Access control
and policy configuration,
tools for security administration

Norman Wu, Ziwei Hu
Outline

Access control introduction
Demos of different access control systems
A quick look at papers
Other aspects of AC beyond required reading
Usability problems of access control
Class discussion on conflict AC rules
Introduction
Access control is the selective restriction of access to resource. [1]

Its function is to control which principals (persons, processes, machines, ...) have access to which resources in the system — which files they can read, which programs they can execute, how they share data with other principals, and so on.[2]
Common access control mechanisms
Scenarios & Demo

- Physical Access Control
- File System Access Control
- Photo Sharing
- File Sharing
Physical Access Control
Windows: File System Access Control
Facebook: Photo Sharing

Share This Photo

Share: On your own timeline

Write something...

From the album: Timeline Photos
By Tianqi Tong
White House

Only Me Share Photo Cancel

Public
Friends

Only Me
Custom
CMU
The Second High School Attached to Beijing Normal U
Baidu
See all lists...
Google Doc: File Sharing

Sharing settings

Link to share (only accessible by collaborators)

https://docs.google.com/presentation/d/11_VquaejCrzCCe6WcwoqXHTREfGQ58KxeR

Share link via: 📥➡️➡️➡️➡️

Who has access

Shared with specific people - Only the people listed below can access

Ziwei Hu (you) ziweihuocmu@gmail.com
Luo Wu luow.cmu@gmail.com

Invite people:

Can edit

Send Cancel

Send a copy to myself

Editors will be allowed to add people and change the permissions. [Change]
A naive access control system

PC data access control system based mobile phone, 2011
Typical Mechanisms

• Access groups and roles
• Access control list
Access groups

Role-Based Access Control (RBAC)

• Information will be repeatedly shared with that particular group
• Group membership information is normally visible to all members of an organization
• Lack of transparency
Access Control List

• Store the access control matrix a column at a time, along with the resource to which the column refers.
• ACLs are suited to environments where protection is data-oriented
• ACLs are less suited where the user population is large and constantly changing
Some of the slides in this section are stolen from Prof. Lorrie, Lujo and Reb’s paper and lecture slides.
Policy configuration on Grey

- Smartphone-based, end-user-driven access-control system for physical and virtual resources
- Deployed in CMU’s Collaborative Innovation Center
  - Approximately 40 Grey-capable doors and 60+ users at the moment
How the policy in grey works

Grey: An Example Scenario

- Lujo’s students are allowed in 2121
- Faculty are allowed in 2121
- At CMU, Lujo’s secretary speaks on behalf of Lujo

---

Lujo's Office, 2121

Lujo

I need to grade the midterms for Lujo’s class

Scott

Lujo must authorize access
How the policy in grey works

Grey: An Example Scenario

Scott is a student.

1. Hi, Please open 2121
2. Prove Lujo says open 2121
3. Prove Scott says open 2121 → Lujo says open 2121
4. Proof of Scott says open 2121 → Lujo says open 2121
5. Proof of Lujo says open 2121

This is Lujo’s belief. I’ll ask Lujo for help.

Generate credential stating Scott’s desire to open 2121
How to make configuration correct

Setting up policies takes effort

Incorrectly set up policies can allow or deny access

How to help user easily set up correct policies
How to make configuration correct

Mechanism involves two steps:

1. Identifying *intended policy* and *misconfigurations* in the *implemented policy*
2. Resolving misconfigurations by augmenting the implemented policy

“Misconfiguration” refers to authority that is intended to exist but has not been given
Tools for security administration

2nd worst Windows UI of all time

Rob Reeder
Sr. Research Scientist, Google
Scenario: You are a TA in a Music Department and have to maintain the department file server

Task: 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 can the file in the folder.
Jana setup

Jana is a TA “this” year (did the study in 2007)

Is in the group

Jana was a TA last year

Is in the group

2007 TAs are allowed READ & WRITE
2006 TAs are denied READ & WRITE
Since Jana is in both groups, she is denied access
Learn Jana’s effective permissions

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

Bring up Computer Management interface

Click on “Users”

Double-click Jana

Click “Member Of”

Read Jana’s group membership

TAS 2009

TAS 2009
Learn Jana’s group membership

10. Click on TAs 2006

11. Read permissions for TAs 2006

12. Read permissions for TAs 2007

13. Click on TAs 2007
Change Jana’s groups’ permission

14
Click on TAs 2006

15
Change permissions for TAs 2006
Check Jana’s permission

16. Click “Advanced”
17. Click “Effective Permissions”
18. Select Jana
19. View Jana’s Effective Permissions
Solution: Expandable grid
Solution: Expandable grid
## Result: Grid vs Windows

<table>
<thead>
<tr>
<th>Task type</th>
<th>Small-size</th>
<th></th>
<th></th>
<th>Large-size</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Accuracy</td>
<td>Time</td>
<td></td>
<td>Accuracy</td>
<td>Time</td>
</tr>
<tr>
<td>View simple</td>
<td></td>
<td>89%</td>
<td>29s</td>
<td>61%</td>
<td>42s</td>
<td></td>
</tr>
<tr>
<td>View complex</td>
<td></td>
<td>94%</td>
<td>35s</td>
<td>100%</td>
<td>39s</td>
<td></td>
</tr>
<tr>
<td>Change simple</td>
<td></td>
<td>89%</td>
<td>30s</td>
<td>100%</td>
<td>50s</td>
<td></td>
</tr>
<tr>
<td>Change complex</td>
<td></td>
<td>61%</td>
<td>70s</td>
<td>67%</td>
<td>100s</td>
<td></td>
</tr>
<tr>
<td>Compare groups</td>
<td></td>
<td>89%</td>
<td>39s</td>
<td>100%</td>
<td>111s</td>
<td></td>
</tr>
<tr>
<td>Conflict simple</td>
<td></td>
<td>67%</td>
<td>55s</td>
<td>72%</td>
<td>73s</td>
<td></td>
</tr>
<tr>
<td>Conflict complex</td>
<td></td>
<td>89%</td>
<td>29s</td>
<td>100%</td>
<td>52s</td>
<td></td>
</tr>
<tr>
<td>Memogate simulation</td>
<td></td>
<td>100%</td>
<td>20s</td>
<td>94%</td>
<td>105s</td>
<td></td>
</tr>
<tr>
<td>Precedence rule test</td>
<td></td>
<td>89%</td>
<td>42s</td>
<td>78%</td>
<td>71s</td>
<td></td>
</tr>
</tbody>
</table>
But... The grid changed conflict-resolution method to recency-takes-precedence

Were the effects of original study due to the new visualization idea, the new conflict resolution method, or both?

Ran another study to find out

More than Skin Deep
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
Semantics study: result

1. Does semantics make a difference?  
   YES!

2. Does specify help resolve rules conflicts  
   YES!

3. Is specificity semantics always better than Windows  
   NO!
Changing semantics has effect on usability, regardless of interface.
Usability problems
Usability problems

- Permission errors
  - Only discovered at the time access is really needed
- Lack of transparency
  - Unaware of the actual membership of a group
- Conflict rules
Discussion
Access control conflict rules

Scenario: You are a TA in a Music Department and have to maintain the department file server

Jana comes back to pursue her master degree at Carnegie Mellon University and once again become a TA for Theory 101 in 2014.

In 2014, TA are only allowed to READ but not WRITE.

How would you resolve the conflict in access control rules under Windows and Grid?

Recall:
2007 TAs are allowed READ & WRITE
2006 TAs are denied READ & WRITE
[1] RFC 4949