Security, Privacy, and Performance Considerations for the Mobile Web

Wendy Seltzer
Technology & Society Domain
World Wide Web Consortium (W3C/MIT)
weltzer@w3.org
Priority of Constituencies

HTML design principles:

- In case of conflict, consider users over authors over implementors over specifiers over theoretical purity. In other words costs or difficulties to the user should be given more weight than costs to authors; which in turn should be given more weight than costs to implementors; which should be given more weight than costs to authors of the spec itself, which should be given more weight than those proposing changes for theoretical reasons alone. Of course, it is preferred to make things better for multiple constituencies at once.
User Privacy & Security Concerns

• 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]
W3C TAG Findings

- Securing the Web
  - Securing the Web. W3C TAG Finding, January 2015
  - https://www.w3.org/2001/tag/doc/web-https
- End-to-end encryption on the Web
  - https://www.w3.org/2001/tag/doc/encryption-finding/
- Unsanctioned Tracking
  - https://www.w3.org/2001/tag/doc/unsanctioned-tracking/
Web Security Updates (WebAppSec)

• Secure Contexts:
  - Powerful features should be exposed only in secure contexts (HTTPS all the way down)
    • access to sensitive or private data
    • sensors: geolocation, camera, microphone
    • user tracking: persistent state; IDs and hardware
    • UI manipulation

• Upgrade Insecure Requests

• Mixed Content blocking

• Sub-Resource Integrity

• elsewhere: HSTS, HPKP, Let's Encrypt
Emerging Privacy Model of the Web

- User expectations emerge from experience, contextual norms, feedback from privacy breach “events”
  - Clearable identifiers
  - Origin-scoped contexts, isolation
- Dual-use privacy protections
  - Anonymity and privacy love company: it's best if privacy seekers can use platform-standard features
  - When changing feature behavior, be aware that some users may derive privacy from old functions
- Fingerprinting: at the heart of the tussle
- Transparency+
Cooperative Performance

- Web Performance
- Sub-Resource Integrity + Caching
- Informed user choice
• draft-nottingham-transport-metadata-impact