Human-Computer Interaction Opportunities for Improving Security/Privacy

Ben Shneiderman  

Founding Director (1983-2000), Human-Computer Interaction Lab  
Professor, Department of Computer Science  
Member, Institutes for Advanced Computer Studies & Systems Research
Interdisciplinary research community
- Computer Science & Psychology
- Information Studies & Education

(www.cs.umd.edu/hcil)
User Interface Design Goals

• Cognitively comprehensible:
  Consistent, predictable & controllable

• Affectively acceptable:
  Mastery, satisfaction & responsibility

NOT:
  Adaptive, autonomous & anthropomorphic
Scientific Approach (beyond user friendly)

• Specify users and tasks
• Predict and measure
  • time to learn
  • speed of performance
  • rate of human errors
  • human retention over time
• Assess subjective satisfaction
  (Questionnaire for User Interface Satisfaction)
• Accommodate individual differences
• Consider social, organizational & cultural context
Design Issues

- Input devices & strategies
  - Keyboards, pointing devices, voice
  - Direct manipulation
  - Menus, forms, commands
- Output devices & formats
  - Screens, windows, color, sound
  - Text, tables, graphics
  - Instructions, messages, help
- Collaboration & communities
- Manuals, tutorials, training
U.S. Library of Congress

American Memory
Historical Collections for the National Digital Library

- Scholars, Journalists, Citizens
- Teachers, Students
Visible Human Explorer (NLM)

- Doctors
- Surgeons
- Researchers
- Students
NASA Environmental Data

- Scientists
- Farmers
- Land planners
- Students
Bureau of the Census

- Economists, Policy makers, Journalists
- Teachers, Students

American FactFinder™
NSF Digital Government Initiative

- Find what you need
- Understand what you find

Census, NCHS, BLS, EIA, NASS, SSA

www.ils.unc.edu/govstat/

FedStats

HCIL
International Children’s Digital Library

A project of the University of Maryland and the Internet Archive

Choose a version of the library

Enter Library
- Basic
- Enhanced

Search for books

Explore the fun - read 324 books online...

Featured Books
- The Mouse Bride
  Lao shu chu hai niang
- Akrarash’s zakhida web
  Farsi book about Dragons
- Rosa elada
  (A Rose with Wings)

Announcements

DEC 27, 2003:
The ICDL has added 52 more books! These books add to our collection with books in Chinese, Spanish, Vietnamese, Farsi, French, English, and Russian.

DEC 2, 2003:
A new version of ICDL Basic has just been published, the new features include:
- Unicode compliance: ICDL web pages can now display languages from all over the world
- Improved text search: search in multiple languages, view results in ranked order
- New books: 13 new books

DEC 1, 2003:
A recent study of our ICDL users shows:
- ICDL users come from 150 countries world wide.
- Taiwan has the most frequent users of the ICDL after the United States.
- Poland is among the top ten countries of most frequent Basic users.
For more information, go to our "Fun Facts" page.

Our Mission

The mission of the ICDL is to select, collect, digitize, and organize children’s materials in their original languages and to create appropriate technologies for access and use by children 3-13 years old.

www.icdlbooks.org
Piccolo: Toolkit for 2D zoomable objects

Structured canvas of graphical objects in a hierarchical scenegraph
- Zooming animation
- Cameras, layers

Open, Extensible & Efficient
Java, C#, PocketPC versions

www.cs.umd.edu/hcil/piccolo
PhotoMesa

www.cs.umd.edu/hcil/photomesa
Pocket PhotoMesa

www.windsorinterfaces.com
CRA Grand Challenges, 2003

4) For the dynamic, pervasive computing environments of the future, give endusers:
   - security they can understand
   - privacy they can control.

   - patient health record
   - electronic voting
   - law enforcement databases
   - financial management

http://www.cra.org/Activities/grand.challenges/security/
For end-users:
Incorrectly used software or hostile or confusing user interfaces can lead to user frustration and unauthorized workarounds that can compromise even the most robust security schemes.

