For this Wednesday: vote papers up/down

Which papers were LEAST valuable?
Please choose up to 3 papers that you did NOT enjoy reading and that we should consider replacing in future years.

- 08/29: Bush. As We May Think
- 08/31: Grossman. The Bubble Cursor
- 09/07: Wilson. Combining Multiple Depth Cameras...
- 09/07: Wilson. Depth-Sensing Video Cameras for 3D Tangible Tabletop Interaction
- 09/07: Wilson. Using a Depth Camera as a Touch Sensor
- 09/12: Hutchins. Direct Manipulation Interfaces
- 09/12: Weiser. The Computer for the 21st Century
- 09/14: Wellner. DigitalDesk
- 09/14: Han. Low-cost multi-touch sensing through frustrated total internal reflection
- 09/19: Harrison. Skinput.
- 09/21: Hollan. Beyond Being There
- 09/26: Bernstein. Soylent: A Word Processor with a Crowd Inside
- 09/26: von Ahn. Designing Games with a purpose.
- 09/28: Houde. What do Prototypes Prototype?
- 10/03: Marks. Design Galleries
- 10/03: Song. The ModelCraft Framework
- 10/05: Kuhn. The Structure of Scientific Revolutions
- 10/10: McGuire. Creative Hypothesis Generation
- 10/10: McGrath. Methodology Matters
- 10/12: Kohavi. Practical Guide to Controlled Experiments on the Web
- 10/13: Shneiderman. User Interface Strategy Reconsidered
USER INTERFACE RESEARCH

CS260 Presentations + Demos

Tuesday 12/6/2011 4-6:30pm
Visual Computing Lab 510 Soda Hall

Presentations start at 4pm, demos & posters at 5:30pm.
Deadlines

Wednesday 11/30: (i.e., Tue 7pm) Vote papers up/down

Friday 12/2, 5pm: Paper draft. Requirements:
Decide on final paper title
Draft must be in CHI extended abstract format
6 pages long (+/- 2 for draft)
Section-complete: at least bullet points for all sections
At least placeholders for figures

Monday 12/5, 9am: Posters on wiki
(if you want us to print them)

Monday 12/5, 2:30pm: Practice presentations in BiD
Usable Security

Unusable security & privacy

Unpatched Windows machines are compromised in minutes
Phishing web sites increasing by 28% each month
Most PCs are infected with spyware
Users have more passwords they can remember and practice poor password security
Enterprises store confidential information on laptops and mobile devices that are frequently lost or stolen
Grand Challenge

Give end-users **security controls** they can **understand** and **privacy** they can control for the dynamic, pervasive computing environments of the future.

- Computing Research Association, 2003
Security vs. Privacy

**Security**: protecting the confidentiality, integrity and availability of information (CIA); ensuring authenticity.

**Privacy**: control over the collection and revelation of personally identifiable information to others.
The goal of security is not to build systems that are \textit{theoretically} secure, but to build ones that are \textit{actually} secure.
Psychological acceptability

Concept due to Saltzer and Schroeder, 1975.

The principle of psychological acceptability states that security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present.

In practice, the principle is interpreted to mean that the security mechanism may add some extra burden, but that burden must be both minimal and reasonable.”
Unacceptable Security?
Security is a supporting task

Production tasks advance us toward a goal.

Supporting tasks are not essential for the goal, but enable or enhance production tasks.

Examples of production tasks?
Supporting Task: Implications

Security tasks must be designed to support production tasks.

Users need to understand and accept the need for security tasks.
Passwords - Typical Advice

Pick a hard-to-guess password.
Don’t use it anywhere else.
Change it often.
Don’t write it down.
Top Passwords of 2011

- password
- 123456
- 12345678
- qwerty
- abc123
- monkey
- 1234567
- letmein
- trustno1
- dragon
- baseball
- 111111
- iloveyou
- master
- sunshine
- ashley
- bailey
- passw0rd
- shadow
- 123123
- 654321
- superman
- qazwsx
- michael
- football
Password Expired

Your password has expired. Please enter a new password.

The password must:

- be 8 characters or longer
- contain at least one numeral
- contain at least one character
- not contain three consecutive identical characters
- not have been used in the past year
- not be the same as your Apple ID

Old Password

New Password

Confirm New Password

Change Password

If you aren't Chris and you have an Apple ID, log-in now. If you don't have an account, click here to set one up.

Click here to see our privacy policy.
Customer ID Standards
- Use 6 to 15 letters and/or numbers
- If your Customer ID is between 9 and 11 characters in length, it must contain at least two letters
- Do not use or spell your first, middle, or last name or identifiable information such as your Social Security number, address, or date of birth. Instead, use your initials in a consistent format (e.g., JSmith1985)
- Do not use numbers or letters that could be easily guessed (e.g., 7777 or 12345)
- Do not use symbols (e.g., #, @, /, *, -)

PIN Standards
- Use 6 to 12 letters
- Do not use one element of information such as your Social Security number, address, or telephone number to disguise it (e.g., Jane12345Sm)
- Do not use more than one letter, or easily recognizable elements (e.g., 11111)
- Do not use symbols (e.g., #, @, /, *, -)

Security Answer Standards
- Answers must be between 3 and 31 characters
- Select a question that you can easily answer
- Answers are not case sensitive
- Do not use symbols, punctuation marks, or spaces (e.g., #, @, /, *, -)
Password advice meets the web

# of users

# of systems

users access

Bank = b3aYZ
Amazon = aa66x!
Phonebill = p$2$ta1
User’s perspective on passwords

**Goal**: Easy to remember, difficult to guess.

Requires a mental model of what is “easy” to guess. Many people do not have this.

