CSE 484 / CSE M 584: Computer Security and Privacy

Autumn 2019

Tadayoshi (Yoshi) Kohno
yoshi@cs.Washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Franzi Roesner, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Announcements

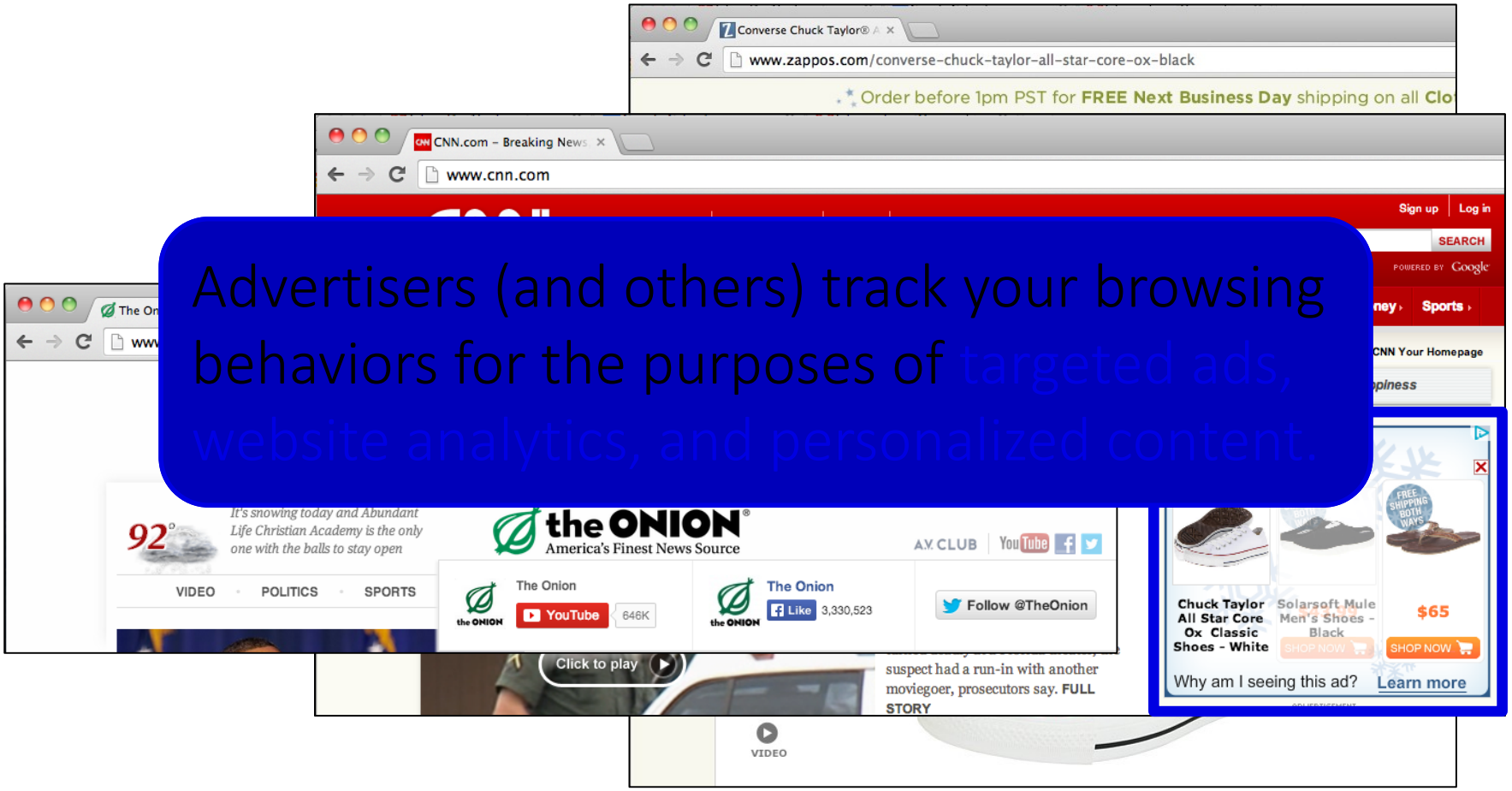
- My office hours
  - 11/20 (Wed), 2:30pm, CSE1 403
  - 11/27 (Wed), None
  - 12/4 (Wed), 12:30pm, CSE1 403
- Final Project checkpoints looked great!
- Next Final Project deadline Nov 22
  - Outline + references
  - Doesn't need to be super-detailed
- Lab 2: Nov 22

Review: User Authentication: Stepping Back

- What is the threat model?
  - Someone with access to your physical possessions (e.g., key logger, steal written password book)
  - Someone across the Internet (e.g., who compromises one or multiple sites)
- What "costs" are one willing to expend?
  - Usability
  - Legal protection (e.g., passwords vs biometrics and the law)
- Keep in mind password recovery mechanisms

Web Tracking and Privacy

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 (2010 – 2011)

THE WALL STREET JOURNAL.

