A Cross-Disciplinary Study of User Circumvention of Security

Jim Blythe, PhD
USC ISI
Research Scientist, CS

Ross Koppel, PhD
University of Pennsylvania
Sociology & Senior Fellow LDI

Sean Smith, PhD
Dartmouth College
Professor, CS

Vijay Kothari
Information Sciences Institute
PhD Student, CS

David Harmon
Dartmouth College
Undergraduate, CS

Christopher Novak
Dartmouth College
Undergraduate, CS

Talk Outline

The Problem

How We Approach It

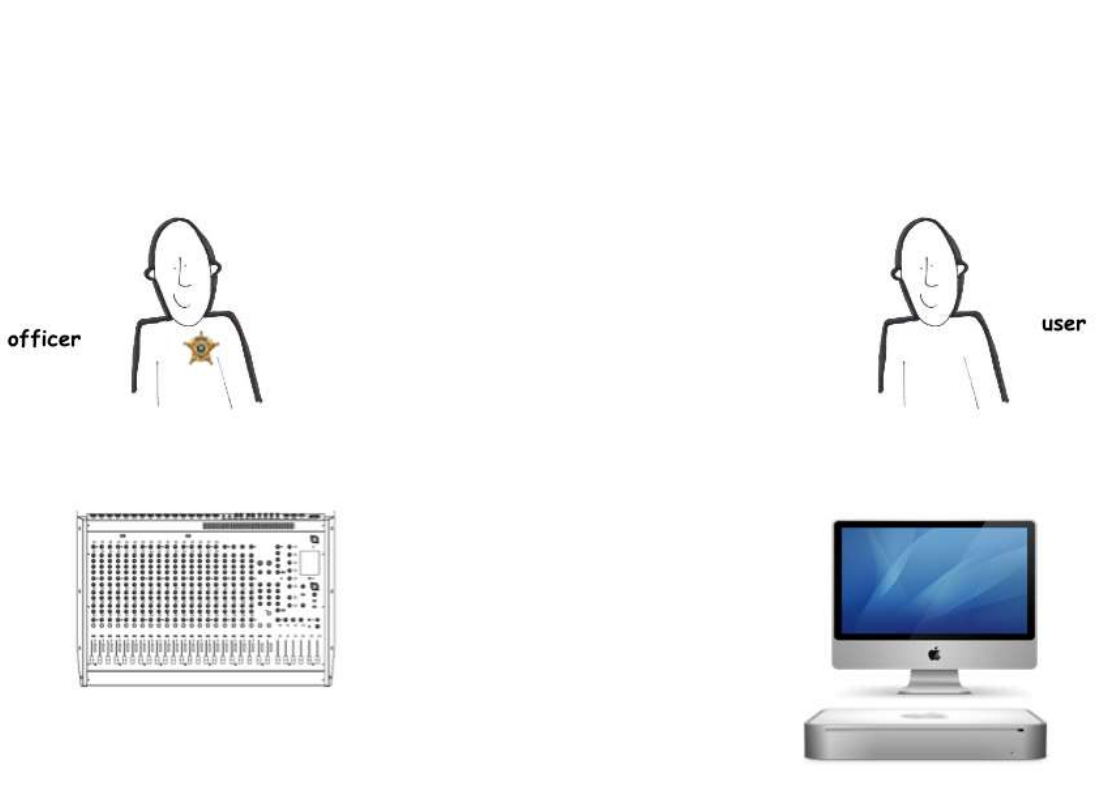
Thrust 1: Fieldwork and Observation

Thrust 2: Analysis

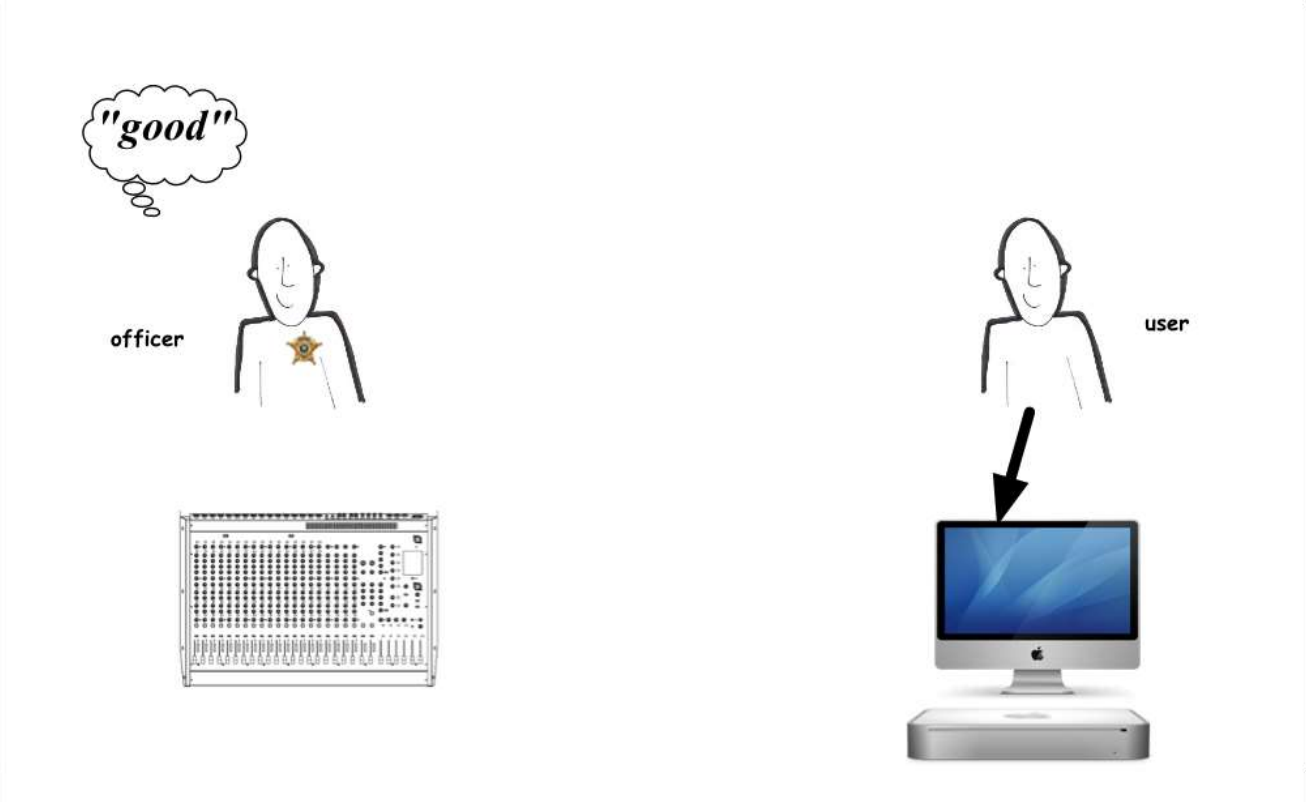
Thrust 3: Towards a Solution

Next Steps

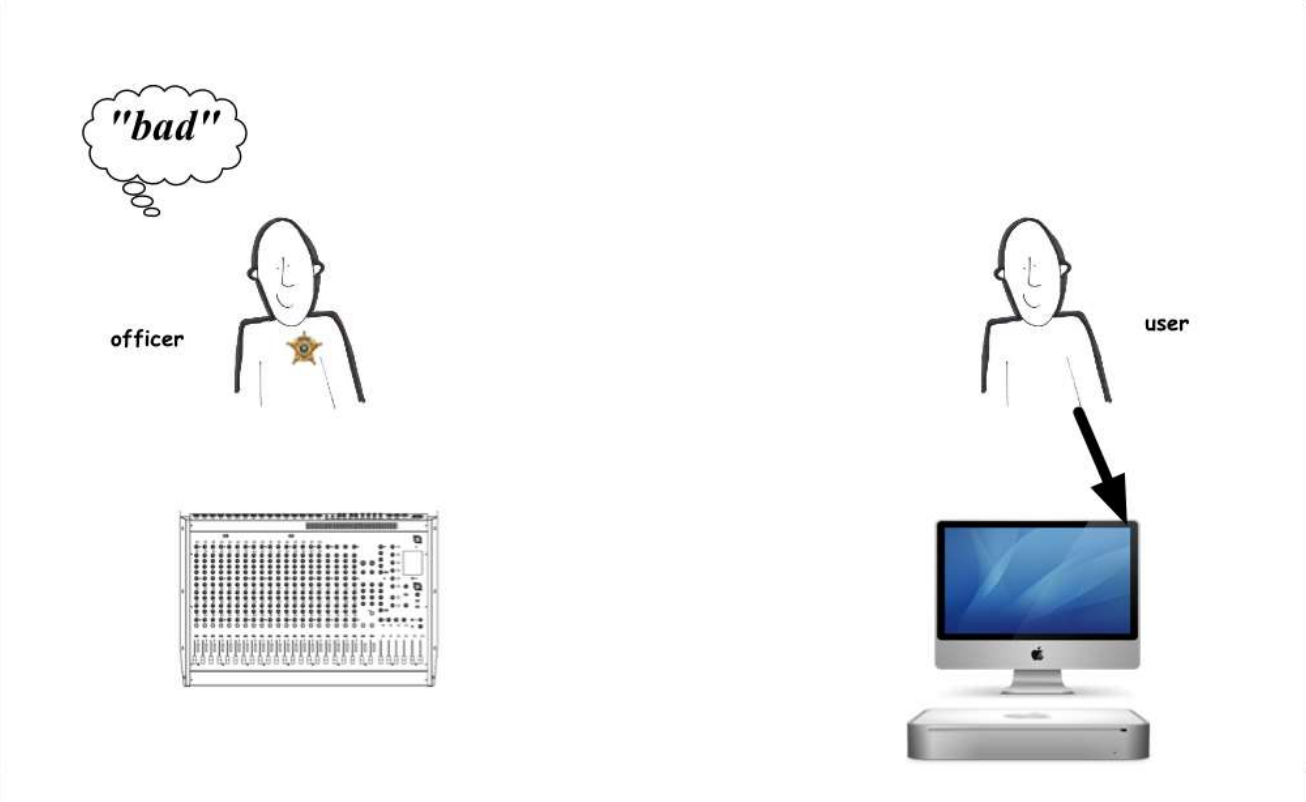
The Problem



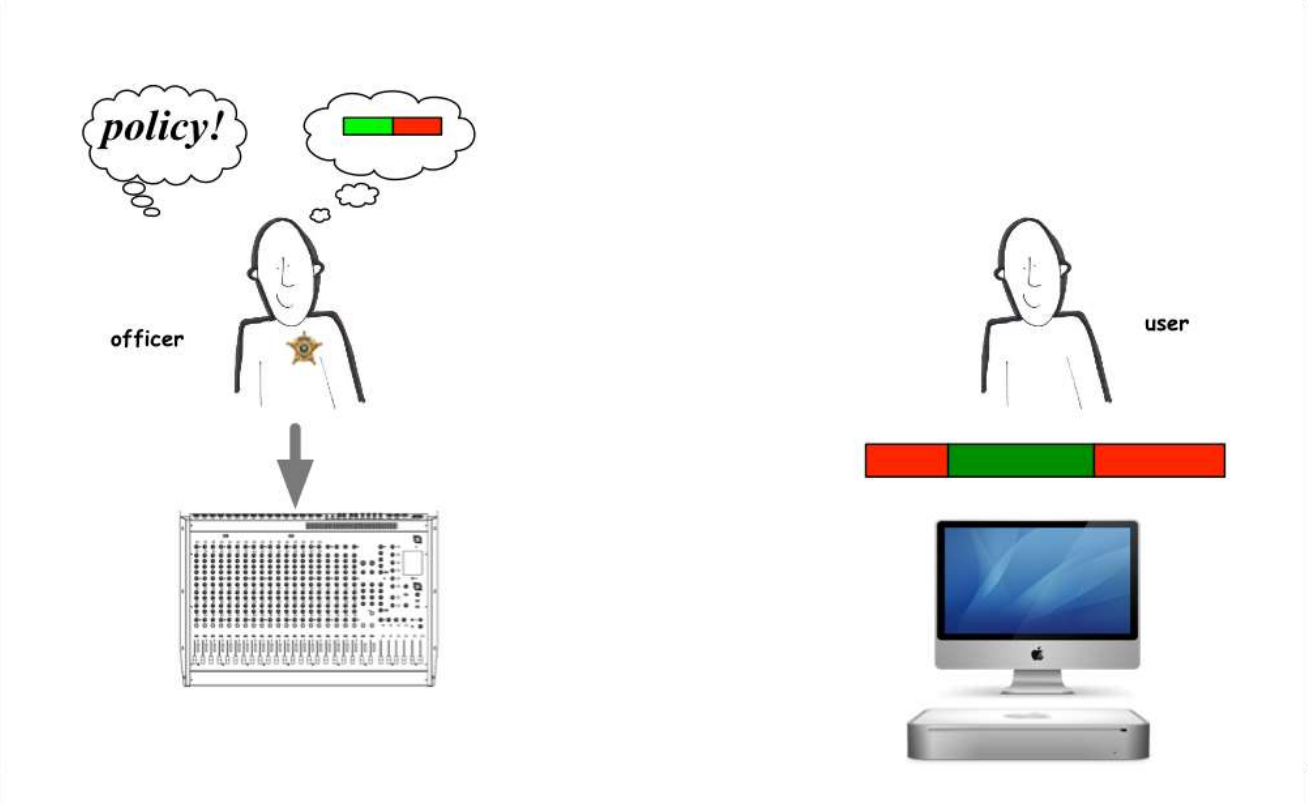
The Problem



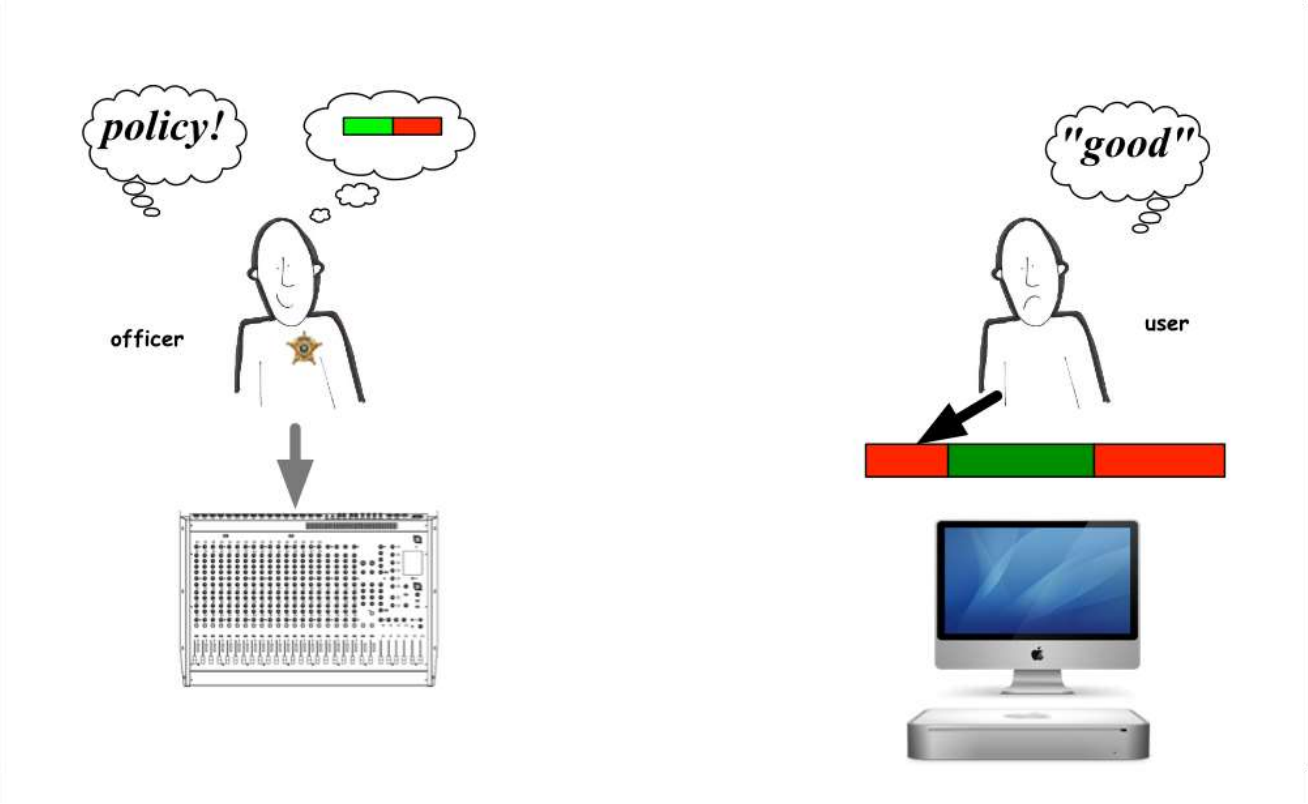
The Problem



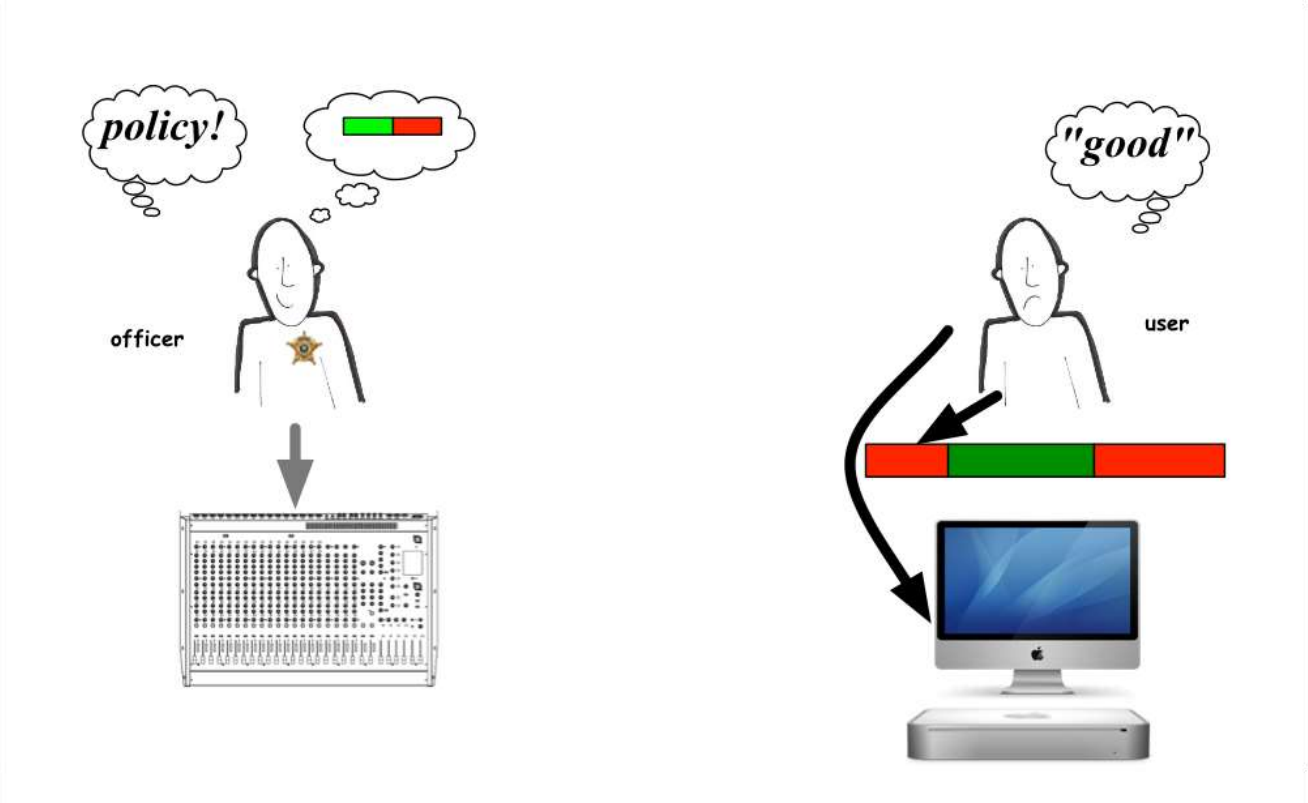
The Problem



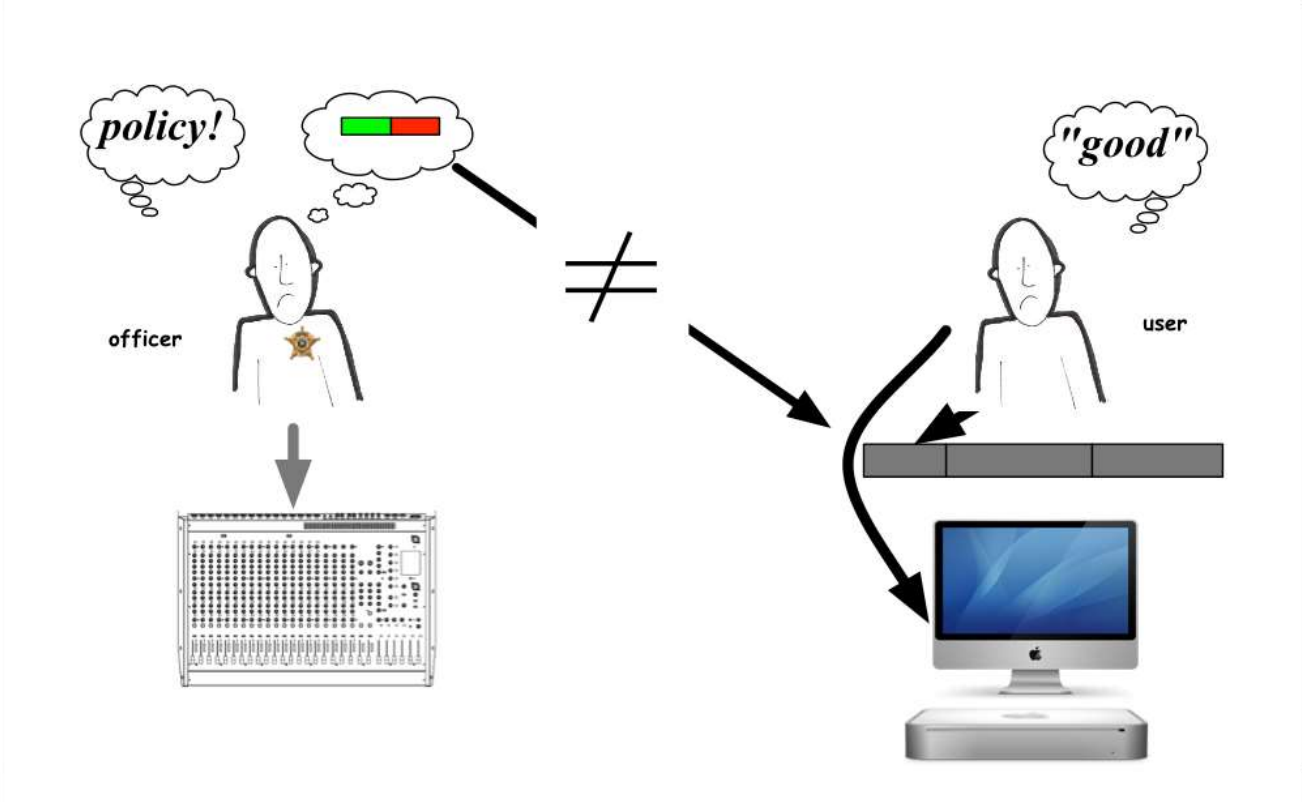
The Problem



The Problem



The Problem



The Problem

Good people circumvent security controls to get their jobs done...and to accomplish the mission of their organizations)

“Eppur si muove”….we can’t pretend it doesn’t happen.

How We Approach It

Faculty leads:

- Ethnography and sociology
- Computer security
- Agent-based modeling

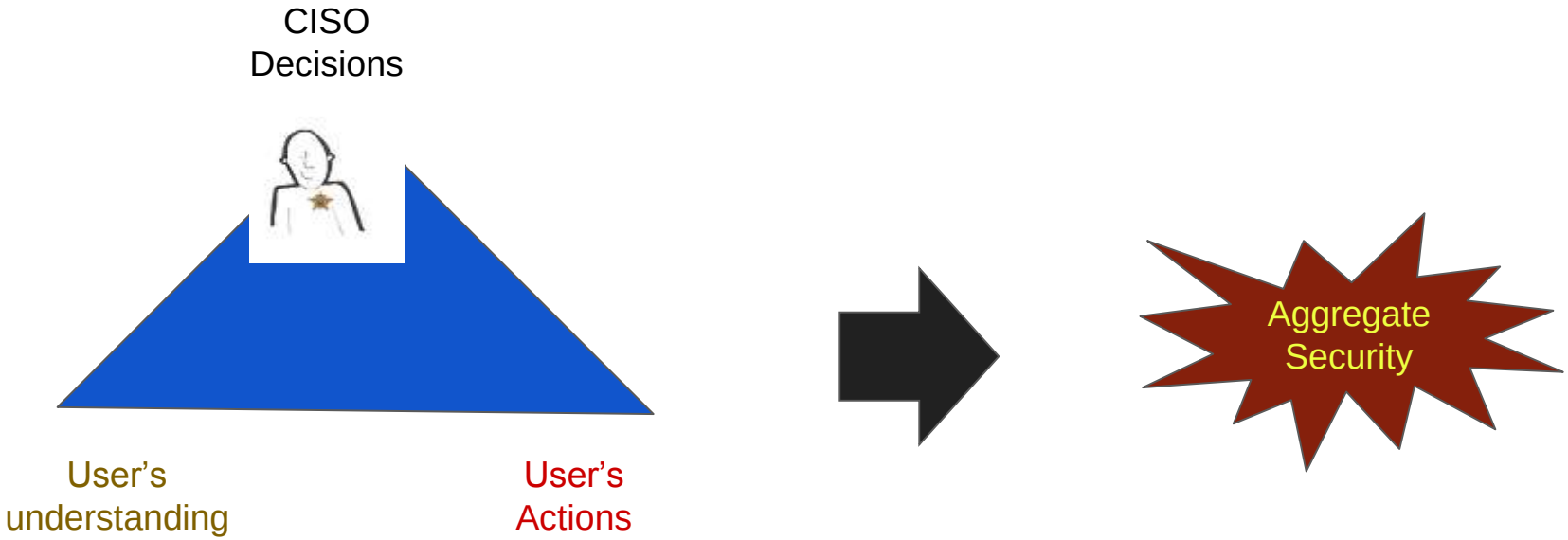
Hardworking PhD student

And undergraduate interns

Thrust 1: Sociology, Ethnography, Surveys, Log Analyses

- Observations & shadowing of users in hospitals, offices, banks, Wall St firms, academia, industry.
