User Circumvention of Cybersecurity: A Cross-Disciplinary Approach

Sean W. Smith

Professor---Department of Computer Science
Director---Institute for Security, Technology, and Society

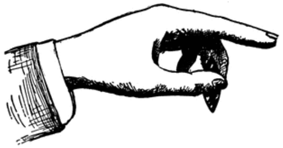
Dartmouth College

24 April 2017

This Talk

1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security
6. Towards Understanding Policy Creation
7. Next Steps

This Talk

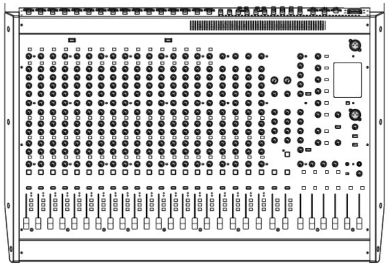


1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security
6. Towards Understanding Policy Creation
7. Next Steps

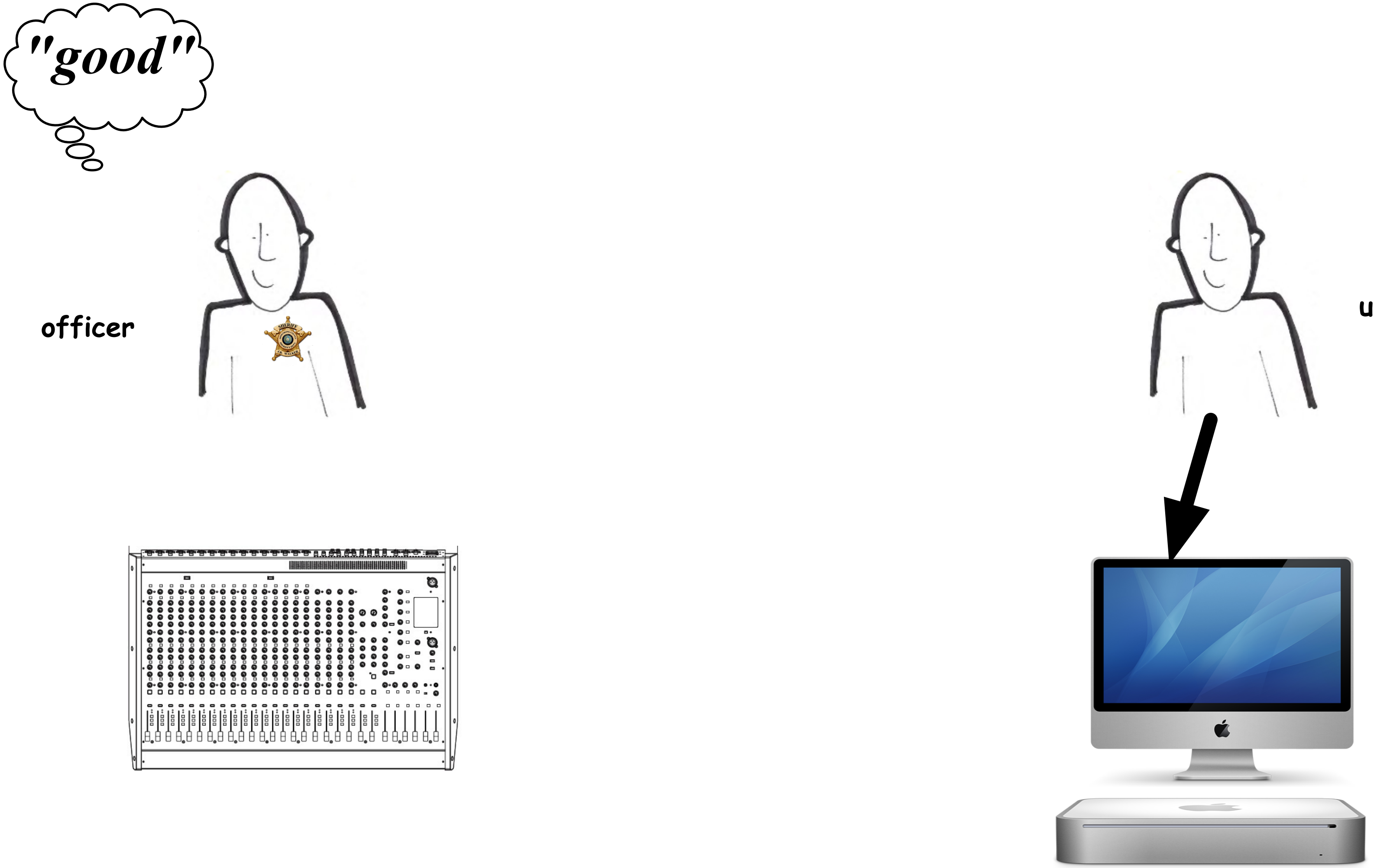
Access Control for Data Big and Little

officer

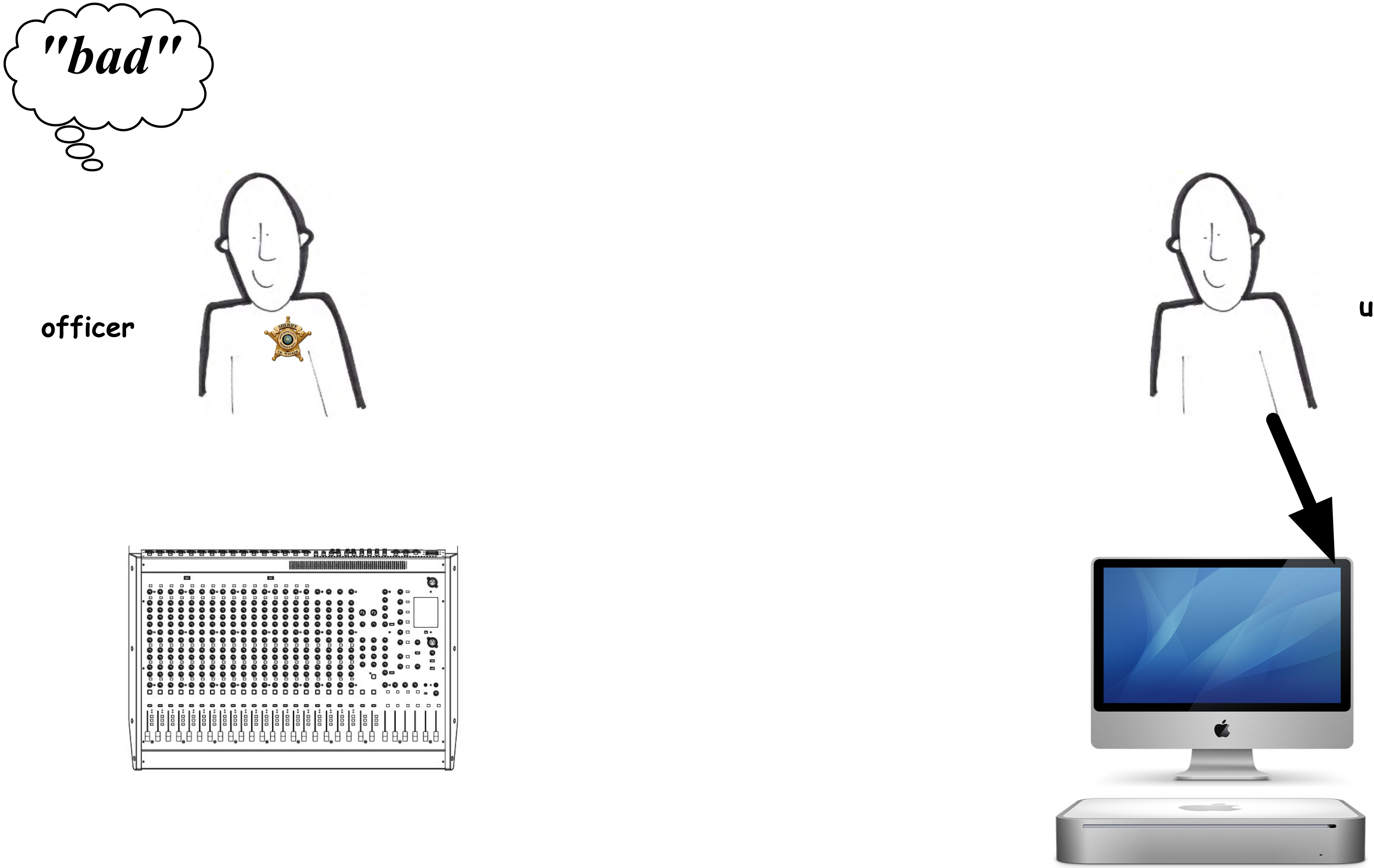
user



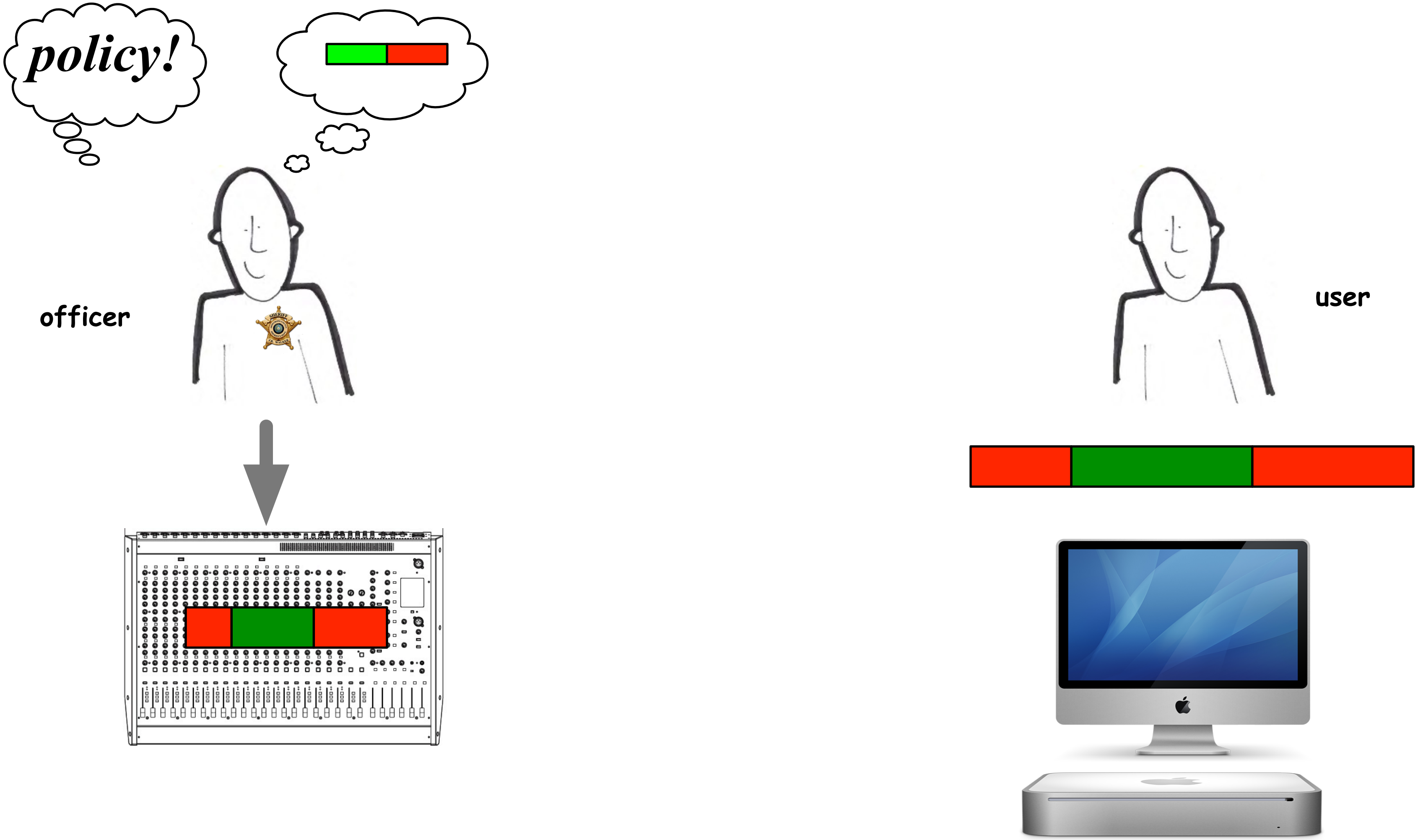
Access Control for Data Big and Little



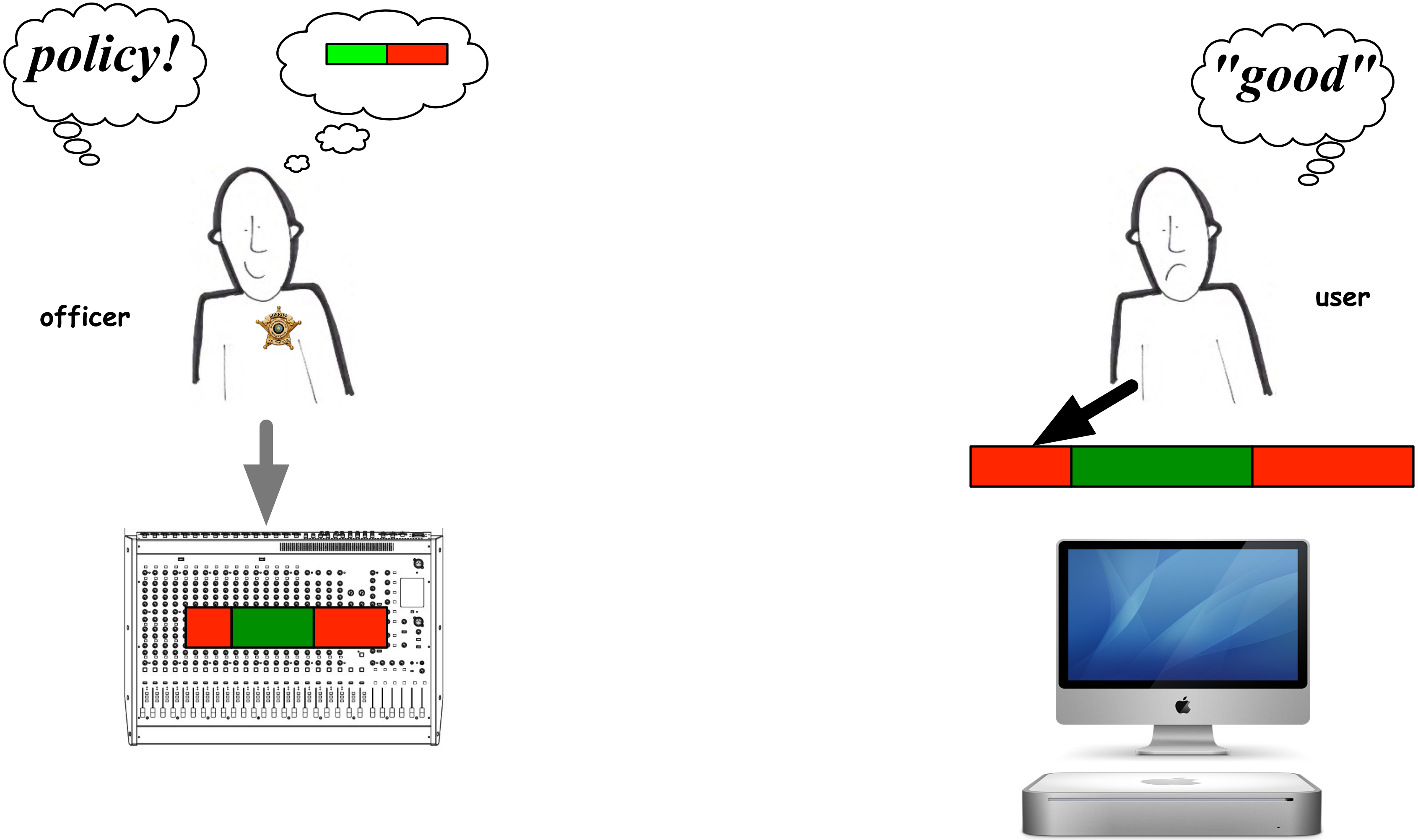
Access Control for Data Big and Little



Access Control for Data Big and Little



Access Control for Data Big and Little



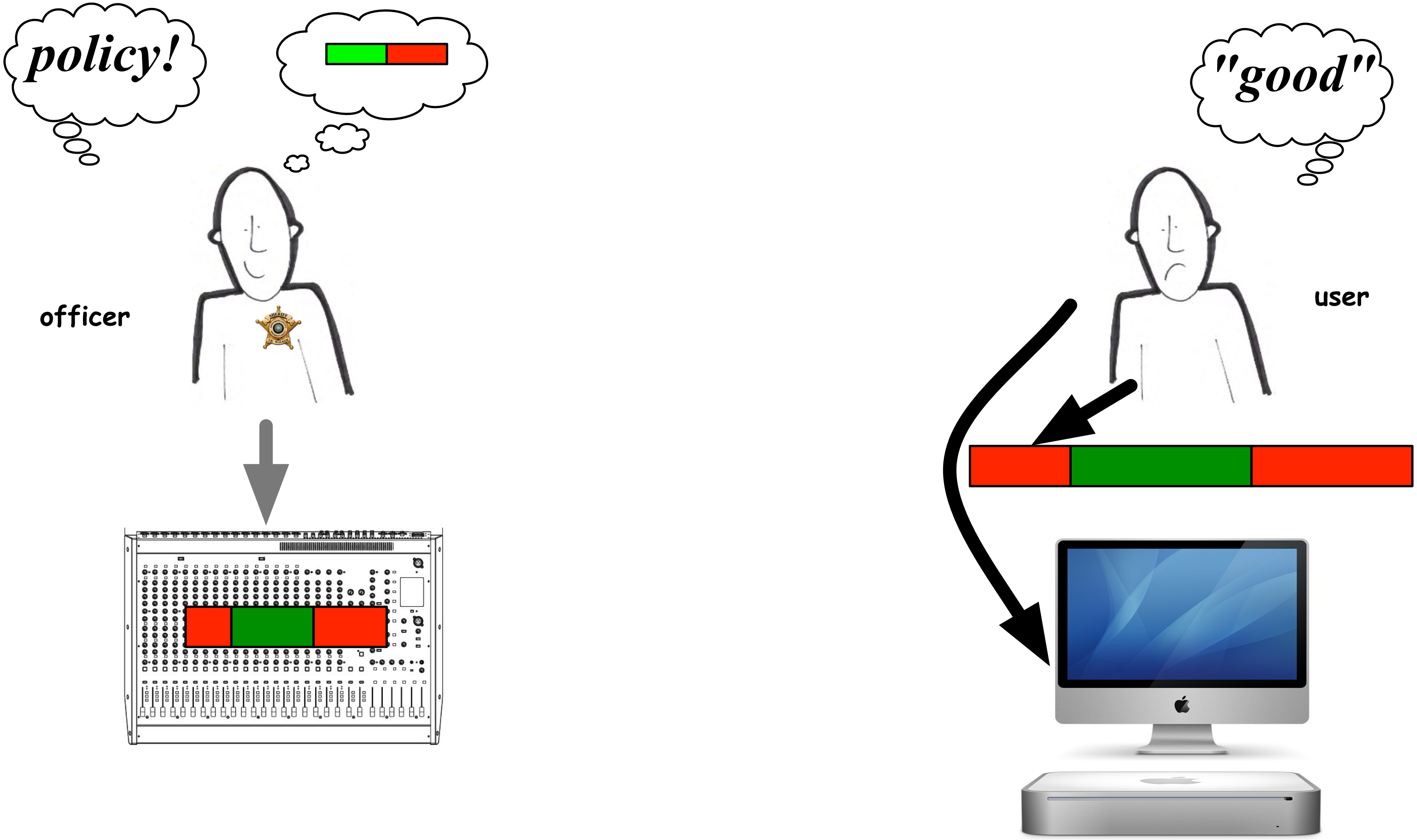
policy!

officer

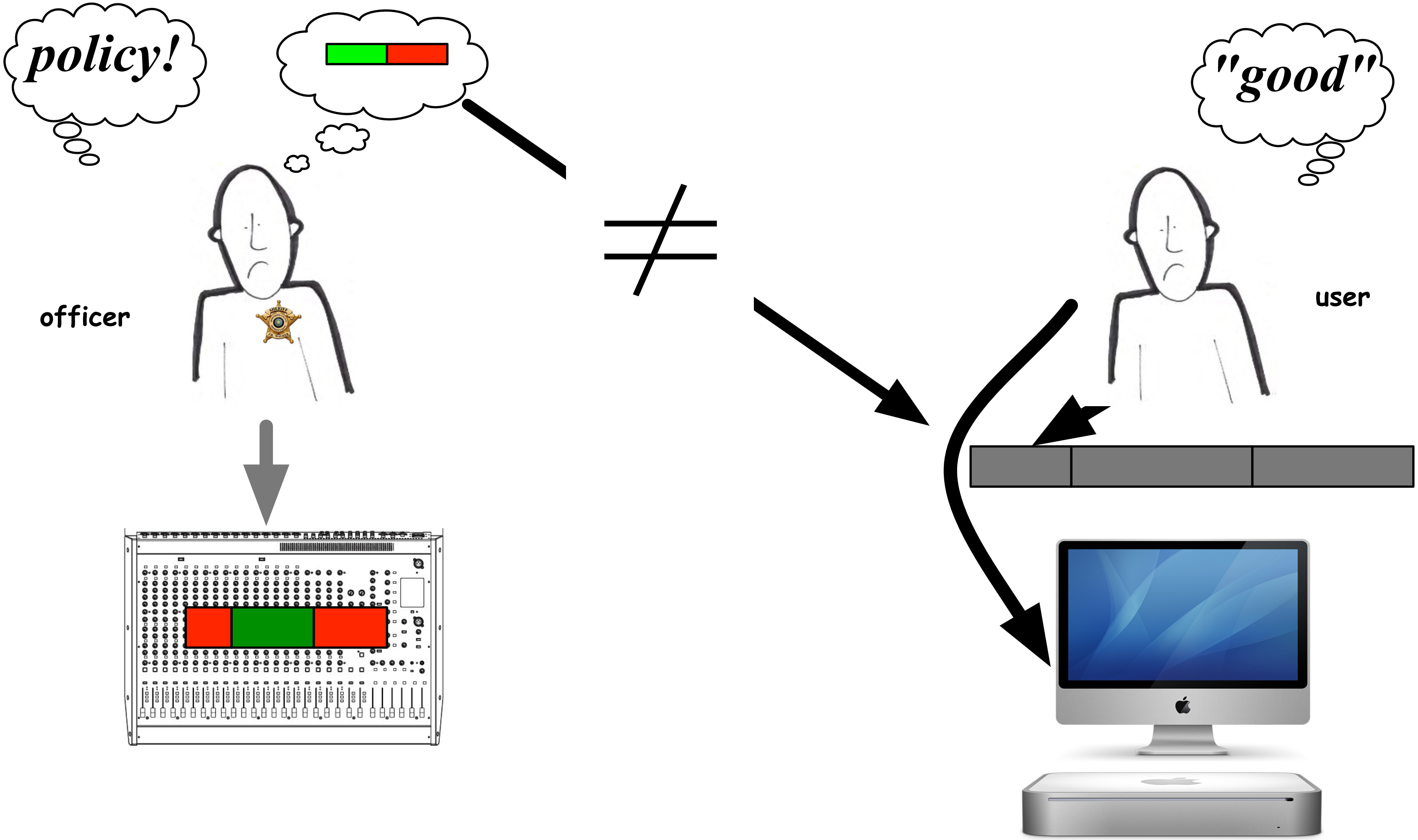
"good"

user

Access Control for Data Big and Little



Access Control for Data Big and Little



policy!

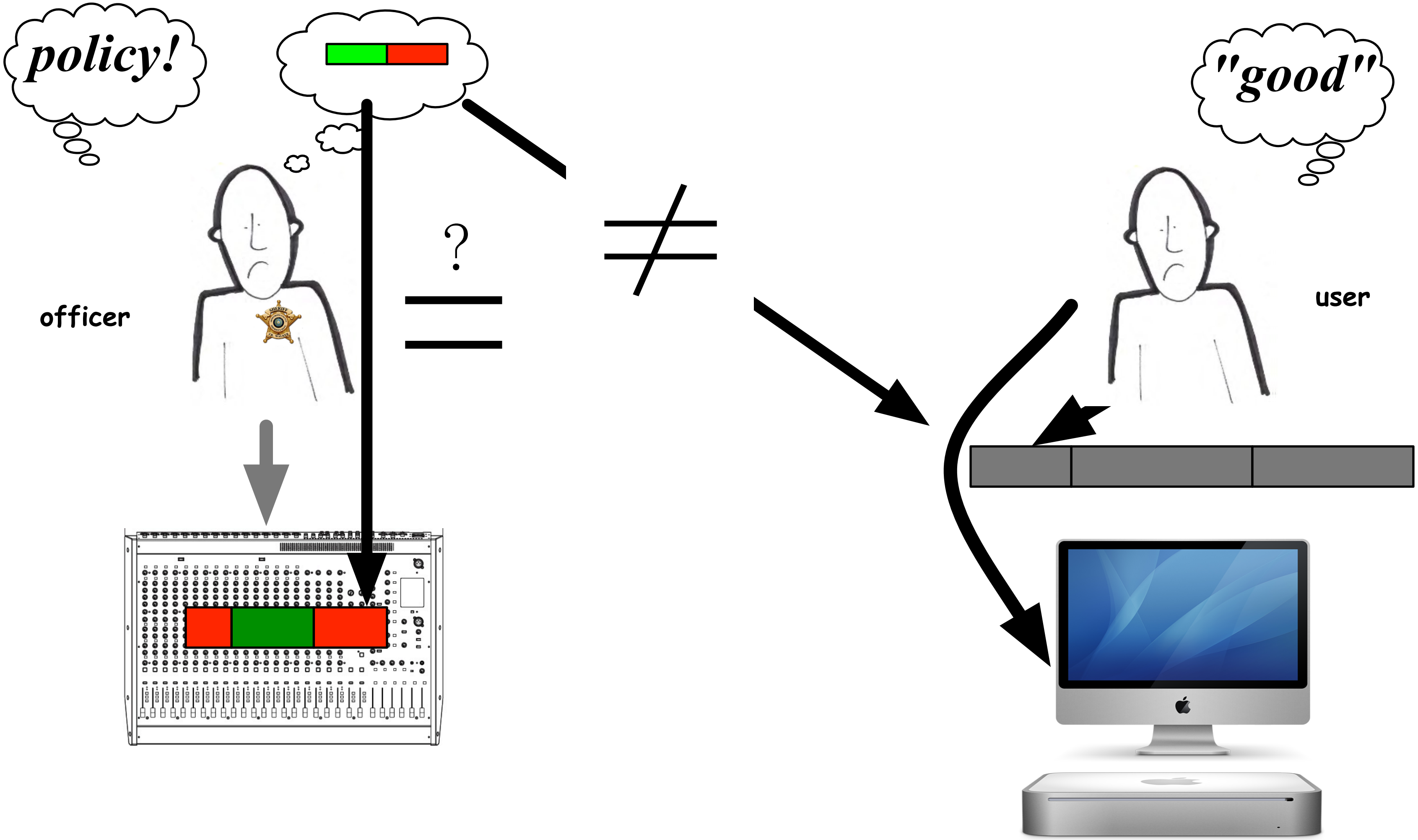
≠

"good"

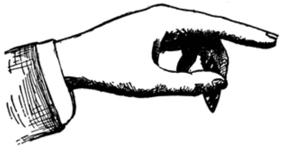
officer

user

Access Control for Data Big and Little