WHAT THEY KNOW | JULY 30, 2010

The Web's New Gold Mine: Your Secrets

A Jou
busin

By JU

Hidd
all to

The
ident

The New York Times

May 6, 2011, 5:01 pm | 3 Comments

'Do Not Track' Privacy Bill Appears in Congress

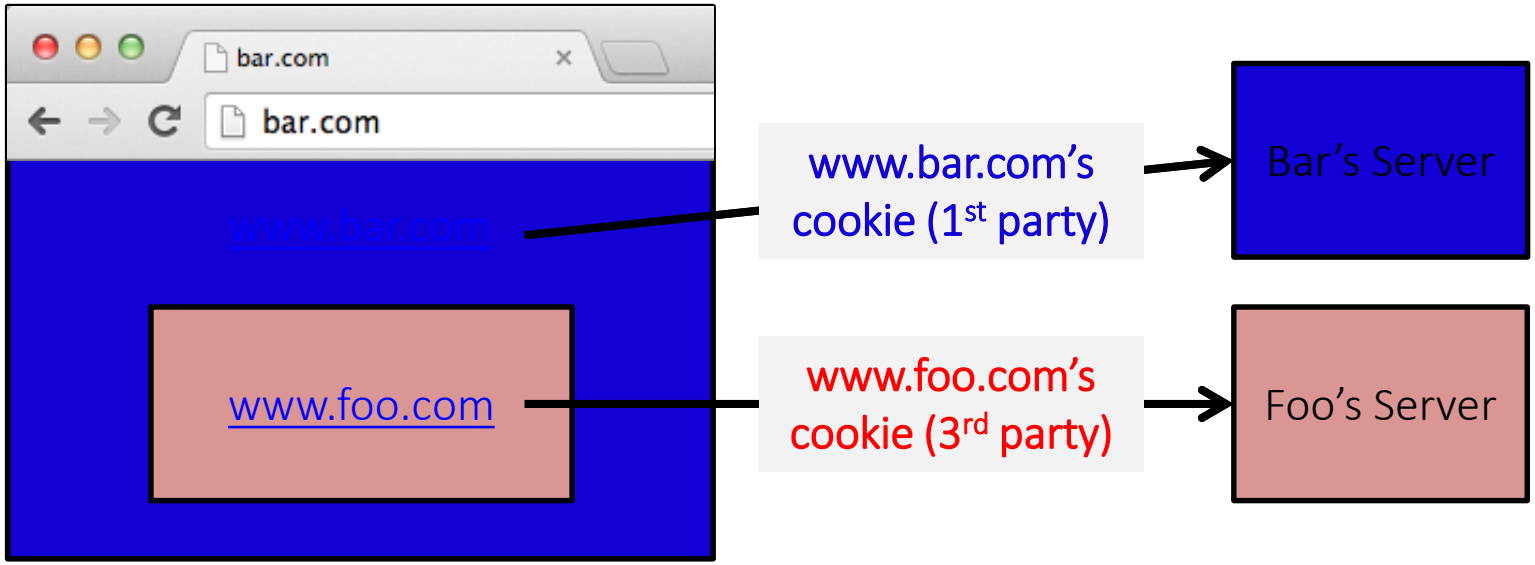
By TANZINA VEGA

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.

