27 – Access control and policy configuration

Lorrie Cranor, Blase Ur, and Rich Shay

April 23, 2015
Home access control

• Plethora of networked consumer electronics
  – Who handles security and access control in the digital home?
• Home security will only work if it works for home users
  – “Normal people” who don’t do technology 24/7/365
• Seek to understand attitudes, needs, and current practices
  – Current access-control practices: digital, paper

Interview study

• In-situ, semi-structured interviews
  – Recruitment via Craigslist, fliers
  – Limited to non-programmer households

• Interviewed 33 users in 15 households
  – Families, couples, roommates
  – Ages 8 to 59

• Recorded and transcribed over 30 hours of interviews
House Maps Guided Interviews
Interview protocol

• For each dimension, start with a specific scenario

• Example: Imagine that a friend is in your house when you are not. What kinds of files would you want them to be able to view?
  – Would it be different if you were also in the house?

• Extend to discuss that dimension in general

• Likert scale to rate concern over policy violations:
  – From 1 = don’t care, to 5 = devastating
Current methods aren’t working

- People do worry about sensitive data
  - Many potential breaches rated as “devastating”
  - Almost all worry about file security sometimes
  - Several have suffered actual breaches

- Access-control mechanisms varied and ad hoc
  - Encryption, user accounts (some people)
  - Hide sensitive files in the file system
    “If you name something ‘8F2R349,’ who’s going to look at that?”
  - Delete sensitive data so no one can see it
    “If I didn’t want everyone to see them, I just had them for a little while and then I just deleted them.”
Policy needs are complex

• Fine-grained divisions of people and files
  – Public/private not enough
  – More than friends, family, colleagues, strangers

• Presence of file owner matters
  – “If you have your mother in the room, you are not going to do anything bad. But if your mom is outside the room you can sneak.”
  – Also gives a chance to explain

• Location sometimes matters
  – People in my home are trusted

• Some people tend to share, some tend to restrict
Twenty-something middle school Spanish teacher:

“Wouldn’t want my boss to see me in my swimsuit…. I just wouldn’t like him to see it.”
Twenty-something paralegal and law student would let her boss see photo of her drunk, dancing on a table: “he’s seen me do it in person before.”
A-priori policy not good enough

- People don’t feel as much in control when they set policy up front
- People like to be asked permission
  “I’m very willing to be open with people, I think I’d just like the courtesy of someone asking me.”
- People want to know both who is accessing files and why
- People want to review accesses, revise policy
- This finding led us to conduct a follow-up study on reactive access control

Exploring reactive access control
[Mazurek, Klemperer, Shay, Takabi, Bauer, and Cranor, CHI 2011]
File system access control

• Access control on Windows file systems often incorrect

• Mistakenly misconfigured server used by both Republican and Democrat staffers led to 2003 “Memogate” scandal

• Windows access control is difficult because it has no holistic view of effective file permissions, and conflict resolution is complicated
Problem: Rule-centered interfaces
What makes policy authoring difficult?

- Default rules
  - What happens when no rule applies?
- Composite values (groups, folders, etc.)
  - What are the component values?
- Rule conflicts & precedence rules
  - What if more than one rule applies?
- Scale
  - Large policies can get tricky
Solution: policy visualization

![Image of policy visualization tool](image-url)
Four fundamental policy-authoring operations to support

1. Viewing policy decisions
2. Changing policy decisions
3. Viewing composite value memberships
4. Detecting and resolving conflicts
Example task: Jana

Jana, a Theory 101 TA, complained that when she tried to change the Four-part Harmony handout to update the assignment, she was denied access. Set permissions so that Jana can read and write the Four-part Harmony.doc file in the Theory 101\Handouts folder.
Jana setup

• Jana is a TA this year
  – Is in the group *Theory 101 TAs 2007*
• Jana was a TA last year
  – Is in the group *Theory 101 TAs 2006*
• 2007 TAs are allowed READ & WRITE
• 2006 TAs are denied READ & WRITE
• Since Jana is in both groups, she is denied access
Jana task – common error
Learning Jana’s effective permissions

