CENTER FOR DEMOCRACY & TECHNOLOGY

Issue Brief: The Time Has Come to Move to HTTPS!

October 6, 2016

All Web Users Deserve Confidentiality and Integrity:

All interactions on the web benefit from protection. People online increasingly face serious risks, from financial fraud and spying and surveillance to malware in downloads and advertisements. On the web, protection is achieved by HTTPS, and now is the time to move your websites from (insecure) HTTP to (secure) HTTPS. It's easier than you may think, and getting easier every day.

Privacy & Security Concerns:

- **Without HTTPS, ISPs and governments can spy on what your users are doing:** Traffic on the web traverses many different networks from server to browser, and each of these networks (or equipment installed on these networks) can see the full contents of unencrypted (HTTP) traffic. This means ISPs can do things like monitor your web traffic to build advertising profiles.[1] This also means that the government can monitor unencrypted traffic at chokepoints such as undersea cable landing sites.[2] This is especially problematic since the U.S. government treats traffic encountered outside the United States as foreign – free from the restrictions imposed by the U.S. constitution – and subject to interception. However, traffic travelling from one computer in the United States to another computer in the United States can easily cross international borders, and when it does, it can be intercepted.
- **Using HTTPS makes hacked routers powerless:** Malicious hackers can gain unauthorized access to network equipment – hacked routers, for example – in order to do the same things we mention above. Malicious actors may even "inject" malware into an unencrypted stream of data as China did recently with their "Great Cannon"[3] tool. The Great Cannon was able to inject malicious JavaScript into unencrypted web pages to perform distributed denial of service (DDoS) attacks against targets such as Github.[4] Chinese ISPs have been found injecting other malware and advertisements as well.[5]

Business Risks of not using HTTPS:

- **Without HTTPS, ISPs can strip out your ads/referrals and add their own:** Your site may use advertising or other digital marketing features or depend on accurate analytics about visitors and customers. If your site is using (unencrypted) HTTP, ISPs or other network operators can remove your own advertisements, analytics, and marketing code and add their own. For example, NebuAd[6] partnered with ISPs to snoop on their customer traffic and deliver targeted advertisements.
- **Without HTTPS your website cannot have the fastest performance:** HTTPS is required for the best performance the web offers. HTTP/2,[7] the latest revision to the HTTP protocol, yields massive performance enhancements (faster page loads and less data to transmit). Major browser makers such as Firefox and Chrome only support

[1] http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html
[2] https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[3] https://citizenlab.org/2015/04/chinas-great-cannon/
[4] http://arstechnica.com/security/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/
[5] https://thehackernews.com/2016/02/china-hacker-malware.html
[6] http://arstechnica.com/tech-policy/2008/11/nebuad-isps-sued-over-dpi-snooping-ad-targeting-program/
[7] https://tools.ietf.org/html/rfc7540

HTTP/2 over HTTPS. You'll be missing out on these performance gains if you stay on plain HTTP. Google also gives a (small) search ranking boost[8] to HTTPS sites. And major browser makers such as Chrome[9] and Firefox[10] will soon begin to mark unencrypted HTTP as insecure.

- **Without HTTPS, you can't use the latest cool web features:** The web is gaining some neat new tools and features that will only be available to secure (HTTPS) websites, and HTTP sites simply will not have access to those features. Some of the most innovative things you can do with your website, for example HD video chat (WebRTC) or using geolocation in the browser, require that your site use HTTPS to function.
- **You already need HTTPS to do payments anyway:** If you accept payments, tips, donations, or provide subscription access to content or services, the Payment Card Industry Data Security Standards (PCI DSS)[11] specify that you must encrypt data in transit and require HTTPS for e-commerce transactions. Websites should treat all of their customers' browsing as private – not just their financial data. By enabling HTTPS for your entire website, operators can show that they view privacy as more than mere compliance, but an important part of good customer service.
- **Without HTTPS, you can't enforce your terms of service and privacy policy:** Through your terms of service and privacy policy, you inform your users about legal issues related to your website, and you make commitments to your users, for example, to protect their personal and financial information. If your site is HTTP and not HTTPS, you can't actually know if the information you send to them (or that they send to you) is what you intended to send; because it is unprotected and not HTTPS, that information could be modified and information exchanged over HTTP should be considered unprotected. Without HTTPS, you can't be sure you're keeping the promises you make your users about what your site does and what third parties you share your users' information with.

Previous CDT work on this topic: *"No Half Measures: Digital Marketing Properties Must Adopt Encryption Best Practices"* https://cdt.org/?p=75853.

For more information, please contact:

- CDT Chief Technologist Joseph Lorenzo Hall (joe@cdt.org)
- CDT Communications (comms@cdt.org)

[8] https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.htm
[9] https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure
[10] https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/
[11] https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf