Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff’s Exhibit 36

SHARE

OPERATIONS, TECHNOLOGY

The future of HTTPS on Wikimedia projects

By Ryan Lane

August 1st, 2013

The Wikimedia Foundation believes strongly in protecting the privacy of its readers and editors. Recent leaks of the NSA's XKeyscore program have prompted our community members to push for the use of HTTPS by default for the Wikimedia projects. Thankfully, this is already a project that was being considered for this year's official roadmap and it has been on our unofficial roadmap since native HTTPS was enabled. Our current architecture cannot handle HTTPS by default, but we've been incrementally making changes to make it possible. Since we appear to be specifically targeted by XKeyscore, we'll be speeding up these efforts.

THIS ARTICLE IS AVAILABLE IN:

ENGLISH 中文

The Wikimedia Foundation believes strongly in protecting the privacy of its readers and editors. Recent leaks of the NSA's XKeyscore program have prompted our community members to push for the use of HTTPS by default for the Wikimedia projects. Thankfully, this is already a project that was being considered for this year's official roadmap and it has been on our unofficial roadmap since native HTTPS was enabled.

Our current architecture cannot handle HTTPS by default, but we've been incrementally making changes to make it possible. Since we appear to be specifically targeted by XKeyscore, we'll be speeding up these efforts. Here's our current internal roadmap:

1. Redirect to HTTPS for log-in, and keep logged-in users on HTTPS. ~~This change is scheduled to be deployed on August 21, at 16:00 UTC.~~ **Update as of 21 August**: we have delayed this change and will now deploy it on Wednesday, August 28 at 20:00 UTC/1pm PT.
2. Expand the HTTPS infrastructure: Move the SSL terminators directly onto the frontend varnish caches, and expand the frontend caching clusters as necessitated by increased load.
3. Put in engineering effort to more properly distribute our SSL load across the frontend caches. In our current architecture, we're using a source hashing based load balancer to allow for SSL session resumption. We'll switch to an SSL terminator that supports a distributed SSL cache, or we'll add one to our current solution. Doing so will allow us to switch to a weighted round-robin load balancer and will result in a more efficient SSL cache.
4. Starting with smaller projects, slowly soft-enable HTTPS for anonymous users by default, gradually moving toward soft-enabling it on the larger projects as well. By soft-enable we mean changing our rel=canonical links in the head section of our pages to point to the HTTPS version of pages, rather than the HTTP versions. This will cause search engines to return HTTPS results, rather than HTTP results.

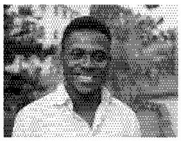
GET CONNECTED

GET OUR EMAIL UPDATES

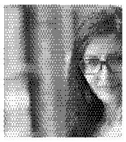
Your email address

Subscribe

MEET OUR COMMUNITY



The one-man band writing the history of Nigerian cinema into Wikipedia



Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics tea

ARCHIVES

FEBRUARY 2018

JANUARY 2018

5. Consider enabling perfect forward secrecy. Enabling perfect forward secrecy is only useful if we also eliminate the threat of traffic analysis of HTTPS, which can be used to detect a user's browsing activity, even when using HTTPS.
6. Consider doing a hard-enable of HTTPS. By hard-enable we mean force redirecting users from HTTP pages to the HTTPS versions of those pages. A number of countries, China being the largest example, completely block HTTPS to Wikimedia projects, so doing a hard-enable of HTTPS would probably block large numbers of users from accessing our projects at all. Because of this, we feel this action would probably do more harm than good, but we'll continue to evaluate our options here.
7. Consider enabling HTTP Strict Transport Security (HSTS) to protect against SSL-stripping man-in-the-middle attacks. Implementing HSTS could also lead to our projects being inaccessible for large numbers of users as it forces a browser to use HTTPS. If a country blocks HTTPS, then every user in the country that received an HSTS header would effectively be blocked from the projects.

Currently we don't have time frames associated with any change other than redirecting logged-in users to HTTPS, but we will be making time frames internally and will update this post at that point.

Until HTTPS is enabled by default, we urge privacy-conscious users to use HTTPS Everywhere or Tor [1].

Ryan Lane
Operations Engineer, Wikimedia Foundation

[1]: There are restrictions with Tor; see Wikipedia's information on this.

50 Comments on The future of HTTPS on Wikimedia projects

zzo38 3 years

Can you ***PLEASE*** add another domain name that disables HTTPS? I want to opt-out of HTTPS and I can no longer do so.

Share

peter 3 years

Are you kidding Wikimedia?

"Consider doing a hard-enable of HTTPS. By hard-enable we mean force redirecting users from HTTP pages to the HTTPS versions of those pages. A number of countries, China being the largest example, completely block HTTPS to Wikimedia projects, so doing a hard-enable of HTTPS would probably block large numbers of users from accessing our projects at all. Because of this, we feel this action would probably do more harm than good, but we'll continue to evaluate our options here."

Because Chinese government is raping the Internet in China you do not enable HTTPS as hard-enable? Are you getting payed from Chinese government? Are you technicians that stupid? What is the reason to not hard-enable it? Because other people are doing bad things you do not the good? WTF?

