

---

# SecurePlace



---

Usable privacy protection

# Timeliness

“The main reason we do not have usable security is that users don’t have a model of security they can understand. “

“We need to build systems that improve users’ ability to make sense of, and thereby regulate, their privacy.”

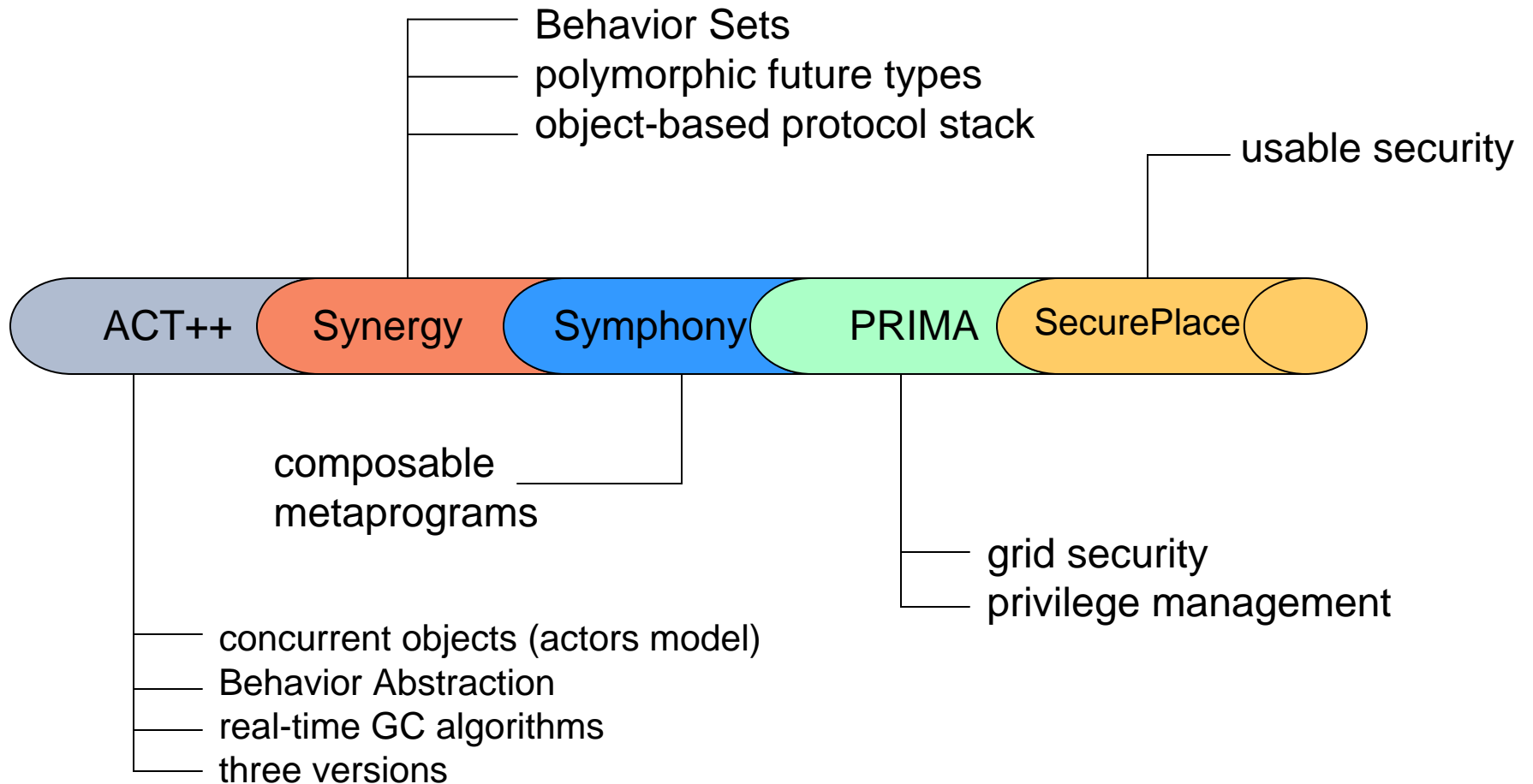


Communication of the ACM, November 9, 2009

# Characterization



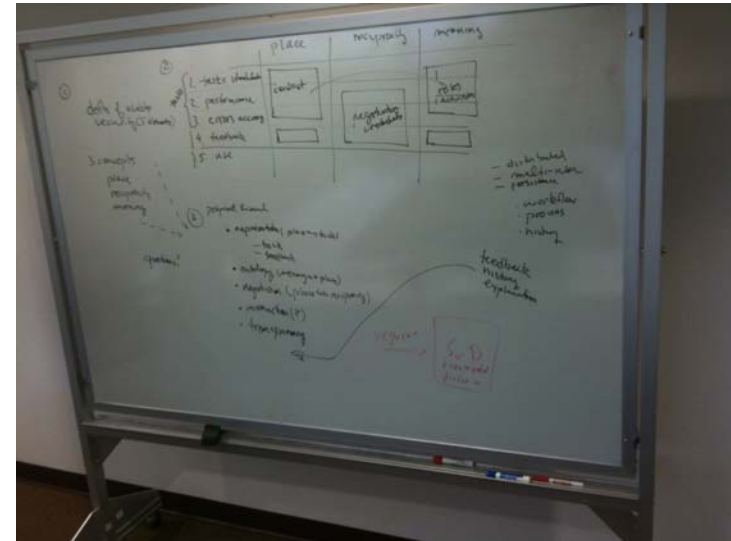
# Research Trajectory



# Getting Started

Draw pictures...

Form a team...



Teach a class...

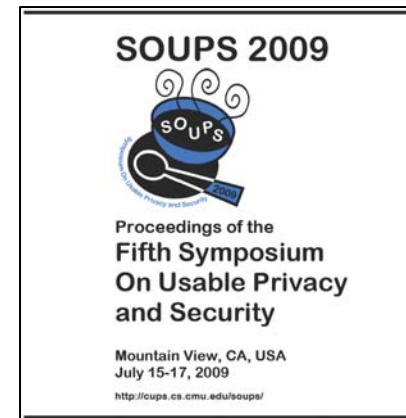


<http://courses.cs.vt.edu/cs6204/UsableSecurity>

Read papers...



Go to the meeting...