- Interviews with CSOs and Cybersec luminaries (including leaders at Google, banks, etc)
- Analysis of requests for access, fixes and modifications from IT offices (request logs > 20,000 items)
- Review of password lists
- Analysis of password notebooks/logbooks (thousands sold on Amazon)
- Surveys on cybersec circumvention: general users and cybersec administrators
- Help desk and security logs
- Literature reviews…and our own publications and presentations N >40
- IRB approval for surveys, observations, interviews...and now Mech Turk
- Work with Intel and NSF on IoT cybersecurity
- 20 years of work with medical institutions, medical device makers, medical informatics association.

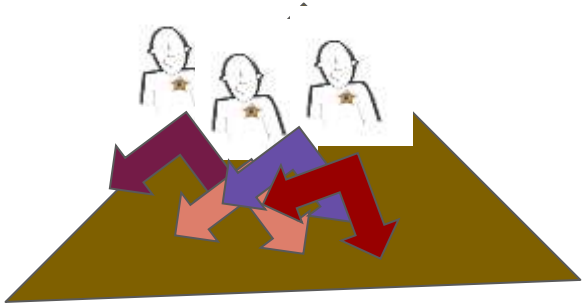
Thrust 1: Fieldwork & Observation (Simplified Version)



Thrust 1: Fieldwork & Observation (Adding Complexity)

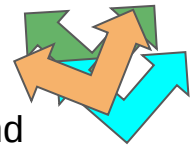
closer to reality:

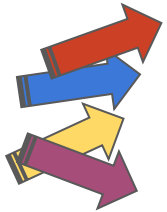
CISOs Decisions (MANY and MANY)



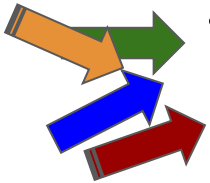
User's under-standing

Many and conflicting rules and advice





Users' Actions



Aggregate security across many devices and many networks????

Thrust 1: Fieldwork & Observation

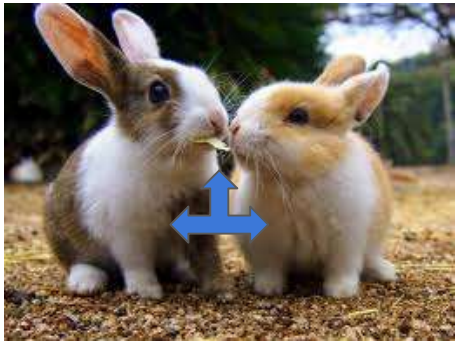
Unuseful Guides to the Perplexed

User now their own CISO(s)

IoT

How Common is Circumvention of Password Rules?

From the Pew Survey (2016): Americans Don't Follow Guidelines:



Sharing passwords

Passwords: Fluffy Fluffy1 Fluffy2 Fluffie Fluffie$ FluFfy FluFFies