This Talk



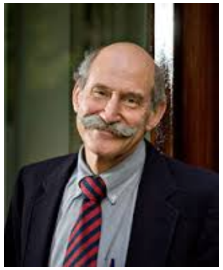
1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security
6. Towards Understanding Policy Creation
7. Next Steps

Crossing Disciplines

- Computer security
- Sociology
- Ethnography
- AI
- Simulation
- Psychology

SHUCS

Jim Blythe, USC

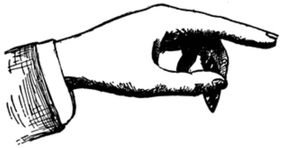


Ross Koppel, Penn

VIjay Kothari, Dartmouth

And a stream of undergraduate interns

This Talk

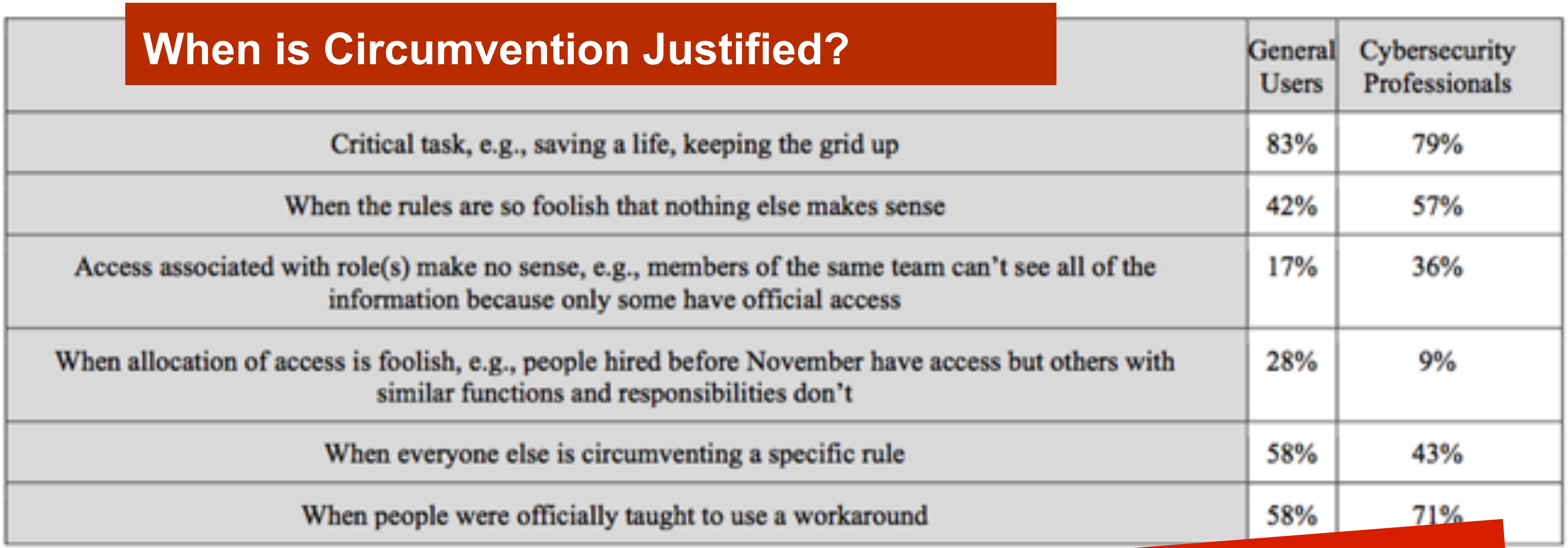


1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security
6. Towards Understanding Policy Creation
7. Next Steps

Sociology, Ethnography, Surveys, Log Analysis

- 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.

When is Circumvention Justified?



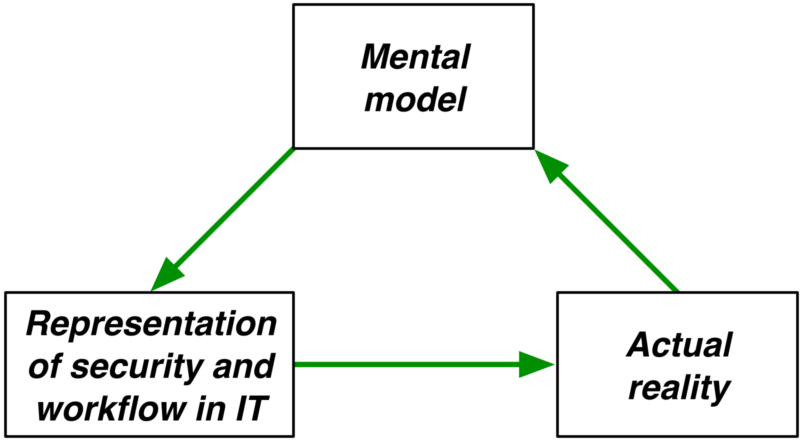
	General Users	Cybersecurity Professionals
Critical task, e.g., saving a life, keeping the grid up	83%	79%
When the rules are so foolish that nothing else makes sense	42%	57%
Access associated with role(s) make no sense, e.g., members of the same team can't see all of the information because only some 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"

This Talk

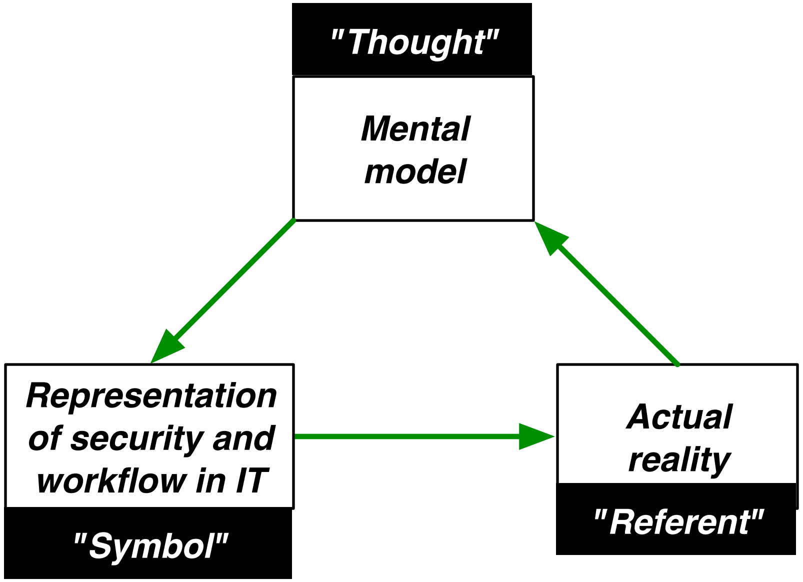
1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security
6. Towards Understanding Policy Creation
7. Next Steps