1. Click “Advanced”
2. Click “Effective Permissions”
3. Select Jana
4. View Jana’s Effective Permissions
Learning Jana’s group membership

Bring up Computer Management interface

1. Double-click Jana

2. Click on “Users”

3. Click “Member Of”

4. Read Jana’s group membership

Theory 101 TAs 2006
Checking work

1. Click “Advanced”

2. Click “Effective Permissions”

3. Select Jana

4. View Jana’s Effective Permissions
XP support for fundamental operations

1. Viewing policy decisions
   – Effective policy decisions are 3 screens away (most authors don’t find them)

2. Changing policy decisions
   – Authors operate on rules, not effective policy

3. Viewing group memberships
   – In a separate application from file permissions

4. Detecting and resolving conflicts
   – Has to be done manually
Policies as lists of rules

• Natural to think of a policy as a list of rules…

• So, natural to design policy-authoring interfaces around lists of rules…

• But *it doesn’t provide the information authors need*

• Makes authors construct true policy by combining rules in their heads
Key insight: Center policy-authoring user interfaces around a display of the whole effective policy, not a list of rules
Solution: Expandable Grids
Viewing effective policy
Viewing effective policy
Expandable Grids

- Shows effective policy instead of policy rules
- Shows both user and file hierarchies (groups)
- Entire policy on one screen
- Click cell to change policy (direct manipulation interface)
- In user study, Expandable Grids outperformed Windows XP on a variety of tasks

Expandable Grids for Visualizing and Authoring Computer Security Policies [Reeder, Bauer, Cranor, Reiter, Bacon, How, and Strong, CHI 2008]
Conflict resolution

• How can we resolve access control rule conflicts?
Conflict Resolution

• Alice is a member of a group denied access to SECRET.TXT. What happens if I later set a policy rule that Alice should have access to SECRET.TXT?

• Windows: Deny-precedence, deny access

• Expandable Grids: Recency-precedence, allow access
  – Change in conflict-resolution was needed for direct manipulation interface to work
  – One drawback is that it is easy to accidently override exceptions
  – Later version of Expandable Grids used specificity-precedence

• Were the effects of our study due to the grid visualization, the new conflict-resolution method, or both?
User study of Expandable Grids for XP

• Laboratory study

• 2 conditions:
  – (1) Expandable Grids
  – (2) native Windows file permissions interface

• 36 participants, 18 per condition

• 20 tasks per participant

• Training:
  – 3.5 minutes for Grid
  – 5.5 minutes for Windows
Tasks in user study

- Used Teaching Assistant scenario
- 20 total tasks varied by:
  - Size of pre-existing policy
  - Pre-configuration of policy
  - What they asked participant to do
- 2 policy sizes: small and large
  - Small: ~50 principals and ~50 resources
  - Large: ~500 principals and ~500 resources
- 10 different tasks per policy size
- Task order: small size first, then large, but counterbalanced within each size
Tasks in user study

- 10 configurations
  - each used twice, for small and large policies

<table>
<thead>
<tr>
<th>Training</th>
<th>Make simple policy change</th>
</tr>
</thead>
<tbody>
<tr>
<td>View simple</td>
<td>Does user X have write access to file Y?</td>
</tr>
<tr>
<td>View complex</td>
<td>Same, with rule conflict present</td>
</tr>
<tr>
<td>Change simple</td>
<td>Allow user X to have write access to file Y</td>
</tr>
<tr>
<td>Change complex</td>
<td>Make 3 different changes to policy</td>
</tr>
<tr>
<td>Compare groups</td>
<td>Who is in both group A and group B?</td>
</tr>
<tr>
<td>Conflict simple</td>
<td>Make exception for user X in group A</td>
</tr>
<tr>
<td>Conflict complex</td>
<td>Resolve conflict for user X in groups A and B</td>
</tr>
<tr>
<td>Memogate simulation</td>
<td>Does group A have access it shouldn’t?</td>
</tr>
<tr>
<td>Precedence rule test</td>
<td>Give group A, except user X, access to folder Z</td>
</tr>
</tbody>
</table>
Results - errors

