Understanding and Accounting for Human Behavior

Jim Blythe
USC ISI
blythe@isi.edu

Information Sciences Institute
USC Viterbi School of Engineering

Sean Smith
Dartmouth
sws@cs.dartmouth.edu

Dartmouth College
INSTITUTE for SECURITY, TECHNOLOGY, and SOCIETY

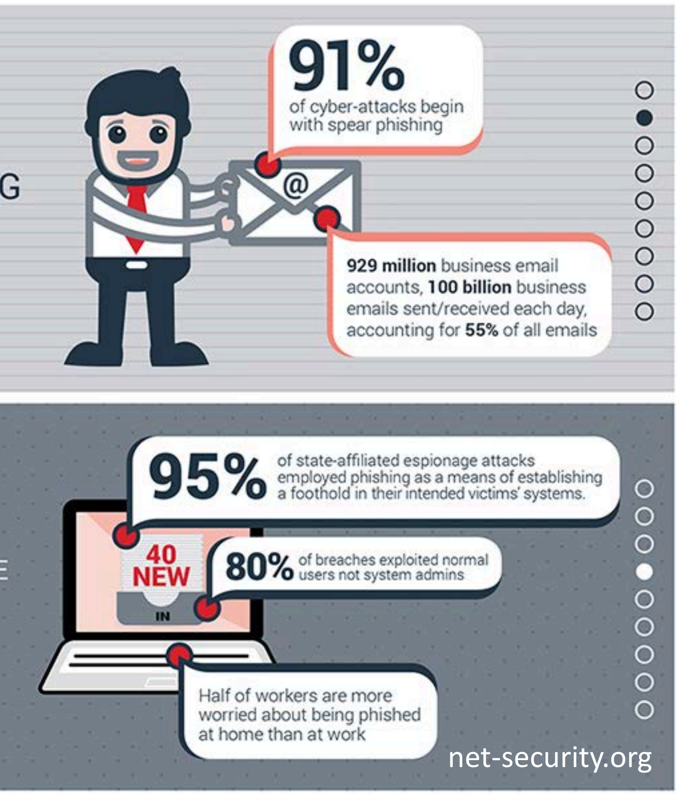
April 21, 2015

This Talk

- The Problem
- Quick mentions
  - Ethnography and security
  - Economics and security
  - HCISEC
  - Law and regulation
- Deeper dives:
  - Cognitive bias and security
  - Mental models and security
  - Semiotics and usability and security
  - Simulation

Problem

Human Behavior



91% of cyber-attacks begin with spear phishing

929 million business email accounts, 100 billion business emails sent/received each day, accounting for 55% of all emails

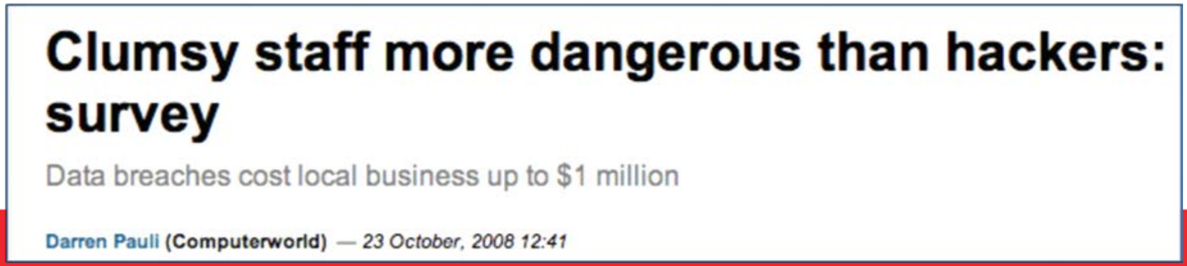
95% of state-affiliated espionage attacks employed phishing as a means of establishing a foothold in their intended victims' systems.

80% of breaches exploited normal users not system admins

Half of workers are more worried about being phished at home than at work

net-security.org

- Most attacks rely on human behavior
- Inadvertent insiders equally dangerous
- A long-time blind spot in security research



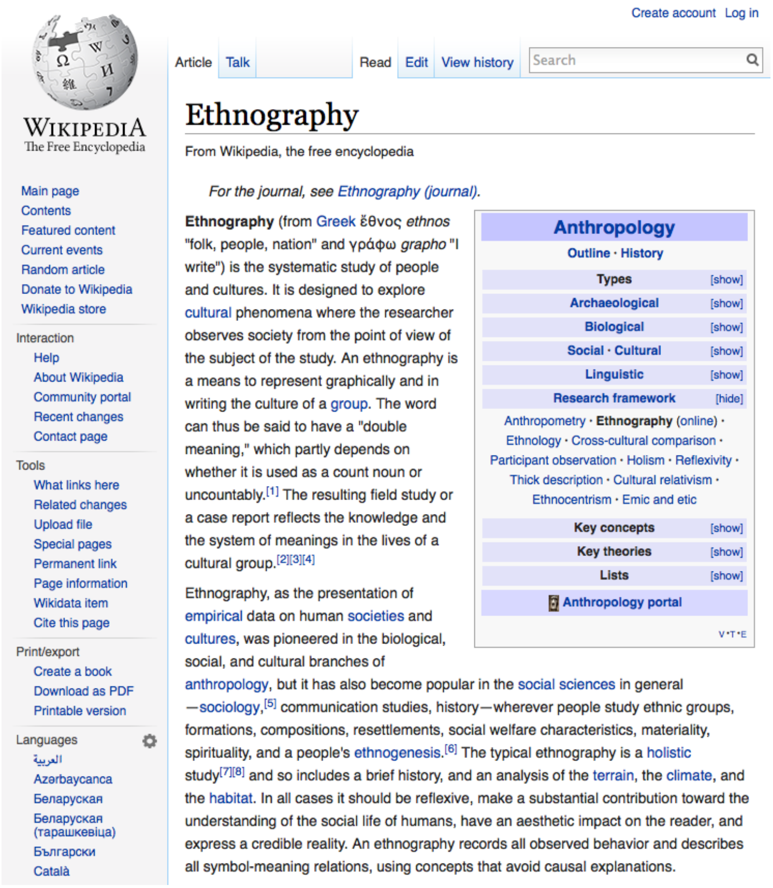
Clumsy staff more dangerous than hackers: survey

Data breaches cost local business up to $1 million

Darren Pauli (Computerworld) — *23 October, 2008 12:41*

Observing Humans

Ethnographic Methods



Ethnography

From Wikipedia, the free encyclopedia

For the journal, see Ethnography (journal).

Anthropology

Outline · History

Types	[show]
Archaeological	[show]
Biological	[show]
Social · Cultural	[show]
Linguistic	[show]
Research framework	[hide]

Anthropometry · **Ethnography** (online) · Ethnology · Cross-cultural comparison · Participant observation · Holism · Reflexivity · Thick description · Cultural relativism · Ethnocentrism · Emic and etic

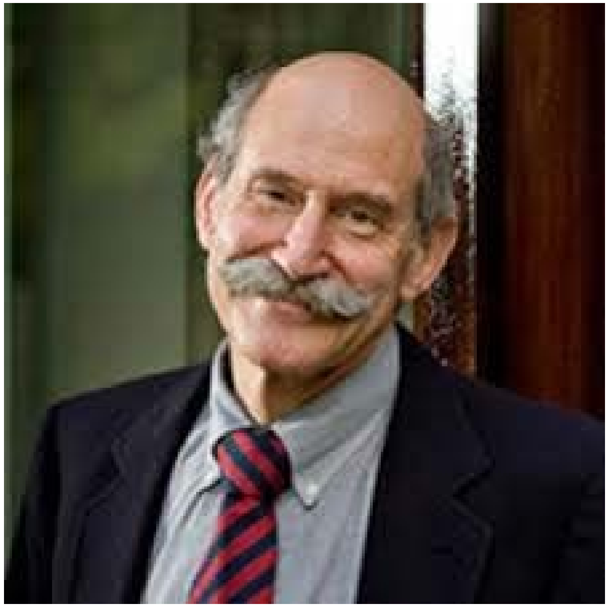
Key concepts	[show]
Key theories	[show]
Lists	[show]

Anthropology portal

V·T·E

Ethnography (from Greek ἔθνος *ethnos* "folk, people, nation" and γράφω *grapho* "I write") is the systematic study of people and cultures. It is designed to explore cultural phenomena where the researcher observes society from the point of view of the subject of the study. An ethnography is a means to represent graphically and in writing the culture of a group. The word can thus be said to have a "double meaning," which partly depends on whether it is used as a count noun or uncountably.[1] The resulting field study or a case report reflects the knowledge and the system of meanings in the lives of a cultural group.[2][3][4]

Ethnography, as the presentation of empirical data on human societies and cultures, was pioneered in the biological, social, and cultural branches of anthropology, but it has also become popular in the social sciences in general—sociology,[5] communication studies, history—wherever people study ethnic groups, formations, compositions, resettlements, social welfare characteristics, materiality, spirituality, and a people's ethnogenesis.[6] The typical ethnography is a holistic study[7][8] and so includes a brief history, and an analysis of the terrain, the climate, and the habitat. In all cases it should be reflexive, make a substantial contribution toward the understanding of the social life of humans, have an aesthetic impact on the reader, and express a credible reality. An ethnography records all observed behavior and describes all symbol-meaning relations, using concepts that avoid causal explanations.



Penn
UNIVERSITY of PENNSYLVANIA

Why ethnographic methods? (1)

- People don’t use computers the way people who design software think people use computers
- Especially true for cyber security and computer access
- Many “Illegal” actions taught as part of training
- Many unseen and unknown
- Affects: us, personal data, security

Why ethnographic methods? (2)

- Workarounds pandemic
- Failure to see work in practice
- Failure to Search….Independence helps
- Self report/Self examination unreliable. Why?
- Every change anywhere means….
- Failure to design….

Humans as Agents

Some approaches

- WEIS, SOUPS, USEC….

- Another idea: tune human behavior via the legal process
- Challenges
  - which branch?
    - Legislative:
      - can’t move quickly, questionable expertise
    - Executive:
      - not democratic
    - Judicial:
      - often bad track record in US
      - “Software on the Witness Stand”
  - jurisdiction overlaps and conflicts
- Cautionary tales
  - The crypto export wars
  - Lucifer -> DES
  - Orange Book
- Success story
  - AES

Cognitive Bias

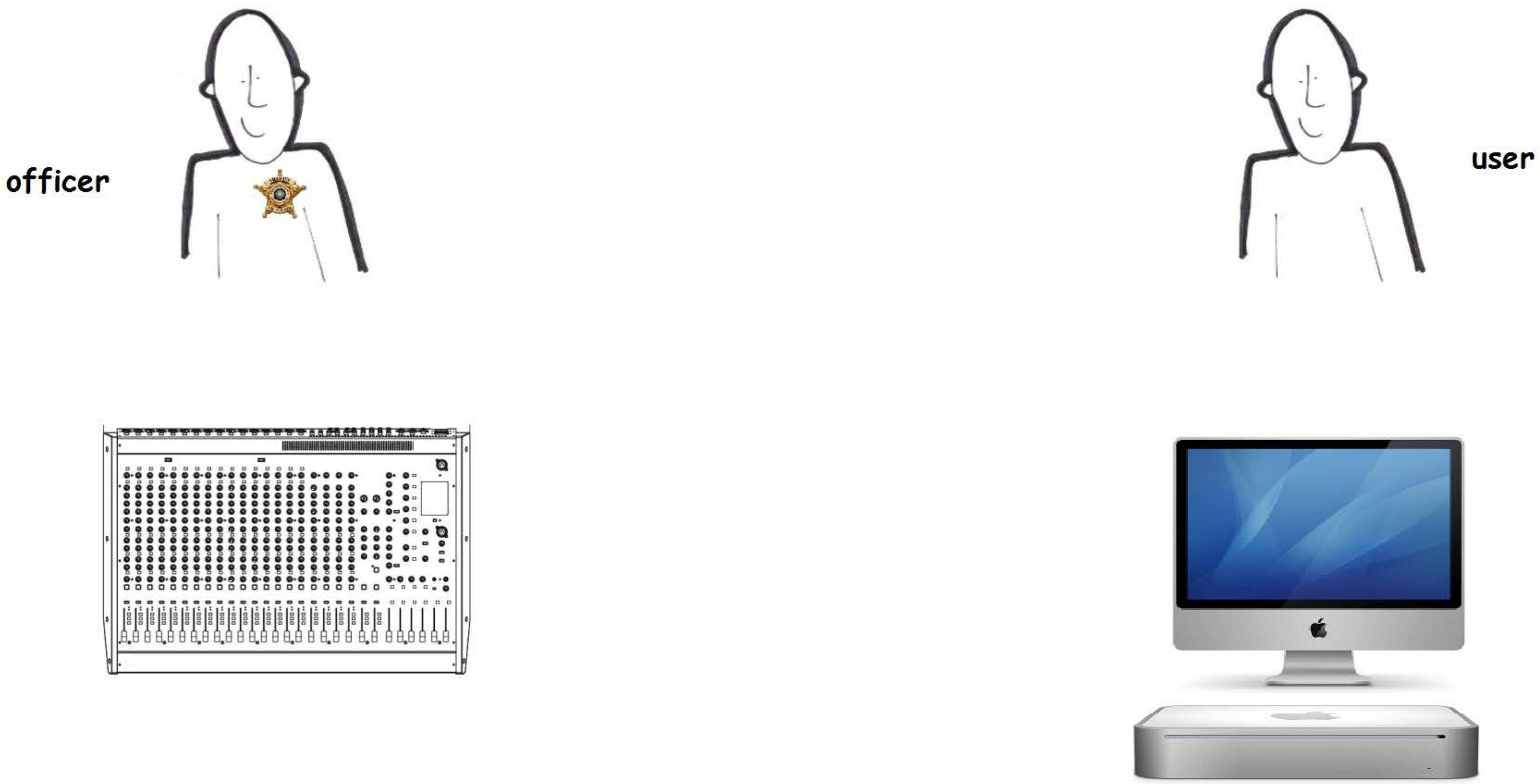
Cognitive Bias and Security

- 1. Annoyingly Hard Problems
- 2. Secret Weapon
- 3. Some Initial Results
- 4. New Places to Try It