Mismatches



Smith and Koppel 2014

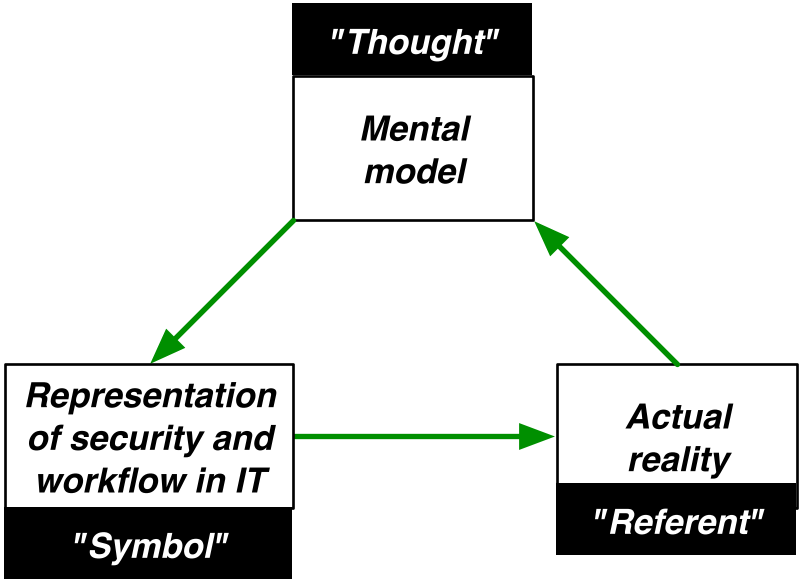
Mismatches



Smith and Koppel 2014

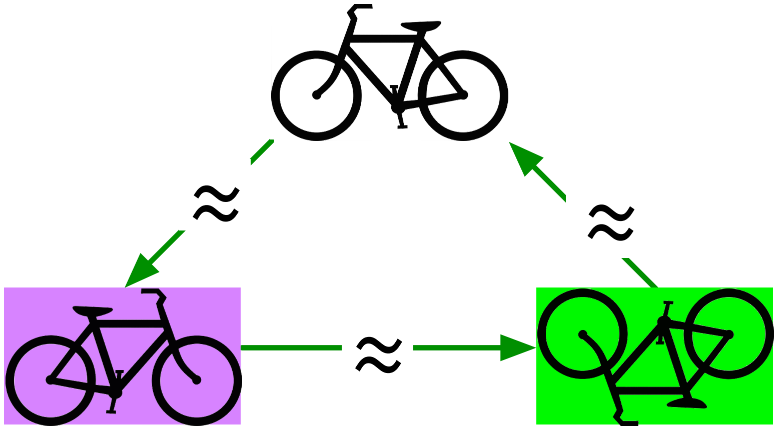
Ogden and Richards, 1927

In Language: Morphism



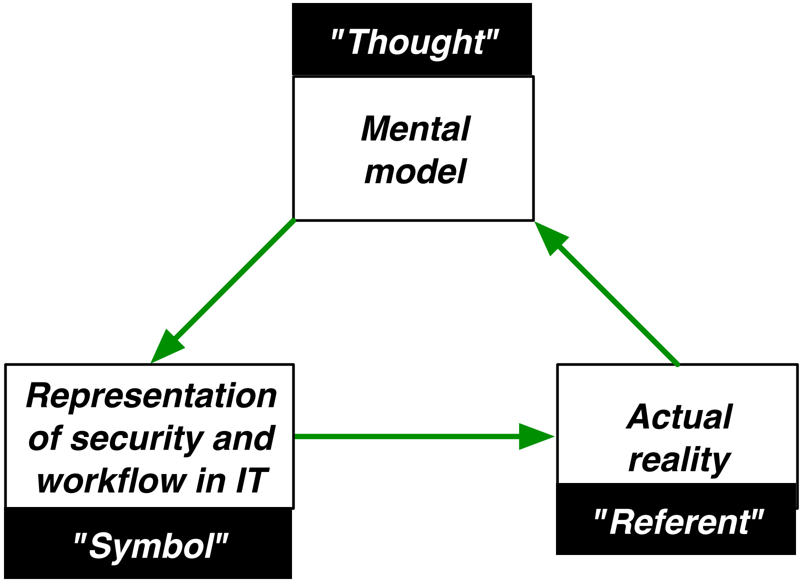
Smith and Koppel 2014

Ogden and Richards, 1927

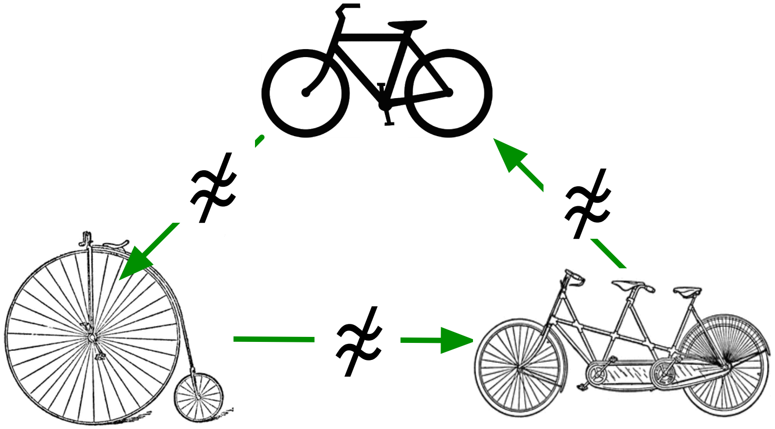


- Regular semiotics: ***morphisms.***
- Mappings ***preserve*** structure

In Security Usability: ***Mis***morphism

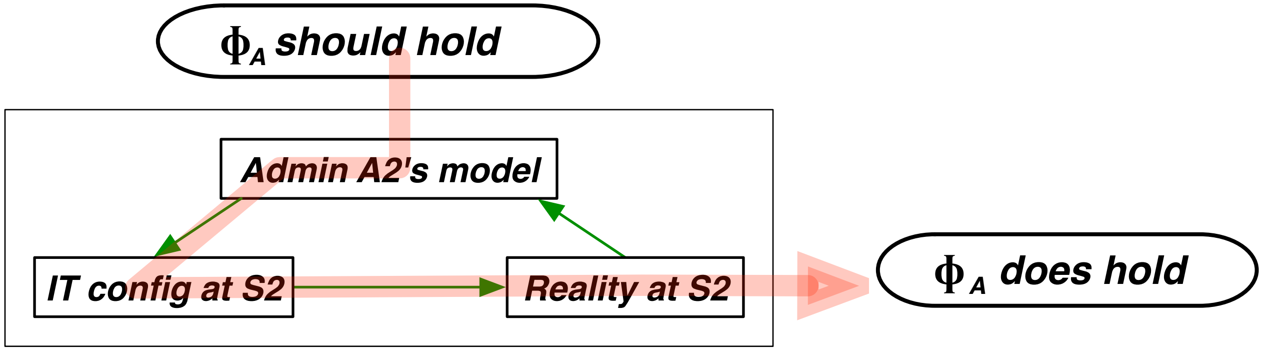


This project!

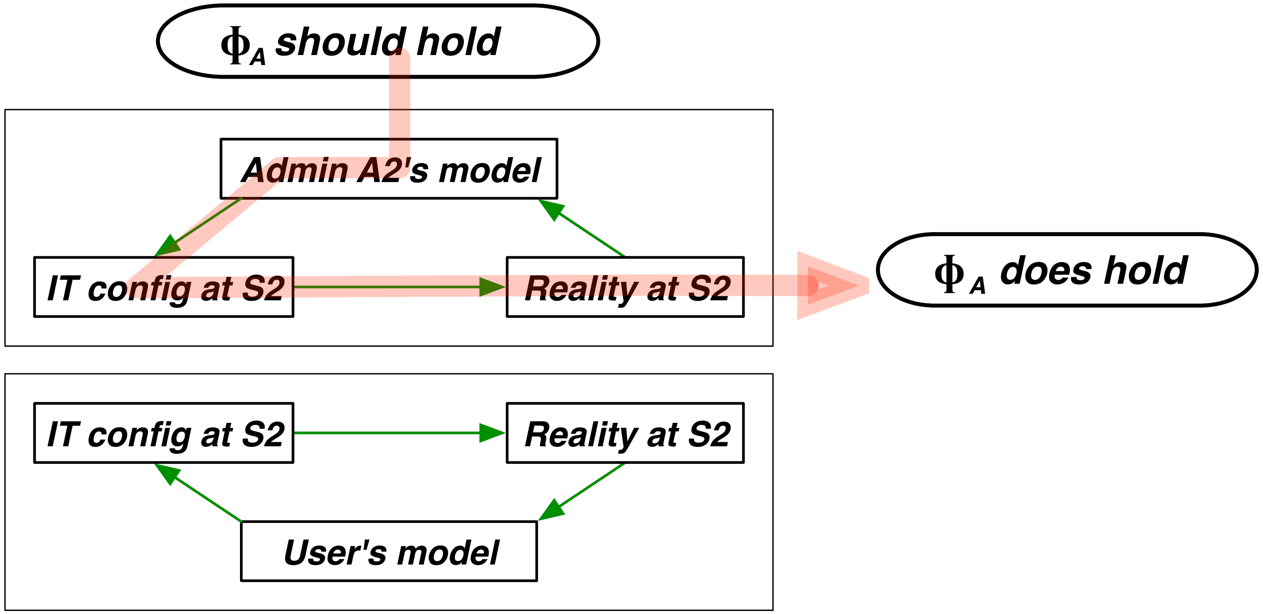


- Circumvention semiotics: ***mismorphisms.***
- Mappings ***fail to preserve*** structure