• Most common errors in Windows:
  – Not understanding the effective policy
    • Failing to realize deny rules take precedence
    • Failing to notice a relevant rule
    • Failing to check group membership

• Most common errors in Grid:
  – Mistaking one label for another, e.g.,
    • Changing permissions for TAs instead of Students
    • Confusing Opera and Orchestra
  – Mouse slipping off correct column or row
Semantics Study

• Laboratory study
• 3 conditions:
  – Expandable Grid with specificity semantics
  – Expandable Grid with Windows semantics
  – Native Windows file permissions interface
• 54 participants, 18 per condition, novice policy authors
• 10 minutes training for all conditions
• 12 tasks, measured speed and accuracy of task completion

More than skin deep: Measuring effects of the underlying model on access-control system usability
[Reeder, Bauer, Cranor, Reiter, and Vaniea, CHI 2011]
Charles Task

• Charles has just graduated, but is going to come back to sing in the choir with his friends

• Add Charles to the Alumni group, but make sure he can still read the same files in the Choir 1\Lyrics folder that his good friend Carl can read
Results

• Expandable Grid with specificity semantics performed better than Expandable Grid with Windows semantics on most tasks
  – Semantics makes a difference
  – Specificity semantics often helps resolve rule conflicts without removing user from group or changing permissions for entire group
  – But specificity semantics is not always better than Windows

• Changing semantics has effect on usability, regardless of interface
Why usability can’t be just skin deep

• Early system design decisions can impact usability

• Sometimes early UI prototypes and user studies may be needed to understand implications of these decisions on usability

• User studies before designing system can reveal unexpected system requirements

• Usability should be a prime consideration during the formative stages of security system design
Other applications for Expandable Grids

- P3P
- Grey
- Perspective
P3P Expandable Grid

### 1. Access log and cookies
Our Web server collects access logs and cookies. A cookie is a small data file that is transferred to your computer’s hard drive through your web browser when you visit our sites. Cookies enable our systems to recognize your computer, so that we can provide you with personalized information and features. We also use cookies to track user traffic patterns. Retention Time: Indefinitely

<table>
<thead>
<tr>
<th>Types of Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name, address, phone number, etc.</td>
</tr>
<tr>
<td>E-mail address, online contact info</td>
</tr>
<tr>
<td>IDs (not government or financial)</td>
</tr>
<tr>
<td>Information about your purchases</td>
</tr>
<tr>
<td>Financial information</td>
</tr>
<tr>
<td>Information about your computer</td>
</tr>
<tr>
<td>Pages you visited on this website</td>
</tr>
<tr>
<td>Activities you engaged in on this website</td>
</tr>
<tr>
<td>Social and economic categories</td>
</tr>
<tr>
<td>Messages you send us or post on this site</td>
</tr>
<tr>
<td>Cookies and similar mechanisms</td>
</tr>
<tr>
<td>Which groups you might be a member of</td>
</tr>
<tr>
<td>Health-related information</td>
</tr>
<tr>
<td>Information about your tastes or interests</td>
</tr>
<tr>
<td>Exact geographic location</td>
</tr>
<tr>
<td>Social Security numbers and gov't IDs</td>
</tr>
</tbody>
</table>

### 2. Ordering Books and Conferences
We collect information in order to process your purchase. If you register for an ACME conference or sign up for a conference email list, we will send you email announcements and updates about ACME conferences. We collect conference brochures to pass conference attendees. Retention Time: Indefinitely

<table>
<thead>
<tr>
<th>Types of Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name, address, phone number, etc.</td>
</tr>
<tr>
<td>E-mail address, online contact info</td>
</tr>
<tr>
<td>IDs (not government or financial)</td>
</tr>
<tr>
<td>Information about your purchases</td>
</tr>
<tr>
<td>Financial information</td>
</tr>
<tr>
<td>Information about your computer</td>
</tr>
<tr>
<td>Pages you visited on this website</td>
</tr>
<tr>
<td>Activities you engaged in on this website</td>
</tr>
<tr>
<td>Social and economic categories</td>
</tr>
<tr>
<td>Messages you send us or post on this site</td>
</tr>
<tr>
<td>Cookies and similar mechanisms</td>
</tr>
<tr>
<td>Which groups you might be a member of</td>
</tr>
<tr>
<td>Health-related information</td>
</tr>
<tr>
<td>Information about your tastes or interests</td>
</tr>
<tr>
<td>Exact geographic location</td>
</tr>
<tr>
<td>Social Security numbers and gov't IDs</td>
</tr>
</tbody>
</table>
Perspective
Studying Access-Control Usability in the Lab
Lessons Learned from Four Studies

