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

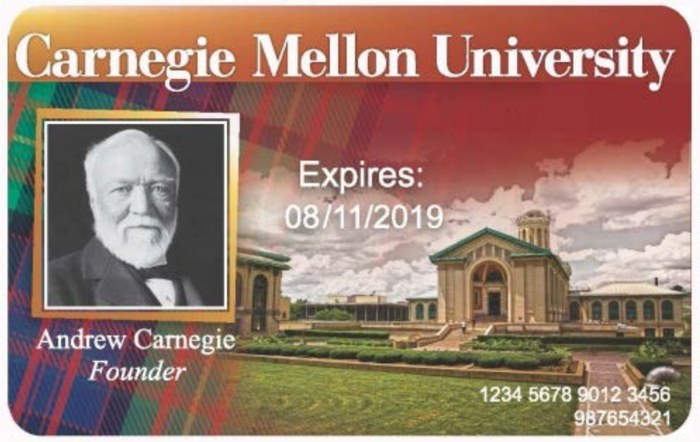
Introduction

Access control definition

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

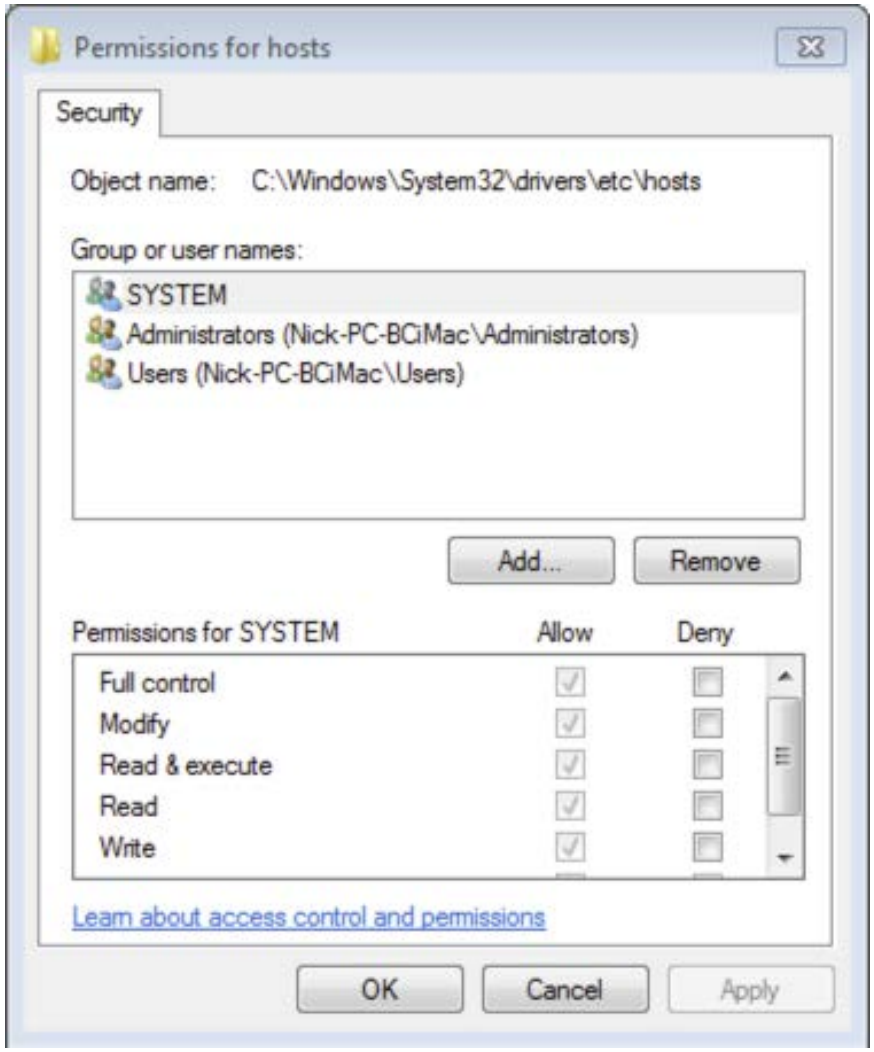


Scenarios & Demo

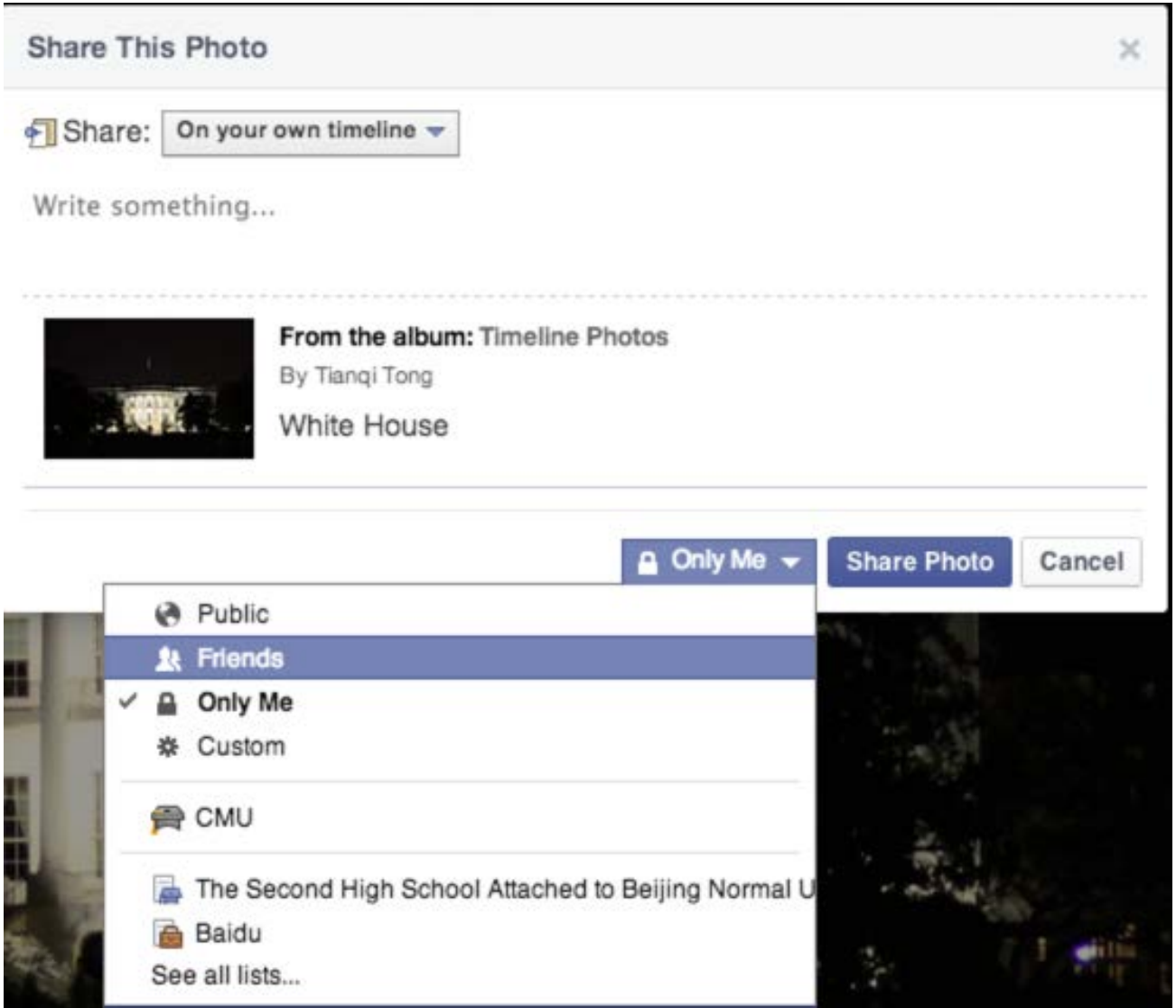
- Physical Access Control
- File System Access Control
- Photo Sharing
- File Sharing

