Everything you always wanted to know about web-based device fingerprinting
(but were afraid to ask)

Nick Nikiforakis
echo `whoami`

• Postdoctoral researcher at KU Leuven
• Working, mainly, on web security and privacy
• Identify online ecosystems
  – Players
  – Interactions
  – Common patterns
• Search for systematic problems
Study Finds News Sites Fail to Aim Ads at Users

By TANZINA VEGA
Published: February 13, 2012

Web sites for newspapers, magazines and television stations might be hungry to make money with digital advertising, but you wouldn’t know it by the way some of them do business online.

A new study released Monday by the Pew Research Center Project for Excellence in Journalism looked at 22 news Web sites and more than 5,300 digital ads. It found that many of the sites had not attracted the same advertisers online as they did on other platforms.

In part, these sites were failing to attract online ads because they were not using technology that would customize ads based on their users’ online behavior. For example, a user searching for tickets to a Broadway show might see ads for that show.

The study, which looked at Web sites for 11 newspapers, four magazines and six television outlets, as well as two online-only sites, focused on premium digital ad placements on home pages or at the top of article pages, which have generally cost more to buy.

“One of the great challenges that faces the financial future of journalism is, how can you begin to charge more for digital advertising?” said Tom Rosenstiel, the director of the center. “The fact is, it’s not possible today.”
3rd Party Tracking

• “Suddenly” all sorts of websites that you’ve never heard about, can create a browsing profile of you and sell it to advertising companies
  – quantserve.com
  – scorecardresearch.com
  – addthis.com
Motivation & Contributions

• Tracking involves more than just 3rd party cookies
• Fingerprinting: Telling users apart based on their browsing environments, without extra stateful identifiers
• Thorough study of current fingerprinting practices on the web
• Difficulty of hiding the true nature of a user’s browsing environment
Users reacted...

- 1/3 of users delete first & third-party cookies within a month after they’ve been setup
- Multiple extensions revealing hidden trackers
  - Ghostery
  - Lightbeam
- Private mode of browsers used to avoid traces of cookies from certain websites
However...

• What if you could track users without the need of cookies or any other stateful client-side identifier?
  – Hidden from users
  – Hard to avoid it / opt-out

Web-based device fingerprinting
• Eckersley showed in 2010 that certain attributes of your browsing environment can be used to accurately track you
• These attributes, when combined, created a quite unique fingerprint of your system?
  – How?
Properties fingerprinted by Panopticlick
Resulting fingerprints

• 94.2% of the users with Flash/Java could be uniquely identified

• Simple heuristic algorithms could track updates of the same browser
Paywall

Feds Are Suspects in New Malware That Attacks Tor Anonymity

BY KEVIN POULSEN 08.05.13  3:57 AM

Follow @kpoulsen
Fast forward 2 years

• In mid 2012, all we knew is that fingerprinting is possible and that a small number of companies offer it as a service

• Questions that begged answering:
  – How are they doing it?
  – Could they do more?
  – Who is using them?
  – How are users trying to hide?
    • Is it working?
Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting

Nick Nikiforakis*, Alexandros Kapravelos†, Wouter Joosen*, Christopher Kruegel†, Frank Piessens*, Giovanni Vigna†
*IMinds-DistriNet, KU Leuven, 3001 Leuven, Belgium
{firstname.lastname}@cs.kuleuven.be
†University of California, Santa Barbara, CA, USA
{kapravel,chris,vigna}@cs.ucsb.edu

Abstract—The web has become an essential part of our society and is currently the main medium of information delivery. Billions of users browse the web on a daily basis, and there are single websites that have reached over one billion user accounts. In this environment, the ability to track users and their online habits can be very lucrative for advertising companies, yet very intrusive for the privacy of users.

In this paper, we examine how web-based device fingerprinting currently works on the Internet. By analyzing the code of three popular browser-fingerprinting code providers, we reveal the techniques that allow websites to track users without the need of client-side identifiers. Among these techniques, we show how current commercial fingerprinting approaches use questionable practices, such as the circumvention of HTTP proxies to discover a user’s real IP address and the installation of intrusive browser plugins.