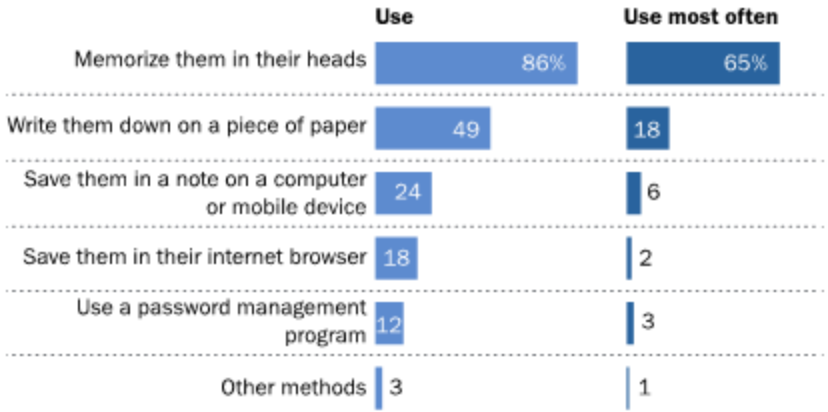
How Common is Circumvention of Authentication Rules?

Pew Survey 2016: Few practice cyber security rules. Not even close.

How Common is Circumvention of Authentication Rules?

Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Note: Results for "use most often" category include those who use only one technique to manage their passwords.
Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

How Many Worry About Their Online Passwords

Pew Survey: **Fully 69% of online adults say they do not worry about how secure their online passwords are**
(Several months ago…. Pre DNC and last week's wikileaks-CIA hack)

From the Interviews and Observations

From the Interviews and Observations

From the Interviews and Observations

From the Interviews and Observations

From the Interviews and Observations

Our Pilot Surveys

Two Parallel Surveys: CSOs and Regular Users:

Who sets policies? (Anyone know the policies?)

Do they make sense…and to whom?

How often circumvented? (What's the justifications for that?)

How Frustrated Are You by Access Policies?

	1 (Not Frustrated)	2	3	4	5 (Very Frustrated)
General users	23%	39%	15%	23%	0
Cybersecurity professionals	33%	27%	33%	7%	0

Most are frustrated…

What They Say:

Cybersecurity Pros

“Waiting so long when turning on/off the computer as it decrypts/encrypts information.”

General Users

“The work is delayed.”
“Frustration. [Coworkers] not able to do their job. Give up or don't care anymore.”