---

# Outline

- The Problem
- Privacy
- SecurePlace
  - Overview
    - General idea
    - Applications/Scenarios
  - Conceptual framework
  - Assessing usability
  - Research framework
  - Architecture
  - Interface metaphors
- Conclusion

---

# Concern

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be left alone”. ... modern enterprise and invention have, through invasions upon his privacy, subject him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”

## **“The Right to Privacy”**

**Warren and Brandeis**

---

Harvard Law Review.

# Concern

## “The Right to Privacy”

Warren and Brandeis

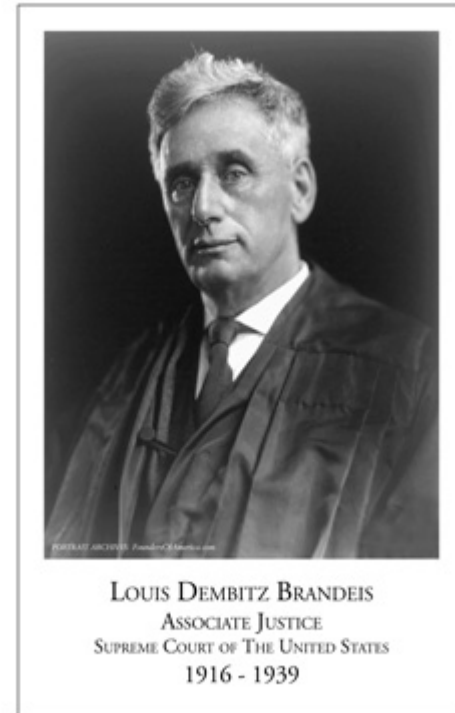
---

Harvard Law Review.

