User Authentication
+
Other Human Aspects

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
Goals for Today

- User authentication
- Phishing
Password Managers

- Idea: Software application that will store and manage passwords for you.
  - You remember one password.
  - Each website sees a different password.
Key ideas

- User remembers a single password
- Password managers
  - On input: (1) the user’s single password and (2) information about the website
  - Compute: Strong, site-specific password
- Goal: Avoid problems with passwords
The problem

Alice needs passwords for all the websites that she visits
Possible solutions

- **Easy to remember**: Use same password on all websites. Use “weak” password.
  - Poor security (don’t share password between bank website and small website)

- **More secure**: Use different, strong passwords on all websites.
  - Hard to remember, unless write down.
Alternate solution: Password managers

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

- Potentially:
  - Easier for users
  - More secure

- Examples:
  - PwdHash (Usenix Security 2005)
  - Password Multiplier (WWW 2005)
Both solutions target simplicity and transparency.
Usenix 2006: Usability testing

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

- Two main approaches for evaluating usability:
  - Usability inspection (no users)
  - Cognitive walk throughs
  - Heuristic evaluation
  - User study
  - Controlled experiments

This paper stresses the need to observe real users.

HCI is important!
Study details

- **26 participants**, across various backgrounds (4 technical)
- Five assigned tasks per plugin
- Data collection
  - **Observational data** (recording task outcomes, difficulties, misconceptions)
  - **Questionnaire data** (initial attitudes, opinions after tasks, post questionnaires)
## Task completion results

<table>
<thead>
<tr>
<th>Success</th>
<th>Potentially Causing Security Exposures</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dangerous Success</td>
<td>Failures</td>
</tr>
<tr>
<td></td>
<td>Success</td>
<td>Failure</td>
</tr>
<tr>
<td>PwdHash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log In</td>
<td>48%</td>
<td>44%</td>
</tr>
<tr>
<td>Migrate Pwd</td>
<td>42%</td>
<td>35%</td>
</tr>
<tr>
<td>Remote Login</td>
<td>27%</td>
<td>42%</td>
</tr>
<tr>
<td>Update Pwd</td>
<td>19%</td>
<td>65%</td>
</tr>
<tr>
<td>Second Login</td>
<td>52%</td>
<td>28%</td>
</tr>
<tr>
<td>Password Multiplier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log In</td>
<td>48%</td>
<td>44%</td>
</tr>
<tr>
<td>Migrate Pwd</td>
<td>16%</td>
<td>32%</td>
</tr>
<tr>
<td>Remote Login</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Update Pwd</td>
<td>16%</td>
<td>4%</td>
</tr>
<tr>
<td>Second Login</td>
<td>16%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Questionnaire responses

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**.
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.
- PwdHash: Think passwords unique to them.
When “nothing works”

- Tendency to try all passwords
- A poor security choice.
- May make the use of PwdHash or Password Multiplier worse than not using any password manager.
- Usability problem leads to security vulnerabilities.
Facebook founder Mark Zuckerberg 'hacked into emails of rivals and journalists'

By MAIL FOREIGN SERVICE
Last updated at 2:09 AM on 06th March 2010

Business Insider claimed he then told a friend how he had hacked into the accounts of Crimson staff.

He allegedly told the friend that he used TheFacebook.com to search for members who said they were Crimson staff.

Then, he allegedly examined a report of failed logins to see if any of the Crimson members had ever entered an incorrect password into TheFacebook.com.

In the instances where they had, Business Insider claimed that Zuckerberg said he tried using those incorrect passwords to access the Crimson members' Harvard email accounts.

In two instances, the magazine claimed, he succeeded - and was able to read emails between Crimson staff discussing the possibility of writing an article on the accusations surrounding him.

'In other words,' Business Insider claimed, 'Mark appears to have used private login data from TheFacebook to hack into the separate email accounts of some TheFacebook users'.
Human Verification

◆ Problem:
  • Want to make it hard for spammers to automatically create many free email accounts
  • Want to make it difficult for computers to automatically crawl some data repository

◆ Need a method for servers to distinguish between
  • Human users
  • Machine users

◆ Approach: CAPTCHA
  • Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAPTCHAs

Idea: “easy” for humans to read words in this picture, but “hard” for computers
Caveats

- Usability challenges with visual impairments
- Researchers studying how to break CAPTCHAs
- Some attackers don’t break CAPTCHAs; they hire or trick others
How did they do it? Most online ticket Web sites like Ticketmaster employ CAPTCHA technologies, which requires users to read images that are recognizable to the human eye but confusing to computers, and type them into a box before buying tickets.

The defendants, however, worked with computer programmers in Bulgaria to develop a technology that allowed a network of computers to impersonate individual visitors to online ticket vendors. The ticket vendors did not immediately recognize the purchases as computer-generated, so these "CAPTCHA Bots" let Wiseguy Tickets to flood ticket vendors as soon as tickets went on sale and purchase tickets faster than any human.
I've loved our online chats these past few months, Lisa.  
Me too. I really like you, Rob.

It's just... now and then you mention products you like, and... I worry.

What? Honey...  
I just want to be sure.

Before this goes any further, I think we should go get tested. You know, together.

You don't trust me?

VK Couples Testing  
Test ID: 1234567890
Waiting... Partner connected.

Okay, mine says "library". Yours?

I'm more than a spambot! Our love... oh god. Goodbye, Lisa. Was real!
Phishing

- “The Emperor’s New Security Indicators”
- “Why Phishing Works”

- In one study: 27 out of 27 people entered personal information if HTTPS was changed to HTTP (no SSL)
- Other security indicators not very effective (lock icons, ...)
- If a site looks “professional”, people likely to believe that it is legitimate
Experiments at Indiana University [Jagatic et al.]

- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
- Sent 921 Indiana University students a spoofed email that appeared to come from their friend
- Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu
- 72% of students entered their real credentials into the spoofed site
More Details

- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information

- 70% of responses within first 12 hours
- Adversary wins by gaining users’ trust
## More Details

<table>
<thead>
<tr>
<th></th>
<th>To Male</th>
<th>To Female</th>
<th>To Any</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Male</td>
<td>53%</td>
<td>78%</td>
<td>68%</td>
</tr>
<tr>
<td>From Female</td>
<td>68%</td>
<td>76%</td>
<td>73%</td>
</tr>
<tr>
<td>From Any</td>
<td>65%</td>
<td>77%</td>
<td>72%</td>
</tr>
</tbody>
</table>
More Details

![Success Rate Chart]

<table>
<thead>
<tr>
<th>Class</th>
<th>Control</th>
<th>Social</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior</td>
<td>5%</td>
<td>68%</td>
</tr>
<tr>
<td>Junior</td>
<td>13%</td>
<td>69%</td>
</tr>
<tr>
<td>Sophomore</td>
<td>26%</td>
<td>71%</td>
</tr>
<tr>
<td>Freshman</td>
<td>14%</td>
<td>76%</td>
</tr>
<tr>
<td>Other</td>
<td>50%</td>
<td>76%</td>
</tr>
</tbody>
</table>
More Details

![Success Rate Chart](chart.png)

- **Business**: Control 19%, Social 72%
- **Education**: Control 19%, Social 68%
- **Liberal Arts**: Control 50%, Social 71%
- **Science**: Control 0%, Social 80%
- **Technology**: Control 0%, Social 36%
- **Other**: Control 14%, Social 67%