Visualization

Alex Endert
aendert@cs.vt.edu
Overview

Presentation of Papers


Critique / Discussion
EXPANDABLE GRIDS FOR VISUALIZING AND AUTHORING COMPUTER SECURITY POLICIES (2008)

Robert W. Reeder, Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter, Kelli Bacon, Keisha How, Heather Strong
Background

- **Expandable Grid**
  - Matrix-based visualization of a policy

- **Windows XP policy management is not adequate.** ("list-of-rules model")
  - Must give administrator overview (for context) of all rules.
  - Also on Linux, Mac OS X Server
Fundamental Operations of Policy-authoring Interfaces

1. Viewing Policy
2. Changing Policy
3. Viewing Composite Value Memberships
   1. “groups”
4. Detecting and Resolving Conflicts
List-of-Rules Model

Why does Jana not have access to Four-part Harmony.doc??
Expandable Grids

Jana has read, not write access

Change in WinXP Semantics: Allow > Deny!!
Expandable Grids

- Features:
  - Whole Policy
  - Effective Policy
  - Group Membership Info
  - Simple Changes
  - New Policy Semantics
  - Visual pop-out
  - **Highlighting**
  - **Search**

Figure 2. Screenshot of our Expandable Grid interface when the Jana task has been halfcompleted.
User Study Methodology

- 36 engineering undergrads (10 female, 26 male)
  - No sys admin experience (?)
- Windows XP
- Collected:
  - Video
  - Audio
  - Policies Created
User Study Tasks

- 20 (10 pairs) tasks, requiring:
  - Training
  - View-simple
  - View-complex
  - Change-simple
  - Change-complex
  - Compare-groups
  - Conflict-simple
  - Conflict-complex
  - Memogate
  - Precedence
Results

Figure 3. Accuracy results, showing proportion of participants correctly completing each task with Grid and Windows interfaces.
## Results

- **Bottom line:** Expandable Grid allows authors to complete tasks more accurately and faster (significantly!)

<table>
<thead>
<tr>
<th>Task pair</th>
<th>Small-scale</th>
<th></th>
<th>Large-scale</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$a_G$</td>
<td>$a_W$</td>
<td>$p$-value</td>
<td>$a_G$</td>
</tr>
<tr>
<td>View-simple</td>
<td>0.89</td>
<td>0.56</td>
<td>$p = 0.03$</td>
<td>0.61</td>
</tr>
<tr>
<td>View-complex</td>
<td>0.94</td>
<td>0.17</td>
<td>$p &lt; 0.001$</td>
<td>1.00</td>
</tr>
<tr>
<td>Change-simple</td>
<td>0.89</td>
<td>0.94</td>
<td>No test</td>
<td>1.00</td>
</tr>
<tr>
<td>Change-complex</td>
<td>0.61</td>
<td>0.00</td>
<td>$p &lt; 0.001$</td>
<td>0.67</td>
</tr>
<tr>
<td>Compare-groups</td>
<td>0.89</td>
<td>0.83</td>
<td>No test</td>
<td>0.67</td>
</tr>
<tr>
<td>Conflict-simple</td>
<td>0.67</td>
<td>0.61</td>
<td>$p = 0.5$</td>
<td>0.72</td>
</tr>
<tr>
<td>Conflict-complex</td>
<td>0.89</td>
<td>0.00</td>
<td>$p &lt; 0.001$</td>
<td>1.00</td>
</tr>
<tr>
<td>Memogate</td>
<td>1.00</td>
<td>0.94</td>
<td>$p = 0.5$</td>
<td>0.94</td>
</tr>
<tr>
<td>Precedence</td>
<td>0.89</td>
<td>0.94</td>
<td>$p = 0.5$</td>
<td>0.78</td>
</tr>
</tbody>
</table>
IN THE EYE OF THE BEHOLDER: A VISUALIZATION-BASED APPROACH TO INFORMATION SYSTEM SECURITY (2005)

Rogerio de Paula, Xianghua Ding, Paul Dourish, Kari Nies, Ben Pillet, David F. Redmiles, Jie Ren, Jennifer A. Rode, Roberto Silva Filho
View on Security

- Focus on “whether a system is secure enough for [the user’s] immediate needs”
  - Effective Security < Theoretical Security
  - Control over Security

- 3 major elements:
  - Empirical investigation into everyday security practices
  - “systems approach”: vis & event based architectures
  - Initial prototype of P2P file sharing (face-to-face)
through information systems (as the examples here show). Researchers in the HCI community have long argued that “usability” cannot be an afterthought in information system design; a system cannot be made usable merely by the addition of a graphical user interface, however pretty. Security researchers have made a similar argument about the design of secure systems; insecure systems cannot be turned into secure ones merely by the addition of a layer of encryption. Both of these argue, then, that security and usability need to be understood as a holistic design problem. A lick of “usability paint” will not cure the difficulty of making use of, say,
Empirical Investigation Results (Users)

- **Optimization**
  - Security is not the point of their work, their task is...

