Lecture 17: Usable Access Control

CS 181W

Fall 2022

Where we were…

- **Authentication:** mechanisms that bind principals to actions
- **Authorization:** mechanisms that govern whether actions are permitted

Access Control Policy

- An **access control policy** specifies which of the **operations** associated with any given **object** each **principal** is authorized to perform

- Expressed as a relation $Auth$:

$Auth$		Objects	
		dac.tex	dac.pptx
principals	ebirrell	r,w	r,w
	drdave	r	r
	studenta		r

Access Control Mechanisms

- A **reference monitor** is consulted whenever one of a predefined set operations is invoked
  - operation $\langle P, O, op \rangle$ is allowed to proceed only if the invoker P is authorized to perform op on object O
- Can enforce **confidentiality** and/or **integrity**

- **Assumption:** Predefined operations are the sole means by which principals can learn or update information.
- **Assumption:** All predefined operations can be monitored (complete mediation).

Access control examples

- Door locks

- File access
- Computer system access

- Social network settings
- Smartphone app permissions
- Notification settings (e.g. iOS, Slack)

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

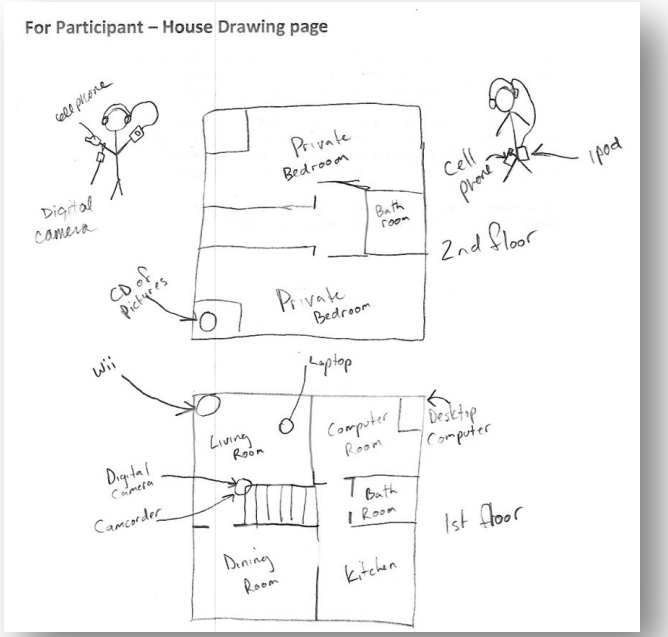
Access Control for Home Data Sharing: Attitudes, Needs and Practices [Mazurek, Arsenault, Bresee, Gupta, Ion, Johns, Lee, Liang, Olsen, Salmon, Shay, Vaniea, Bauer, Cranor, Ganger, and Reiter, CHI 2010]

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

- Draw a map of your home (may be dorm room, parents' house, etc.)
- Mark which rooms/areas/devices you consider private



- What rules (formal or informal) or policies do you have about who can access private rooms/areas/devices/files?

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

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
  - “Wouldn’t want my boss to see me in my swimsuit.”
  - Ok with boss seeing photo dancing on a table, “he’s seen me do it in person”

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."

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

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

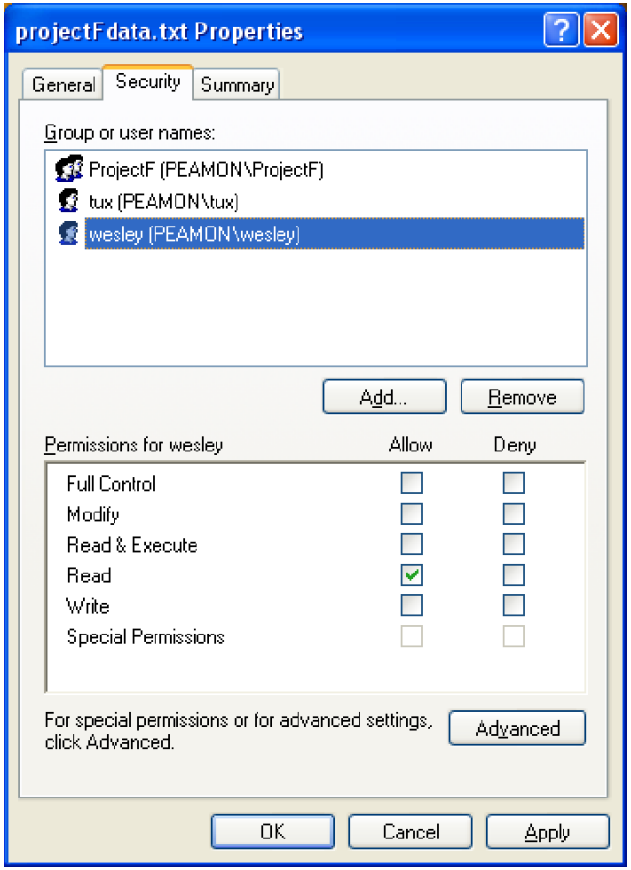
  "I'm very willing to be open with people, I think I'd just like the courtesy of someone asking me."
- People want to know both who is accessing files and why
- People want to review accesses, revise policy
- We conducted a follow-up study on reactive access control

