CSE 484 / CSE M 584

Computer Security: Web Security

TA: Franzi Roesner

franzi@cs.washington.edu

Logistics

- Homework #3 out today, due March 8.
- Lab #3 out SOON.

- Today:
  - Finish web tracking.
  - Wireshark demo (helps with lab #3).
  - Authentication grab bag.
- Next week (3/7): Android security
- Week after (3/14): Last section, final review.

Final Words on Web Tracking

Our Tracking Taxonomy

Name	Scope	User Visits Directly?	Overview
N/A	Within-Site	Yes	Site does its own on-site analytics.
Analytics	Within-Site	No	Site uses third-party analytics engine (e.g., Google Analytics).
Vanilla	Cross-Site	No	Site embeds third-party tracker that uses third-party storage (e.g., Doubleclick).
Forced	Cross-Site	Yes (forced)	Site embeds third-party tracker that forced the user to visit directly (e.g., via popup).
Referred	Cross-Site	No	Tracker relies on another cross-site tracker to leak unique identifier values.
Personal	Cross-Site	Yes	Site embeds third-party tracker that the user otherwise visits directly (e.g., Facebook).

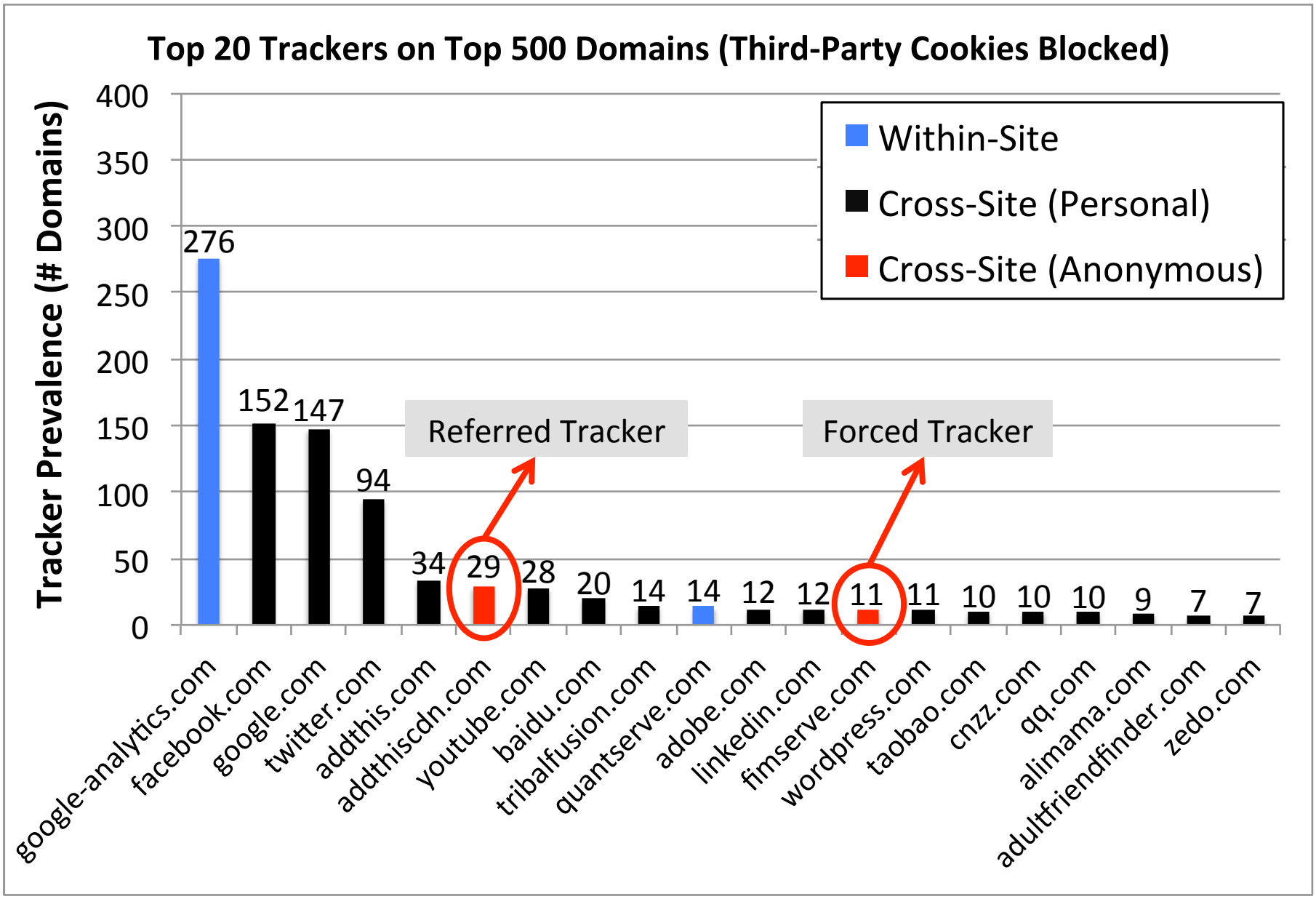
Evolution: Embedding analytics libraries

