27 – Access control and policy configuration

Lujo Bauer, Nicolas Christin, and Abby Marsh

April 20, 2016

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security
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.”

http://www.flickr.com/photos/an0nym0usmuse/288944380/
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
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

![Image of Four-part Harmony.doc Properties dialog boxes]
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. Click on “Users”
2. Double-click Jana
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
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
Key insight: Center policy-authoring user interfaces around a display of the whole effective policy, not a list of rules.
Solution: Expandable Grids
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>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
<td>Make simple policy change</td>
</tr>
<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>
### Study Results: Grid vs Windows

<table>
<thead>
<tr>
<th>Task type</th>
<th>Small-size Accuracy</th>
<th>Time</th>
<th>Large-size Accuracy</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>View simple</td>
<td>Grid: 89%</td>
<td>69s</td>
<td>Windows: 56%</td>
<td>56s</td>
</tr>
<tr>
<td></td>
<td>Grid: 94%</td>
<td>29s</td>
<td>Windows: 61%</td>
<td>64s</td>
</tr>
<tr>
<td>View complex</td>
<td>Grid: 89%</td>
<td>35s</td>
<td>Windows: 17%</td>
<td>55s</td>
</tr>
<tr>
<td></td>
<td>Grid: 100%</td>
<td>39s</td>
<td>Windows: 100%</td>
<td>39s</td>
</tr>
<tr>
<td>Change simple</td>
<td>Grid: 29s</td>
<td>61s</td>
<td>Windows: 56%</td>
<td>56s</td>
</tr>
<tr>
<td></td>
<td>Grid: 30s</td>
<td>61s</td>
<td>Windows: 52s</td>
<td>52s</td>
</tr>
<tr>
<td>Change complex</td>
<td>Grid: 61%</td>
<td>70s</td>
<td>Windows: 0%</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>Grid: 72s</td>
<td>Insufficient data</td>
<td>Windows: 78%</td>
<td>100%</td>
</tr>
<tr>
<td>Compare groups</td>
<td>Grid: 67%</td>
<td>39s</td>
<td>Windows: 83%</td>
<td>103s</td>
</tr>
<tr>
<td></td>
<td>Grid: 100%</td>
<td>39s</td>
<td>Windows: 103s</td>
<td>103s</td>
</tr>
<tr>
<td>Conflict simple</td>
<td>Grid: 67%</td>
<td>55s</td>
<td>Windows: 61%</td>
<td>100s</td>
</tr>
<tr>
<td></td>
<td>Grid: 52s</td>
<td>55s</td>
<td>Windows: 100%</td>
<td>100s</td>
</tr>
<tr>
<td>Conflict complex</td>
<td>Grid: 89%</td>
<td>29s</td>
<td>Windows: 0%</td>
<td>103s</td>
</tr>
<tr>
<td></td>
<td>Grid: 94s</td>
<td>29s</td>
<td>Windows: 100%</td>
<td>103s</td>
</tr>
<tr>
<td>Memogate simulation</td>
<td>Grid: 20s</td>
<td>Insufficient data</td>
<td>Windows: 52s</td>
<td>Insufficient data</td>
</tr>
<tr>
<td>Precedence rule test</td>
<td>Grid: 89%</td>
<td>42s</td>
<td>Windows: 94%</td>
<td>115s</td>
</tr>
<tr>
<td></td>
<td>Grid: 94%</td>
<td>42s</td>
<td>Windows: 78%</td>
<td>118s</td>
</tr>
</tbody>
</table>
But… 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?
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
Semantics Study: Results

1. Does semantics make a difference?  
   YES

2. Does specificity help resolve rule conflicts?  
   YES

3. Is specificity semantics always better than Windows?  
   NO
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**