Are Access Rules Sensible: Pros vs. Users

	Generally Sensible		Sometimes Sensible		Not Sensible		Don't Know	
	Gen	Pros	Gen	Pros	Gen	Pros	Gen	Pros
Log on rules	46%	87%	46%	0%	8%	13%	0%	0%
Password rules for different passwords for each app	30	7	20	53	50	27	0	13
Password complexity	23	40	38	20	38	40	0	0
Password change frequency	25	13	58	40	17	33	0	13
Management's rules on granting access	8	31	69	23	15	8	8	38
Inactivity timeouts	31	53	54	33	15	13	0	0
Different rules for different systems	17	21	42	43	33	14	8	21
Rules by how/why access is provided	38	53	46	20	15	13	0	13

Pros a bit more accepting of rules, but most doubt rules' thoughtfulness.

What They Say:

“Everyone writes down passwords”

Everyone “using alternate spellings to work around the dictionary rule;” eg, ‘boyz’ for ‘boys.’

When is Circumvention Justified?

	General Users	Cybersecurity Professionals
Critical task, e.g., saving a life, keeping the grid up	83%	79%
When the rules are so foolish that nothing else makes sense	42%	57%
Access associated with role(s) make no sense, e.g., members of the same team can't see all of the information because only some have official access	17%	36%
When allocation of access is foolish, e.g., people hired before November have access but others with similar functions and responsibilities don't	28%	9%
When everyone else is circumventing a specific rule	58%	43%
When people were officially taught to use a workaround	58%	71%

Answer: When I want to (and we all do it).
Pros often more accepting of "cheating"

Security Pros vs. General Users:

General users: cybersec pros not concerned about our work needs

Both general users and cybersec pros tend to see externally imposed rules as unreasonable

Many general users often see cybersec rules as excuse for laziness (as in why we didn't fix something)

Cybersec pros feel often unloved. And they're right!

Synopsis: Ethnography and Sociology

Cybersecurity as conceptualized vs.

As designed vs

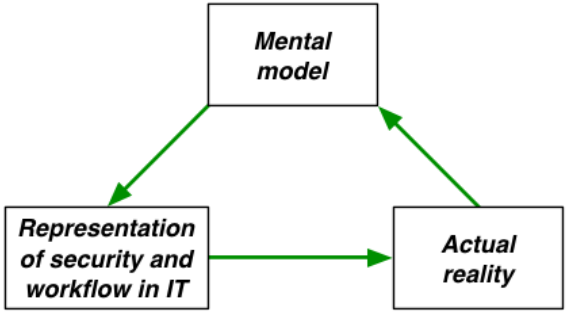
As conveyed: with conflicts, contradictions, incomprension; across many systems

As understood...and

As acted upon: by individuals, enterprises...

And in relation to the many (interacting) networks and to the IoT

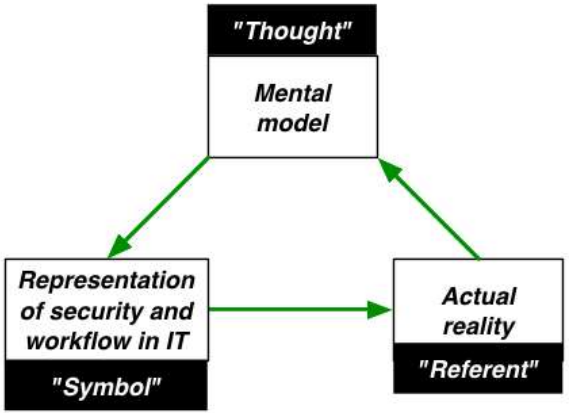
Thrust 2: Analysis



Smith and Koppel 2014

- An organizing model for circumvention: semiotic triads

Thrust 2: Analysis

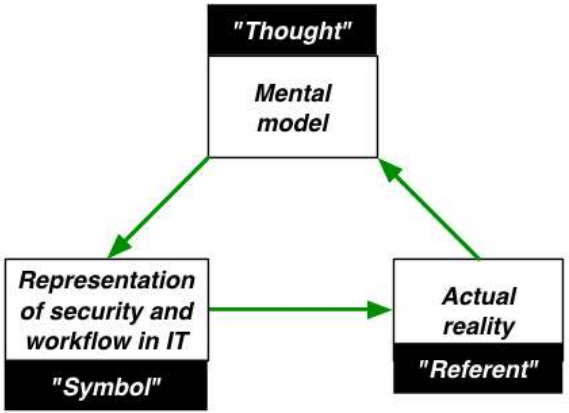


Smith and Koppel 2014

Ogden and Richards, 1927

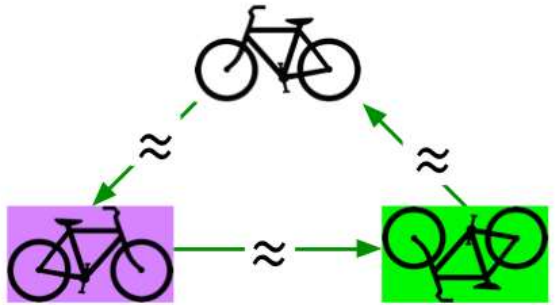
- An organizing model for circumvention: semiotic triads

Thrust 2: Analysis



Smith and Koppel 2014

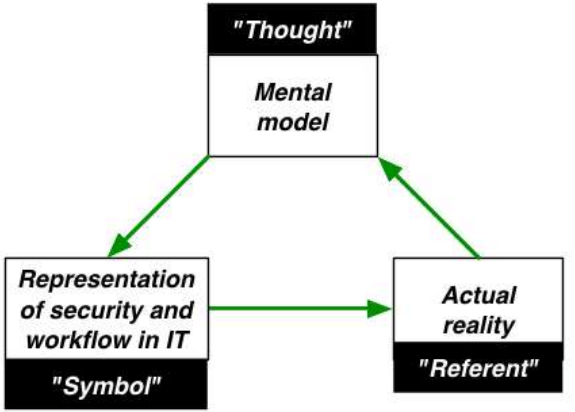
Ogden and Richards, 1927



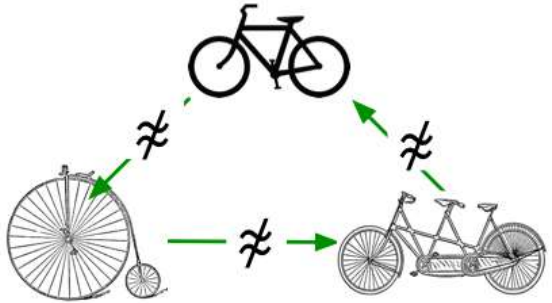
- Regular semiotics: ***morphisms.***
- Mappings ***preserve*** structure

- In language: morphisms

Thrust 2: Analysis



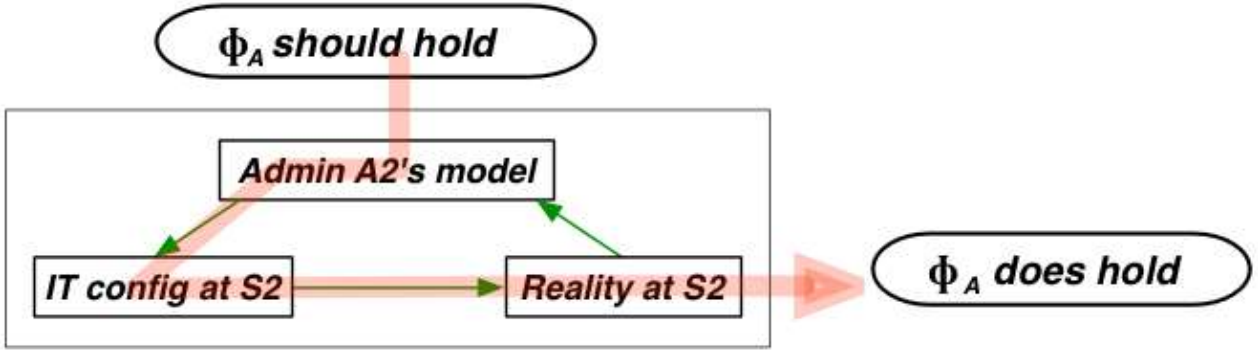
This project!



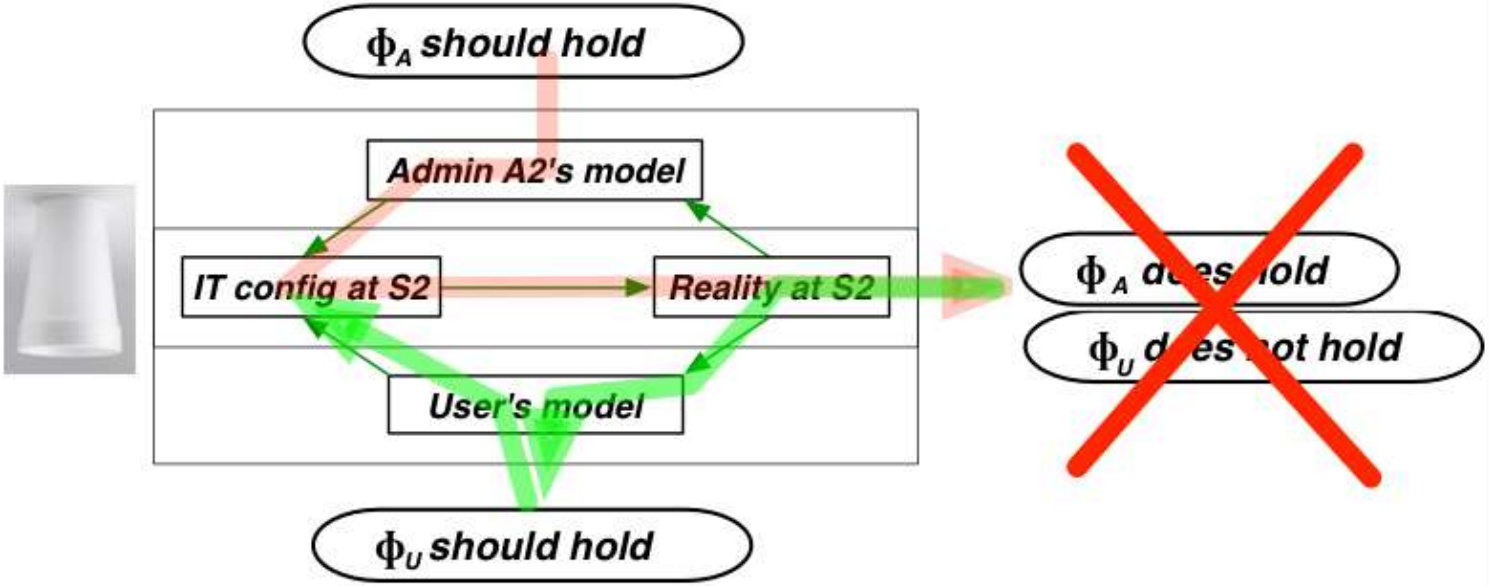
- Circumvention semiotics: ***mismorphisms.***
- Mappings ***fail to preserve*** structure