Physical Access Control

Windows: File System Access Control



Facebook: Photo Sharing



Google Doc: File Sharing

Sharing settings

Link to share (only accessible by collaborators)

https://docs.google.com/presentation/d/11_VquaejCrzCCe6WcwqXHTREfGQ58KxeR

Share link via:

Who has access

Shared with specific people - Only the people listed below can access — Change...

Ziwei Hu (you) ziweihucmu@gmail.com — Is owner

Luo Wu luow.cmu@gmail.com — Can edit

Invite people:

fr

Friends (group)

Can edit

via email - Add message

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

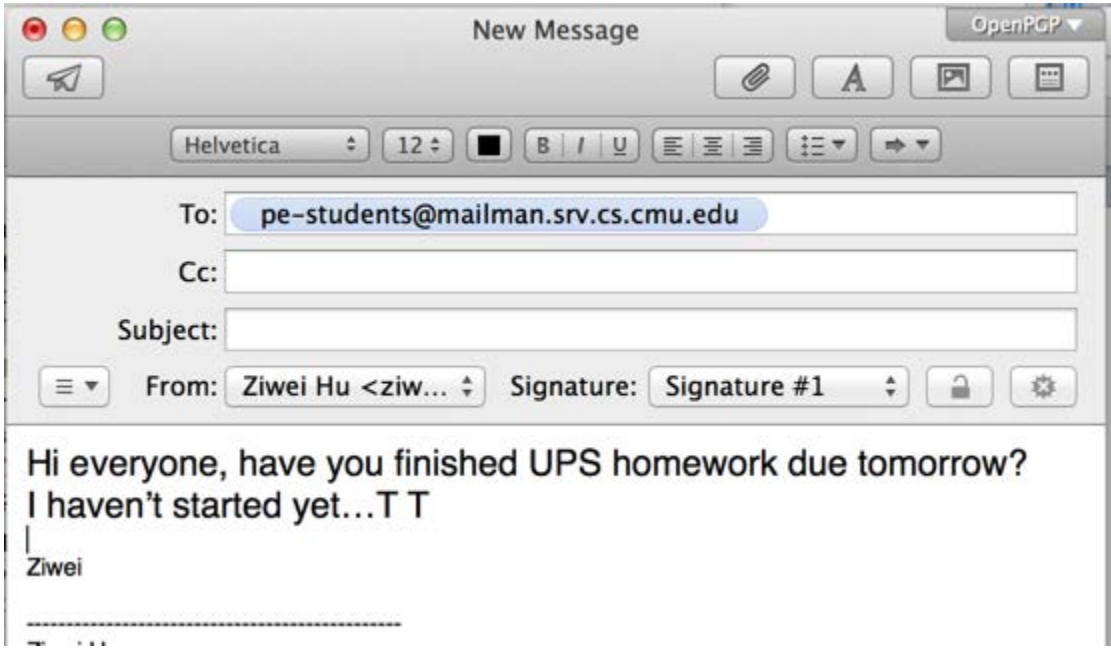
Typical Mechanisms

- 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

Vivian — bash — 73×13

bash

```
Ziweis-MacBook-Pro:~ Vivian$ ls -l
total 32
drwxr-xr-x    4 Vivian  staff   136 Mar 22 15:44 Applications
drwx------+  22 Vivian  staff   748 Apr 14 16:15 Desktop
drwx------+  32 Vivian  staff  1088 Apr  8 16:03 Documents
drwx------+ 259 Vivian  staff  8806 Apr 14 16:21 Downloads
drwx------@  15 Vivian  staff   510 Apr 11 15:38 Dropbox
drwxr-xr-x    3 Vivian  staff   102 Oct 13  2013 ISaP_Project
drwxr-xr-x    5 Vivian  staff   170 Feb 26 23:28 IdeaProjects
drwx------@  68 Vivian  staff  2312 Feb 27 21:43 Library
drwx------+   3 Vivian  staff   102 Aug  1  2013 Movies
drwx------+   5 Vivian  staff   170 Aug 16  2013 Music
drwxr-xr-x    4 Vivian  staff   136 Mar 27 16:05 NetBeansProjects
```

