

Why Usability Can't Be Just Skin Deep

Lujo Bauer
CyLab, Carnegie Mellon University

Jul 27, 2009

- **“Usability” often seen as a last phase in system design**

- ***Thesis: Creating usable systems often requires not just the help of usability experts, but that the system architects are usability experts***
 - ▼ Semantics of access-control systems can affect usability
[Reeder, Bauer, Cranor, Reiter, Vaniea '08,'09]

 - ▼ Machine learning can help with policy configuration
[Bauer, Garriss, Reiter '08]

Example 1: Access-control Policy Semantics



The Expandable Grid

The screenshot displays the 'the eXPandable grid' application window. The title bar reads 'the eXPandable grid' and includes standard window controls. The menu bar contains 'File', 'Edit', and 'Sort'. A 'Legend' section on the left defines permissions: Read, Execute, and Administrate (represented by a 2x2 grid); Write and Delete (represented by a 2x1 grid). It also defines access levels: Allow (green square), Deny (red square), and Some access allowed (yellow square). The main area shows a tree view of folders and files. The 'Handouts' folder is expanded, showing a list of files: 'Four-part Harmony.doc', 'Musical Analysis1.doc', 'Musical Analysis2.doc', 'Pitch Training.doc', 'Simple Harmony.doc', and 'Simple Solo.doc'. A grid of colored squares represents permissions for each file across various users. A 'Subgrid shows:' section at the bottom has checkboxes for Read, Write, Execute, Delete, and Administrate, all of which are checked. A search box and 'Search' button are also present. Navigation buttons 'Prev' and 'Next' are at the bottom.

File/Folder	Theory 101 Students 2006	Theory 101 Students 2007	Theory 101 TAs 2006	chan	edna	henry	jana	kavita	Theory 101 TAs 2007	clayton	jana	makana
Handouts	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Four-part Harmony.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Musical Analysis1.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Musical Analysis2.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Pitch Training.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Simple Harmony.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Simple Solo.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow

Study Results: Grid vs Windows

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

Study Results: Conflict Resolution

- **But... We changed conflict-resolution method to recency-takes-precedence**
- **Were the effects of our original study due to the new visualization idea, the new conflict-resolution method, or both?**
- **We ran another study to find out**

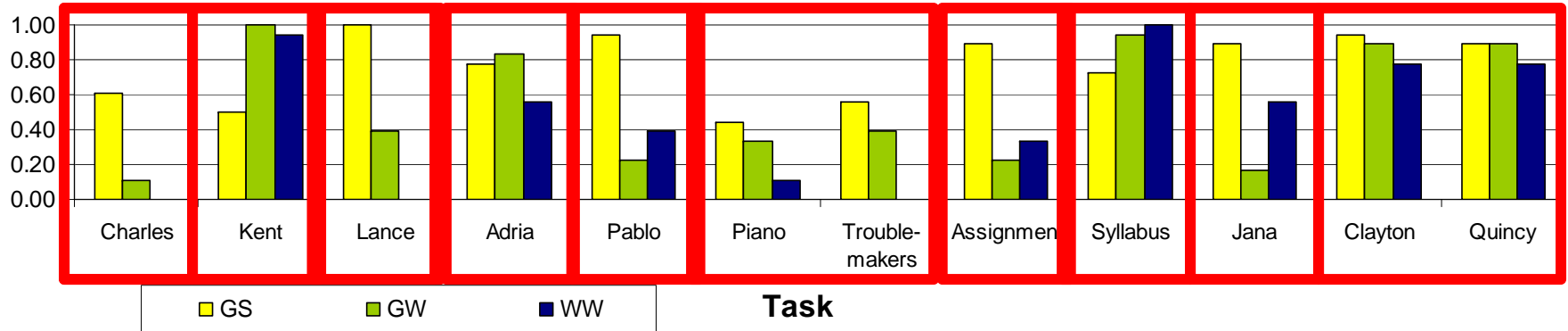
Semantics Study

- **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**

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

Example 1 Summary

- **Changing semantics has effect on usability, regardless of interface**

Example 2: Policy Configuration in Grey

- Smartphone-based, end-user-driven access-control system for physical and virtual resources
- Deployed in Carnegie Mellon's Collaborative Innovation Center
 - ▼ Approximately 35 Grey-capable doors and 30+ users at the moment



