Carnegie Mellon CyLab

CONFIDENCE FOR A NETWORKED WORLD

Smartphone-based Access Control: Adventures in Usability

Lujo Bauer

Device-enabled Authorization

- **Smartphones on a trajectory to “win” in the market**
  - Stand to inherit mobile phone market that shipped over 1.1 billion units in 2008 [IDC]—**or more than one phone per six people in the world**
- **Unique combination of capabilities**
  - Computation, communication, user interface

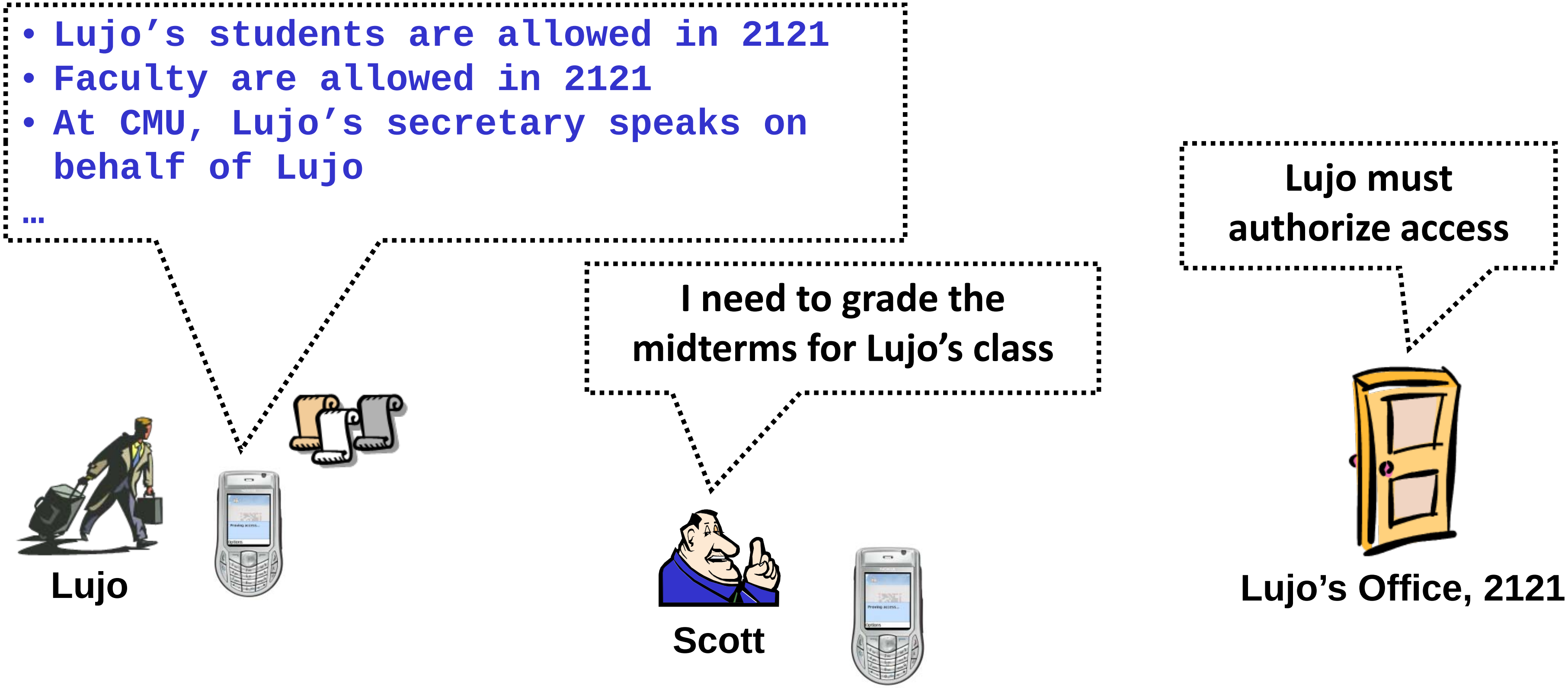
- **Goal: to use smartphones to intelligently control environment**
  - Loan you my car without giving you my phone
  - Send money from my phone to my friend’s phone
  - Give my secretary temporary access to my email without revealing information (e.g., password) that could be used at a later time
  - Use my phone to open my hotel room door, without ever stopping by the front desk

… and do it all from a distance

Grey Deployment

- **Universal, flexible, 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-compatible Windows XP, Vista and Linux login modules
- **Plus a deployment in progress at UNC Chapel Hill**

