Web Security

LEONARD ROSENTHOL
ADOBE SYSTEMS

In a single word…

TRUST

Trust: Knowing where things come from

- On the Web, it’s therefore all about the domain or “Origin” for content
  - Content from “w3c.org” is treated differently from “badsite.net”
  - https://www.w3.org/Security/wiki/Same_Origin_Policy
- **Everything** is tied to the origin
  - Permissions granted by the site (eg. Cross origin access & security policies)
  - Permissions granted by the browser/UserAgent (eg. White & black list)
  - Permissions granted by the user (eg. microphone & camera access)
  - Cookies
  - Local Storage
- But origins are tied to domains and organizations – not individuals
  - So how do we handle ad-hoc distribution models?

Trust: Protecting against attacks

[From EPUB 3.1, 5.4 - http://www.idpf.org/epub/31/spec/epub-contentdocs.html]

- **against the runtime environment** (e.g., stealing files from a user's hard drive);
- **against the Reading System itself** (e.g., stealing a list of a user's books or causing unexpected behavior);
- **against the local network** (e.g., stealing data from a server behind a firewall).
- **one Content Document against another** (e.g., stealing data that originated in a different document);
- **an unencrypted script against an encrypted portion of a document** (e.g., an injected malicious script extracting protected content);

- And I'll add one more
- **against the user** (e.g. a phishing attack or rogue advertisements)

Trust: Don’t surprise the user

- “Do what you say, say what you do, and don’t surprise the user”

- Do users have the same expectations of a publication as they do a web site?
  - Is it OK to access the network? At all or only for some things (eg. fonts & streaming media)?
  - Is it OK to send analytics data?
  - Is it OK to store “cookies” (or other local things) on the user’s computer?

Questions