Evolution: Third-party cookie blocking

Evolution: Complex ad networks

Evolution: Social networks

Anonymous


Top 20 Trackers on Top 500 Domains (Third-Party Cookies Blocked)
Tracker Prevalence (# Domains)
400
350
300
250
200
150
100
50
0
Within-Site
Cross-Site (Personal)
Cross-Site (Anonymous)
276
152
147
94
34
29
28
20
14
14
12
12
11
11
10
10
10
9
7
7
Referred Tracker
Forced Tracker
google-analytics.com
facebook.com
google.com
twitter.com
addthis.com
addthiscdn.com
youtube.com
baidu.com
tribalfusion.com
quantserve.com
adobe.com
linkedin.com
fimserve.com
wordpress.com
taobao.com
cnzz.com
qq.com
alimama.com
adultfriendfinder.com
zedo.com

Personal Tracking Revisited

- Not anonymous!
- Most popular, based on measurements:

  Facebook, Google, Twitter, AddThis, YouTube, LinkedIn, Digg, Stumbleupon
- No good defenses:
  - Third-party cookie blocking is ineffective.
  - Existing browser extension solutions remove the buttons (undesirable to some users).
- Can we reduce tracking but allow use?

ShareMeNot

http://sharemenot.cs.washington.edu

- A browser extension that protects against tracking from third-party social media buttons while still allowing them to be used.
- For Firefox and Chrome.
- Two modes:
  1. Remove cookies from relevant requests until user clicks button.
  2. Replace buttons with local stand-in button until user click.

Effectiveness of ShareMeNot (Top 500)

Tracker	Without ShareMeNot	With ShareMeNot
Facebook	154	9
Google	149	15
Twitter	93	0
AddThis	34	0
YouTube	30	0
LinkedIn	22	0
Digg	8	0
Stumbleupon	6	0

Back to General Web Security

Broadcast Nature of WiFi

- Anyone can eavesdrop on wireless communications.
  - Even on some secured networks (e.g., secured with WEP) if eavesdropper is also on network.
- Firesheep: one-click session hijacking
  - http://codebutler.github.com/firesheep/
- Solution: end-to-end encryption (SSL/TLS)

Wireshark

- Free & open-source network packet analyzer.
- http://www.wireshark.org/
- Demo
  - Capturing packets
  - Filtering packets
  - Inspecting packets
    - GET vs. POST
    - HTTP vs. HTTPS

Authentication

Measuring Password Strength

- How many possible passwords are there?
- How many passwords are likely to be chosen?
- How long will it take to guess?

- Bits of entropy: $\log_2$(# of guesses)

