Wendy Seltzer, W3C, wseltzer@w3.org, August 7, 2015
Submission to Managing Radio Networks in an Encrypted World (MaRNEW) Workshop

Security, Privacy, and Performance Considerations for the Mobile Web

The Web is an important application on mobile networks. W3C's Technical Architecture Group has expressed strong guidance that Web traffic should be encrypted end-to-end, to assure its authentication, integrity and confidentiality. [Securing the Web], [EndToEnd] These assurances are, if anything, more necessary on the mobile Web, because users frequently entrust their mobile browsers and devices with highly sensitive information, including contacts, location, and daily activity. In a global study last year, 64% of Internet users worldwide said their concerns about online privacy had increased in the last year. [CIGI-IPSOS] 67% of mobile Internet users surveyed "would like to do more" to protect the privacy of their personal information online, compared to 52% of non-mobile Internet users. [Pew2014]

Work items at W3C target several points at the intersection of security, privacy, and performance.

Security

Pursuant to the TAG recommendation, the Web Application Security Working Group is working on several specifications to help Web application developers HTTPS-enable their Web Apps, including the Upgrade Insecure Requests and Mixed Content drafts. These, along with work such as HSTS and HPKP, help to ease the HTTPS transition for server operators, and as the proportion of HTTPS traffic grows, set user expectations that Web traffic should be secure and authenticated.

The Privileged Contexts draft recommends that powerful features of the Web platform, including application code with access to sensitive or private data, be delivered only in secure contexts, over authenticated and confidential channels that guarantee data integrity. As the draft indicates, "delivering code securely cannot ensure that an application will always meet a user's security and privacy requirements, but it is a necessary precondition."

Privacy

Web users seeking privacy should not have to identify themselves as such. Privacy, like anonymity, loves company.[DingledineMathewson] The more people using a given technology, especially if it has non-privacy-specific purposes, the less its users stand out as "privacy seekers." The use of privacy-specific technologies was used as a selector in the NSA's XKeyscore system.[XKeyscore], [XKeyscore2] It is counterproductive if individuals trying to preserve privacy, whether web browsers from advertisers or dissidents from repressive political regimes, stand out from the crowd by virtue of the tools they use.

Because we cannot predict what information users deem sensitive, or when data not in itself sensitive may be used to link user activity in a way that impairs privacy, the TAG has called for tracking mechanisms to follow well-defined standards, promoting visibility, transparency, and user consent. [UnsanctionedTracking]. Many aspects of a user's Web behavior can be used to "fingerprint" or uniquely identify the uesr, including features of the browser and patterns of browsing activity. [FingerprintingGuidance] If network intermediaries add metadata to Web traffic, even for user-helpful purposes, that can increase users' fingerprinting surface area and vulnerability to data-collection and tracking by other observers. We should not without warning break users' expectations of privacy.

Performance

In order to earn and retain user trust, mobile networks must not interfere with encryption, and should promote its use. While encryption blocks intermediaries from inspecting or modifying Web traffic, it need not prevent cooperative measures to improve performance and availability. Indeed, because cryptography can supply integrity-verification for resources included from multiple sources, including those at network edges and local caches, it can support improved network performance for Web applications and content.

For example, the Subresource Integrity (SRI) draft specification enables Web authors to provide integrity metadata for subresources they include, enabling client-side verification of the specified components that does not require trusting the source from which those subresources were retrieved. This specification may be extended to permit reuse of resources from local caches, or leveraged to support network caching.

Toward a trustworthy, high-performance Web

With joint work from Web security, privacy, and network performance communities, we can lay the foundation for a mobile Web platform that is both high-performance and worthy of users' trust.

References

[EndToEnd]
Yan Zhu. End-to-End Encryption and the Web. W3C TAG Finding., July 2015. URL: http://www.w3.org/2001/tag/doc/encryption-finding/

[SecuringTheWeb]
Mark Nottingham. Securing the Web. W3C TAG Finding, January 2015. URL: https://www.w3.org/2001/tag/doc/web-https

[Pew2014]
Mary Madden. Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Research, November 12, 2014. URL: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

[CIGI-IPSOS]
CIGI-Ipsos Global Survey on Internet Security and Trust, November, 2014. URL: https://www.cigionline.org/internet-survey#online-privacy

[DingledineMathewson]
Dingledine, R. and Mathewson, N. Anonymity Loves Company: Usability and the Network Effect"URL: http://freehaven.net/anonbib/cache/usability:weis2006.pdf

[XKeyscore]
Glenn Greenwald. XKeyscore: NSA tool collects 'nearly everything a user does on the internet, The Guardian, 31 July 2013. URL: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[XKeyscore2]
Bruce Schneier. NSA Targets the Privacy-Conscious for Surveillance" URL: https://www.schneier.com/blog/archives/2014/07/nsa_targets_pri.html

[UnsanctionedTracking]
Mark Nottingham. Unsanctioned Web Tracking. W3C TAG Finding., July 2015. URL: http://www.w3.org/2001/tag/doc/unsanctioned-tracking/

[FingerprintingGuidance]
Nick Doty Fingerprinting Guidance for Web Specification Authors Draft, February 2015. URL: http://w3c.github.io/fingerprinting-guidance/