**Strategies?**
Possible design solutions?
Passwords and Errors

Did I type what I think I typed?

What’s the purpose of the dots anyways?
Exploit the difference between user and attacker

From: Tognazzini, Ch3 in Security and Usability

User:
knows what she wants to type
close to the screen

Password: ●●●●●●●

Eavesdropper:
must reconstruct every character
some feet away from screen
DESIGN CHECKLIST

Achieving balance:

☐ Are you exploiting the differences between users and attackers?
   ☐ Users know what they are typing in—they are only looking for errors.
   ☐ Eavesdroppers, meanwhile, have to reconstruct every character accurately.
   ☐ Users are closer to the screen and therefore can read with lower contrast and can differentiate better between green and blue (unless they are colorblind).

☐ Are you detecting and exploiting differences in physical location?
   ☐ Home
   ☐ Office
   ☐ Airport and other public venues

☐ Are you providing a way that your software can track location changes or the user can casually indicate such changes?

☐ Are you varying security with the task?
   ☐ Temporary versus archival security
   ☐ “Here” versus “there” versus “en route”
   ☐ “Hide from co-workers” versus “Hide from competitors”

☐ Does your design exploit the special skills of your user population?

☐ Does it serve to reduce the user’s burden?
Activity: Mobile Passwords

Young mobile professionals carry laptop, cell phone, iPad, others.

Each of these devices requires a password for use. The users will need easy access to their data at a moment's notice. However, the consequences of someone else gaining access to their data are severe. Hardware limitations preclude the use of biometrics.

Discuss how to address security needs with passwords in this context.

Should each device have its own password or should there be one password? Should users change their passwords on a regular basis? Should passwords be randomly assigned or chosen by users? What precautions should be taken for password entry in public spaces?
Privacy
Do you know what you are sharing with the world?
The case of KaZaA

Early 2000s, the “golden years” of P2P filesharing:
Napster, Grokster, LimeWire, KaZaA, Morpheus, Soulseek...

Default behavior on many services:
Your downloads are shared with the rest of the network.

Intuition: unintended information leaks
(esp. for shared account machines)
Evidence for inadvertent sharing

Experiment 1:
100+ hits when searching for *inbox.dbx*, *Outlook.pst* (Outlook email file)

Experiment 2:
Other users downloaded (dummy) files named *inbox.dbx* and *creditcards.xls* from the researchers’ client.
Shared Directory in KaZaA

Referred to variously as My Media, My Shared Folder, My KaZaA, and the folder for downloaded files.

Automatic recursive sharing or subdirs.
User Study: Do people know what is shared?

12 participants, 10 with file sharing experience.

Desktop machine that had file sharing enabled, with the shared folder set to C: \n
Questions:  
Are files being shared?  
If so, which files?
Results

2/12 found that all files were shared.

9 assumed only multimedia files were shareable.

Considerable confusion between different views/controls for sharing.
Fast forward to today: Facebook

Matt McKeon

http://mattmckeon.com/facebook-privacy/
Activity: Implications of Facebook Data Sharing

Make a list of risks when your Facebook data is exposed according to the last privacy defaults. List possible negative consequences for you, and possible parties which benefit from this data.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Examples of possible consequences</th>
<th>Examples of parties to whom personal information might be exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsolicited marketing</td>
<td>Unwanted email, postal mail, and telephone calls; time wasted deleting email, throwing away mail, answering calls</td>
<td>Employees of personalized website; employees of companies to whom marketing lists are sold; employees of companies that perform marketing services</td>
</tr>
<tr>
<td>Computer “figuring things out” about me</td>
<td>Individuals feel uncomfortable or embarrassed; characteristics inferred by computer become available to people who would otherwise not know this information; inaccurate information inferred by computer becomes available to people who believe it to be accurate</td>
<td>Employees of personalized website; any other parties that gain access to profile</td>
</tr>
<tr>
<td>Price discrimination</td>
<td>Individuals are treated differently based on profile; higher prices</td>
<td>Employees of personalized website</td>
</tr>
<tr>
<td>Information revealed to other users of same computer</td>
<td>Other users of computer may learn confidential information; other users of computer may be able to gain access to accounts</td>
<td>Other users of computer such as family members or co-workers</td>
</tr>
<tr>
<td>Unauthorized access to accounts</td>
<td>Identity theft, fraud, stalking</td>
<td>People that run personalized website, someone who steals password</td>
</tr>
<tr>
<td>Subpoena</td>
<td>Information used against individual in court case</td>
<td>Law enforcement officers or participants in legal dispute; public (if information obtained becomes part of public record)</td>
</tr>
<tr>
<td>Government surveillance</td>
<td>Individual could be detained by law enforcement for questioning or arrested</td>
<td>Law enforcement officers</td>
</tr>
</tbody>
</table>
Security and Usability
Designing Secure Systems That People Can Use

Edited by Lorrie Faith Cranor & Simson Garfinkel

O’Reilly, 2005