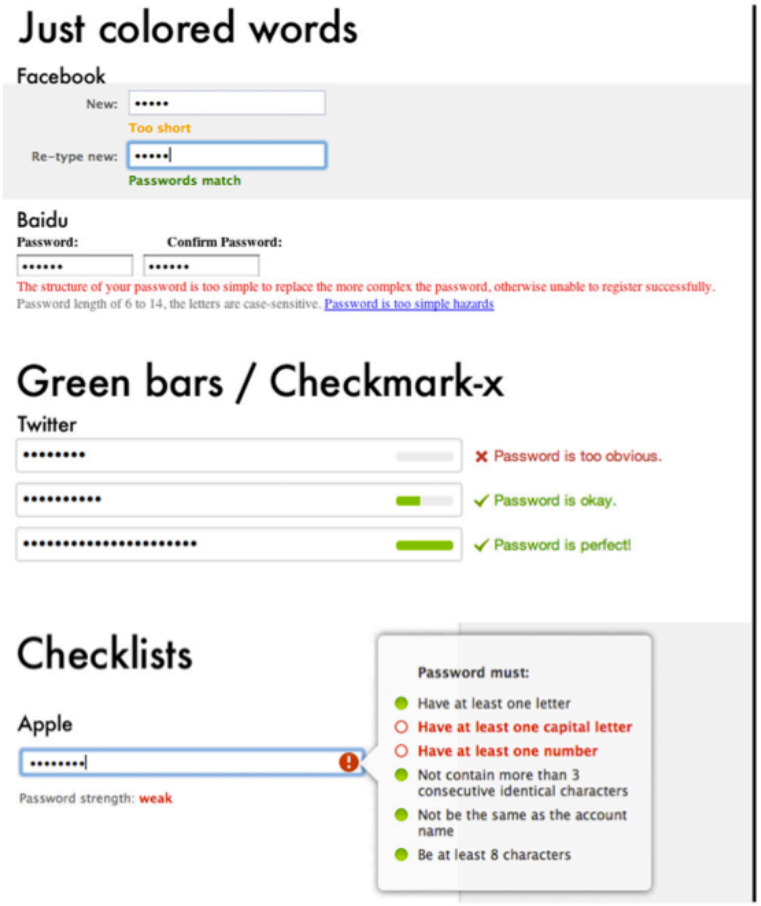
  Example: password of 10 bits chosen randomly