Papers

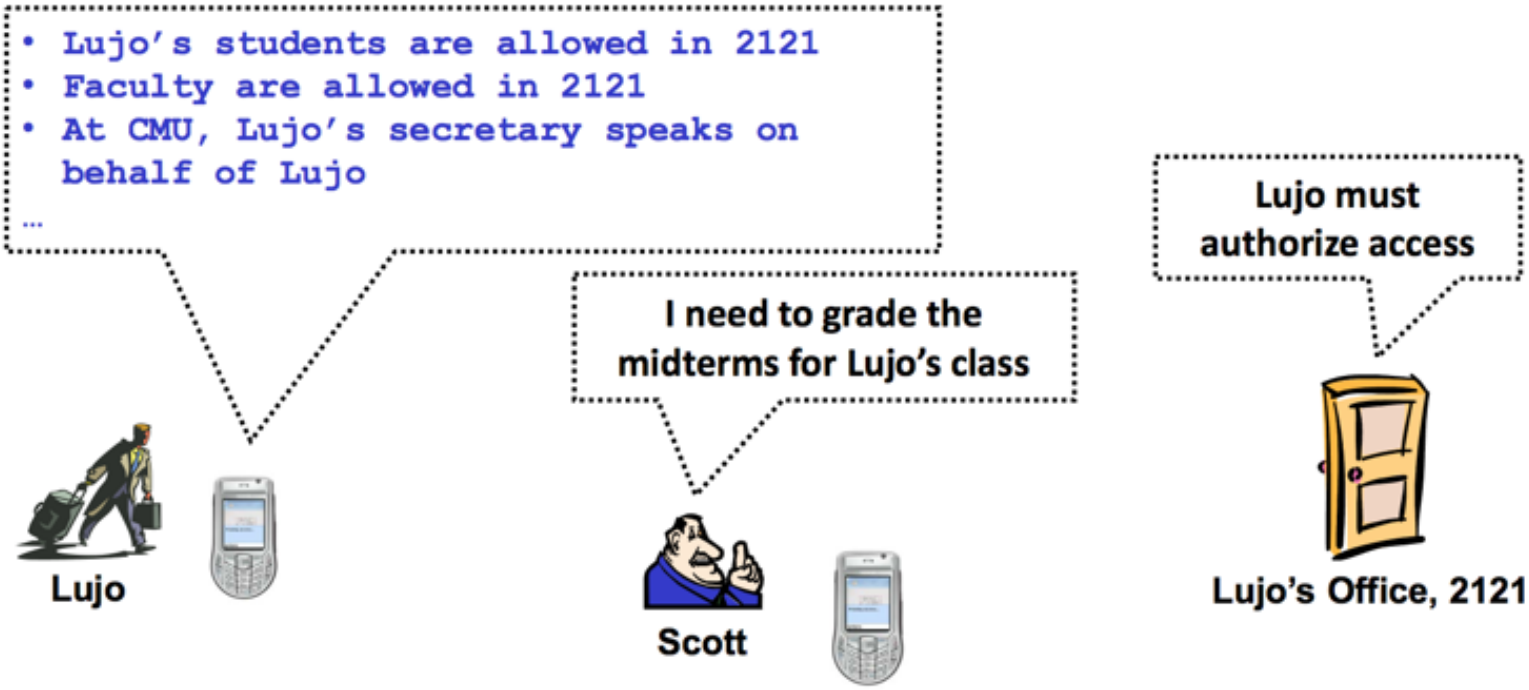
Some of the slides in this section are stolen from Prof. Lorrie, Lujo and Reb’s paper and lecture slides.

Policy configuration on Grey

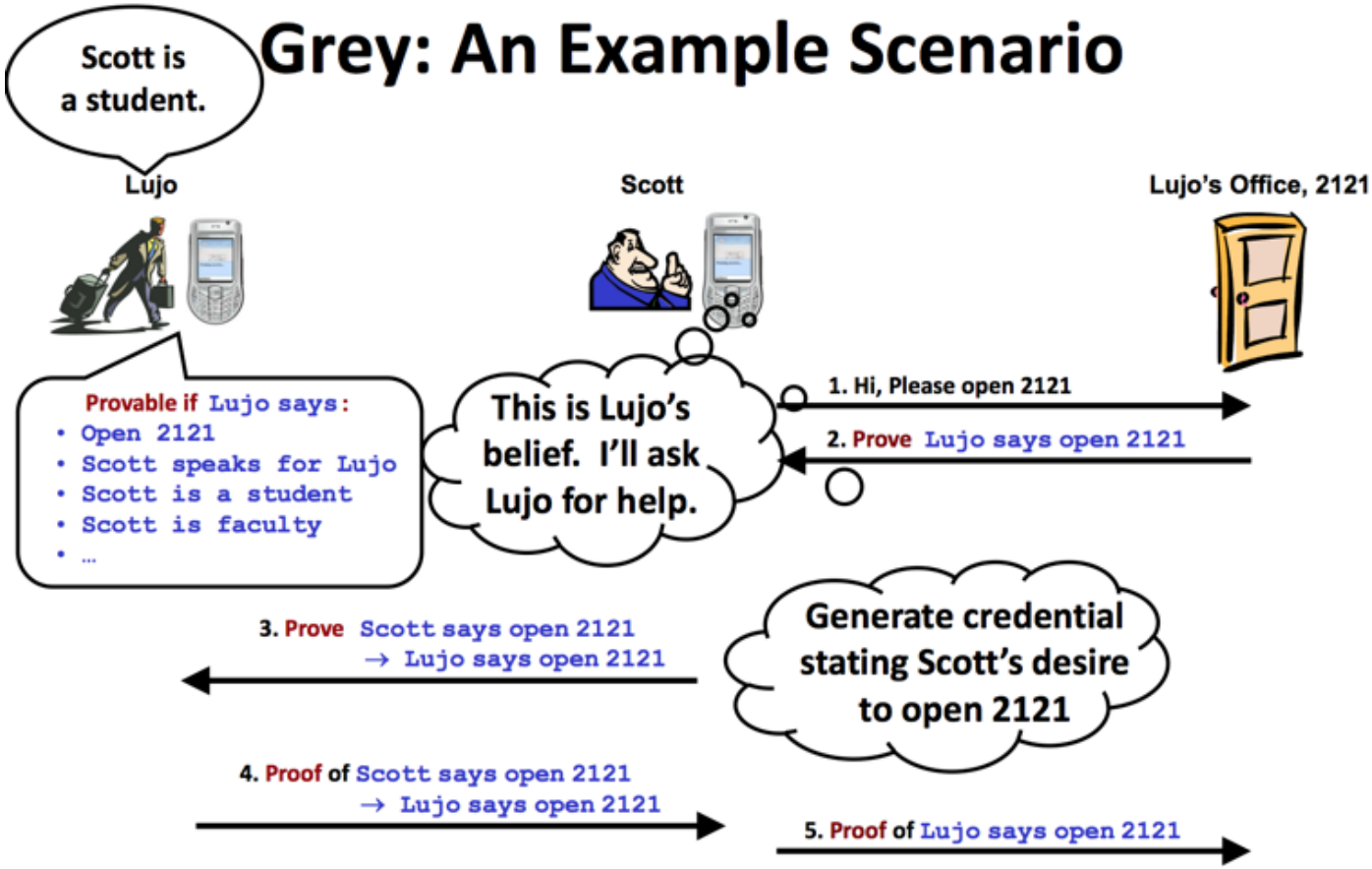
- **Smartphone-based, end-user-driven access-control system for physical and virtual resources**
- **Deployed in CMU's Collaborative Innovation Center**
  - Approximately 40 Grey-capable doors and 60+ users at the moment

