Usability Meets Access Control: Challenges and Research Opportunities

Konstantin (Kosta) Beznosov (moderator)

Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
University of British Columbia, Vancouver, Canada

to paraphrase

C. Kaufman, R. Perlman, and M. Speciner
Network Security–Private Communication in a Public World

Humans are incapable of correctly using DAC, MAC, or RBAC, and they have unacceptable error rates and attention span when configuring access controls. (They are also large, expensive to maintain, difficult to manage, and they pollute environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our models, architectures, and technologies around their limitations.)

panel schedule

- 15-20 minute panel description and introduction of the panelists

- 4x(5-7) minute presentation from each panelist

- Q&A the rest of the time

recent resurgence of interest in usable security

- e-mail crypto
- password managers
- authentication of
  - users to web sites
  - web sites to users
- anti-phishing
- CAPTCHAS

Hey!
What about access control?

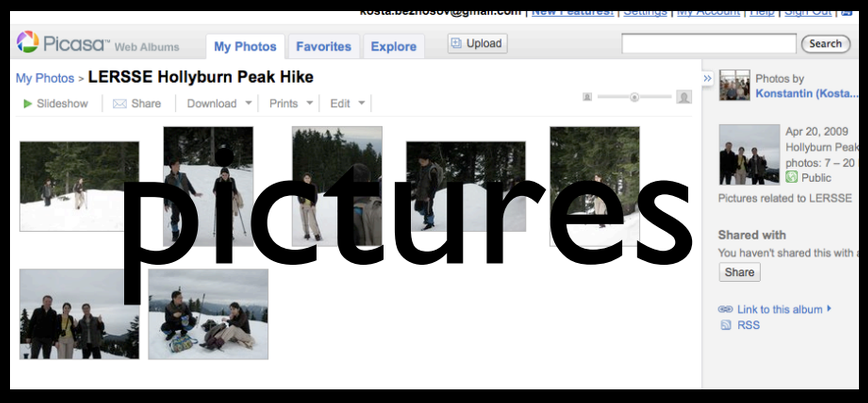
new applications require useful access controls

- controlled sharing of Web 2.0 content
  - social networks
  - software as services (SaaS)
- ad-hoc sharing
  - P2P
- Grid and cloud computing

