Tracking on the Web

CS 161: Computer Security
Prof. David Wagner

April 28, 2013
Tracking Your Web Surfing

• The sites you visit learn:
  – The **URLs** you’re interested in
    • Google/Bing also learns *what you’re searching for*
  – Your **IP address**
    • Thus, your service provider & geo-location
    • Can often link you to other activity including at other sites
  – Your browser’s capabilities, which OS you run, which language you prefer
  – Which URL you looked at that took you there
    • Via “**Referer**” header
• Oh and also cookies.
• Cookies = state that server tells browser to store locally
  – Name/value pair, plus expiration date
• Browser returns the state any time visiting the same site

• Where’s the harm in that? And are these used much anyway?
Let’s remove all of our cookies.
The following cookies are stored on your computer:

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
</table>

Cool, no web site is tracking us …
We do a search on "private browsing"
Private Browsing - Browse the web without saving information about ...
support.mozilla.org/.../private-browsing-browse-web-without-saving-inf...▼
When using a shared computer, Private Browsing is great for viewing websites without saving stuff like cookies, temp files and a history of the pages you visit.

Firefox 20 Launches With Improved Private Browsing, New ...
techncrunch.com/.../firefox-20-launches-with-per-tab-private-bro...▼
by Frederic Lardinois - in 18,052 Google+ circles
Apr 2, 2013 – Firefox 20 is now available for download. The emphasis of today's release is on Firefox's private browsing mode, which now allows Firefox ...

Privacy mode - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Privacy_mode▼
Internet Explorer 8 in InPrivate mode. Google Chrome in Incognito mode. Privacy mode or "private browsing", sometimes informally referred to as "porn mode", ...

Firefox 20 improves private browsing, fixes three critical flaws | ZDNet
www.zdnet.com/firefox-20-improves-private-browsing-fixes-three-critic...▼
Apr 3, 2013 – Mozilla has released the latest version of its Firefox web browser which features new enhancement to private browsing and fixes a number of ...

Private Browsing - Web Browsers - About.com
browsers.about.com › ... › Web Browsers › Web Browser Glossary › FAQs▼
The methods for activating private browsing mode differ across browsers, operating systems, and device types. These step-by-step tutorials teach you how to ...
Google has stored a couple of cookies on our system.
Goodness knows what info they decided to put in the cookie.
But it lasts for 6 months ...
We click on the top result.
Note that this mode is privacy from your family, not from web sites!
Ironically, we’ve gained a bunch of cookies in the process.
The following cookies are stored on your computer:

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td></td>
</tr>
<tr>
<td>google.com</td>
<td>PREF</td>
</tr>
<tr>
<td>google.com</td>
<td>NID</td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td>_utma</td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td>_utmb</td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td>_utmcs</td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td>_utmz</td>
</tr>
<tr>
<td>youtube.com</td>
<td></td>
</tr>
<tr>
<td>youtube.com</td>
<td>VISITOR_INFO1_LIVE</td>
</tr>
<tr>
<td>youtube.com</td>
<td>YSC</td>
</tr>
<tr>
<td>youtube.com</td>
<td>PREF</td>
</tr>
</tbody>
</table>

Name: _utma
Content: 62528430.549021593.1398719659.1398719659.1398719659.
Domain: .support.mozilla.org
Path: /  
Send For: Any type of connection
Expires: April 27, 2016 at 2:14:27 PM

This one sticks around for two years.
How did YouTube enter the picture??
YouTube is remembering the version of Flash I’m running…
We navigate to The New York Times …
U.S. Announces More Sanctions Against Russia Over Ukraine

By PETER BAKER and MARK LANDLER

The United States ordered travel bans and asset freezes for seven Russian officials, including two said to be in President Vladimir V. Putin’s inner circle, and froze assets for 17 firms.

Egypt Sentences More Than 680 to Death

The Muslim Brotherhood’s spiritual leader and hundreds of others were sentenced on charges of inciting or committing violence. Supporters, above, reacted to the verdict Monday.

The Opinion Pages

Political Executions in Egypt
It is clear from the sentencing of 680 people to death in a mass trial that the country’s judges have become a government tool.

- Editorial: Smartphones and the 4th Amendment
- Krugman: High Plains Moochers

Today’s Times Insider

Behind the scenes of The New York Times

- Thinking of Wine as Food With Eric Asimov
- Introducing Times Insider

MARKETS

At close 04/28/2014

S&P 500
Dow
Nasdaq
What a lot of yummy cookies!