How the policy in grey works

Grey: An Example Scenario



How the policy in grey works



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

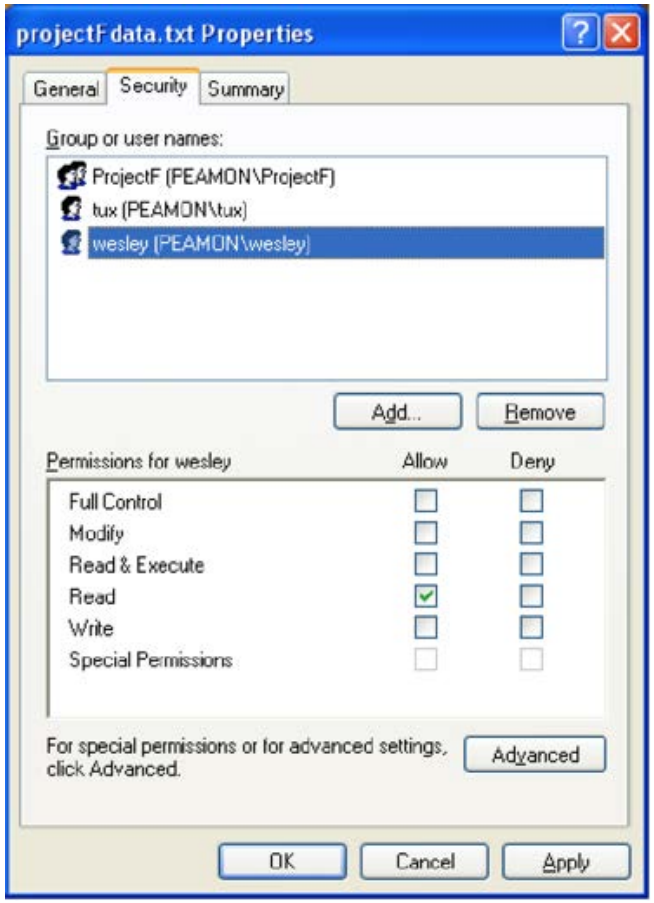
Mechanism involves two steps:

