CSS History Hack History

Sai saizai.com
github.com/saizai/cssfingerprint

tl;dr:

:visited / :link CSS
+ JS getComputedStyle
+ AJAX, SVM, Bayes, etc.
= robust behavioral fingerprinting

History

2002: Mozilla bug #147777 filed by David Baron

2006: Jeremiah Grossman publishes hack

Early 2010: CSS Fingerprint, iSecLab's deanon

Late 2010: Fixed. Finally.

Possible solutions

1. Ignore it — how bad could it be?

2. Per-site visitation history

   breaks UX — link shows visited on one page, not on another

3. Total lockdown on :visited CSS + lying to JS

   only color allowed — no images, alpha, font, etc

   need DOM to lie to JS

Extraction

- Simple (JS, browser local)
  - Create element, check color
- Simple (image)
  - Background-image to hit counter
- Super fast (up to ~3.4M URL/min)
  - Visited is inline, unvisited is display:none
  - Per browser
    - Chrome: Reuse same <a>, swap URL, test
    - Firefox: Insert batch, test individually
    - Explorer, Safari: Insert batch, run jQuery :visible

Analysis

1. Naïve Bayes + Alexa
   - Demographics — age, ethnicity, income, kids, etc
2. Support Vector Machine (SVM)
   - Each visitor = one vector
   - Similar behavior on other computers
   - Fingerprinting *behavior* not *browser*
3. Social network groups (credit: iSecLabs)
   - Check visitation of group pages
   - Intersection → unique human by name

Screw the spec

Now adopted in all browsers:

1. :visited, :link take color *only* (not even alpha)
2. JS always thinks it has not-visited color

Caveat: “Color does not affect DOM” is now a *security critical* feature (!)

… might break in the future (eg weird antialiasing leaks)

Kudos to David Baron (even if it took 8 years)

Questions?

Sai saizai.com/pubs

bugzilla.mozilla.org #147777

iseclab.org/people/gilbert

dbaron.org/mozilla/visited-privacy

P.S. Speed records (URL/min):

Local server, full round trip, April 2010

Explorer: 200k Firefox: 540k Opera: 620k

Chrome: 2M Safari: 3.4M