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



I need to grade the
midterms for Lujo's class



Scott

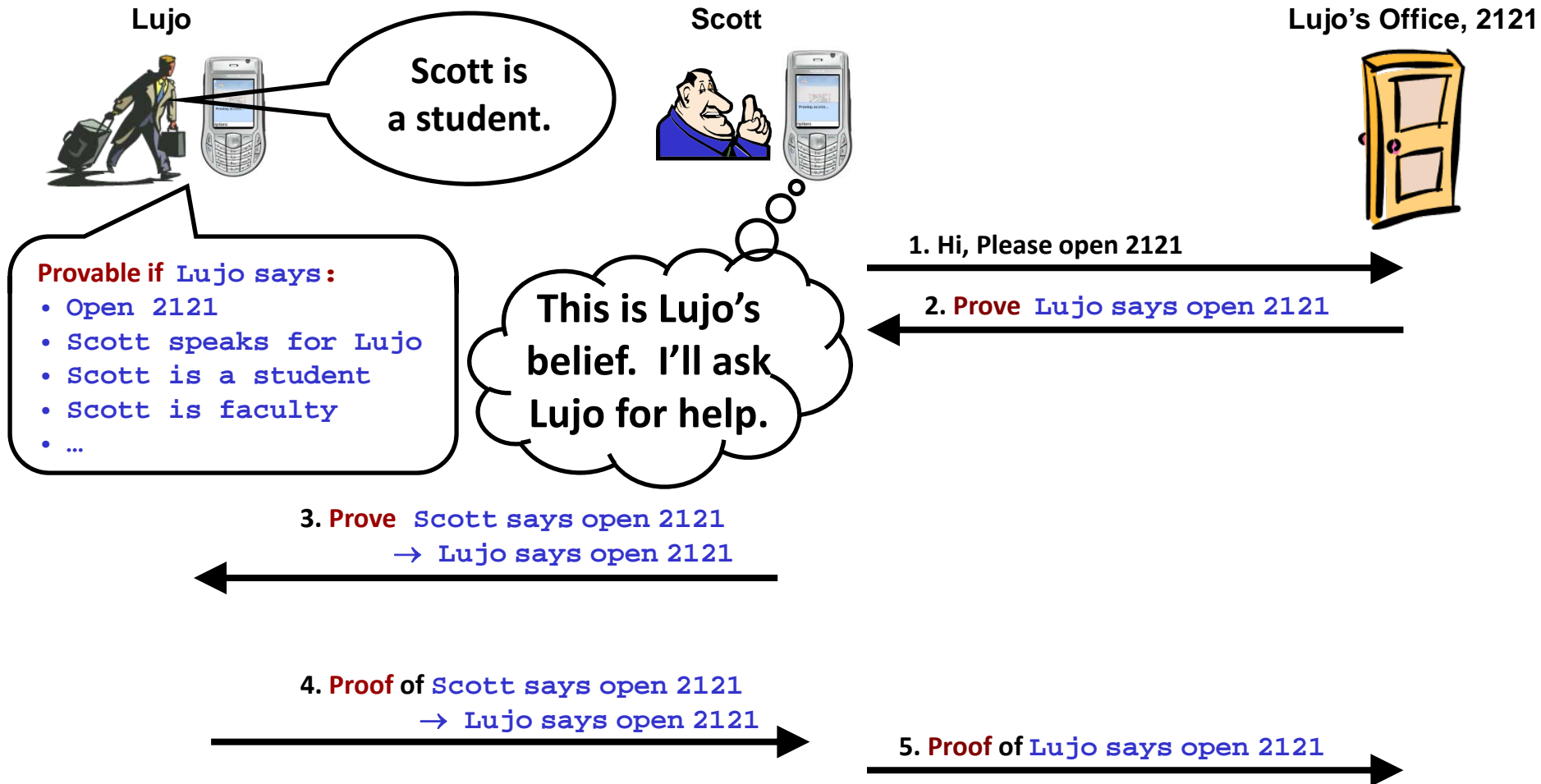


Lujo must
authorize access



Lujo's Office, 2121

Grey: An Example Scenario



Can We Make Configuration Easier?

- Setting up policies takes effort
- Incorrectly set up policies can wrongly allow or deny access
- How to help users easily set up *correct* policies?



Can We Make Configuration Easier?