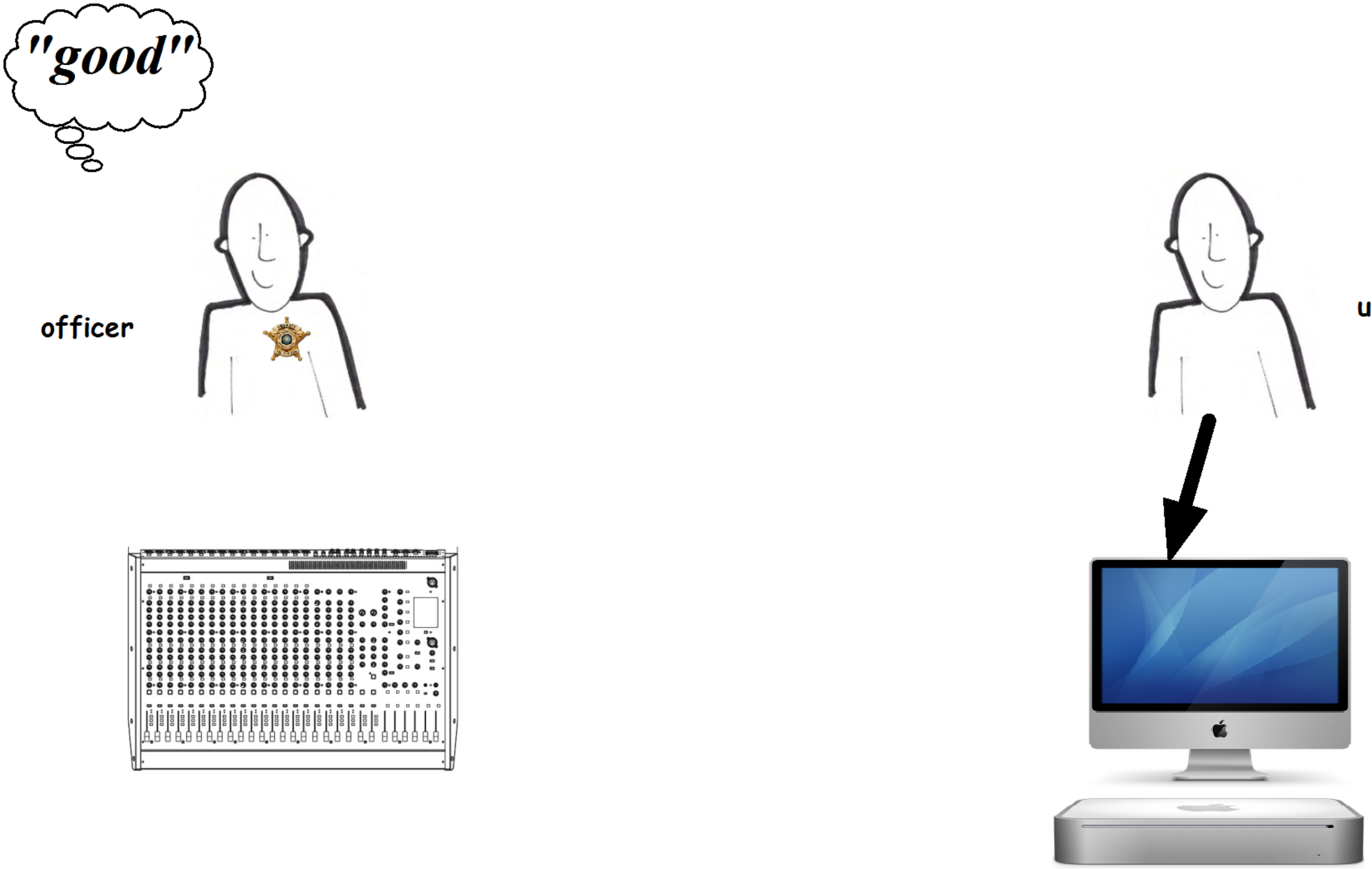
Cognitive Bias and Security

1. Annoyingly Hard Problems

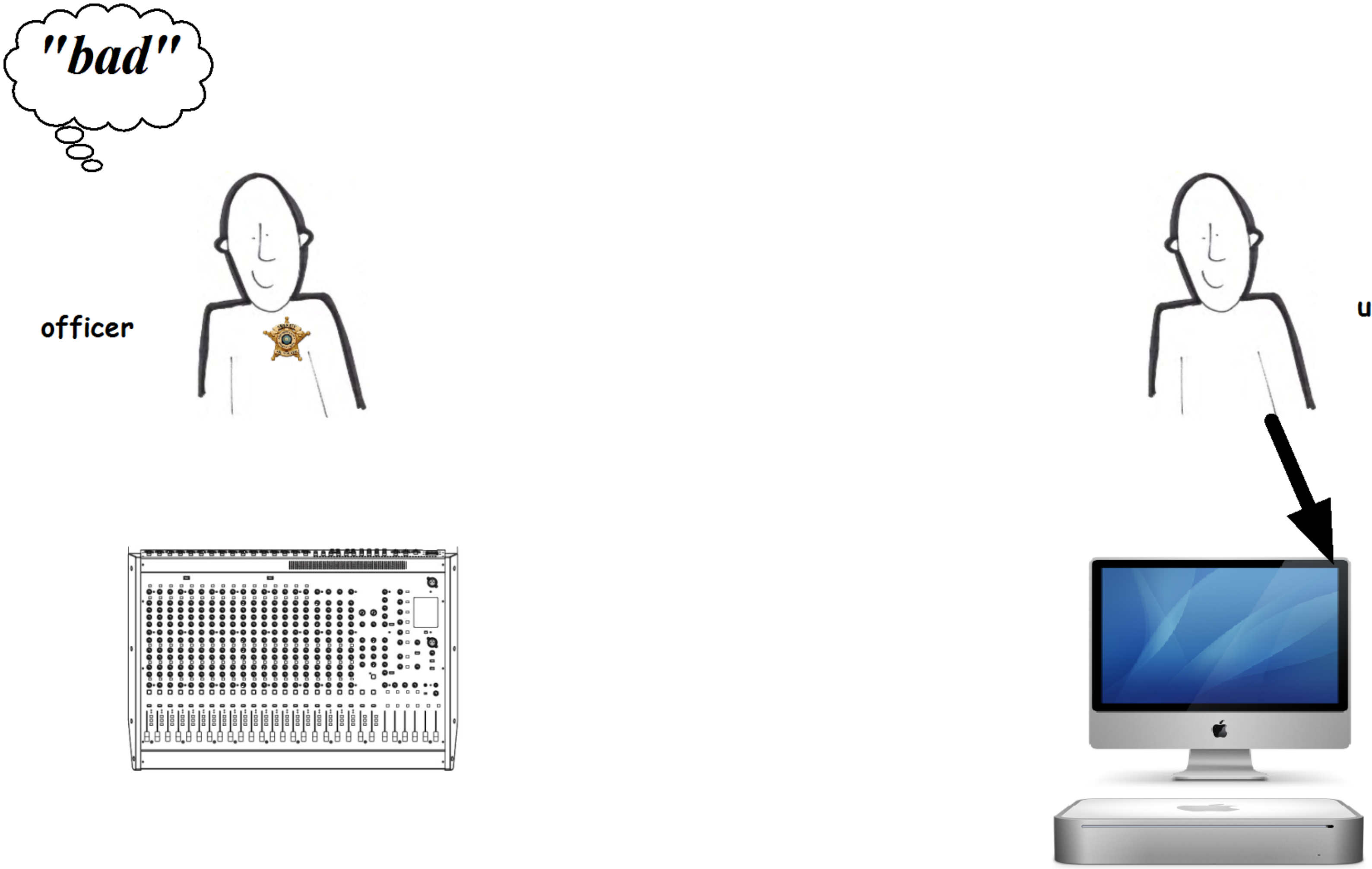
Access Control



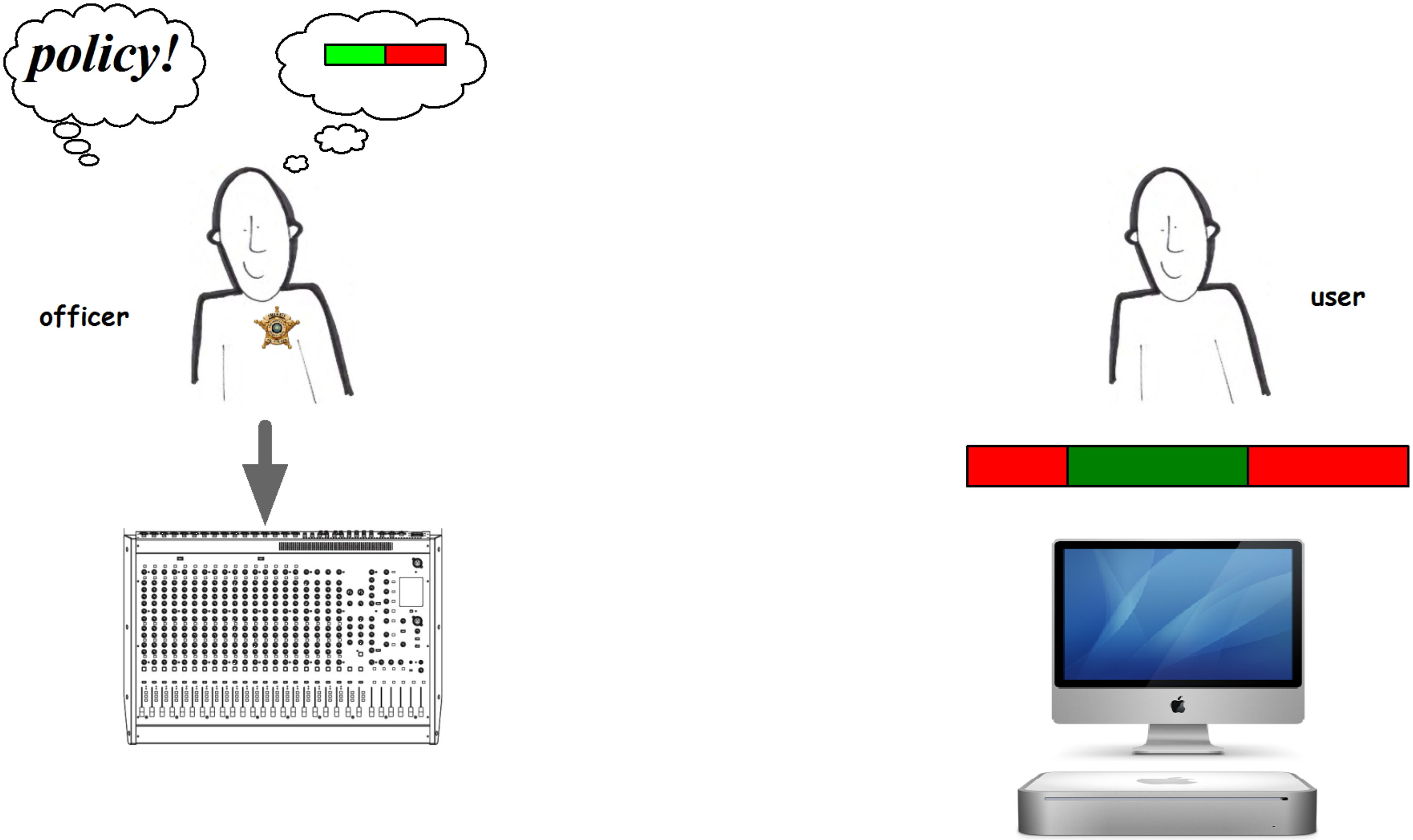
Access Control



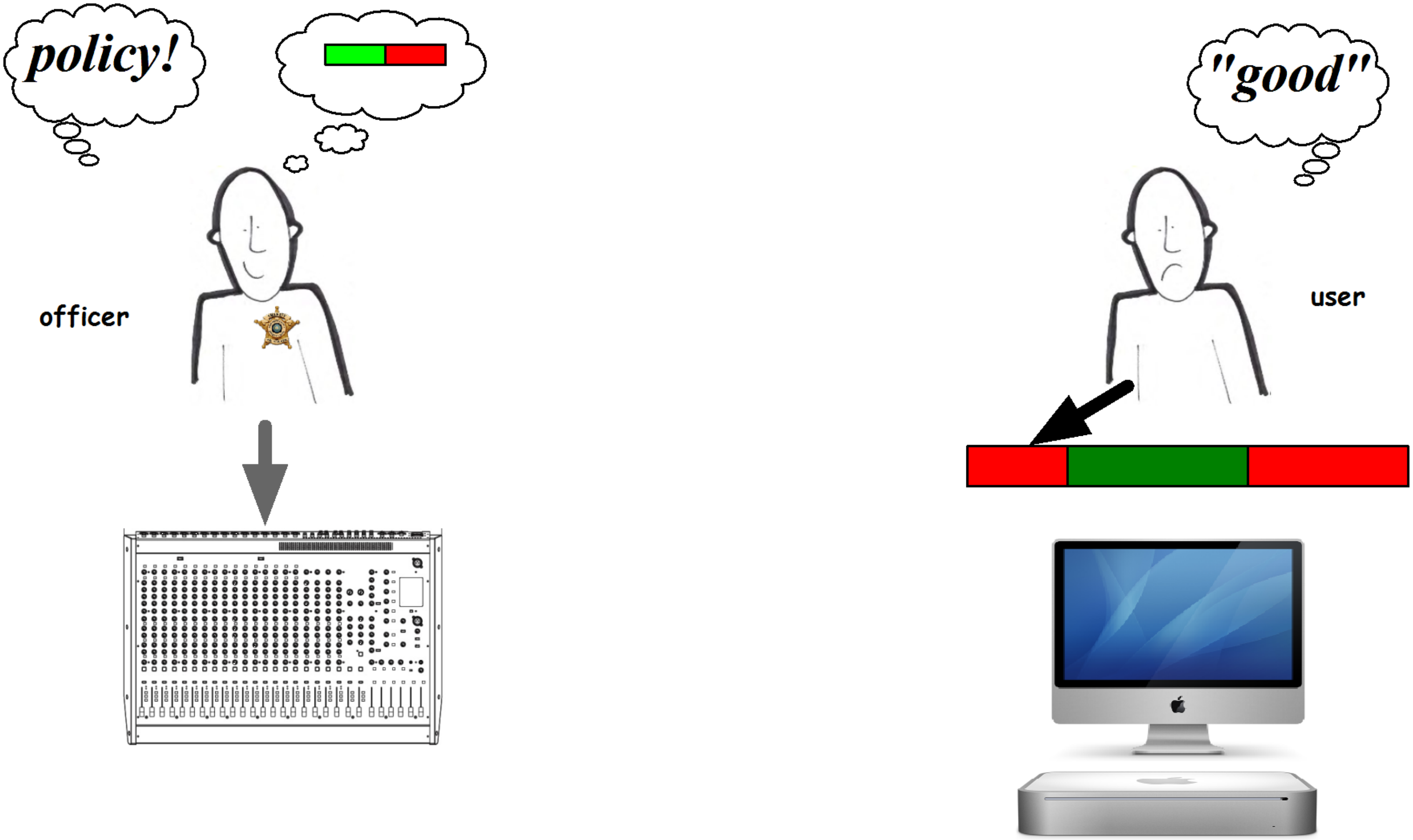
Access Control



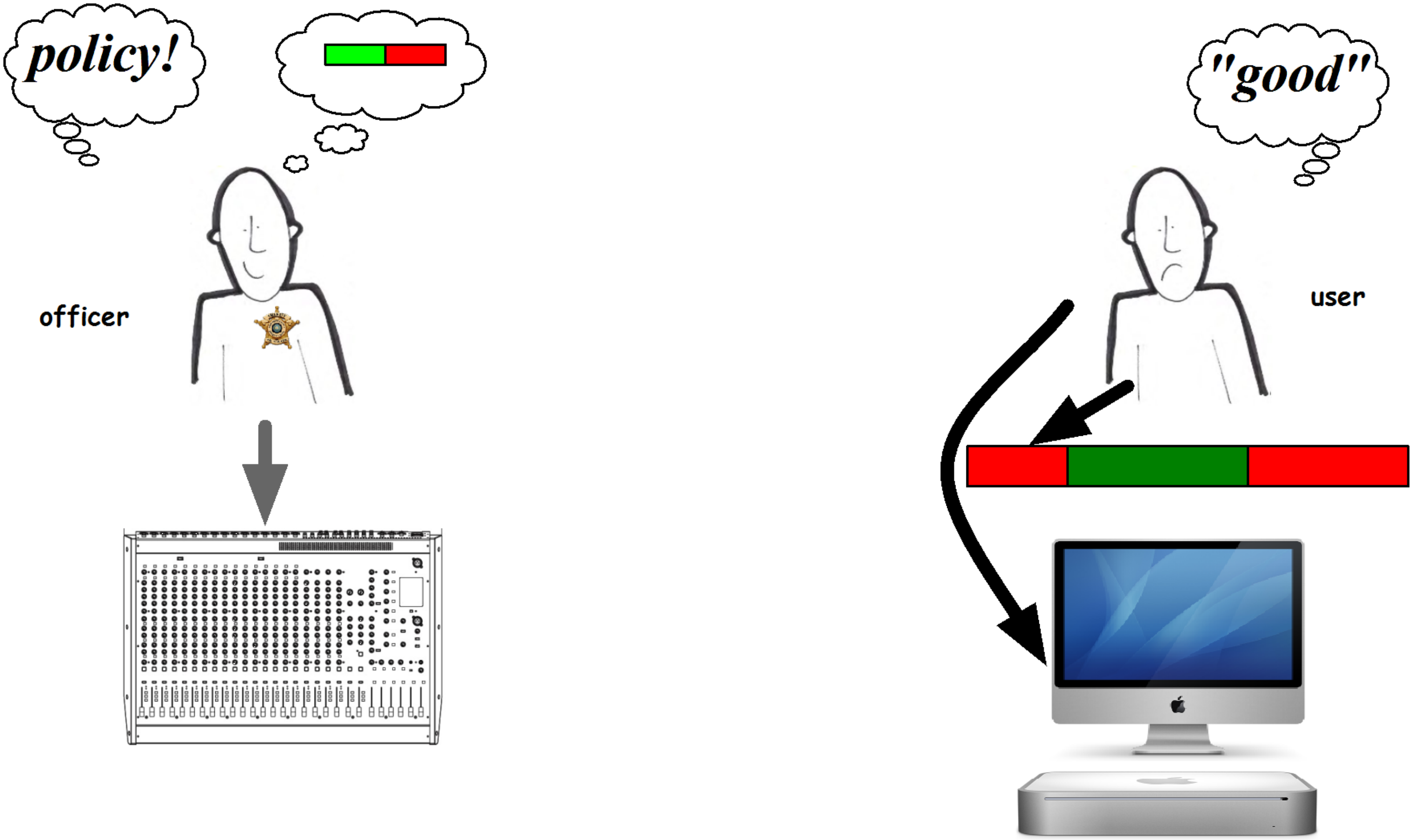
Access Control



