebook.com: 10 request(s)",
    "int.nyt.com: 8 request(s)",
    "www.nytimes.com: 6 request(s)",
    "web-player.art19.com: 6 request(s)",
    "et.nytimes.com: 6 request(s)",
    "cdn.krxd.net: 6 request(s)",
    "messaging-notifications.api.nytimes.com: 6 request(s)",
    "pagead2.googlesyndication.com: 5 request(s)"
```

JANUARY 20, 2015 | BY COOPER QUINTIN

HealthCare.gov Sends Personal Data to Dozens of Tracking Websites

The Associated Press reports that healthcare.gov–the flagship site of the Affordable Care Act, where millions of Americans have signed up to receive health care–is quietly sending personal health information to a number of third party websites. The information being sent includes one's zip code, income level, smoking status, pregnancy status and more.

An example of personal health data being sent to third parties from healthcare.gov

EFF researchers have independently confirmed that healthcare.gov is sending personal health information to at least 14 third party domains, even if the user has enabled Do Not Track. The information is sent via the referrer header, which contains the URL of the page requesting a third party resource. The referrer header is an essential part of the HTTP protocol, and is sent for every request that is made on the web. The referrer header lets the requested resource know what URL the request came from. This would for example let a website know who else was linking to their pages. In this case however the referrer URL contains personal health information.

Unlike HTTPS, no user-visible indicators at all

Your web host is also a third party

How do they handle data collected at their network edge?

The Security Impact of HTTPS Interception

Zakir Durumeric*∨, Zane Ma†, Drew Springall*, Richard Barnes‡, Nick Sullivan§,
Elie Bursztein¶, Michael Bailey†, J. Alex Halderman*, Vern Paxson‖∨

*University of Michigan †University of Illinois Urbana-Champaign ‡Mozilla §Cloudflare
¶Google ‖University of California Berkeley ∨International Computer Science Institute

***Abstract*—As HTTPS deployment grows, middlebox and antivirus products are increasingly intercepting TLS connections to retain visibility into network traffic. In this work, we present a comprehensive study on the prevalence and impact of HTTPS interception. First, we show that web servers can detect interception by identifying a mismatch between the HTTP User-Agent header and TLS client behavior. We characterize the TLS handshakes of major browsers and popular interception products, which we use to build a set of heuristics to detect interception and identify the responsible product. We deploy these heuristics at three large network providers: (1) Mozilla Firefox update servers, (2) a set of popular e-commerce sites, and (3) the Cloudflare content distribution network. We find more than an order of**

connection to the destination server. We show that web servers can detect such interception by identifying a *mismatch* between the HTTP User-Agent header and the behavior of the TLS client. TLS implementations display varied support (and preference order) for cipher suites, extensions, elliptic curves, compression methods, and signature algorithms. We characterize these variations for major browsers and popular interception products in order to construct heuristics for detecting interception and identifying the responsible product.

Next, we assess the prevalence and impact of HTTPS interception by applying our heuristics to nearly eight billion

Product	Grade	Validates Certificates	Modern Ciphers	Advertises RC4	TLS Version	Grading Notes
A10 vThunder SSL Insight	F	✓	✓	Yes	1.2	Advertises export ciphers
Blue Coat ProxySG 6642	A*	✓	✓	No	1.2	Mirrors client ciphers
Barracuda 610Vx Web Filter	C	✓	✗	Yes	1.0	Vulnerable to Logjam attack
Checkpoint Threat Prevention	F	✓	✗	Yes	1.0	Allows expired certificates
Cisco IronPort Web Security	F	✓	✓	Yes	1.2	Advertises export ciphers
Forcepoint TRITON AP-WEB Cloud	C	✓	✓	No	1.2	Accepts RC4 ciphers
Fortinet FortiGate 5.4.0	C	✓	✓	No	1.2	Vulnerable to Logjam attack
Juniper SRX Forward SSL Proxy	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
Microsoft Threat Mgmt. Gateway	F	✗	✗	Yes	SSLv2	No certificate validation
Sophos SSL Inspection	C	✓	✓	Yes	1.2	Advertises RC4 ciphers
Untangle NG Firewall	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
WebTitan Gateway	F	✗	✓	Yes	1.2	Broken certificate validation

Fig. 3: **Security of TLS Interception Middleboxes**—We evaluate popular network middleboxes that act as TLS interception proxies. We find that nearly all reduce connection security and five introduce severe vulnerabilities. *Mirrors browser ciphers.

