User-Controllable Privacy and Security for Pervasive Computing

Norman Sadeh (PI), Lujo Bauer, Lorrie Cranor, Jason Hong, Bruce McLaren, Michael Reiter, Paul Hankes Drielsma

School of Computer Science & CyLab - Carnegie Mellon University

URL: www.cs.cmu.edu/~sadeh/user_controllable_security_and_privacy.htm - NSF Award Number: CNS-0627513 (Sept. 2006 - Aug. 2010)

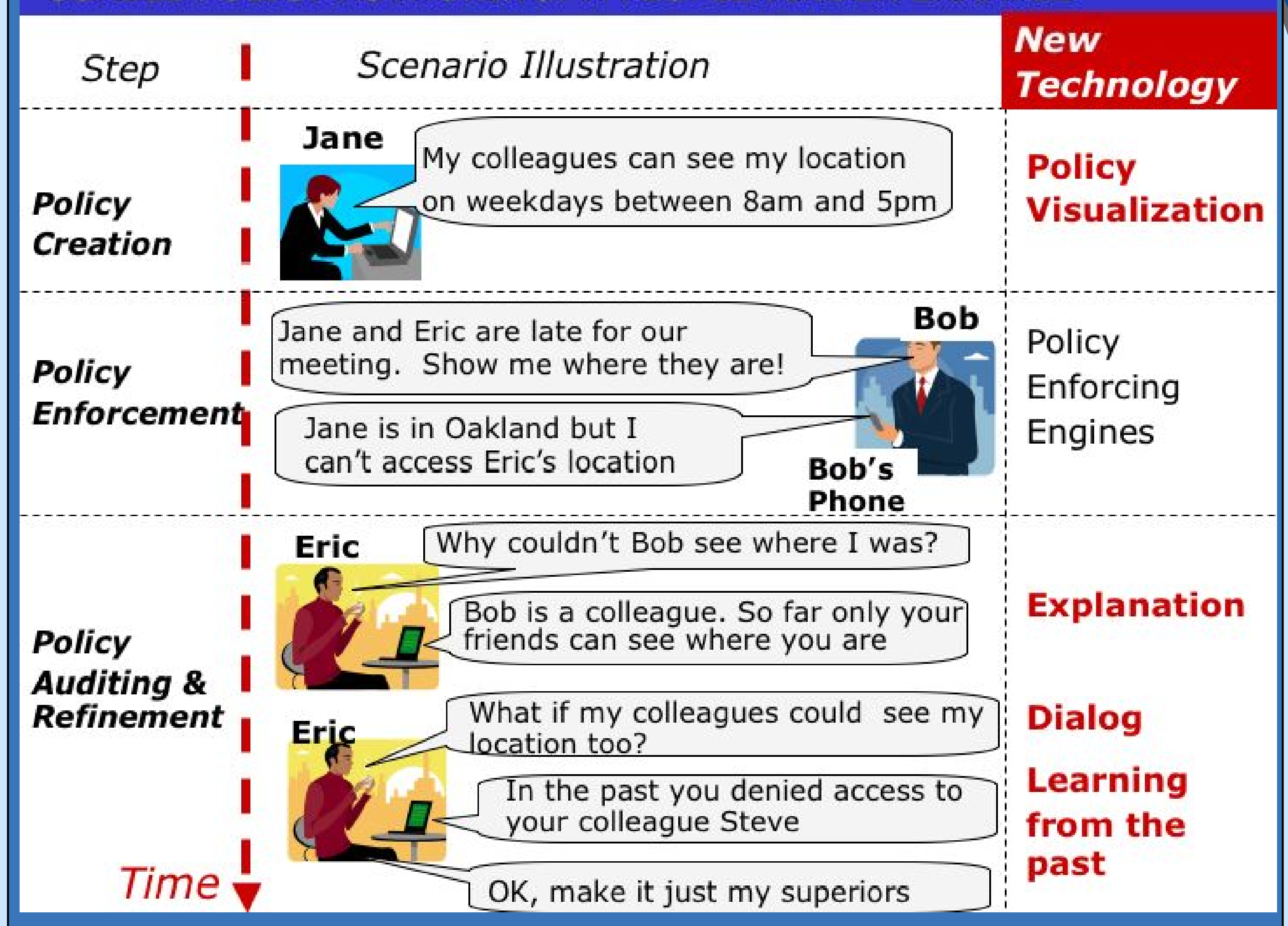
MOTIVATION

- **Users interact with a large and growing number of policies**, e.g. mobile location-based applications, social networking privacy policies, home firewalls and routers
- But end users have great difficulty **specifying and maintaining their security and privacy policies**
- Poor specification can lead to security breaches **or unintended disclosure of private information**

OBJECTIVES

- Develop interface technologies that **help users maintain their security & privacy policies**
- Evaluate tradeoffs **between expressiveness, tolerance for errors, burden on users and overall user acceptance.**
- Validation through frequent and extensive **user studies** – lab studies as well as studies “in the wild”

USABLE POLICY AUTHORING: A PEOPLE FINDER EXAMPLE



Step
Scenario Illustration
New Technology
Policy Creation
Jane
My colleagues can see my location on weekdays between 8am and 5pm
Policy Visualization
Policy Enforcement
Jane and Eric are late for our meeting. Show me where they are!
Bob
Jane is in Oakland but I can’t access Eric’s location
Bob’s Phone
Policy Enforcing Engines
Policy Auditing & Refinement
Eric
Why couldn’t Bob see where I was?
Bob is a colleague. So far only your friends can see where you are
Explanation
What if my colleagues could see my location too?
Eric
Dialog
In the past you denied access to your colleague Steve
Learning from the past
OK, make it just my superiors
Time

Using dialog, explanation, learning, and visualization technologies to empower users to more effectively control their security & privacy policies

Multiple Lines of Attack: 2 Examples

Visualization

Expandable grids allow users to effectively view and manipulate policies at different levels of granularity, enhancing the ability to identify policy errors & supporting conflict resolution.

Benefits: Improved accuracy & heightened sense of user control.

- Higher accuracy measured across 14 Windows file permission configuration tasks – with improvements up to 80%

Mixed-Initiative Policy Improvement

New family of machine learning (ML) techniques provide users with suggestions of how to improve their policies.

Benefits:

- Moves away from traditional “black box” configuration of ML algorithms
- Users retain control over policy changes (e.g. avoiding poor generalizations) & work hand-in-hand with system on common model
- Validated on scenarios derived from PeopleFinder pilots – up to 90% accuracy

Current Application Domains

Contextual Instant Messenger

Users inquire about each other’s context (interruptability, location, and current task) through an instant messaging service.

PeopleFinder

Laptop and cell-phone users can selectively share their locations with others, subject to privacy policies they can refine over time.

Phone-Based Access Control

Smart phones act as tokens by which users grant access to rooms, subject to security policies maintained directly on the phones

RESULTS AND BROADER IMPACT

- Broad adoption of many mobile and pervasive computing applications hinge on users feeling that they have **adequate control** over their privacy and security
- Our policy authoring solutions have been shown to empower users to more **accurately** define their policies in different domains

National Science Foundation
WHERE DISCOVERIES BEGIN

**NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT**

Carnegie Mellon
CyLab
CONFIDENCE FOR A NETWORKED WORLD