For operators:
Usable presentation interfaces that allow operators to better understand incidents in progress.

http://www.nitrd.gov
Profusion of Concepts for Security/Privacy

Personal computing was easier
- File protection vs sharing
- Passwords & Access Control

Networking adds complexity
- Firewalls & Virtual Private Networks
- Cookies: good or bad?
- Trusted sources & Digital signatures
- Certificates & Authentication
- Viruses & Worms
Profusion of Concepts for Security/Privacy

Goals

• Availability: Accessible when needed
• Confidentiality: Crypto & limit access
• Data integrity: Prevent modifying your data
• Control: Access rights & physical security
• Audit: Logging, review & damage assessment
Profusion of Concepts for Security/Privacy

Goals

• Availability: Accessible when needed
• Confidentiality: Crypto & limit access
• Data integrity: Prevent modifying your data
• Control: Access rights & physical security
• Audit: Logging, review & damage assessment

Most current systems present the user with an intricate interface for specifying his protection needs. The result is that the user has trouble figuring out how to make the specification and verifying that he requested the right thing. User interfaces that more closely match the mental models people have of information protection are needed.
Profusion of Concepts for Security/Privacy

Goals

• Availability: Accessible when needed
• Confidentiality: Crypto & limit access
• Data integrity: Prevent modifying your data
• Control: Access rights & physical security
• Audit: Logging, review & damage assessment

Most current systems present the user with an intricate interface for specifying his protection needs. The result is that the user has trouble figuring out how to make the specification and verifying that he requested the right thing. User interfaces that more closely match the mental models people have of information protection are needed.

Saltzer & Schroeder, 1975
Security setting - IE
Security zones – Online Help

Understanding security zones

Internet Explorer divides your Internet world into zones, so that you can assign a Web site to a zone with a suitable security level.

You can tell which zone the current Web page is in by looking at the right side of the Internet Explorer status bar: Whenever you attempt to open or download content from the Web, Internet Explorer checks the security settings for that Web site's zone.

There are four zones:

- **Internet zone**: By default, this zone contains anything that is not on your computer or an intranet, or assigned to any other zone. The default security level for the Internet zone is Medium. You can change your privacy settings for the Internet zone on the Privacy tab in Internet Options. For more information, click Related Topics.

- **Local intranet zone**: This zone typically contains any addresses that don't require a proxy server, as defined by the system administrator. These include sites specified on the Connections tab, network paths (such as \computername\folder\name), and local intranet sites (typically addresses that don't contain periods, such as http://internal). You can add sites to this zone. The default security level for the Local intranet zone is Medium, therefore, Internet Explorer will allow all cookies from Web sites in this zone to be saved on your computer and read by the Web site that created them.

- **Trusted sites zone**: This zone contains sites you trust—sites that you believe you can download or run files from without worrying about damage to your computer or data. You can assign sites to this zone. The default security level for the Trusted sites zone is Low, therefore, Internet Explorer will allow all cookies from Web sites in this zone to be saved on your computer and read by the Web site that created them.

- **Restricted sites zone**: The zone contains sites you don’t trust—sites that you’re not sure whether you can download or run files from without damage to your computer or data. You can assign sites to this zone. The default security level for the Restricted sites zone is High, therefore, Internet Explorer will block all cookies from Web sites in this zone.

In addition, any files already on your local computer are assumed to be very safe, so minimal security settings are assigned to them. You cannot assign a folder or drive on your computer to a security zone.

You can change the security level for a zone; for example, you might want to change the security settings for your Local intranet zone to Low, or, you can customize the settings within a zone. You can also customize settings for a zone by importing a privacy settings file from a certification authority.

Related Topics
Privacy setting

- Move the slider to select a privacy setting for the Internet zone.

**Medium**
- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

**Advanced Privacy Settings**
You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

**Cookies**
- First-party Cookies
  - Accept
  - Block
  - Prompt
- Third-party Cookies
  - Accept
  - Block
  - Prompt
- Always allow session cookies
To customize your privacy settings for all Web sites

1. In Internet Explorer, on the Tools menu, click Internet Options.
2. Click the Privacy tab, and then click Advanced.
3. Click Override automatic cookie handling, and then specify how you want Internet Explorer to handle cookies from first-party Web sites and third-party Web sites (a Web site other than the one you are currently viewing).
   - To specify that you want Internet Explorer to always allow cookies to be saved on your computer, click Accept.
   - To specify that you want Internet Explorer to never allow cookies to be saved on your computer, click Block.
   - To specify that you want Internet Explorer to ask whether or not you want to allow a cookie to be saved on your computer, click Prompt.
4. If you want Internet Explorer to always allow session cookies (cookies that will be deleted from your computer when you close Internet Explorer) to be saved on your computer, click Always allow session cookies.