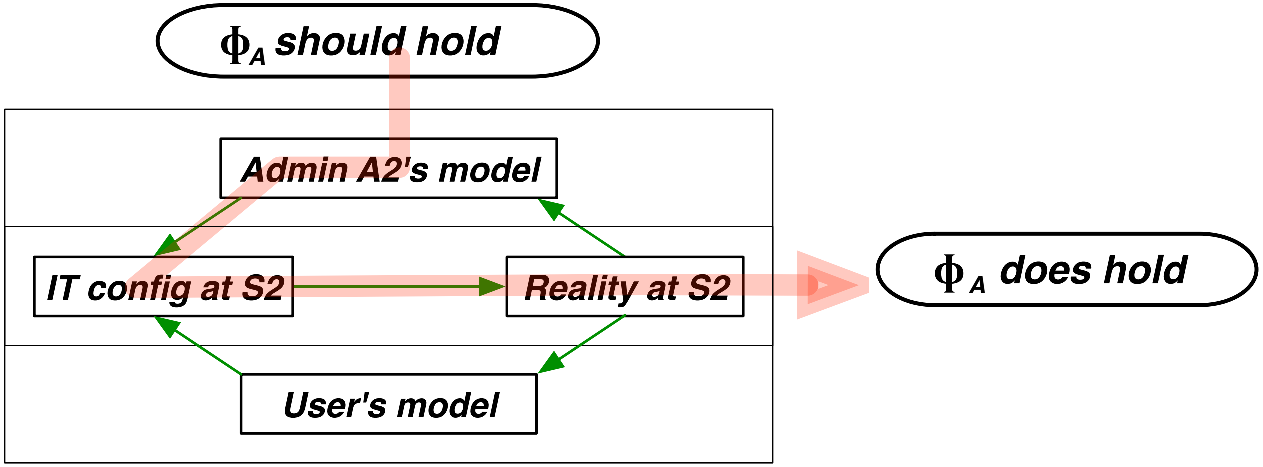
Causing Circumvention



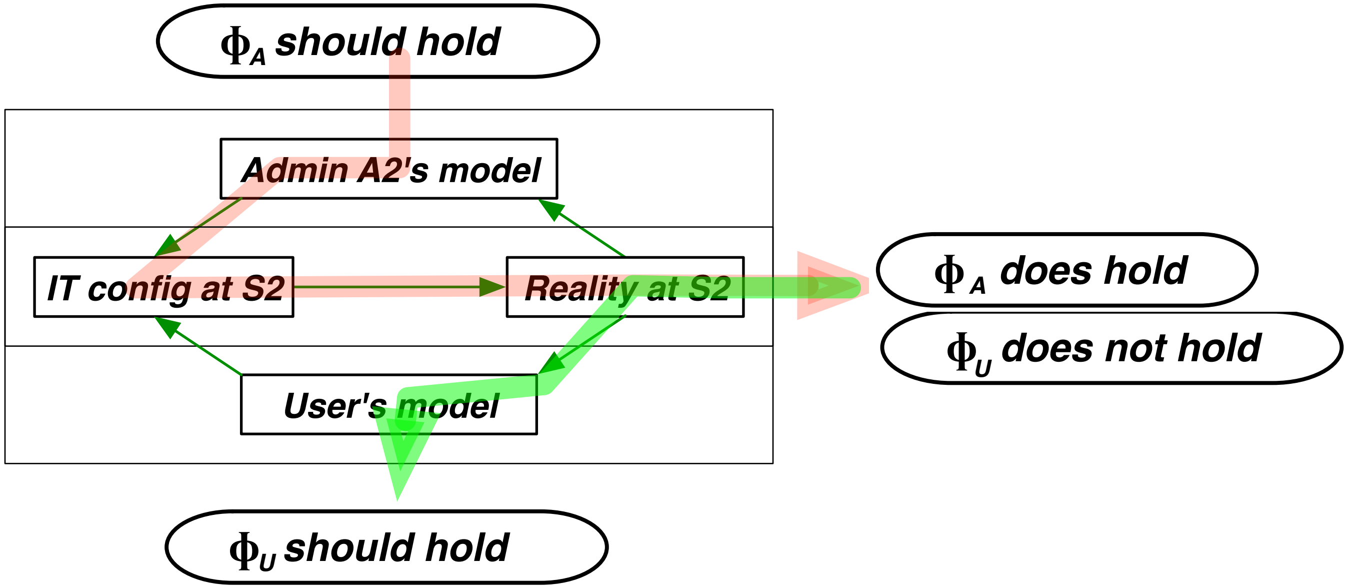
Causing Circumvention



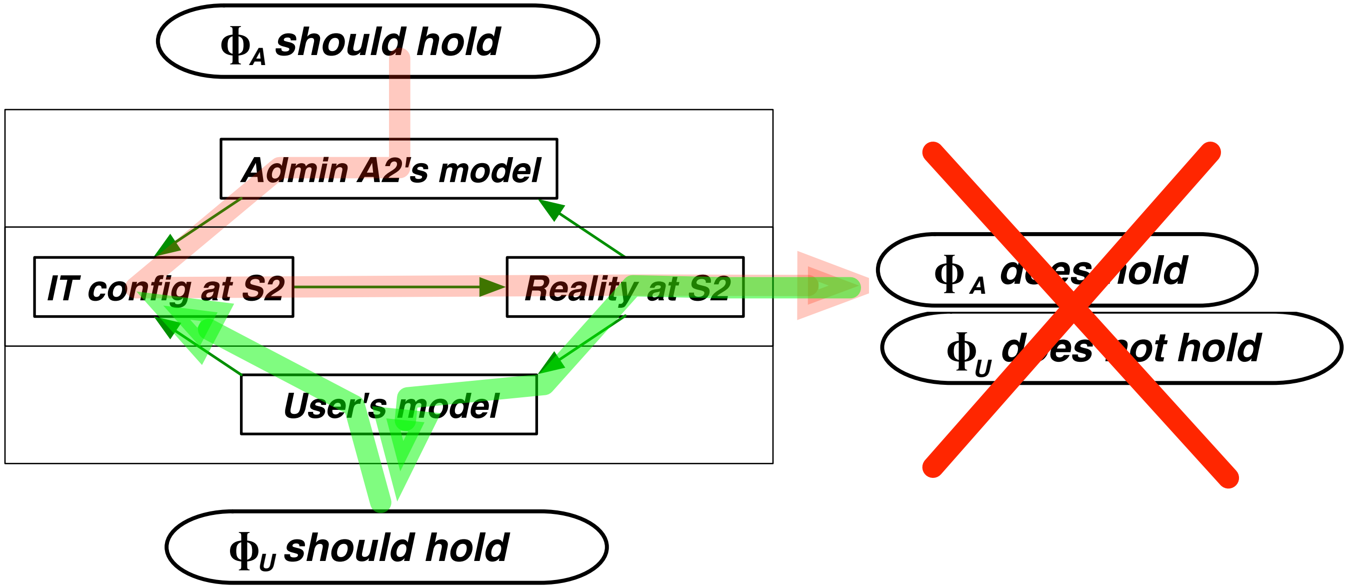
Causing Circumvention



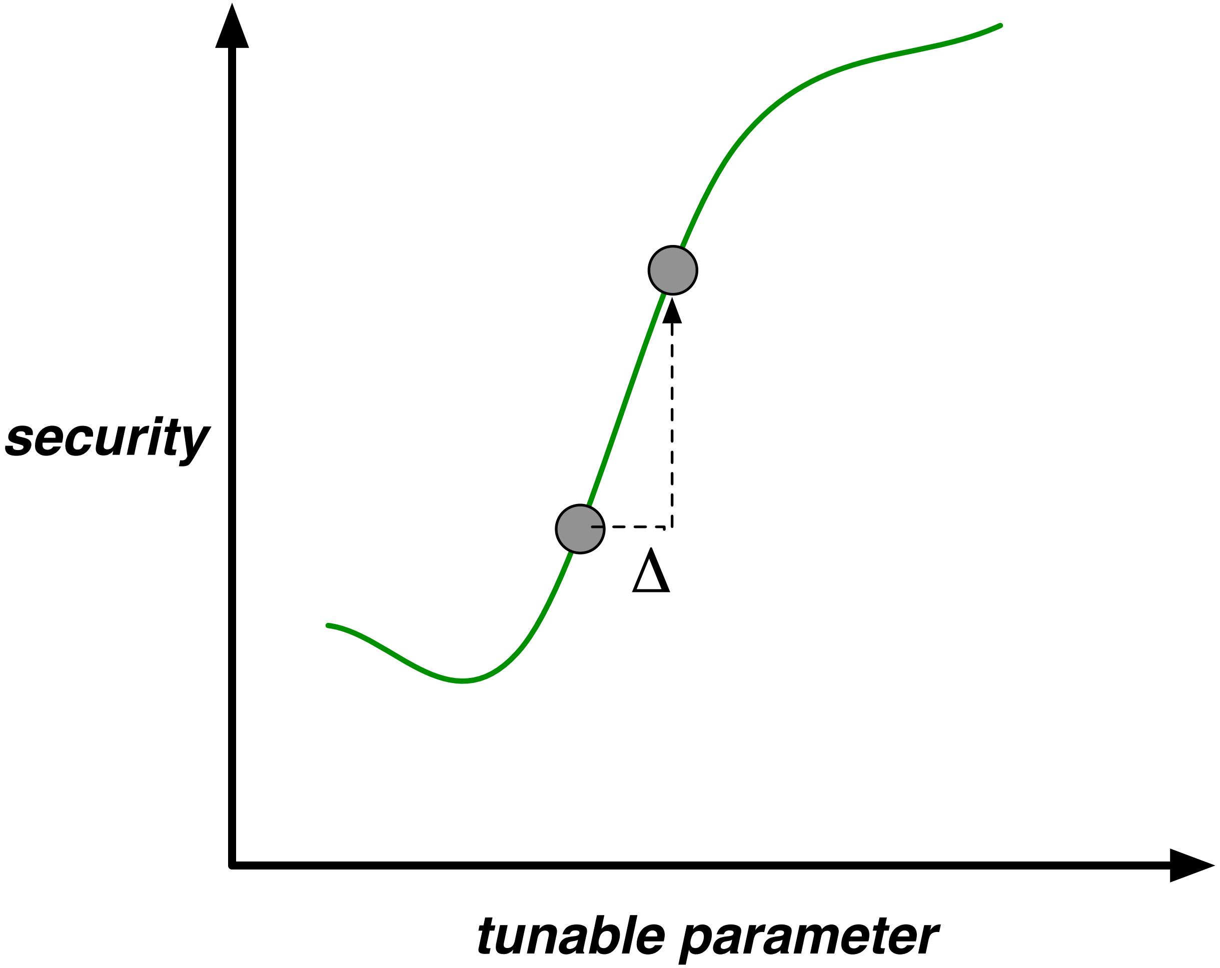
Causing Circumvention

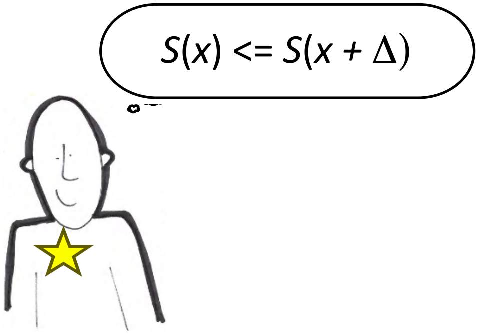


Causing Circumvention

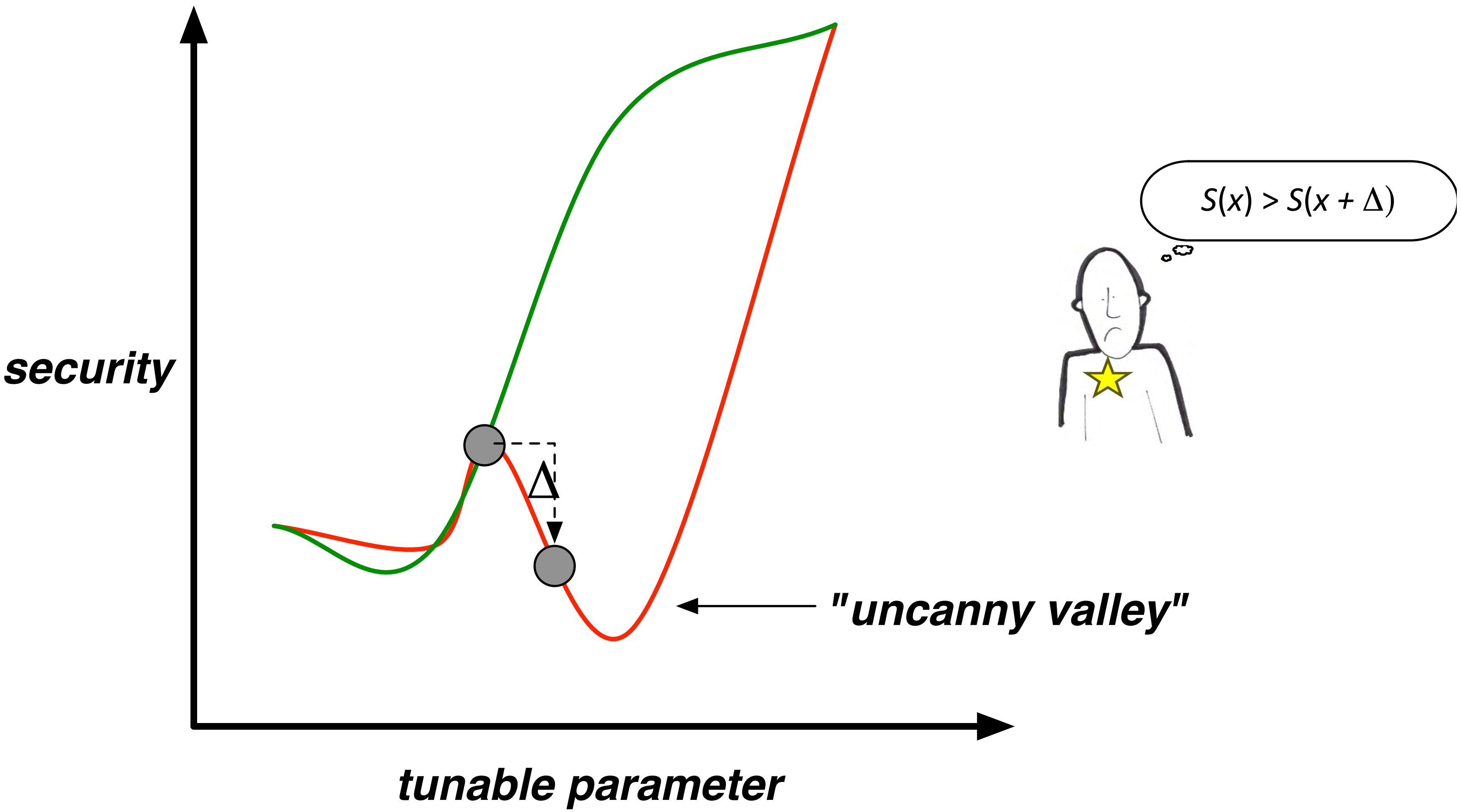


Trouble: Loss of Monotonicity





Trouble: Loss of Monotonicity



Trouble: Loss of Monotonicity

Uncanny ***descent***

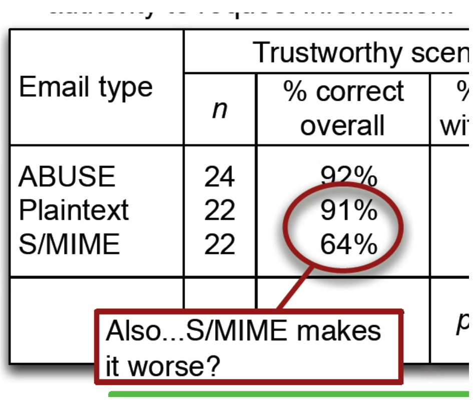
- timeouts
- password practices
- computerizing medical workflow

Uncanny ***ascent***

- "qwertyqwerty"
- executive passwords

Uncanny ***nop***

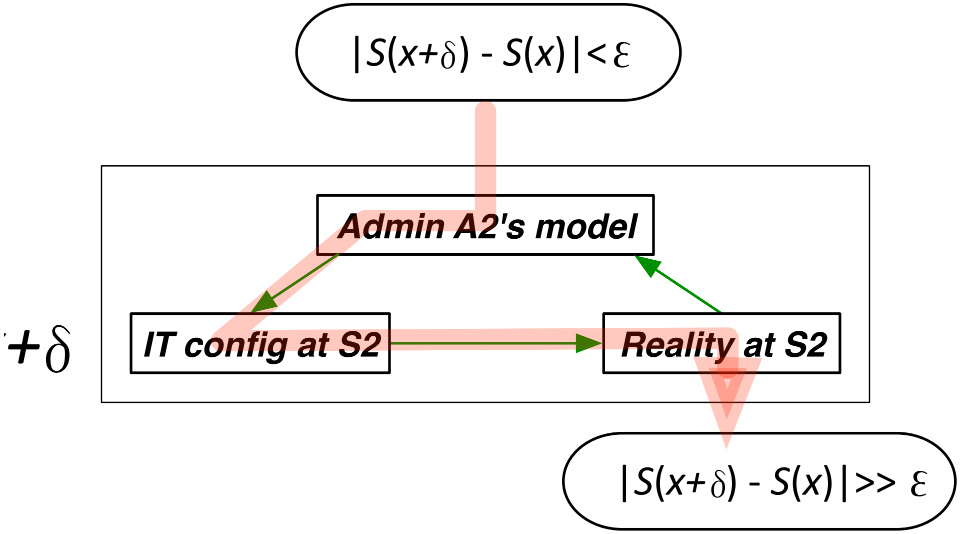
- public/internal wifi
- check diff password via hash
- deleting links, not files
- education not help



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

Also...S/MIME makes it worse?