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

…

I need to grade the midterms for Lujo’s class

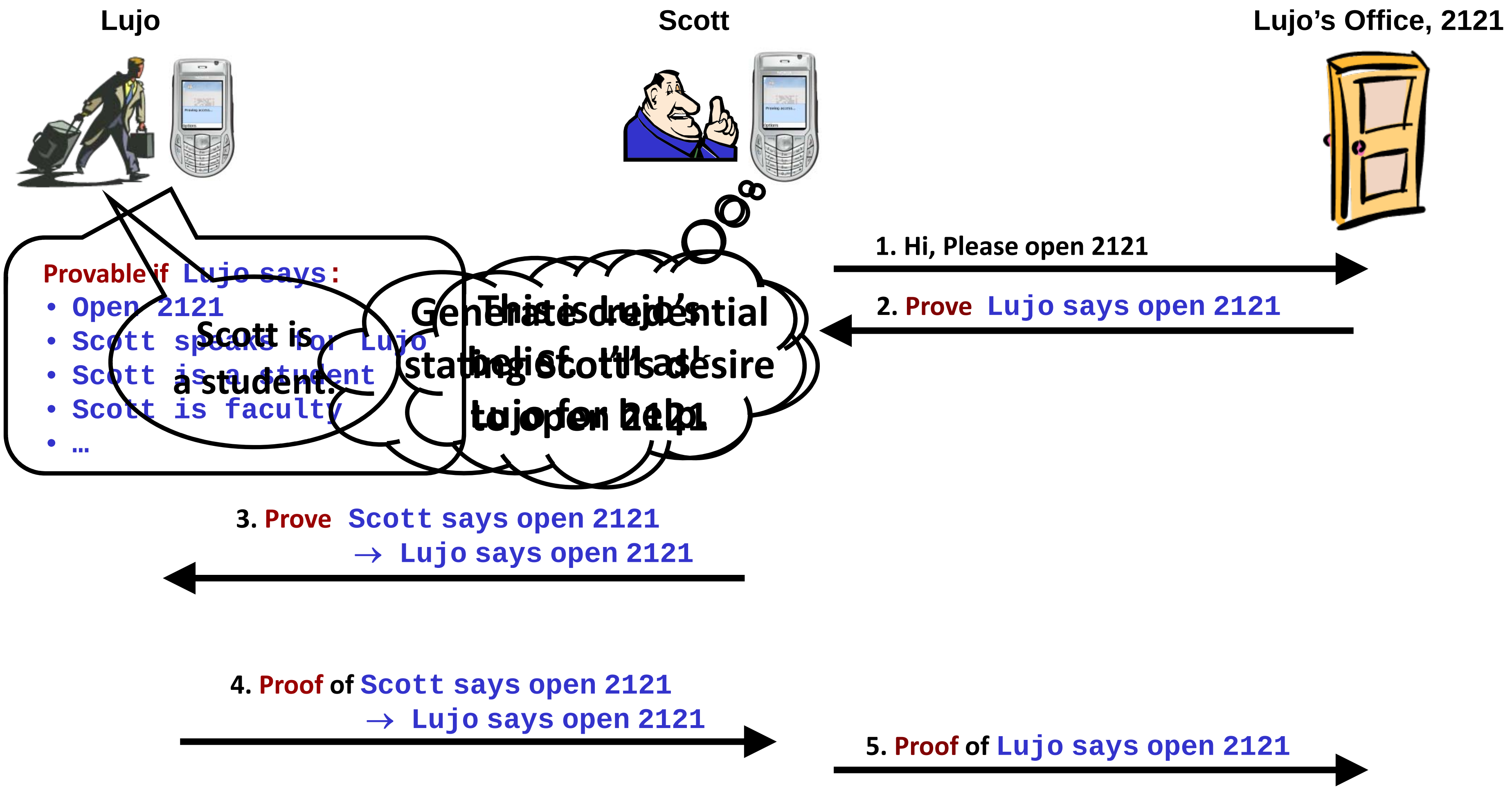
Lujo must authorize access

Lujo

Scott

Lujo’s Office, 2121

Grey: An Example Scenario



Lujo

Scott

Lujo’s Office, 2121

Provable if Lujo says:
- Open 2121
- Scott speaks for Lujo
- Scott is a student
- Scott is faculty
- …

Scott is a student.

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

Generate credential stating Scott’s desire to open 2121

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

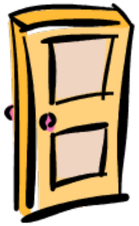
5. Proof of Lujo says open 2121

Grey: An Example Scenario

Lujo

Scott

Lujo’s Office, 2121



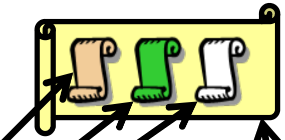
1. Hi, Please open 2121

2. Prove `Lujo says open 2121`

- High assurance
- Rich audit logs
- Flexibility in policies

4. Proof of `Scott says open 2121` → `Lujo says open 2121`

5. Proof of `Lujo says open 2121`



Digitally signed credentials …

… assembled in a formal, mechanically verifiable proof

EXIT

[w/ Reiter, Cranor, others]

Some Research Challenges

- **Logics for access control**

  [ESORICS 2006, NDSS 2007, SACMAT 2009]

- **Distributed theorem proving**

  [IEEE S&P 2005, ESORICS 2007]

- **Helping users configure access-control policies**

  [CHI 2008a, SACMAT 2008, CMU TR 2009]

- **Improving usability / evaluating usefulness in practice**

  [SOUPS 2007, CHI 2008b]

Lessons Learned From the Deployment of a Smartphone-Based Access-Control System

Lujo Bauer, Lorrie Cranor,
Michael K. Reiter and Kami Vaniea

Carnegie Mellon

CMU Usable Privacy and Security Laboratory
http://cups.cs.cmu.edu/

Deployment Study

Research Question

- Can a smartphone-based access control system gain acceptance?
- Our contribution is to illustrate how six design principles manifest themselves in a smartphone-based access-control system

Deployment Study

Grey Field Trial

- Year long study
- 19 users
- Periodic interviews
- Analysis of log data

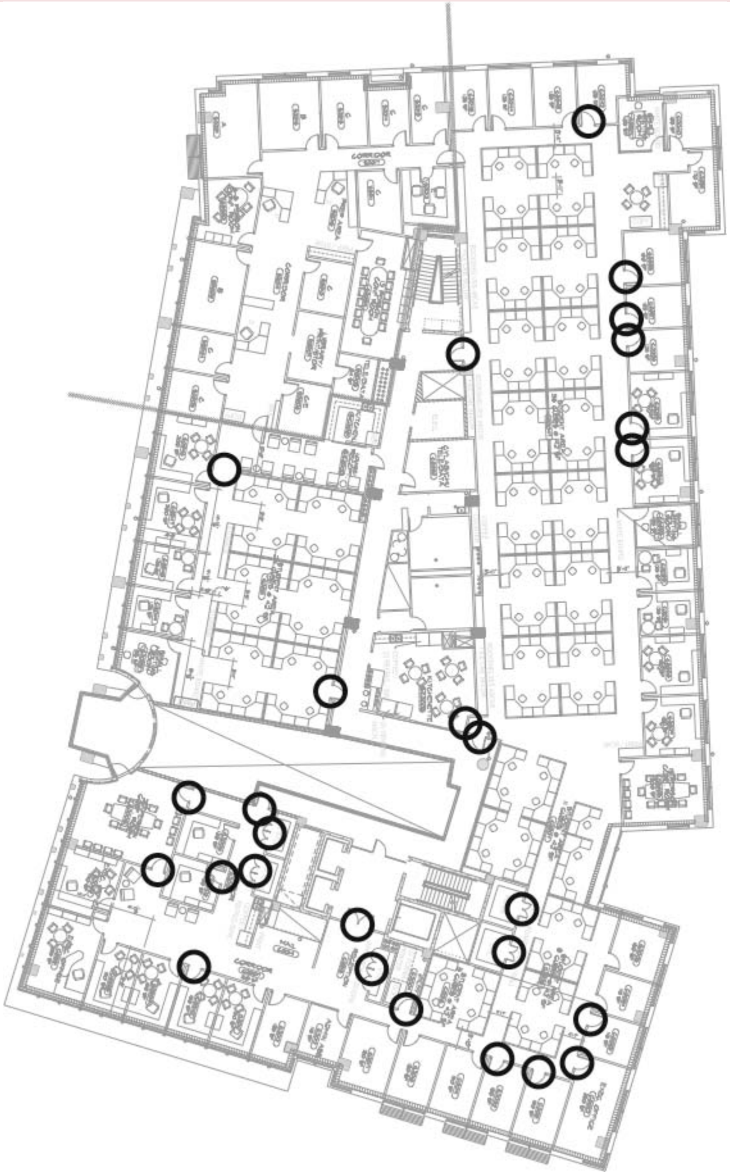
Field Trial: Participants

- Solicited from those who need access to resources protected by Grey
- 6 computer science and engineering faculty
- 9 computer science and engineering graduate students
- 3 technical staff
- 1 administrative assistant

Deployment Study

Field Trial: Environment

- 5 perimeter doors to a large research area (locked at 6pm)
- 11 offices
- 2 storage closets
- 1 conference room
- 1 lab space
- 1 machine room



