Empirical User Studies of a Smartphone-Based Access-Control System

Mike Reiter

University of North Carolina at Chapel Hill

Joint work with Lujo Bauer, Lorrie Cranor,
Rob Reeder and Kami Vaniea.

Research question

- How well does a deployed smartphone-based access-control system match users' needs?

- Do users make more or less secure access-control decisions when using Grey than when using physical keys?

28

Policies

- A policy is a collection of rules

- A rule is a tuple containing a user, resource and condition (Bob, Alice's office, true)

Bob — True → Alice's Office
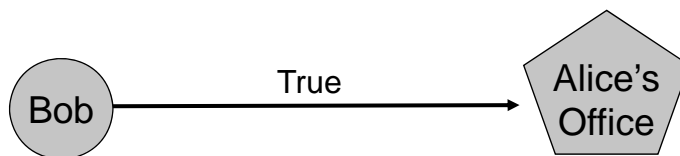
Methodology overview

- Examined access-control policies created by 8 resource owners
  - 8 offices
  - 1 machine room

- Using interviews we created ideal, key and Grey policies for each of 9 resources

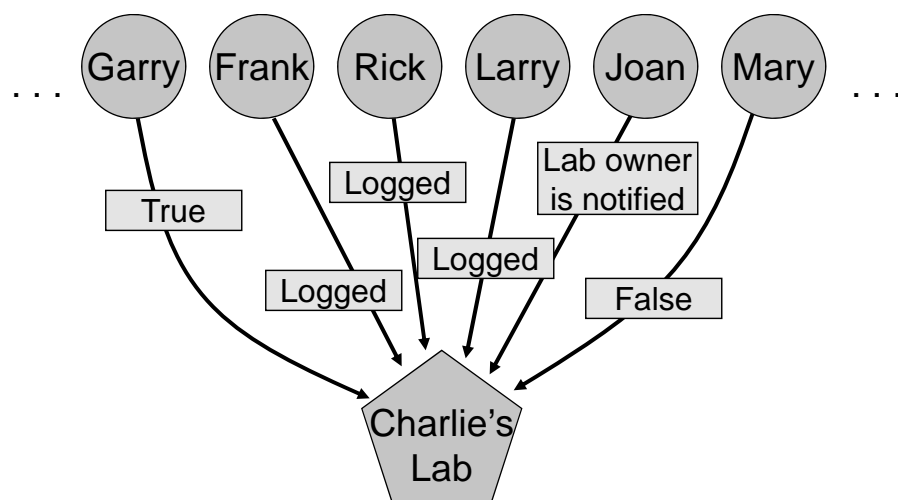- Compared ideal and implemented rules

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 synthesis

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 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
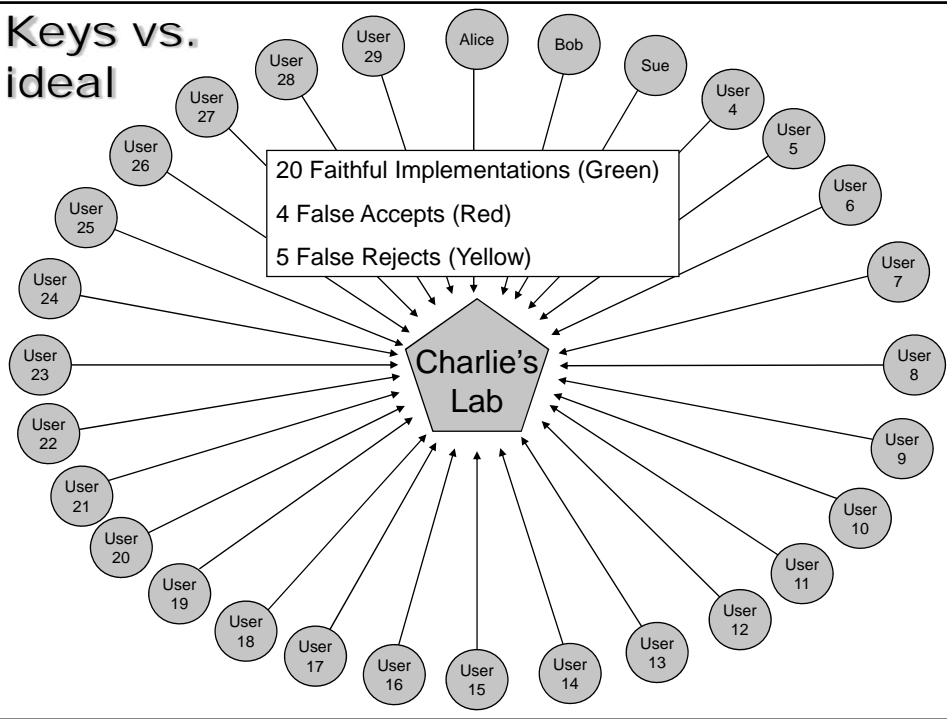 - **Faithfully Implemented** – Matched the ideal policy