Kami Vaniea
Lujo Bauer
Lorrie F. Cranor
Michael K. Reiter
Proximity displays
We want to know:

- Do proximity displays enable participants to:
  - Notice permission errors
  - Remember permissions
  - Experience no negative effects to non-permission tasks
Methodology goals

• Realistic environment
  – Permissions a secondary task
  – Participant responsibility

• Measuring accuracy
  – Ideal-policy comprehension
  – Effective outcome measurement
## The studies

<table>
<thead>
<tr>
<th></th>
<th>Location</th>
<th>Type</th>
<th>Length</th>
<th>Tasks</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Study 1</td>
<td>Lab</td>
<td>Between-subjects</td>
<td>1 hour</td>
<td>9</td>
<td>26</td>
</tr>
<tr>
<td>Study 2</td>
<td>Lab</td>
<td>Between-subjects</td>
<td>1.5 hour</td>
<td>12</td>
<td>34</td>
</tr>
<tr>
<td>Study 3</td>
<td>Lab</td>
<td>Between-subjects</td>
<td>1.5 hour</td>
<td>15</td>
<td>33</td>
</tr>
<tr>
<td>Study 4</td>
<td>Online</td>
<td>Within-subjects</td>
<td>1 hour</td>
<td>16</td>
<td>600</td>
</tr>
</tbody>
</table>
Photo sharing site

- Photo sharing preferences range from public to personal
- Easy to understand the type of content
- Gallery is an open source photo sharing system
Global Storage Shared Albums

- Around the office
- Project Fair
- Career Development
- People
- New Products
- Conference

**Album info**
- Title: Global Storage Shared Albums
- Owner: Kami Variea

**Popular tags**
- Career development
- Easter
- 2011
- Oakland
- Pittsburgh
- Pirates
- Snowstorm
- 2010
- Vanderbilt Mansion NY

**Available RSS feeds**
- All new comments
- Comments on Global Storage Shared Albums
- Latest photos and movies
Under photo
Common protocol

• Training
  – Rotate, title, permissions, tags, move, delete
• Warm-up tasks
• Information page
• Tasks
• Survey
  – Memory questions
  – Demographics
Information page

Information: Pat's Family

Your parents can barely operate their computer much less manage a photo site. So you let your family post photographs in their own album but you help out by checking each album to make sure it is not visible to everyone on the Internet.

You help your parents manage their photos when they upload new albums. Your mother doesn't understand the photo management software on her computer and tends to make a ton of silly mistakes like once accidentally titling your Dad "Fido". She is a perfectionist and not being able to make her photos look perfect really annoys her so you help her out by fixing up the photographs before she lets her friends and family see anything.

Your mother's name is Samantha and all her photographs can be found in "Samantha Jones's Albums".

Pat’s Family

• Aspect of Pat’s life
• Relationship with people
**Task content**

- Tasks communicated via printed “emails”

**Explicit task components**

To: Pat Jones <pat@jones.com>
From: Mom <samantha@jones.com>
Subject: New albums

Hi Pat,

I just uploaded the Christmas photos at Jennifer’s to my web album. Aunt Sue has been asking about the Christmas photos for months. I’m so glad I finally found time to do this.

I followed the instructions you gave me last time you showed me how to put photos on your photo site but they were so complex I didn’t get through all of them. I’m concerned I might have made a few mistakes. To begin with I think I uploaded some photos from my Mexico vacation into the Christmas album. So could you please go and delete any Mexican vacation photos that look out of place. Also, I think I might have mixed up a few titles.