- Setting up policies takes effort
- Incorrectly set up policies can wrongly allow or deny access
- How to help users easily set up *correct* policies?
- Mechanism involves two steps:
 - ▼ Identifying intended policy and misconfigurations in the implemented policy
 - ▼ Resolving misconfigurations by augmenting the implemented policy
- “Misconfiguration” refers to authority that is intended to exist but has not been given

Identifying Misconfigurations

- **Observation: access-control policy exhibits patterns**
 - ▼ Inconsistencies in these patterns can indicate misconfigurations
 - ▼ These patterns are observable from access-control logs
 - ▼ Need centralized collection of logs to analyze
- **Use Association Rule Mining [Agrawal and Srikant '94]**
 - ▼ Input: series of records characterized by a fixed number of attributes
 - ▼ Output: rules (or statistical patterns)
- **Use rules to identify anomalies**

Data Representation

	AttA	AttB	AttC	AttD
Record1	T	-	T	-

Constructing Rules

	AttA	AttB	AttC	AttD
Record1	T	-	T	-
Record2	T	T	-	-
Record3	T	T	T	-
Record4	T	-	T	T

Rule: $A \rightarrow B$

Confidence = 0.5

Rule: $A \rightarrow C$

Confidence = 0.75

Identifying Misconfigurations

	ResA	ResB	ResC	ResD
Alice	T	-	T	-
Bob	T	T	-	-
Charlie	T	T	T	-
David	T	-	T	T

Resources

Users

Rule: ResA → ResC

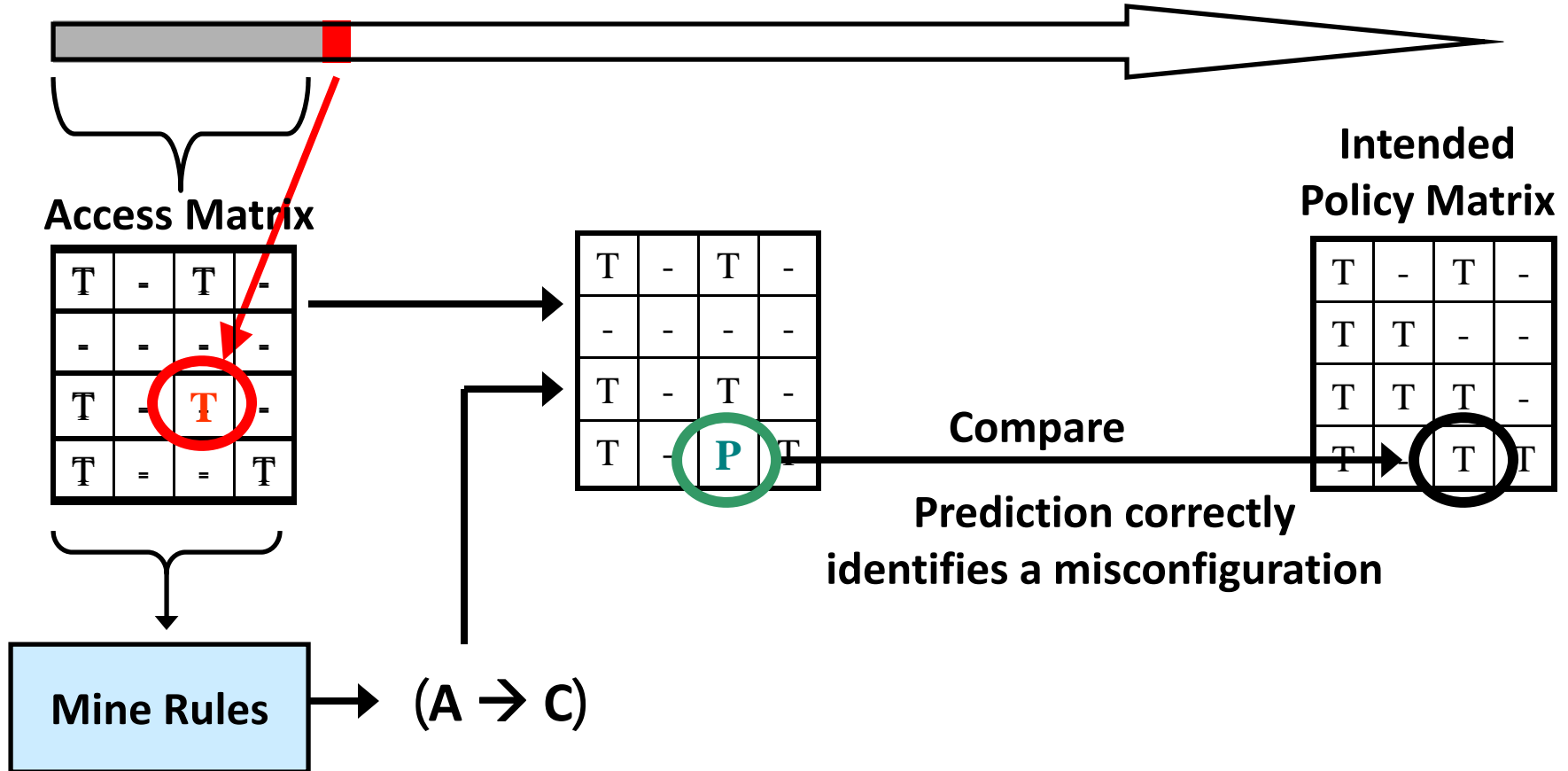
Potential Misconfiguration (a.k.a., a prediction)

