CSE 484: Computer Security and Privacy

Biometrics and Privacy

Fall 2021

David Kohlbrenner

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
Administrivia
Secondary Factors Do Help!

Account takeover prevention rates, by challenge type

Both device- and knowledge-based challenges help thwart automated bots, while device-based challenges help thwart phishing and even targeted attacks.
Graphical Passwords

• Many variants... one example: Passfaces
  • Assumption: easy to recall faces
Graphical Passwords

• Another variant: draw on the image (Windows 8)

• Problem: users choose predictable points/lines
Unlock Patterns

• Problems:
  • Predictable patterns (familiar pattern by now)
  • Smear patterns
  • Side channels: apps can use accelerometer and gyroscope to extract pattern!
What About Biometrics?

• Authentication: **What you are**

• Unique identifying characteristics to authenticate user or create credentials
  • Biological and physiological: Fingerprints, iris scan
  • Behaviors characteristics - how perform actions: Handwriting, typing, gait

• Advantages:
  • Nothing to remember
  • Passive
  • Can’t share (generally)
  • With perfect accuracy, could be fairly unique
Issues with Biometrics

• Private, but not secret
  • Maybe encoded on the back of an ID card?
  • Maybe encoded on your glass, door handle, ...
  • Sharing between multiple systems?

• Revocation is difficult (impossible?)
  • Sorry, your iris has been compromised, please create a new one...

• Physically identifying
  • Soda machine to cross-reference fingerprint with DMV?

• Birthday paradox
  • With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples
Shifting Threat Models...

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.
Attacking Biometrics

• An adversary might try to steal biometric info
  • Malicious fingerprint reader
    • Consider when biometric is used to derive a cryptographic key
  • Residual fingerprint on a glass
Attacking Biometrics

Scanning fingerprint from display

[Starbug -- http://istouchidhackedyet.com/]
Attacking Biometrics

Attacking Biometrics

[Starbug -- http://istouchidhackedyet.com/]

Making dummy print from wood glue
Attacking Biometrics

Using dummy print

[Starbug -- http://istouchidhackedyet.com/]
Privacy and web tracking
A topic in flux

• Tracking via cookies

• Tracking via other methods

• Fingerprinting
Ads That Follow You

Advertisers (and others) track your browsing behaviors for the purposes of targeted ads, website analytics, and personalized content.
Third-Party Web Tracking

These ads allow criteo.com to link your visits between sites, even if you never click on the ads.
Concerns About Privacy

The New York Times

‘Do Not Track’ Privacy Bill Appears in Congress

By TANZINA VEGA

May 6, 2011, 5:01 pm 3 Comments

And the privacy legislation just keeps on coming.

On Friday, two bills were introduced in Washington in support of a Do Not Track mechanism that would give users control over how much of their data was collected by advertisers and other online companies.

By JENNIFER VALENTINO-DEVRIES, JEREMY SINGER-VINE and ASHKAN SOLTANI

December 24, 2012
First and Third Parties

- **First-party cookie**: belongs to top-level domain.
- **Third-party cookie**: belongs to domain of embedded content (such as image, iframe).
Anonymous Tracking

Trackers included in other sites use third-party cookies containing unique identifiers to create browsing profiles.
Basic Tracking Mechanisms

• Tracking requires:
  (1) re-identifying a user.
  (2) communicating id + visited site back to tracker.

Hypertext Transfer Protocol

GET /pixel/p-3aud4J6uA4Z6Y.gif?labels=InvisibleBox&busty=2710 HTTP/1.1\r\nHost: pixel.quantserve.com\r\nConnection: keep-alive\r\nAccept: image/webp,/*;q=0.8\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36
Referer: http://www.theonion.com/\r\nAccept-Encoding: gzip, deflate, sdch\r\nAccept-Language: en-US, en; q=0.8\r\nCookie: mc=52a65386-f1de1-00ade-0b26e; d=ENkBRqGHD4GYEA35MMIL74MKiyDs1A2MQI1Q
Tracking Technologies

- HTTP Cookies
- HTTP Auth
- HTTP Etags
- Content cache
- IE userData
- HTML5 protocol and content handlers
- HTML5 storage
- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache

- “Zombie” cookies that respawn
  (http://samy.pl/evercookie)
Other Trackers?

