CSE 484 / CSE M 584: Computer Security and Privacy

Usable Security

Spring 2020

Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
Admin

• Lab 2 due on Friday
• Homework 3 out, due May 29
• There will be a Lab 3 (it is easier than 1+2)
  – Smart home security, preview in Section this week
• This week’s lectures:
  – Usable security
  – Mobile platform security
  – Anonymity
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

• 2 case studies
  – HTTPS indicators + SSL warnings
  – Phishing

• 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?
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”

<table>
<thead>
<tr>
<th>Score</th>
<th>First chose not to enter password...</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>$1 \cup 2$</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>upon noticing HTTPS absent</td>
<td>0 0%</td>
<td>0 0%</td>
<td>0 0%</td>
<td>0 0%</td>
<td>0 0%</td>
</tr>
<tr>
<td>1</td>
<td>after site-authentication image removed</td>
<td>0 0%</td>
<td>0 0%</td>
<td>2 9%</td>
<td>0 0%</td>
<td>2 4%</td>
</tr>
<tr>
<td>2</td>
<td>after warning page</td>
<td>8 47%</td>
<td>5 29%</td>
<td>12 55%</td>
<td>13 37%</td>
<td>25 44%</td>
</tr>
<tr>
<td>3</td>
<td>never (always logged in)</td>
<td>10 53%</td>
<td>12 71%</td>
<td>8 36%</td>
<td>22 63%</td>
<td>30 53%</td>
</tr>
</tbody>
</table>

**Lesson:**

Users don’t notice the absence of indicators!
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 #2: 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?
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.

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).
Opinionated Design Helps!

The site's security certificate is not trusted!

You attempted to reach 192.168.17.129, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, especially if you have never seen this warning before for this site.

<table>
<thead>
<tr>
<th>Adherence</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.9%</td>
<td>4,551</td>
</tr>
</tbody>
</table>
Opinionated Design Helps!

Adherence

<table>
<thead>
<tr>
<th></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>

[Felt et al.]
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
Challenge: Meaningful Warnings

See current designs for different conditions at 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 you pa55w0rds!

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)

Passive (IE)

Active (IE)

Active (Firefox)
Are Phishing Warnings Effective?

- CMU study of 60 users
- Asked to make eBay and Amazon purchases
- All were sent phishing messages in addition to the real purchase confirmations
- **Goal:** compare active and passive warnings

[Egelman et al.]
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
Active vs. Passive Warnings

• Some fail to notice warnings entirely
  – Passive warning takes a couple of seconds to appear; if user starts typing, his keystrokes dismiss the warning

• Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings... repeated 4-5 times
  – Conclusion: “website is not working”
  – Users never bothered to read the warnings, but were still prevented from visiting the phishing site
  – Active warnings work!
Why Warnings Fail

• Don’t trust the warning
  – “Since it gave me the option of still proceeding to the website, I figured it couldn’t be that bad”

• Ignore warning because it’s familiar (IE users)
  – “Oh, I always ignore those”
  – “Looked like warnings I see at work which I know to ignore”
  – “I thought that the warnings were some usual ones displayed by IE”
  – “My own PC constantly bombards me with similar messages”

• Common issue: Warning/prompt fatigue
  – We’ll see this issue again re: mobile security...
FYI: Site Authentication Image

If you don’t recognize your personalized “SiteKey”, don’t enter your Passcode.
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!)