Policy analysis example

Charlie's Lab

	Faithfully implemented	False Accept	False Reject
	Alice	Bob	Sue
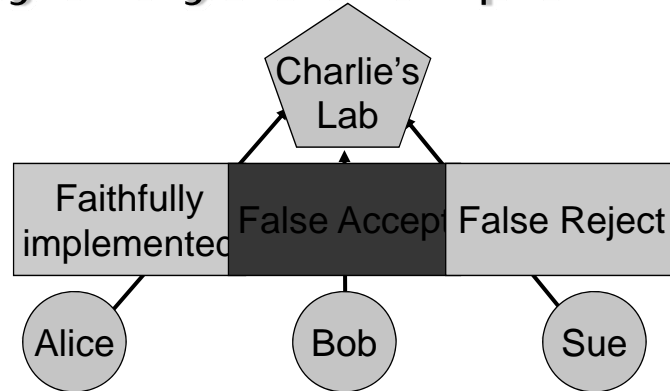
Ideal Conditions	Access anytime	Owner Notified	Logged
Key Conditions	Has a key	Has a key	Doesn't have a key

Keys vs. ideal

User 29 Alice Bob Sue User 28 User 27 User 4 User 5 User 26 User 25 User 6 User 24 User 7 User 23 Charlie's Lab User 8 User 22 User 9 User 21 User 10 User 20 User 11 User 19 User 12 User 18 User 17 User 16 User 15 User 14 User 13

20 Faithful Implementations (Green)

4 False Accepts (Red)

5 False Rejects (Yellow)

Conditions

Ideal	**Keys**
■ True (can access anytime)	■ True (has a key)
■ Logged	■ Ask trusted person with key access
■ Owner notified ⟶ ?	■ Know location of hidden key
■ Owner gives real-time approval	■ Ask owner who contacts witness
■ Owner gives real-time approval and witness present	■ False (no access)
■ Trusted person gives real time approval and is present	
■ False (no access)	

Assumptions about Hidden Keys

■ Suppose
  - Room X contains a hidden key to room Y
  - Alice can enter room X
  - Alice can enter Y's enclosure

■ Three conditions under which Alice can enter Y
  - <u>Optimistic</u>: Key policy grants Alice access to Y.
    - ■ "Users will respect the key policy".
  - <u>Moderate</u>: Key policy grants Alice access to X.
    - ■ "A user will use any hidden key in a space to which she has access by the key policy."
  - <u>Pessimistic</u>: True.
    - ■ "Users will use any key they can find."