Mazurek, Klemperer, Shay, Takabi, Bauer, and Cranor. Exploring reactive access control. CHI 2011.

File system access control

- Access control on Windows file systems often incorrect
- Access control is difficult because it has no holistic view of effective file permissions, and conflict resolution is complicated
- Example: Mistakenly misconfigured server used by both Republican and Democrat staffers led to 2003 “Memogate” scandal

Problem: Rule-centered interfaces



Why is 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 rules applies?
- Scale
  - Large policies can get tricky

Example task: Jana

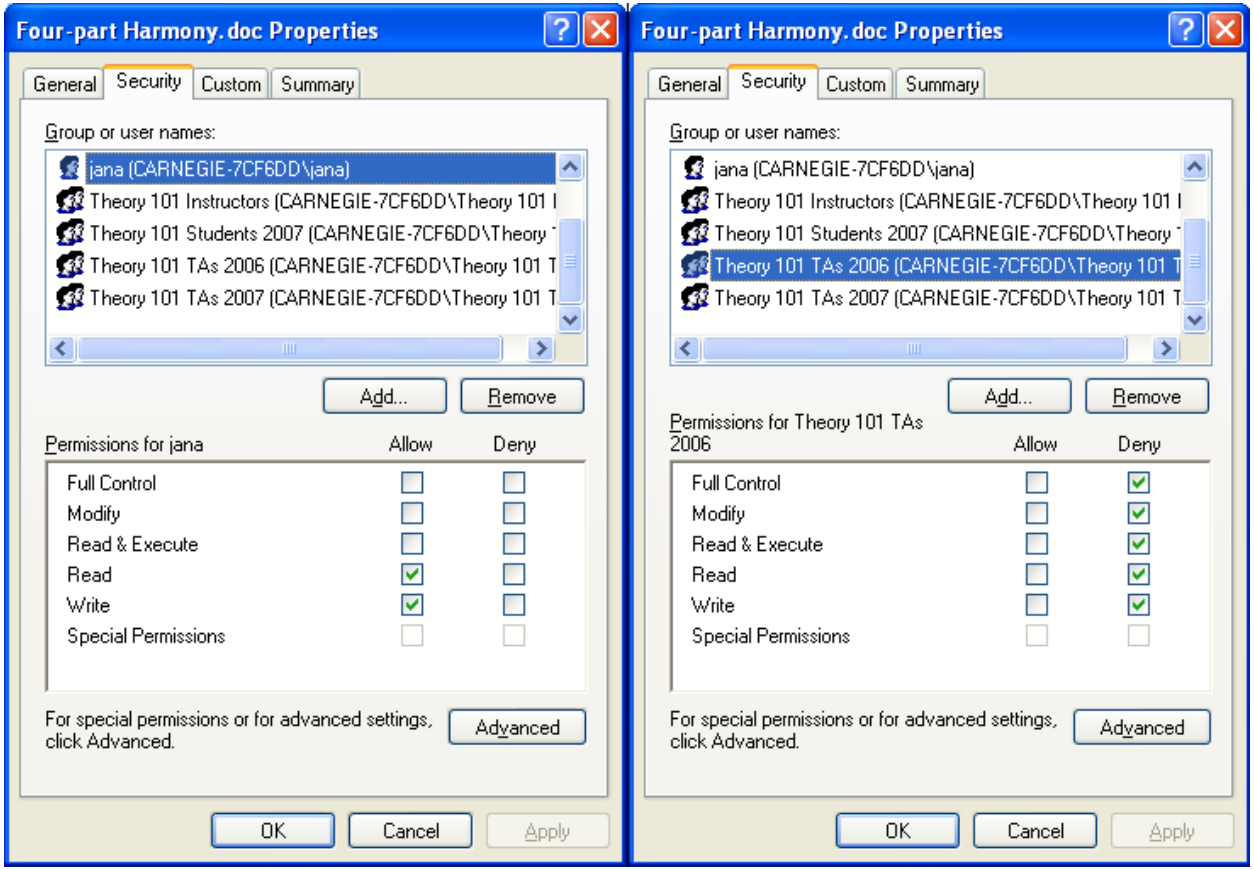
Jana, a CS 101 TA, complained that when she tried to change the Four-part Harmony handout to update the assignment, she was denied access.

