Web Privacy Topics

Andy Zeigler

Senior Program Manager, Internet Explorer

Microsoft

Overview

- Web Standards and Privacy
  - CSS 2.1
  - Geolocation
- User Tracking
  - Previous Approaches
    - P3P
  - Tracking Protection, “Do Not Track”

WEB STANDARDS AND PRIVACY

CSS

- CSS (Cascading Style Sheets)
  - Core Web technology used for visually styling HTML markup
  - Develops use CSS to select HTML elements and apply a variety of styles (fonts, colors, sizes, etc.)
  - 1998: CSS 2.0 (W3C Recommendation)
    - Defines :visited selector

:visited

- Selects elements in a page that have previously been visited by a user:
  - `:visited { color: red }`
    - Changes all visited links to red
  - `:visited { font-size: 200%}`
    - Changes the font size of visited links to be 200% of what they normally would be
    - Causes changes in layout of the page
  - `getComputedStyle()`
    - Returns the actual style of any element in a page

:visited -- Attack

1) Create a bunch of links in a page (like – 10000)
2) Style them with :visited
3) Detect that they have been visited either by detecting changes in layout, or by calling getComputedStyle()
4) Combine with XHR to send back to server

CSS 2.0

If the following link:

```
<A class="external" href="http://out.side/">external link</A>
```

has been visited, this rule:

```
A.external:visited { color: blue }
```

will cause it to be blue.

CSS 2.1

If the following link:

```
<A class="external" href="http://out.side/">external link</A>
```

has been visited, this rule:

```
A.external:visited { color: blue }
```

will cause it to be blue.

- Note. It is possible for style sheet authors to abuse the :link and :visited pseudo-classes to determine which sites a user has visited without the user's consent.
- UAs may therefore treat all links as unvisited links, or implement other measures to preserve the user's privacy while rendering visited and unvisited links differently. See [P3P] for more information about handling privacy.

Geolocation

- Allows a website to obtain the physical location of the user
- Javascript API, supports
  - Latitude
  - Longitude
  - Accuracy
  - Elevation
  - …

Table of Contents

Geolocation Privacy Considerations

- Considerations for browser vendors
  - "User agents must not send location information to Web sites without the express permission of the user. User agents must acquire permission through a user interface, unless they have prearranged trust relationships with users…"
- Considerations for Websites
  - "Recipients must only request location information when necessary. Recipients must only use the location information for the task for which it was provided to them. Recipients must dispose of location information once that task is completed…"
- Many other great examples in the spec

Takeaways

- Take privacy into consideration when authoring specifications
- Privacy risks exist in most technologies – even ones that might appear to have little risk
- Privacy issues can be very difficult to fix after a spec is implemented – privacy risk, compatibility, interoperability, etc. all must be balanced