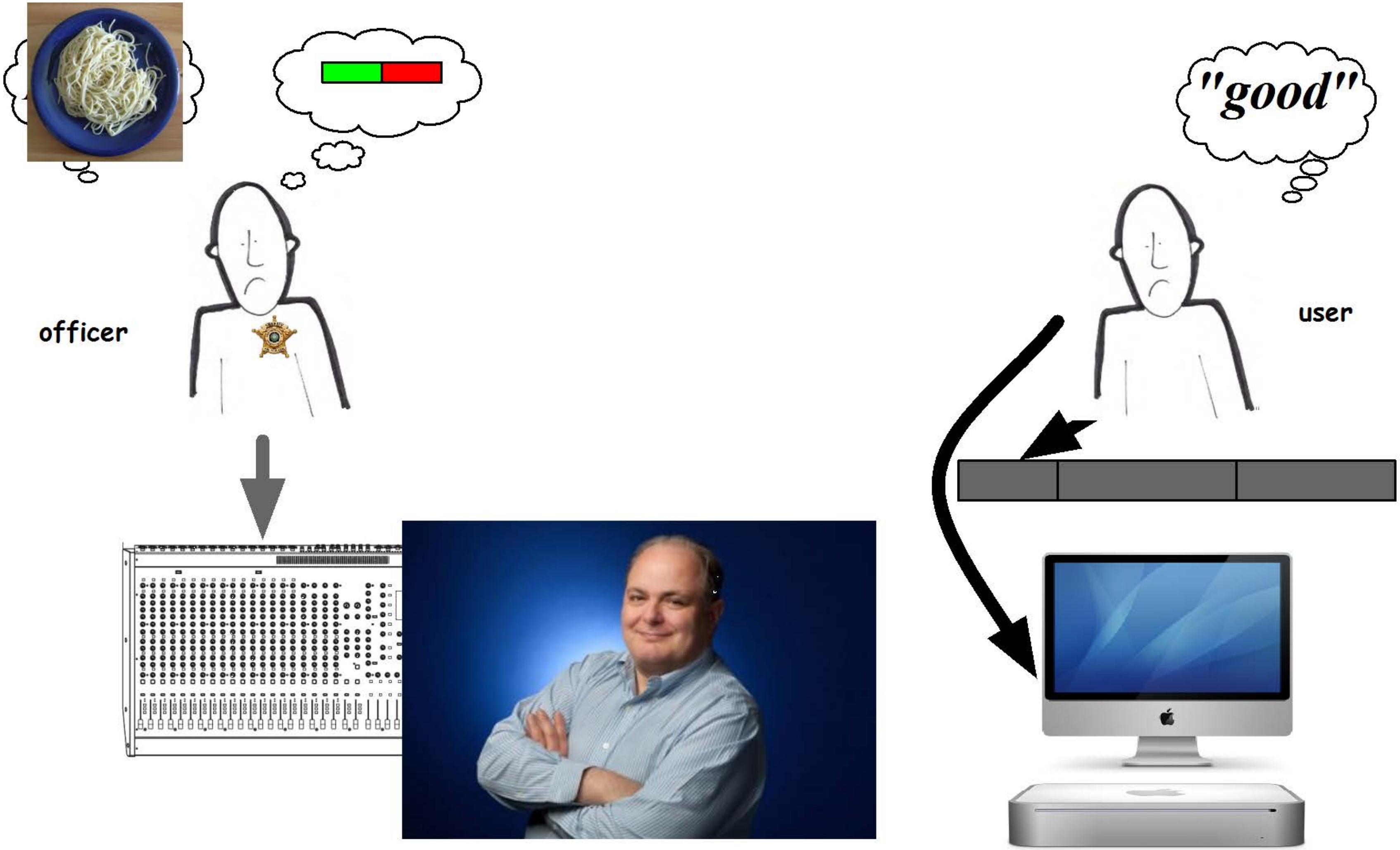
Access Control



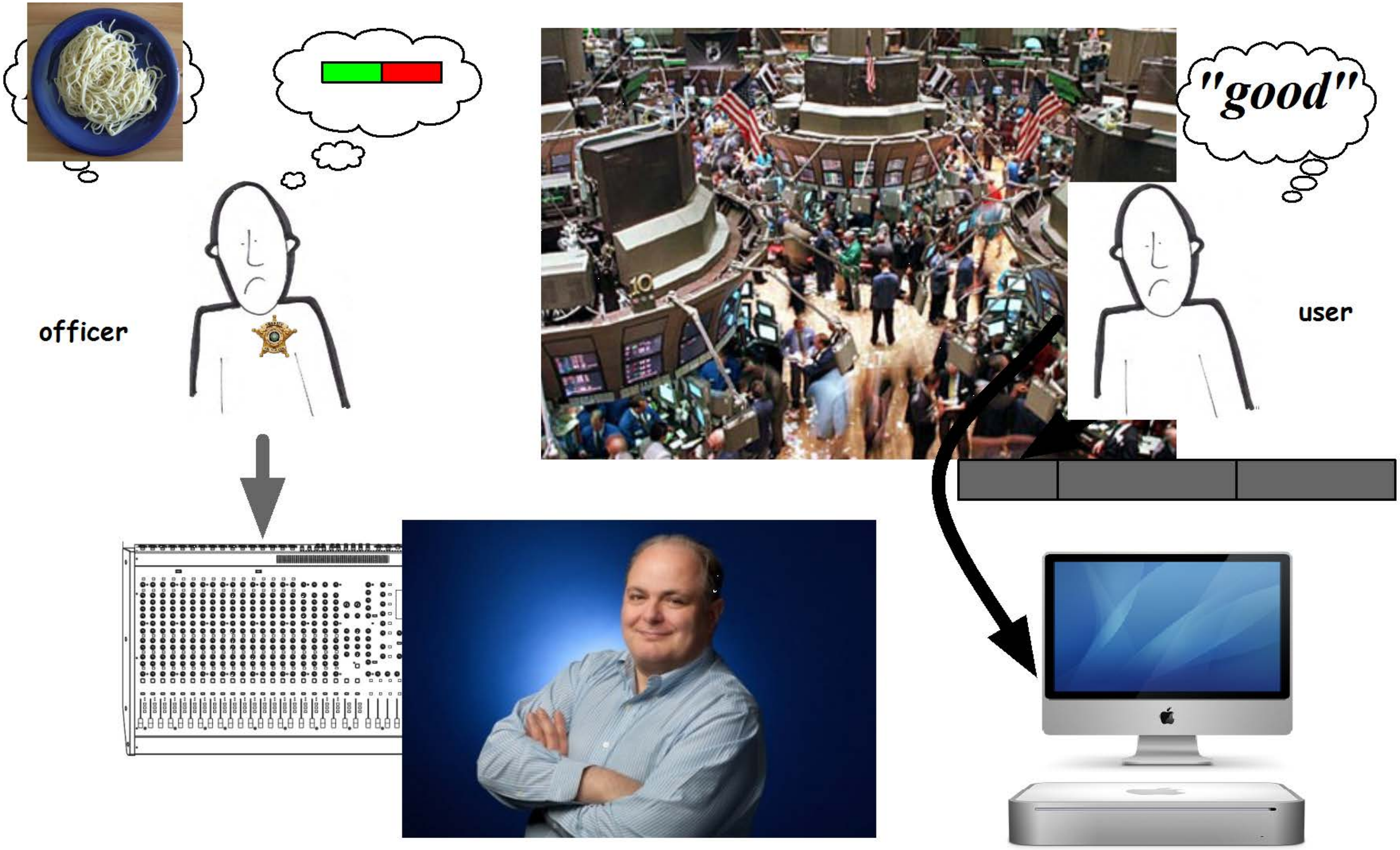
Access Control



Access Control Hygiene

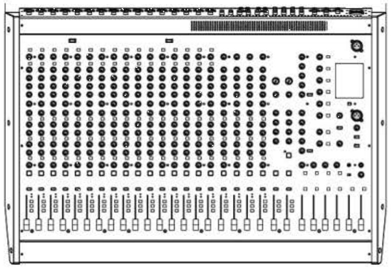


Access Control Hygiene



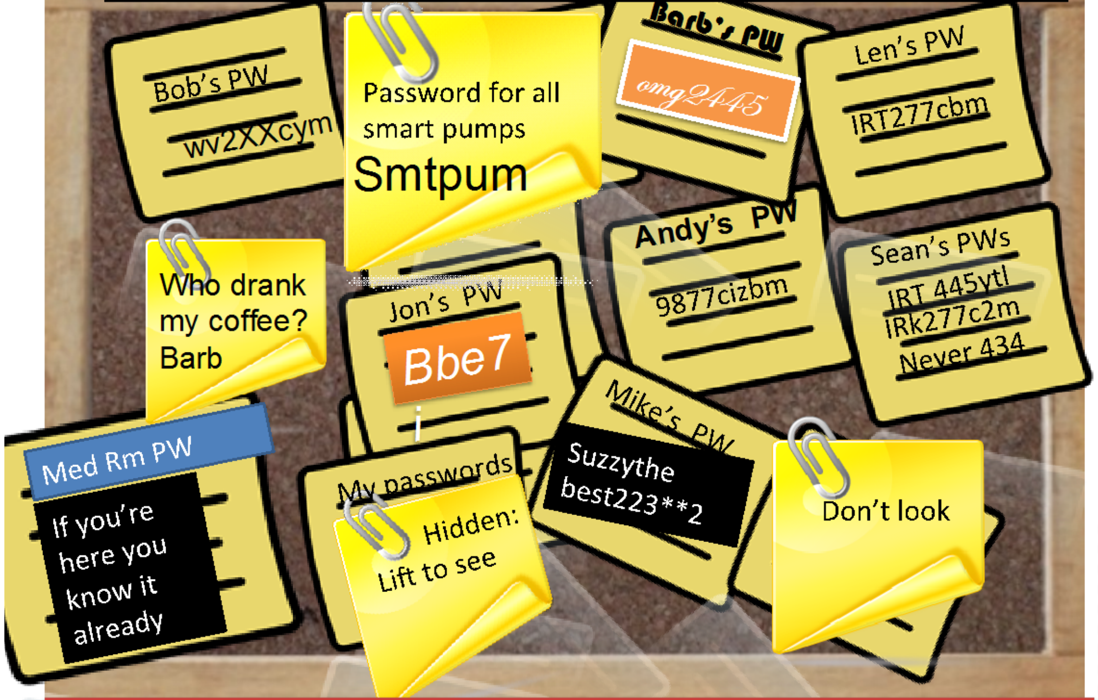
…in medical IT

"Are you here to help patients? Or do you just want to build a better policeman?"
user