Set permissions so that *Jana* can *read and write* the *Four-part Harmony.doc* file in the *Theory 101\Handouts* folder.

Jana setup

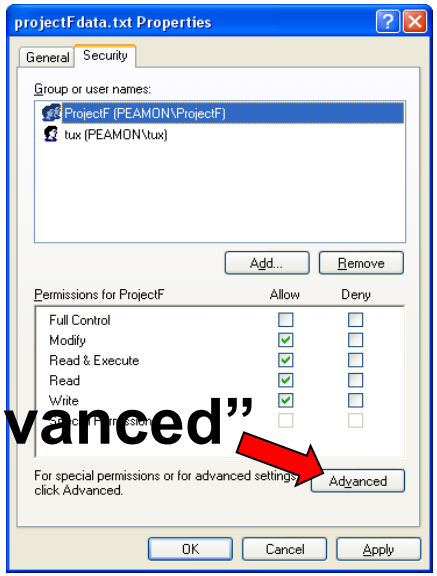
- Jana is a TA this year
  - Is in the group *Theory 101 TAs 2007*
- Jana was a TA last year
  - Is in the group *Theory 101 TAs 2006*
- 2007 TAs are allowed READ & WRITE
- 2006 TAs are denied READ & WRITE
- Since Jana is in both groups, she is denied access

Jana task – common error



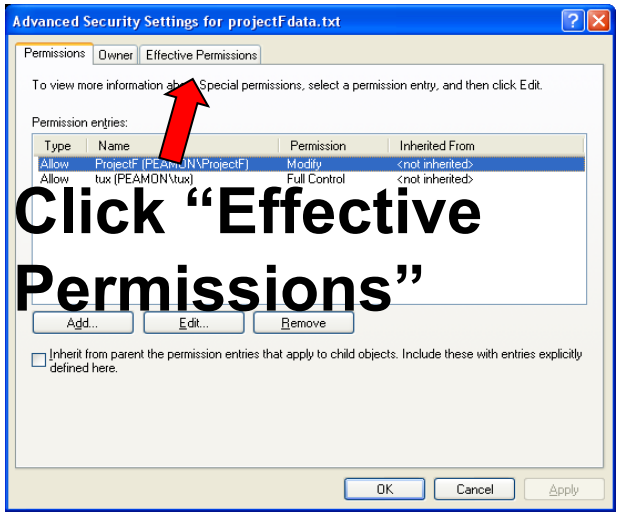
Learning Jana's effective permissions

1



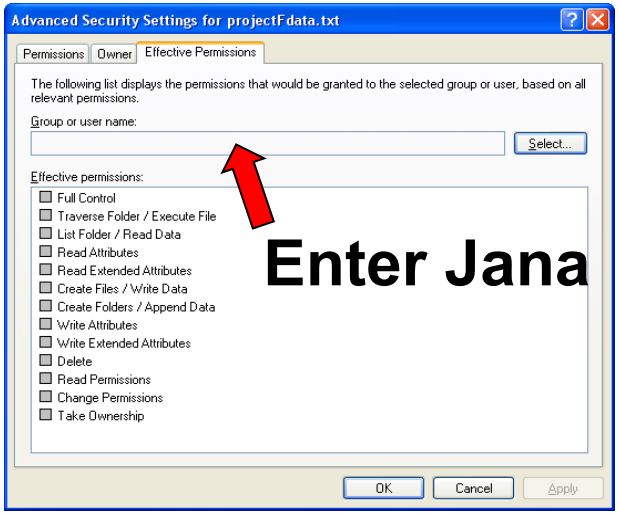
Click "Advanced"

2



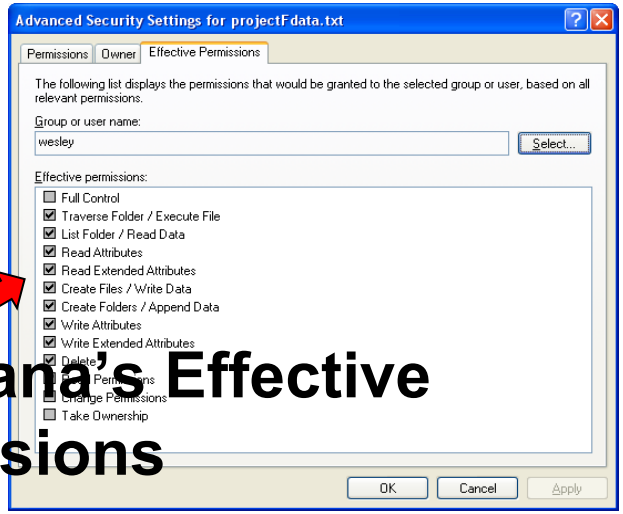
Click "Effective Permissions"