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dotomi.com</td>
<td></td>
</tr>
<tr>
<td>doubleclick.net</td>
<td></td>
</tr>
<tr>
<td>dynamicyield.com</td>
<td></td>
</tr>
<tr>
<td>google.com</td>
<td></td>
</tr>
<tr>
<td>imrworldwide.com</td>
<td></td>
</tr>
<tr>
<td>krxd.net</td>
<td></td>
</tr>
<tr>
<td>markets.on.nytimes.com</td>
<td></td>
</tr>
<tr>
<td>mediaplex.com</td>
<td></td>
</tr>
<tr>
<td>nytimes.com</td>
<td></td>
</tr>
<tr>
<td>revsci.net</td>
<td></td>
</tr>
<tr>
<td>scorecardresearch.com</td>
<td></td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td></td>
</tr>
<tr>
<td>wt.o.nytimes.com</td>
<td></td>
</tr>
<tr>
<td>youtube.com</td>
<td></td>
</tr>
</tbody>
</table>

Name: <no cookie selected>
Content: <no cookie selected>
Host: <no cookie selected>
Path: <no cookie selected>
Send For: <no cookie selected>
Expires: <no cookie selected>

Remove Cookies  Remove All Cookies
Here are the ones from the website itself ...

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>nytimes.com</td>
<td>RMD</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>nyt5_disable</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyid</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyfs</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_cb_is</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>nytnew3p</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag281772.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>nyt-m</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>nyt-recommend</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>adxcl</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>adxc</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>tagx-l</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>tagx-s</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>tagx-p</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>WT_FPC</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyaud_page</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dysvar_8765260</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyuss_8765260</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyest</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dy_geo</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyaud_nchc</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyaud_sess</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyus_8765260</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>rsi_segs</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag27935.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag27728.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag15486.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag21418.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag21233.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag28173.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_chartbeat2</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_chartbeat_uuniq</td>
</tr>
</tbody>
</table>
This one tracks the details of my system & browser.
doubleclick.net - who's that? And how did it get there from visiting www.nytimes.com?
Third-Party Cookies

• How can a web site enable a third party to plant cookies in your browser & later retrieve them?
  – Answer: using a “web bug”
  – Include on the site’s page (for example):
    • `<img src="http://doubleclick.net/ad.gif" width=1 height=1>`

• Why would a site do that?
  – Site has a business relationship w/ DoubleClick*
  – Now DoubleClick sees all of your activity that involves their web sites (each of them includes the web bug)
    • Because your browser dutifully sends them their cookies for any web page that has that web bug
    • Identifier in cookie ties together activity as = YOU

* Owned by Google, by the way
Remember this 2-year Mozilla cookie?

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>PREF, NID</td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td>__utma</td>
</tr>
<tr>
<td></td>
<td>__utmb</td>
</tr>
<tr>
<td></td>
<td>__utmz</td>
</tr>
<tr>
<td></td>
<td>__utmc</td>
</tr>
<tr>
<td>youtube.com</td>
<td>VISITOR_INFO1_LIVE, YSC, PREF</td>
</tr>
</tbody>
</table>
Google Analytics

• Any web site can (anonymously) register with Google to instrument their site for analytics
  – Gather information about who visits, what they do when they visit
• To do so, site adds a small Javascript snippet that loads http://www.google-analytics.com/ga.js
  – You can see sites that do this because they introduce a "__utma" cookie
• Code ships off to Google information associated with your visit to the web site
  – Shipped by fetching a GIF w/ values encoded in URL
  – Web site can use it to analyze their ad “campaigns”
  – Not a small amount of info …
Values Reportable via Google Analytics

- Affiliation
- Billing City
- Billing Country
- Billing Region
- Browser Lang.
- Complete URL
- Cookie Values
- Current Page
- Event Tracking
- Flash Version
- Grand Total
- Host Name
- Java-enabled
- Language Encoding
- Order ID
- Page Title
- Product Code
- Product Name
- Profile Number
- Repeat Campaign Visit
- Quantity
- Screen Color Depth
- Screen Resolution
- Shipping Cost
- Special Event
- Start Campaign Sess.
- Tax
- Tracking Code Version
- Unique GIF ID
- Unit Price
- User Defined Var
- Variations on an Item
Still More Tracking Techniques …

- Any scenario where browsers execute programs that manage persistent state can support tracking by cookies
  - Such as .... Flash ?
My browser had Flash cookies from 67 sites!

Sure, this is where you’d think to look to analyze what Flash cookies are stored on your machine.

Some Flash cookies “respawn” regular browser cookies that you previously deleted!
A new bug in Internet Explorer allows hackers to commandeer your computer.

If you're using Internet Explorer and click on the wrong link, a hacker could hijack your computer.
What does Facebook learn?

• Many pages include a Facebook “Like” button.
• What are the implications, for user tracking?
Tracking – So What?

