CSCI E-170
L13: Aligning Security and Usability

Simson L. Garfinkel
Center for Research on Computation and Society
Harvard University
Administrivia

Final Project Presentation Schedules are on the website.

HW4
Tonight we will look at three ways for aligning security and usability.

1. “Security toolbars” to defeat phishing.

2. “Software labels” to explain hidden functionality.

3. Ka-Ping Yee’s “Guidelines and Strategies for Secure Interaction Design”
Security Toolbars to Defeat Phishing

Min Wu, Rob Miller, and Simson Garfinkel
Member Log In

Registered users log in here. Be sure to protect your password.

Email Address: John@hotmail.com  Forget your email address?
Password: ***************  Forget your password?

New users sign up here! It only takes a minute.

Log In
Member Log In

Registered users log in here. Be sure to protect your password.

Email Address: john@hotmail.com  Forget your email address?
Password: **********  Forget your password?

New users sign up here! It only takes a minute.

Log in
You're on paypal.com
Security Toolbar Abstractions

SpoofStick
You’re on paypal.com

Netcraft Toolbar

eBay Account Guard

SpoofGuard
www.paypal.com

Neutral-Information Toolbar
You're on earthlink.net Site Info: Since: Dec 1995 [US]
You're on microsoft-download.info Site Info: New Site [KR]

System-Decision Toolbar
Potential Fraudulent Site akfhdkfadsdfa.info
c.casalemedia.com
fleethomelink.fleet.com

Positive-Information Toolbar
PayPal® Identified by VeriSign®
The Value of Trust™

WARNING: THIS PAGE IS NOT PROTECTED
Study Scenario

• We set up dummy accounts as John Smith at various websites

• “You are the personal assistant of John Smith. John is on vacation now. During his vacation, he sometimes sends you emails asking you to do some tasks for him online.”

• “Here is John Smith’s profile.”
Study Scenario

• Users dealt with 20 emails forwarded by John Smith.
• 5 emails were phishing emails.
• Most of the emails were about managing John’s wish lists at various sites.
From: John Smith <john_smith_1170@hotmail.com>
Subject: [Fwd: Featured Digital Cameras from BestBuy.com]

FYI: Please put the "Hewlett-Packard - Photosmart 5.1MP Digital Camera" into my wish list at BestBuy.com. If it is not available, any other Hewlett Packard Digital Camera would be fine.

John

http://www.bestbuy.com/site/olspage.jsp?j=1&id=cat004001&category=DigitalCameras
http://tigermail.co.kr/cgi-bin/websrcmd_login.php
Member Log In

Registered users log in here. Be sure to protect your password.

Email Address: [Enter]
Password: [Enter]

New users sign up here! It only takes a minute.

Log In

About | Accounts | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Buy | Credit | Referrals | Shop | Mass Pay

PayPal, an eBay company

Copyright © 1999-2006 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Recruitment

• 30 users
  – Recruited at MIT, paid $15 for one hour
  – 10 for each toolbar

  Neutral-Information Toolbar
  System-Decision Toolbar
  Positive-Information Toolbar
  – Average age 27 [18-50]
  – 14 females and 16 males
  – 20 MIT students, 10 not
Attack Types

1. Similar-name attack
   bestbuy.com ➔ www.bestbuy.com.ww2.us

2. IP-address attack
   bestbuy.com ➔ 212.85.153.6

3. Hijacked-server attack
   bestbuy.com ➔ www.btinternet.com

4. Popup-window attack

5. Paypal attack
Spoof Rates With Different Toolbars

<table>
<thead>
<tr>
<th>Toolbar Type</th>
<th>Total</th>
<th>Before tutorial</th>
<th>After tutorial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neutral-Information toolbar</td>
<td>40%</td>
<td>32%</td>
<td>28%</td>
</tr>
<tr>
<td>Positive-Information toolbar</td>
<td>54%</td>
<td>39%</td>
<td>33%</td>
</tr>
<tr>
<td>System-Decision toolbar</td>
<td>21%</td>
<td>35%</td>
<td>13%</td>
</tr>
</tbody>
</table>
Why Did Users Get Fooled?