3



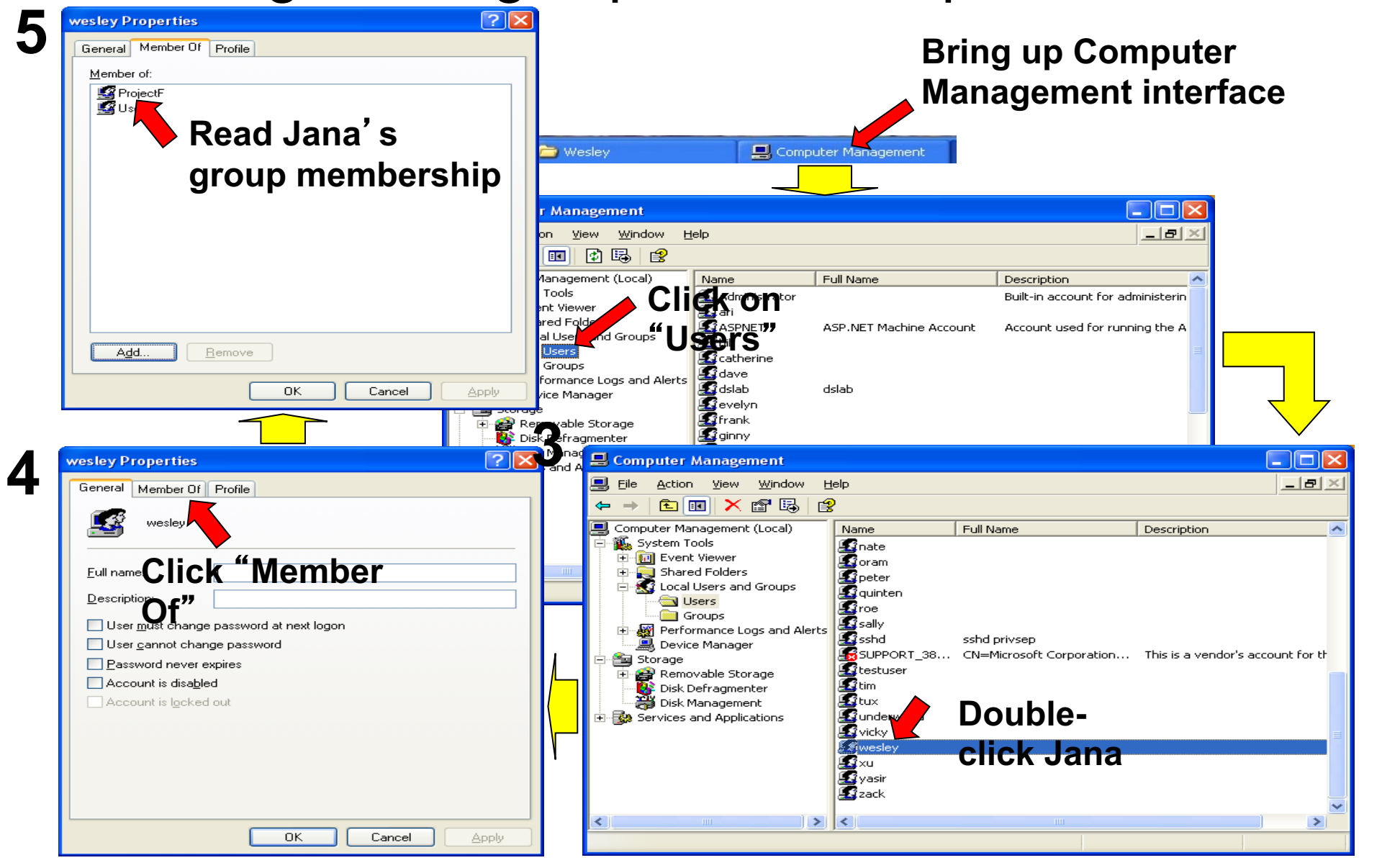
Enter Jana

4



View Jana's Effective Permissions

Learning Jana's