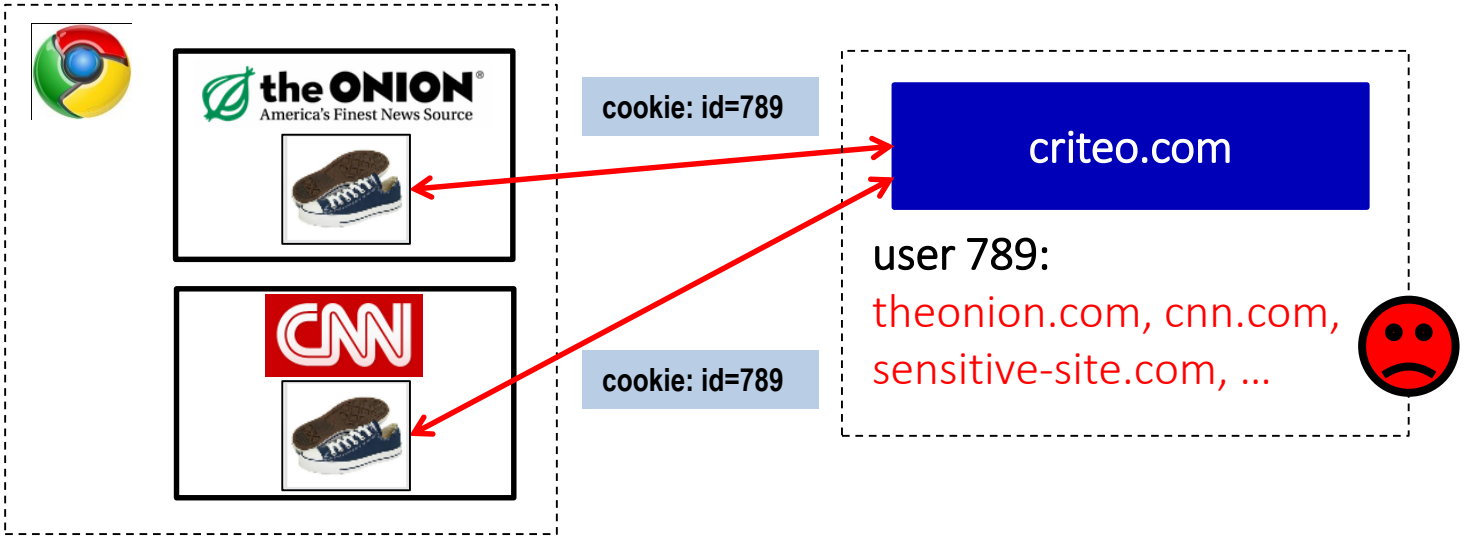
First and Third Parties

- 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\n
    Host: pixel.quantserve.com\r\n
    Connection: keep-alive\r\n
    Accept: image/webp,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36
    Referer: http://www.theonion.com/\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Cookie: mc=52a65386-f1de1-00ade-0b26e; d=ENkBRgGHD4GYEA35MMIL74MKiyDs1A2MQI1Q
```

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)

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!)

EFF's Panopticlick

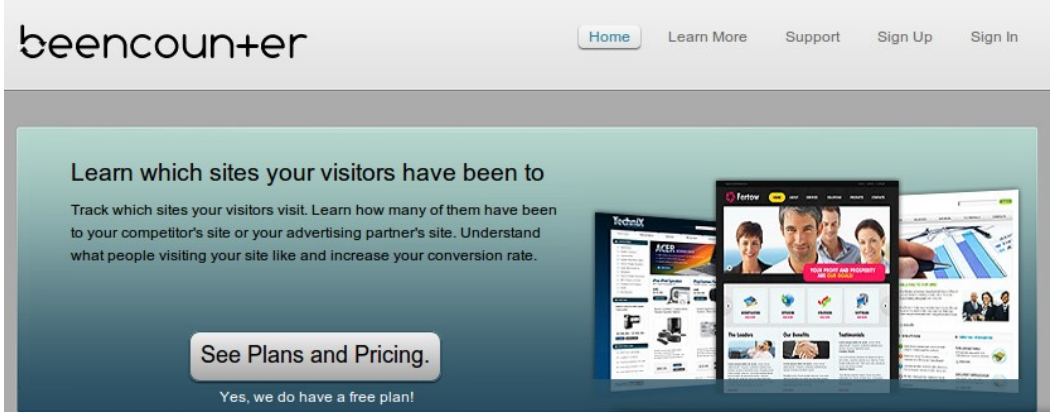
- https://panopticlick.eff.org/

Q: How might a website figure out what *other* site you have visited, without using cookies or tracking?

History Sniffing

How can a webpage figure out which sites you visited previously?

- Color of links
  - CSS :visited property