- In security usability: *mis*morphism

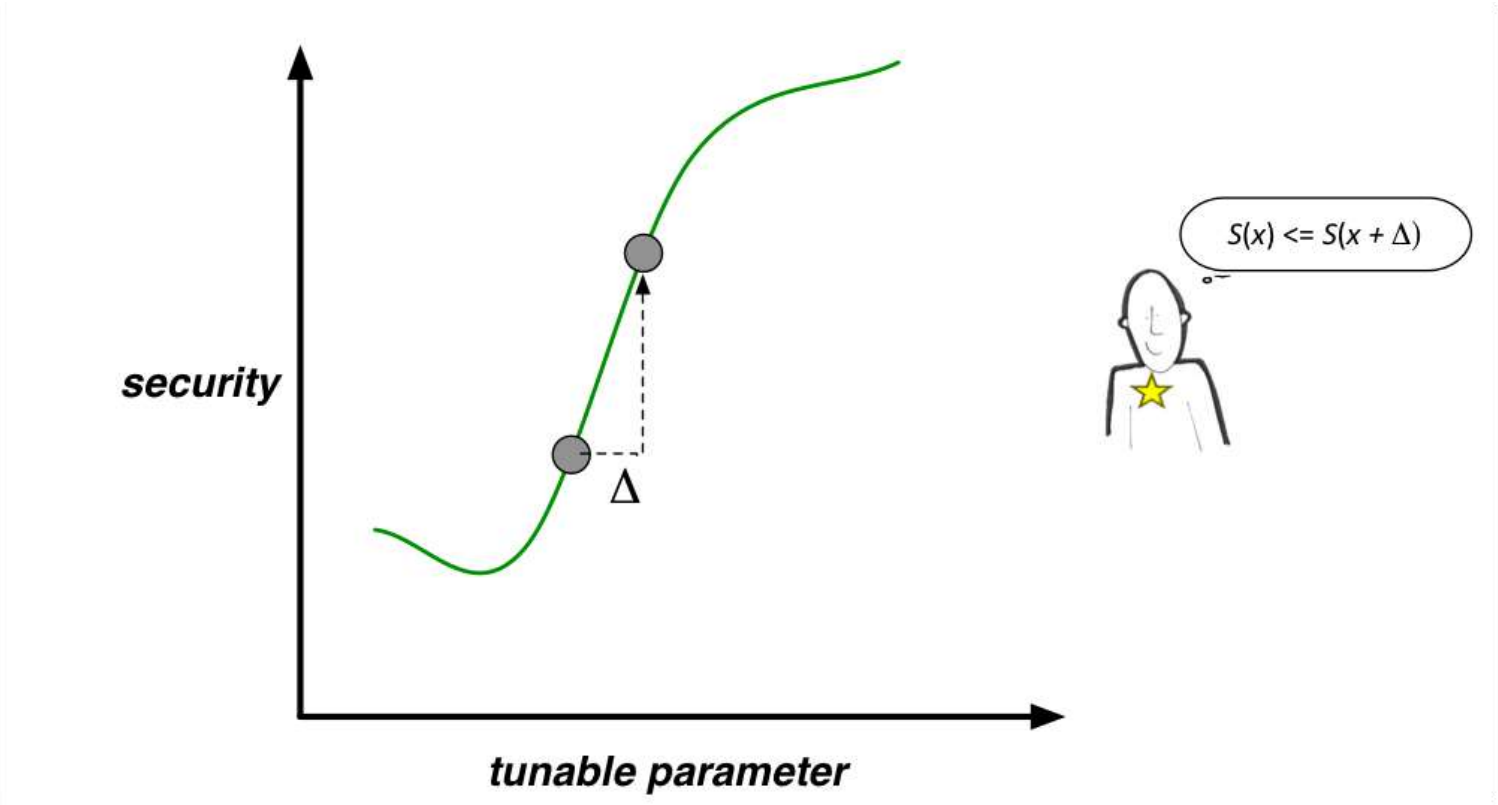
Causing Circumvention



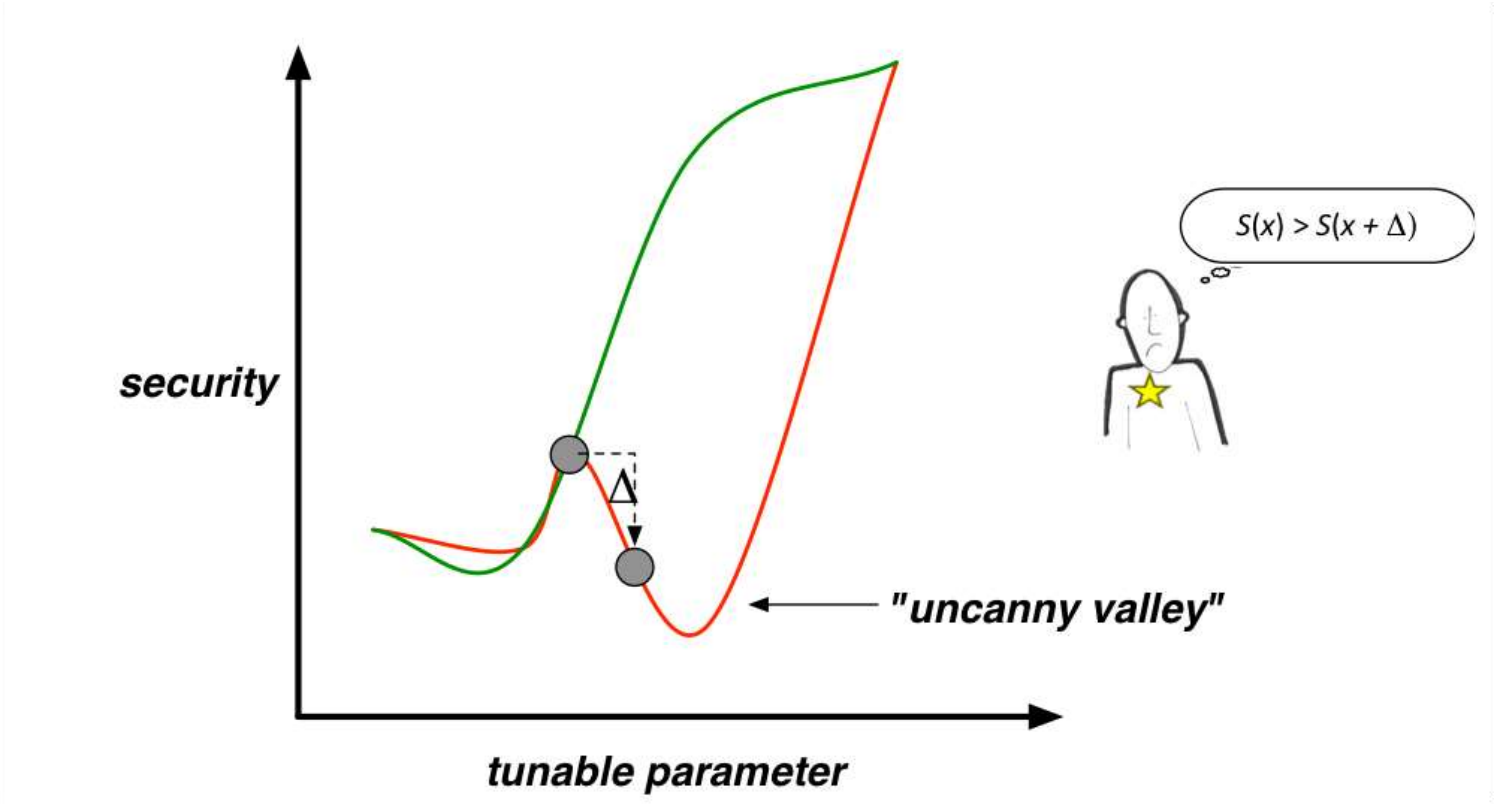
Causing Circumvention



Trouble: Loss of Monotonicity



Trouble: Loss of Monotonicity

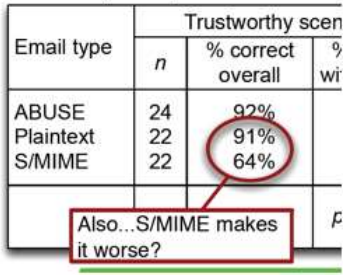


Trouble: Loss of Monotonicity

Uncanny ***descent***
- timeouts
- password practices
- computerizing medical workflow

Uncanny ***ascent***
- "qwertyqwerty"
- executive passwords

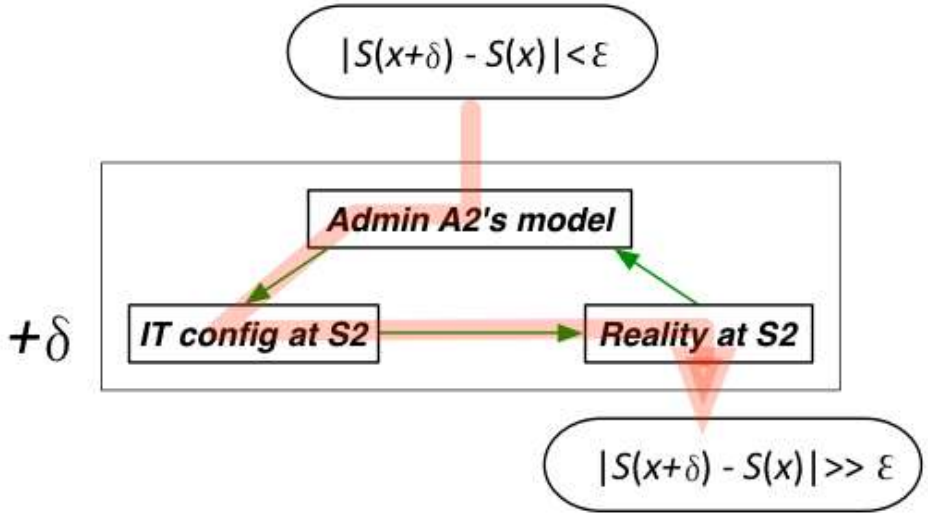
Uncanny ***nop***
- public/internal wifi
- check diff password via hash
- deleting links, not files
- education not help



Email type	Trustworthy scen	
	n	% correct overall
ABUSE	24	92%
Plaintext	22	91%
S/MIME	22	64%

Also...S/MIME makes it worse?