group membership



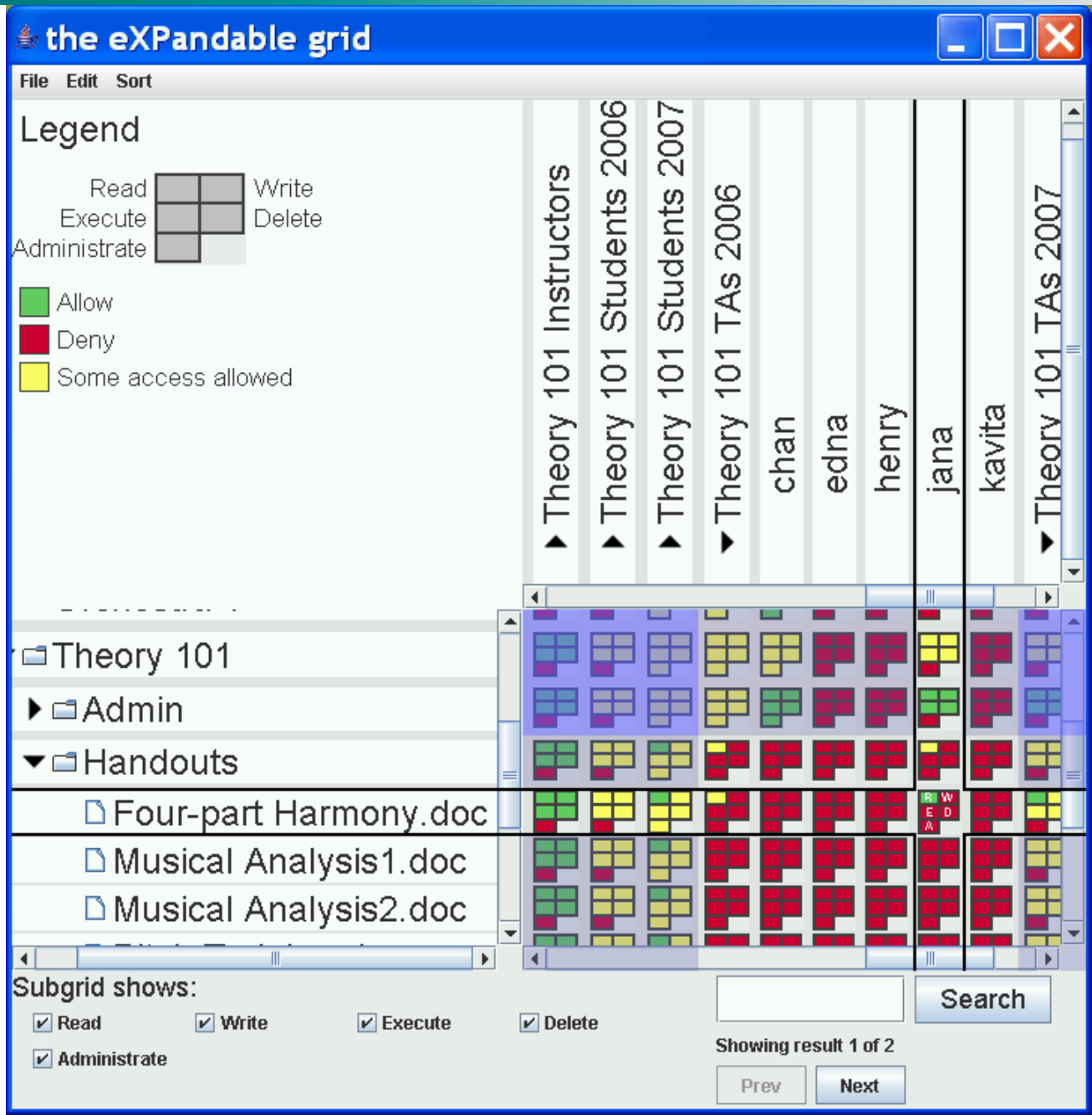
Four fundamental policy-authoring operations to support

