

The background features a complex network of blue lines and arrows. Some lines are solid, while others are dashed. The arrows point in various directions, creating a sense of movement and connectivity. The overall aesthetic is technical and modern.

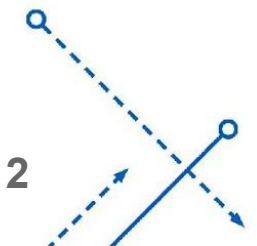
Formal mental models for inclusive privacy and security

Adam M. Houser
Matthew L. Bolton, Ph.D.

Department of Industrial and Systems Engineering

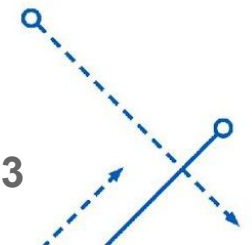
Presentation Outline

- Perspectives on mental models in human factors engineering
- The use of folk models in cybersecurity
- Mental model analysis with formal methods
- Brief conceptual demonstration with a use case and specifications



Mental models in human factors engineering

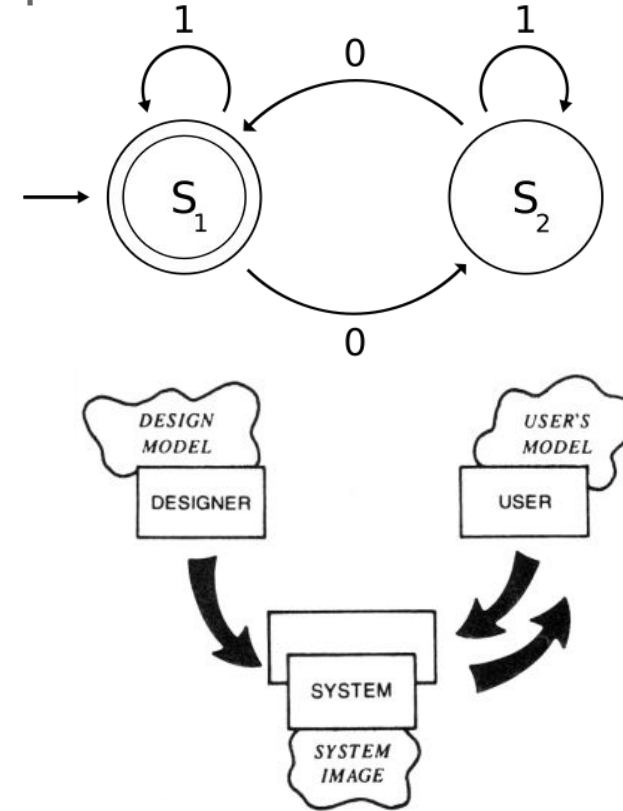
- Internalized representations of system functionality
- Different representational strategies:
 - “Pictures in the mind” (de Kleer & Brown, 1981)
 - Descriptive system abstractions (Rasmussen, 1971; Rouse & Hunt, 1986)
 - “Structured knowledge” (Dutton & Starbuck, 1971)
- Strategies are not mutually exclusive (Sanderson, 1990)



Mental models in human factors engineering

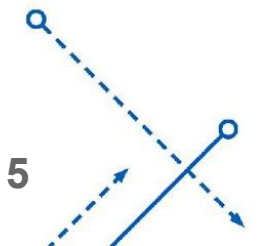
- For this work, Norman (1983) outlines key aspects:

- “Runnability” of mental models
- Agreement between the user’s model and the system image (Norman, 1986)



Folk models in cybersecurity

- Similarities and differences between folk and mental models
 - Description of user expectations about system behavior
 - Folk models rely more heavily on metaphor (Camp, 2009)
 - Mental models more heavily emphasize runnability
- Some work moving towards mental models (Blythe & Camp, 2012)