---

Vol. IV December 15, 1890 No. 5

---

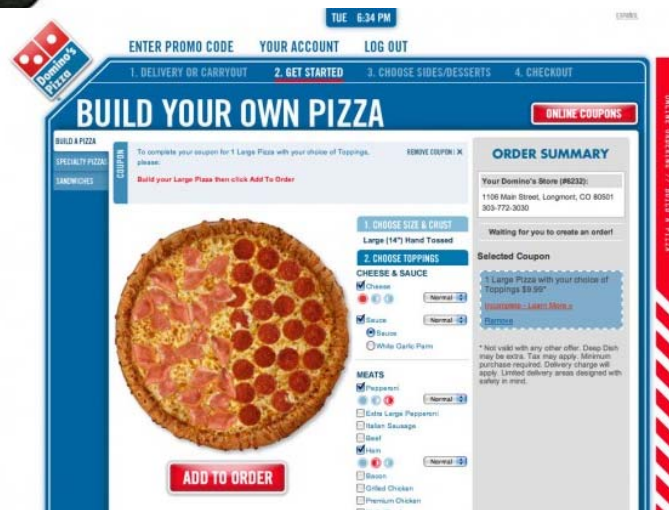


FoundersOfAmerica.com

# Promise and Peril

	Service	Threat
Web	e-commerce email social networking news, entertainment search electronic medical records recommendations	identity theft spam phishing unwanted correlation privacy incursion denial of service viruses, worms, ...
Ubiquitous systems	context awareness location awareness pervasive services smart objects	loss of privacy, anonymity electronic stalking invasive monitoring loss of control

# A view of the future?



<http://www.aclu.org/pizza/images/screen.swf>

# Grand Challenge

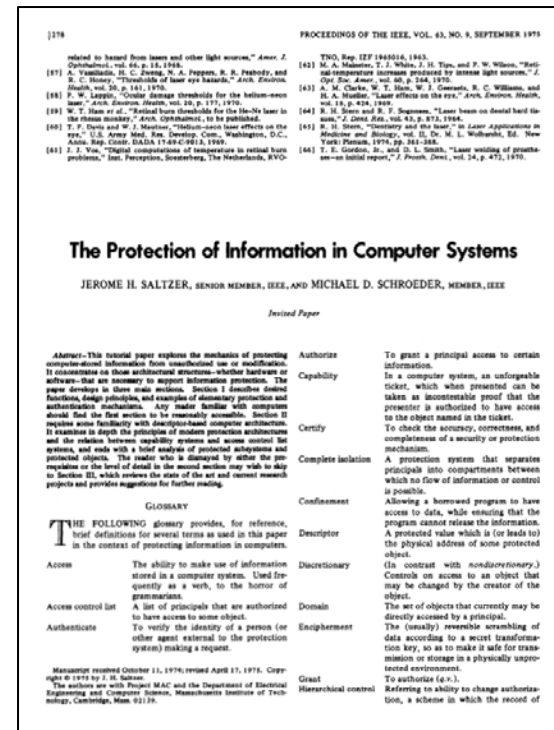
“For the dynamic, pervasive computing environments of the future, give computing end-users security they can understand and privacy they can control.”



Computer Research Association (CRA), 2003. Four Grand Challenges in Trustworthy Computing, CRA Conference on Grand Research Challenges in Information Security and Assurance, Airlie House, Warrenton, Virginia, November 16–19, 2003.

# Not a new issue

“ h) Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.”



Jerome H. Saltzer and Michael D. Schroeder, The protection of information in computer systems, in *Proceedings of the IEEE*, Institute of Electrical and Electronics Engineers, Inc., 63(9), September 1975, pp.1278-1308.