Key implementation accuracy

Conditions

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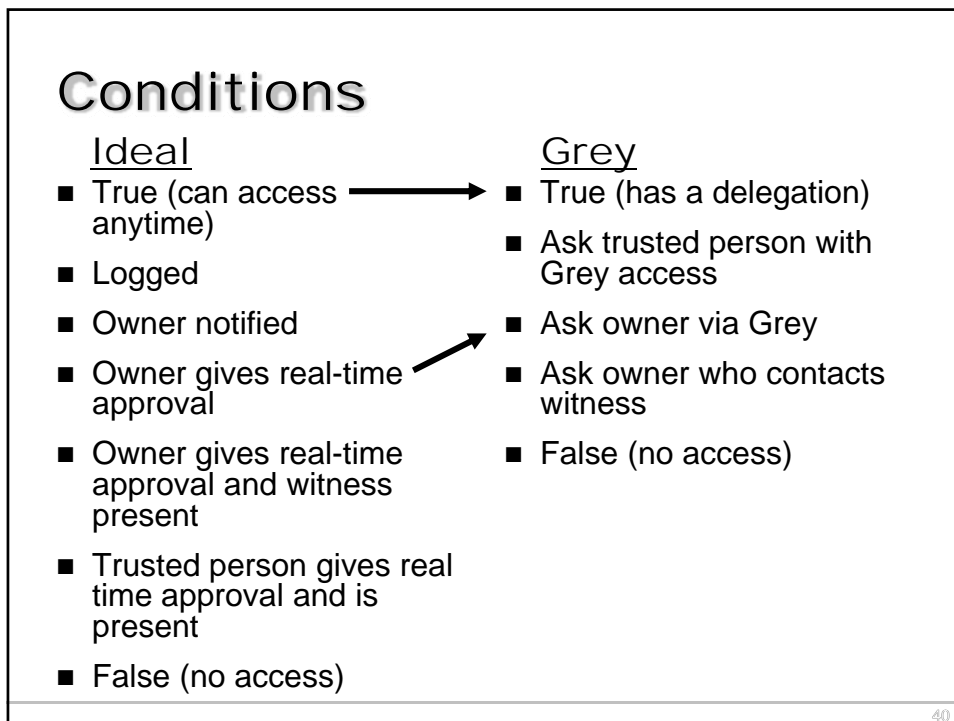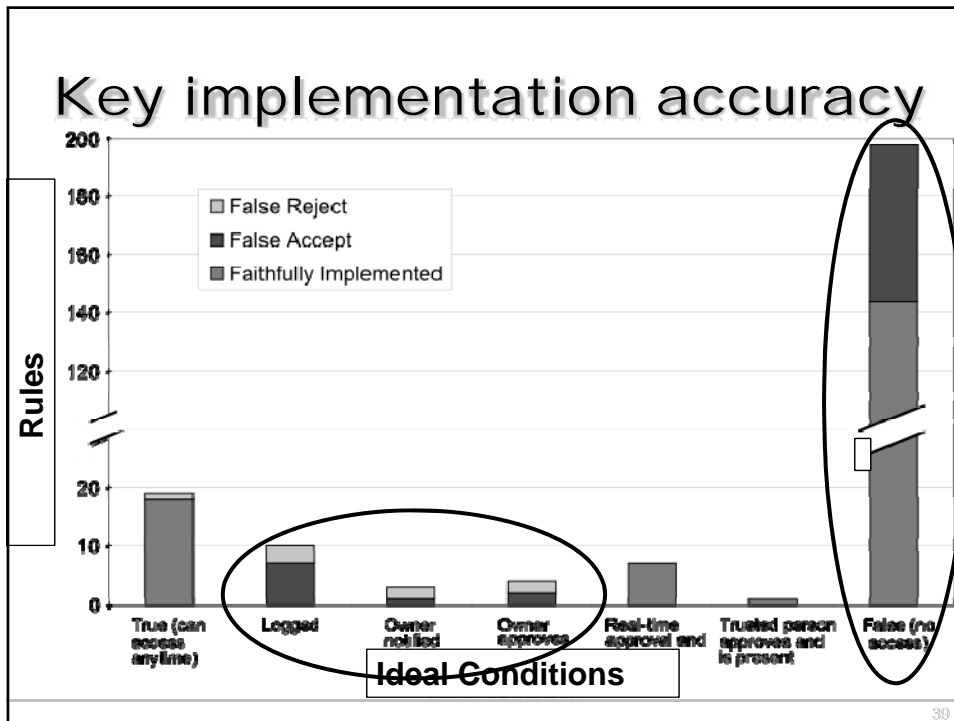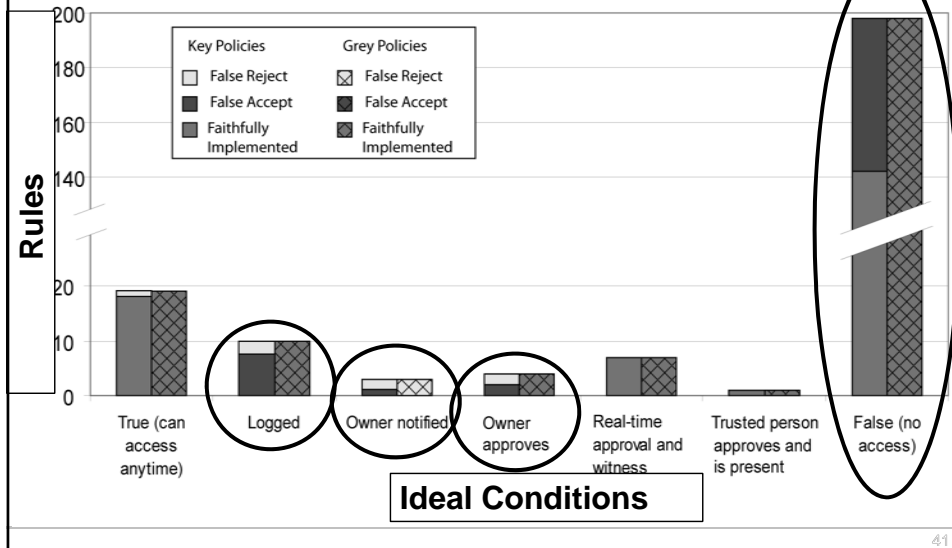- Trusted person gives real time approval and is present
- False (no access)

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

Study 2: Contributions

- Documented the collection of ideal policy data

- Developed a metric and methodology for quantitatively comparing accuracy of implemented policies

- Showed that a smarphone access-control system outperformed keys in overall security and effectiveness

42