Admin

- Lab 3 out soon™
- Homework 2 grades out
  - https://forms.gle/C2RJNaTGv2N1dF197
Importance of Usability in Security

• Why is usability important?
  • People are the critical element of any computer system
    • People are the reason computers exist in the first place
  • Even if it is possible for a system to protect against an adversary, people may use the system in other, less secure ways
Usable Security Roadmap

• 3 case studies
  • HTTPS indicators + SSL warnings
  • Phishing
  • Password managers

• Step back: root causes of usability problems, and how to address
Case Study #1: Browser HTTPS Indicators

- **Design question 1:** How to indicate encrypted connections to users?
- **Design question 2:** How to alert the user if a site’s SSL certificate is untrusted?
  - You discussed this in section a couple weeks ago
The Lock Icon

- Goal: identify secure connection
  - SSL/TLS is being used between client and server to protect against active network attacker

- Lock icon should only be shown when the page is secure against network attacker
  - Semantics subtle and not widely understood by users
  - Whose certificate is it??
  - Problem in user interface design
Will You Notice?

Clever favicon inserted by network attacker
Do These Indicators Help? (2007)

- “The Emperor’s New Security Indicators”

### Lesson:

Users don’t notice the **absence** of indicators!

<table>
<thead>
<tr>
<th>Score</th>
<th>First chose not to enter password...</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>upon noticing HTTPS absent</td>
<td>0 0%</td>
</tr>
<tr>
<td>1</td>
<td>after site-authentication image removed</td>
<td>0 0%</td>
</tr>
<tr>
<td>2</td>
<td>after warning page</td>
<td>8 47%</td>
</tr>
<tr>
<td>3</td>
<td>never (always logged in)</td>
<td>10 53%</td>
</tr>
</tbody>
</table>

**Total**: 18 17 22 35 57
Newer Versions of Chrome

c. 2017

Secure | https://mail.google.com/mail/u/0/#inbox

2020

mail.google.com/mail/u/0/#inbox

Not Secure | http-password.badssl.com
Case Study #1: Browser HTTPS Indicators

- **Design question 1:** How to indicate encrypted connections to users?
- **Design question 2:** How to alert the user if a site’s SSL certificate is untrusted?
  - You discussed this in section a couple weeks ago
  - Recall: Opinionated design
Challenge: Meaningful Warnings

See current designs for different conditions at [https://badssl.com/](https://badssl.com/).
Case Study #2: Phishing

• **Design question:** How do you help users avoid falling for phishing sites?
A Typical Phishing Page

Weird URL
http instead of https
Safe to Type Your Password?
Safe to Type Your Password?

Bank of the West

Gives me your password!

User name: 

Password: 

Login
Safe to Type Your Password?
Safe to Type Your Password?

“Picture-in-picture attacks”

Trained users are more likely to fall victim to this!
Phishing Warnings (2008)
Active vs. Passive Warnings

- Active warnings significantly more effective
  - Passive (IE): 100% clicked, 90% phished
  - Active (IE): 95% clicked, 45% phished
  - Active (Firefox): 100% clicked, 0% phished
If you don’t recognize your personalized “SiteKey”, don’t enter your Passcode.
Case Study #3: Password Managers

• **Password managers** handle creating and “remembering” strong passwords

• Potentially:
  • Easier for users
  • More secure

• Early examples:
  • PwdHash (Usenix Security 2005)
  • Password Multiplier (WWW 2005)
**PwdHash**

@@ in front of passwords to protect; or F2

\[
\text{sitePwd} = \text{Hash}(\text{pwd}, \text{domain})
\]

Prevent phishing attacks

**Password Multiplier**

Activate with Alt-P or double-click

\[
\text{sitePwd} = \text{Hash}(\text{username}, \text{pwd}, \text{domain})
\]

Both solutions target simplicity and transparency.
Usability Testing

• Are these programs usable? If not, what are the problems?

• Approaches for evaluating usability:
  • **Usability inspection** (no users)
    • Cognitive walkthroughs
    • Heuristic evaluation
  • **User study**
    • Controlled experiments
    • Real usage
## Task Completion Results