  - getComputedStyle()
- Cached Web content timing
- DNS timing



How Websites Get Your Identity

Personal trackers

Leakage of identifiers

GET http://ad.doubleclick.net/adj/...
Referer: http://submit.SPORTS.com/...?email=jdoe@email.com
Cookie: id=35c192bcfe0000b1...

Security bugs

Third party buys your identity

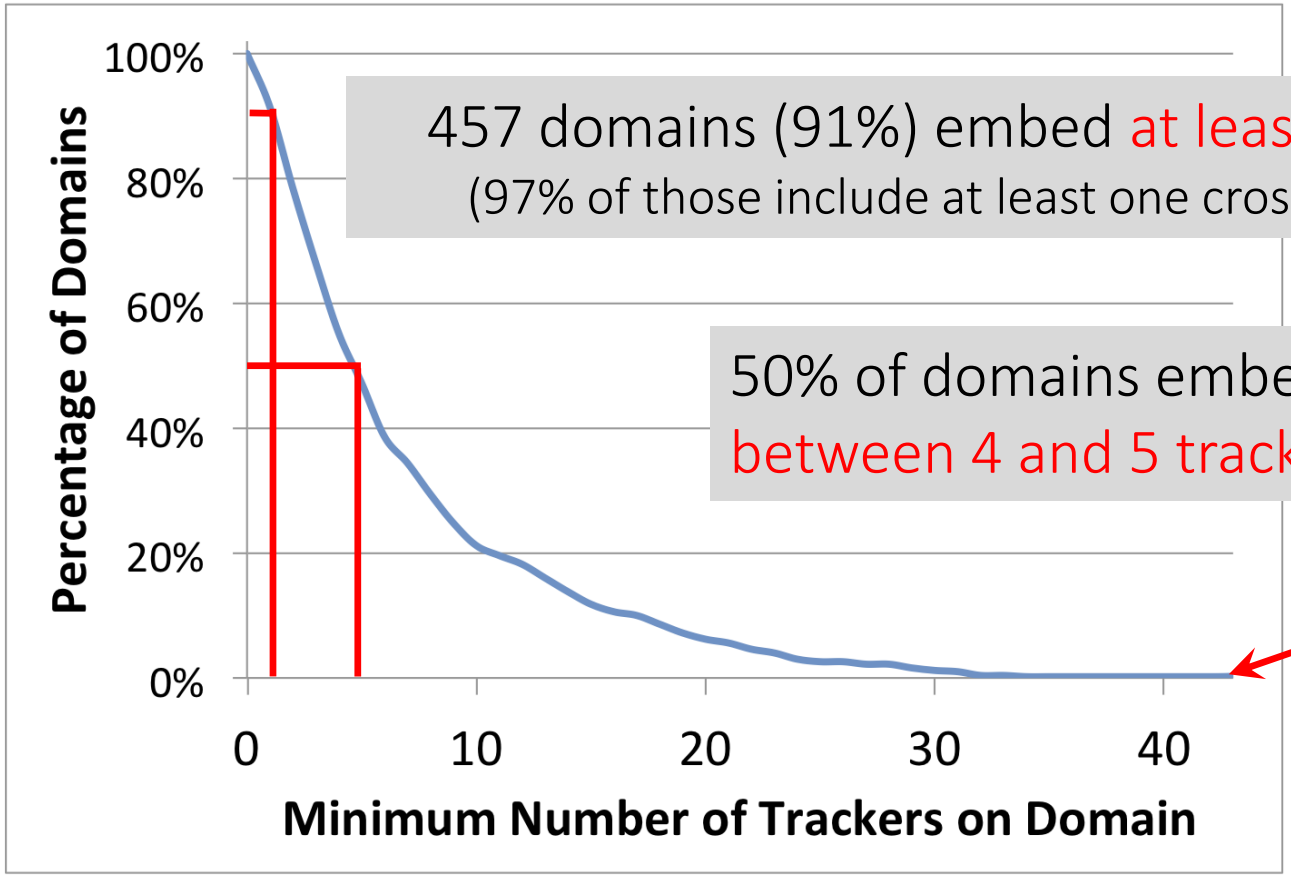
Measurement Study (2011)

- **Questions:**
  - How prevalent is tracking (of different types)?
  - How much of a user's browsing history is captured?
  - How effective are defenses?
- **Approach:** Build tool to automatically crawl web, detect and categorize trackers based on our taxonomy.

Longitudinal studies since then: tracking has increased and become more complex.

How prevalent is tracking?

524 unique trackers on Alexa top 500 websites (homepages + 4 links)

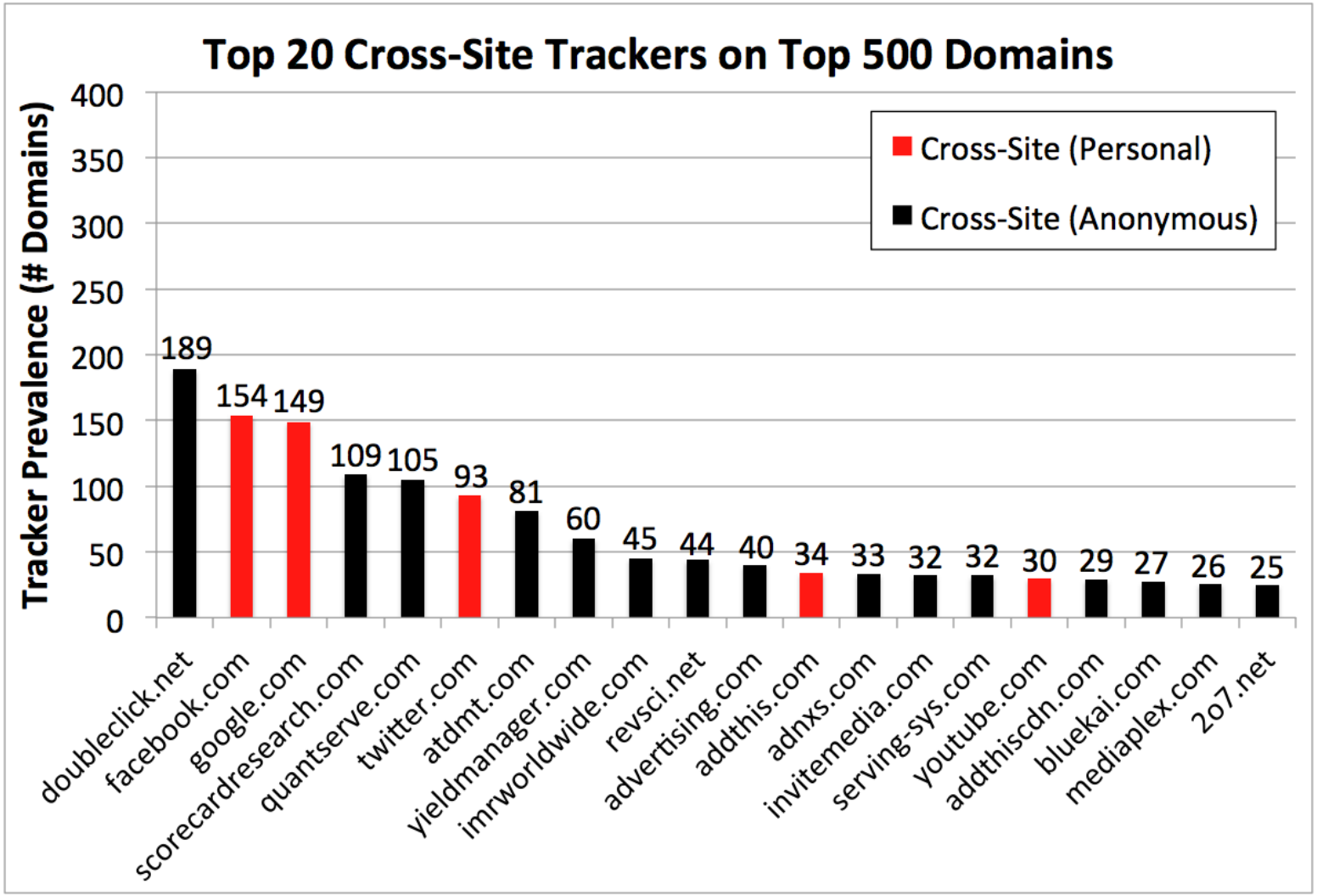


457 domains (91%) embed at least one tracker.