“Personal” Trackers
Personal Tracking

- Tracking is **not anonymous** (linked to accounts).
- Users **directly visit tracker’s site** → evades some defenses.
How prevalent is tracking? (2011)

524 unique trackers on Alexa top 500 websites (homepages)

- 457 domains (91%) embed at least one tracker.
  (97% of those include at least one cross-site tracker.)

- 50% of domains embed between 4 and 5 trackers.

- One domain includes 43 trackers.
Who/what are the top trackers? (2011)

Top 20 Cross-Site Trackers on Top 500 Domains

- DoubleClick
- Facebook
- Google
- QuantServe
- Twitter
- AdMn
- YieldManager
- ImrWorldwide
- Revsci
- Adthrive
- ADX
- InviteMedia
- Serving-SYS
- YouTube
- Addthis
- BlueKai
- MediaPlex
- 207

Tracker Prevalence (# Domains)
How has this changed over time?

• The web has existed for a while now...
  - What about tracking before 2011?
  - What about tracking before 2009?

• Solution: time travel!
The Wayback Machine to the Rescue

Time travel for web tracking: http://trackingexcavator.cs.washington.edu
1996-2016: More & More Tracking

- More trackers of more types, more per site, more coverage
Defenses to Reduce Tracking

• Do Not Track?

Send a ‘Do Not Track’ request with your browsing traffic

Do Not Track is not a technical defense: trackers must honor the request.
Defenses to Reduce Tracking

- Do Not Track proposal?
- Private browsing mode?

Private browsing mode protects against local, not network, attackers.

You’ve gone incognito

Now you can browse privately, and other people who use this device won’t see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome won’t save the following information:
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:
- Websites you visit
- Your employer or school
- Your internet service provider
Defenses to Reduce Tracking

• Do Not Track proposal?
• Private browsing mode?
• Third-party cookie blocking?

www.bar.com

www.foo.com

Bar’s Server

www.bar.com’s cookie (1st party)

www.foo.com’s cookie (3rd party)

Foo’s Server
Its real!

• Safari and FF (mostly) now block 3<sup>rd</sup> party cookies
  • https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

• Chrome...

  “By undermining the business model of many ad-supported websites, blunt approaches to cookies encourage the use of opaque techniques such as fingerprinting (an invasive workaround to replace cookies), which can actually reduce user privacy and control. We believe that we as a community can, and must, do better.”
Fingerprinting is out there

• Better than a ‘voluntary’ cookie: involuntary, unchangeable id!
  • “Fingerprint”

• Idea: Measure ‘behavior’ of browser
  • Smash into unique ID
Fingerprinting Web Browsers

- User agent
- HTTP ACCEPT headers
- Browser plug-ins
- MIME support
- Clock skew

- Installed fonts
- Cookies enabled?
- Browser add-ons
- Screen resolution
- HTML5 canvas
  (differences in graphics SW/HW!)
HTML5 Canvas Fingerprinting - Text

Figure 7: Difference maps for a group on text_arial

Mowery and Shacham, 2012
HTML5 Canvas Fingerprinting - Image

Figure 10: Original render and difference maps for Group 24

Mowery and Shacham, 2012
And its out there!

Figure 4: Different images printed to canvas by fingerprinting scripts. Note that the phrase “Cwm fjordbank glyphs vext quiz” in the top image is a perfect pangram, that is, it contains all the letters of the English alphabet only once to maximize diversity of the outcomes with the shortest possible string.
Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

**Our tests indicate that you have strong protection against Web tracking.**

**IS YOUR BROWSER:**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking tracking ads?</td>
<td>Yes</td>
</tr>
<tr>
<td>Blocking invisible trackers?</td>
<td>Yes</td>
</tr>
<tr>
<td>Protecting you from fingerprinting?</td>
<td>Your browser has a nearly-unique fingerprint</td>
</tr>
</tbody>
</table>

Still wondering how fingerprinting works?

**One in 145,235 browsers have the same fingerprint**

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 145,235** browsers have the same fingerprint as yours.
Fingerprinting as a security measure

• Blocking bots (e.g. reCAPTCHA)

• Validating users over-time
How should we view tracking and fingerprinting efforts?
“Privacy preserving” personalized ads

• [https://github.com/WICG/turtledove](https://github.com/WICG/turtledove)
  • The browser, not the advertiser, holds the information about what the advertiser thinks a person is interested in.
  • Advertisers can serve ads based on an interest, but cannot combine that interest with other information about the person — in particular, with who they are or what page they are visiting.
  • Web sites the person visits, and the ad networks those sites use, cannot learn about their visitors' ad interests.