Product	OS	Browser MITM				Grade	Validates Certificates	Modern Ciphers	TLS Version	Grading Notes
		IE	Chrome	Firefox	Safari					
Avast ...										
AV 11	Win	●	○	○		A*	✓	✓	1.2	Mirrors client ciphers
AV 11.7	Mac		●	●	●	F	✓	✓	1.2	Advertises DES
AVG ...										
Internet Security 2015–6	Win	●	●	○		C	✓	✓	1.2	Advertises RC4
Bitdefender ...										
Internet Security 2016	Win	●	●	●		C	✓	○	1.2	RC4, 768-bit D-H
Total Security Plus 2016	Win	●	●	●		C	✓	○	1.2	RC4, 768-bit D-H
AV Plus 2015–16	Win	●	●	●		C	✓	○	1.2	RC4, 768-bit D-H
Bullguard ...										
Internet Security 16	Win	●	●	●		A*	✓	✓	1.2	Mirrors client ciphers
Internet Security 15	Win	●	●	●		F	✓	✗	1.0	Advertises DES
CYBERsitter ...										
CYBERsitter 11	Win	●	●	●		F	✗	✗	1.2	No cert. validation, DES
Dr. Web ...										
Security Space 11	Win	●	●	●		C	✓	○	1.2	RC4, FREAK
Dr. Web 11 for OS X	Mac		●	●	●	F	✓	✗	1.0	Export ciphers, DES, RC2
ESET ...										

Alert (TA17-075A)

HTTPS Interception Weakens TLS Security

More Alerts

Original release date: March 16, 2017

Systems Affected

All systems behind a hypertext transfer protocol secure (HTTPS) interception product are potentially affected.

Overview

Many organizations use HTTPS interception products for several purposes, including detecting malware that uses HTTPS connections to malicious servers. The CERT Coordination Center (CERT/CC) explored the tradeoffs of using HTTPS interception in a blog post called The Risks of SSL Inspection [1].

Organizations that have performed a risk assessment and determined that HTTPS inspection is a requirement should ensure their HTTPS inspection products are performing correct transport layer security (TLS) certificate validation. Products that do not properly ensure secure TLS communications and do not convey error messages to the user may further weaken the end-to-end protections that HTTPS aims to provide.

Network Security Devices Utilizing Vulnerable Weak Signature Algorithms in TLS

To access: Get File

Abstract:

Network security devices, such as wireless access points, TLS proxies, security management systems, and web servers, use digital signatures so systems can discern that the devices are authentic, network traffic has been processed by the device, and traffic has not been modified in transit between the device and the system (via a man-in-the-mid-

Have Questions?