Trouble: Loss of Continuity

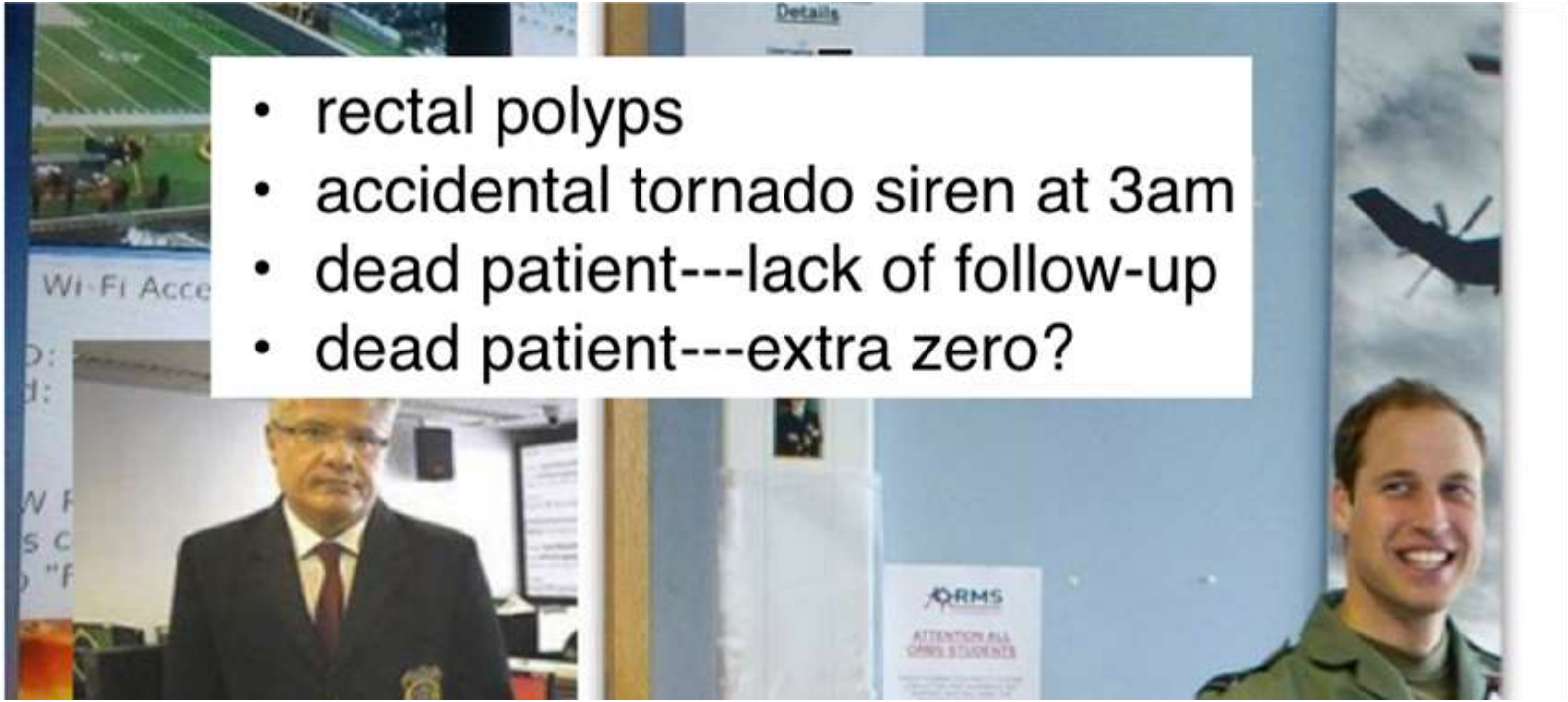


Trouble: Loss of Continuity

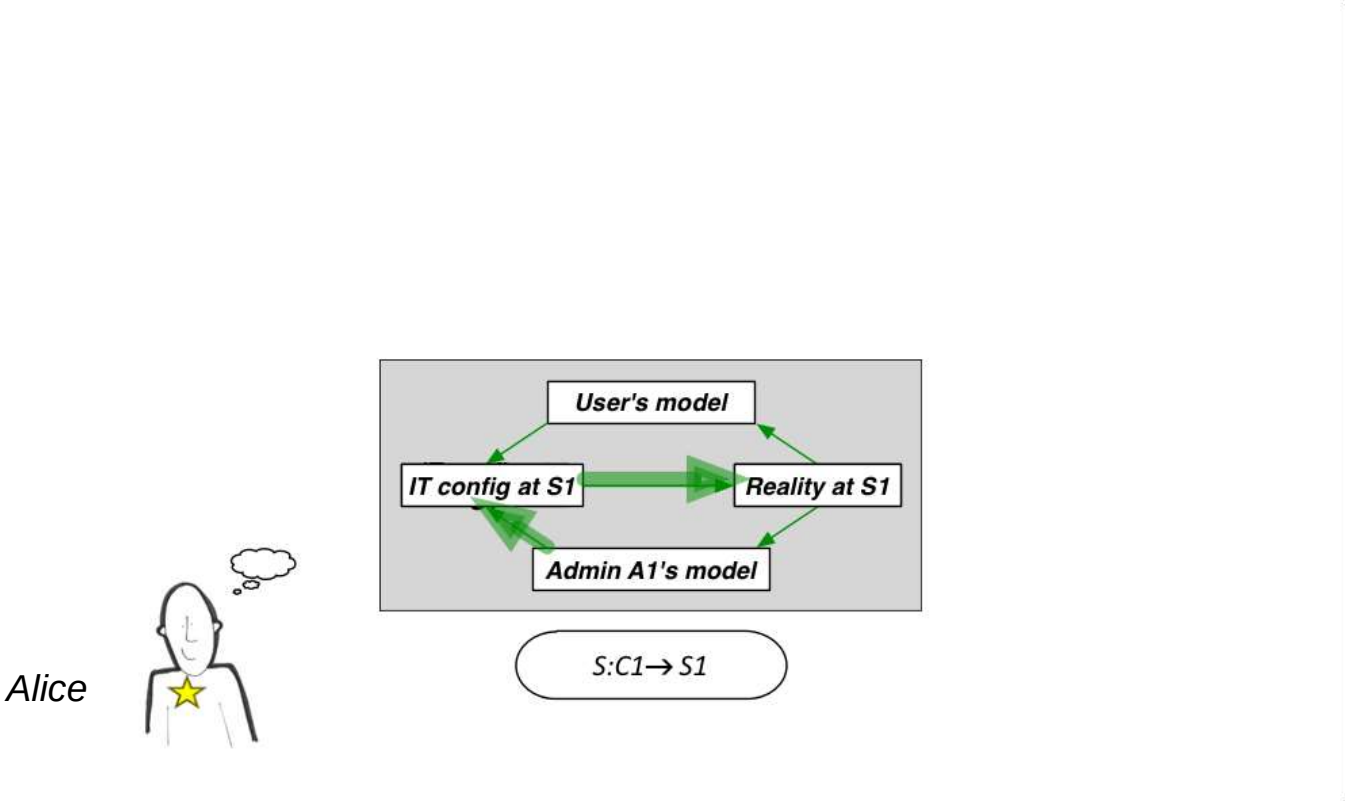
Trouble: Loss of Continuity

Trouble: Loss of Continuity

Trouble: Loss of Continuity

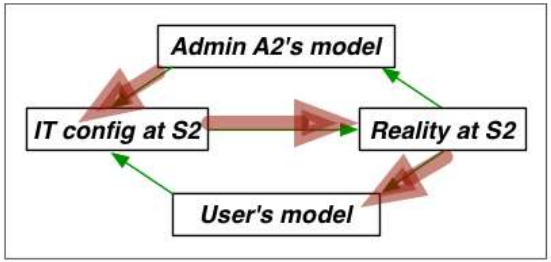


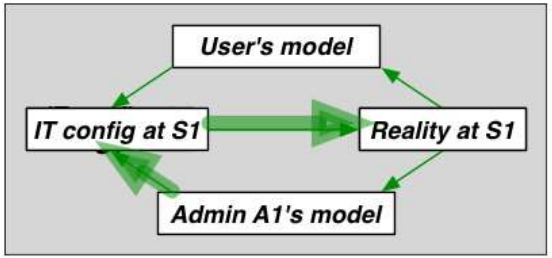
Trouble: Action at a Distance



Trouble: Action at a Distance

Bob

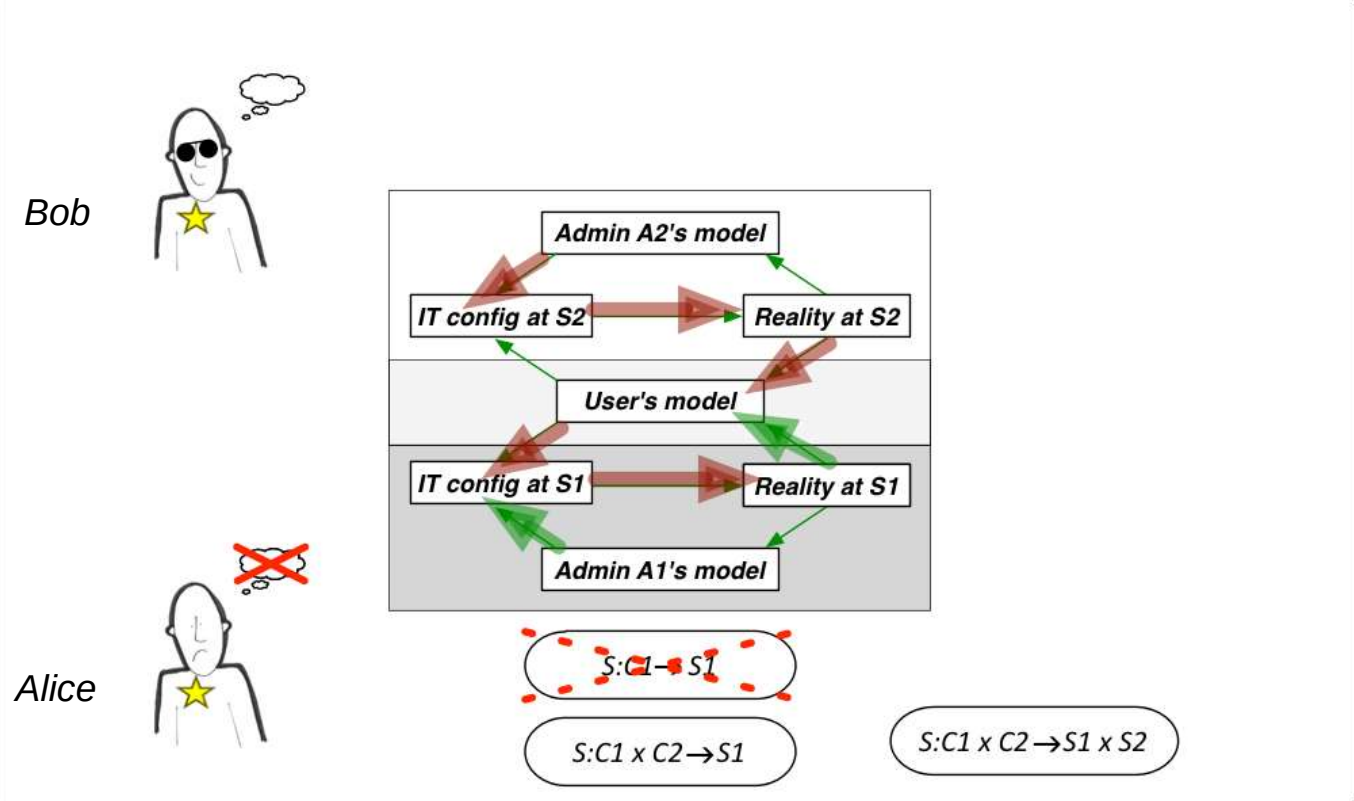




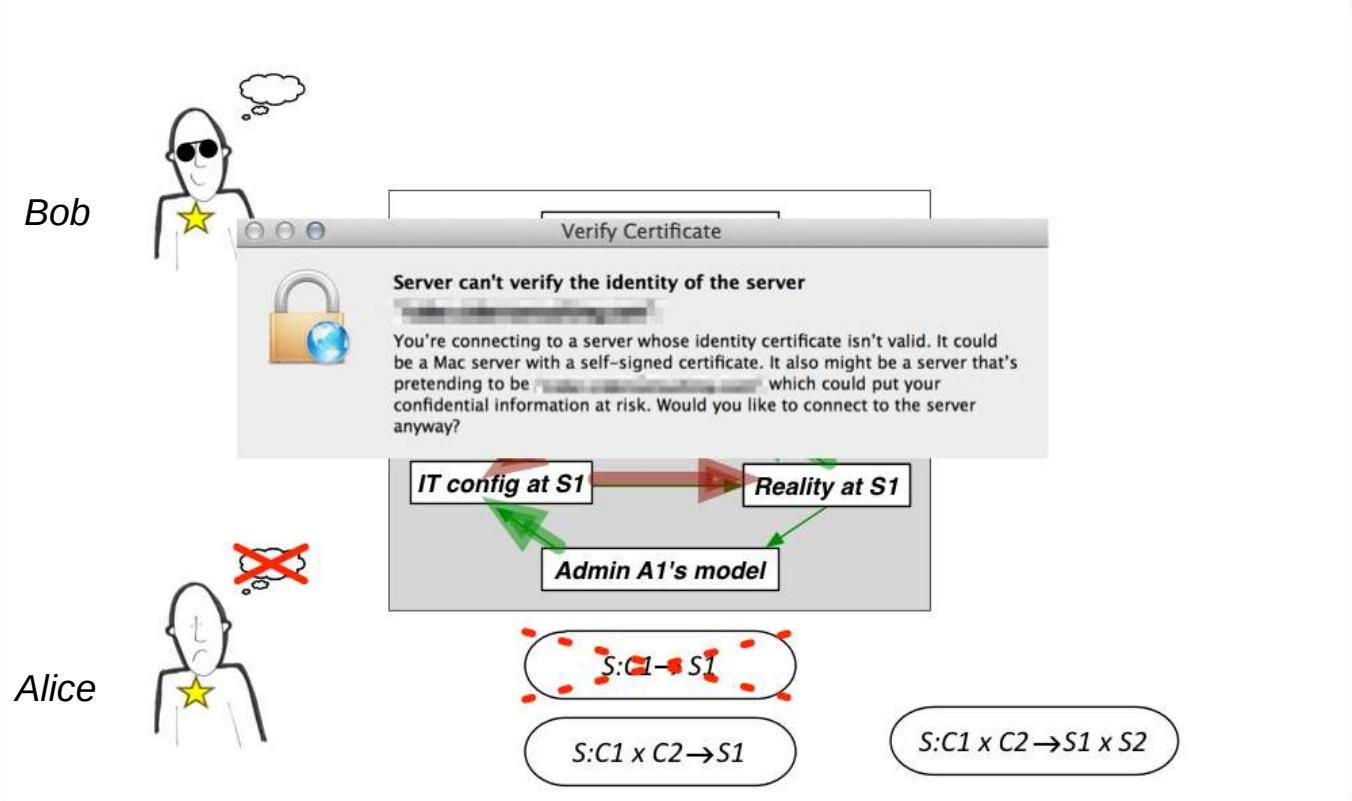
Alice

S:C1→ S1

Trouble: Action at a Distance



Trouble: Action at a Distance



Synopsis: Thrust 2

Mismatches between reality and mental models lead to circumvention

Circumvention leads to ***significant*** mismatches between the admin's mental models and resulting reality

- What do we do?
- How can we move from ***fantasy-based cybersecurity*** to ***evidence-based cybersecurity***?