Folk models in cybersecurity

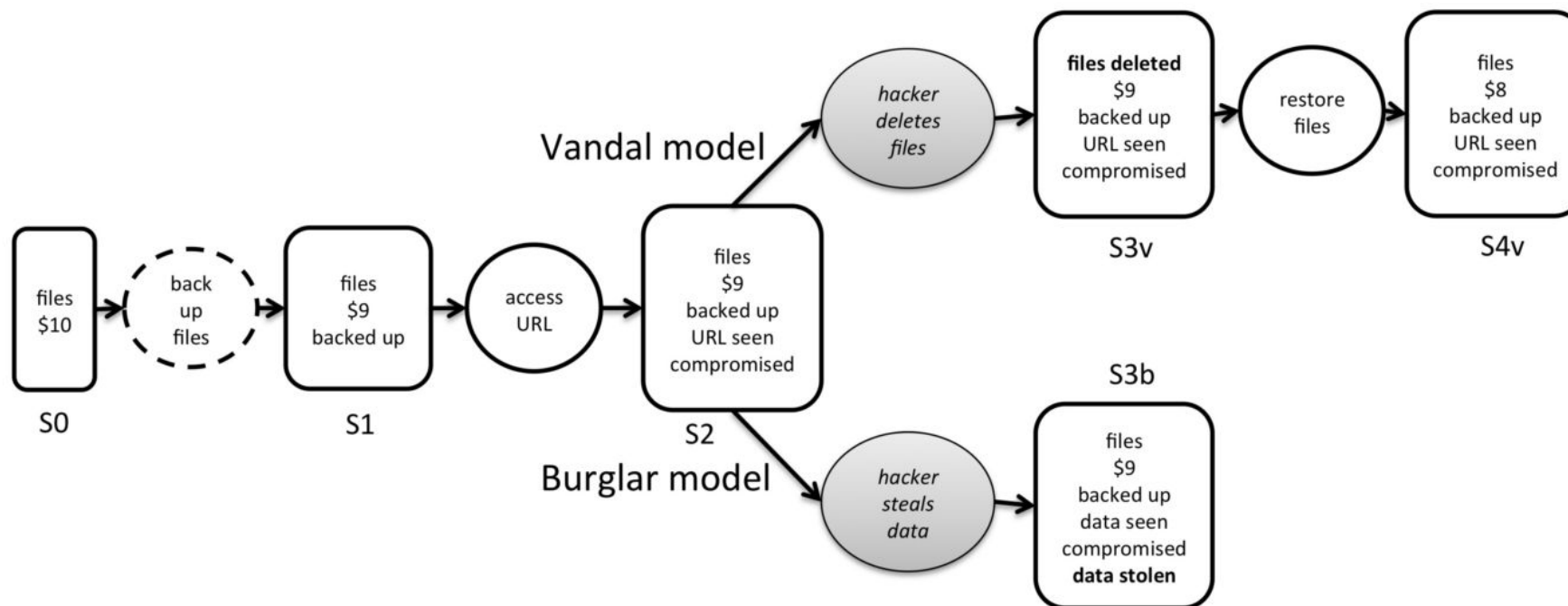
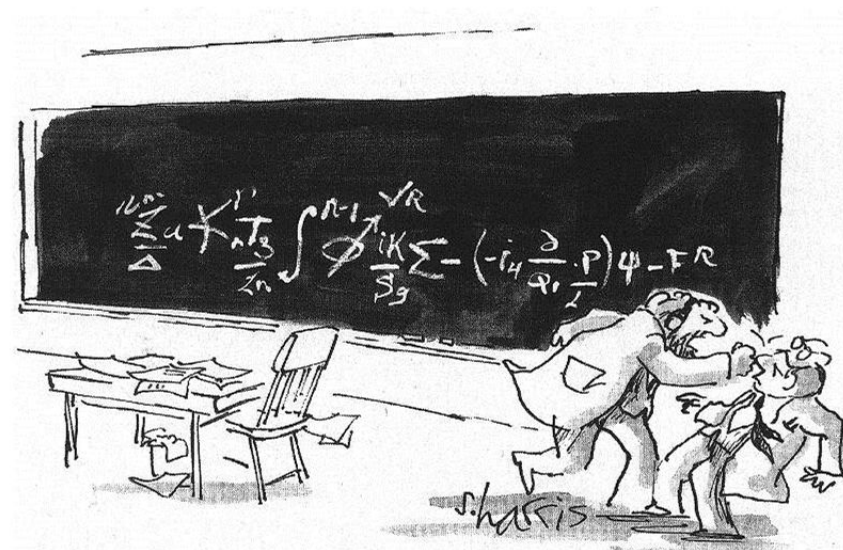