Trouble: Loss of Continuity



$|S(x+\delta) - S(x)| < \varepsilon$

Admin A2's model

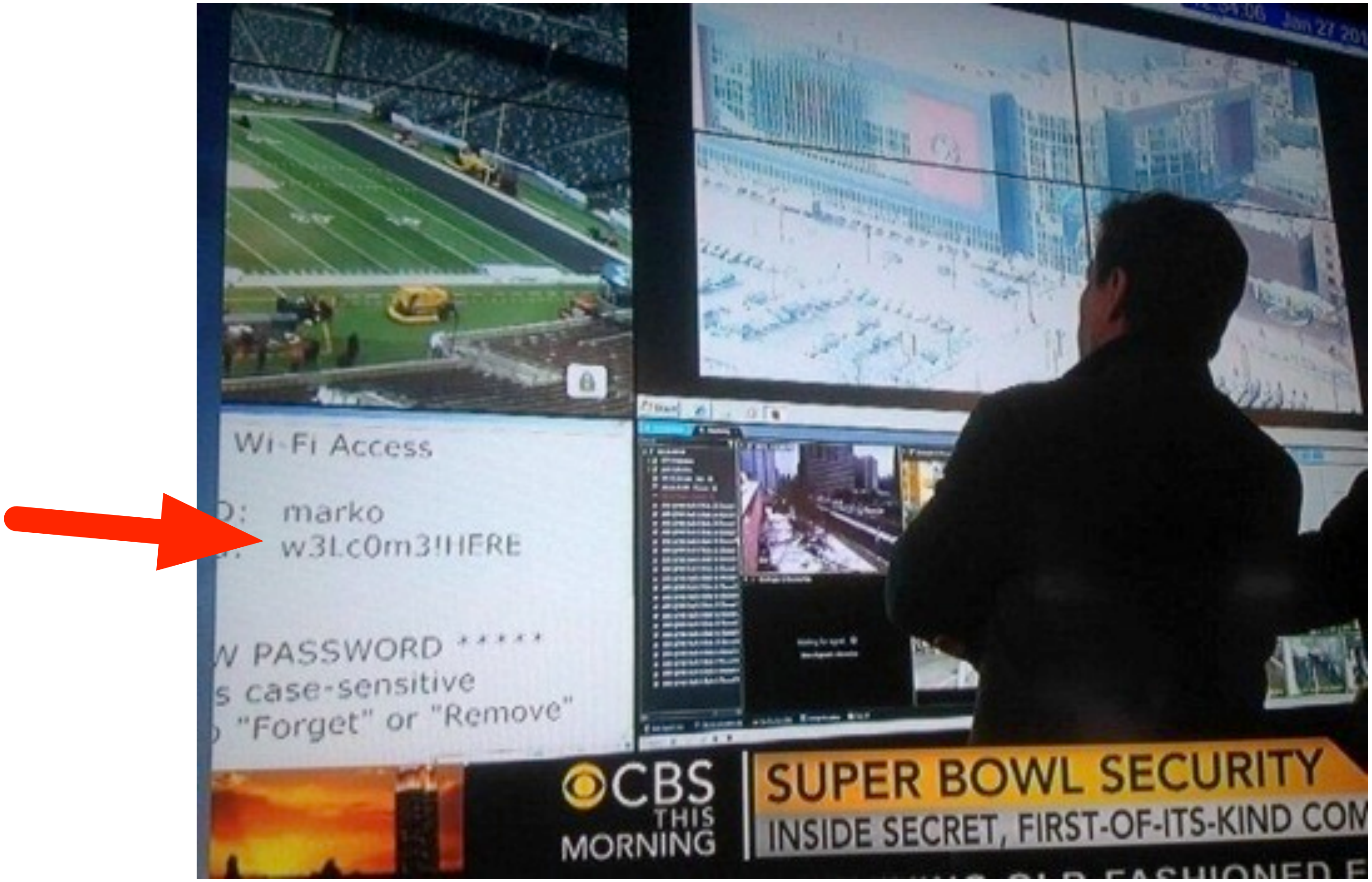
IT config at S2

Reality at S2

$+\delta$

$|S(x+\delta) - S(x)| >> \varepsilon$

Trouble: Loss of Continuity

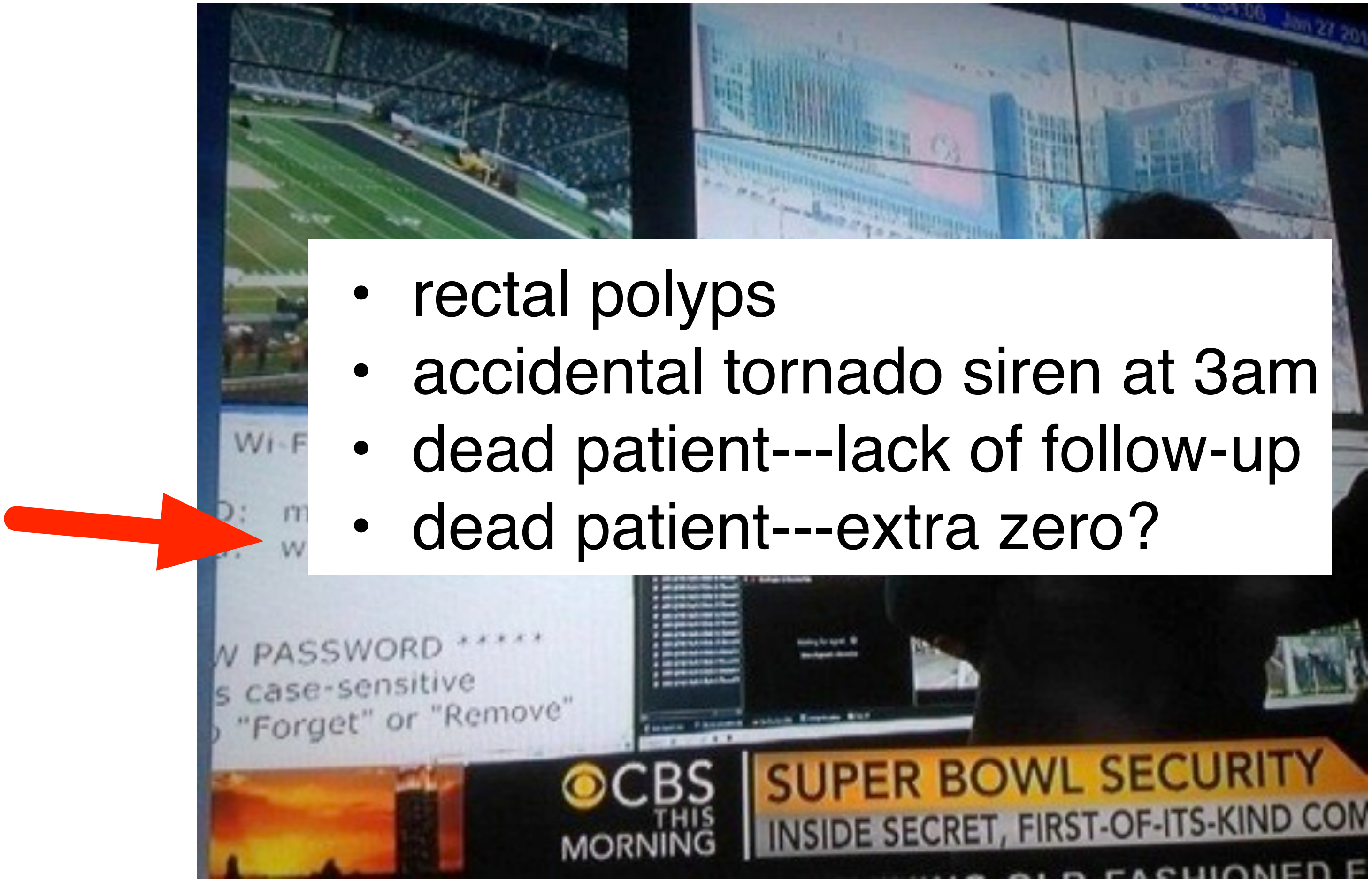


Wi-Fi Access

D: marko
: w3Lc0m3!HERE

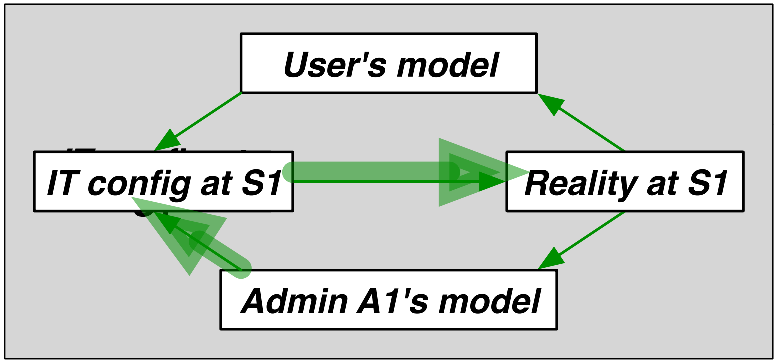
W PASSWORD *****
s case-sensitive
"Forget" or "Remove"

Trouble: Loss of Continuity



- rectal polyps
- accidental tornado siren at 3am
- dead patient---lack of follow-up
- dead patient---extra zero?

Trouble: Action at a Distance



User's model

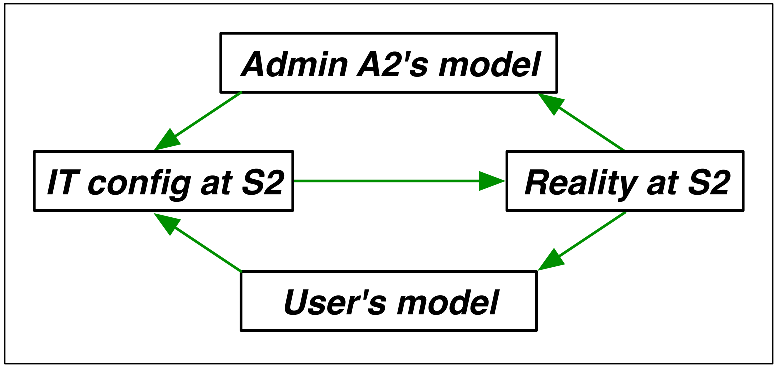
IT config at S1

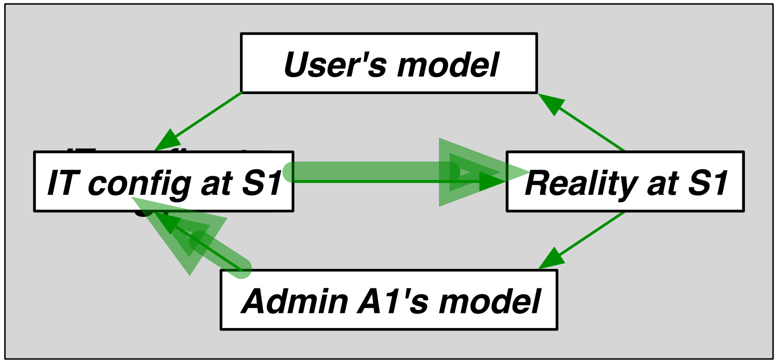
Reality at S1

Admin A1's model

S:C1→ S1

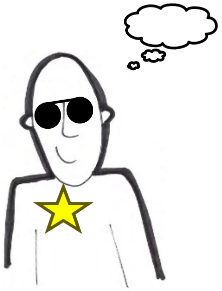
Trouble: Action at a Distance

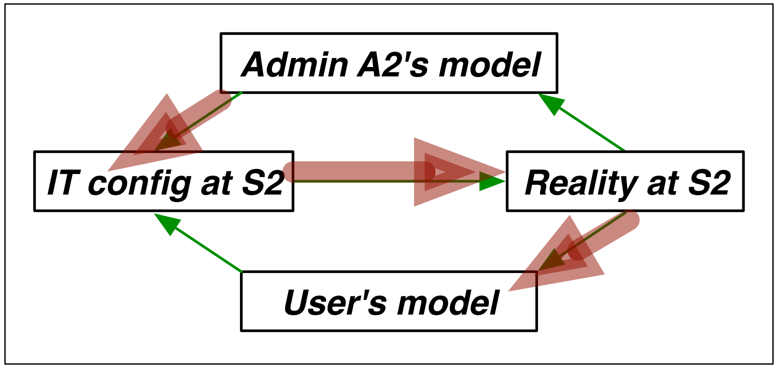


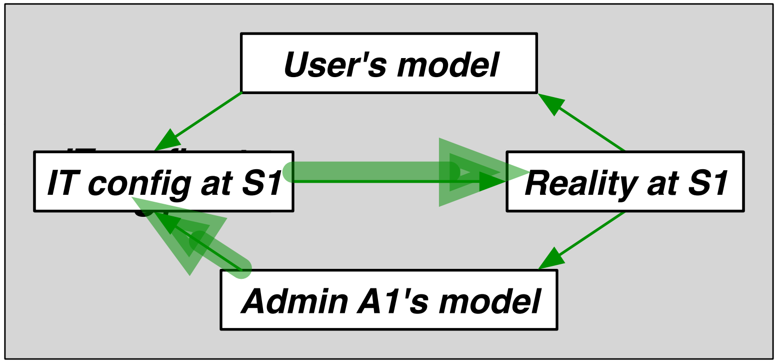


S:C1→ S1

Trouble: Action at a Distance

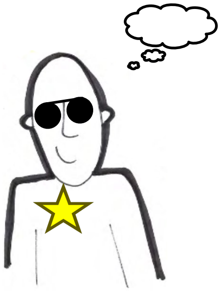


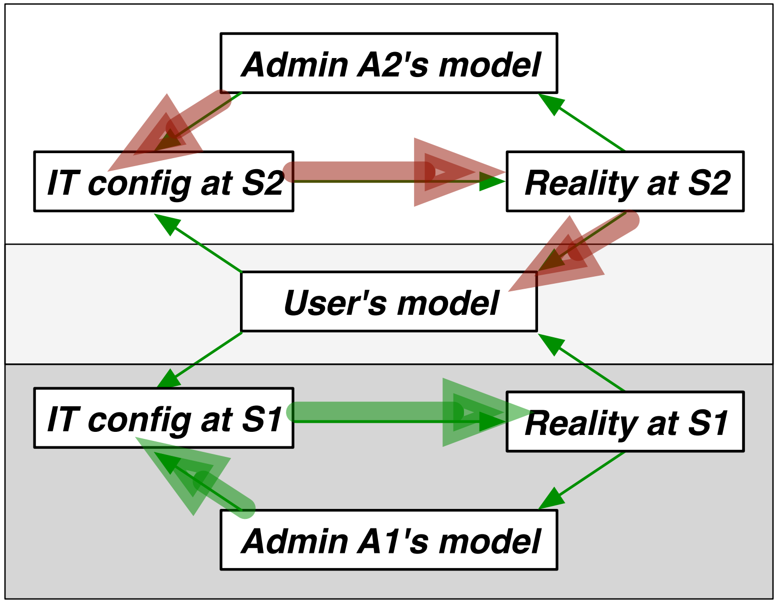




S:C1→ S1

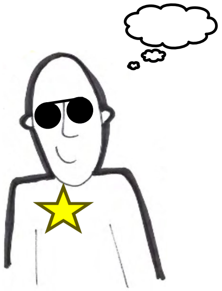
Trouble: Action at a Distance

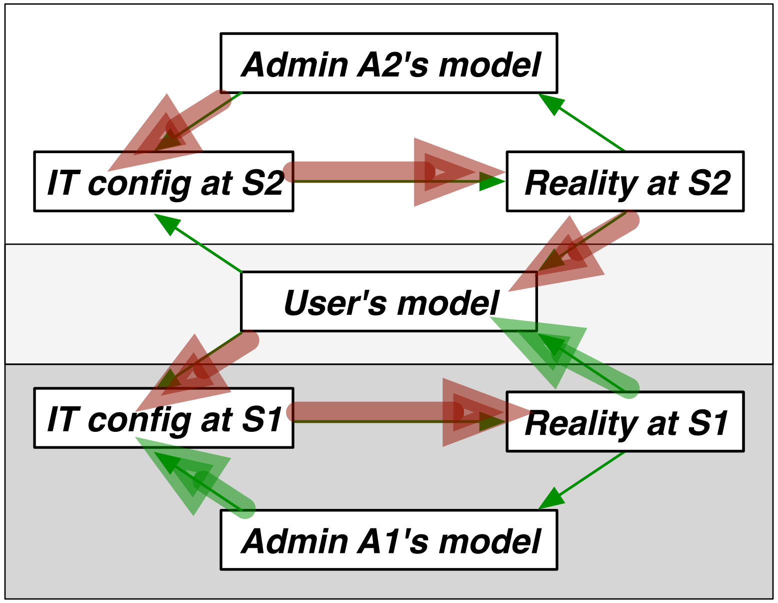


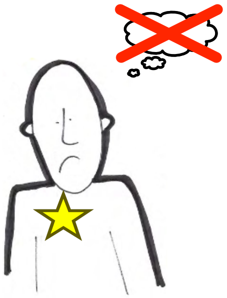


S:C1→ S1

Trouble: Action at a Distance





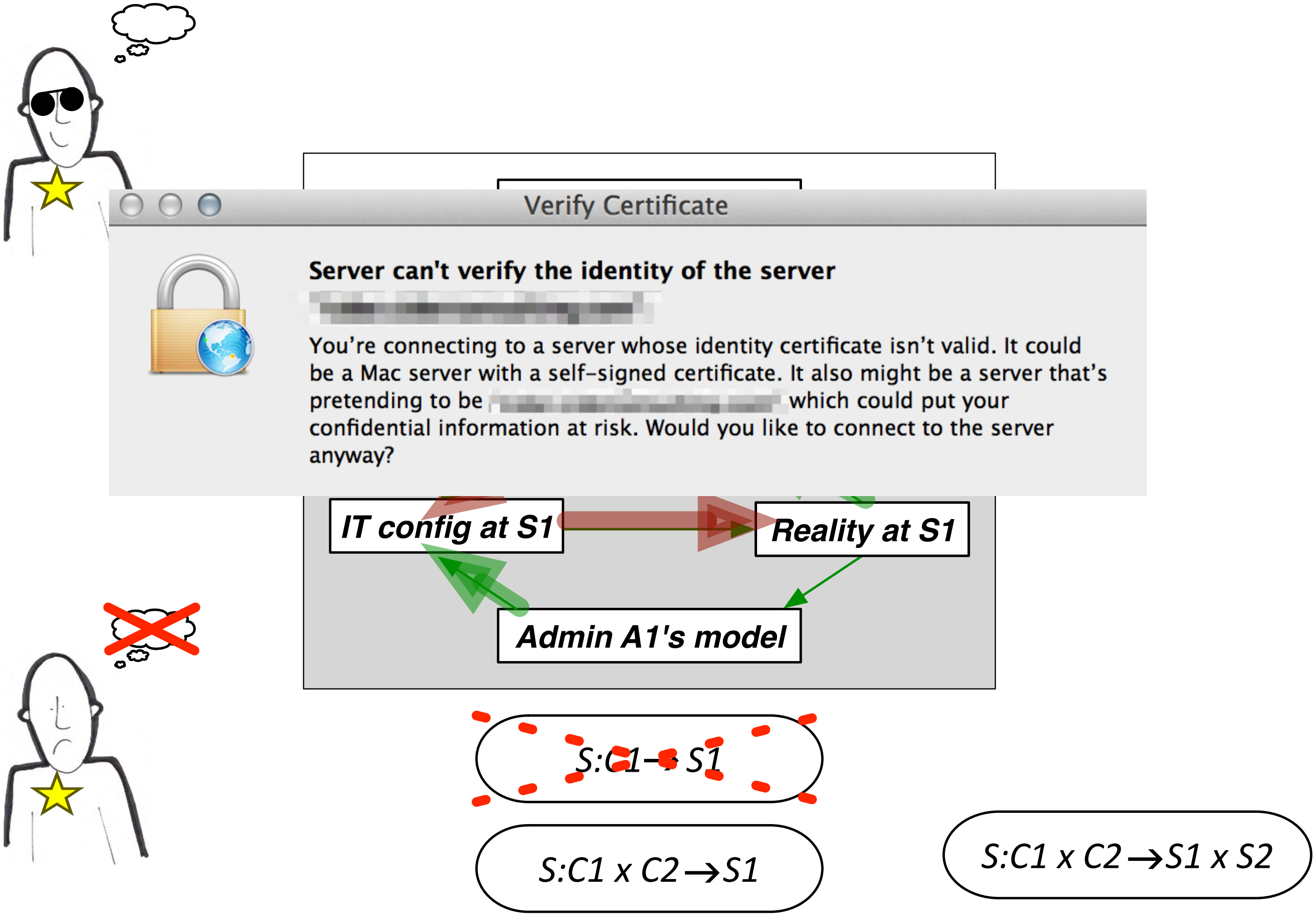


~~S:C1→S1~~

S:C1 x C2→S1

S:C1 x C2→S1 x S2

Trouble: Action at a Distance



Verify Certificate

Server can't verify the identity of the server

[redacted]

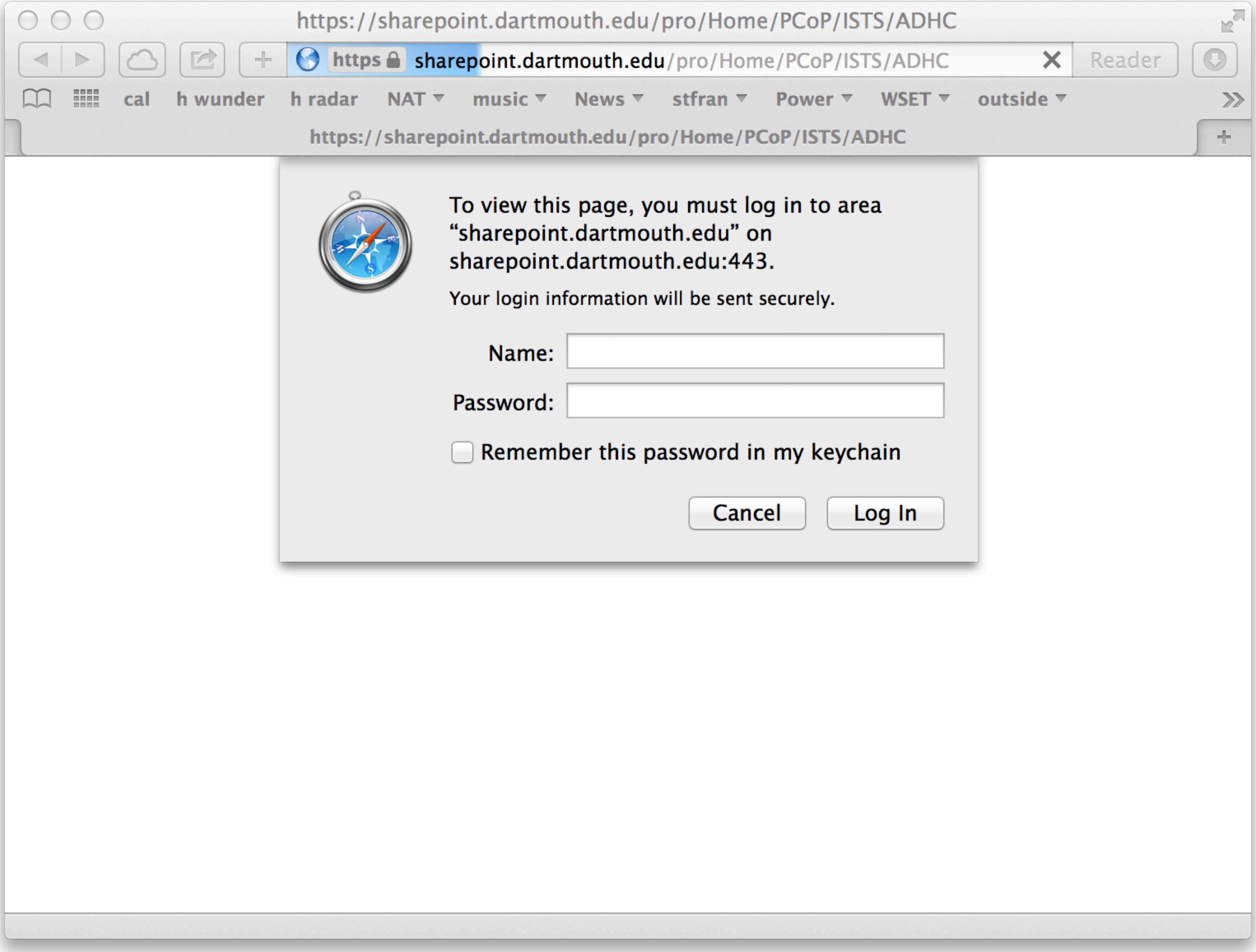
You're connecting to a server whose identity certificate isn't valid. It could be a Mac server with a self-signed certificate. It also might be a server that's pretending to be [redacted] which could put your confidential information at risk. Would you like to connect to the server anyway?