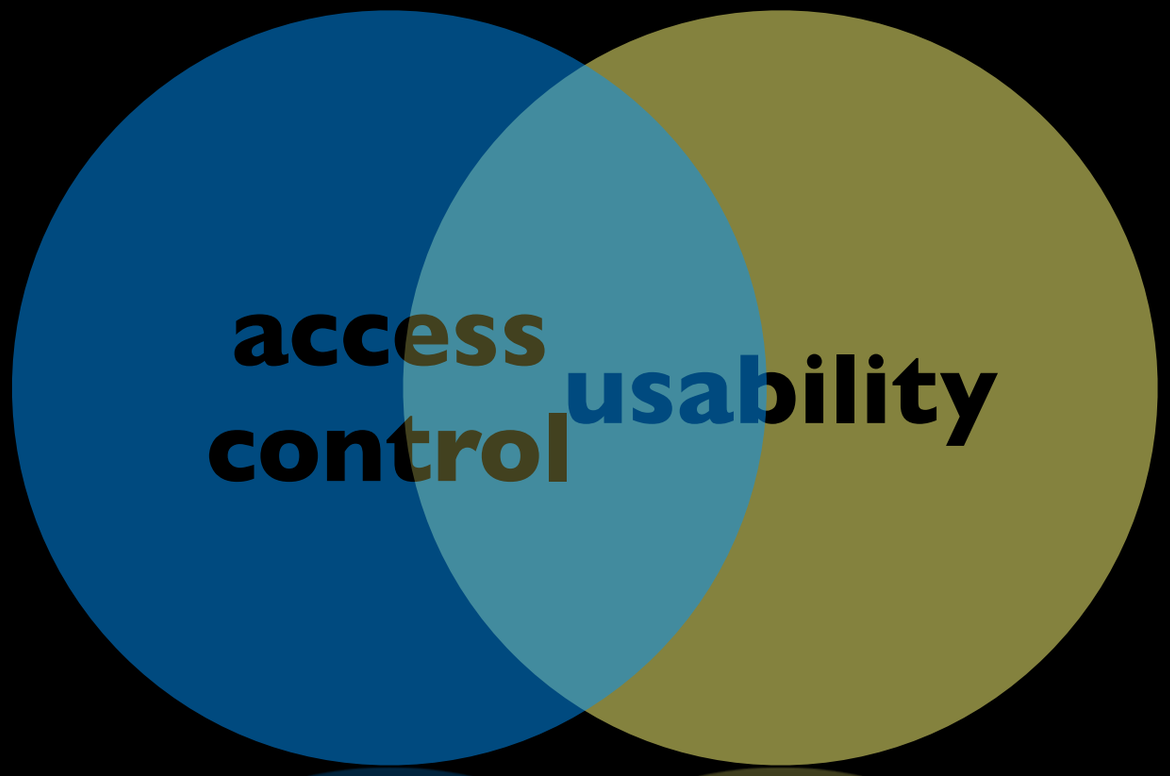
Web 2.0

users without special technical skills

generate, post, and share content on the Web



- personal biographic information
- user physical location information



numerous
practical & research
challenges & questions

just few for starters

controlling access to personal computer files

- Why very few use ACLs on the files?
  - users cannot understand implications of their changes on ACLs [Reeder at al.; CHI '08]