Could you please go look at the albums and fix any mistakes I might have made? Let me know when you are done so I can email the family so they can see the pictures.

Thanks,
Mom
Chirstmas

Susan and new pillow
# Manage Permissions

Return to Gallery

<table>
<thead>
<tr>
<th></th>
<th>Everybody</th>
<th>Coworkers</th>
<th>Family</th>
<th>Friends</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gallery</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pat Jones's Albums</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Backgrounds</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cats</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Animal Shelter Shared Albums</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dogs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>John Doe's Albums</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Survey

<table>
<thead>
<tr>
<th></th>
<th>True</th>
<th>False</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone can add to the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Anyone can view the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Family can add to the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Family can view the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Coworkers can add to the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Coworkers can view the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Adventure Friends can add to the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Adventure Friends can view the People album.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
Data collected

• Quantitative
  – Post study snapshot of system state (permissions and non-permissions)
  – Survey answers

• Qualitative
  – Screen capture
  – Audio capture
  – Researcher in-session notes
Methodology goals

• Ideal-policy comprehension
• Secondary permission task
• Effective outcome measurement
Why this is hard and important

- Conveying goal without over priming towards security
- SSL studies [Sunshine09, Sotirakopoulos11]
  - Assumed goal “obvious”
  - Participants claimed post-study that they would not ignore at home, but study was “safe”
- Studies want to isolate effectiveness from participant bias
Real policies vs Role playing

- Observer effect (physics)
- Asking participants what their ideal policy is changes their behavior and their answers are impacted by recent behavior
- Users’ ideal policies change over time [Mazurek ‘08]
- In role playing ground truth is known
Security as a secondary task

Benefits

• Study based
  – Hawthorn effect
  – Sense of accomplishment

• Real world
  – Sense of safety

Costs

• Time required to check permissions
  – Opportunity cost

• Cognitive load switch
  – Distract primary task
Issues like sideways photos, misspelled titles, or blurry photos really bother you so you fix them when ever you see them.

1. No spelling errors
2. Albums are tagged with the name of the friend or family member who took the photos.
3. Photos are not sideways.
4. Family albums can only be viewed by Family, and friend albums can only be viewed by Friends.
5. No blurry photos.
6. Pat can view, add, and edit all albums.

You have completed the training for this website. Next, you, as Pat Jones, will be shown a sequence of eight emails from your friends and family asking you to do photo management tasks. Respond to the emails by making any changes on the photo sharing site that you consider to be appropriate based on the email and the information below.

**Pat Jones**

You maintain an online photo website where you upload and share all your personal photos with family and friends. You set up your friends and family create new albums on your site but you make sure that all albums are tagged with the name of the photographer. You care that all the photos on your website look good. Issues like sideways photos, misspelled titles, or blurry photos really bother you so you fix them whenever you see an issue.

**Instructions**

Your sister is concerned for her kid's safety she asks you to not put photos of their kids on any albums visible to non-Family.
We want to know:

Do proximity displays enable participants to:

• **Notice** permission errors
• Remember permissions
• Experience no negative effects to non-permission tasks
Why this is hard and important

• Measuring perception
• Use self reporting
• Assume participant will react and measure the reaction
• Not all reactions are immediate
We started by defining:

We counted a permission error as being noticed iff corrected

Did not quite work
Next step

• Think aloud
• Eye tracker
Noticing re-defined

We counted a permission error as being noticed iff permissions *checked*

• Permission modification interface opened

• Verbally read permissions

• Non-verbal reading behavior
Eye tracker
Eye tracker

Experimental: Looking at the proximity display

Fixations vs. Percent time on page
Noticing re-defined

We counted a permission error as being noticed iff permissions checked

• Permission modification interface opened
• Verbally read permissions
• Non-verbal reading behavior
Eye tracker

• Over estimate “notice”
  – “Fixations” not the same as participant processing the information

• Experimental participants look at proximity displays throughout the task
  – However they “check” permissions only at the beginning or end
Re-re-defining noticing

We counted a permission error as being noticed iff corrected