Notes
- Some Web sites require cookies; therefore, if you select a setting that does not allow cookies to be saved on your computer, you might not be able to view certain Web sites.
- When you change your privacy settings, the changes might not affect cookies that are already on your computer. If you want to ensure that all of the cookies on your computer meet your privacy settings, you should delete all of the existing cookies on your computer. When you return to Web sites that previously had saved cookies on your computer, the Web sites that meet your privacy settings will save cookies on your computer again. The Web sites that do not meet your privacy settings will not be allowed to save cookies on your computer, and might not function properly.
- Your privacy settings only affect Web sites in the Internet zone. For more information about zones, click Related Topics.
- You can also specify custom privacy settings for a specific Web site. For more information, click Related Topics.
VPN Virtual Private Network

[Image of VPN software interfaces]
Keep your Word documents secure

Microsoft Word provides several security and document protection features. You can do any of the following to protect your documents and the information they contain:

Protect against macro viruses
For the best protection against macro viruses, you should purchase and install specialized antivirus software.

You can also use the following methods in Word:
- Set the security level
- Warn about installed templates and add-ins that contain macros
- Digitally sign macros

Protect a document from unauthorized changes
Do any of the following:
- Seal your document with a digital certificate
- Require a password to open or modify a document
- Have Microsoft Word recommend opening a document as read-only
- Prevent users from changing a form
- Protect for comments and tracked changes
Emerging Research

- Saltzer & Schroeder, IEEE, 1975
- Adams & Sasse, CACM, 1999
- Whitten & Tygar, USENIX, 1999
  “Why Johnny Can’t Encrypt”
- Gene Spafford, Purdue Univ
  Center for Education and Research Information and Assurance and Security
- Ka-Ping Yee, UC-Berkeley, 2002
Guidelines

**Match** the most comfortable way to do tasks with the least granting of authority

**Grant** authority to others in accordance with user actions indicating consent

**Offer** the user ways to reduce others' authority to access the user's resources

**Maintain** accurate awareness
- of others' authority as relevant to user decisions
- the user's own authority to access resources

K-P Yee, http://www.sims.berkeley.edu/~ping/sid/
Guidelines

Protect the user's channels to agents that manipulate authority on the user's behalf

Enable the user to express safe security policies in terms that fit the user's task

Draw distinctions among objects and actions along boundaries relevant to the task

Present objects and actions using distinguishable, truthful appearances

Indicate clearly the consequences of decisions that the user is expected to make

K-P Yee, http://www.sims.berkeley.edu/~ping/sid/
Emerging Research

- Good & Krekelberg, CHI 2003, Kazaa
- Simson Garfinkel, MIT, 2004 (David Clark, Rob Miller)
- Lorrie Cranor, CMU
  - Center for Usable Privacy and Security (CUPS)
  - Symposium on Usable Privacy and Security (SOUPS 2005)
- Karat, Karat & Brodie, IJHCS 2005 Special Issue: HCI Privacy & Security
Controlled Experiment: XPFP

(Maxion & Reeder, IJHCS Special Issue, 2005)
Controlled Experiment: Salmon

(Maxion & Reeder, IJHCS Special Issue, 2005)
## Controlled Experiments

- 12 subjects for each interface

<table>
<thead>
<tr>
<th>Tasks</th>
<th>% done</th>
<th>XPFP</th>
<th>Salmon</th>
</tr>
</thead>
<tbody>
<tr>
<td>W</td>
<td>58</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>J</td>
<td>25</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>75</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors</th>
<th>XPFP</th>
<th>Salmon</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

- Successful users: XPFP=178s  Salmon=61s

(Maxion & Reeder, IJHCS Special Issue, 2005)
Possible Strategies

- Multi-layer interface that:
  - Ties increasing complexity to increasing control
  - Permits evolutionary learning as needed
- Cleaner cognitive model
  - Fewer objects & actions
  - Clearer feedback about decisions
- Show consequences of decisions
- Show dynamics of activity with viewable log
Commercial Practice - Usability Engineering

• User-centered design processes
  • Contextual Design - Beyer and Holtzblatt
  • Participatory Design

• Guidelines documents and processes

• User interface building tools

• Expert reviews and usability testing
Usability Testing

• Physical place and permanent staff vs. discount usability testing
• Focuses attention on user interface design
• Encourages iterative testing
  • Pilot test of paper design
  • Online prototype evaluation
  • Refinement of versions
  • Testing of manuals, online help, etc.
  • Rigorous acceptance test

• Must participate from early stages
• Must be partners, not "the enemy"

(Dumas & Redish, 1999; Nielsen, 1993)
The eye... the window of the soul, is the principal means by which the central sense can most completely and abundantly appreciate the infinite works of nature.