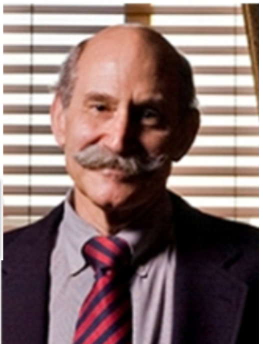


…in medical IT

View of passwords inside the supply room



“Simulated” to avoid ethical violations and jail



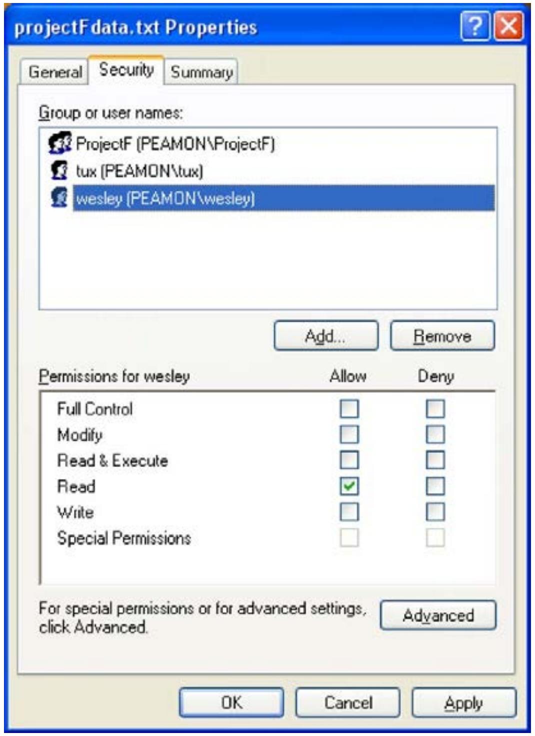
…in enterprise networks

```
RANCID-CONTENT-TYPE: cisco

Chassis type: WS-C3550-12G - a 3550 switch
CPU: PowerPC

Memory: main 65526K/8192K
Serial Number: CHK0641V006
Model revision number: D0
Model number: WS-C3550-12G
Motherboard assembly number: 73-5526-06
Motherboard serial number: CAT064004XA
Motherboard revision number: A0
Power supply part number: 34-0967-01
Power supply serial number: LIT063100GL

Processor ID: CHK0641V006

Power: RPS is NOT PRESENT

Image: Software: C3550-IPBASEK9-M, 12.2(44)SE5, RELEASE SOFTWARE (fc2)
Image: Compiled: Thu 22-Jan-09 08:27
Image: flash:c3550-ipbasek9-mz.122-44.SE5/c3550-ipbasek9-mz.122-44.SE5.bin
```

```
vlan 2835
 name my-service
!
interface GigabitEthernet0/1
 description Feed from Somewhere crt
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mls qos trust dscp
 wrr-queue cos-map 1 0 1
 wrr-queue cos-map 3 4
 priority-queue out
!
interface GigabitEthernet0/2
 description SecretPlace
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 2802
 switchport trunk allowed vlan 104,2802
 switchport mode dynamic desirable
 mls qos trust dscp
 wrr-queue cos-map 1 0 1
 wrr-queue cos-map 5 6
 priority-queue out
!
access-list 1 permit 333.041.18.0 0.0.0.255 lo
access-list 1 permit 333.041.18.0 0.0.0.255 lo
```

…in file permissions

er / Int. J. Human-Computer Studies 63 (2005) 25–50 31



projectFdata.txt Properties

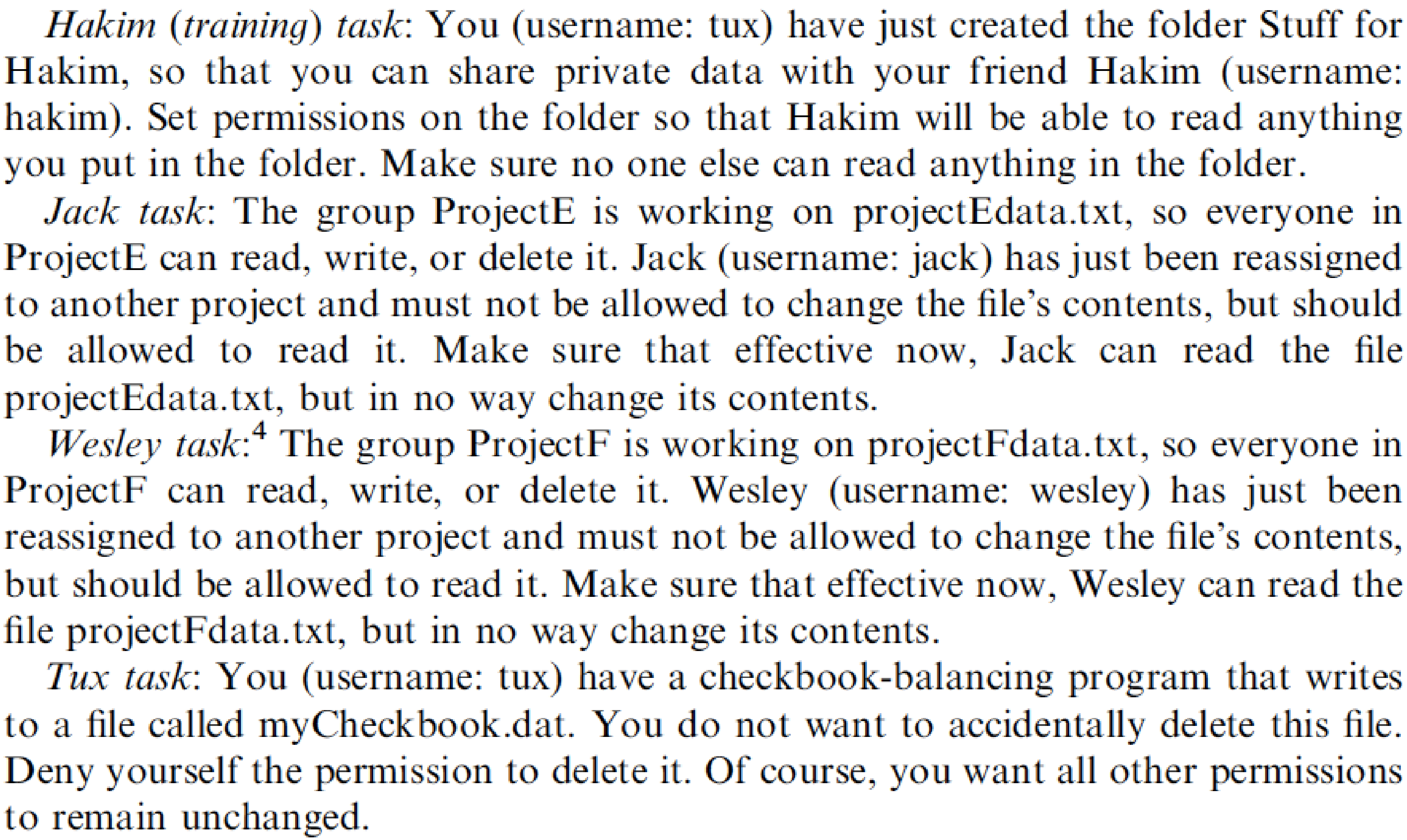
Group or user names:

- ProjectF (PEAMON\ProjectF)
- tux (PEAMON\tux)
- wesley (PEAMON\wesley)

Permissions for wesley	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
Read	☑	□
Write	□	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

…in file permissions



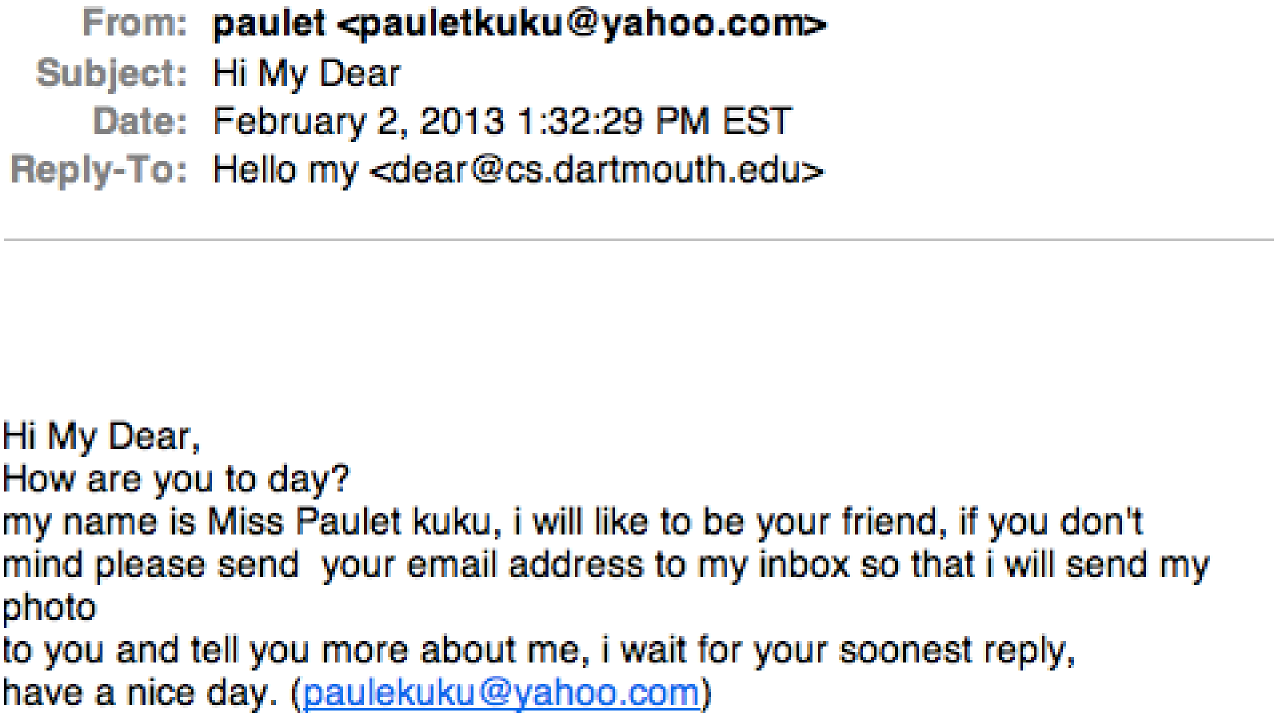
Hakim (training) task: You (username: tux) have just created the folder Stuff for Hakim, so that you can share private data with your friend Hakim (username: hakim). Set permissions on the folder so that Hakim will be able to read anything you put in the folder. Make sure no one else can read anything in the folder.

Jack task: The group ProjectE is working on projectEdata.txt, so everyone in ProjectE can read, write, or delete it. Jack (username: jack) has just been reassigned to another project and must not be allowed to change the file's contents, but should be allowed to read it. Make sure that effective now, Jack can read the file projectEdata.txt, but in no way change its contents.

Wesley task:[4] The group ProjectF is working on projectFdata.txt, so everyone in ProjectF can read, write, or delete it. Wesley (username: wesley) has just been reassigned to another project and must not be allowed to change the file's contents, but should be allowed to read it. Make sure that effective now, Wesley can read the file projectFdata.txt, but in no way change its contents.

Tux task: You (username: tux) have a checkbook-balancing program that writes to a file called myCheckbook.dat. You do not want to accidentally delete this file. Deny yourself the permission to delete it. Of course, you want all other permissions to remain unchanged.