# Unique challenges of privacy/security

- Security is not the user's primary goal
- Must be usable by a wide range of individuals with differing skills sets
- Higher risk associated with failure of security applications than for other application types
- Need for updates to account for changes in law, organizational practices, or personal preferences.

Karat, C.-M., J. Karat, and C. Brodie, Editorial: why HCI research in privacy and security is critical now. International Journal of Human-Computer Studies, 2005. 63(1-2): p. 1-4.

# Nature of Privacy

- A “boundary regulation process” of accessibility depending on “context” (Altman)
- A “personal adjustment process” (Westin) balancing the desire for privacy against the desire to interact in the context of social norms and their environment
- A distinction (Solove) between *access control* (regulating access to information about oneself) and *risk management* (reducing likelihood of unintended/undesired usage)
- Preferences (Westin’s classifications)
  - ❑ Fundamentalists (15-25%)
  - ❑ Pragmatists (40-60%)
  - ❑ Unconcerned (15-25%)

**Privacy is a vital part of your identity and self-presentation. Deciding what to reveal to whom is part of deciding who you are.**

Katie Shilton, “Four Billion Little Brothers? Privacy, mobile phones, and ubiquitous computing,” CACM November, 2009.

---

# SecurePlace

**Goal:** the development of an integrated set of devices, interfaces, services, and protocols which together create a usable means for ordinary individuals to have effective privacy control.

**Domain:** socio-technical settings, that is, technology-rich environments in which people are in direct face-to-face contact with each other but which extend beyond that location and time.

## Theoretical Foundations:

- **Place:** the social constructions made in a given spatial/physical context
- **Reciprocity:** the exchange of information/credentials appropriate to a given place, a set of people, and their relationships
- **Meaning:** semantic descriptions of the place, activities, actors,...

## Applications:

- Personal Medical Information
- Smart Home

# Scenario



The local place:

- Certificates: authoritative, place-specific, sense-able
- User's device: secure, context-aware, networked
- Disclosure: visible, controllable
- Capture: information, including a spatial representation, that allows subsequent control of disclosed personal information



The extended place:

- Use the spatial representation and captured information to present a place-based interface.
- Support via the place-based interface audit/review of access, policy authoring, changes in policy