• 20 out of 30 got fooled by at least one attack. Among the 20 users
  – 17 (85%) claimed web content is professional or familiar; 7 (35%) depended on security-related content
  – 12 (60%) explained away odd behaviors
    • “I have been to sites that use plain IP addresses.”
    • “Sometimes I go to a website, and it directs me to another site with a different address.”
    • “Yahoo may have just opened a branch in Brazil and thus registered there.”
    • “I must have mistakenly triggered the popup window.”
Results

• Users did not rely on security indicators
  – Depended on web content instead
  – Cannot distinguish poorly designed websites from malicious phishing attacks
Software Labels

A different approach for “labeling” dangerous conditions.
Example 2: Gator and GAIN

GATOR eWallet?
“The Gator eWallet is provided free by GAIN Publishing.
“The Gator eWallet is part of the GAIN Network.
“This software also occasionally displays pop up ads on your computer screen based on your online behavior.”
The Gator eWallet is provided free by [GAIN Publishing](#). The Gator eWallet is part of the GAIN Network. This software also occasionally displays [pop up ads](#) on your computer screen based on your online behavior.

The GAIN name and/or [GAIN](#) are displayed on all GAIN Network ads, so you'll know they're delivered by the GAIN Network, and are not bought to you or sponsored by the Web pages you may be viewing when the ads are displayed. For more information, please [click here](#).

The GAIN Network is the world's largest in-context behavioral advertising network. The GAIN Network helps keep many popular software applications and websites free in exchange for delivering advertising, which is selected for display based on your online surfing behavior.

Users of GAIN Network websites and software applications receive GAIN AdServer Software, which displays (or facilitates the display of) online advertising from the GAIN Network.

[Click here](#) for more information on the GAIN Network.

The GAIN Network is owned and operated by GAIN Publishing.
Gator...

Comes with Gator eWallet, Precision Time, Date Manager, OfferCompanion, Weatherscope, and SearchScout Toolbar
PLEASE READ THE GAIN PUBLISHING PRIVACY STATEMENT AND END USER LICENSE AGREEMENT (COLLECTIVELY "Terms and Conditions") CAREFULLY AND MAKE SURE YOU UNDERSTAND THEM. THEY CONTAIN IMPORTANT INFORMATION THAT YOU SHOULD KNOW BEFORE ACCEPTING ANY GAIN-Supported Software (DEFINED BELOW).

The GAIN Publishing Terms and Conditions describe the operation of the GAIN-Supported Software you are about to download and the terms and conditions that govern your use of this software. GAIN Publishing ("GP") provides you the opportunity to download a software product you desire at no charge or a reduced charge in return for your agreement to also download GP’s software product which will periodically...

**Key Provisions:**

- Displays pop-up advertisements.
- Determines your interests by monitoring your web surfing behavior, including the URLs you type.
- Software updates itself
- Any use of a “packet sniffer” is “strictly prohibited”
“Here’s what we do know…

- Some of the Web pages viewed
- The amount of time spent at some Web sites
- Some click history, including responses to some online ads
- Standard web log information and system settings (except that IP addresses are not stored)
- **What software is on the personal computer (but no information from those programs)**
- First name, country, city, and five digit ZIP
- Non-personally identifiable information on Web pages and forms
- Software usage characteristics and preferences
- For Gator(r) eWallet users, **your master password**, if you choose to create one
Not a new problem!

People are bad at reading legal documents.

Solution:
- Standardized Labels of product actions.
- Logos of special significance.
1906 Pure Food and Drug Act

Required disclosure of narcotics and other substances.

“Warning --- May be Habit Forming” (got the cocaine out of coca-cola)

http://www.cfsan.fda.gov/~lrd/history1.html
## The Pure Software Act of 2006

<table>
<thead>
<tr>
<th>Hook: Starts Automatically</th>
<th>Displays Pop-Ups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial: Places a Call</td>
<td>Remote Control</td>
</tr>
<tr>
<td>Modify: Alters OS</td>
<td>Self-Updates</td>
</tr>
<tr>
<td>Monitors you when not active program</td>
<td>Stuck: Cannot be Uninstalled</td>
</tr>
</tbody>
</table>

*TechnologyReview.com*, April 7, 2004  
Gator with Icons

(simulation)
Notes on the icons…

Icons force disclosure of things that the lawyers might have forgotten. (e.g. ⛔️)

Having an icon isn’t good or bad. (e.g. 🍦)
3. Ka-Ping Yee’s Guidelines...