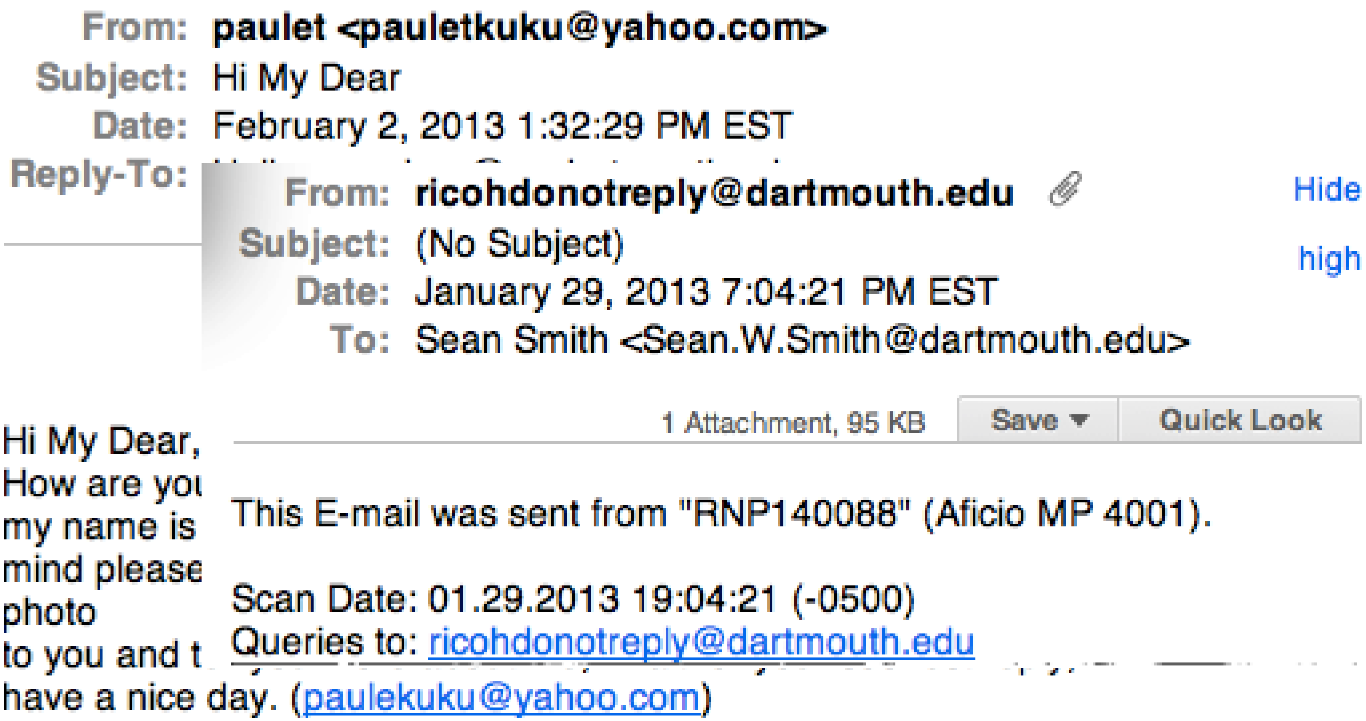
…in email



From: paulet <pauletkuku@yahoo.com>
Subject: Hi My Dear
Date: February 2, 2013 1:32:29 PM EST
Reply-To: Hello my <dear@cs.dartmouth.edu>

Hi My Dear,
How are you to day?
my name is Miss Paulet kuku, i will like to be your friend, if you don't
mind please send your email address to my inbox so that i will send my
photo
to you and tell you more about me, i wait for your soonest reply,
have a nice day. (paulekuku@yahoo.com)

…in email



From: paulet <pauletkuku@yahoo.com>
Subject: Hi My Dear
Date: February 2, 2013 1:32:29 PM EST
Reply-To:

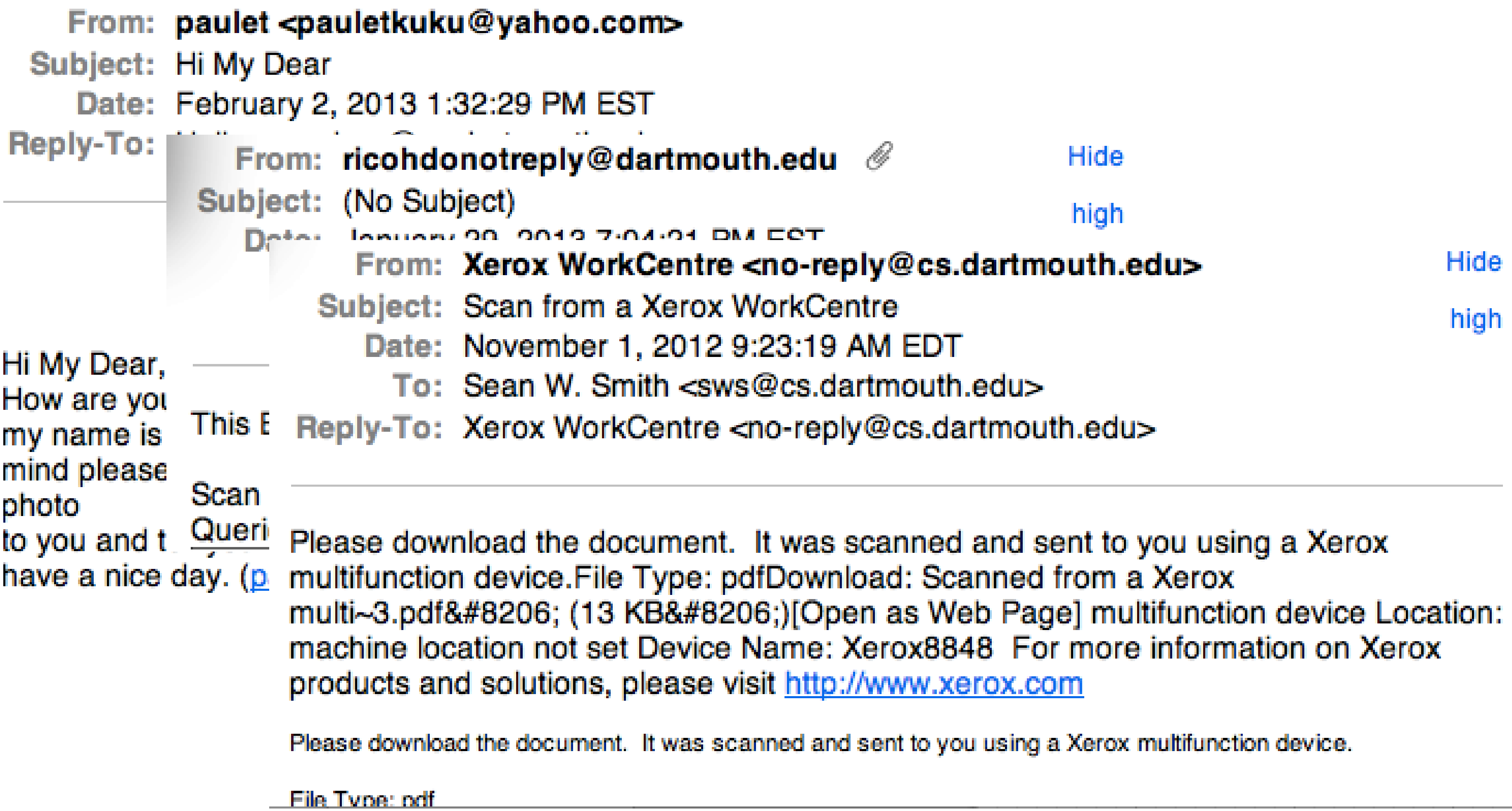
From: ricohdonotreply@dartmouth.edu
Subject: (No Subject)
Date: January 29, 2013 7:04:21 PM EST
To: Sean Smith <Sean.W.Smith@dartmouth.edu>

This E-mail was sent from "RNP140088" (Aficio MP 4001).

Scan Date: 01.29.2013 19:04:21 (-0500)
Queries to: ricohdonotreply@dartmouth.edu

Hi My Dear,
How are you
my name is
mind please
photo
to you and t
have a nice day. (paulekuku@yahoo.com)

…in email



From: paulet <pauletkuku@yahoo.com>
Subject: Hi My Dear
Date: February 2, 2013 1:32:29 PM EST
Reply-To:

Hi My Dear,
How are yo
my name is
mind please
photo
to you and t
have a nice day. (p

From: ricohdonotreply@dartmouth.edu
Subject: (No Subject)
Date: January 30, 2013 7:04:21 PM EST

This E

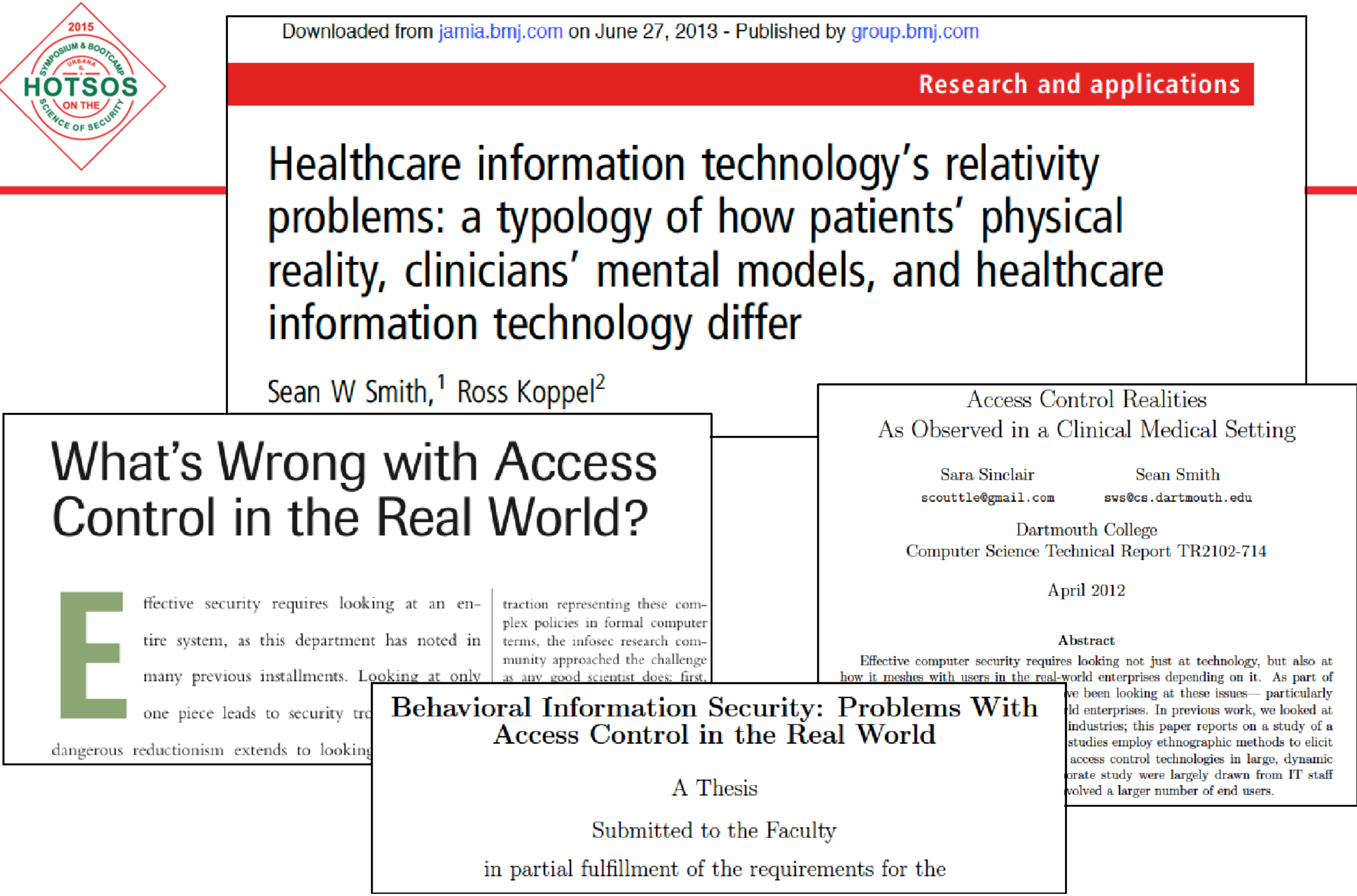
Scan
Queri

From: Xerox WorkCentre <no-reply@cs.dartmouth.edu>
Subject: Scan from a Xerox WorkCentre
Date: November 1, 2012 9:23:19 AM EDT
To: Sean W. Smith <sws@cs.dartmouth.edu>
Reply-To: Xerox WorkCentre <no-reply@cs.dartmouth.edu>

Please download the document. It was scanned and sent to you using a Xerox multifunction device.File Type: pdfDownload: Scanned from a Xerox multi~3.pdf&#8206; (13 KB&#8206;)[Open as Web Page] multifunction device Location: machine location not set Device Name: Xerox8848 For more information on Xerox products and solutions, please visit http://www.xerox.com

Please download the document. It was scanned and sent to you using a Xerox multifunction device.

File Type: pdf



Downloaded from jamia.bmj.com on June 27, 2013 - Published by group.bmj.com

Research and applications

Healthcare information technology's relativity problems: a typology of how patients' physical reality, clinicians' mental models, and healthcare information technology differ

Sean W Smith,[1] Ross Koppel[2]

What's Wrong with Access Control in the Real World?

Effective security requires looking at an entire system, as this department has noted in many previous installments. Looking at only one piece leads to security tro

dangerous reductionism extends to looking

traction representing these complex policies in formal computer terms, the infosec research community approached the challenge as any good scientist does: first,

Access Control Realities

As Observed in a Clinical Medical Setting

Sara Sinclair
scouttle@gmail.com

Sean Smith
sws@cs.dartmouth.edu

Dartmouth College

Computer Science Technical Report TR2102-714

April 2012

Abstract

Effective computer security requires looking not just at technology, but also at how it meshes with users in the real-world enterprises depending on it. As part of

ve been looking at these issues— particularly

ld enterprises. In previous work, we looked at

industries; this paper reports on a study of a

studies employ ethnographic methods to elicit

access control technologies in large, dynamic

orate study were largely drawn from IT staff

volved a larger number of end users.