At the same time, we show how fragile the browser ecosystem is against fingerprinting through the use of novel browser-identifying techniques. With so many different vendors involved in browser development, we demonstrate how one can use diversions in the browsers’ implementation to distinguish servers. With every request toward a third-party website, that website has the ability to set and read previously-set cookies on a user’s browser. For instance, suppose that a user browses to travel.com, whose homepage includes a remote image from tracking.com. Therefore, as part of the process of rendering travel.com’s homepage, the user’s browser will request the image from tracking.com. The web server of tracking.com sends the image along with an HTTP Set-Cookie header, setting a cookie on the user’s machine, under the tracking.com domain. Later, when the user browses to other websites affiliated with tracking.com, e.g., buy.com, the tracking website receives its previously-set cookies, recognizes the user, and creates a profile of the user’s browsing habits. These third-party cookies, due to the adverse effects on a user’s privacy and their direct connection with online behavioral advertising, captured the attention of both the research community [2], [3], [4] and the popular media outlets [5] and caregivers, cause the public’s
FPDetective: Dusting the Web for Fingerprinters

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

¹KU Leuven, Dept. of Electrical Engineering (ESAT), COSIC, iMinds, Leuven, Belgium
{gunes.acar, marc.juarez, claudia.diaz, seda.gurses, bart.preneel}@esat.kuleuven.be

²IIIA-CSIC, Bellaterra, Spain
mjuarez@iiia.csic.es

³KU Leuven, Dept. of Computer Science, iMinds-DistriNet, Leuven, Belgium
{nick.nikiforakis, frank.piessens}@cs.kuleuven.be

⁴New York University, Dept. of Media, Culture, and Communication, NY, USA

ABSTRACT

In the modern web, the browser has emerged as the vehicle of choice, which users are to trust, customize, and use, to access a wealth of information and online services. However, recent studies show that the browser can also be used to invisibly fingerprint the user: a practice that may have serious privacy and security implications.

In this paper, we report on the design, implementation services; K.4.4 [Computers and Society]: Electronic Commerce — Security

Keywords

Web security; privacy; device fingerprinting; tracking; dynamic analysis; JavaScript; Flash

1. INTRODUCTION
Manual analysis of 3 fingerprinting companies

1. Find the domains that they use to serve their fingerprinting scripts
2. Find some websites that use them and extract the code
3. De-obfuscate and analyze
4. Compare and classify
Step 3 took a while...
Results

• After extracting all features, we created a taxonomy of all fingerprinted features, and compared each company to Panopticlick

• Collectively, Panopticlick was fully covered

<table>
<thead>
<tr>
<th>Hardware &amp; Network</th>
<th>Browser customizations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Browser-level User Conf.</td>
</tr>
<tr>
<td></td>
<td>Browser Family &amp; Version</td>
</tr>
<tr>
<td></td>
<td>OS &amp; Applications</td>
</tr>
</tbody>
</table>

ActiveX + CLSIDs
DNT Choice
Math constants
Windows Registry
TCP/IP Parameters
Non-trivial extras

• Non-plugin font detection
  – Comparison of text’s width & height

• Native Fingerprinting plugins
  – Accessing highly-specific registry value

• Fingerprint delivery mechanisms

• Proxy detection
<table>
<thead>
<tr>
<th>String</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>I_DO_NOT_NEED_FLASH</td>
<td>500 x 84</td>
</tr>
<tr>
<td>I_DO_NOT_NEED_FLASH</td>
<td>520 x 84</td>
</tr>
<tr>
<td>I_DO_NOT_NEED_FLASH</td>
<td>580 x 87</td>
</tr>
<tr>
<td>I_DO_NOT_NEED_FLASH</td>
<td>399 x 82</td>
</tr>
</tbody>
</table>
Non-trivial extras

• Non-plugin font detection
  – Comparison of text’s width & height

• Native Fingerprinting plugins
  – Accessing highly-specific registry values

• Fingerprint delivery mechanisms

• Proxy detection
Proxy-detection

Proxy Server

Fingerprinting server

http://www.example.com

JS  ↔  SWF

token

token
Adoption

Dataset A

– Crawled top 10,000 sites, searching for inclusions from the 3 fingerprint providers

– 40 sites discovered
  • Porn & dating sites most prominent
    – Shared credentials & Sybil attacks
  • skype.com the highest ranking one
Adoption

Dataset B

– 3,804 domains from Wepawet
But wait... there’s more!