Deployment Study

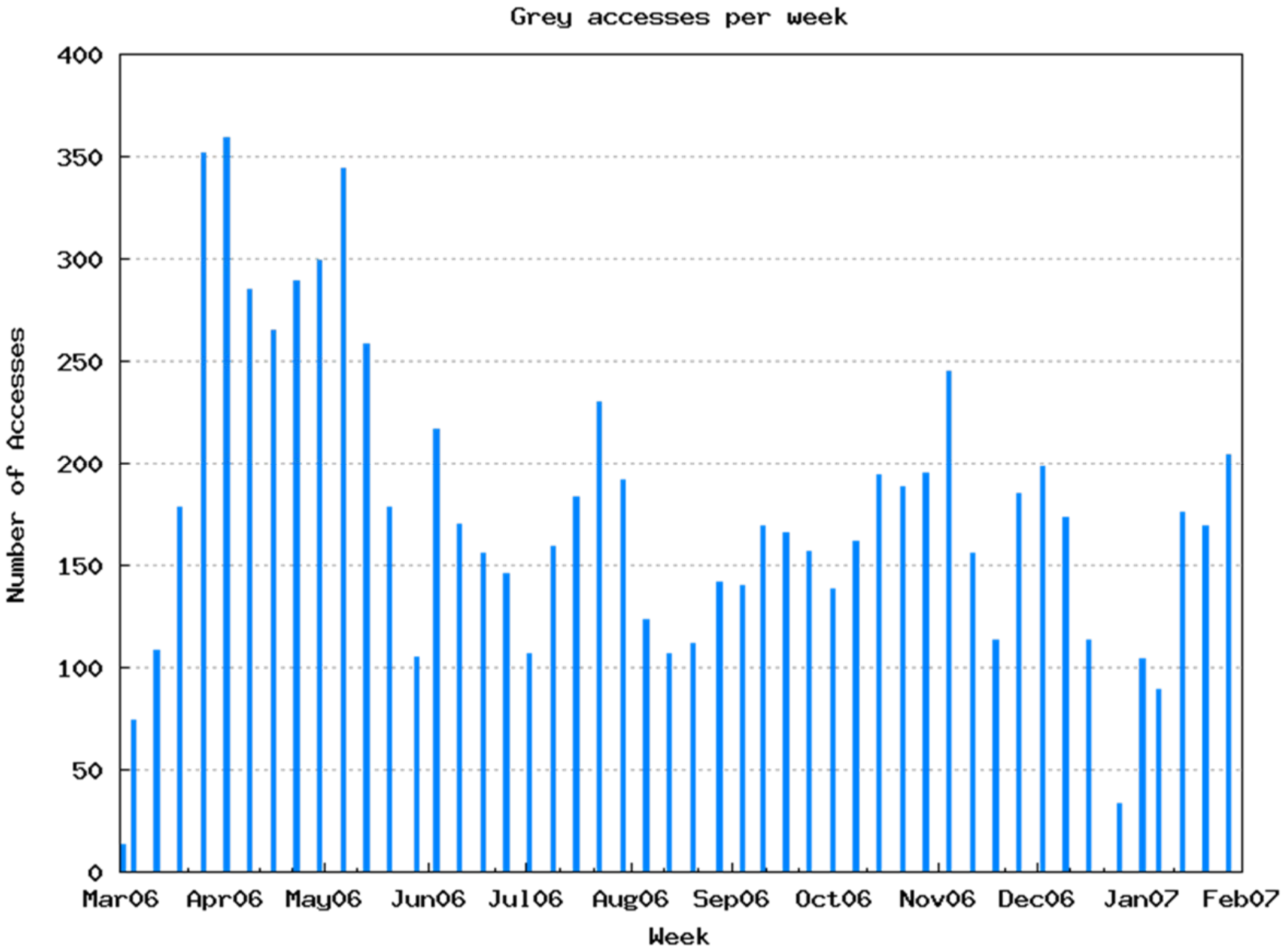
Field Trial: Interview Procedure

- **Interviewed participants**
  - Security practices
  - Types of resources managed and needed
- **Gave participants a smartphone with Grey pre-installed and brief instruction on use**
- **Interviewed one month later**
  - Changes in security practices
  - Resource management activity
  - General reactions to Grey
- **Additional interviews as needed**

Data

- **Audiotaped over 30 hours of interviews**
- **Logged 19,500 Grey access requests**
- **Active users averaged 12 access a week**
  - Five users accessed their office almost exclusively with Grey
  - Three users gave away their keys
- **Users interacted with an average of 7.4 different doors during the study**

Overall Usage



Deployment Study

Lessons Learned

- Observed how six known principles apply to the design of applications based on emerging technology

Deployment Study

Principle 1

- **Perceived speed and convenience are critical to user satisfaction and acceptance**

Deployment Study

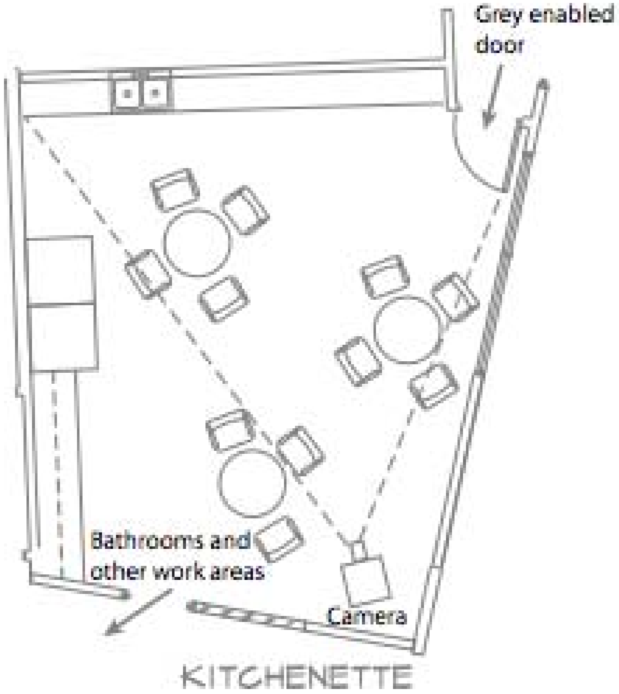
Perceived Speed

- Users quickly began to complain about speed and convenience
- We knew Grey and keys required similar amounts of time to open a door
- Videotaped a highly trafficked door to better understand how doors are opened differently with Grey and keys

Deployment Study

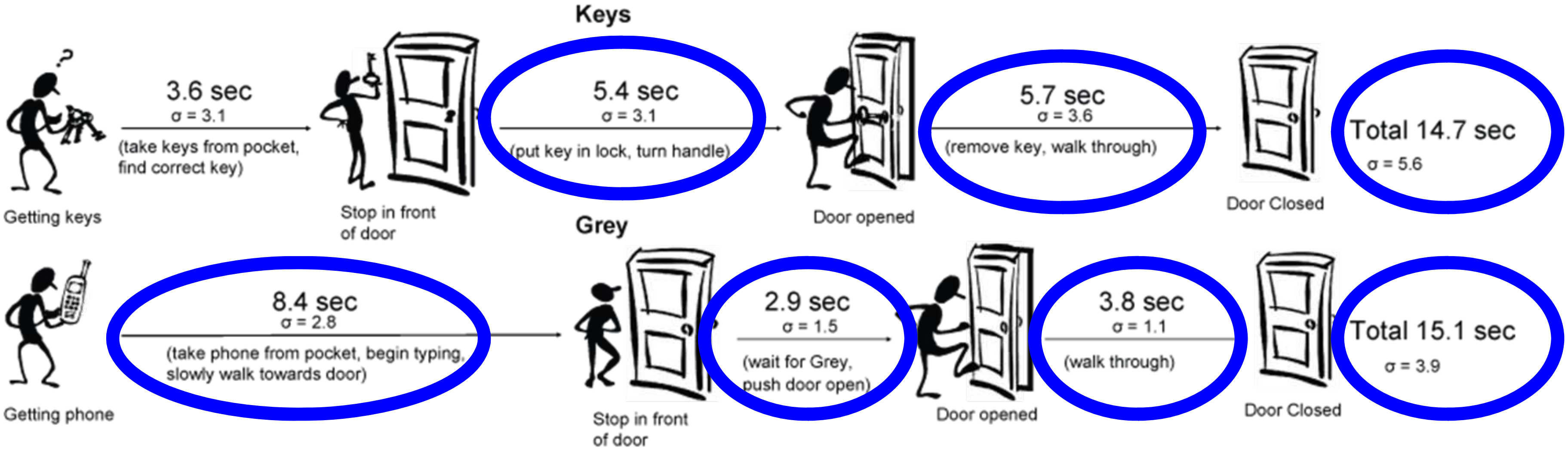
Videotaping

- **Videotaped participants accessing kitchenette door**
- **Videotaped two hours daily after 6pm for two weeks**
- **18 users taped**
  - 5 Grey participants
  - 13 additional participants were solicited as they passed through the door