~~S:C1→S1~~

S:C1 x C2→S1

S:C1 x C2→S1 x S2

Trouble: Action at a Distance


https://sharepoint.dartmouth.edu/pro/Home/PCoP/ISTS/ADHC
https sharepoint.dartmouth.edu/pro/Home/PCoP/ISTS/ADHC
Reader
cal
h wunder
h radar
NAT
music
News
stfran
Power
WSET
outside
https://sharepoint.dartmouth.edu/pro/Home/PCoP/ISTS/ADHC

To view this page, you must log in to area "sharepoint.dartmouth.edu" on sharepoint.dartmouth.edu:443.

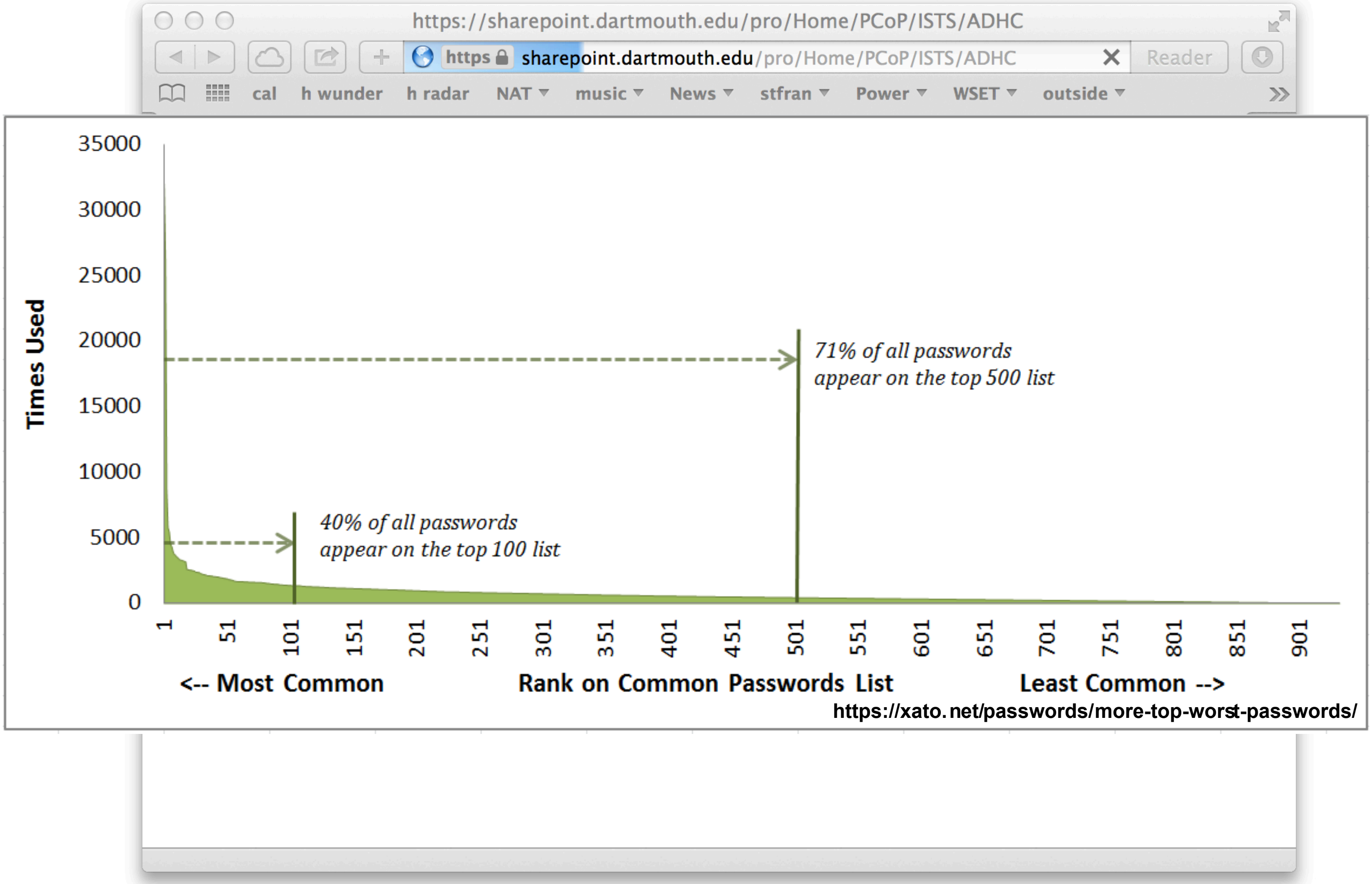
Your login information will be sent securely.

Name:

Password:

□ Remember this password in my keychain

Trouble: Action at a Distance



71% of all passwords appear on the top 500 list

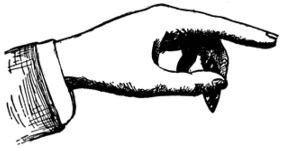
40% of all passwords appear on the top 100 list

https://xato.net/passwords/more-top-worst-passwords/

- 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***?

This Talk

1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security
6. Towards Understanding Policy Creation
7. Next Steps



Building Tools to Evaluate Aggregate Security *before* Deployment

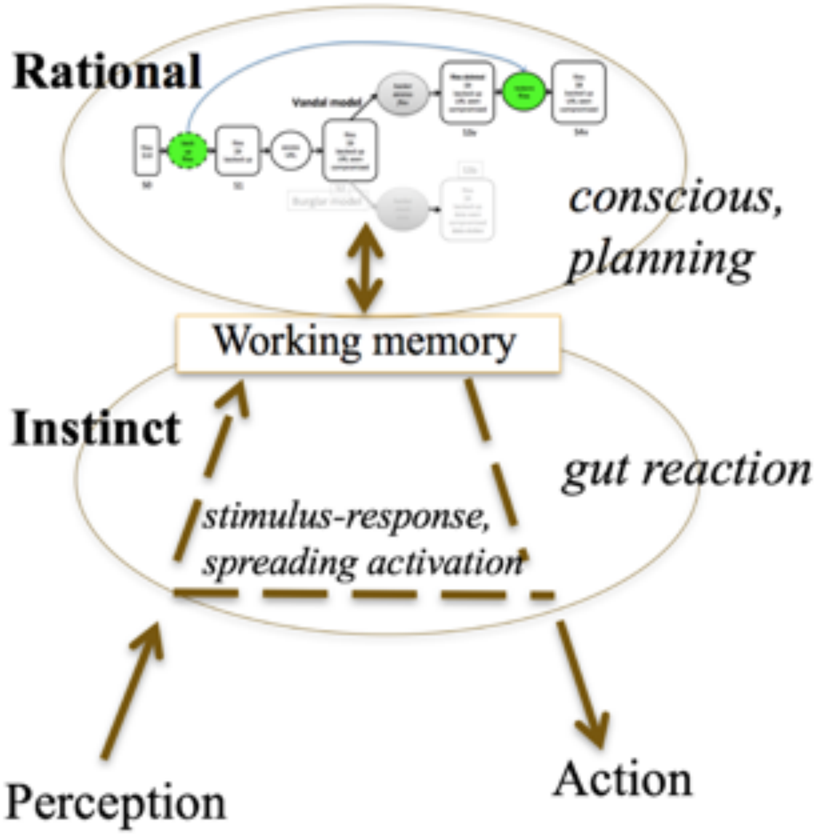
Once we know the likely behavior of individuals based on survey data and behavioral experimentation,

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



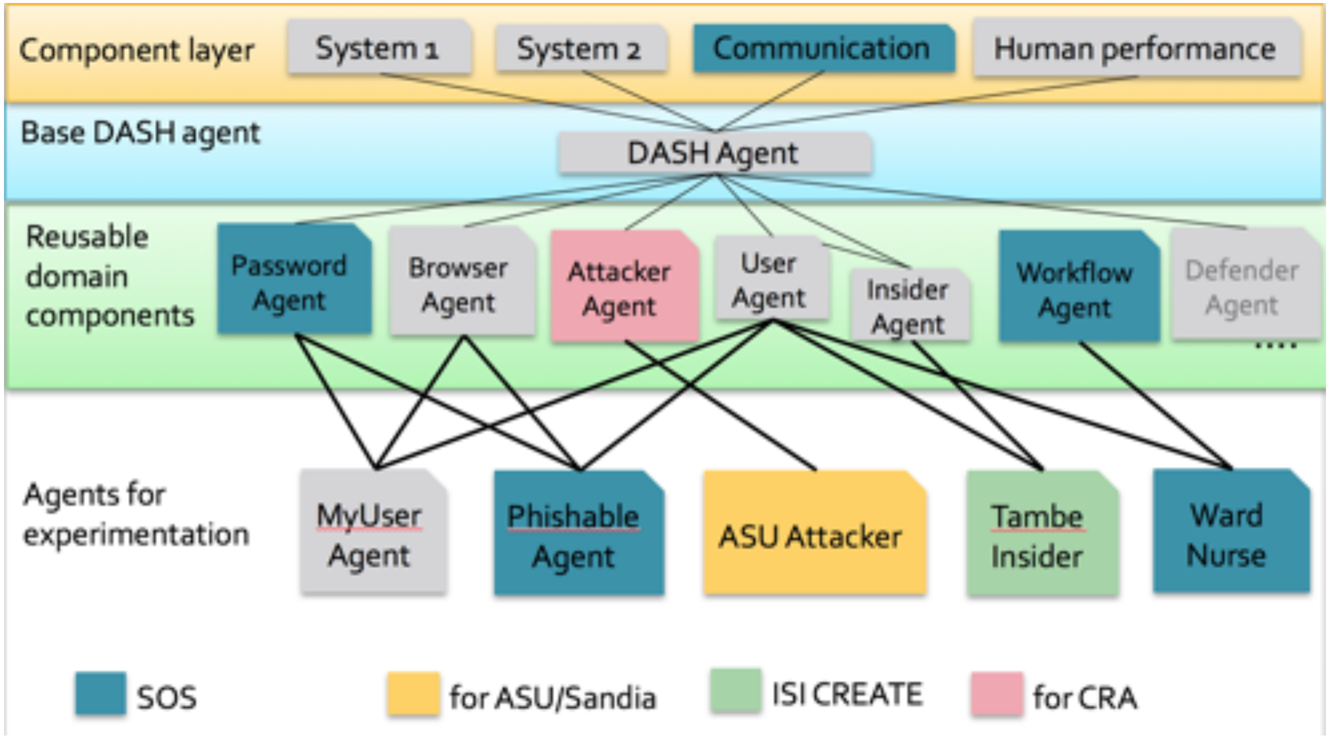
Dual process

Reactive planning

Mental models

Spreading activation

Designed for Speed, Reuse and Customization



Re-implemented in object-oriented Python

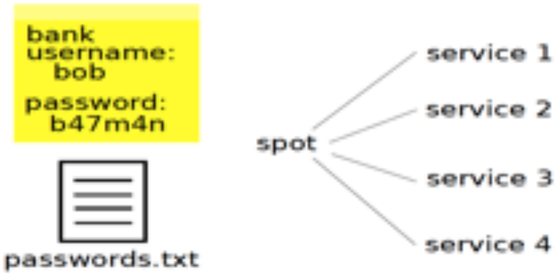
Have run millions of agents in DETER simulation

E.g. DASH Agent Models ("DASHwords")

Levenshtein measure of cognitive burden

Circumvention models from survey

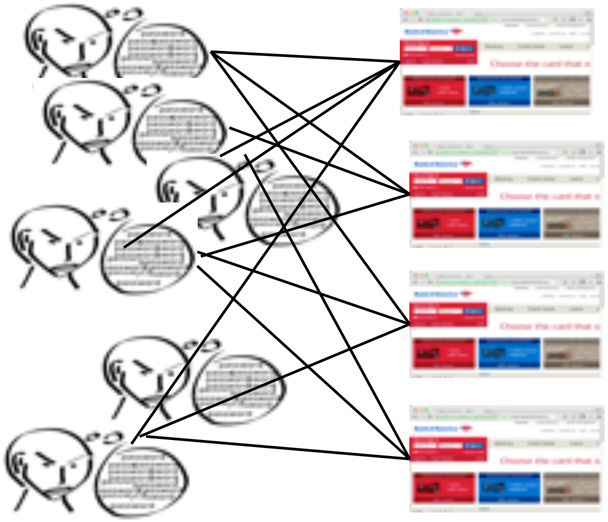
[Kothari et al. 15]

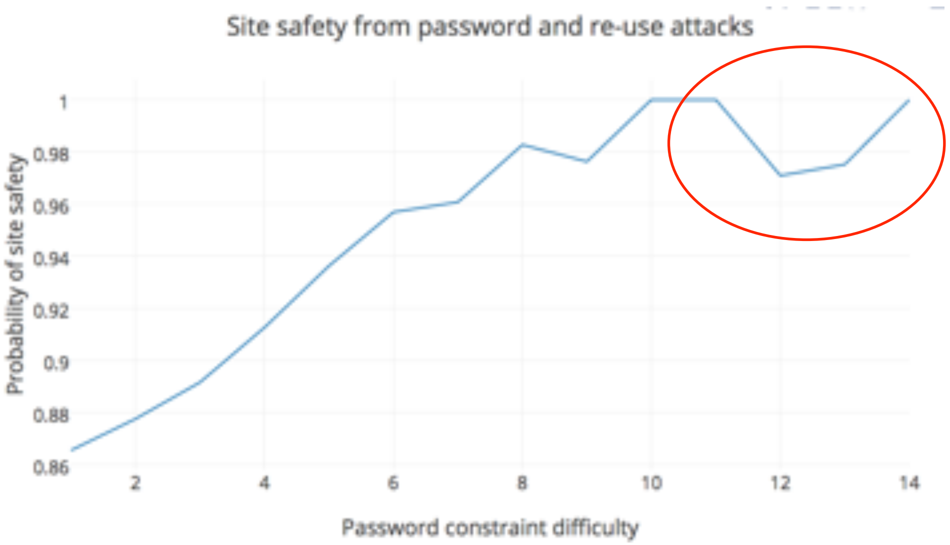


Direct + reuse measure of security

Demonstrates Uncanny Descent

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

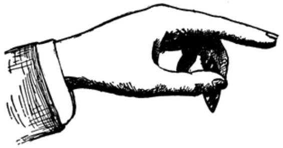



Site safety from password and re-use attacks
Probability of site safety
1
0.98
0.96
0.94
0.92
0.9
0.88
0.86
2
4
6
8
10
12
14
Password constraint difficulty

[Kothari et al. 15, 16]