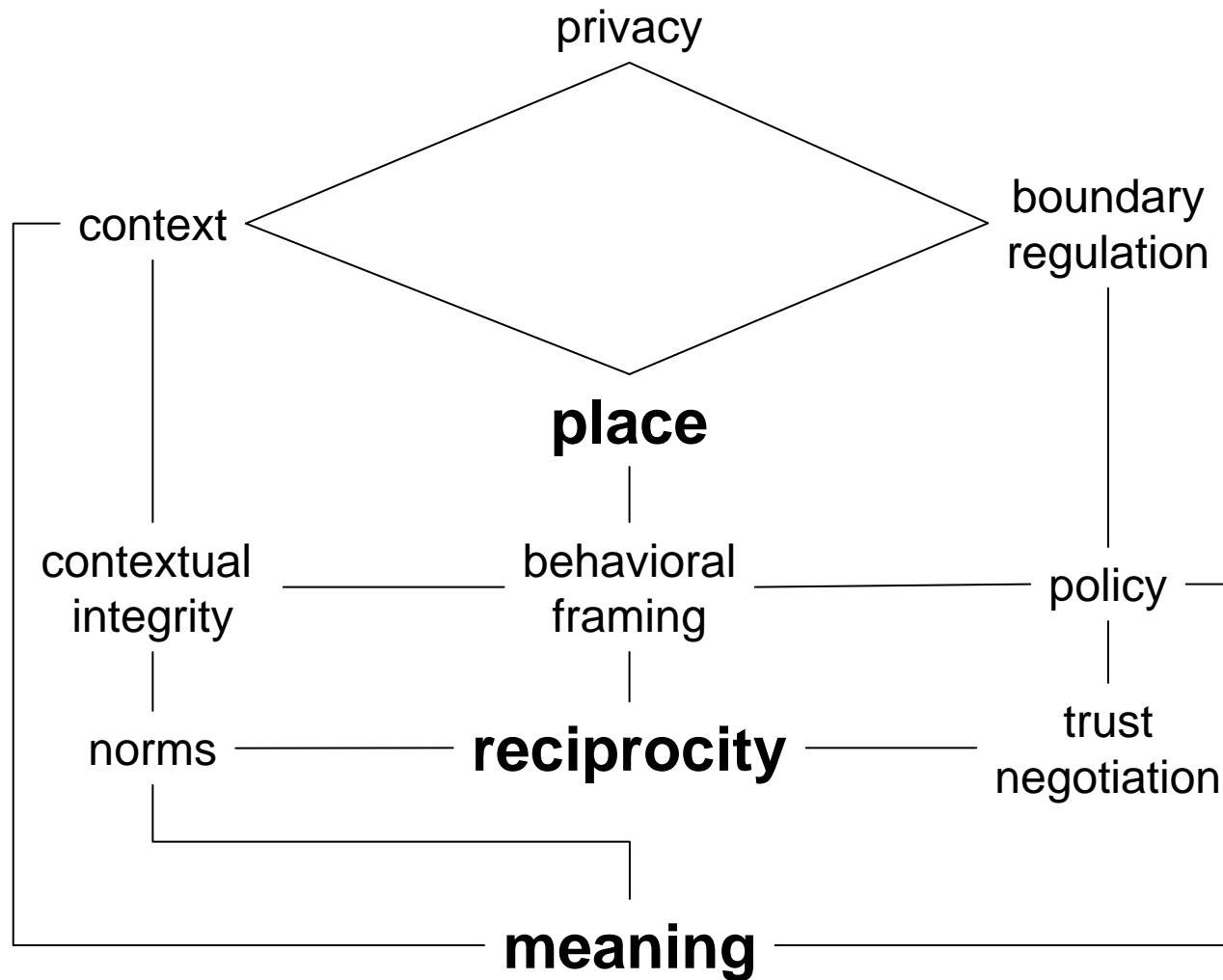
Google earth

# Smart Home

- Physical privacy/security
- Remote access
- Conflicts and priorities
- Second Life Model



# Conceptual Framework



---

# Assessing Usability

**Definition:** A system to control privacy of personal information is usable if the people who are expected to use it:

1. (**awareness**) are reliably made aware of the privacy-related tasks they need to perform;
2. (**function**) are able to figure out how to successfully perform those tasks;
3. (**reliability**) don't make dangerous errors;
4. (**transparency**) are provided evidence that the system is operating in accordance with their stated intentions; and
5. (**satisfaction**) are sufficiently comfortable with the system to continue using it.

# Research Framework

		Conceptual Framework		
		place	reciprocity	meaning
Usability	awareness	context boundary regulation behavioral framing		
	function		trust negotiation behavioral framing norms	<i>ontology, reasoning</i> (context, policy, norms)
	reliability			
	transparency	<i>review</i>	<i>explanation, notification, approval</i>	
	satisfaction	contextualized	empowering	comprehensible