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

Key insight

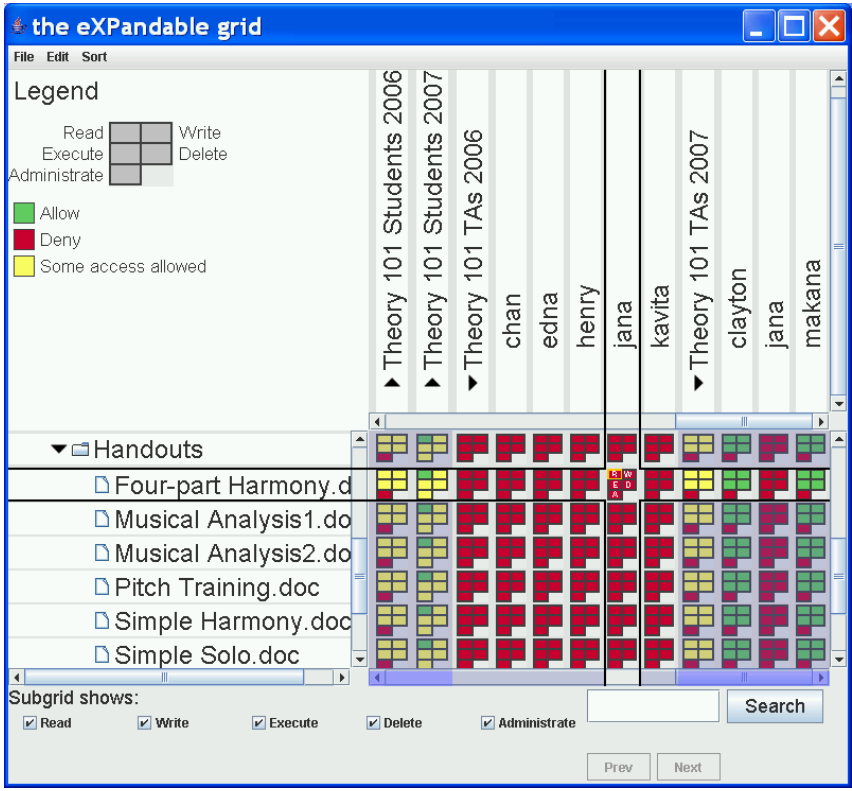
Key insight: Center policy-authoring user interfaces around a display of the *whole effective policy, not a list of rules*

Solution: Expandable Grids



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)
- 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]

User study of Expandable Grids for XP

- Laboratory study
- 2 conditions:
  - Expandable Grids
  - native Windows file permissions interface
- 36 participants, 18 per condition
- Training + 20 tasks per participant

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
- Task order: small first, then large, but counterbalanced within each size

Tasks in user study

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

Training	Make simple policy change
View simple	Does user X have write access to file Y?
View complex	Same, with rule conflict present
Change simple	Allow user X to have write access to file Y
Change complex	Make 3 different changes to policy
Compare groups	Who is in both group A and group B?
Conflict simple	Make exception for user X in group A
Conflict complex	Resolve conflict for user X in groups A and B
Memogate simulation	Does group A have access it shouldn't?
Precedence rule test	Give group A, except user X, access to folder Z

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

But… Conflict resolution

- Alice is 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 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 + 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

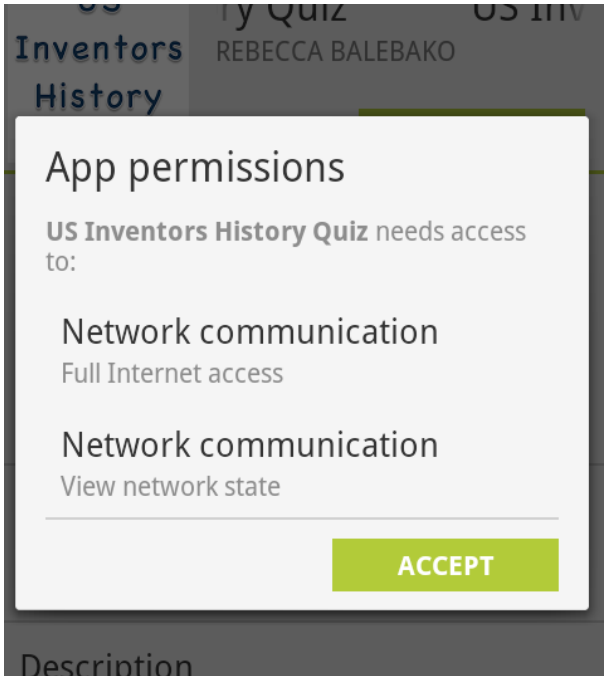
Results

- 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 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

Mobile app permissions problematic



See 3-minute video: Designing Effective App Permission Requests.
https://www.nngroup.com/videos/app-permission-requests/