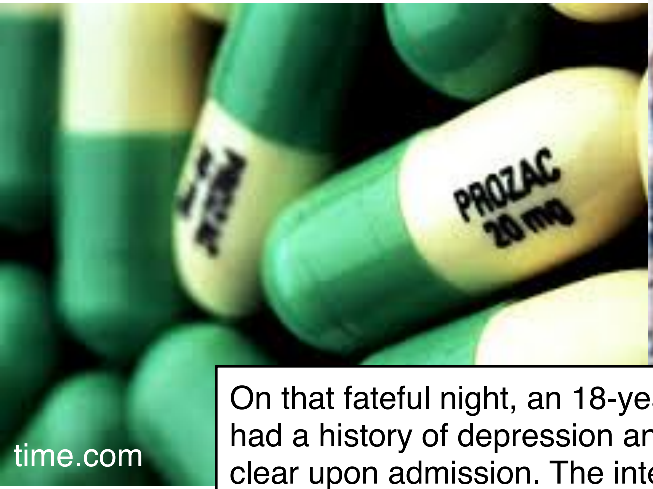
This Talk

1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security



6. Towards Understanding Policy Creation
7. Next Steps

The Problem of Expressing What We Want



time.com

buse.gov

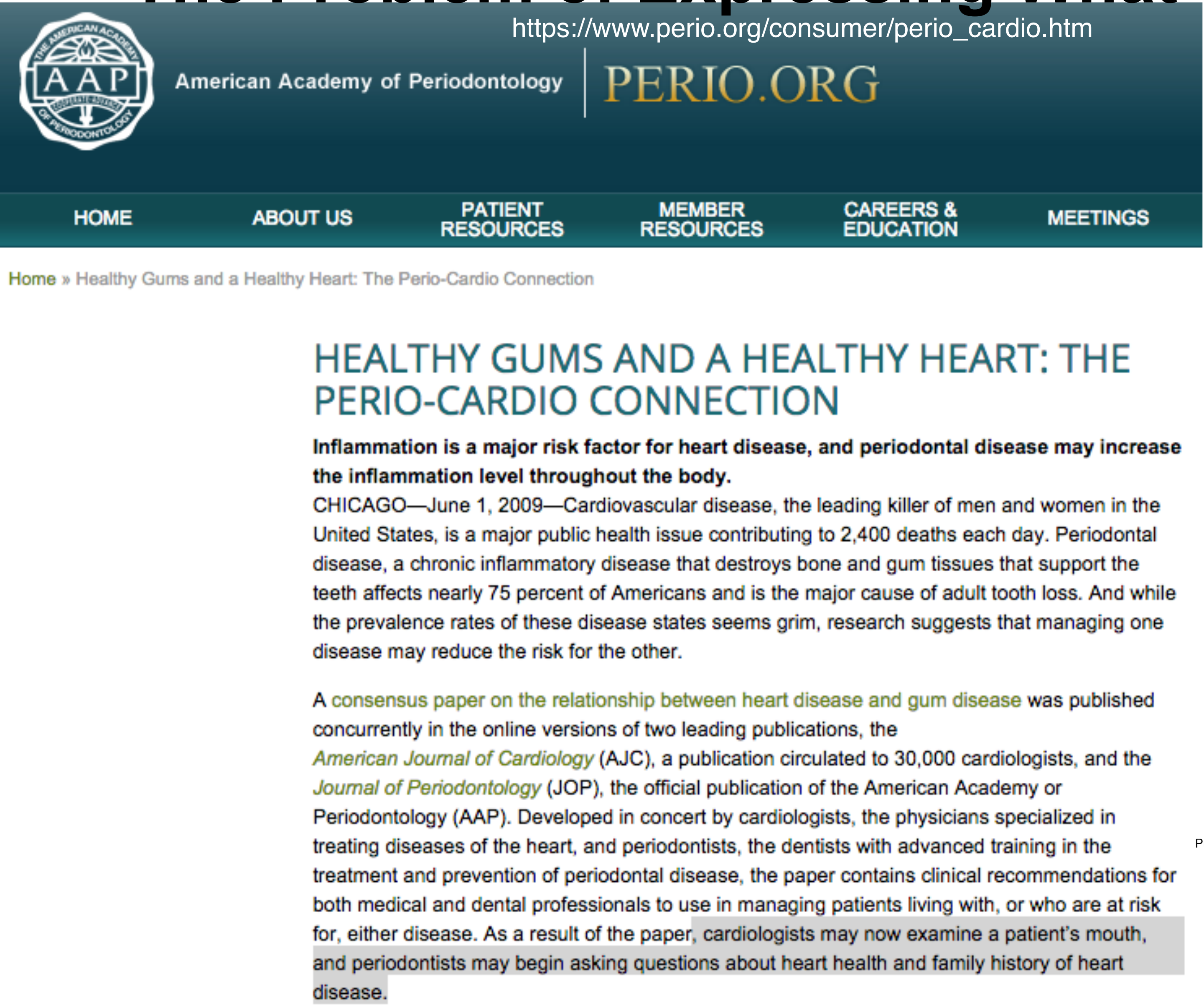
On that fateful night, an 18-year-old woman named Libby Zion was admitted to The New York Hospital. She had a history of depression and was taking a drug called Nardil, an MAO inhibitor. Her diagnosis was not clear upon admission. The intern and resident in charge of her care had been in contact with Ms. Zion's family physician. After admission, Libby Zion became more agitated. She was given the drug Demerol. Tragically, at that time, there was little information disseminated about a serious drug interaction between the antidepressant Nardil and the drug Demerol. As it turned out, this drug interaction proved deadly. After receiving Demerol, Miss Zion's temperature climbed to 107 degrees, she had a cardiac arrest and she died.

http://www.conciergemedicinemd.com/blog/2013/11/07/october-4-1984-libby-zion-the-day-medicine-changed-forever/

http://www.nybooks.com/articles/archives/1996/feb/29/what-doctors-dont-tell-us/

The Problem of Expressing What We Want

https://www.perio.org/consumer/perio_cardio.htm


American Academy of Periodontology
PERIO.ORG
HOME
ABOUT US
PATIENT RESOURCES
MEMBER RESOURCES
CAREERS & EDUCATION
MEETINGS
Home » Healthy Gums and a Healthy Heart: The Perio-Cardio Connection

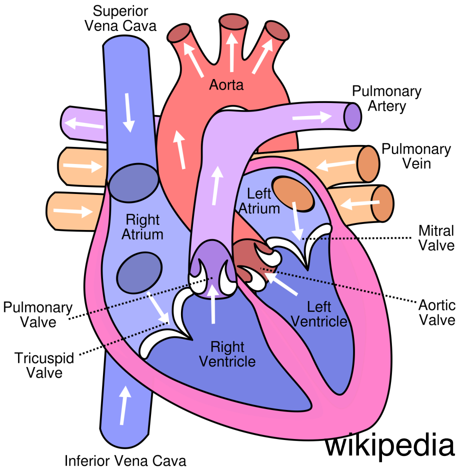
HEALTHY GUMS AND A HEALTHY HEART: THE PERIO-CARDIO CONNECTION

Inflammation is a major risk factor for heart disease, and periodontal disease may increase the inflammation level throughout the body.

CHICAGO—June 1, 2009—Cardiovascular disease, the leading killer of men and women in the United States, is a major public health issue contributing to 2,400 deaths each day. Periodontal disease, a chronic inflammatory disease that destroys bone and gum tissues that support the teeth affects nearly 75 percent of Americans and is the major cause of adult tooth loss. And while the prevalence rates of these disease states seems grim, research suggests that managing one disease may reduce the risk for the other.

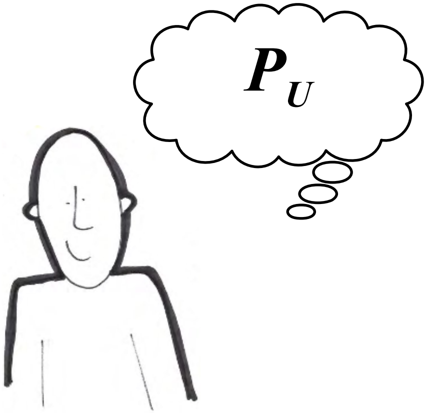
A consensus paper on the relationship between heart disease and gum disease was published concurrently in the online versions of two leading publications, the *American Journal of Cardiology* (AJC), a publication circulated to 30,000 cardiologists, and the *Journal of Periodontology* (JOP), the official publication of the American Academy or Periodontology (AAP). Developed in concert by cardiologists, the physicians specialized in treating diseases of the heart, and periodontists, the dentists with advanced training in the treatment and prevention of periodontal disease, the paper contains clinical recommendations for both medical and dental professionals to use in managing patients living with, or who are at risk for, either disease. As a result of the paper, cardiologists may now examine a patient's mouth, and periodontists may begin asking questions about heart health and family history of heart disease.

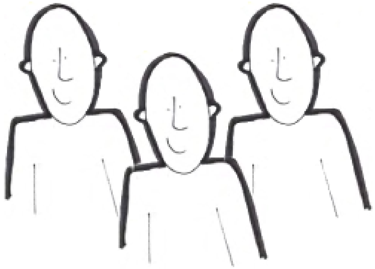
colgateprofessional.com

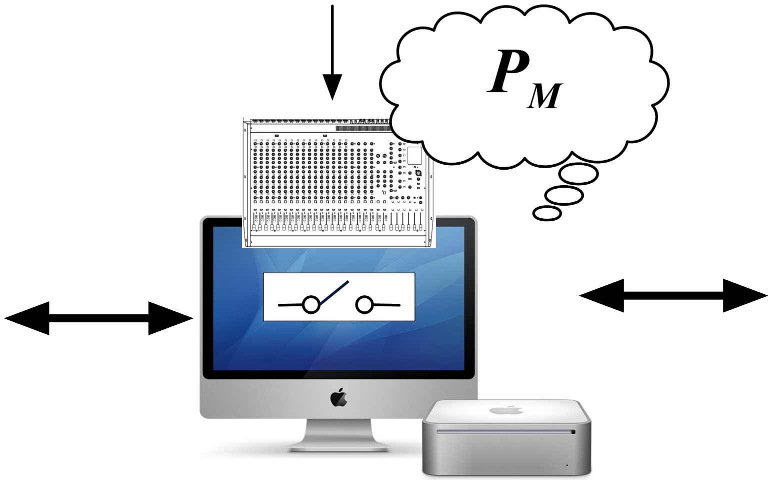


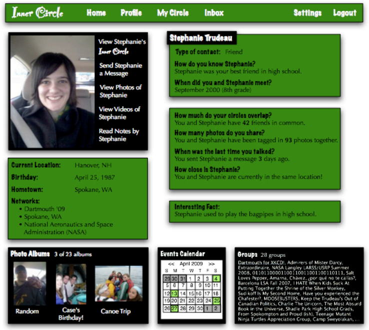
wikipedia

How do we protect users from dangerous privacy spills?









Inner Circle Home Profile My Circle Inbox Settings Logout

View Stephanie's Inner Circle
Send Stephanie a Message
View Photos of Stephanie
View Videos of Stephanie
Read Notes by Stephanie

Current Location: Hanover, NH
Birthday: April 25, 1987
Hometown: Spokane, WA
Networks:

- Dartmouth '09
- Spokane, WA
- National Aeronautics and Space Administration (NASA)

Stephanie Trudeau

Type of contact: Friend

How do you know Stephanie?
Stephanie was your best friend in high school.

When did you and Stephanie meet?
September 2000 (8th grade)

How much do your circles overlap?
You and Stephanie have 42 friends in common.

How many photos do you share?
You and Stephanie have been tagged in 93 photos together.

When was the last time you talked?
You sent Stephanie a message 3 days ago.

How close is Stephanie?
You and Stephanie are currently in the same location!

Interesting Fact:
Stephanie used to play the bagpipes in high school.

Photo Albums 3 of 23 albums
Random Case's Birthday! Canoe Trip

Events Calendar
<< April 2009 >>

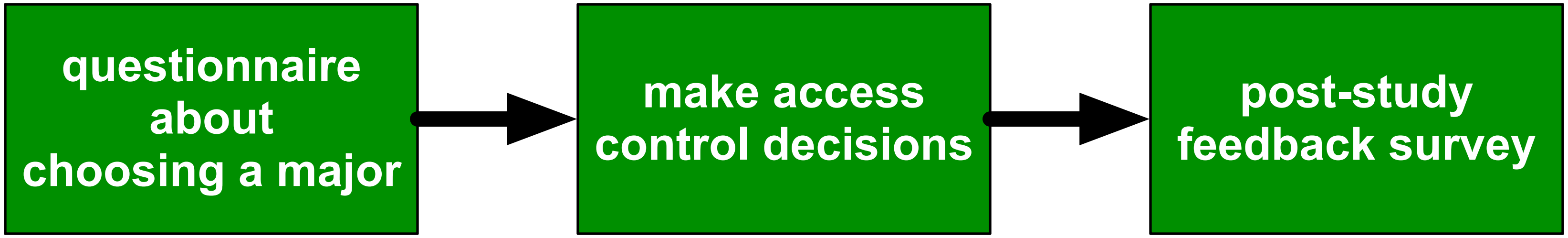
S	M	T	W	T	F	S
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2

Groups 28 groups
Dartmouth for XKCD!, Admirers of Mister Darcy, Extraordinaire, NASA Langley LARSS/USRP Summer 2008, 0110110000110011001100110011011, Salt Loves Pepper, Amarna, Chávez, ¿por qué no te callas?, Barcelona LSA Fall 2007, I HATE When Kids Suck At Putting Together the Shrine of the Silver Monkey, Sudikoff Is My Second Home, Have you experienced the Chafester?, MOOSEBUSTERS, Keep the Trudeau's Out of Canadian Politics, Charlie The Unicorn, The Most Absurd Book in the Universe, Shadle Park High School Grads, From Spokompton and Proud (ish), Teenage Mutant Ninja Turtles Appreciation Group, Camp Sweyolakan, ...

WPES

Methodology

Control group:

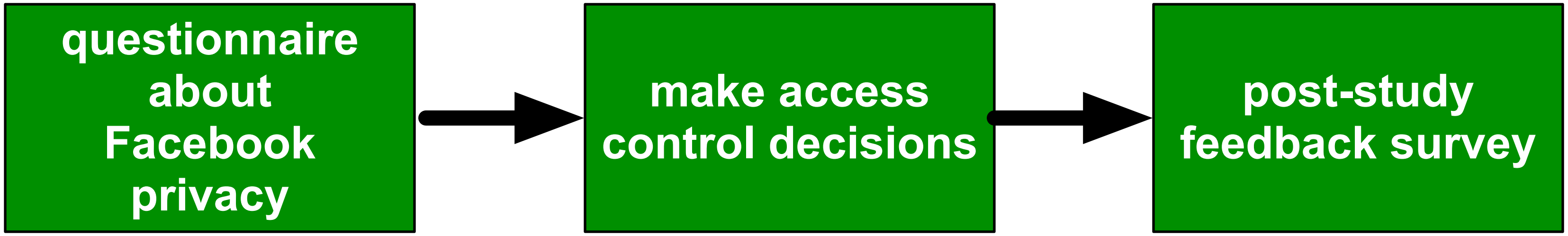


questionnaire about choosing a major

make access control decisions

post-study feedback survey

Introspective group:



questionnaire about Facebook privacy

make access control decisions

post-study feedback survey

Results

Implication: If you want to protect users from privacy spills, then

- ***educating*** users about privacy issues
- letting them configure their own ***policies***

will make things ***worse!***

Post-study feedback:

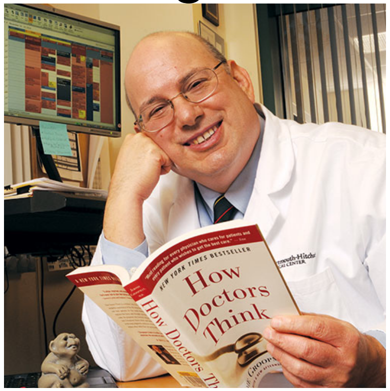
- In the control group, many wanted to go to Facebook and constrain their settings
- In the introspect group, many said they already had fine settings; many said they were ***more*** constrained in InnerCircle than Facebook
- Many in the introspect group felt *"if X is a friend, then I guess I'll share everything."* ***NO ONE*** in the control group said that.
- Many in both groups liked InnerCircle better than Facebook