• Can we find unknown fingerprinting parties?
  – How do we separate a fingerprinting script from a generic analytics script?

• Fonts!
  – Separating feature between normal analytics and fingerprinting
  – Second most identifying feature according to Eckersley
FPDetective

• Fingerprinting-sensitive crawler
  – If fonts are touched, record site

• Detection of font snooping
  – JS-based font probing (Modified browser)
  – Flash-based font probing (decompilation of Flash)
Adoption (revisited)

Dataset A

– Crawled top 10,000 sites, searching for inclusions from the 3 fingerprint providers

– 40 sites discovered
  • Porn & dating sites most prominent
    – Shared credentials & Sybil attacks

• skype.com the highest ranking one
Adoption (revisited)

Dataset A

– Crawled top 10,000 sites, searching for inclusions from the 3 fingerprint providers
– 40 sites discovered
  • Porn & dating sites most prominent
    – skype.com the highest ranking one
  • 145 fingerprinting sites in the top Alexa 10K
  • DNT does not matter
  • Shared credentials & Sybil attacks
Status

• Fingerprinting is out there
  – Quite a number of new techniques over Panopticlick
• Large and popular sites are using them
• Could they be doing more?
  – How do the browser internals relate to a browser’s identity?
DIY Fingerprinting

• We decided to try some fingerprinting of our own
• Focus on the two special JS objects that fingerprinters probe the most:
  – navigator
  – screen
• Perform a series of everyday operations and search for differences across browsers
  – Add properties
  – Remove properties
  – Modify properties
Novel methods discovered

• E.g., Natural ordering of properties can give away a browser family, and occasionally, a browser version

navigator.geolocation
navigator.onLine
navigator.cookieEnabled
navigator.vendorSub
navigator.vendor

navigator.appCodeName
navigator.appName
navigator.appVersion
navigator.language
navigator.mimeTypes

⟵ navigator.appCodeName
⟵ navigator.appName
navigator.appMinorVersion
navigator.cpuClass
navigator.platform
Status

• Fingerprinting is out there
  – Quite a number of new techniques over Panopticlick
• Large and popular sites are using them
• There could be more fingerprinting done by the companies
• How could a user react?
Browser extensions

• Reviewed 11 different browser extensions that spoof a browser’s user-agent
  – 8 Firefox + 3 Chrome
  – More than 800,000 users

• Advice to use such extensions:
  – Previous research in web tracking
  – Underground hacking guides

• How do they stand-up against fingerprinting?
Worse than nothing...

• All of them had one or more of the following:
  – Incomplete coverage of the navigator object
  – Impossible configurations
  – Mismatch between UA header and UA property

• Iatrogenic problem:
  – When installing these, a user becomes more visible and more fingerprintable than before
Worse than nothing...

• All of them had one or more of the following:
  - Incomplete coverage of the navigator object
  - Impossible configurations
  - Mismatch between UA header and UA property

• Iatrogenic problem:
  - When installing these, a user becomes more visible and more fingerprintable than before
Conclusion

• Fingerprinting is a real problem
• Browsers are so complex that it is really hard to make them seem identical
• Current browser extensions should not be used for privacy reasons
• Long term solutions will most-likely not be pure technical ones
  – Legislation required, like in stateful tracking
"I spy with my free fingerprint kit."

If you're going on a spying mission, you need a fingerprint kit you can hide down your sock.

Now you can get one free, with Trebor Double Agents. It comes with fingerprint powder, a brush, magnifying glass, record cards and full instructions. Everything you need to be a dab hand at catching spies.

To get your fingerprint kit, just send us the coupon with any four Double Agents (for postage and packaging). Before enemy agents foil your plans.

nick.nikiforakis@cs.kuleuven.be
http://www.securitee.org