Deployment Study

Door Access Average Times



Deployment Study

Principle 2

- **A single failure can strongly discourage adoption**

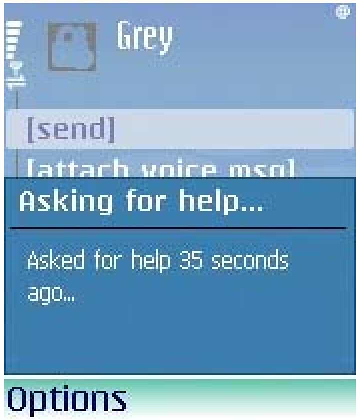
Deployment Study

A Single Failure

- Cost of failure is potentially high
- Rebooting a phone or door was considered very inconvenient
- Several users stopped using Grey actively after a single inopportune failure

Delays Interpreted as Failures

- **Delays can be interpreted as failures even when the system is functioning perfectly**
  - Humans can be slow or unresponsive
- **Providing feedback on the status of the request is very important**
  - Did it arrive?
  - Is a human currently responding?



Grey

[send]

[attach voice msg]

Asking for help...

Asked for help 35 seconds ago...

Options

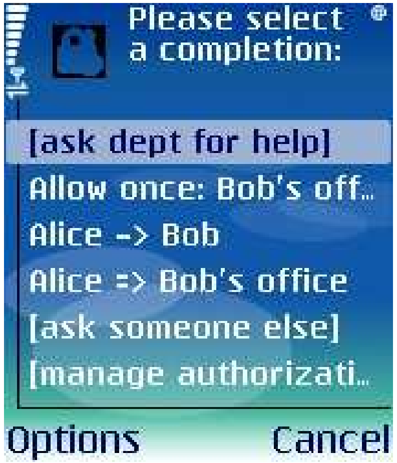
Deployment Study

Principle 3

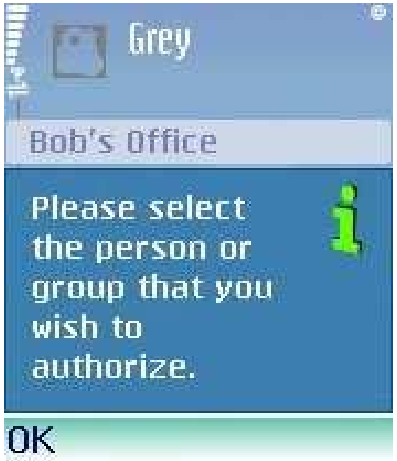
- Users won’t use features they don’t understand

Confusing Features

- Users would rather choose a suboptimal solution that they understand than one with an uncertain outcome
- Initially tried for terse interface (top)
- Adopted wizard solution (bottom)



Please select a completion:



Please select the person or group that you wish to authorize.

Principle 4

- **Systems that benefit from the network effect are often untenable for small user populations**

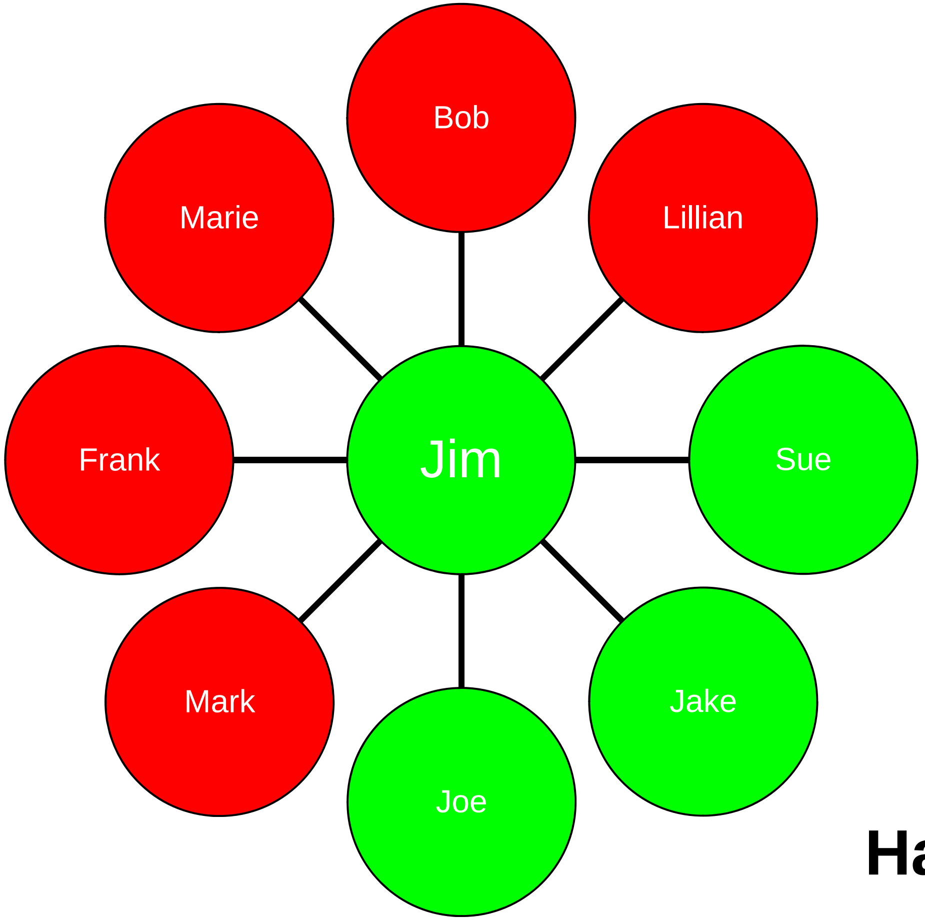
Deployment Study

Network Effect

- A service becomes more valuable as more people use it
- Our participants were selected so that their work network included others with Grey
- Still had many people who would have benefited if Grey participant could have given access

Deployment Study

Jim's Colleagues



No Grey

Have Grey

Deployment Study

Principle 5

- **Low overhead for creating and changing policies encourages policy change**

Deployment Study

Policy Change

- **Using Grey our participants successfully granted and received more access than they previously had**
- **Participants granted new access because it was convenient**
- **Covered further in technical report**
  - L. Bauer, L. Cranor, R. W. Reeder, M. K. Reiter and K. Vaniea. Comparing access-control technologies: a study of keys and smartphones, Technical Report CMU-CyLab-07-005. http://www.cylab.cmu.edu/default.aspx?id=2284