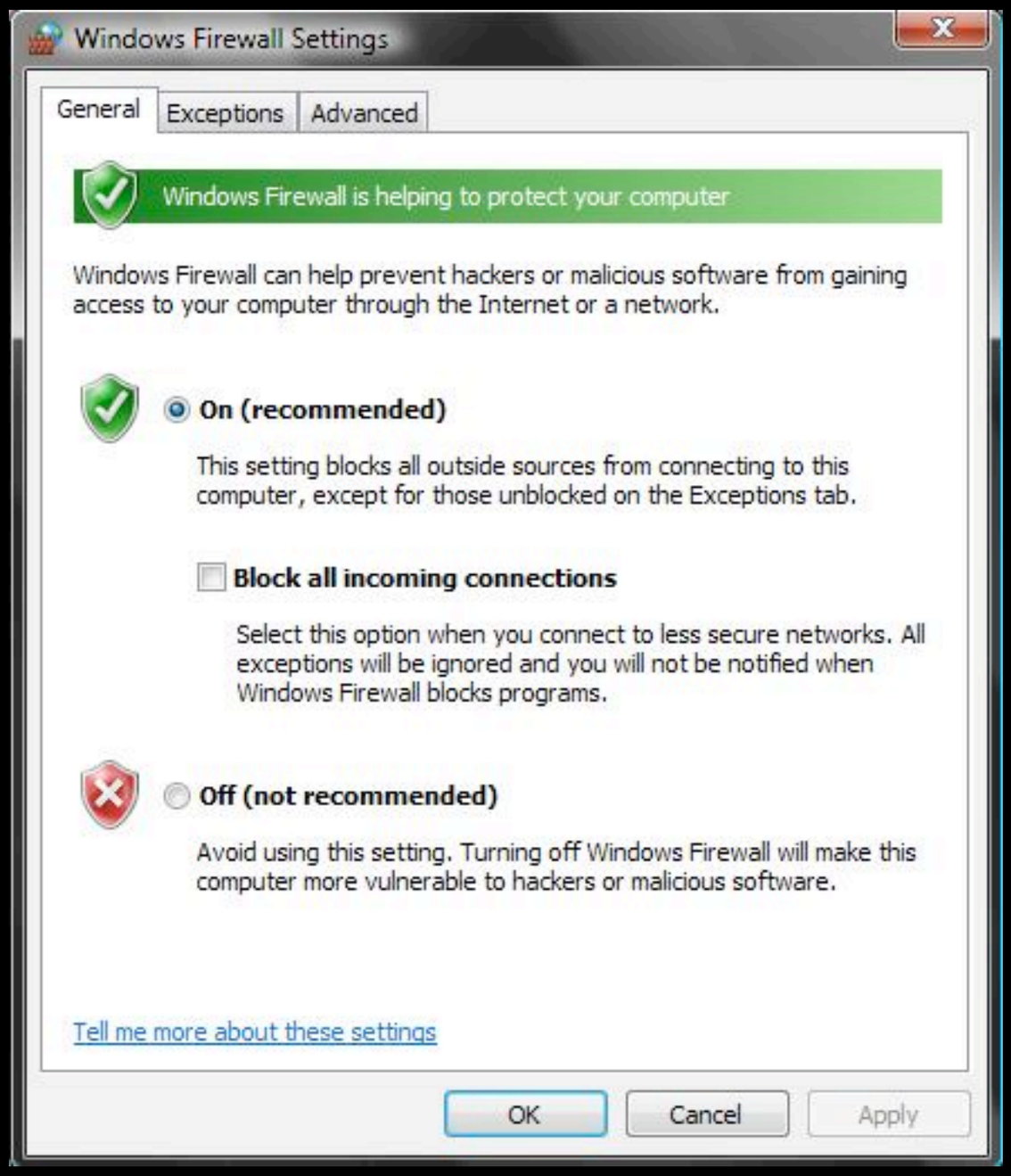
needs for access controls vary

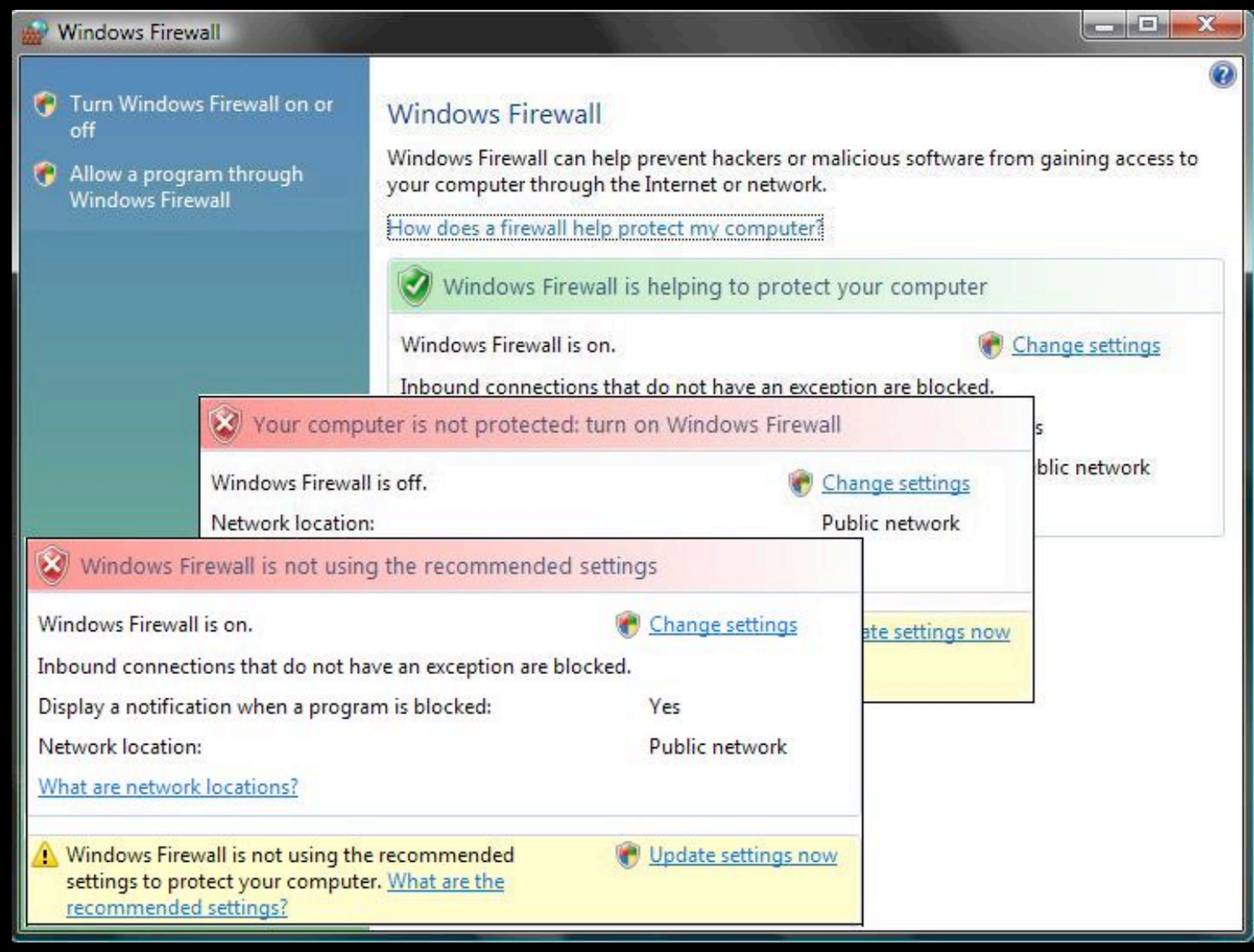
- novices -- average user from the street
- intermediate -- know what they are doing
- power -- IT guys
- experts -- system and security admins