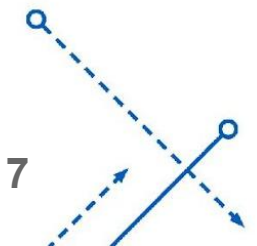
Figure 1. Simulation of a decision to “back up files” run against Wash (2010)’s vandal and burglar hacker models (Blythe & Camp, 2012, p. 89).

Mental model analysis with formal methods

- Well-defined mathematical languages and techniques for modeling, specifying, and verifying systems (Wing, 1990).
- Proofs
- Counterexamples
- Exhaustive search

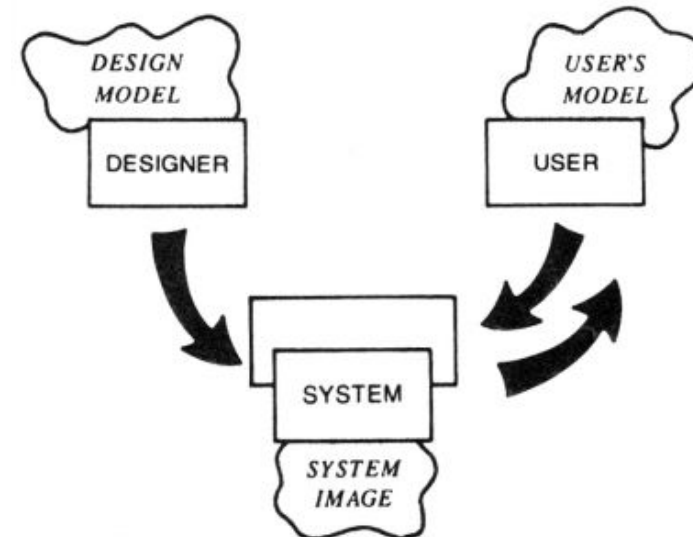


YOU WANT PROOF? I'LL GIVE YOU PROOF!



Examples of analysis with formal methods

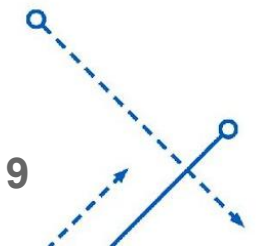
- Particular success with finding user-system mismatches
 - Aircraft autopilot (Degani & Heymann, 2002)
 - Aircraft autoland (Oishi, et al., 2002)
 - Vehicle cruise control (Degani, 2004)
- “Killer feature” is the discovery of unanticipated user-system mismatches through exhaustive statespace search



Our research objective

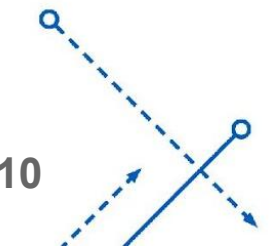
By synergistically integrating work from human factors, cybersecurity, and formal methods, we can discover unanticipated interactions between user mental models and application features or behaviors.

This can help ensure that privacy and security solutions are appropriate, useful, and effective for a plurality of users.