Deployment Study

Principle 6

- **Unanticipated uses can bolster acceptance**

Unanticipated Uses

- Unlocking door from inside the office without having to stand
- Unlocking nearby door for someone else without leaving office

Deployment Study

Discussion

- **Users treat Grey like an appliance**
  - Low tolerance for failure
- **Advanced functionality wasn’t always used**
- **Education and background seemed to have little effect on usage**

A User Study of Policy Creation in a Flexible Access-Control System

Lujo Bauer, Lorrie Faith Cranor, Robert W. Reeder,
Michael K. Reiter, **Kami Vaniea**

Carnegie Mellon

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Policy-creation Study

Our Question

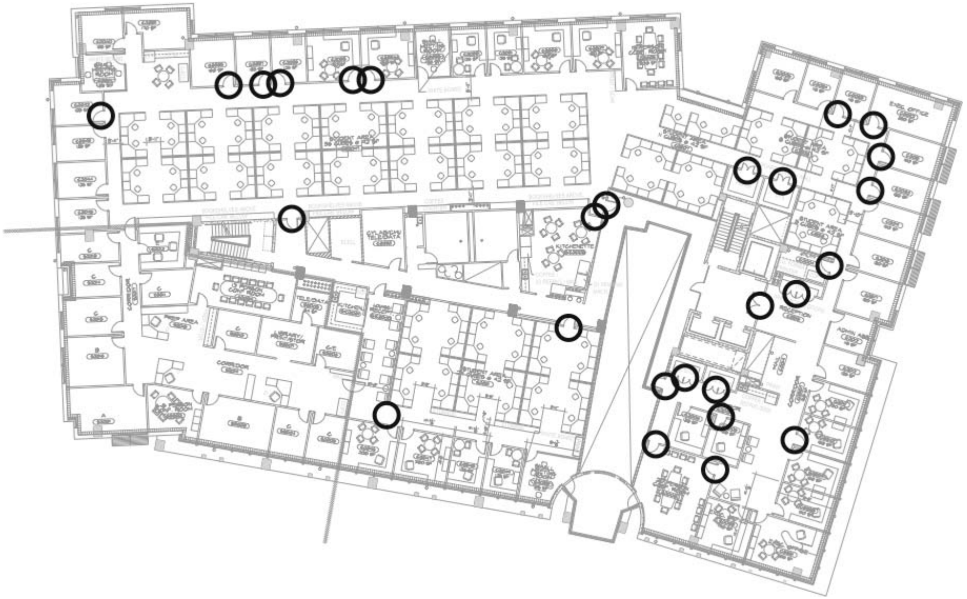
- How well do implemented access-control policies match ideal access-control policies?
- In other words: are users able to create access-control policies that do what they want?

Study Overview

- Interviewed participants about their current access control practices
- Gave participants a Grey phone
- Periodically interviewed
- Used interviews to create policy maps for each resource owner’s ideal, key and Grey policy
- Counted number of potential false rejects and accepts based on the policies

Environment

- **Over three dozen Grey-enabled doors**
  - 8 offices
  - A machine room
- **29 Grey users**
  - 9 faculty
  - 11 graduate students
  - 9 staff
- **8 resource owners**



Building Floor Plan

Policy-creation Study

Interview Procedure

- **Interviewed 8 resource owners**
  - Security policies
  - Types of resources managed and needed
- **Gave participants a smartphone with Grey pre-installed and brief instruction on use**
- **Interviewed one month later**
  - Changes in policy
  - Resource management activity
  - General reactions to Grey
- **Periodically conducted follow-up interviews at approximately one month intervals**

Data

- **Audiotaped over 20 hours of interviews for the eight resource owners**
- **System was actively used**
  - Logged 19,500 Grey accesses for 29 users
  - Active users averaged 12 accesses a week
  - Five users accessed their office almost exclusively with Grey
  - Users interacted with an average of 7.4 different doors during the study
- **Study lasted a year**

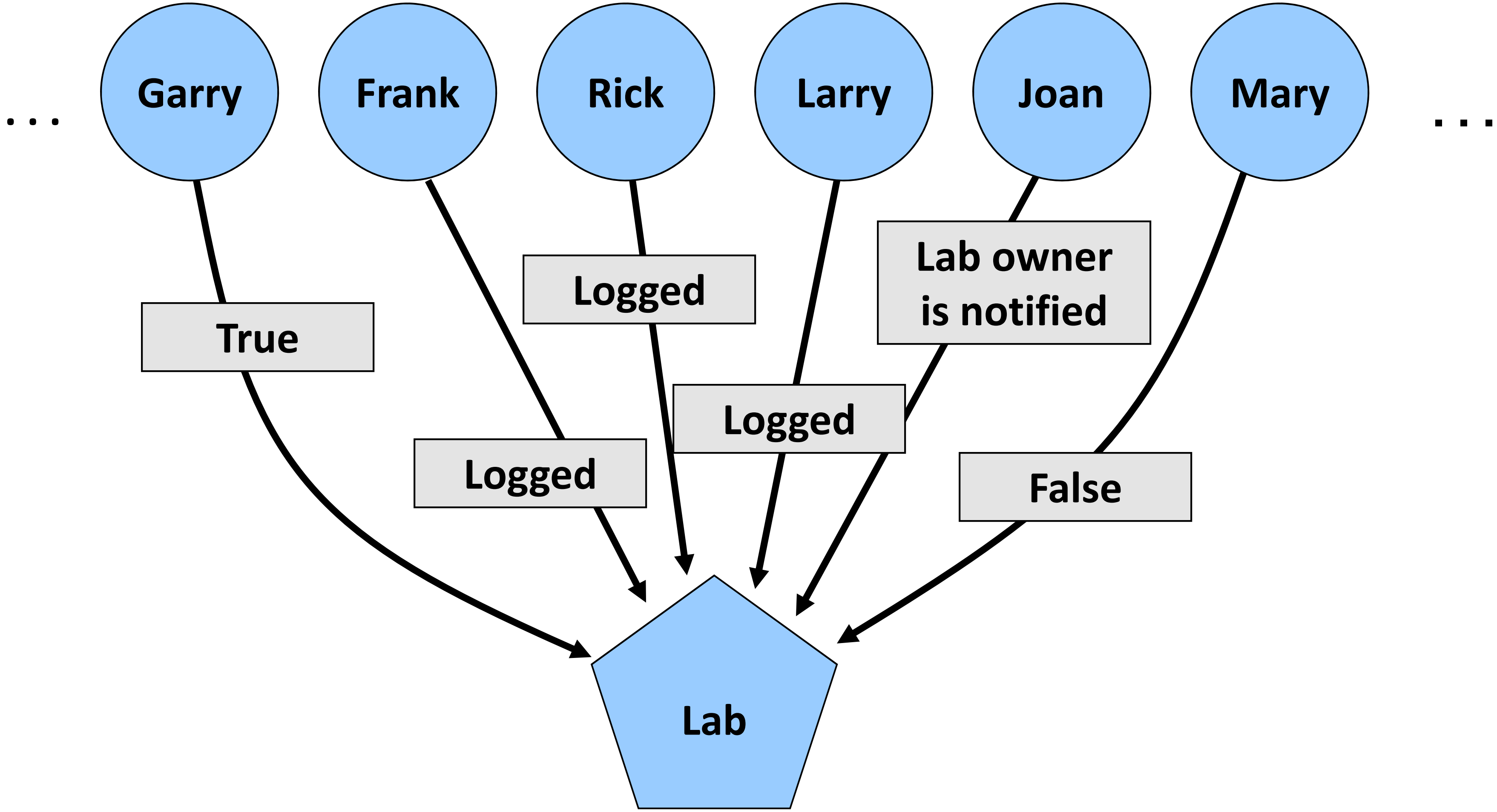
Policy-creation Study

Ideal Policies

- Ideal Policy – Policy the user would enact if not restricted by technology
- Based on interview data
- Looked at not only what was enacted but endeavored to determine why

