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

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>User Visits Directly?</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Within-Site</td>
<td>Yes</td>
<td>Site does its own on-site analytics.</td>
</tr>
<tr>
<td><strong>Evolution: Embedding analytics libraries</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics</td>
<td>Within-Site</td>
<td>No</td>
<td>Site uses third-party analytics engine (e.g., Google Analytics).</td>
</tr>
<tr>
<td><strong>Evolution: Third-party cookie blocking</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vanilla</td>
<td>Cross-Site</td>
<td>No</td>
<td>Site embeds third-party tracker that uses third-party storage (e.g., Doubleclick).</td>
</tr>
<tr>
<td><strong>Evolution: Complex ad networks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forced</td>
<td>Cross-Site</td>
<td>Yes (forced)</td>
<td>Site embeds third-party tracker that forced the user to visit directly (e.g., via popup).</td>
</tr>
<tr>
<td><strong>Anonymous</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Referred</td>
<td>Cross-Site</td>
<td>No</td>
<td>Tracker relies on another cross-site tracker to leak unique identifier values.</td>
</tr>
<tr>
<td><strong>Evolution: Social networks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal</td>
<td>Cross-Site</td>
<td>Yes</td>
<td>Site embeds third-party tracker that the user otherwise visits directly (e.g., Facebook).</td>
</tr>
</tbody>
</table>
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)

<table>
<thead>
<tr>
<th>Tracker</th>
<th>Without ShareMeNot</th>
<th>With ShareMeNot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>154</td>
<td>9</td>
</tr>
<tr>
<td>Google</td>
<td>149</td>
<td>15</td>
</tr>
<tr>
<td>Twitter</td>
<td>93</td>
<td>0</td>
</tr>
<tr>
<td>AddThis</td>
<td>34</td>
<td>0</td>
</tr>
<tr>
<td>YouTube</td>
<td>30</td>
<td>0</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>Digg</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Stumbleupon</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>
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: $\log_2(\# \text{ of guesses})$

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]