(97% of those include at least one cross-site tracker.)

50% of domains embed between 4 and 5 trackers.

One domain includes 43 trackers.

Who/what are the top trackers? (2011)



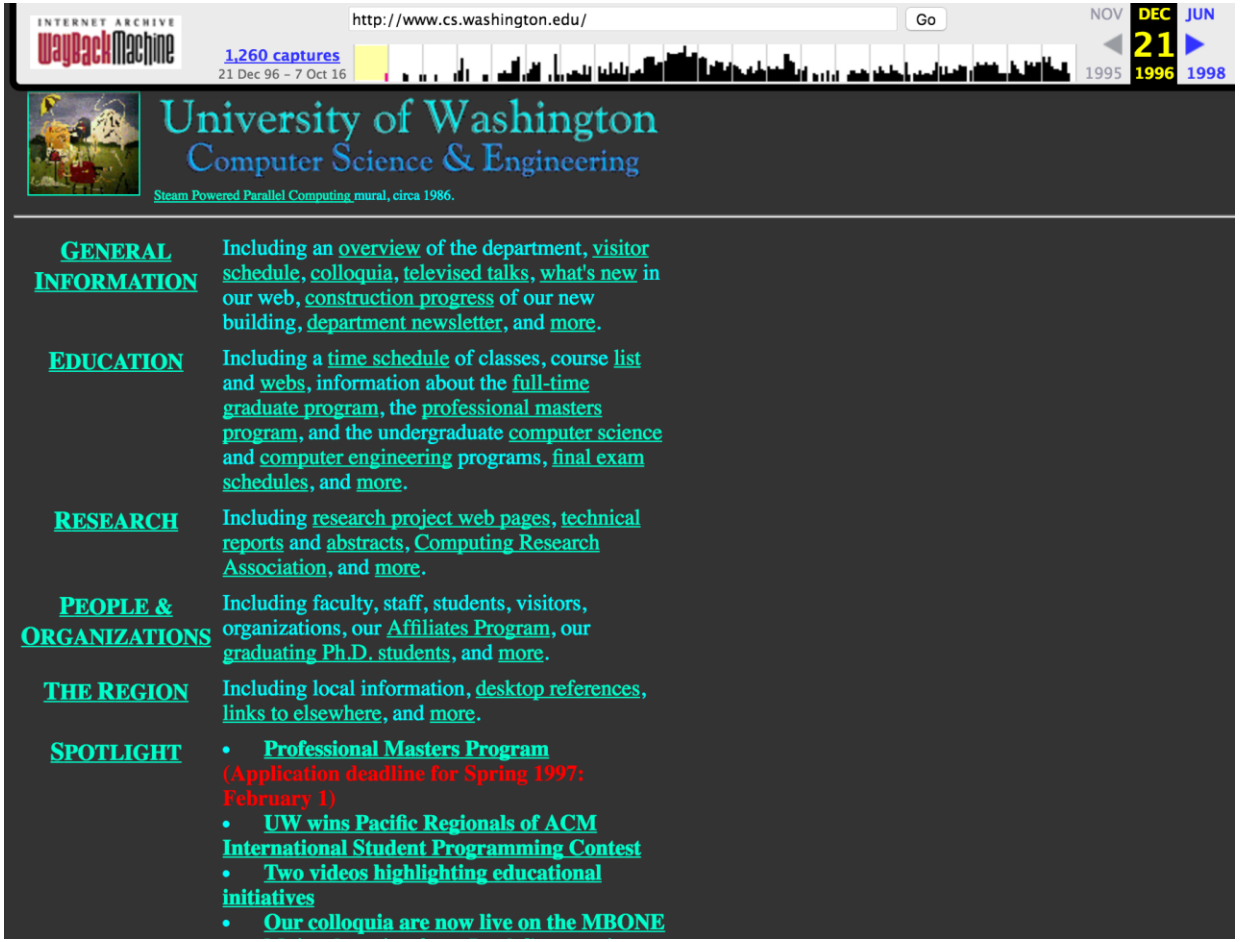
How has this changed over time?

- The web has existed for a while now…
  - What about tracking before 2011? (our first study)
  - What about tracking before 2009? (first academic study)

- Solution: time travel!

  [USENIX Security '16]

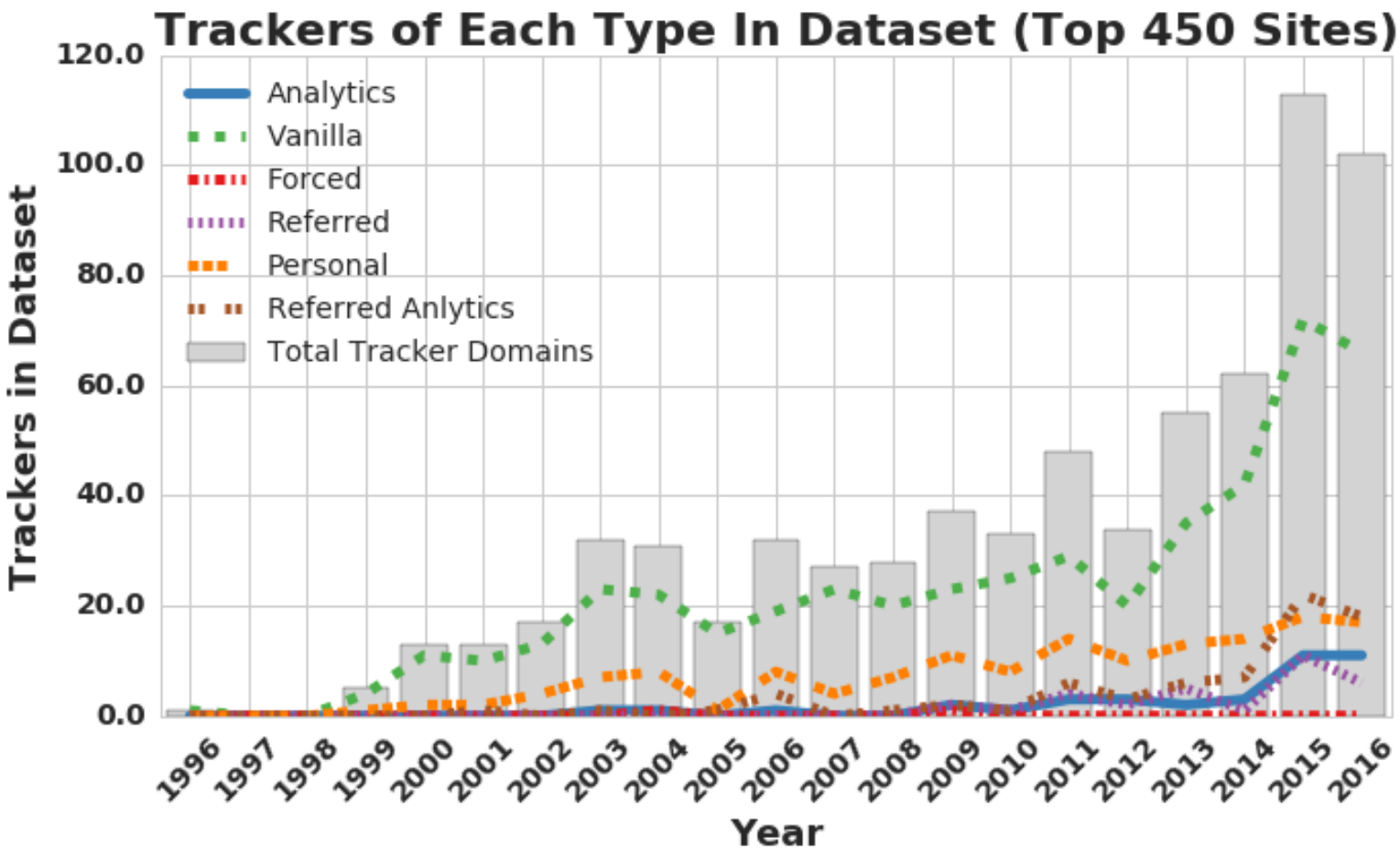
The Wayback Machine to the Rescue



Time travel for web tracking: http://trackingexcavator.cs.washington.edu

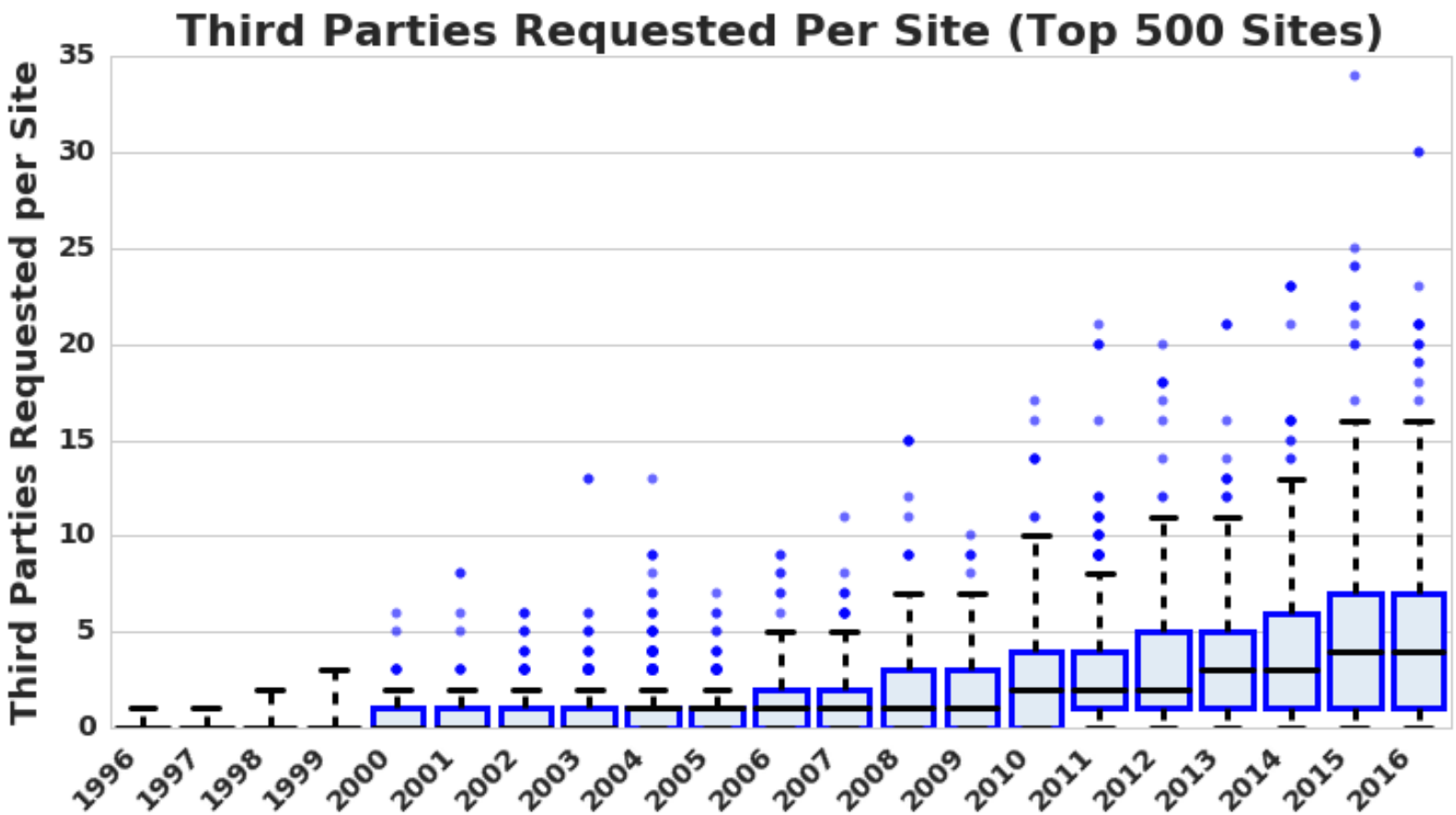
1996-2016: More & More Tracking

- More trackers of more types



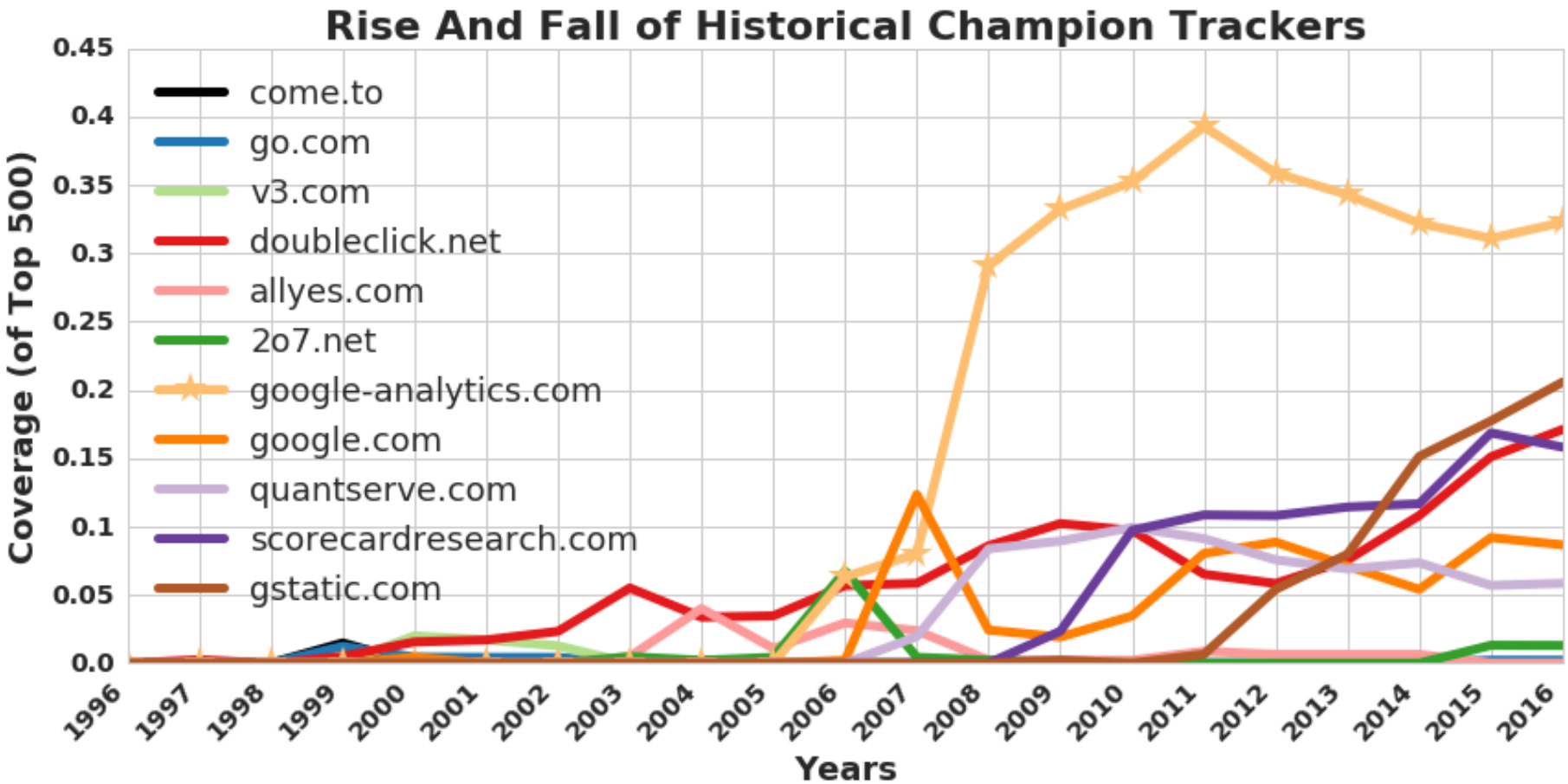
1996-2016: More & More Tracking

- More trackers of more types, more per site



1996-2016: More & More Tracking