zooming in on novices

- what controls if any should be provided?
  - under what circumstances?
- how such controls be both usable and “secure”?
  - correct understanding of the system state
    - mental model
  - no dangerous errors
  - gentle learning curve, low overhead

case in point:
MS Vista personal firewall

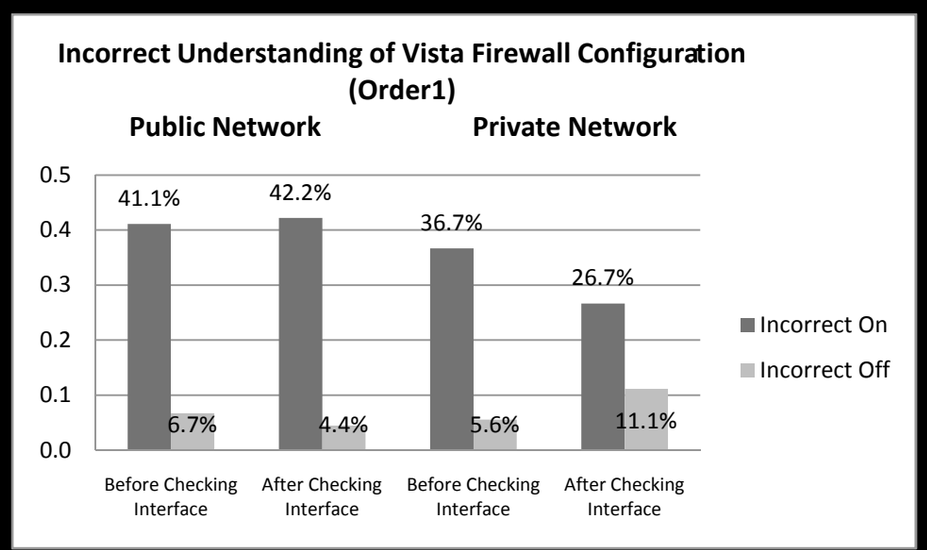


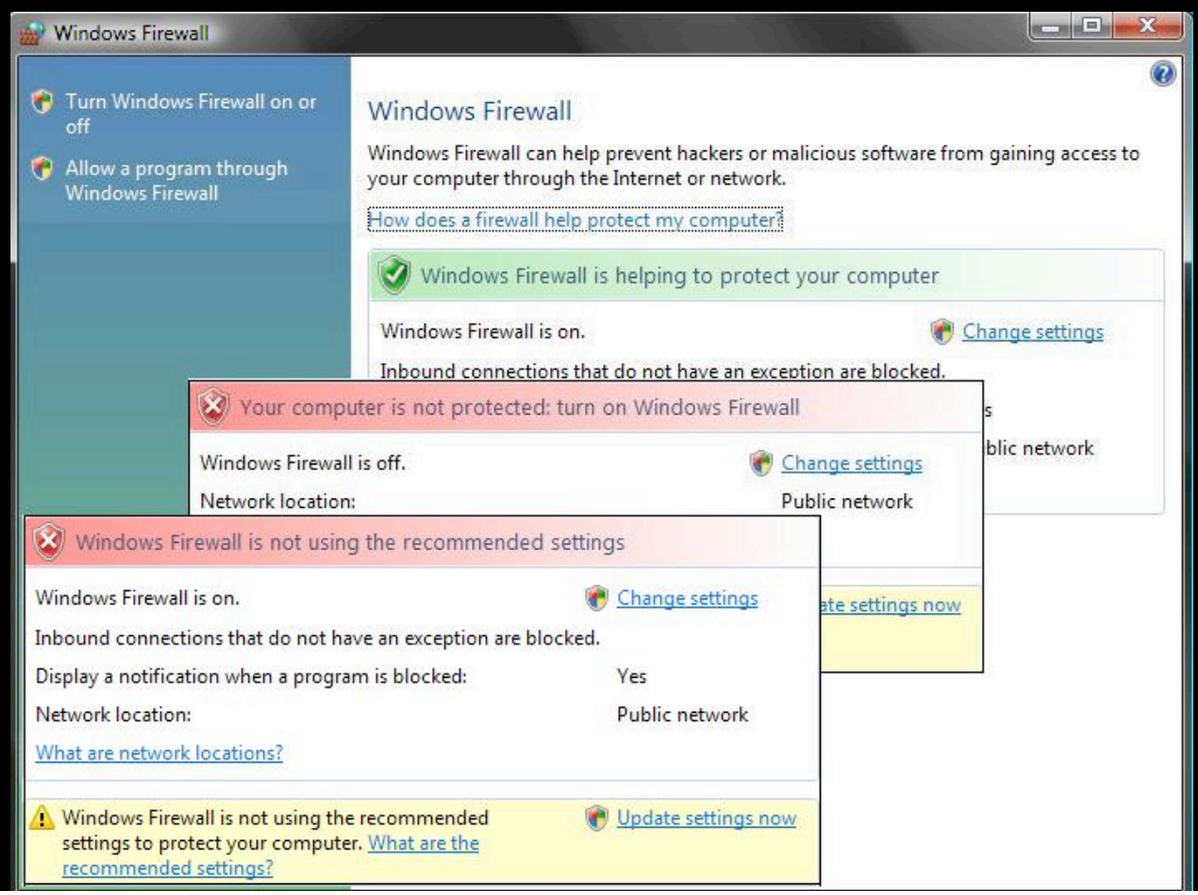


case in point: MS Vista personal firewall

- spectacular failure to make the controls usable and secure [Raja et al., SOUPS '09]

- users could not develop adequate mental models





zooming in on power users and experts

- access control and other security tasks are secondary, performed irregularly, and without necessarily proper training [Botta et al.; SOUPS '07]
- case in point:
  security administrator managing permissions in SAP ERP system for several paper mills
  - started as a temp typist many years ago
  - no CS or other technical education
  - all security training on the job or through product courses

human error

- failures arising from "human error" should be seen as design faults at a system level, rather than blamed on individuals

  (Reason, *Human error: causes and consequences*, 1990)

- research questions
  - what can be done to detect and prevent errors?
  - making access controls more usable or totally "embedded" and invisible?
    - improving languages for textual representation [Inglesant et al.; SOUPS '08] or visualization of controls?

challenges in new applications

- ad-hoc communities and coalitions
  - diffuses the role of security admins
  - access control decisions and policies authoring are moved closer to non-expert users
- Grid computing, etc.
  - splits access control across admin domains
    - hard to evaluate effective permissions on an object
- information sharing among business partners
  - different trust levels require new access control models
  - RBAC & variants hard for non-specialists to understand [Brostoff et al. ,"R-What?: Development of a role-based access control policy-writing tool for e-Scientists"; '05]