Thrust 3: Towards a Solution

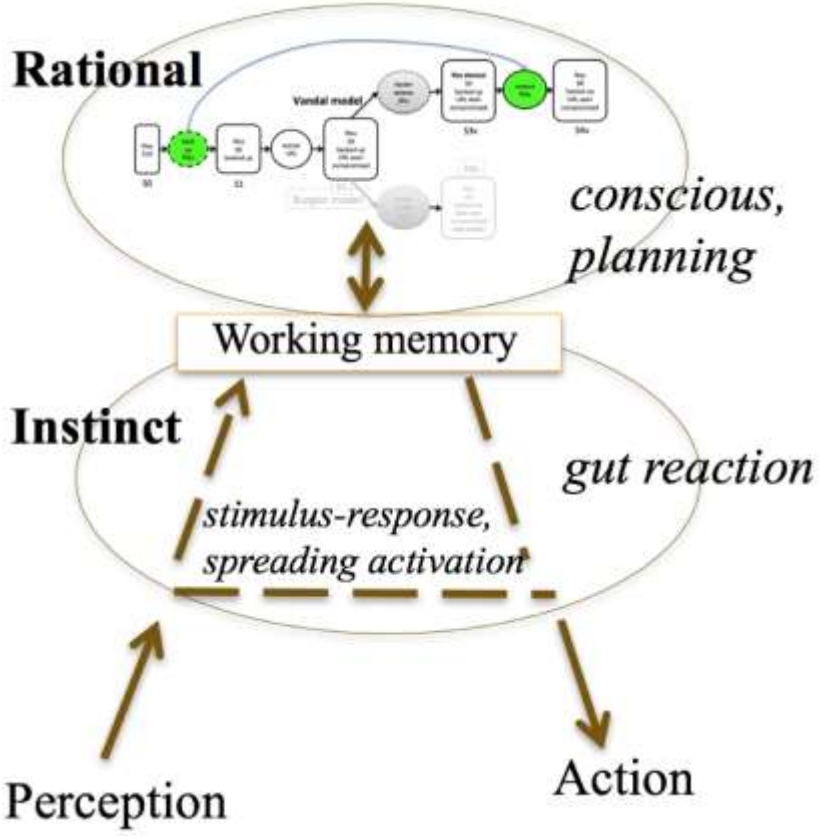
Once we know the likely behavior of individuals based on survey data and behavioral experimentation,

Agent-based simulation can help explore the consequences of that behavior in organizations.

Principled simulation can help explore policies in silico before paying costs for poor fits in the real world.

Simulations that fail to model known group behavior can point to where more field work is needed.

DASH Cognitive Agents



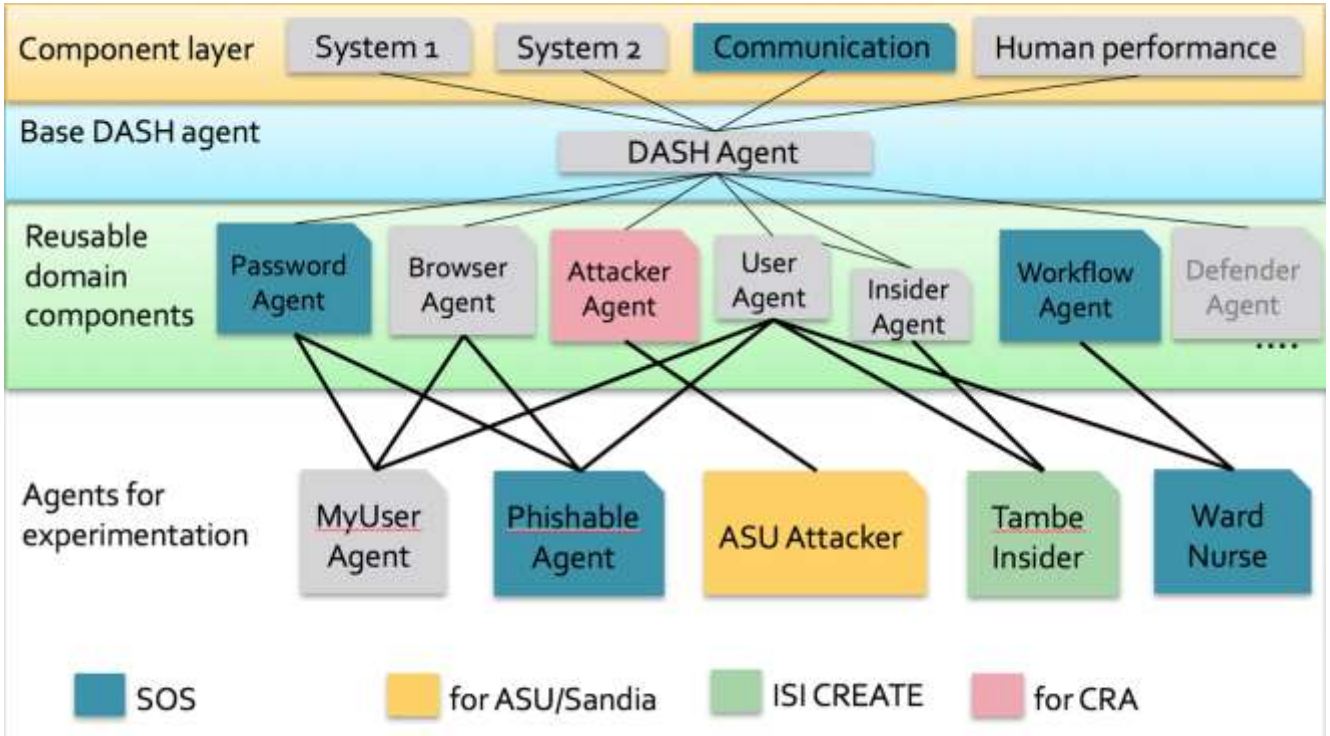
Dual process

Reactive planning

Mental models

Spreading activation

Designed for Speed, Reuse and Customization



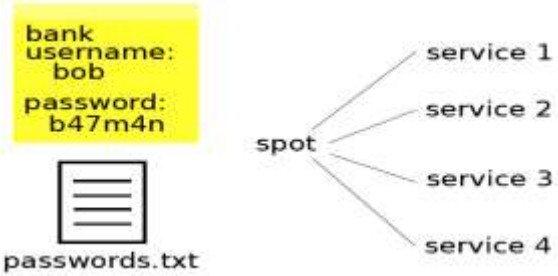
Reimplemented in object-oriented python.

Have run millions of agents in DETER simulation.