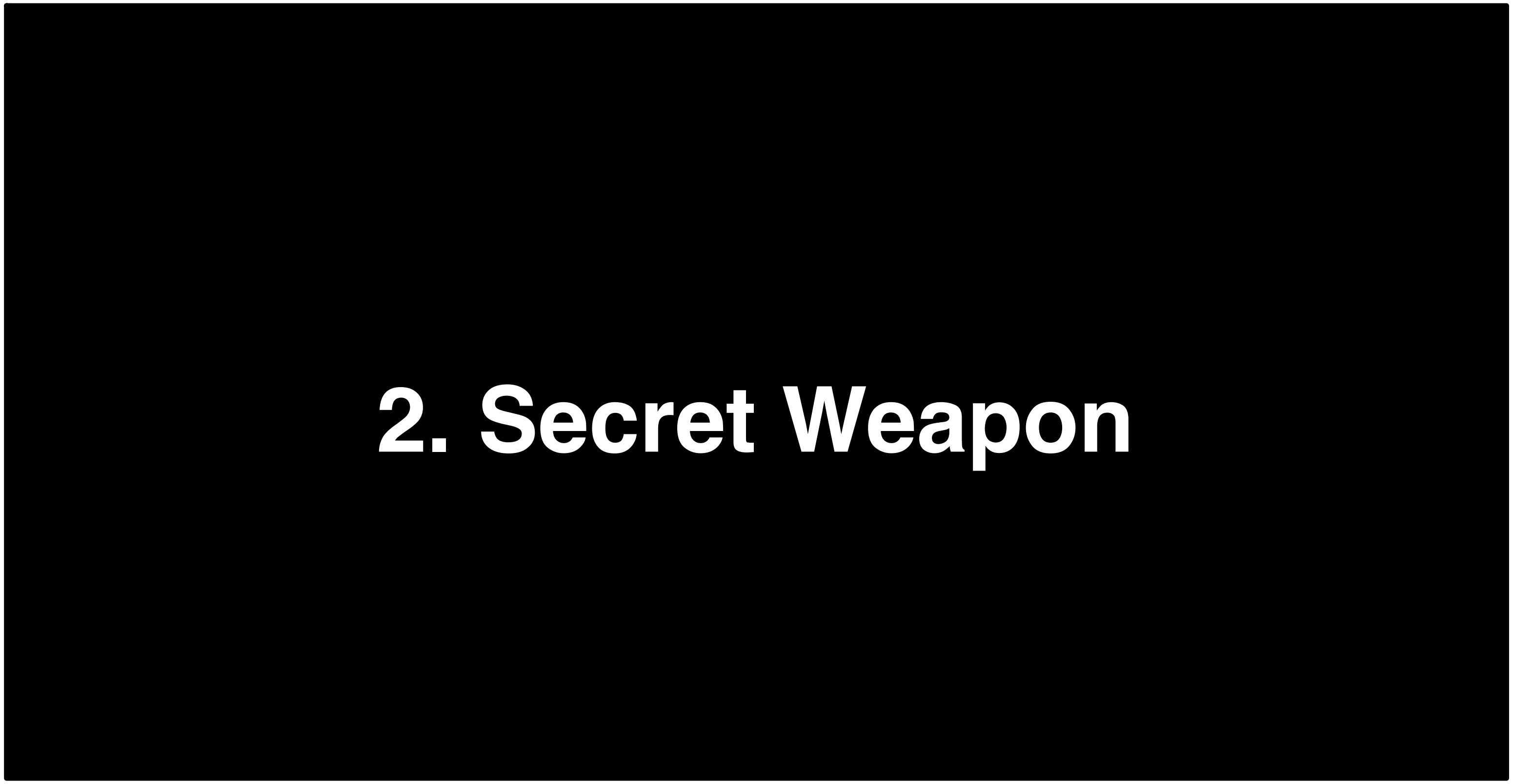
Behavioral Information Security: Problems With Access Control in the Real World

A Thesis

Submitted to the Faculty

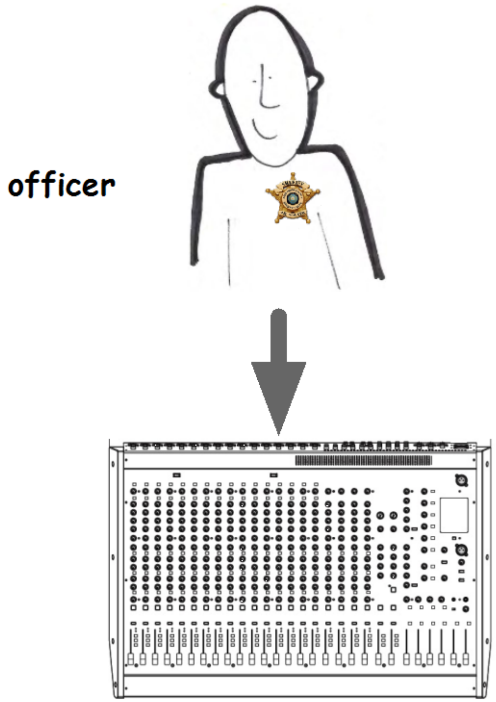
in partial fulfillment of the requirements for the

Cognitive Bias and Security

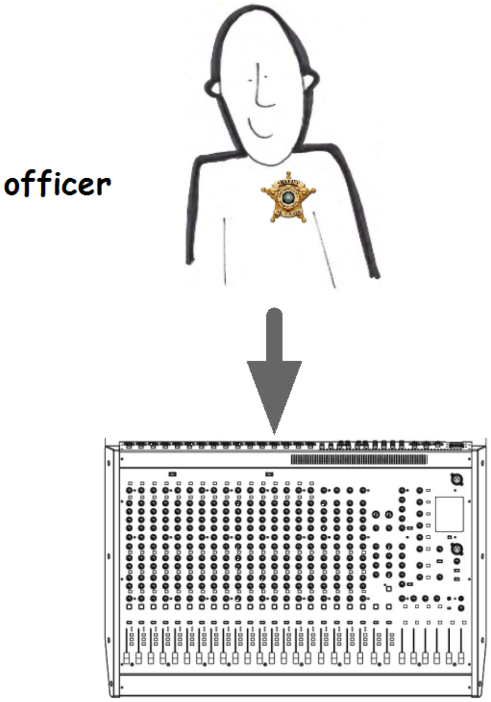


2. Secret Weapon

Secret Weapon

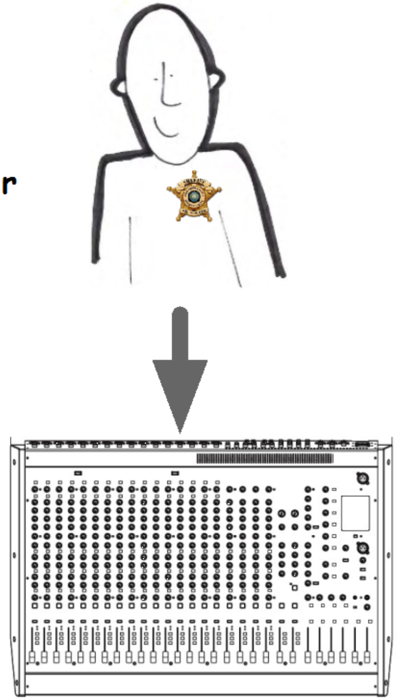


Secret Weapon



Secret Weapon

officer

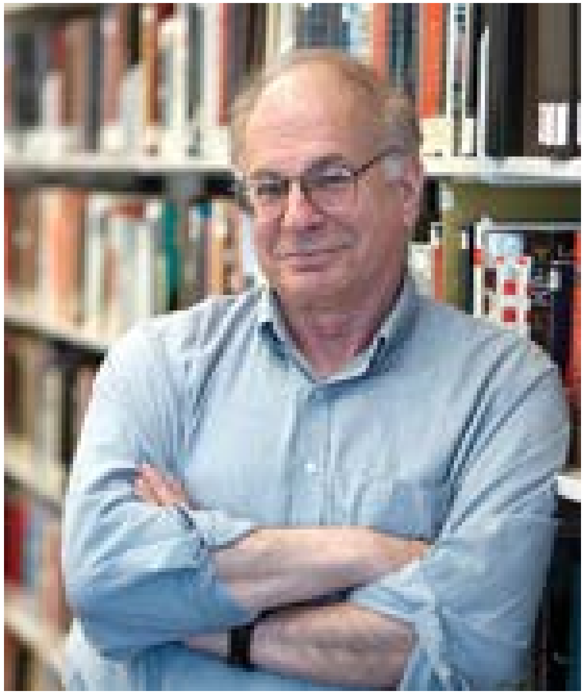


"Eppur si muove..."

Secret Weapon

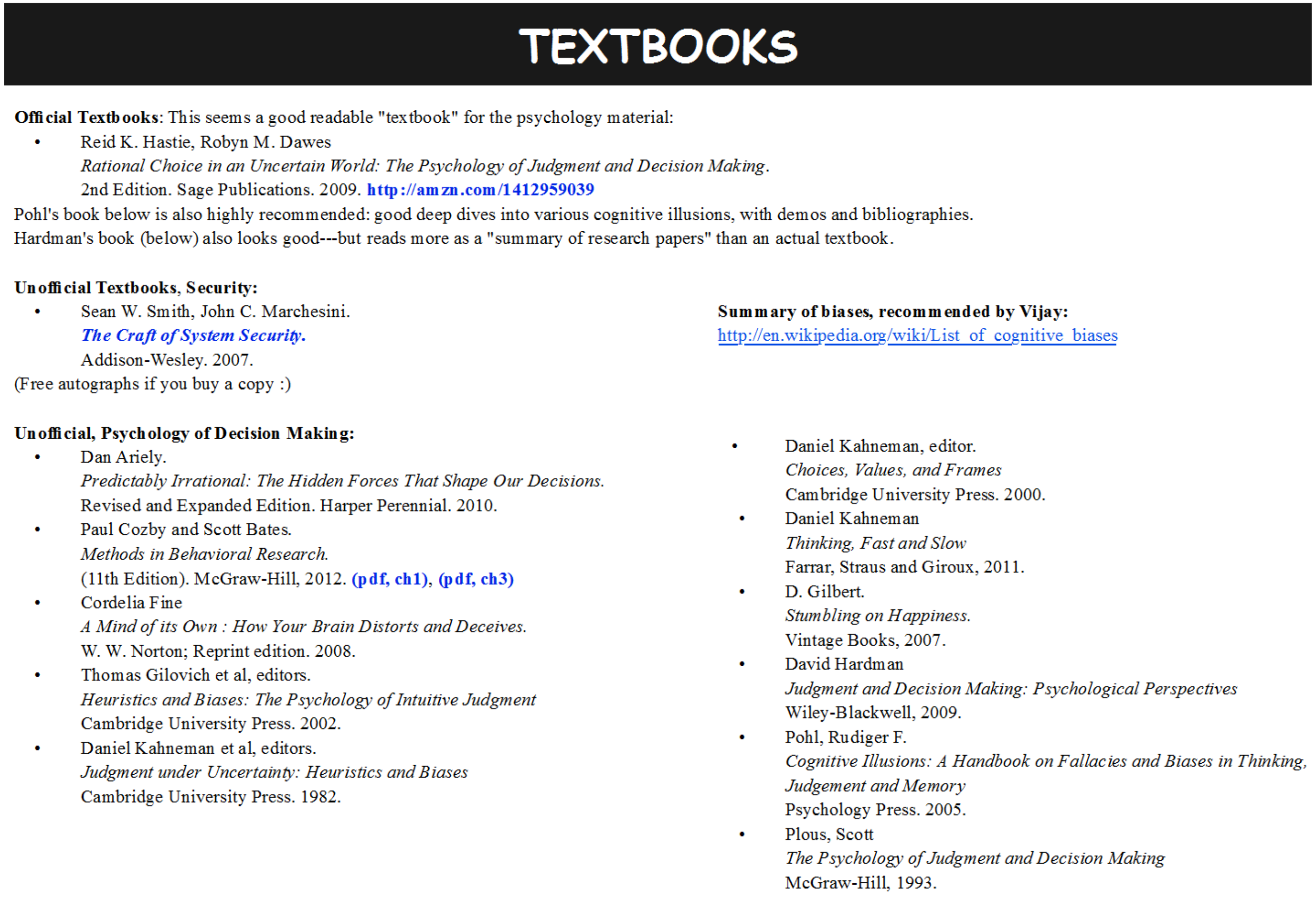
hilobrow.com

Secret Weapon



wikipedia.com

Secret Weapon



TEXTBOOKS

Official Textbooks: This seems a good readable "textbook" for the psychology material:

- Reid K. Hastie, Robyn M. Dawes
  Rational Choice in an Uncertain World: The Psychology of Judgment and Decision Making.
  2nd Edition. Sage Publications. 2009. **http://amzn.com/1412959039**

Pohl's book below is also highly recommended: good deep dives into various cognitive illusions, with demos and bibliographies.
Hardman's book (below) also looks good---but reads more as a "summary of research papers" than an actual textbook.

Unofficial Textbooks, Security:

- Sean W. Smith, John C. Marchesini.
  The Craft of System Security.
  Addison-Wesley. 2007.