Policy-creation Study

Policy Synthesis



Policy-creation Study

Ideal Conditions

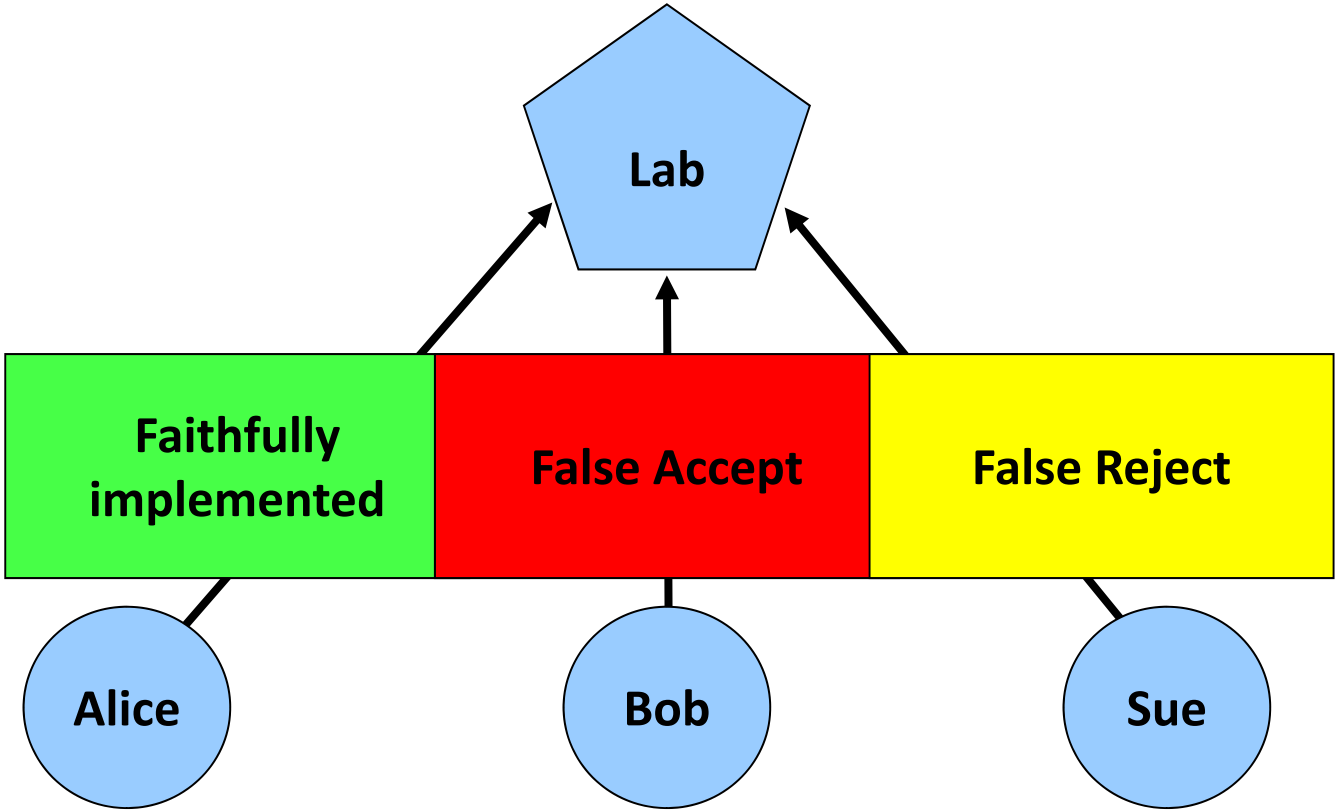
- True (can access anytime)
- Logged
- Owner notified
- Owner gives real-time approval
- Owner gives real-time approval and witness present
- Trusted person gives real time approval and is present
- False (no access)

Policy-creation Study

Policy Analysis

- **We compared each of the 244 ideal access rules, with the key and Grey rules and marked them as:**
  - False Accept – User not required to fulfill all conditions required by the ideal policy
  - False Reject – User must fulfill conditions not required by the ideal policy
  - Faithfully Implemented – Matched the ideal policy
- **The frequency of false accepts, false rejects and faithful implementations were counted**