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

Example: Jana

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

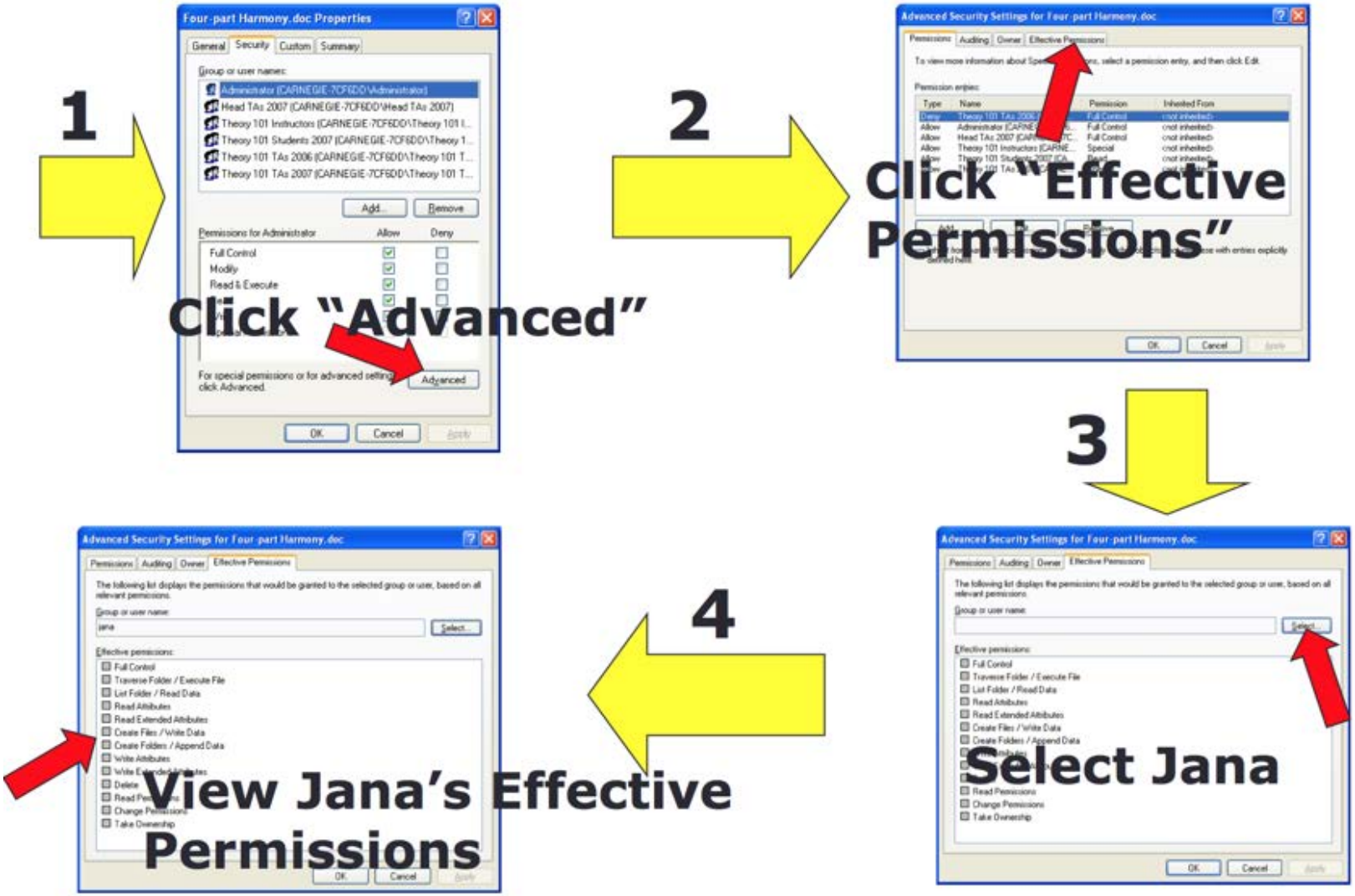
- Is in the group

2007 TAs are allowed READ & WRITE

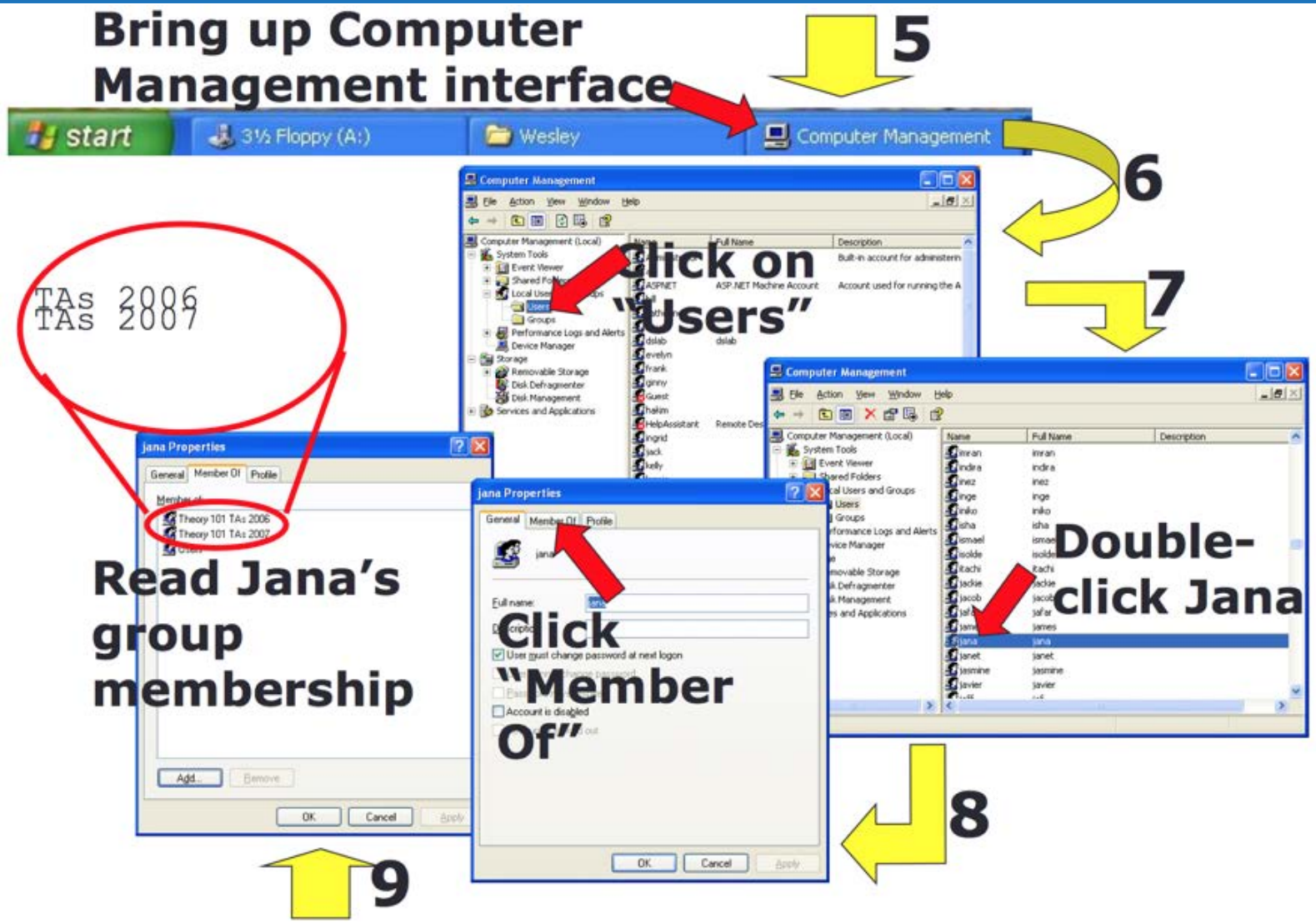
2006 TAs are denied READ & WRITE

Since Jana is in both groups, she is denied access

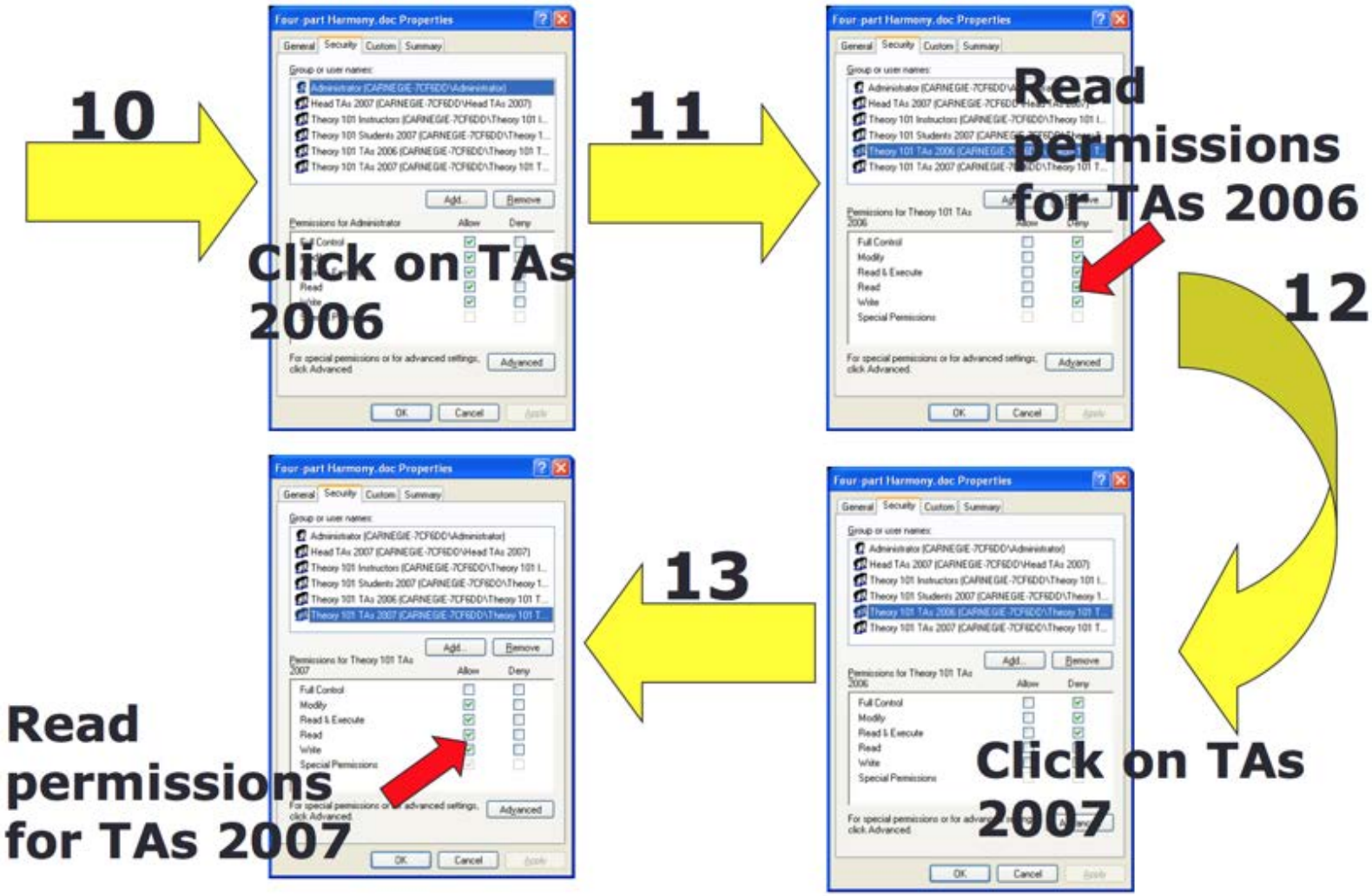
Learn Jana's effective permissions



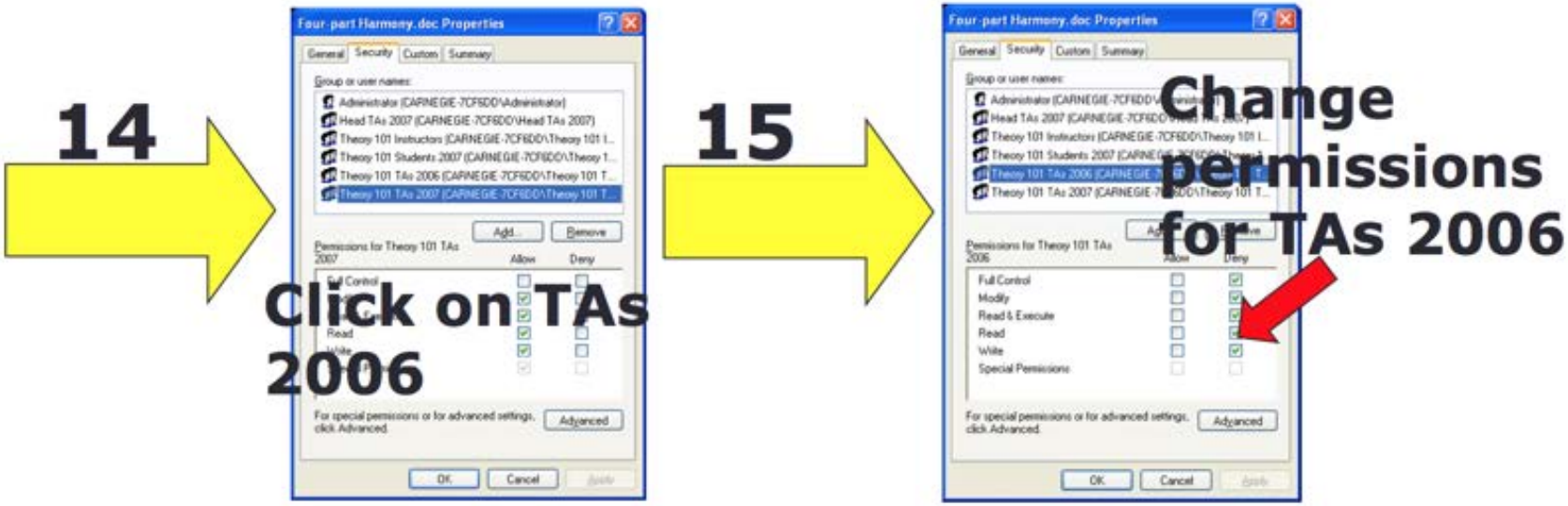