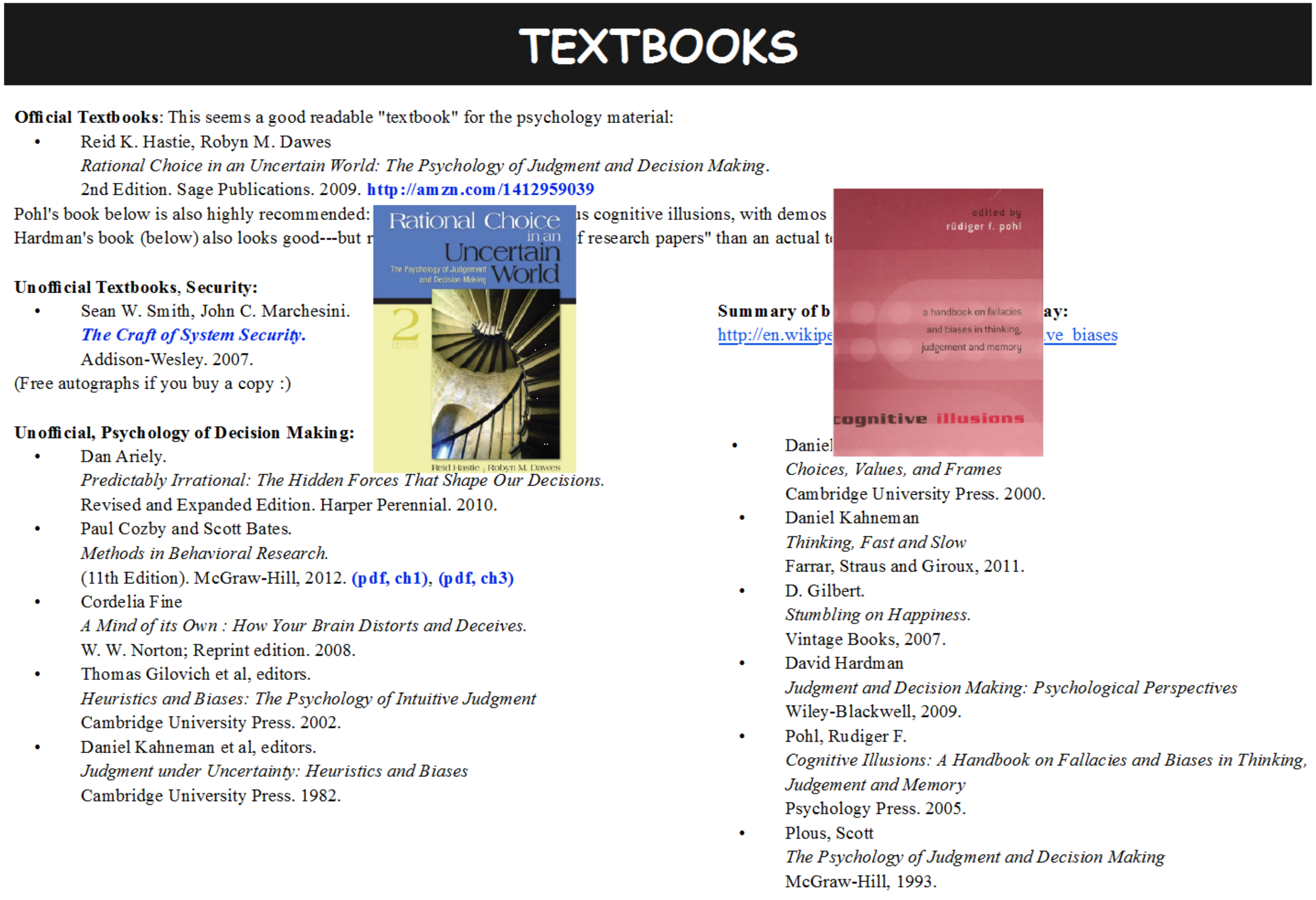
(Free autographs if you buy a copy :)

Summary of biases, recommended by Vijay:
http://en.wikipedia.org/wiki/List_of_cognitive_biases

Unofficial, Psychology of Decision Making:

- Dan Ariely.
  Predictably Irrational: The Hidden Forces That Shape Our Decisions.
  Revised and Expanded Edition. Harper Perennial. 2010.
- Paul Cozby and Scott Bates.
  Methods in Behavioral Research.
  (11th Edition). McGraw-Hill, 2012. **(pdf, ch1)**, **(pdf, ch3)**
- Cordelia Fine
  A Mind of its Own : How Your Brain Distorts and Deceives.
  W. W. Norton; Reprint edition. 2008.
- Thomas Gilovich et al, editors.
  Heuristics and Biases: The Psychology of Intuitive Judgment
  Cambridge University Press. 2002.
- Daniel Kahneman et al, editors.
  Judgment under Uncertainty: Heuristics and Biases
  Cambridge University Press. 1982.
- Daniel Kahneman, editor.
  Choices, Values, and Frames
  Cambridge University Press. 2000.
- Daniel Kahneman
  Thinking, Fast and Slow
  Farrar, Straus and Giroux, 2011.
- D. Gilbert.
  Stumbling on Happiness.
  Vintage Books, 2007.
- David Hardman
  Judgment and Decision Making: Psychological Perspectives
  Wiley-Blackwell, 2009.
- Pohl, Rudiger F.
  Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory
  Psychology Press. 2005.
- Plous, Scott
  The Psychology of Judgment and Decision Making
  McGraw-Hill, 1993.

Secret Weapon



TEXTBOOKS

Official Textbooks: This seems a good readable "textbook" for the psychology material:

- Reid K. Hastie, Robyn M. Dawes
  Rational Choice in an Uncertain World: The Psychology of Judgment and Decision Making.
  2nd Edition. Sage Publications. 2009. **http://amzn.com/1412959039**

Pohl's book below is also highly recommended: us cognitive illusions, with demos
Hardman's book (below) also looks good---but r f research papers" than an actual t

Unofficial Textbooks, Security:

- Sean W. Smith, John C. Marchesini.
  The Craft of System Security.
  Addison-Wesley. 2007.

(Free autographs if you buy a copy :)

Unofficial, Psychology of Decision Making:

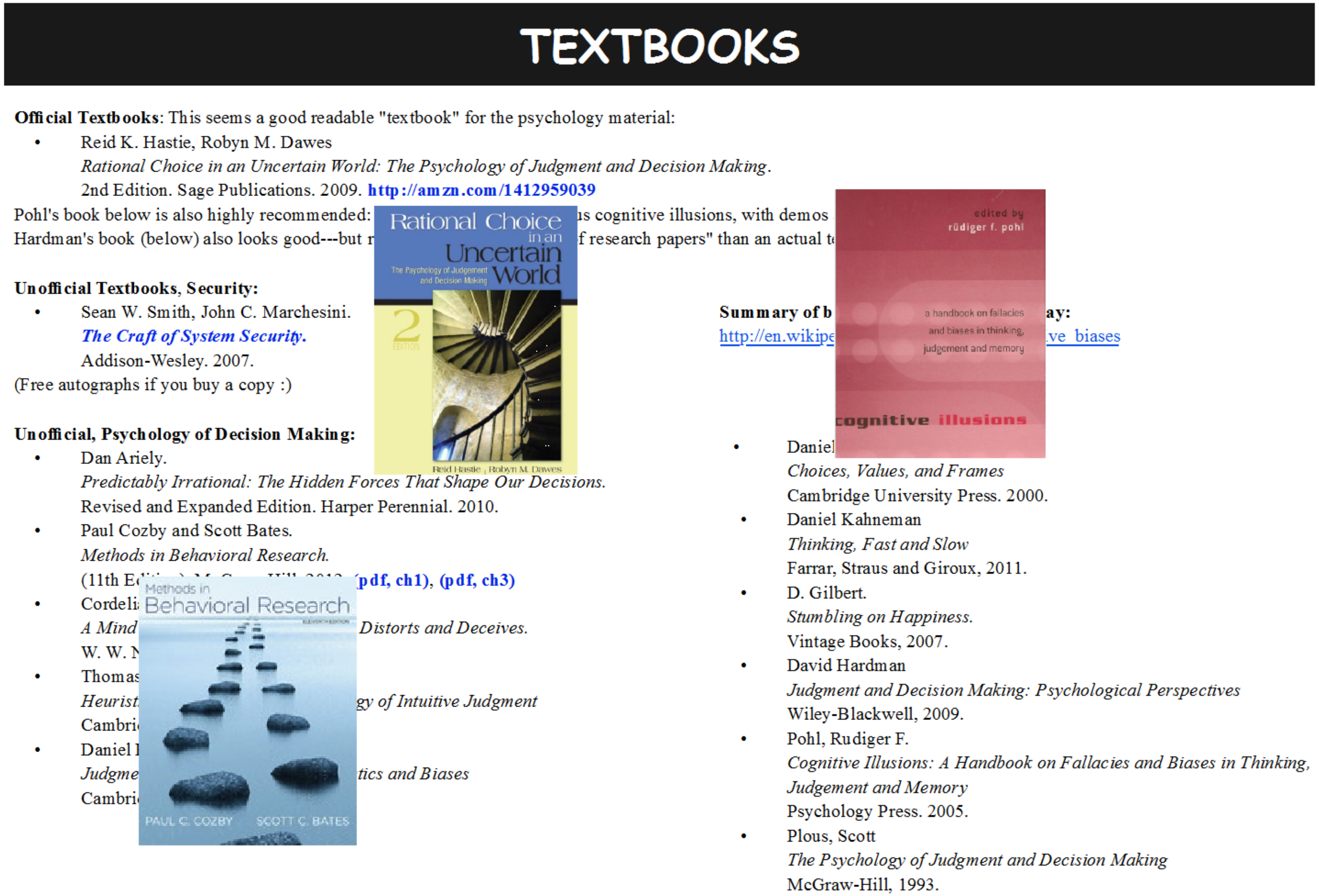
- Dan Ariely.
  Predictably Irrational: The Hidden Forces That Shape Our Decisions.
  Revised and Expanded Edition. Harper Perennial. 2010.
- Paul Cozby and Scott Bates.
  Methods in Behavioral Research.
  (11th Edition). McGraw-Hill, 2012. **(pdf, ch1)**, **(pdf, ch3)**
- Cordelia Fine
  A Mind of its Own : How Your Brain Distorts and Deceives.
  W. W. Norton; Reprint edition. 2008.
- Thomas Gilovich et al, editors.
  Heuristics and Biases: The Psychology of Intuitive Judgment
  Cambridge University Press. 2002.
- Daniel Kahneman et al, editors.
  Judgment under Uncertainty: Heuristics and Biases
  Cambridge University Press. 1982.

Summary of b ay:
http://en.wikipe ve_biases

- Daniel
  Choices, Values, and Frames
  Cambridge University Press. 2000.
- Daniel Kahneman
  Thinking, Fast and Slow
  Farrar, Straus and Giroux, 2011.
- D. Gilbert.
  Stumbling on Happiness.
  Vintage Books, 2007.
- David Hardman
  Judgment and Decision Making: Psychological Perspectives
  Wiley-Blackwell, 2009.
- Pohl, Rudiger F.
  Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory
  Psychology Press. 2005.
- Plous, Scott
  The Psychology of Judgment and Decision Making
  McGraw-Hill, 1993.

Rational Choice in an Uncertain World
The Psychology of Judgement and Decision Making
2 EDITION
Reid Hastie , Robyn M. Dawes
edited by rüdiger f. pohl
a handbook on fallacies and biases in thinking, judgement and memory
cognitive illusions

Secret Weapon



TEXTBOOKS

Official Textbooks: This seems a good readable "textbook" for the psychology material:

- Reid K. Hastie, Robyn M. Dawes
  Rational Choice in an Uncertain World: The Psychology of Judgment and Decision Making.
  2nd Edition. Sage Publications. 2009. **http://amzn.com/1412959039**

Pohl's book below is also highly recommended: us cognitive illusions, with demos
Hardman's book (below) also looks good---but r f research papers" than an actual t

Unofficial Textbooks, Security:

- Sean W. Smith, John C. Marchesini.
  The Craft of System Security.
  Addison-Wesley. 2007.

(Free autographs if you buy a copy :)

Unofficial, Psychology of Decision Making:

- Dan Ariely.
  Predictably Irrational: The Hidden Forces That Shape Our Decisions.
  Revised and Expanded Edition. Harper Perennial. 2010.
- Paul Cozby and Scott Bates.
  Methods in Behavioral Research.
  (11th E **(pdf, ch1)**, **(pdf, ch3)**
- Cordeli
  A Mind *Distorts and Deceives.*
  W. W. N
- Thomas
  Heurist *gy of Intuitive Judgment*
  Cambri
- Daniel
  Judgme *tics and Biases*
  Cambri

Summary of b **ay:**
http://en.wikipe ve_biases

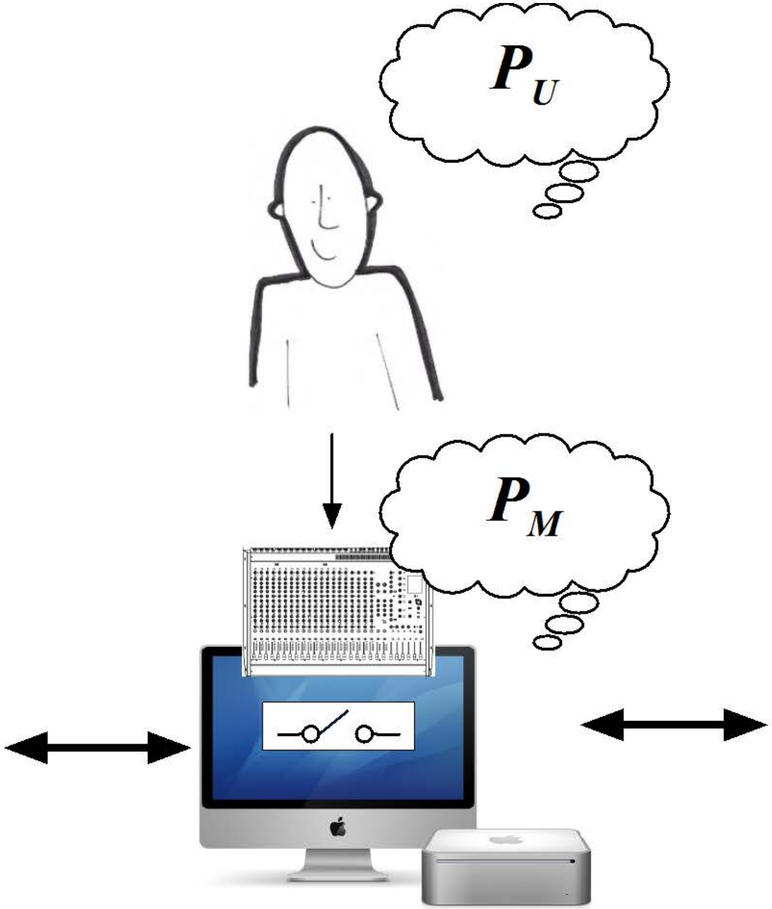
- Daniel
  Choices, Values, and Frames
  Cambridge University Press. 2000.
- Daniel Kahneman
  Thinking, Fast and Slow
  Farrar, Straus and Giroux, 2011.
- D. Gilbert.
  Stumbling on Happiness.
  Vintage Books, 2007.
- David Hardman
  Judgment and Decision Making: Psychological Perspectives
  Wiley-Blackwell, 2009.
- Pohl, Rudiger F.
  Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory
  Psychology Press. 2005.
- Plous, Scott
  The Psychology of Judgment and Decision Making
  McGraw-Hill, 1993.