Representation
Negotiation
Ontology

Feedback
Evaluation

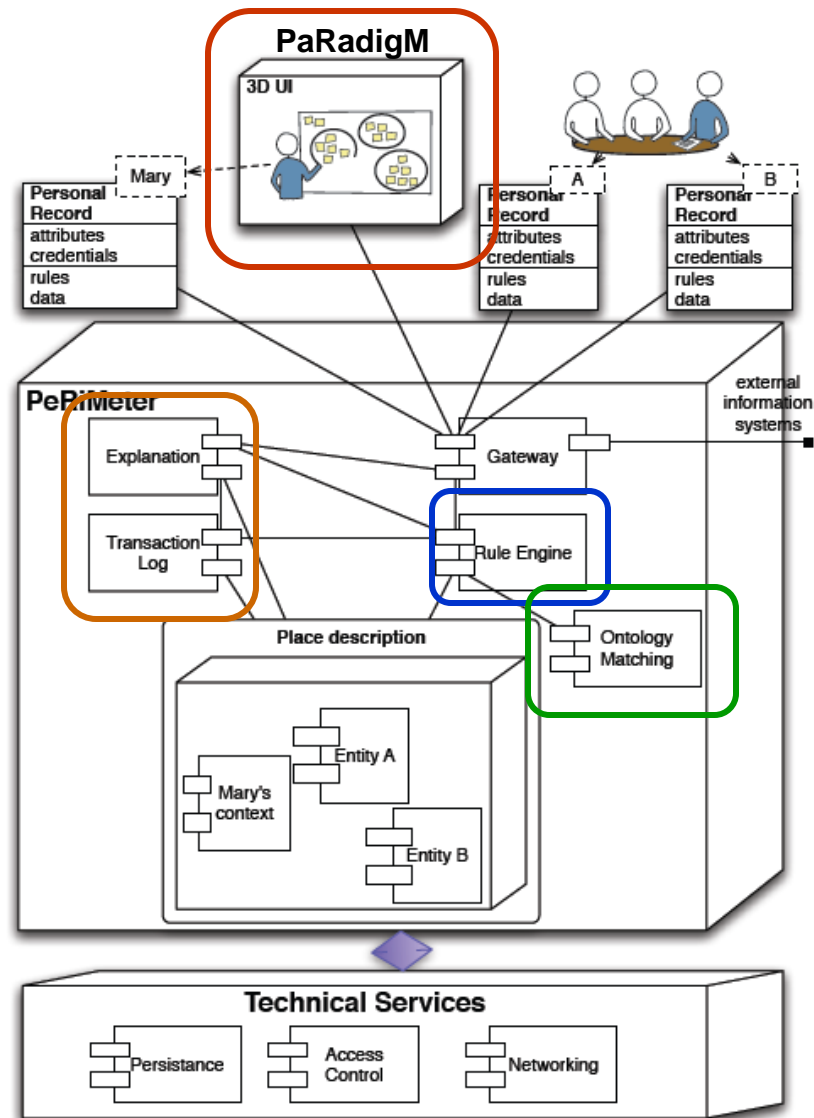
# Architecture

Representation

Negotiation

Ontology

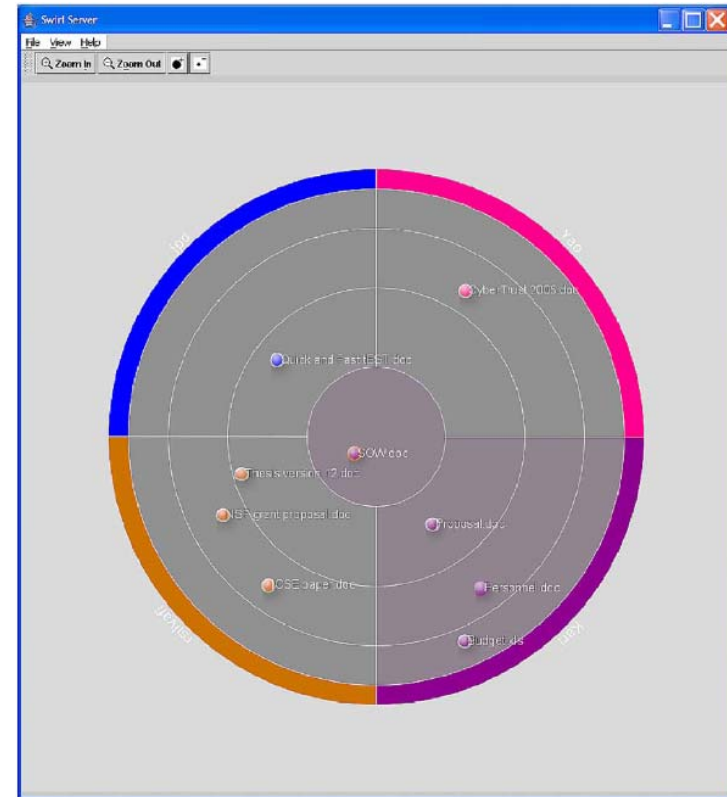
Feedback