- **Contingent Assessment**
  - Balance of immediate needs and overall security

- **Delegation**
  - Rely on trusted “agents” (i.e. encryption agents, pre-configured “security” system).

- **Embeddedness**
  - Defining boundaries of “information systems” is difficult
Empirical Investigation Results (Security)

for their immediate needs. Security is evaluated and managed in a range of contexts—physical, personal, organizational, interactional, and more.

- “security in practice is not an all-or-nothing matter”
- “secure” and “insecure” is not absolute
- Security mechanism visible to user
- Security is “end-to-end” – all components play role
Design Guidelines for Effective Security

In particular, our approach in Swirl is based on supporting informed decision-making. The central problem of security, for end-users, is two-fold: it involves understanding the system’s configuration and state, and understanding their consequences for user action. People act through information technology, and so our goal is to help them understand how an information system might mediate their actions. This turns our attention away from traditional considerations of expression.

- In other words, their focus is on:
  - Visualizing system activity
  - Integrating configuration and action
Testbed: “Impromptu”

- Collaborative, face-to-face P2P file sharing system
  - “evaluation exercise is ongoing”
  - (more detail in later paper)
SEEING FURTHER: EXTENDING VISUALIZATION AS A BASIS FOR USABLE SECURITY (2006)

Jennifer Rode, Carolina Johansson, Paul DiGioia, Roberto Silva Filho, Kari Nies, David H. Nguyen, Jie Ren, Paul Dourish, and David Redmiles
Focus

- File Sharing Visualization (Impromptu) that:
  - Shows system activity
  - Integrates configuration and user action
  - Shows temporal and structural information
  - Allows collaboration
Views on Security

- “Strict Usability”
  - Traditional methods for security measures used regularly
    - E.g. passwords, encryptions, VPNs, etc.

- “Everyday Use”
  - “privacy and security cannot be held to absolute measures…need to be negotiated [per situation]”
  - “people must make informed decisions”
Impromptu Concept

- Design Principles:
  - Visualization Mechanisms
  - Integration of Configuration and Action
  - Use of event-based architectures

  "integrating action and configuration and the concept of dynamic visualization of activity"
Impromptu Design

- Colors = Users
- Closer to center, "more shared"
  - Center = "persistent file"
- Dots = files
  - Color of dots = last user accessing file
Impromptu Design

- Degrees of sharing
  1. Not shared, local only
  2. Visible, local only
  3. Readable
  4. Readable & Writable
  5. Persistent
Impromptu Architecture

- No central server, all P2P
- User leaves, file leaves (unless persistent)
- “strict security is not a requirement”
User Study

- 24 graduate students
- 8 sessions (3 users each)
- Used Impromptu, Excel, and Word

- Did not tell users to focus on security, but rather their task

- “not a usability trial … designed an open-ended, semi-naturalistic study”
## Findings

### User Feedback

Table 2. List of 20 positive comments volunteered during debrief about the ability to visualize system activity:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>The rings and blink around file icons indicate what is open</td>
</tr>
<tr>
<td>5</td>
<td>Permits you to see what others are doing, “awareness”</td>
</tr>
<tr>
<td>4</td>
<td>Clear indication of which files belong to who</td>
</tr>
<tr>
<td>2</td>
<td>Concentric spheres representing levels of privacy</td>
</tr>
<tr>
<td>1</td>
<td>Clear who is logging in</td>
</tr>
<tr>
<td>1</td>
<td>Clear indication of who is looking at what file</td>
</tr>
<tr>
<td>1</td>
<td>Clear indication of who is accessing your own files</td>
</tr>
<tr>
<td>1</td>
<td>Good visualization of different levels of access</td>
</tr>
</tbody>
</table>
Findings

Try:

- Which user (color) most recently accessed the file?
Findings

- History
  - Owner = red
  - Usage history:
    - Yellow (most recent)
    - Red
    - Yellow
    - Blue
    *more recent, closer to middle (?)
Findings

- History
  - Owner: blue
  - Most Recent:
    - Blue
    - Yellow
    - Red (?)

Figure 4: History Pie
Future Work

[Diagram of Impromptu Shared Workspace with notes on media characterization, activity wear, and user characterization.]

- **Media characterization**: Wired network connection icon
- **Activity wear**: Thin edges indicate low activity
- **Activity wear**: Thick edges indicate high activity
- **User characterization**: Warning sign indicating previously unknown user
- **Media characterization**: Wireless network connection icon
Critique

- **Expandable Grid**
  - **Pros**
    - Good design
  - **Cons**
    - User study participants (no experience in sys admin)

- **Impromptu**
  - **Pros**
    - Good initial visualization concept
  - **Cons**
    - Scalability
Next week…