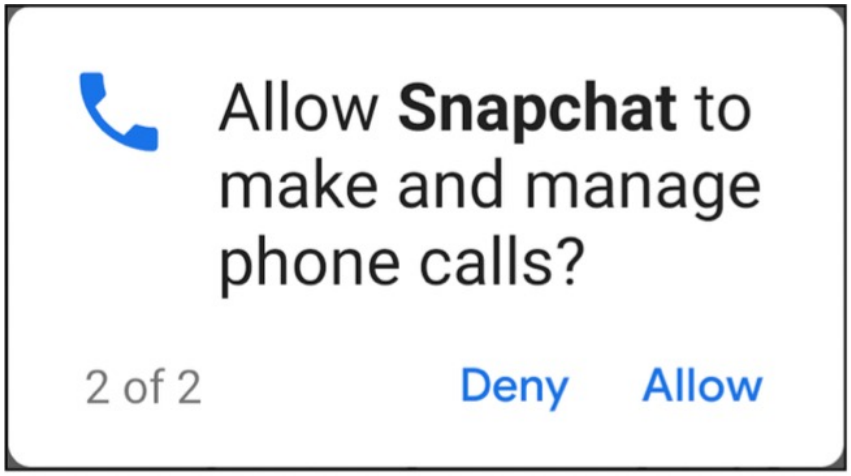
- Users don’t understand what permissions mean
- Users don’t understand why permissions are being requested
- Users often click through without reading
- Users don't know how to change decisions

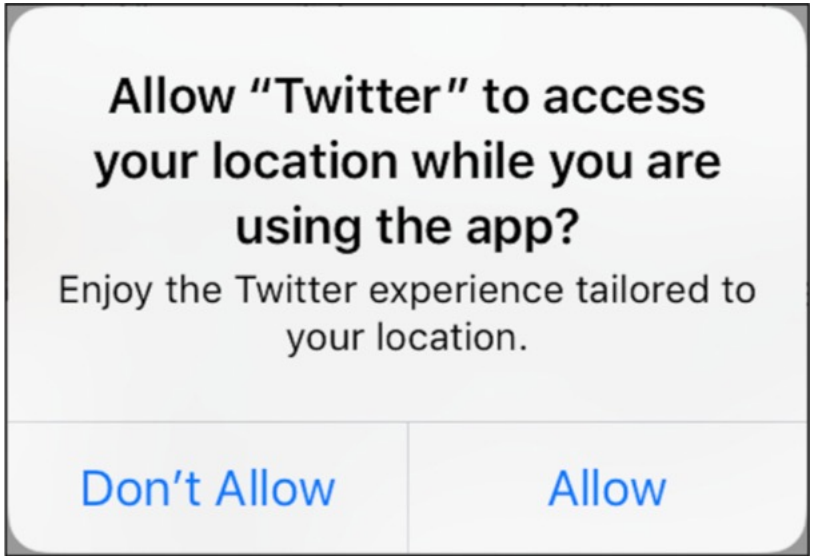
Explaining Permissions Better

- mixed-methods approach
  - observed real-world Android permissions from 4,636 Android users
  - 20-person interview study
  - large-scale internet study (n = 1559)
- identified common misunderstandings
- explored what extra information would help

B. Shen et al. Can Systems Explain Permissions Better? Understanding Users' Misperceptions under Smartphone Runtime Permission Model. USENIX Security 2021.