Frequently Asked Questions

Site Index

E-mail: IA Client Assistance

Yet we're still getting headlines like this

TECH INSIDER

AN EXPERT BLOG ON THE STATE OF FEDERAL TECHNOLOGY

WHY ALL FEDERAL AGENCIES SHOULD BREAK AND INSPECT SECURE TRAFFIC

Follow on Twitter
Subscribe

ARCHIVES

By Contributor
By Date

By Andrew Hickey
July 5, 2017 1 Comment

RECENT POSTS

House of Clouds: The Federal Transition to

Transparency

Take the time and energy to explain things

Publish all the data and code you possibly can

Establish open processes

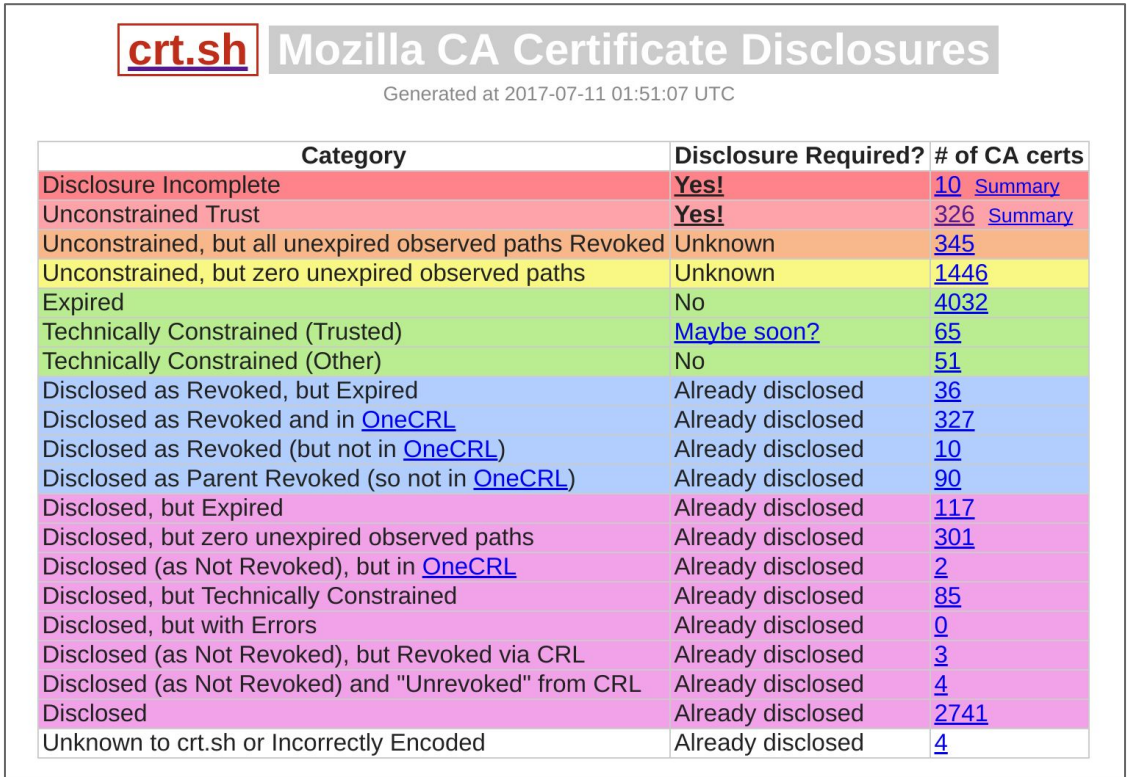
(it doesn’t have to be complicated)

Default to open

Open the door to providence.

Security and privacy through transparency

Eric Mill, eric.mill@gsa.gov



crt.sh Mozilla CA Certificate Disclosures

Generated at 2017-07-11 01:51:07 UTC

Category	Disclosure Required?	# of CA certs
Disclosure Incomplete	**Yes!**	10 Summary
Unconstrained Trust	**Yes!**	326 Summary
Unconstrained, but all unexpired observed paths Revoked	Unknown	345
Unconstrained, but zero unexpired observed paths	Unknown	1446
Expired	No	4032
Technically Constrained (Trusted)	Maybe soon?	65
Technically Constrained (Other)	No	51
Disclosed as Revoked, but Expired	Already disclosed	36
Disclosed as Revoked and in OneCRL	Already disclosed	327
Disclosed as Revoked (but not in OneCRL)	Already disclosed	10
Disclosed as Parent Revoked (so not in OneCRL)	Already disclosed	90
Disclosed, but Expired	Already disclosed	117
Disclosed, but zero unexpired observed paths	Already disclosed	301
Disclosed (as Not Revoked), but in OneCRL	Already disclosed	2
Disclosed, but Technically Constrained	Already disclosed	85
Disclosed, but with Errors	Already disclosed	0
Disclosed (as Not Revoked), but Revoked via CRL	Already disclosed	3
Disclosed (as Not Revoked) and "Unrevoked" from CRL	Already disclosed	4
Disclosed	Already disclosed	2741
Unknown to crt.sh or Incorrectly Encoded	Already disclosed	4