# Spatial Interfaces

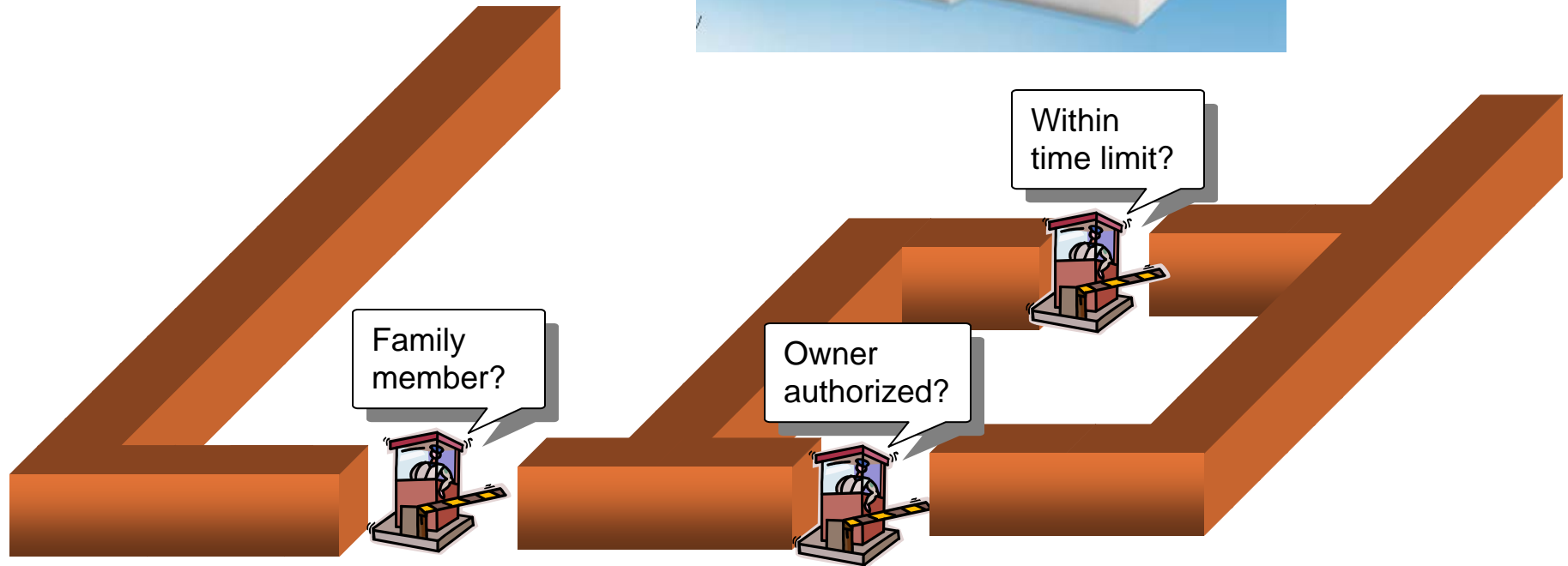


Bergmann, M., M. Rost, and J.S. Pettersson, Exploring the Feasibility of a Spatial User Interface Paradigm for Privacy-Enhancing Technology