Dataset

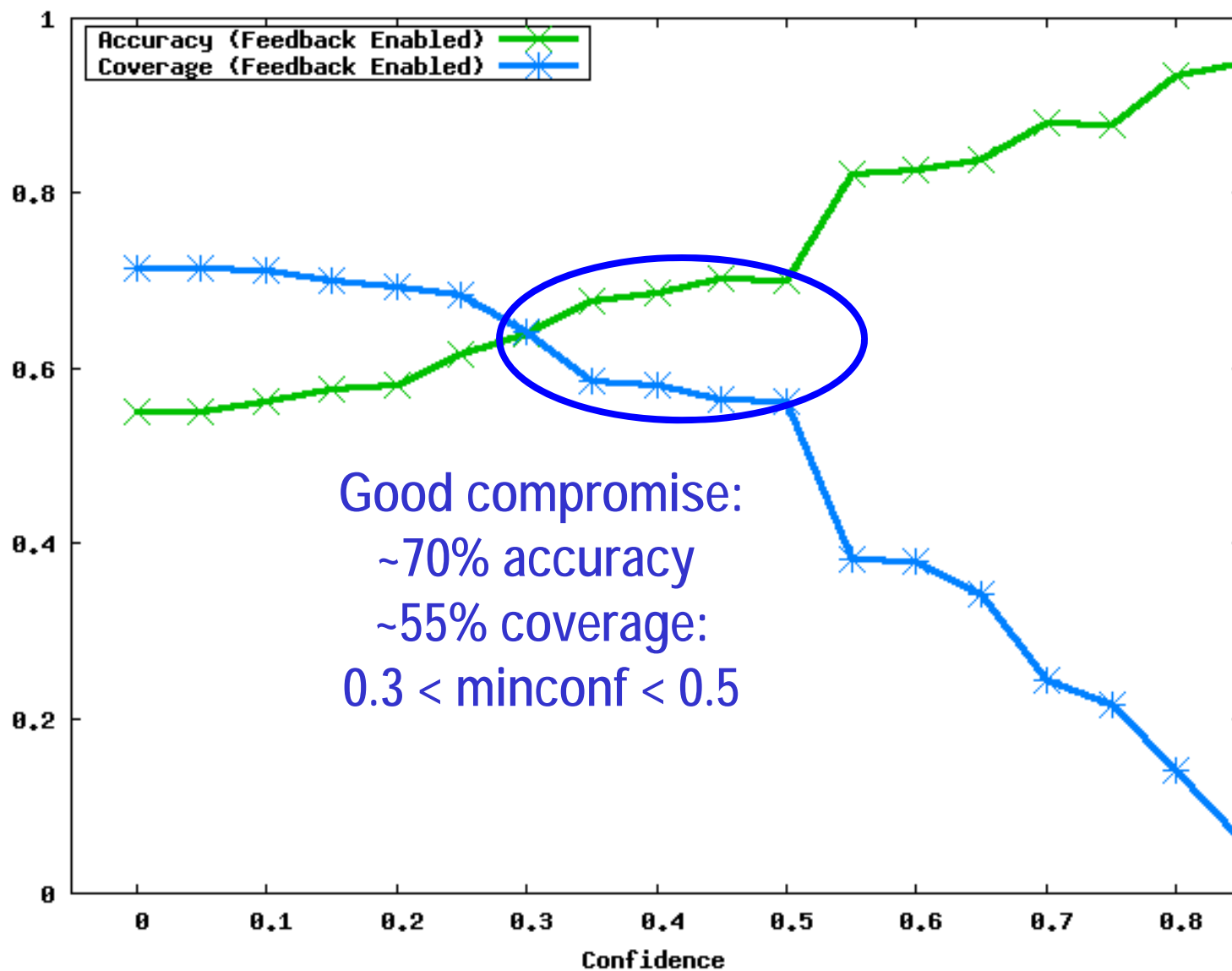
- **Log of 10,911 accesses drawn from Grey deployment**
- **Spans 16 months**
- **Contains accesses by 25 users to 29 resources**