new ACMAT should take usability into account

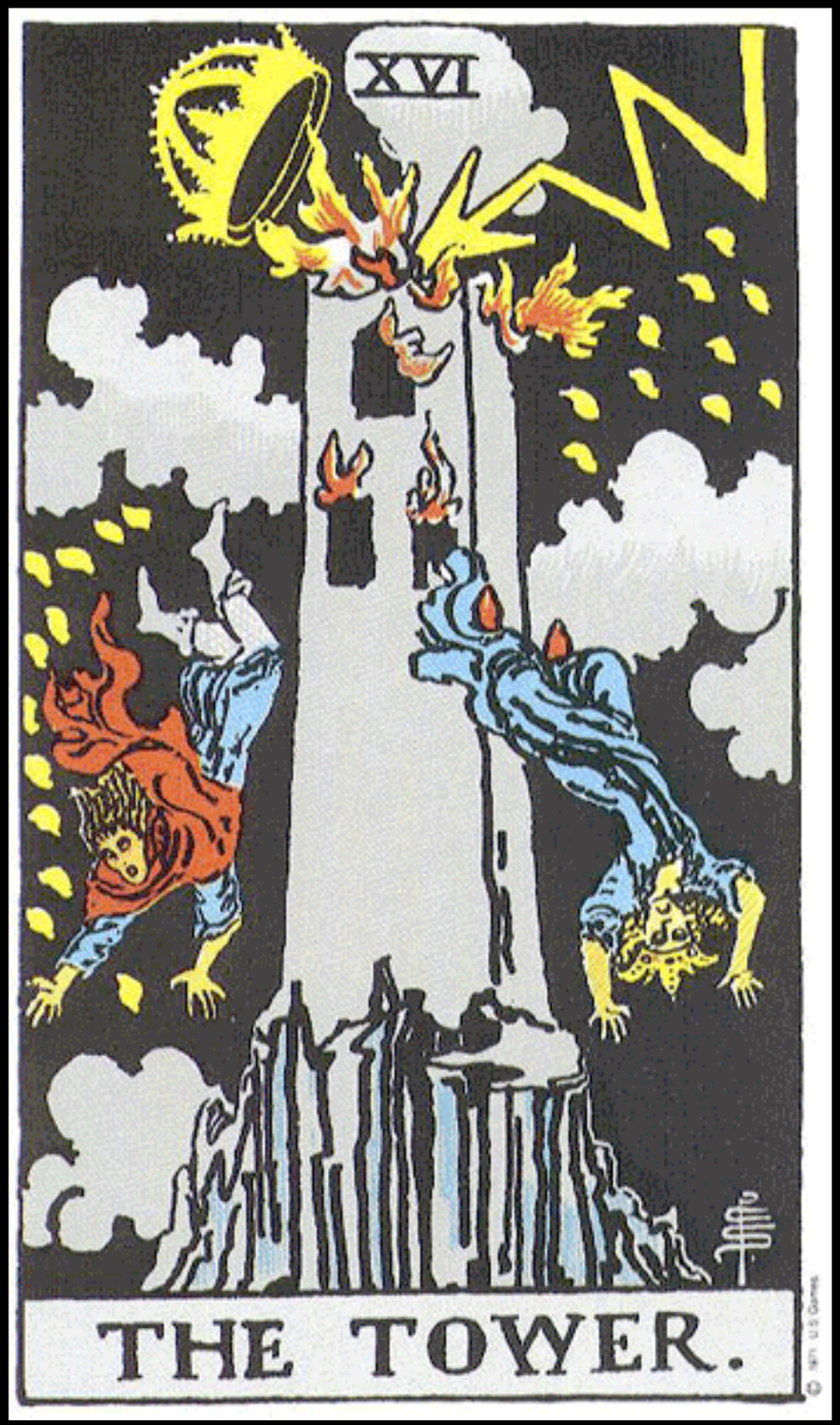
- resolving tension between low-level enforcement and higher-level controls for users?
- evaluating new ACMAT
  - incorporating usability testing in evaluations?
  - user-study methodologies?
    - lab vs. field studies?

panelists

Mary Ellen Zurko (Mez)

- Leads security architecture and strategy for Lotus Workplace, Portal, and Collaboration Software at IBM
- work in user-centered security since early '90s
  - product development, early product prototyping, and research
    - Zurko, Simon, "User-centered Security," New Security Paradigms Workshop, 1996, pp. 27-33.
    - Zurko, Simon, Sanfilippo, "A user-centered, modular authorization service built on an RBAC foundation" IEEE Symposium on Security and Privacy, 1999, pp. 57-71.
  - entire lifecycle of software products, from initial product definition and delivery, to mature product maintenance, with an emphasis on distributed middleware and collaboration.

Tarot Cards



Disruption. Conflict. Change. Sudden violent loss.
Overthrow of an existing way of life.
Major changes.
Disruption of well worn routines.
Ruin and disturbance. Dramatic upheaval. Change of residence or job, sometimes both at once.
Widespread repercussions of actions.
In the end, enlightenment and freedom.

Rob Reeder

- researcher, Trust User Experience group, Microsoft
- Ph.D. in CS, CMU in 2008
  - "Expandable Grids: A user interface visualization technique and a policy semantics to support fast, accurate security and privacy policy authoring"
- broad range of interests in security, privacy, and usability:
  - usable authentication
  - improving website privacy policy presentations
  - making access control easier for people to use

Jorge Lobo

- research staff member, IBM T. J. Watson Research Center
- principal architect at Teltier Technologies (now part of Cisco)
  - policy servers for privacy and availability management of Presence Services
- professor of CS at UIC and member of the Network Computing Research Dep. at Bell Labs
- co-authored books
  - on logic programming, MIT press
  - on policy technologies, IBM Press
- PhD in CS from University of Maryland at College Park

Philip Inglesant

- post-doctoral research fellow, Human Centred Systems Group, CS, University College London
- "Easy Expression of Authorisation Policies" (PERMIS project)
- Ph.D. in CS at UCL
- Masters in New Media, Information and Society at the London School of Economics
- Inglesant, Sasse, Chadwick, Shi, "Expressions of expertness: the virtuous circle of natural language for access control policy specification," best paper at SOUPS '08.