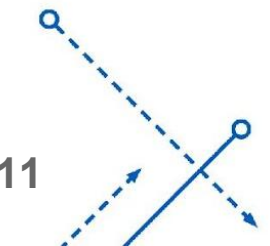
Conceptual demonstration: encrypted chat

- Consider two user groups: domestic violence victims and protesters
- Threat models, environments for use, capability needs
 - Developer sensitivity to these issues?
- Extract and create formal representation user mental models
- Create suite of specifications capturing significant app features
- Verify that app features are compatible with user mental models



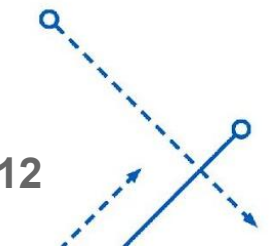
Example specifications

- User expects app data to always be available
- Screenshots should always be allowed
- User expects to be always notified about communication network changes
- User should never be allowed to 'upload' or 'share' a private key



Future work

- We plan to exercise this synergistic approach for the dissertation
- Elicit mental models for ‘attacker’ and ‘defender,’ perhaps with a simple program or program feature set
- Discover unanticipated interactions that defenders *think* are safe, but attackers can use to their advantage
- Potentially evaluate software countermeasures from user perspective



Questions?

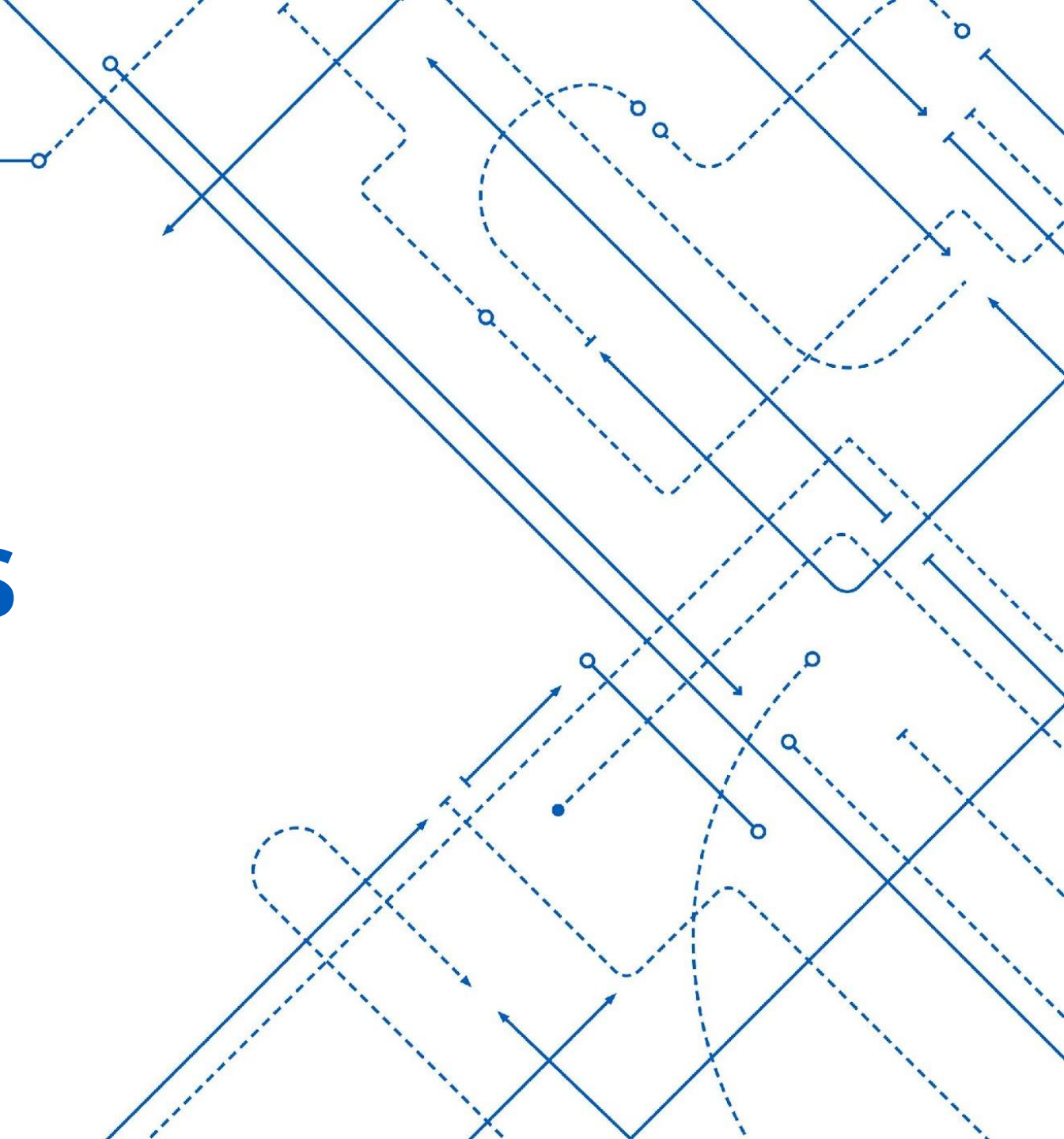
Adam M. Houser

appliedcaffeine.org
adamhous@buffalo.edu
@neutrinos4all

Matthew L. Bolton, Ph.D.

fhsl.eng.buffalo.edu
mbolton@buffalo.edu
@UB_FHSL

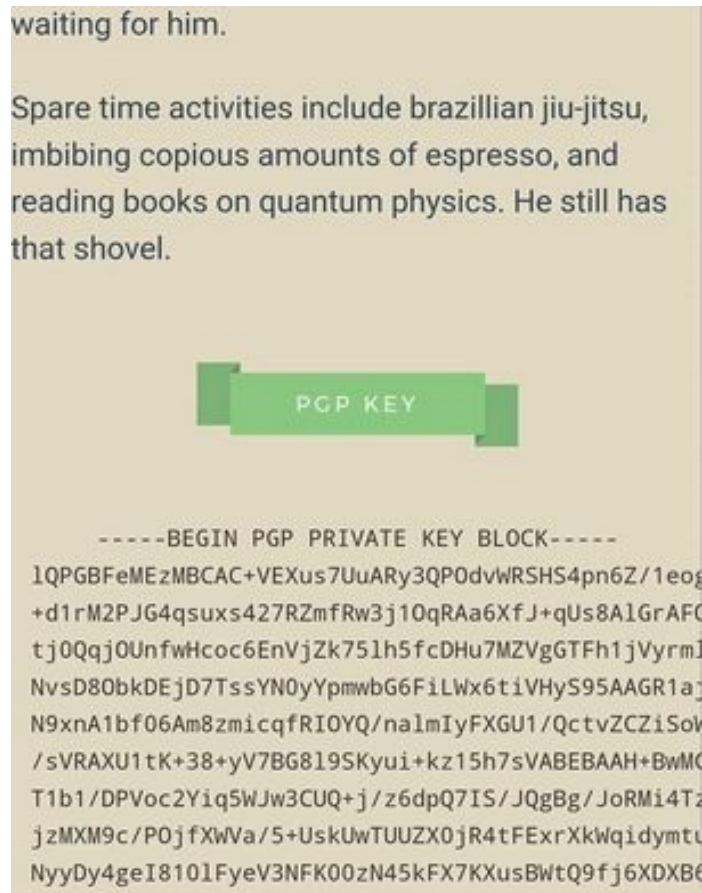
Reserve Slides



Mental model elicitation

- There exist a number of methods for model extraction
 - Card-sorting tasks (Asgharpour, et al., 2007)
 - Structured and semi-structured interviews (Wash, 2010)
 - Task observations (Dutton & Starbuck, 1971)
 - Cognitive walkthroughs (Ford & Sterman, 1997)
 - Training artifact analysis (Rushby, 2001)

End-user key management is still hard



<https://twitter.com/thesl3ep/status/876066176589336576>