Leonardo da Vinci
(1452 - 1519)
Using Vision to Think

• Visual bandwidth is enormous
  • Human perceptual skills are remarkable
    • Trend, cluster, gap, outlier...
    • Color, size, shape, proximity...
  • Human image storage is fast and vast

• Opportunities
  • Spatial layouts & coordination
  • Information visualization
  • Scientific visualization & simulation
  • Telepresence & augmented reality
  • Virtual environments
Information Visualization for Security

- Detecting intrusions
- Anomaly detection
- Network Traffic classification
- Hostile event
- Link Relationships
- Security Situation Awareness
- Fingerprint network attacks
- Attack Graph complexity
- Profiling users & traffic
- Malicious insider detection

VIZSEC 2004
Information Visualization: Mantra

• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
• Overview, zoom & filter, details-on-demand
Treemap: Stock market, clustered by industry
Treemap: Million files

www.cs.umd.edu/hcil/millionvis/
Temporal Data: TimeSearcher 1.3

- Time series
  - Stocks
  - Weather
  - Genes
- User-specified patterns
- Rapid search
Temporal Data: TimeSearcher 2.0

- Long Time series (>10,000 time points)
- Multiple variables
- Controlled precision in match (Linear, offset, noise, amplitude)
“HCE enabled us to find important clusters that we didn’t know about.” - a user
HCE Status

- In collaboration and sponsored by Eric Hoffman: Children’s National Medical Center
- Categorical Variables: 4.0 beta, May 2005
- 60K lines of C++ codes, 58 Classes
- 2,000+ downloads since April 2002

www.cs.umd.edu/hcil/hce
For More Information

• Visit the HCIL website for 350 papers & info on videos
  www.cs.umd.edu/hcil

• Conferences & resources:  www.infovis.org

• See Chapter 14 on Info Visualization
  Shneiderman, B. and Plaisant, C., Designing the User Interface:
  Strategies for Effective Human-Computer Interaction:

• Edited Collections:
  Readings in Information Visualization: Using Vision to Think
  The Craft of Information Visualization: Readings and Reflections
For More Information

- Treemaps
  - HiveGroup: www.hivegroup.com
  - Smartmoney: www.smartmoney.com/marketmap
  - HCIL Treemap 4.0: www.cs.umd.edu/hcil/treemap
- Spotfire: www.spotfire.com
- TimeSearcher: www.cs.umd.edu/hcil/treemap
- Hierarchical Clustering Explorer:
  www.cs.umd.edu/hcil/hce
Logical User Centered Interaction Design

• Design Methodology
  • Management strategy to highlight usability engineering
  • Processes, Deliverables, and Reviews

• Stages for LUCID
  1: Envision
  2: Discovery
  3: Design Foundation
  4: Design Detail
  5: Build
  6: Release

(Cognetics Corp, www.cognetics.com)
Guidelines Document and Processes

- Social process for developers
- Records decisions for all parties to see
- Promotes consistency and completeness
- Facilitates automation of design
- Should contain philosophy and examples of:
  - title screens, menus, forms, buttons, graphics, icons, fonts, colors, instructions, help, tutorials, error messages, ...
- Multiple levels are desirable:
  - standards, practices, guidelines
- Education, Enforcement, Exemption & Enhancement
Expert Reviews and Usability Testing

- Improved product quality
- Shorter development time
- More predictable development lifecycle
- Reduced costs
  - Speed development
  - Simplify documentation
  - Facilitate training
  - Lower support
  - Fewer updates
- Improved organizational reputation
- Higher morale: staff and management
Expert Reviews

• Experienced reviewers
  • Review every screen, menu, dialog box
  • Spot inconsistencies and anomalies
  • Suggest additions

• Disciplined approaches
  • Heuristic evaluation: check if goals are being met
  • Guidelines review: verify adherence
  • Consistency inspection: terms, layout, color, sequencing
  • Cognitive walkthrough: pretend to be a user following scenario
  • Formal inspection: public presentation and discussion