Share

John Gilmore 4 years

Isn't it interesting how the Chinese government and NSA BOTH spy on users of Wikipedia?

I think Chinese users of Wikipedia should blame their government — not Wikipedia — for any problems that result from Wikipedia moving to encrypt more and more of their service. Wikipedia is solving a problem. The Chinese government is creating one.

DECEMBER 2017

NOVEMBER 2017

OCTOBER 2017

OLDER POSTS 26

WORK AT WIKIMEDIA

Work with the foundation that supports W
and its sister projects around the world. A
and join us

It's too much to expect that the entire world should use Wikipedia in plaintext, letting any government or criminal spy on all the users, because a few governments infringe their citizens' right to use encryption. US citizens actively fought the US government's ban on encryption — and won, after a decade of work. Chinese citizens, it's your turn to fix your own government now. The rest of the world can't do it for you.

Share

KoshVorlon 4 years

* FOR ALL THOSE THAT WANT TO FLAME THE DEVS OVER THIS *

Yes – this change breaks Mozilla – it's already known.
I.E and Chrome still handles the change over fine.

You may need to switch over if your a firefox user (as I am).

Flaming the devs won't get this fixed faster.

Share

Ryan Lane 4 years

We have plans on testing SPDY after anonymous users are switched to HTTPS.

Share

Leirn 4 years

Will SPDY be next ?

Share

Ryan Lane 4 years

There wasn't any claim that adding HTTPS would completely alleviate our woes in this regard. This is only a first step towards the goal.

Share

Seb35 4 years

I want just to point that the History of cryptography should teach us to never over-expect the attacker don't have advanced techniques to cryptanalyse or decipher our message with some means (see the period where the cipher was the secret, or Enigma, Purple, recent attacks on TLS; even one-time pads can be broken if the key is not truly random). In this sense I find we should not claim "our infrastructure is secure and TLS is not a false sense of security" but "to the best of our knowledge, access to Wikimedia projects through TLS is secure regarding most of the currently known attacks".

Share

wiiliam gomes 5 years

éu gosto de asistir é irado

Share

Nicolas B. 5 years

Ryan,

Alas, Wikipedia blocks contributions from many proxies, and from TOR.

Ranyv,

Chinese people ≠ people in China.

Share

Int21h 5 years

Leave the Zhongwen Wikipedia behind. Let them keep their HTTP.

Advance the rest of the world into the 20th Century.

Share

300aq300aq 5 years

坚决支持！！！！！！！！！！

Share

qa003qa003 5 years

坚决反对！！！！！！！！！！

Share

Ryan Lane 5 years

So, HTTPS forces them to do traffic analysis, which makes their lives quite a bit harder. So, it's not a false sense of security, but isn't by itself a complete solution. As mentioned, newer protocols will likely help this situation, but we'll also be putting effort into making traffic analysis more difficult for our traffic. Our first priority, of course, is moving people to HTTPS.

Share

Ciara Hoyle 5 years

So much for clarity! That should read the above comment #10

Share

Ciara Hoyle 5 years

For clarity – the above comment #9, is a follow-on from my previous comment #2 on page 2

Share

Ciara Hoyle 5 years

Very interesting. Seeing as we are talking about eavesdropping by those with the resources a nation state (NSA et al.) doesn't the finger printing by traffic analysis issue also compromise the perceived privacy provided by 'vanilla' HTTPS? If so, are the measures described in the blog really just giving ourselves a false sense of privacy (regarding NSA level eavesdropping)?

Share

Walter Grassroot@zhwiki 5 years

As a 5-year Wikipedia editor, I appreciate for WMF's efforts on every promotion, including security protection. However, this attempt of moving to HTTPS on Wikimedia projects will completely destroy the Chinese community to reach all the Wikimedia programs, not only Zh-wikipedia. Since 2008, our Chinese Wikipedia has suffered governmental blocks for different reasons. Although we could access the HTTPS early 2013, the government still blocked this method to reach Wikipedia immediately, when we recommended this in public. Many Wikipedia-unfriendly governments would learn and act same as the Chinese Government on internet control – which means, if WMF act HTTPS on whole Wikimedia projects, more editors will suffered the block reflection in the world. In general, this action would setup all the Wikipedians in the opposite side of the governments. Thank you.

Share

Jsjsjs1111 5 years

Even if this "feature" is brought into practice, I would still strongly recommend you not to enable it on Chinese Wikipedia (zh), as for the reason that Quark stated. You are free to enable it elsewhere.

Share

Ryan Lane 5 years

Matt: China blocks Wikimedia projects on HTTPS currently, yes.

Share

MORE COMMENTS

Comments are closed.

WIKIMEDIA FOUNDATION

The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. Get Involved | Log In

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

WIKIPEDIA COMMONS MEDIAWIKI WIKIBOOKS
WIKIDATA WIKINEWS WIKIQUOTE WIKISOURCE
WIKISPECIES WIKIVERSITY WIKIVOYAGE WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement ha already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

WIKIMEDIA CHAPTERS THEMATIC ORGANIZATIONS WIKIMEDIA USER GROUPS