Access Control Hygiene and the Empathy Gap in Medical IT

Yifei Wang

HealthSec

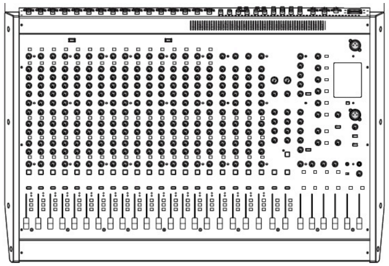
Andrew Gettinger, MD



The Experiment

abstract,
looking at policy GUI

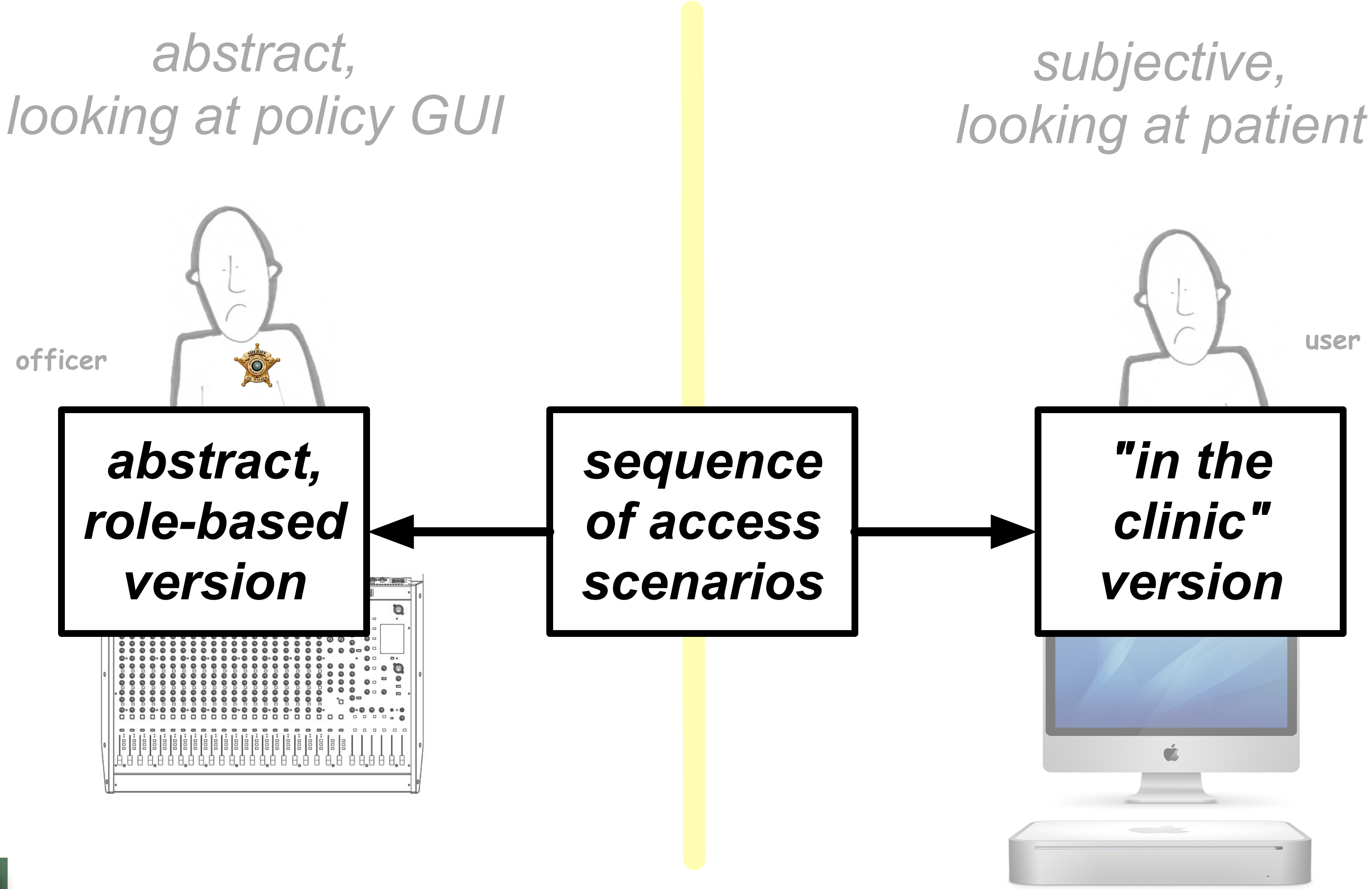
officer



subjective,
looking at patient

user

The Experiment



abstract,
looking at policy GUI

subjective,
looking at patient

abstract, role-based version

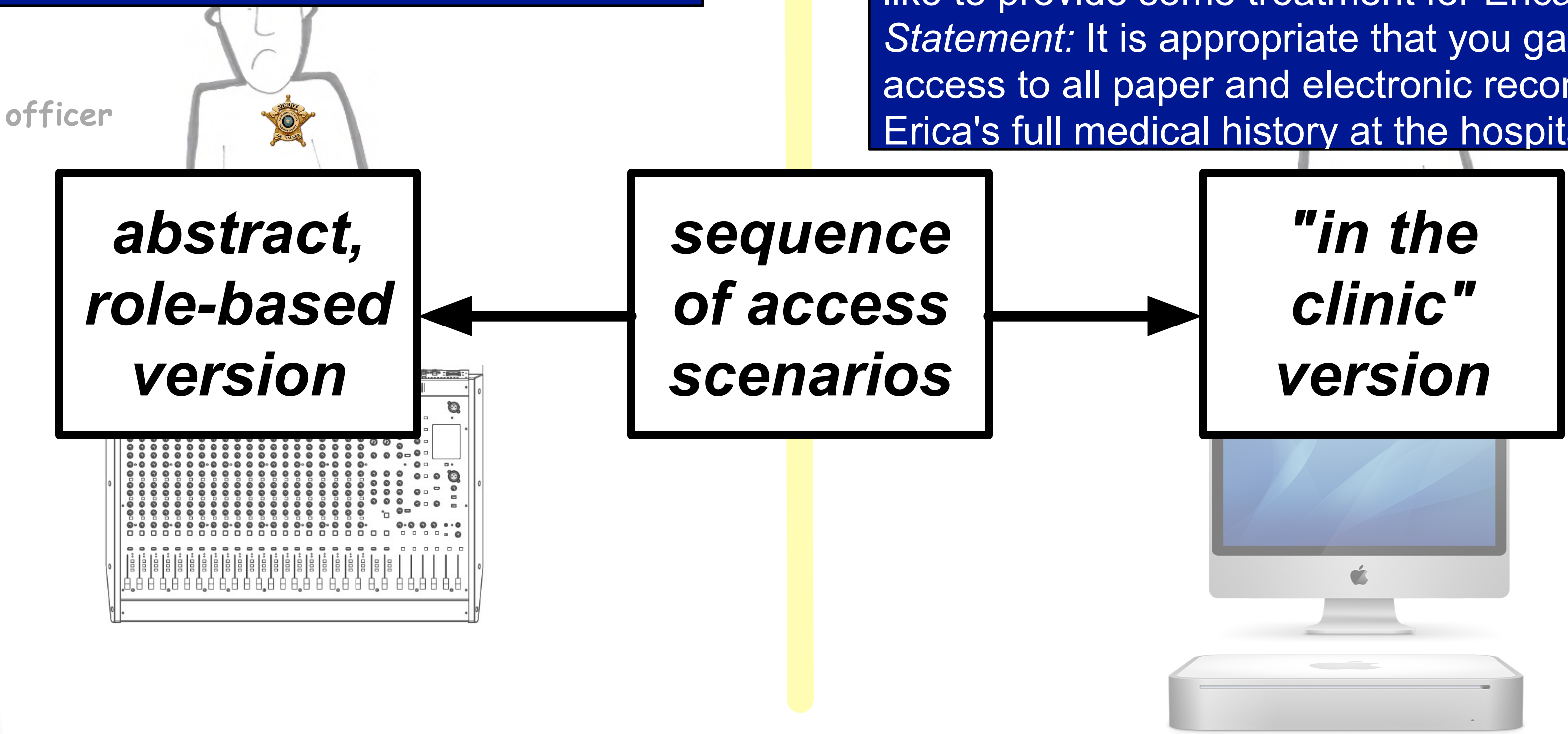
sequence of access scenarios

"in the clinic" version

The Experiment

C1: It is appropriate that the hospital privacy policy gives local addiction treatment programs full access to a patient's medical record if the patient is diagnosed with serious alcohol abuse.

E1: *Patient Condition:* Erica Brown is a patient diagnosed with serious alcohol abuse and was sent to the local addiction treatment program. *Your Position/Relationship with the Patient*: You are a physician who works at the local addiction treatment program. Erica was sent to you from the hospital. You would like to provide some treatment for Erica. *Statement:* It is appropriate that you gain access to all paper and electronic records of Erica's full medical history at the hospital.

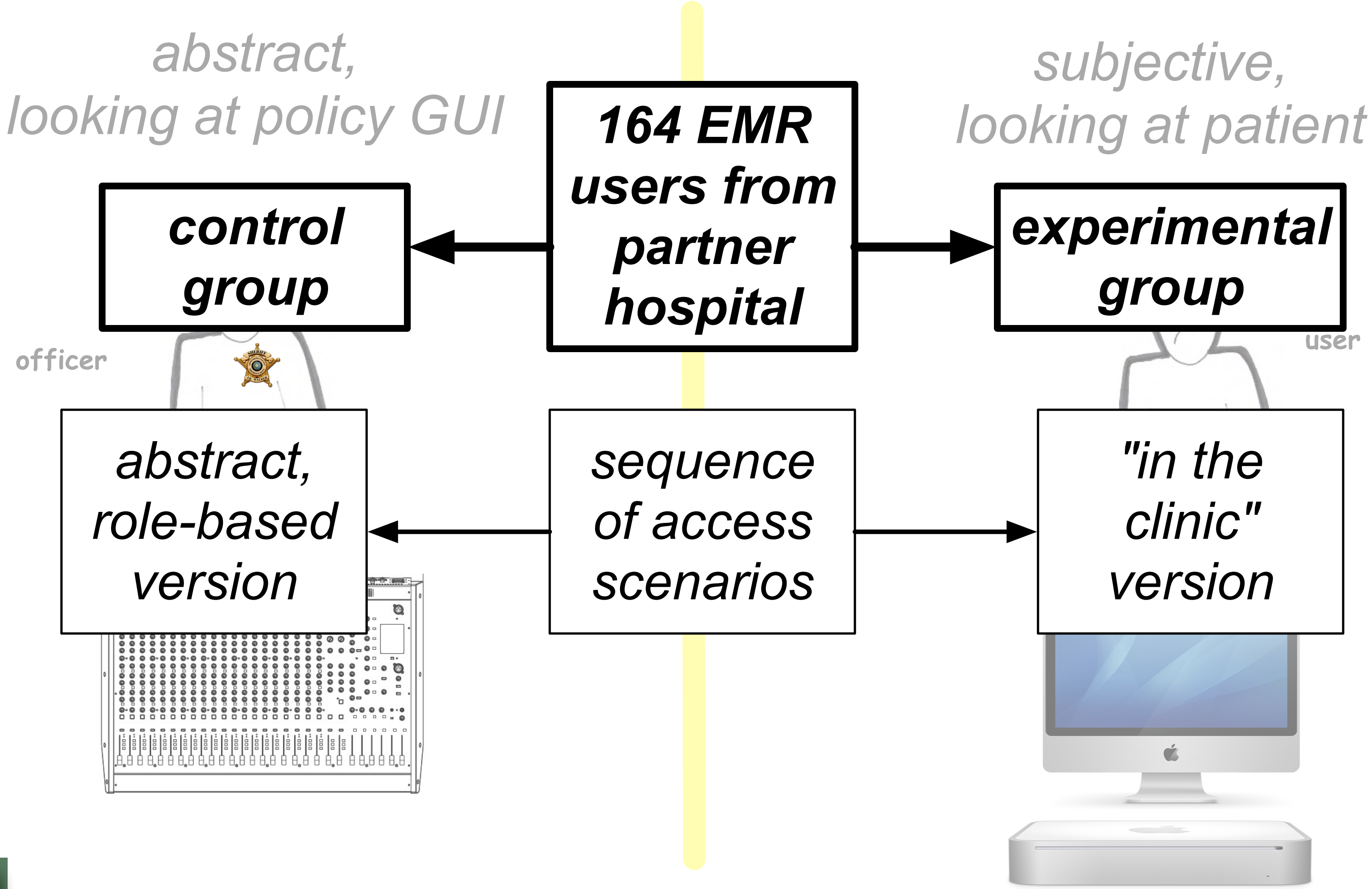


abstract, role-based version

sequence of access scenarios

"in the clinic" version

The Experiment



abstract, looking at policy GUI

subjective, looking at patient

164 EMR users from partner hospital

control group

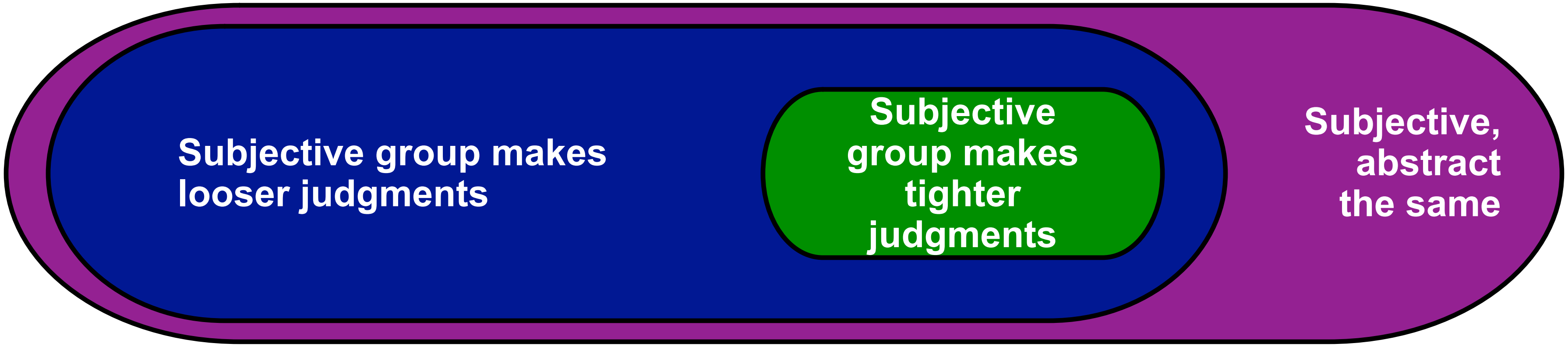
experimental group

abstract, role-based version

sequence of access scenarios

"in the clinic" version

Results

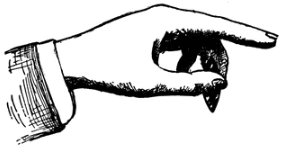

Subjective group makes looser judgments
Subjective group makes tighter judgments
Subjective, abstract the same

- Reasonable EMR users will make policy decisions that reasonable EMR users will find unduly constraining
  - (sometimes)

- Simply including EMR users in the policy creation process is not sufficient.

This Talk

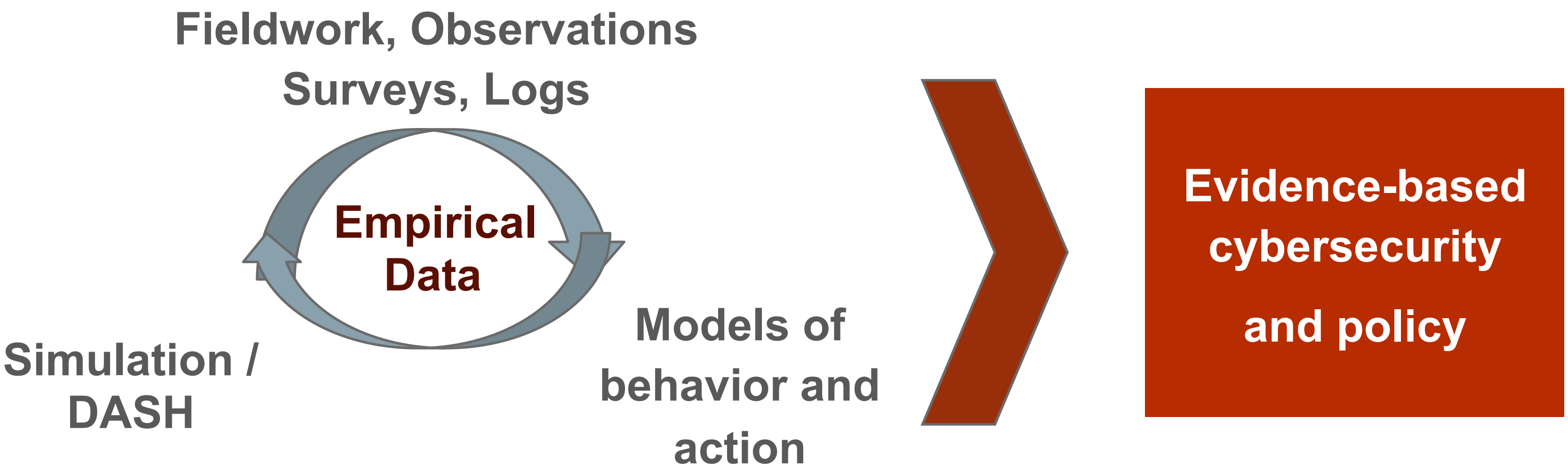
1. The Problem
2. How We Approach It
3. Fieldwork and Observation
4. Analysis
5. Towards Understanding Aggregate Security
6. Towards Understanding Policy Creation
7. Next Steps



Next Steps

- Improve simulations based on new data
- Automatic reasoning about the link between data and simulation (*FARM: Find the Appropriate level of Realism for Modeling*)
- 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?

Thanks!



Fieldwork, Observations
Surveys, Logs

Empirical
Data

Simulation /
DASH

Models of
behavior and
action

Evidence-based
cybersecurity
and policy

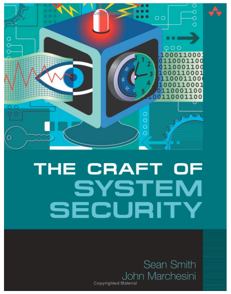
O'REILLY

Sean Smith

The Internet of Risky Things

Trusting the Devices
that Surround Us

sws@cs.dartmouth.edu
www.cs.dartmouth.edu/~sws/



THE CRAFT OF
SYSTEM
SECURITY

Sean Smith
John Marchesini