Learn Jana's group membership



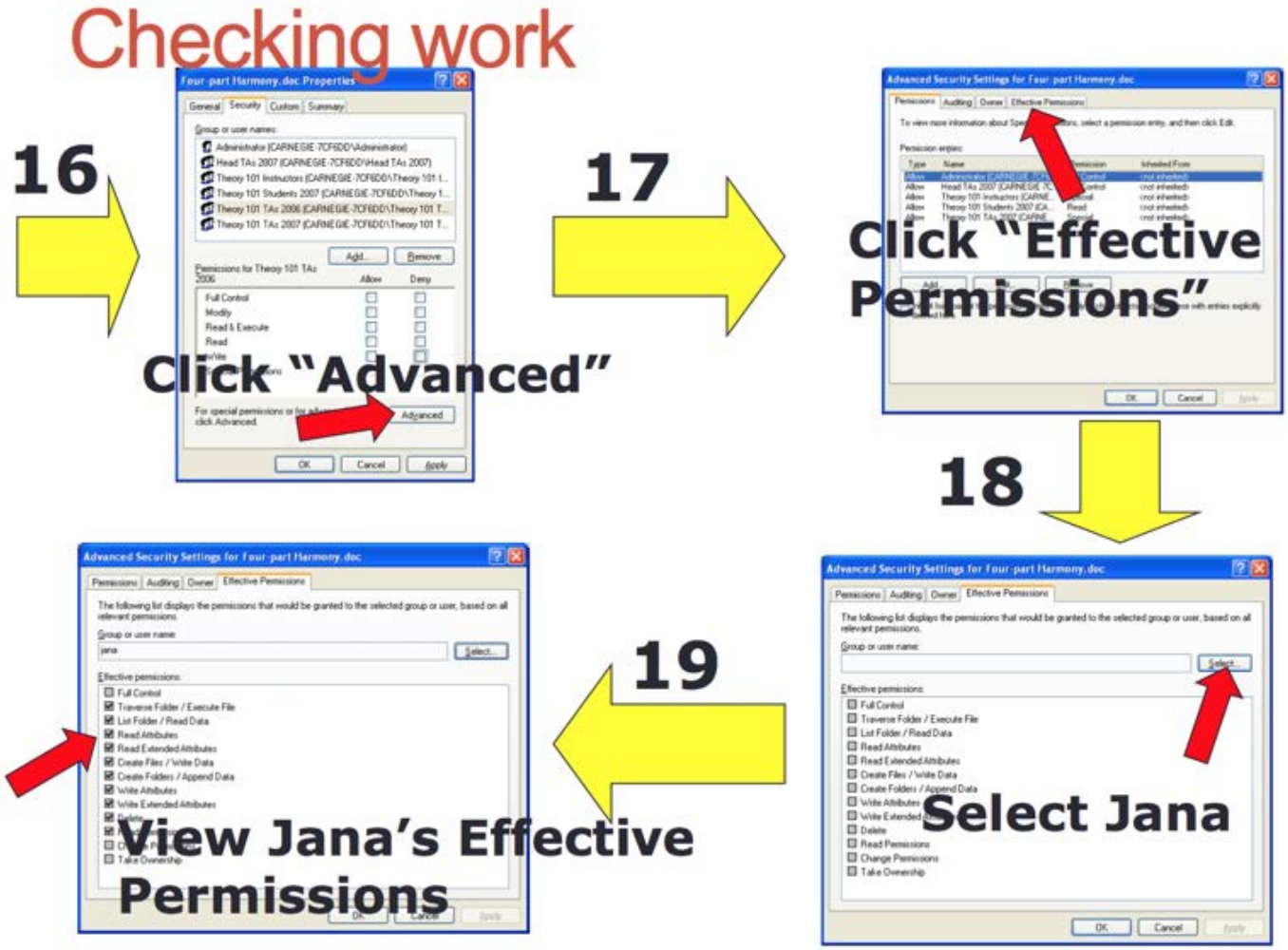
Learn Jana's group membership



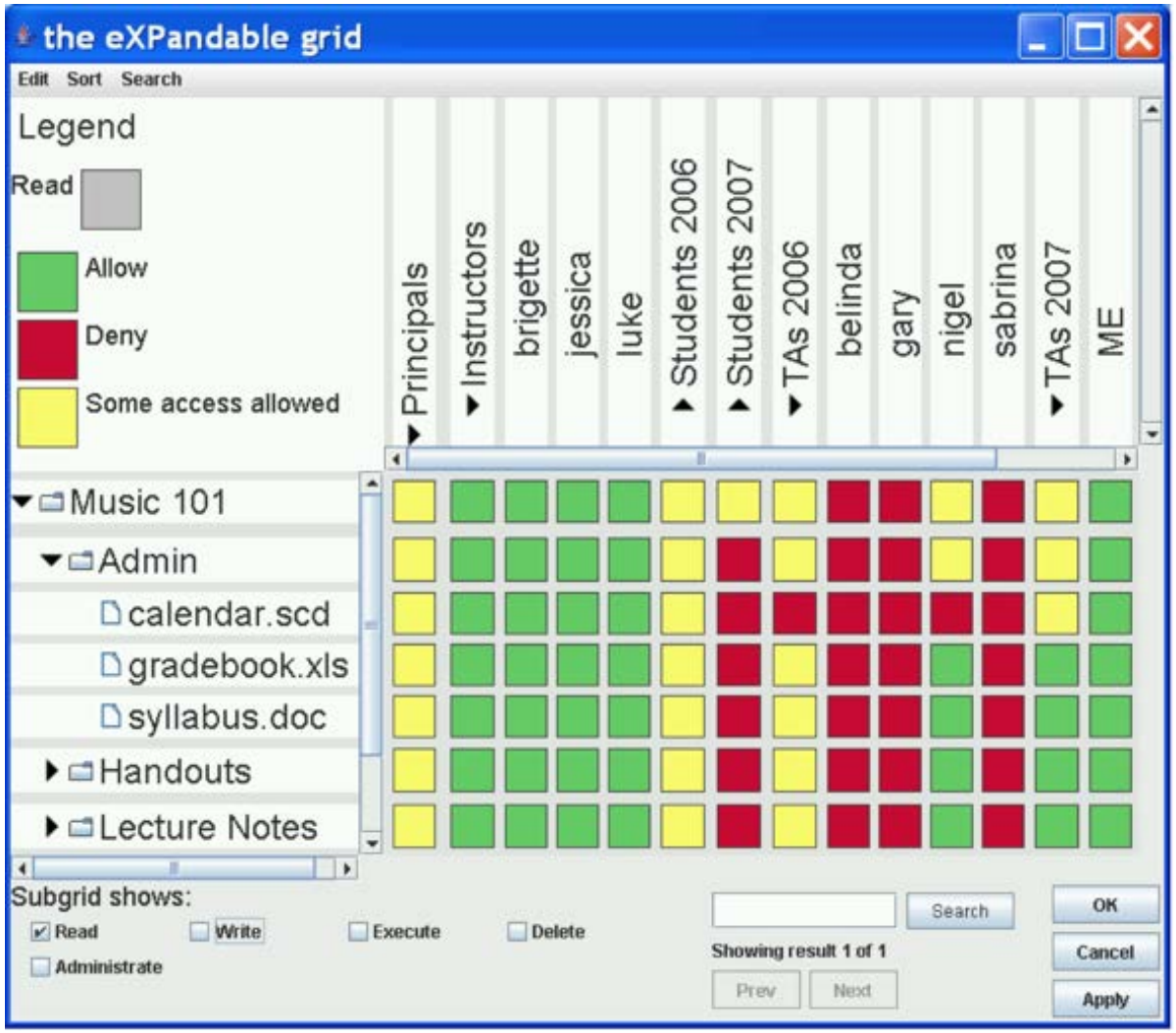
Change Jana's groups' permission



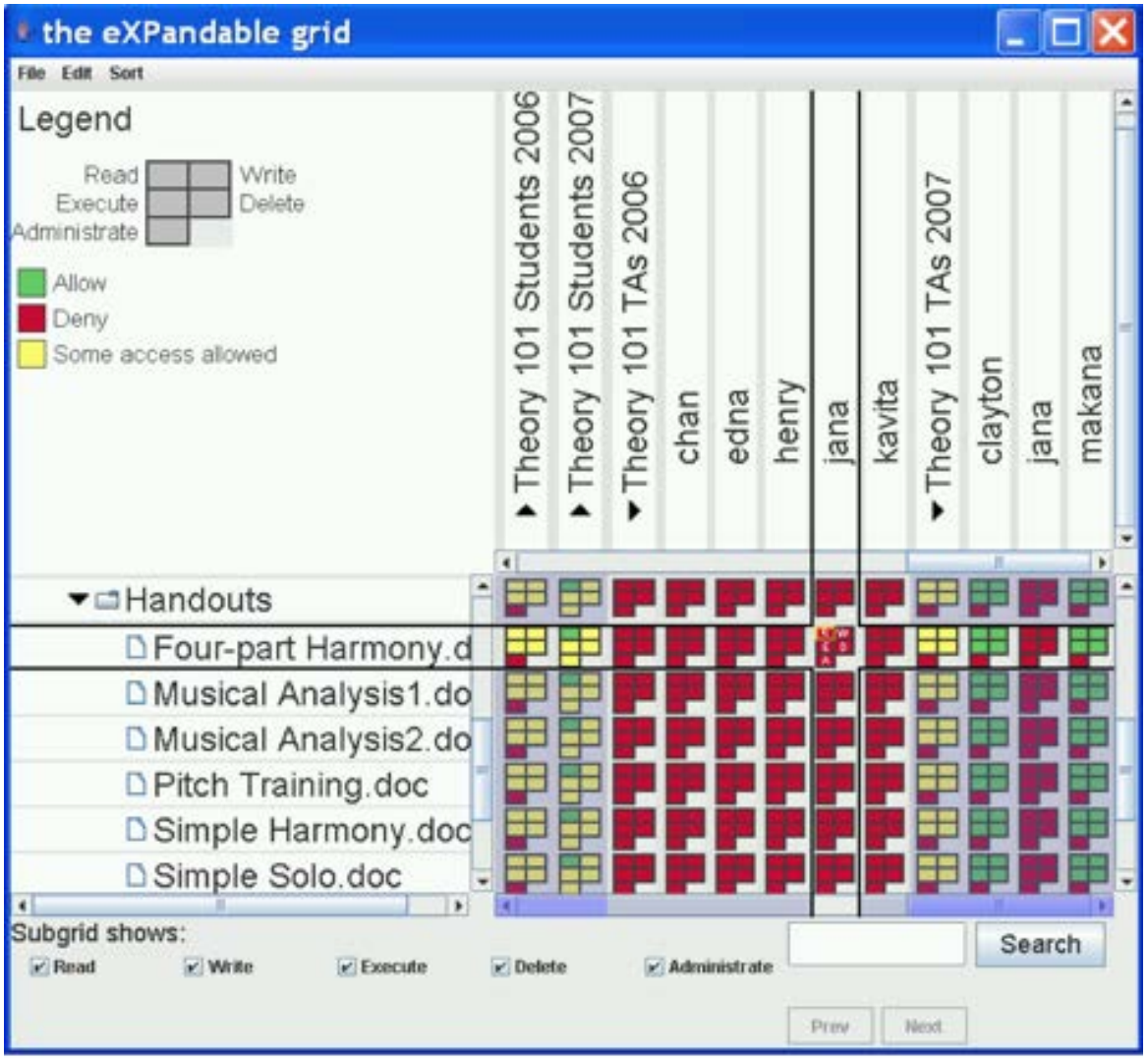
Check Jana's permission



Solution: Expandable grid



Solution: Expandable grid



Result: Grid vs Windows

Grid / Windows	Small-size		Large-size	
Task type	Accuracy	Time	Accuracy	Time
View simple	89% / 56%	29s / 64s	61% / 56%	42s / 61s