- More trackers of more types, more per site, more coverage



ADINT (2017)

- Advertising for Intelligence Gathering
- Adversary can buy ads and use analytics from those ads to learn information about targets
  - Some ad networks provide location-based ad services
- Purchaser of ads can figure out
  - What mobile phone applications are in use in individual homes
  - A target's movements through the physical world (e.g., stores, doctors offices, etc)

Side Channels

Side Channel Attacks

- Attacks based on information that can be gleaned from the physical implementation of a system, rather than breaking its theoretical properties
  - Most commonly discussed in the context of cryptosystems
  - But also prevalent in many contexts
    - E.g., we discussed browser fingerprinting
    - E.g., we discussed history sniffing
    - E.g., we also discussed the TENEX password verification system

Examples (on Cryptosystems)

- Timing attacks
- Power analysis

- Good overview: http://www.nicolascourtois.com/papers/sc/sidech_attacks.pdf

If you do something different for secret key bits 1 vs. 0, attacker can learn something…

Example Timing Attacks

- RSA: Leverage key-dependent timings of modular exponentiations
  - https://www.rambus.com/timing-attacks-on-implementations-of-diffie-hellman-rsa-dss-and-other-systems/ -- seminal paper
  - http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf -- timing attacks on the Web

- Block Ciphers: Leverage key-dependent cache hits/misses

Power Analysis

- Simple power analysis: Directly read off bits from powerline traces
- Differential power analysis: Look for statistical differences in power traces, based on guesses of a key bit

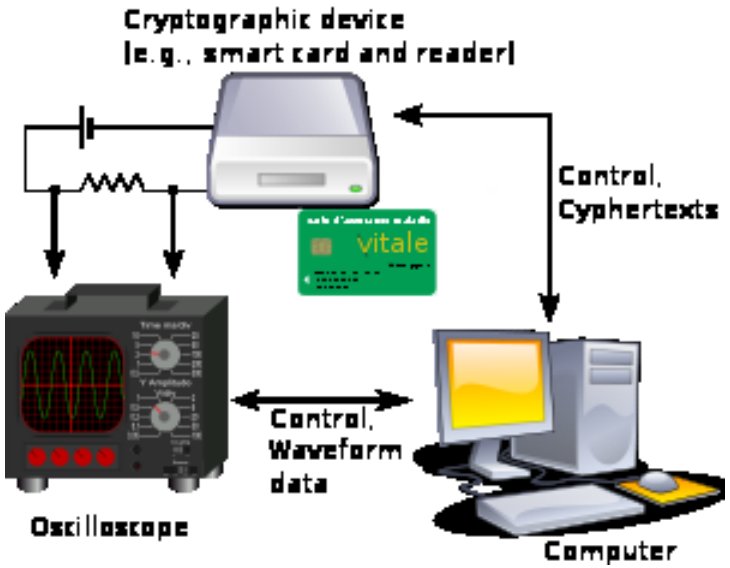
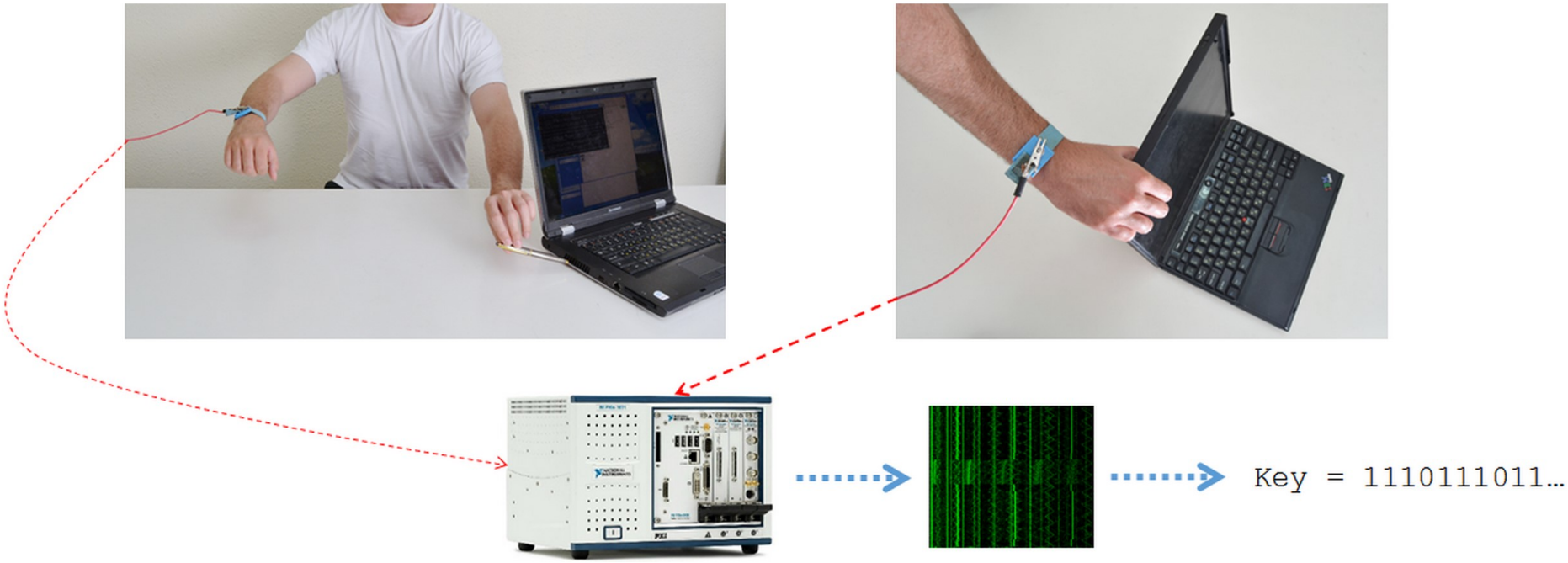


