Obfuscation for and against device fingerprinting

Güneş Acar
University of Leuven
Dept. of Electrical Engineering (ESAT), COSIC
iMinds, Leuven, Belgium
Background

- web tracking
  - via cookies (since 1994)
- small text files automatically sent by the browser
- but cookies...
  - are subject to deletion
  - expire
  - can be modified easily
  - don’t work well with mobile
- alternatives...?
Web-based device fingerprinting

Collection of many data points through the browser to obtain a unique tracking identifier:

- plugins, fonts, screen size, software versions, clock skew, GPU, canvas, JS engine performance…
- 2010 study by EFF: %94.2 of the browsers with Flash or Java enabled were unique
Web-based device fingerprinting

- overcomes the limitations of cookies:
  - not subject to deletion or expiration
  - hard to spoof (cf. unique identifiers (UUID etc.))
  - hard to notice (can work in "tagless" mode)
  - may not be subject to privacy laws
FPDetective: Dusting the Web for Fingerprinters

Güneş Acar¹, Marc Juarez¹;², Nick Nikiforakis³, Claudia Diaz¹, Seda Gürses¹;⁴, Frank Piessens³ and Bart Preneel¹

¹ KU Leuven, Dept. of Electrical Engineering (ESAT), COSIC, iMinds, Leuven, Belgium
² IIIA-CSIC, Bellaterra, Spain
³ KU Leuven, Dept. of Computer Science, iMinds-DistriNet, Leuven, Belgium
⁴ New York University, Dept. of Media, Culture, and Communication, NY, USA
Font probing

- measure the dimensions of an invisible string with different fonts
- compare the dimensions to that of fallback font’s

<table>
<thead>
<tr>
<th>Fingerprinting Provider</th>
<th>Num Fonts</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueCava</td>
<td>231/167/62</td>
</tr>
<tr>
<td>Perferencement</td>
<td>153</td>
</tr>
<tr>
<td>CoinBase</td>
<td>206</td>
</tr>
<tr>
<td>MaxMind</td>
<td>94</td>
</tr>
<tr>
<td>Inside graph</td>
<td>355</td>
</tr>
<tr>
<td>SiteBlackBox</td>
<td>389</td>
</tr>
<tr>
<td>Analytics-engine</td>
<td>98</td>
</tr>
<tr>
<td>Myfreecams</td>
<td>71</td>
</tr>
<tr>
<td>Mindshare Tech.</td>
<td>487</td>
</tr>
<tr>
<td>Cdn.net</td>
<td>297</td>
</tr>
<tr>
<td>AFK Media</td>
<td>503</td>
</tr>
<tr>
<td>Anonymizer</td>
<td>80</td>
</tr>
<tr>
<td>Analyticsengine</td>
<td>93</td>
</tr>
</tbody>
</table>
Proxy Piercing

Nikiforakis et al. (2013)

Circumvent proxy to uncover real IP address

United States

Patent Application Publication

Barber

PROXY PIERCING FOR IDENTIFYING ADDRESS OF AND MARKETING TO A USER DEVICE INVOLVED IN AN ONLINE TRANSACTION

Inventor: Timothy P. Barber, Boise, ID (US)

Assignee: KOUNT INC., Boise, ID (US)

http://www.google.com/patents/US20110218856
Overview of the results

- 145 / Top 10K websites use Flash based fingerprinting
- 404 / Top 1M websites use Javascript based fingerprinting
- DNT didn’t change anything
- Vulnerabilities found in countermeasures
  - including Tor Browser
What else do they collect?

unsalted hashes of passwords!

minFraud Web Service API

http://dev.maxmind.com/minfraud
Where the data ends up?

massive reputation databases

- fingerprints, browsing/transaction history, reputation scores
  - 1.5B devices (iovation)
- bonus: associations
  - “Cross-Screen Reach & Audience Expansion”
  - links devices to consumer and household
Obfuscation as a countermeasure?

- Complex interaction (c.f. Web Search)
  - web sites run arbitrary code on your browser
  - passive server side fingerprinting don’t require extra interaction (e.g. clock skew)
- many side channels to uncover spoofed properties
- browser must provide some information to sustain the communication/protocol
User agent switcher extensions

- Advertised as a countermeasure to fingerprinting
- FireGloves, 12 browser extensions studied (by Nikiforakis et al. 2013)
  - none of them truly cover the real identity of the browser
  - increased distinguishability
  - impossible configurations
- "iatrogenic" problem
  - harm resulting from medical treatment

http://fingerprint.pet-portal.eu
Fingerprinting countermeasures in Tor Browser

- goal is to achieve “Cross-Origin Fingerprinting Unlinkability”
- cooperative obfuscation: same values for every user
  - system language, browser version, timezone, operating system
- reduce granularity (round screen size)
- implementation difficulties
  - Bug #8270, #5798
Conclusion & Open Questions

- device fingerprinting can be an instructive case for obfuscation based countermeasures
- how to decide on...
  - randomize or report same values for everyone
  - what is to be disabled
  - what is to be spoofed
  - what is to be
- need for a more systematic approach
Thanks

Claudia, Helen, Marc, Seda for comments…

https://www.cosic.esat.kuleuven.be/fpdetective/

github.com/fpdetective