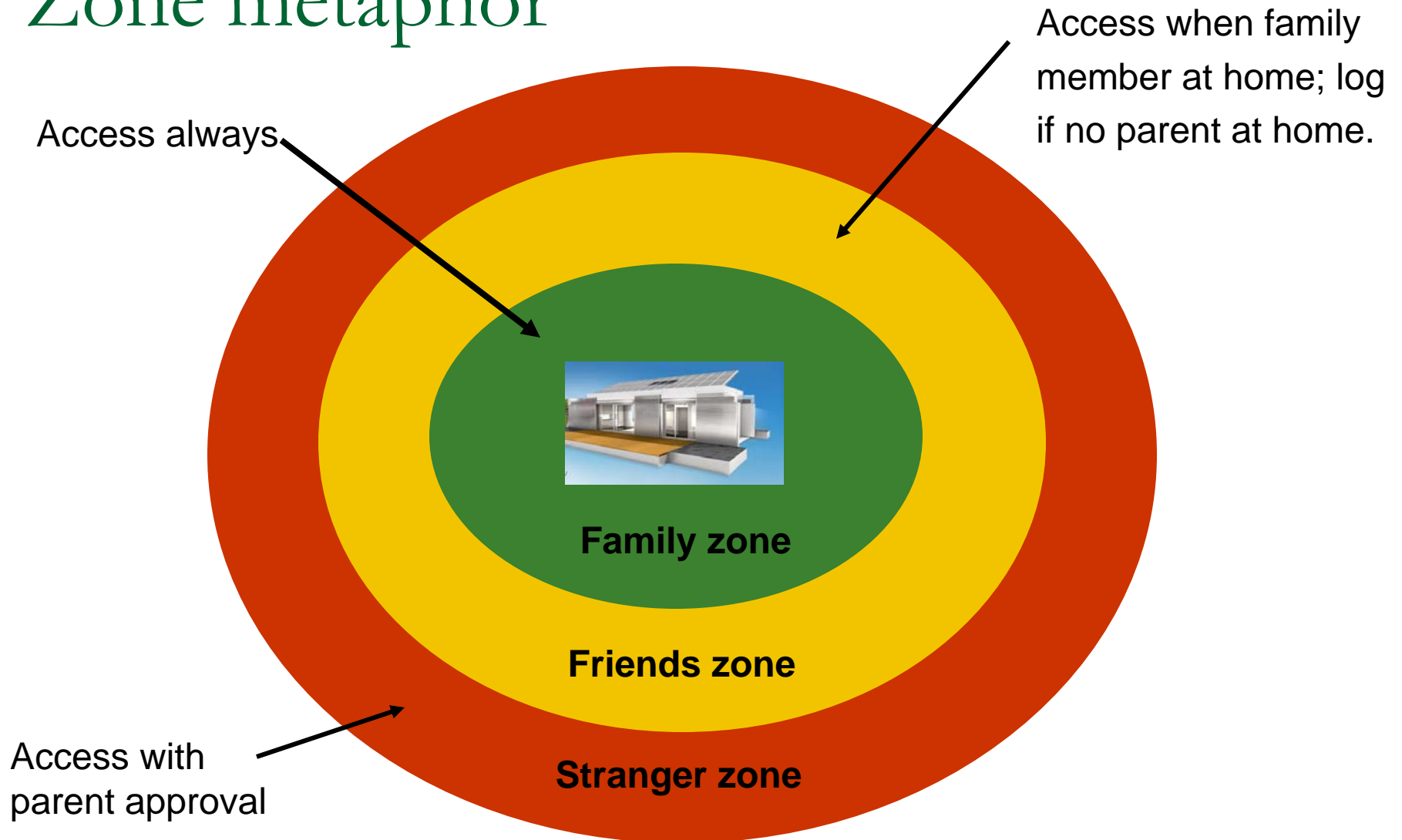


de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Ren, J., Rode, J. A., and Filho, R. S., In the eye of the beholder: a visualization-based approach to information system security.

# Wall/guard metaphor



# Zone metaphor



# Conclusion



---

# Questions?