Policy Analysis Example



Lab

Faithfully implemented

False Accept

False Reject

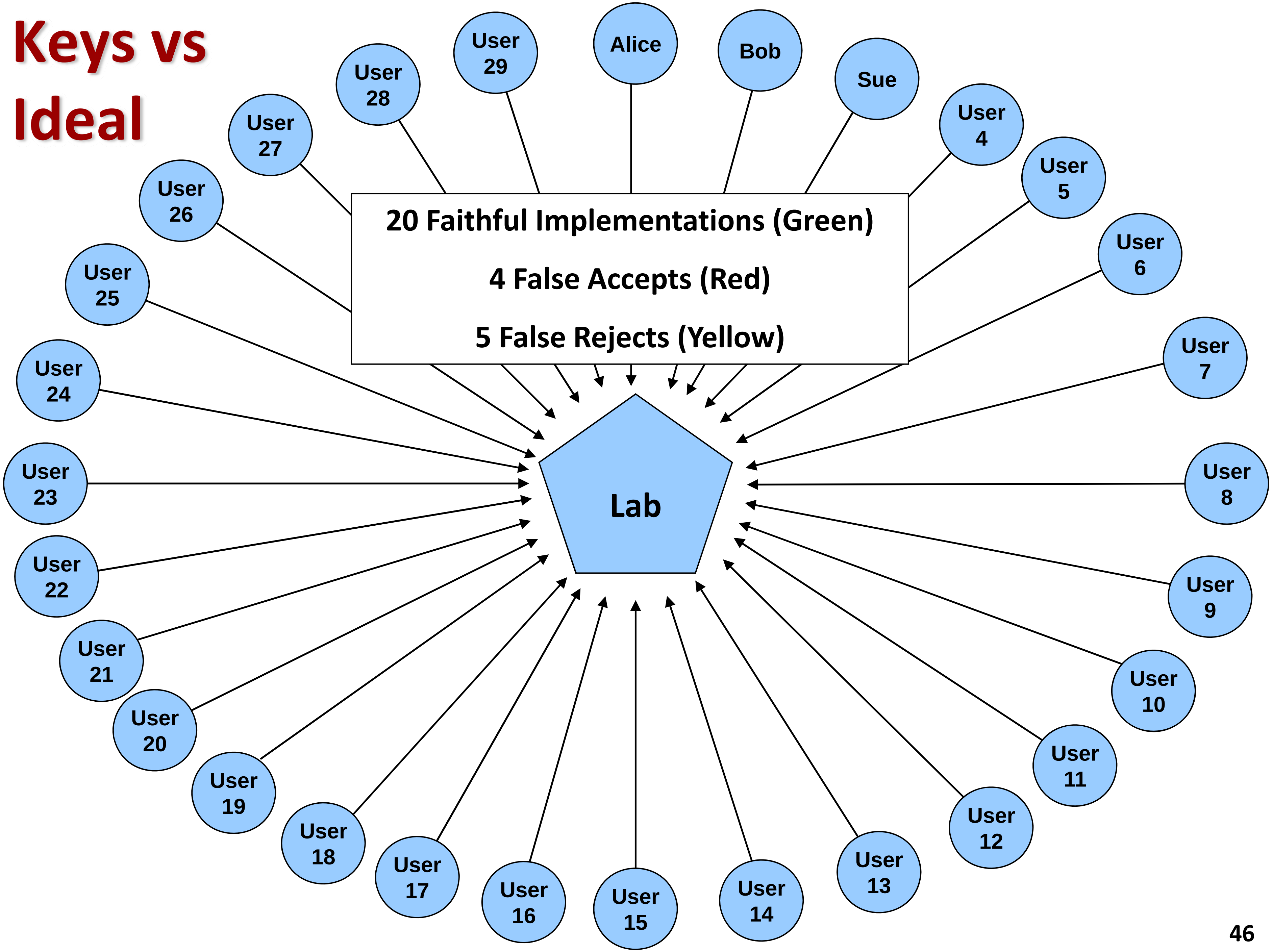
Alice

Bob

Sue

Ideal	Access anytime	Owner notified	Logged
Keys	Has a key	Has a key	No access

Keys vs Ideal

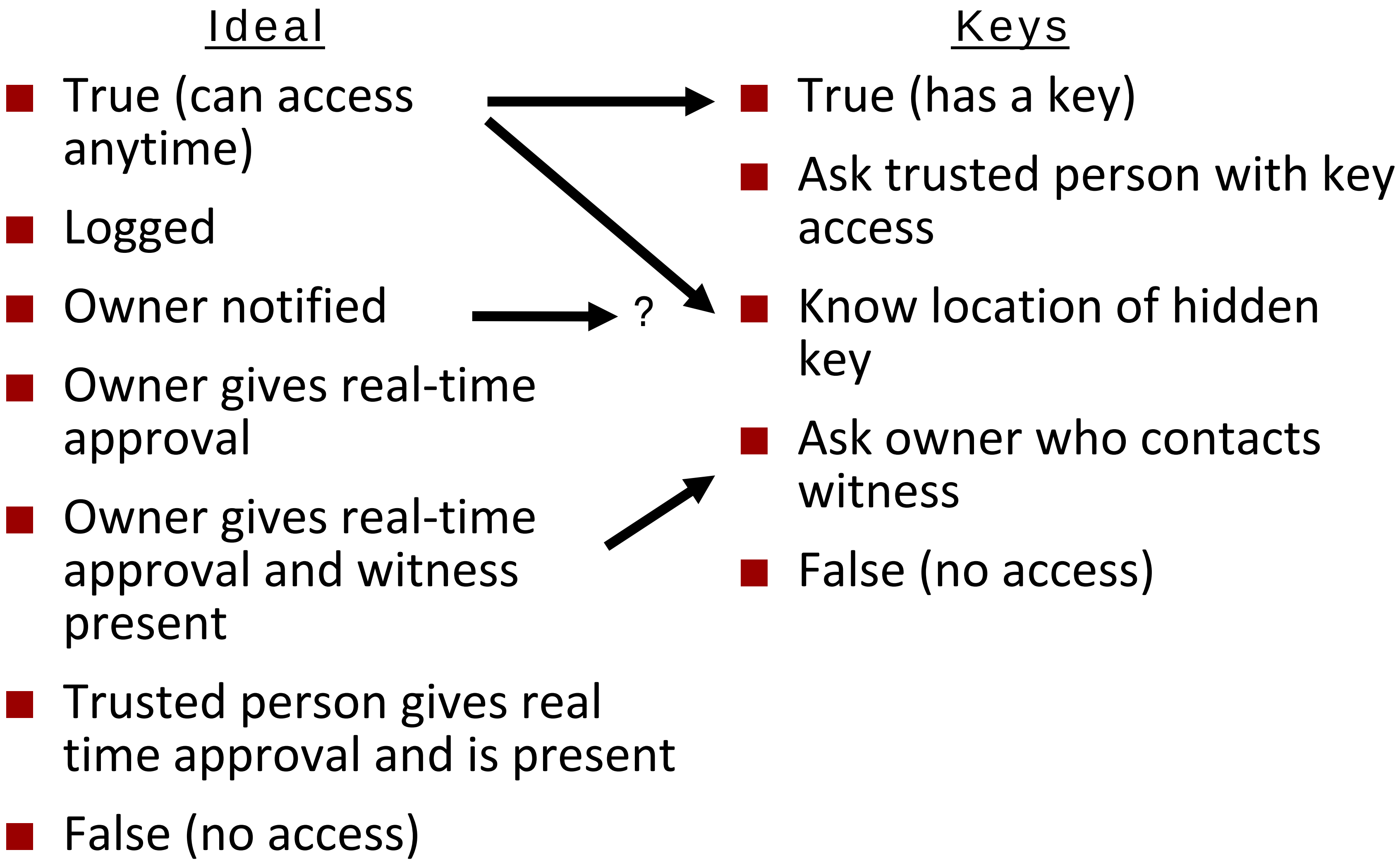


20 Faithful Implementations (Green)

4 False Accepts (Red)

5 False Rejects (Yellow)

Key Conditions



Ideal

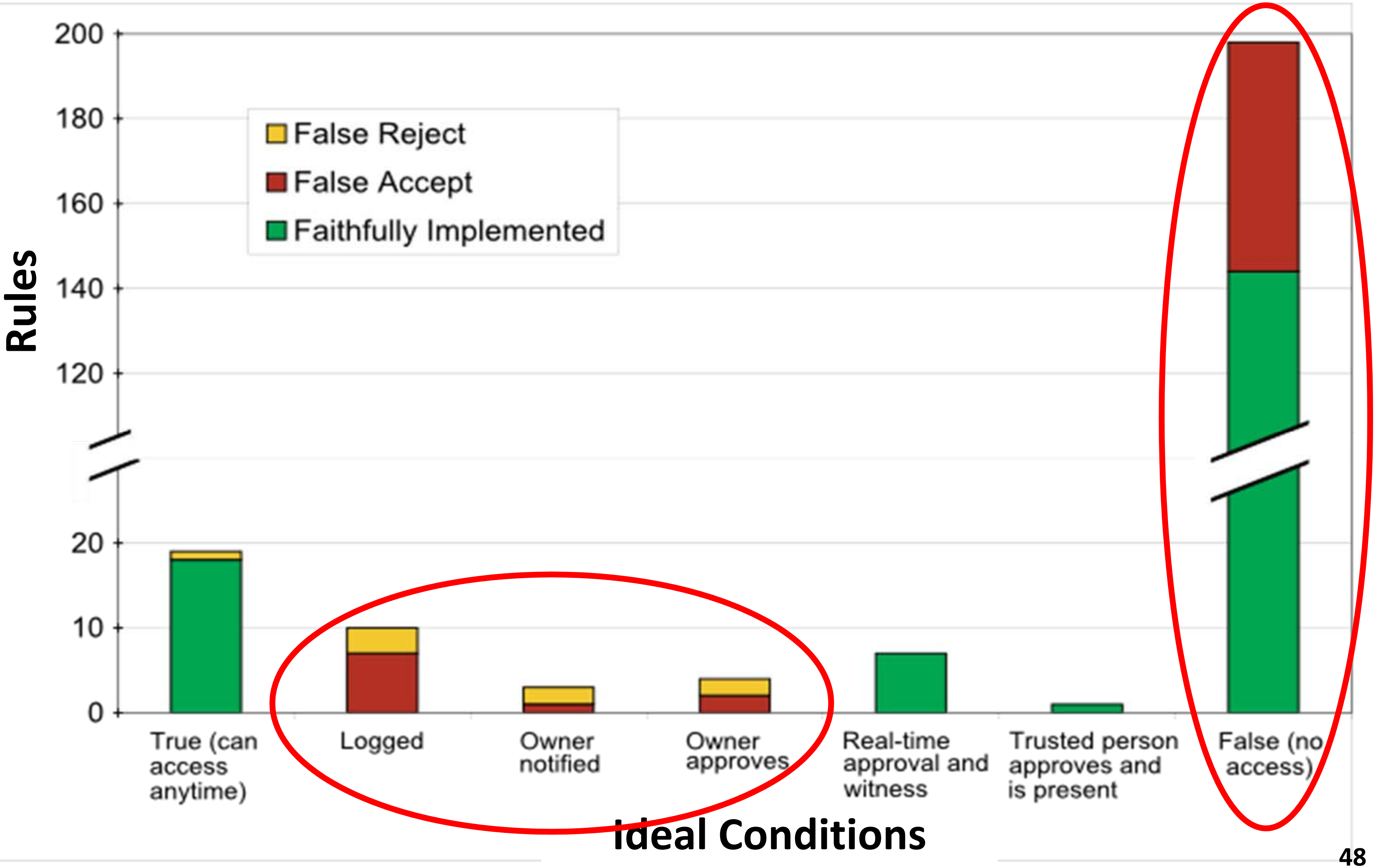
- True (can access anytime)
- Logged
- Owner notified
- Owner gives real-time approval
- Owner gives real-time approval and witness present
- Trusted person gives real time approval and is present
- False (no access)

Keys

- True (has a key)
- Ask trusted person with key access
- Know location of hidden key
- Ask owner who contacts witness