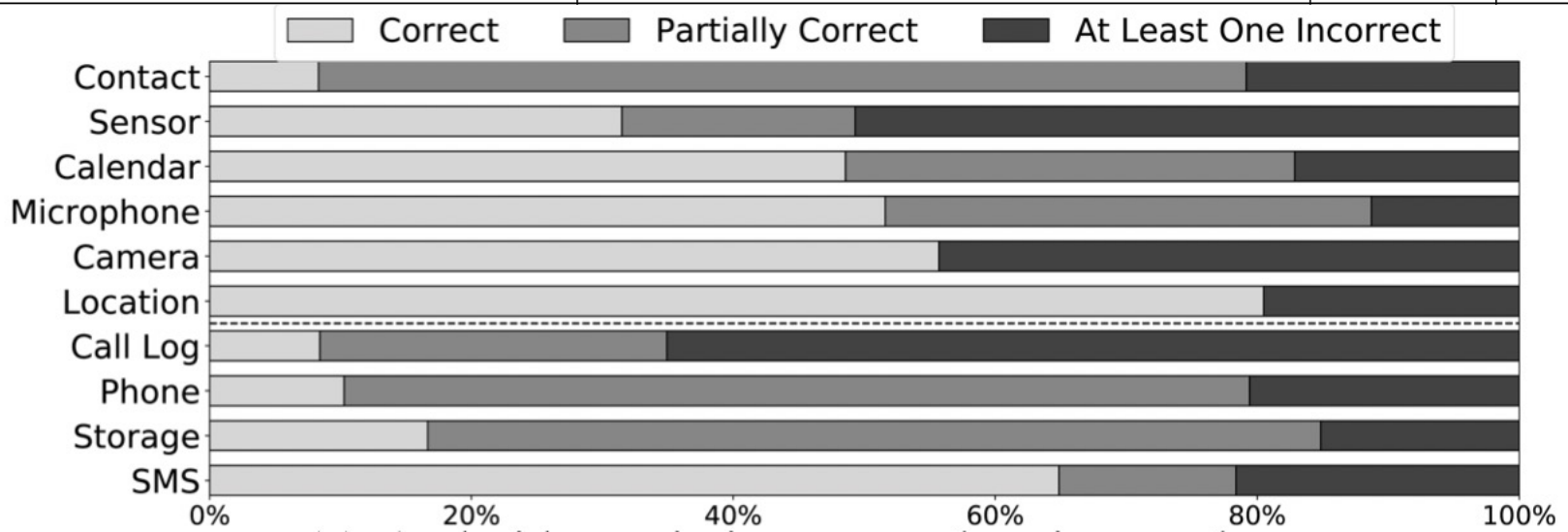
Permission Groups





Permission Group Comprehension

Permission Group	Options	Android		iOS	
Phone (Android only)	✓Get your phone number	32	**47.0%**		
Msg: Allow [App] to make and manage	✓Get your phone unique ID (e.g. IMEI)	16	**23.5%**		
phone calls?	✓Make phone call	54	79.4%		
	✓Answer phone call	45	66.2%	-	
	✓Know whether the phone is making phone calls	42	61.8%		
	◊ Read call history	36	52.9%		
	✗ Read your location	9	13.2%		
Location	✓Read your location	74	90.0%	-	
Android: Allow [App] to access this device's	✓Read your location when you're using the app	-		53	82.3%
location ?	✓Read your location when the app is in the b.g.	-		53	82.3%
iOS: [App] would like to access your	✗ Make phone calls	11	13.4%	6	9.4%
location. (*Always allow* is chosen)	✗ Read your photos	8	9.8%	7	10.9%



What factors might influence decisions?

Factors	Messages
Background access	`Resource` will [not] be accessed when you're not using the app.
Data transmission	`Resource` will [not] be transmitted and [or] stored by `App`.
Rating	The rating of `App` is 2.1 [4.8] rating in app store.
Review[1]	`App` has 13 [no] reviews related to `Resource` in app store.
Grant rate	10% [90%] of `App` users granted `Resource` access.
Brand reputation[2]	`App` has [not] been GDPR certified and [or] ISO/IEC 27001 certified.

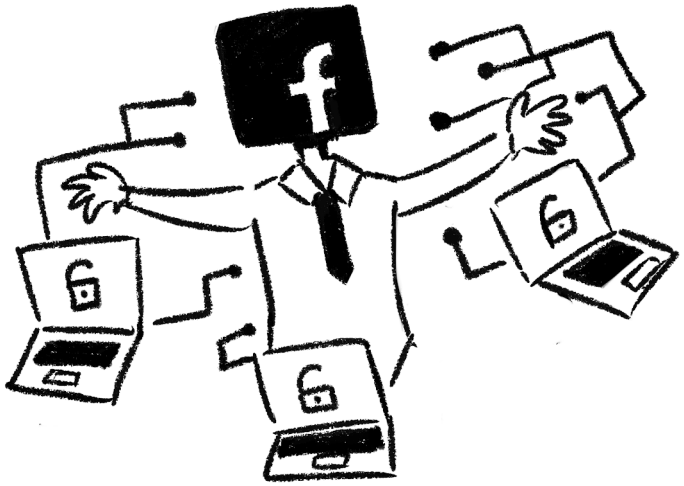
- Negative messages always affected decision
- Background access most helpful, grant rate least helpful

Auditing Mobile app permissions

- For each of the following, figure out how to find the information on your phone and write down the list of steps
  - Which apps have permission for your microphone?
  - Which apps are allowed to use location? Without explicit popup? In background?
  - Pick an app: what permissions does this app have?

Access control for social networks

- It's complicated!
- How do you specify your audience?
  - Public, friends, friends-of-friends, friend lists (circles), friends except restricted
- How do you specify groups of friends?
  - Groups as attributes of each friend (Jane is in group "college friends")
  - Define friend groups based on attributes (all my friends who are alumni of my college are in group "college friends")
  - Setup a FB (or other social network) group and invite people to join



Access Control for Social Media

Pick a social media

1. What are the controls and settings that determine who has access to post on this social media platform?
   - How do you view who has access to a post currently?
   - How do you grant access to the post?
   - How do you revoke access to the post?
2. How might you improve access control on this platform?
   - different controls/settings?
   - different interface?
3. Design a user study to evaluate your ideas.

Usable Access Control