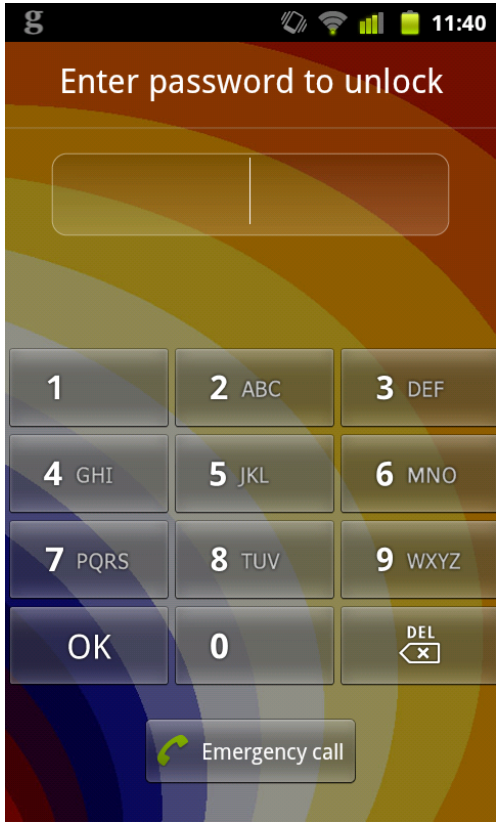
Image from https://en.wikipedia.org/wiki/Power_analysis

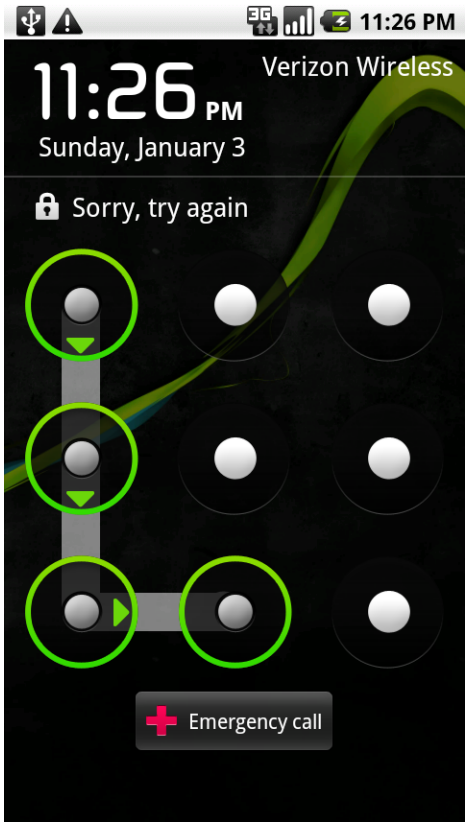
Key Extraction via Electric Potential



Genkin et al. “Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks On PCs” CHES 2014

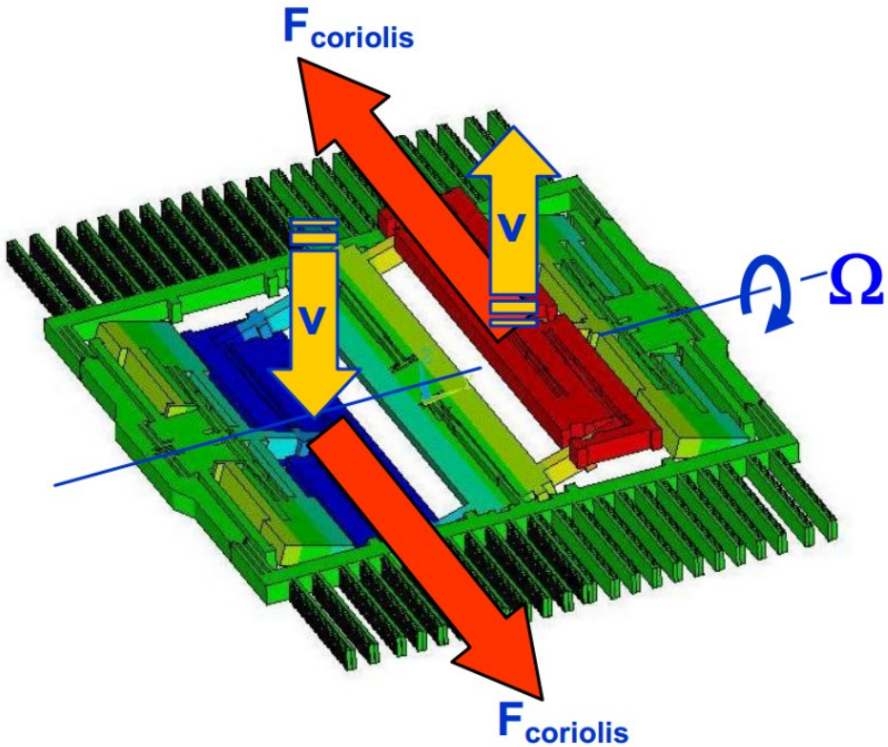
Accelerometer Eavesdropping





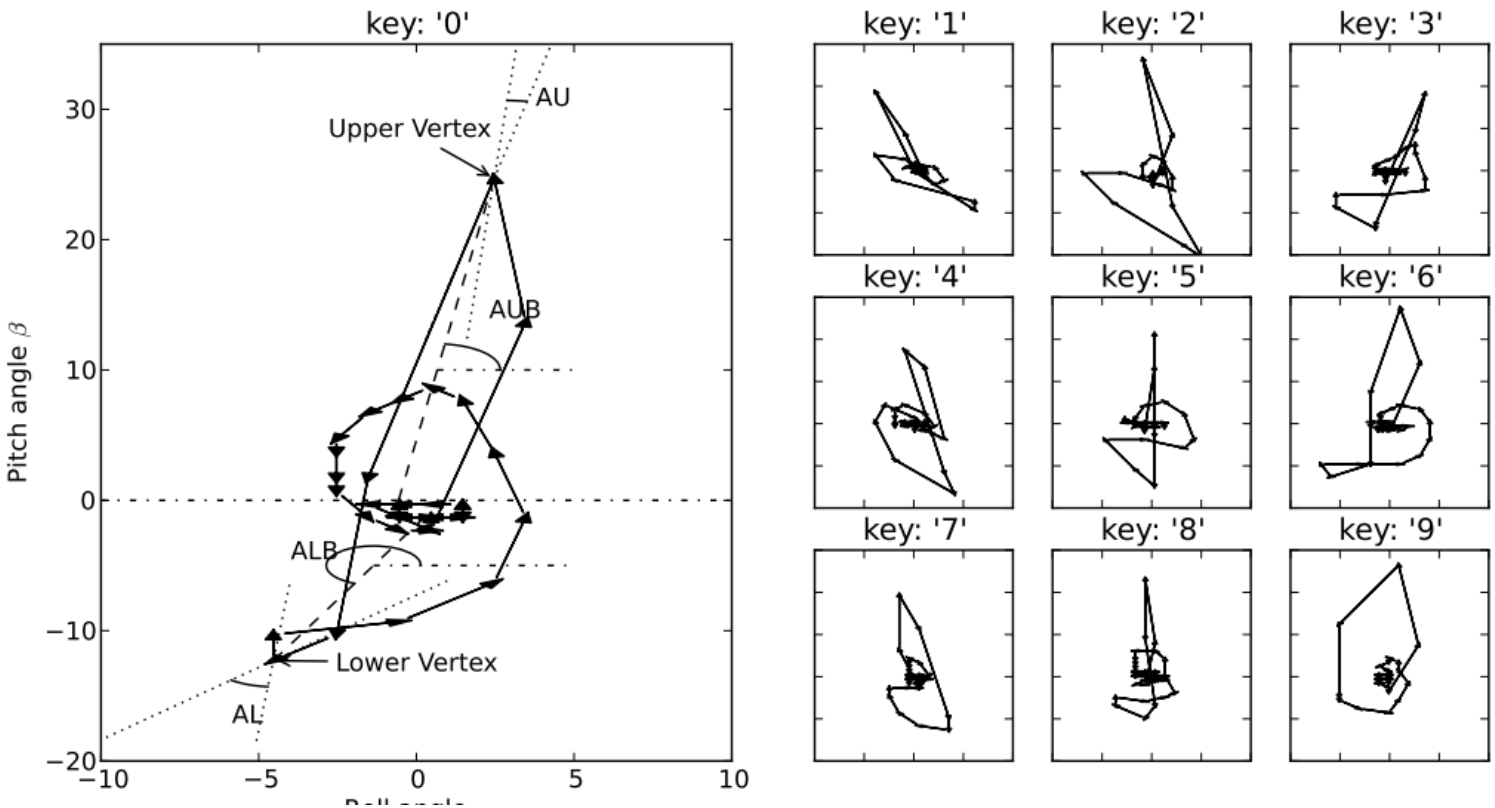
Aviv et al. "Practicality of Accelerometer Side Channels on Smartphones" ACSAC 2012

Gyroscope Eavesdropping



Michalevsky et al. "Gyrophone: Recognizing Speech from Gyroscope Signals" USENIX Security 2014

More Gyroscope



Chen et al. "TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion" HotSec 2011

Keyboard Eavesdropping

Zhuang et al. “Keyboard Acoustic Emanations Revisited” CCS 2005
Vuagnoux et al. “Compromising Electromagnetic Emanations of Wired and Wireless Keyboards” USENIX Security 2009