Google Registry

Broadening HSTS to secure more of the Web

Ben McIlwain, software engineer at Google
mcilwain@google.com

9C3D F6D2 3A28 F680 4ECA 927A BC21 184E FFA6 0567

Google Registry

Why HTTPS is important

- Protects users on open/public access points from man-in-the-middle attacks
- Prevents ads and analytics injection/hijacking, spying, and tracking by ISPs/DNS providers or other intermediaries
- Helps protect against surreptitious censorship and alteration of content
- Promotes trust, security, and privacy on the Internet

“Saying that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about freedom of speech because you have nothing to say.” -- Jean Michel Jarre

Google Registry

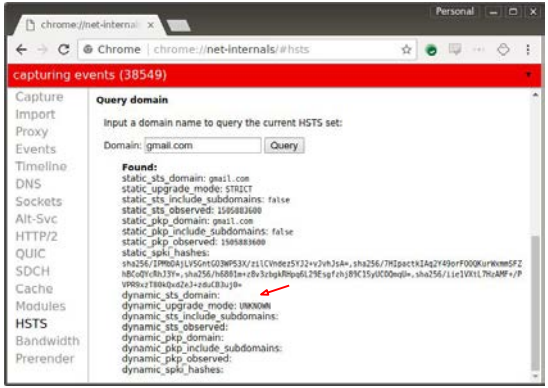
But HTTPS alone isn’t enough ...

… because anyone who intercepts a connection can simply strip SSL.

Google Registry

What is HTTP Strict Transport Security (HSTS)?

- An HTTPS response header configured in web servers
- Specifies that web browsers should *only* load that website using HTTPS
- The browser will rewrite http://foo.bar URLs to https://foo.bar before sending any request
- Long expiration times; typically at least a year
- Can be applied at the domain, or subdomain, or sub-subdomain level, etc.



Google Registry

Why HSTS is important

It protects against:

- SSL stripping attacks
- Mixed content leaking session data despite main URL being https
- DNS-based spoofing attacks to redirect requests to insecure destinations
- Modifications to directly typed URLs that hit http-to-https redirect pages

And yet even HSTS headers aren’t enough ...

… because the *first* request can be intercepted, and headers and SSL stripped.

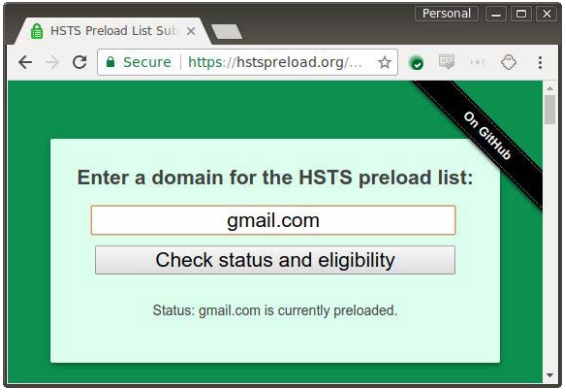
- Witness the recent KRACK attack on WPA2.

So what is the solution?

Google Registry

HSTS preloading

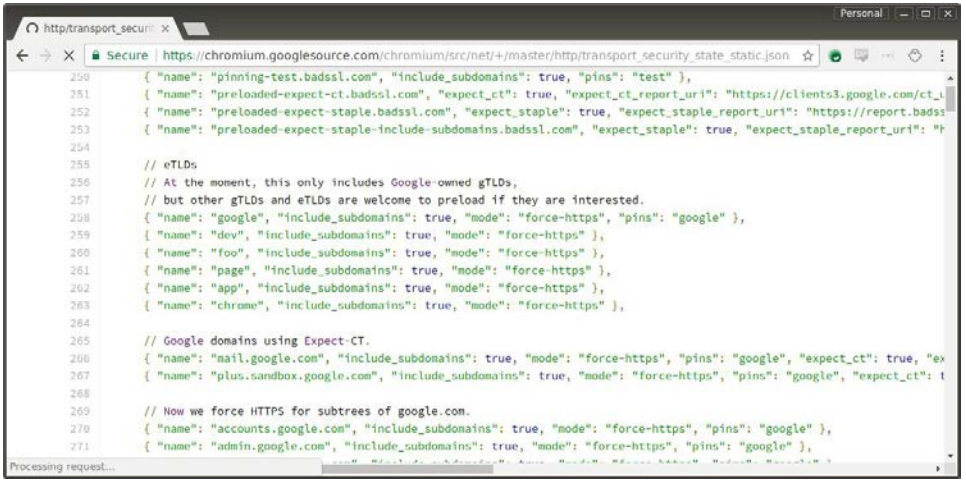
- A list of domain names built into browsers of HSTS-required domain names
- Protects against even the *first* request to a domain being intercepted, before HSTS headers were received
- Included in all major web browsers (Chrome, Firefox, IE/Edge, Safari, Opera)
- Gives the highest possible level of security
- Check website status at: https://hstspreload.org



Google Registry

Using HSTS preload for entire TLDs

- It is possible to include domain names at the *first* level (i.e. TLDs) on the HSTS preload list, and thus make the entire TLD secure
- So, we did:



Google Registry

Benefits of preloading entire TLDs

- Users will associate the entire TLD with being secure
- Eliminates lag time to add new domain names to HSTS preload list
- Configuring HSTS headers on a per-site basis becomes much less important
- More lightweight for browsers (especially relevant for mobile)
- Moves the Internet closer to a secure-by-default, HTTPS everywhere future
- Requires no changes whatsoever in the registry

Google Registry

Potential pitfalls in preloading entire TLDs

- Existing websites on the TLD that do not use HTTPS *will cease to work*
- Requires all webmasters to get and install SSL certificates
  - Fortunately, Let's Encrypt makes this simple and free
  - *And you should already be using HTTPS anyway*
- Can break users who were using fake local domain names on the TLD
  - But using domain names you don't actually own is already broken anyway. Don't do it.
  - Also see RFC 2606 for safe alternatives: .test, .example, .invalid, .localhost
- Registrars will likely need special language for HTTPS-only TLDs
  - But it's a security benefit that should make the TLDs stand out and be more attractive
- Some types of sites cannot use HTTPS at all, like generate_204 (captive portal checking)

Google Registry

Our recommendations

- If you are launching a new TLD, add it to the HSTS preload list first
  - We can help with this
- Add your existing domains to the HSTS preload list (nothing new here)
- If you run existing TLDs with many non-secure sites … wait. There may be more accommodating options in the future, e.g. carve-outs.
- If you run multi-part ccTLDs, consider adding some of them to the list
  - E.g. if all government sites in your country are already secure, then add gov.xy
- Consider a potential future EPP extension to say whether a TLD is secure

And stay tuned for future announcements about availability of some of our HSTS-enabled TLDs.

Google Registry

Q&A

See https://hstspreload.org/ for more info