View complex	94% / 17%	35s / 55s	100 / 39%	39s / 67s
Change simple	89% / 94%	30s / 52s	100 / 100	50s / 42s
Change complex	61% / 0%	70s / Insufficient data	67% / 17%	100s / 143s
Compare groups	89% / 83%	39s / 103s	67% / 83%	111s / 126s
Conflict simple	67% / 61%	55s / 103s	72% / 61%	73s / 104s
Conflict complex	89% / 0%	29s / Insufficient data	100 / 6%	52s / Insufficient data
Memogate simulation	100% / 94%	20s / 66s	94% / 78%	105s / 116s
Precedence rule test	89% / 94%	42s / 118s	78% / 78%	71s / 115s

Study result: conflict resolution

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

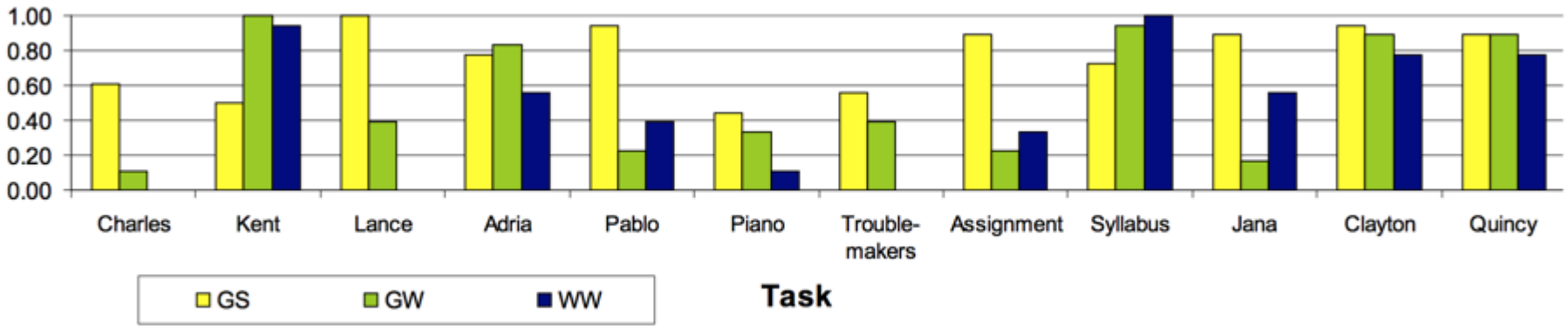
Laboratory study

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!**

Summary of More than Skin Deep

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

Reference

[1] RFC 4949

[2] Ross Anderson. Chapter 4: Access Control In *Security Engineering* (Second Edition). Wiley, 2008.