• Cookies etc. form the core of how Internet advertising works today
  – Without them, arguably you’d have to pay for content up front a lot more
    • (and payment would mean you’d lose anonymity anyway)
  – A “better ad experience” is not necessarily bad
    • Ads that reflect your interests; not seeing repeated ads

• But: ease of gathering so much data so easily ⇒ concern of losing control how it’s used
  – Content shared with friends doesn’t just stay with friends …
When you interview, they Know What You’ve Posted

Gone are the days when all job seekers had to worry about were their résumés and cover letters. Today, those documents remain a staple of the job-search process, but they are joined by a growing phenomenon: social networking.

Forty-five percent of employers reported in a June 2009 CareerBuilder survey that they use social networking sites to screen potential employees, compared to only 22 percent of employers last year. Eleven percent of employers plan to start using social networking sites for the screening process. More than 2,600 hiring managers participated in the survey.
Why employers disregard candidates after screening online

Thirty-five percent of employers reported they have found content on social networking sites that caused them not to hire the candidate, including:

- Candidate posted provocative or inappropriate photographs or information -- 53 percent
- Candidate posted content about them drinking or using drugs -- 44 percent
- Candidate bad-mouthed their previous employer, co-workers or clients -- 35 percent
- Candidate showed poor communication skills -- 29 percent
- Candidate made discriminatory comments -- 26 percent
- Candidate lied about qualifications -- 24 percent
- Candidate shared confidential information from previous employer -- 20 percent
Tracking – So What?

• Cookies etc. form the core of how Internet advertising works today
  – Without them, arguably you’d have to pay for content up front a lot more
    • (and payment would mean you’d lose anonymity anyway)
  – A “better ad experience” is not necessarily bad
    • Ads that reflect your interests; not seeing repeated ads

• But: ease of gathering so much data so easily ⇒ concern of losing control how it’s used
  – Content shared with friends doesn’t just stay with friends …
  – You really don’t have a good sense of just what you’re giving away …
My baby girl.... http://t.co/5qLfLV6

2 minutes ago via Twitter for Android

BritBangert
Brittany Bangert
Who have we stalked recently?

ICanStalkU was able to stalk RangeLifeEnt at 51 Great Jones St New York NY
1 minute ago · Map Location · View Tweet · View Picture · Reply to RangeLifeEnt

ICanStalkU was able to stalk Inicklassen at http://maps.google.com/?q=57.1344444444,12.7141666667
2 minutes ago · Map Location · View Tweet · View Picture · Reply to Inicklassen

ICanStalkU was able to stalk Welerson13 at http://maps.google.com/?q=-15.7380555556,-47.898611111
2 minutes ago · Map Location · View Tweet · View Picture · Reply to Welerson13

ICanStalkU was able to stalk BritBangert at 920 Hawley St Taylorville IL
1 minute ago · Map Location · View Tweet · View Picture · Reply to BritBangert

ICanStalkU was able to stalk jiggy_Owla at http://maps.google.com/?q=13.7830055879,100.518500685
4 minutes ago · Map Location · View Tweet · View Picture · Reply to jiggy_Owla

ICanStalkU was able to stalk gcolony at http://maps.google.com/?q=37.7851666667,-122.404166667
4 minutes ago · Map Location · View Tweet · View Picture · Reply to gcolony

Links

- Mayhemic Labs
- PaulDotCom
- SANS ISC
- Electronic Frontier Foundation
- Center for Democracy & Technology

How did you find me?

Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information.
read more

Help me fix this!

Disabling Geo-Tagging on your phone is easy. Check your user manual of
How To Gain Better Privacy?

• Force of law
  – Example #1: web site privacy policies
    • US sites that violate them commit false advertising
    • But: policy might be “Yep, we sell everything about you, Ha Ha!”
7. Collection of Viewing Information. You acknowledge that you are aware of and consent to the collection of your viewing information during your use of the Software and/or Content. Viewing information may include, without limitation, the time spent viewing specific pages, the order in which pages are viewed, the time of day pages are accessed, IP address and user ID. This viewing information may be linked to personally identifiable information, such as name or address and shared with third parties.
How To Gain Better Privacy?

• Force of law
  – Example #1: web site privacy policies
    • US sites that violate them commit false advertising
    • But: policy might be “Yep, we sell everything about you, Ha Ha!”
  – Example #2: SB 1386
    • Requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed)
    • Quite effective at getting sites to pay attention to securing personal information
May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waqqener, UCB's chief technology officer, said in a press conference Friday afternoon.
How To Gain Better Privacy?

• Technology
  – Special browser extensions
  – Tor and anonymizers – wait for Friday!