Identification Simulation

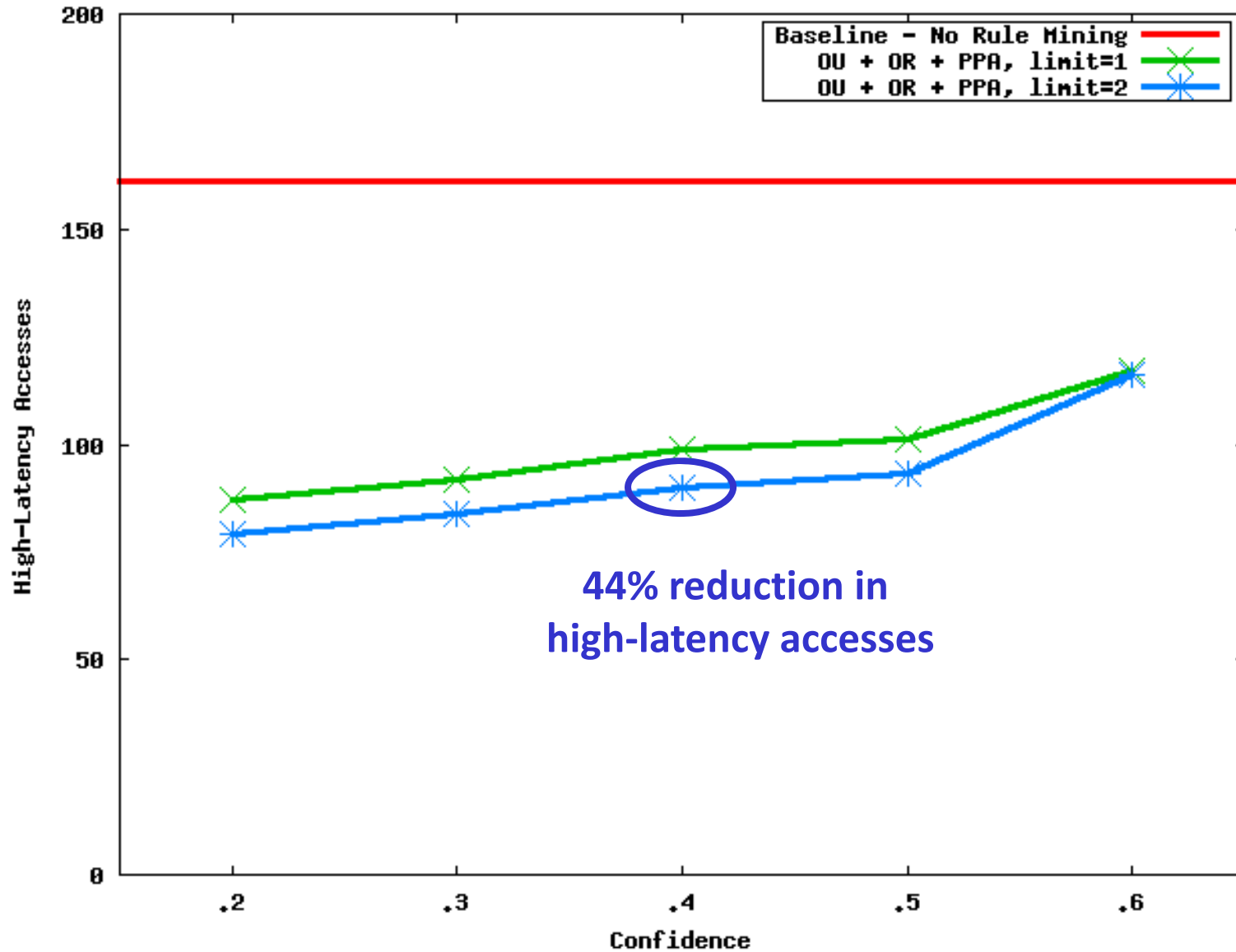
Chronological Access History



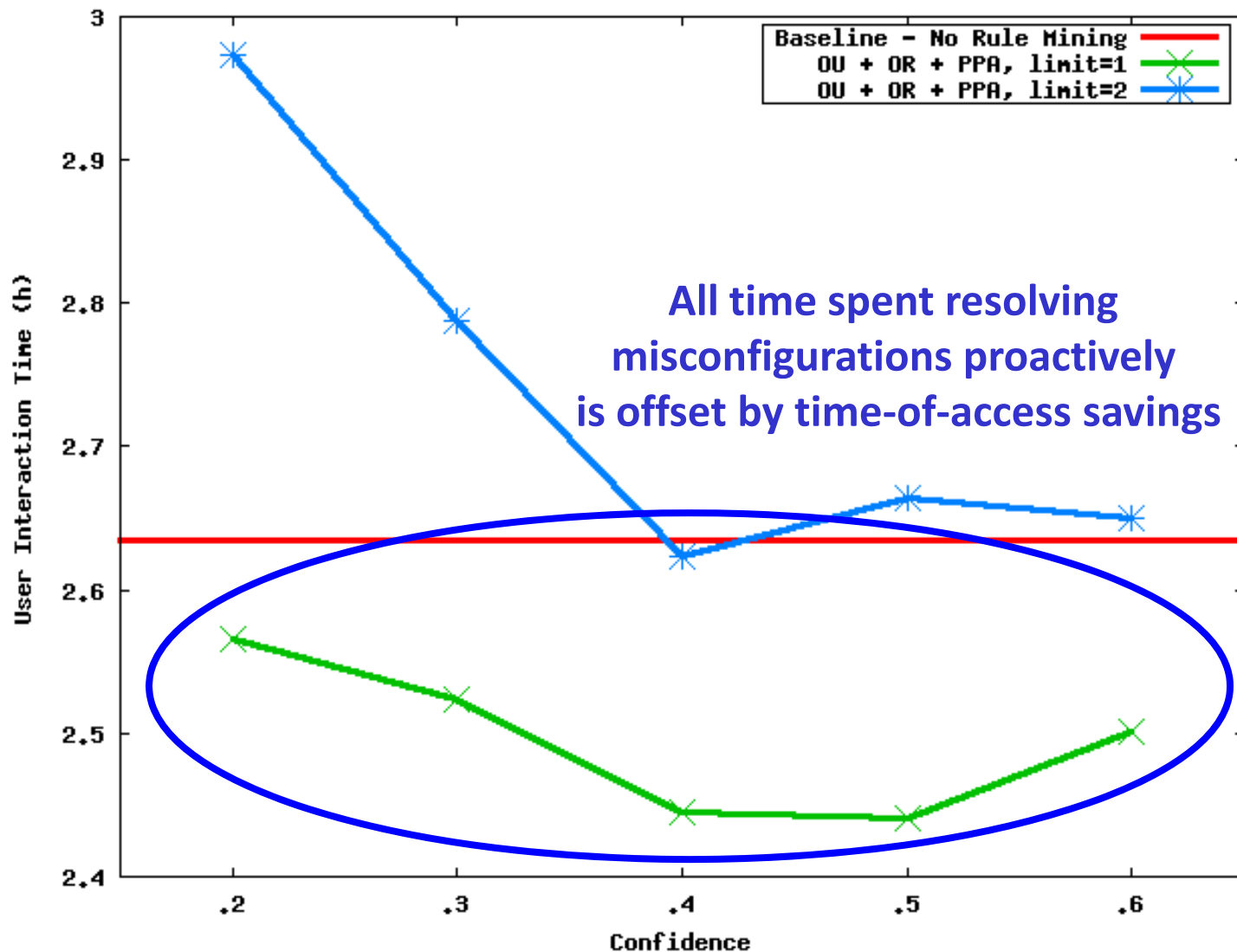
Accuracy/Coverage Tradeoff



High-Latency Accesses



Total User Interaction Time (across all users over 16 months)



Example 2 Summary

- Machine learning can help with policy configuration
- Needs centralized collection of access logs
 - ▼ Helps if access logs explain *why* access was granted

Why Usability Can't Be Just Skin Deep

- **Decisions that affect usability need to be made at the outset**
- **APIs needed for usability may not be available to the application**
- **Certain system designs may be more amenable to advancing usability**
- **Solution?**

Thanks!

<http://www.ece.cmu.edu/~lbauer>