<table>
<thead>
<tr>
<th>Success</th>
<th>Potentially Causing Security Exposures</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dangerous Success</td>
<td>Failures</td>
<td>False Completion</td>
<td>Failed due to Previous</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PwdHash</td>
<td>Log In</td>
<td>48%</td>
<td>44%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Migrate Pwd</td>
<td>42%</td>
<td>35%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td></td>
<td>Remote Login</td>
<td>27%</td>
<td>42%</td>
<td>31%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Update Pwd</td>
<td>19%</td>
<td>65%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td></td>
<td>Second Login</td>
<td>52%</td>
<td>28%</td>
<td>4%</td>
<td>0%</td>
</tr>
<tr>
<td>Password Multiplier</td>
<td>Log In</td>
<td>48%</td>
<td>44%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Migrate Pwd</td>
<td>16%</td>
<td>32%</td>
<td>28%</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td>Remote Login</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Update Pwd</td>
<td>16%</td>
<td>4%</td>
<td>44%</td>
<td>28%</td>
</tr>
<tr>
<td></td>
<td>Second Login</td>
<td>16%</td>
<td>4%</td>
<td>16%</td>
<td>0%</td>
</tr>
</tbody>
</table>

[Chiasson, van Oorschot, Biddle]
Problem: Mental Model

- Users seemed to have misaligned mental models
  - Not understand that one needs to put “@@” before each password to be protected.
  - Think different passwords generated for each session.
  - Think successful when were not.
  - Not know to click in field before Alt-P.
  - Don’t understand what’s happening: “Really, I don’t see how my password is safer because of two @’s in front”
Problem: Transparency

• **Unclear** to users whether actions successful or not.
  • Should be obvious when plugin activated.
  • Should be obvious when password protected.

• Users feel that they **should** be able to **know** their own password.
Problem: Dangerous Errors

• Tendency to **try all passwords**
  • A poor security choice – phishing site could collect many passwords!
  • **May make** the use of PwdHash or Password Multiplier *worse* than not using any password manager.

• **Usability problem leads to security vulnerabilities.**
  • Theme in course: sometimes things designed to increase security can also increase other risks
Root Causes? How to Improve?
Stepping Back: Root Causes?

• Computer systems are complex; users lack intuition
• Users in charge of managing own devices
  • Unlike other complex systems, like healthcare or cars.
• Hard to gauge risks
  • “It won’t happen to me!”
• Annoying, awkward, difficult
• Social issues
  • Send encrypted emails about lunch?...
How to Improve?

• Security education and training
• Help users build accurate mental models
• Make security invisible
• Make security the least-resistance path
• ...?
Beyond Specific Tools: Different User Groups

• Not all users are the same!

• Designing for one group of users, or “generic” users, may lead to dangerous failures or reasons that people will not use security tools.

• Examples from (qualitative) research at UW:
  • Journalists (most sources are not like Snowden!)
  • Refugees in US (security measures may embed US cultural assumptions!)
Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Click-through rates and sample size for conditions.
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td>67.9%</td>
<td>17,479</td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Click-through rates and sample size for conditions.

Figure 1. The default Chrome SSL warning (Condition 1).
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td>67.9%</td>
<td>17,479</td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td>68.9%</td>
<td>17,977</td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td>66.5%</td>
<td>18,049</td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td>68.8%</td>
<td>18,084</td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Click-through rates and sample size for conditions.

Figure 1. The default Chrome SSL warning (Condition 1).

Figure 4. The three images used in Conditions 2-4.
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td>67.9%</td>
<td>17,479</td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td>68.9%</td>
<td>17,977</td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td>66.5%</td>
<td>18,049</td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td>68.8%</td>
<td>18,084</td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td>56.1%</td>
<td>20,023</td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td>55.9%</td>
<td>19,297</td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Click-through rates and sample size for conditions.

![Mock Firefox SSL warning](image)

Figure 2. The mock Firefox SSL warning (Condition 5).
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td>67.9%</td>
<td>17,479</td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td>68.9%</td>
<td>17,977</td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td>66.5%</td>
<td>18,049</td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td>68.8%</td>
<td>18,084</td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td>56.1%</td>
<td>20,023</td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td>55.9%</td>
<td>19,297</td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td>55.8%</td>
<td>19,845</td>
</tr>
</tbody>
</table>

Table 1. Click-through rates and sample size for conditions.

[Figure 3. The Firefox SSL warning with Google styling (Condition 7).]

[Felt et al.]
Opinionated Design Helps!

![The site's security certificate is not trusted!]

Adherence  | N
------------|---
30.9%       | 4,551
Opinionated Design Helps!

[Image: Security certificate warning]

<table>
<thead>
<tr>
<th>Adherence</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.9%</td>
<td>4,551</td>
</tr>
<tr>
<td>32.1%</td>
<td>4,075</td>
</tr>
<tr>
<td>58.3%</td>
<td>4,644</td>
</tr>
</tbody>
</table>
Today’s Warning

Your connection is not private

Attackers might be trying to steal your information from untrusted-root.badssl.com
(for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_INVALID

☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Advanced

Reload
Which warning is ‘better’?

• For user security?
• For user agency?
• For user understanding?
• For... what?