E.g. DASH Agent Model (DASHWords)

Levenshtein measure of cognitive burden

[Kothari et al. 15]

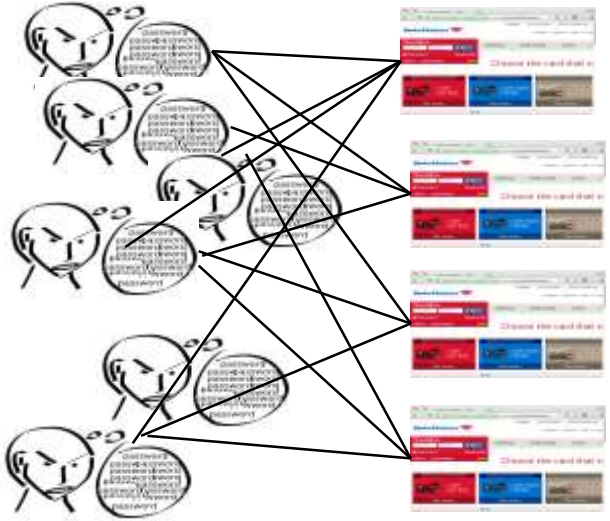


Circumvention models from survey

Direct + reuse measure of security

Demonstrates ‘Uncanny Descent’

As constraints increase, end-to-end security may decrease

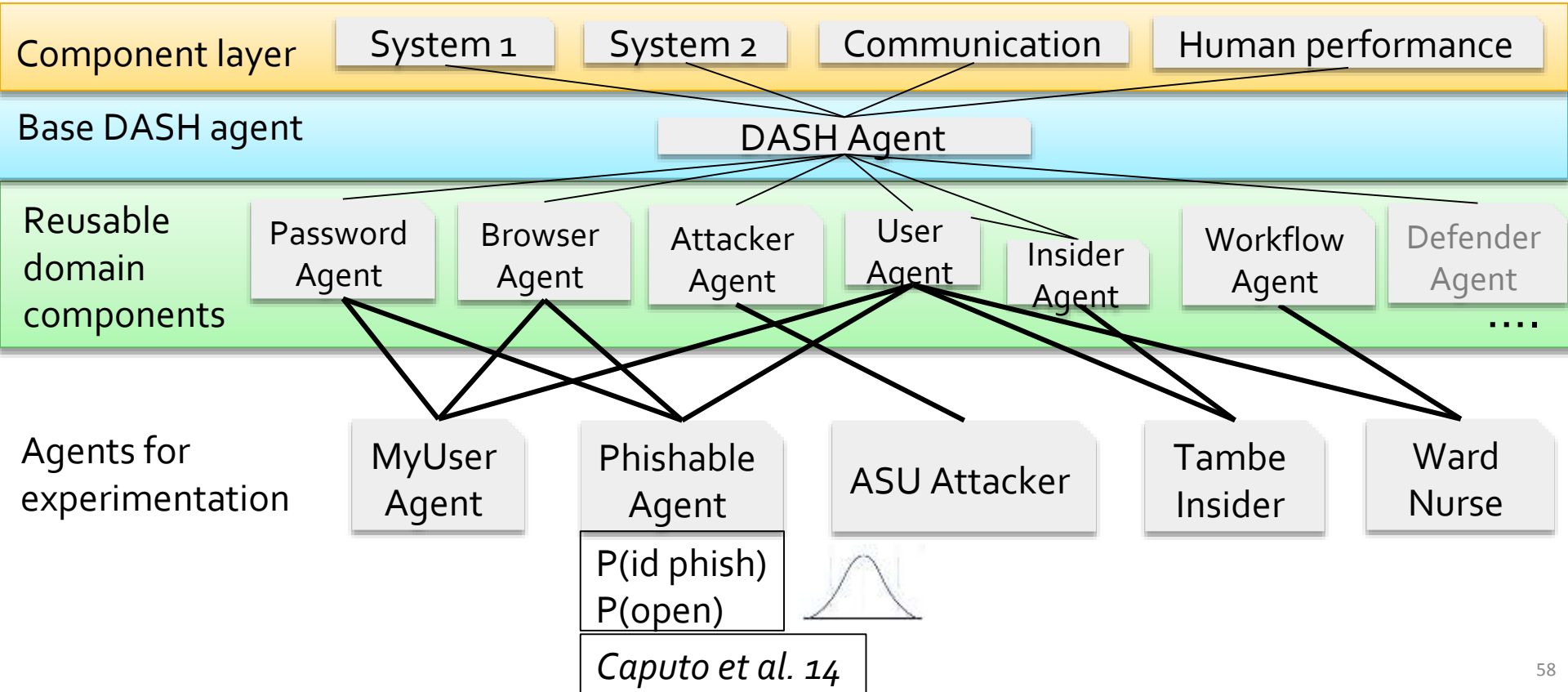


[Kothari et al. 15, 16]

Current & Future work: Evidence-based Cybersecurity

- How well do simulation findings reflect reality?
- Link parameters to experimental results and test their impact

Components Explicitly Linked to Supporting Experiments



FARM Helps User Select Appropriate Settings

- Single most likely scenario:
  - 15 phish emails sent in one day, several hits

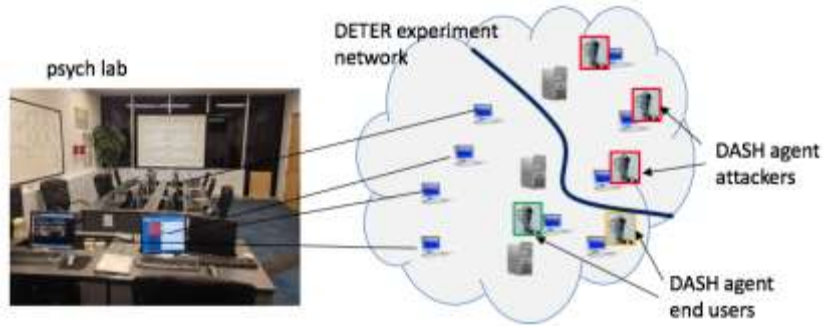
- Samples the space of possible scenarios:

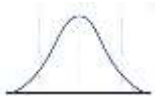
  0.5 ≤ p(id phish) ≤ 0.8,

  0.1 ≤ p(open attachment) ≤ 0.

  ...,

  → number of phish emails from 10--30.





FARM Helps Analyze Results

Reject null hypothesis w prob 0.95, (teaming is better) *when there are 15 phishing targets*.

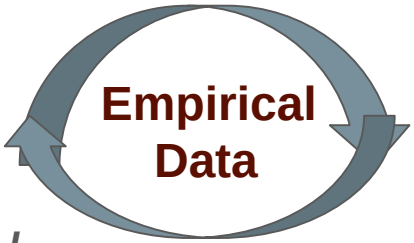
Experimenter knows more phish ⇒ teaming less important

FARM can

- estimate probability ≤ 25 phish by sampling parameter space.
- find most likely scenario *given* > 20 phish by subsampling

Next Steps

Fieldwork, Observations
Surveys, Logs



Simulation /
DASH

Models of
behavior and
action

Evidence-based
cybersecurity
and policy

Acquiring More Data

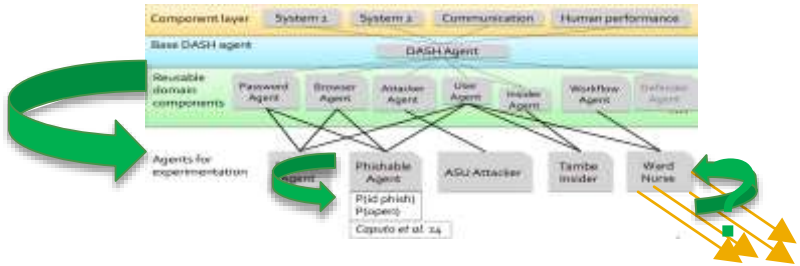
- Sources of data:
  - Mechanical Turk password experiment
    - Infrastructure in place---and IRB approval just arrived!
  - Available data: help-desk logs, server logs, etc.
  - Follow-up surveys and experiments to:
    - compare user and expert security behaviors and perceptions
    - determine how users interpret security advice

Revising and Extending Simulations

- Improve simulations based on new data
- Further explore interconnectedness of prescribed behaviors, user decision-making processes, and actual behaviors
- ...***and impact on aggregate security***
  - What do the curves really look like?
  - Can we help with ***evidence-based*** cybersecurity policy decisions?
- Extend from enterprise scenarios to home IoT scenarios

Automatic Reasoning About the Link Between Data and Simulation

- FARM will record the link from data to simulation parameters to:
  - find most likely settings for behavior under test
  - explore dependence of recommendations on data
  - sometimes suggests refined experiments/analysis



Potential to link simulation community to experimental community

Publications

- J. Blythe, R. Koppel, S.W. Smith. Circumvention of Security: Good Users do Bad Things. IEEE Security and Privacy. 11 (5): 80--83. September/October 2013.
- S.W. Smith and R. Koppel. Healthcare Information Technology's Relativity Problems: A Typology of How Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ. Journal of the American Medical Informatics Association. 21: 117-131, 2014.
- V. Kothari, J. Blythe, S.W. Smith, R. Koppel. Agent-Based Modeling of User Circumvention of Security. ACySE '14: Proceedings of the 1st International Workshop on Agents and CyberSecurity. ACM. 2014.
- R. Koppel, S.W. Smith, J. Blythe, V. Kothari. Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? Driving Quality in Informatics: Fulfilling the Promise. IOS Press, Studies In Health Technology and Informatics, Volume 208, pp 215-20, February 2015.
- V. Kothari, J. Blythe, S.W. Smith, R. Koppel. Measuring the Security Impacts of Password Policies Using Cognitive Behavioral Agent-Based Modeling. ACM Symposium and Bootcamp on the Science of Security (HotSoS). April 2015.
- S.W. Smith, R. Koppel, J. Blythe, V. Kothari. Mismorphism: a Semiotic Model of Computer Security Circumvention. International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015). July 2015.
- H. Thimbleby, R. Koppel. The Healthtech Declaration. IEEE Security and Privacy. 13 (6): 82-84, Nov/Dec 2015.
- B. Korbar, J. Blythe, R. Koppel, V. Kothari, and S.W. Smith. Validating an Agent-Based Model of Human Password Behavior The AAAI-16 Workshop on Artificial Intelligence for Cyber Security (AICS). February 2016.
- R. Koppel, J. Blythe, V. Kothari, S.W. Smith. Beliefs About Cybersecurity Rules and Passwords: A Comparison of Two Survey Samples of Cybersecurity Professionals Vs. Regular Users. SOUPS 2016 Security Fatigue Workshop.

Conclusion (Our Project in a Nutshell)

- Problem
  - *Security engineering doesn't work if predicated on the fantasy that good users fully comply!*
- Key Questions:
  - Why do users circumvent?
  - How does circumvention affect aggregate security?
  - How do we improve aggregate security?
- Project Goal:
  - To ***propose*** security solutions and develop metrics to make meaningful, quantifiable ***comparisons***, ***decisions***, and other ***evaluations*** of proposed solutions in light of what users do.

Thank you! Questions?