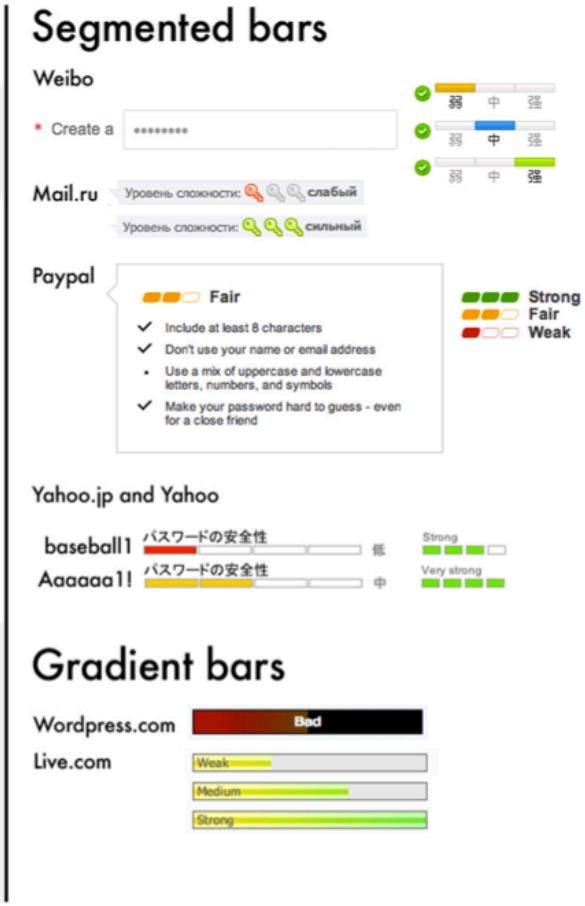
  Possible passwords = 2^10

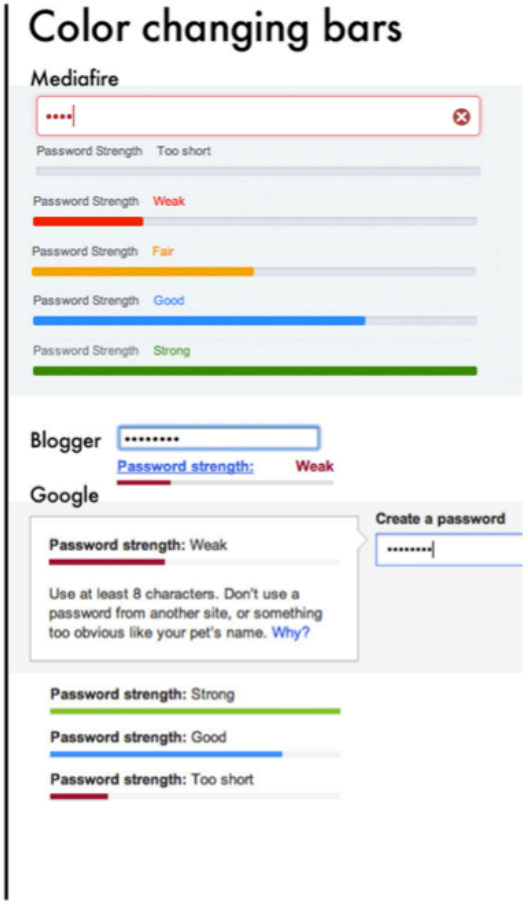
  Bits of entropy = $\log_2$(2^10) = 10

Additional bit of entropy doubles number of guesses needed.

Password Meters







[From "How does your password measure up? The Effect of Strength Meters on Password Creation", Ur et al., USENIX Security 2012]

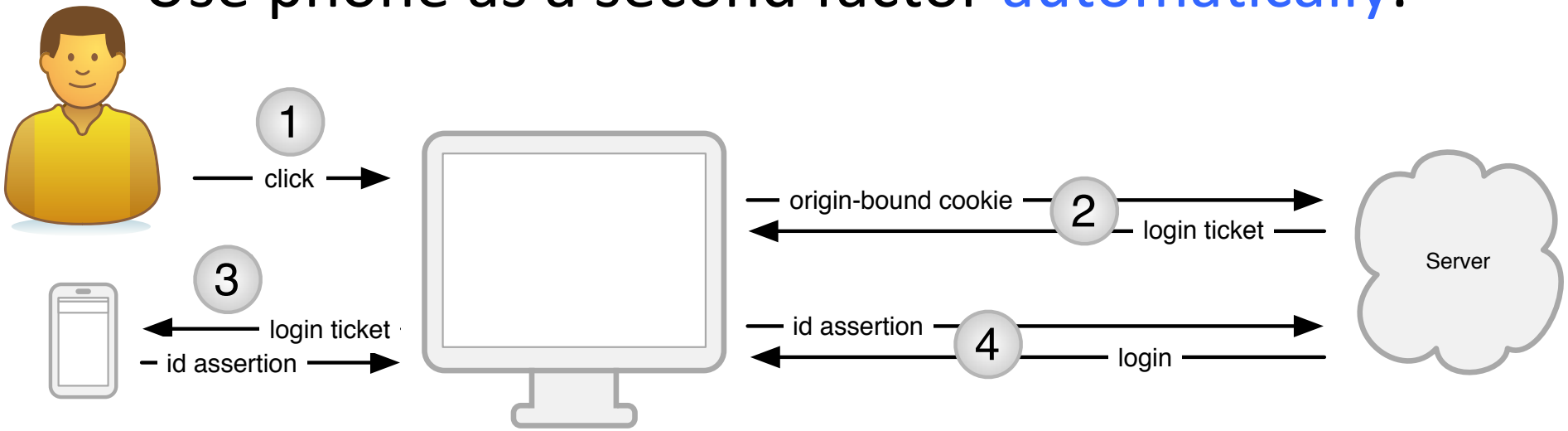
Password Meters

- Meters lead to longer passwords.
- Are passwords harder to guess?
  - Visual feedback alone has no effect.
  - More stringent meters do lead to stronger passwords.
- Meters lead to people taking longer to create passwords, and change their mind during creation.
- Meters don't affect memorability.

[From "How does your password measure up? The Effect of Strength Meters on Password Creation", Ur et al., USENIX Security 2012]

Usable Two-Factor Authentication

- Use phone as a second factor automatically.



- What if phone is not present?
  - Server can treat login session differently (e.g., don't allow transactions above a threshold $ amount).

[From "Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions", Czeskis et al., CCS 2012]