- False (no access)

Policy-creation Study

Key Implementation Accuracy



Grey Conditions

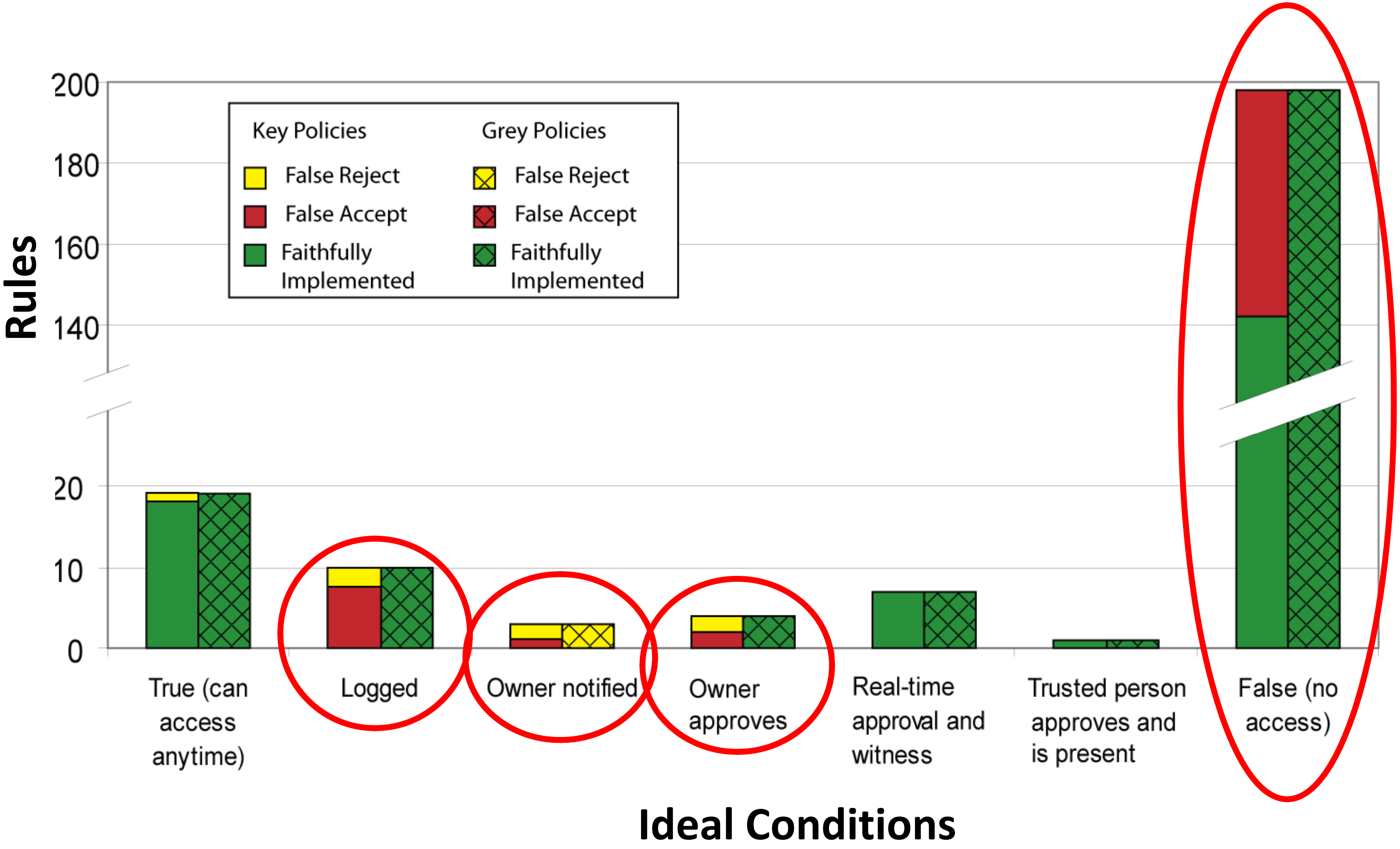
Ideal

- True (can access anytime)
- Logged
- Owner notified
- Owner gives real-time approval
- Owner gives real-time approval and witness present
- Trusted person gives real time approval and is present
- False (no access)

Grey

- True (has a delegation)
- Ask trusted person with Grey access
- Ask owner via Grey
- Ask owner who contacts witness
- False (no access)

Implementation Accuracy



Conclusion

- Grey policies more accurately implemented the desired policy
- Logging, notification and real-time approval upon request were desired features
- Future work: explore organization-wide policy and provide more supportive access-control technologies