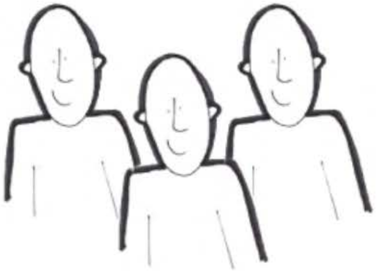
Rational Choice in an Uncertain World
The Psychology of Judgement and Decision Making
2 EDITION
Reid Hastie , Robyn M. Dawes
edited by rüdiger f. pohl
a handbook on fallacies and biases in thinking, judgement and memory
cognitive illusions
Methods in Behavioral Research
PAUL C. COZBY
SCOTT C. BATES

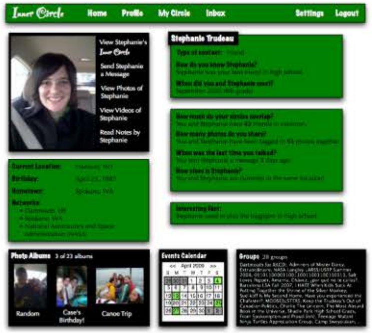
Cognitive Bias and Security

3. Initial Results

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

Stephanie Trudeau

Type of contact: [illegible]
How do you know Stephanie? [illegible]
When did you and Stephanie meet? [illegible]

Current Location: [illegible]
Birthday: [illegible]
Hometown: [illegible]
Networks: [illegible]

How much do your circles overlap? [illegible]
How many photos do you share? [illegible]
When was the last time you talked? [illegible]
How close is Stephanie? [illegible]

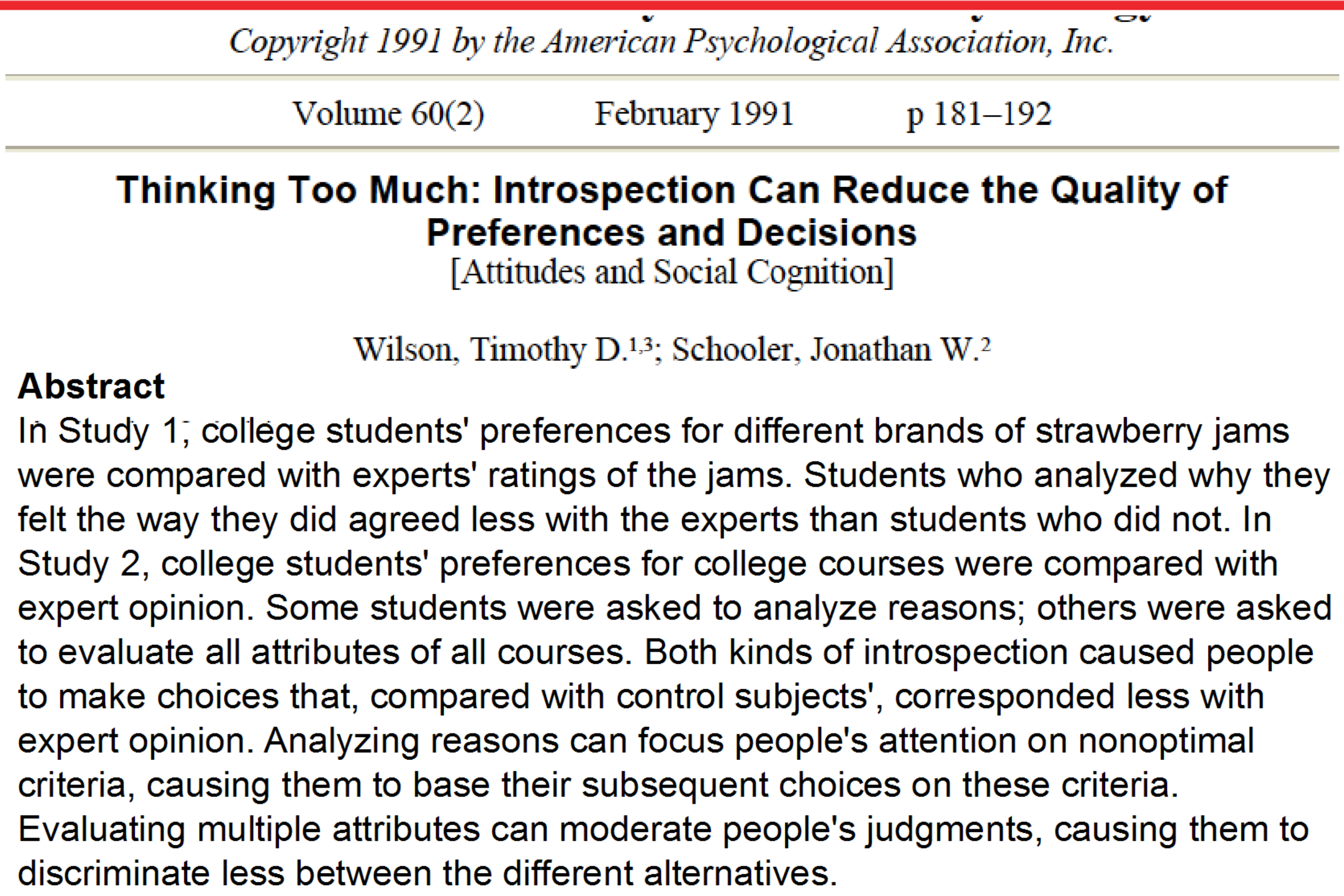
Interesting fact: [illegible]

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

Events Calendar
<< April 2009 >>

Groups 28 groups
[illegible]

From Psychology: Introspection Inhibits Intuition



Copyright 1991 by the American Psychological Association, Inc.

Volume 60(2) February 1991 p 181–192

Thinking Too Much: Introspection Can Reduce the Quality of Preferences and Decisions

[Attitudes and Social Cognition]

Wilson, Timothy D.[1,3]; Schooler, Jonathan W.[2]

Abstract

In Study 1, college students' preferences for different brands of strawberry jams were compared with experts' ratings of the jams. Students who analyzed why they felt the way they did agreed less with the experts than students who did not. In Study 2, college students' preferences for college courses were compared with expert opinion. Some students were asked to analyze reasons; others were asked to evaluate all attributes of all courses. Both kinds of introspection caused people to make choices that, compared with control subjects', corresponded less with expert opinion. Analyzing reasons can focus people's attention on nonoptimal criteria, causing them to base their subsequent choices on these criteria. Evaluating multiple attributes can moderate people's judgments, causing them to discriminate less between the different alternatives.

From Psychology: Introspection Inhibits Intuition

and Schooler, 1991:

From Psychology: Introspection Inhibits Intuition

and Schooler, 1991:

- $P_E \approx P_C$

From Psychology: Introspection Inhibits Intuition

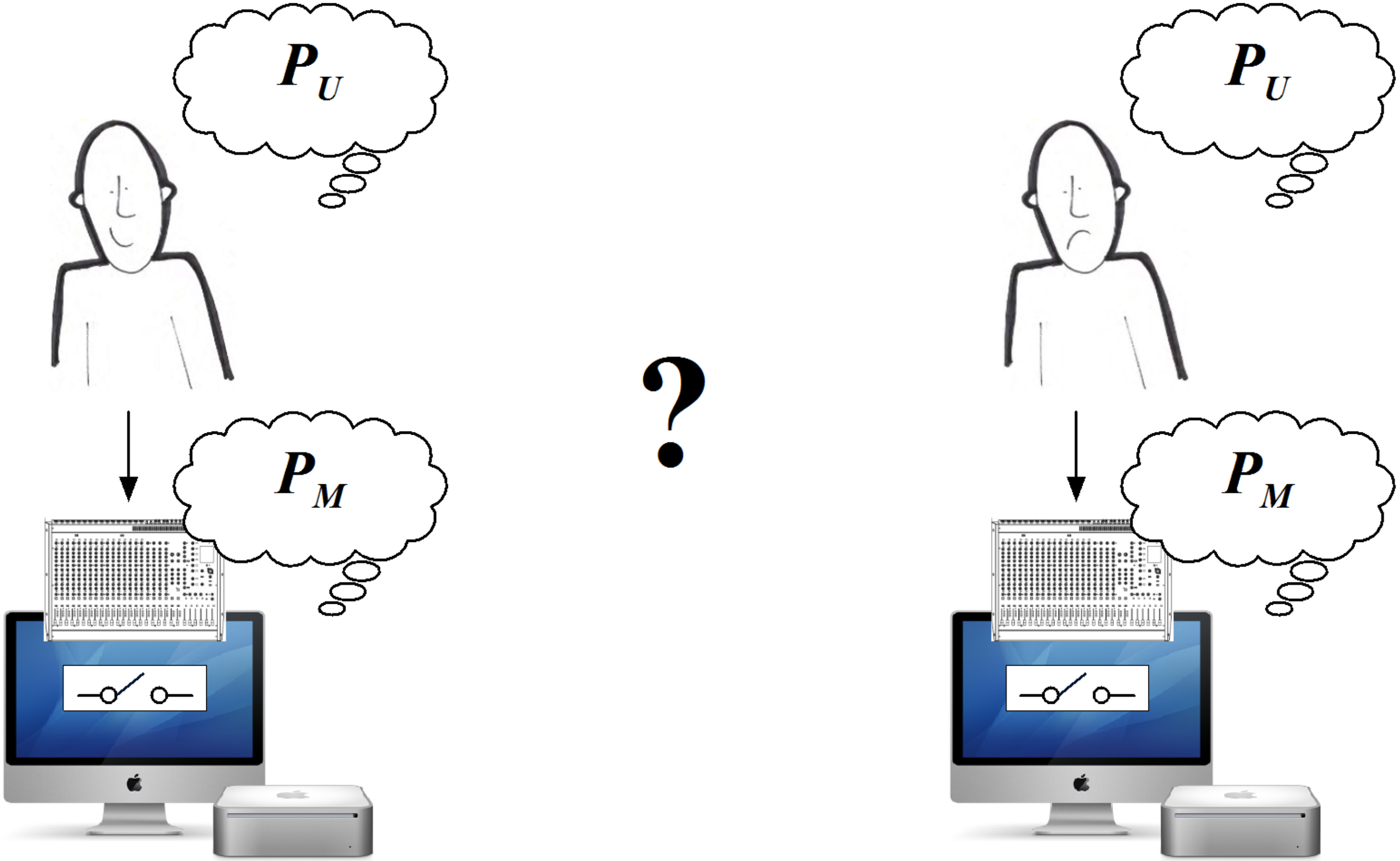
$$P_E \approx P_C$$

From Psychology: Introspection Inhibits Intuition

$P_E \approx P_C$

- $P_E \not\approx P_I$

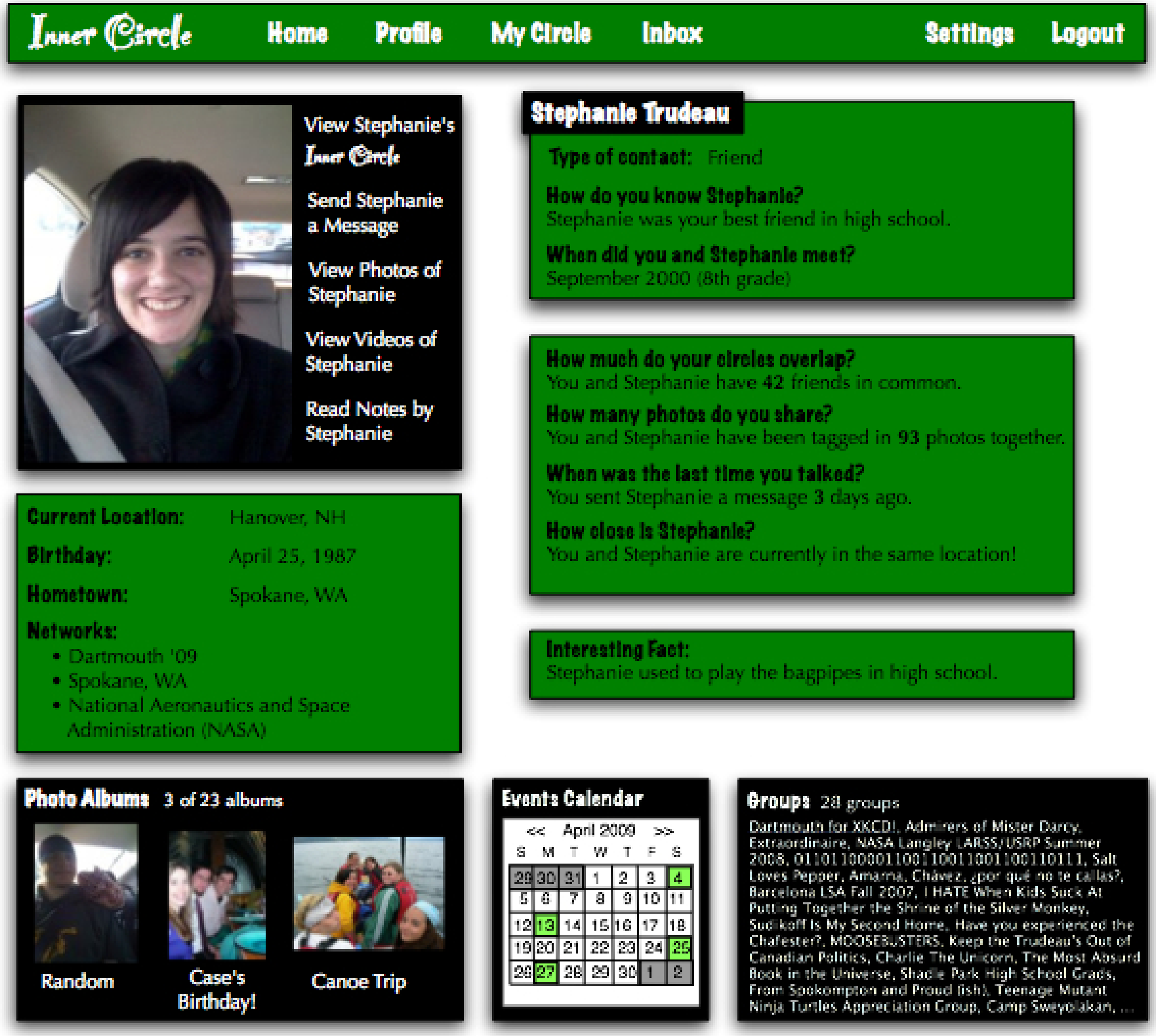
Implications for security?



$P_U \approx P_M$

$P_U \not\approx P_M$

Fake Social Network



View Stephanie's Inner Circle

Send Stephanie a Message

View Photos of Stephanie

View Videos of Stephanie

Read Notes by Stephanie

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.

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

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

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

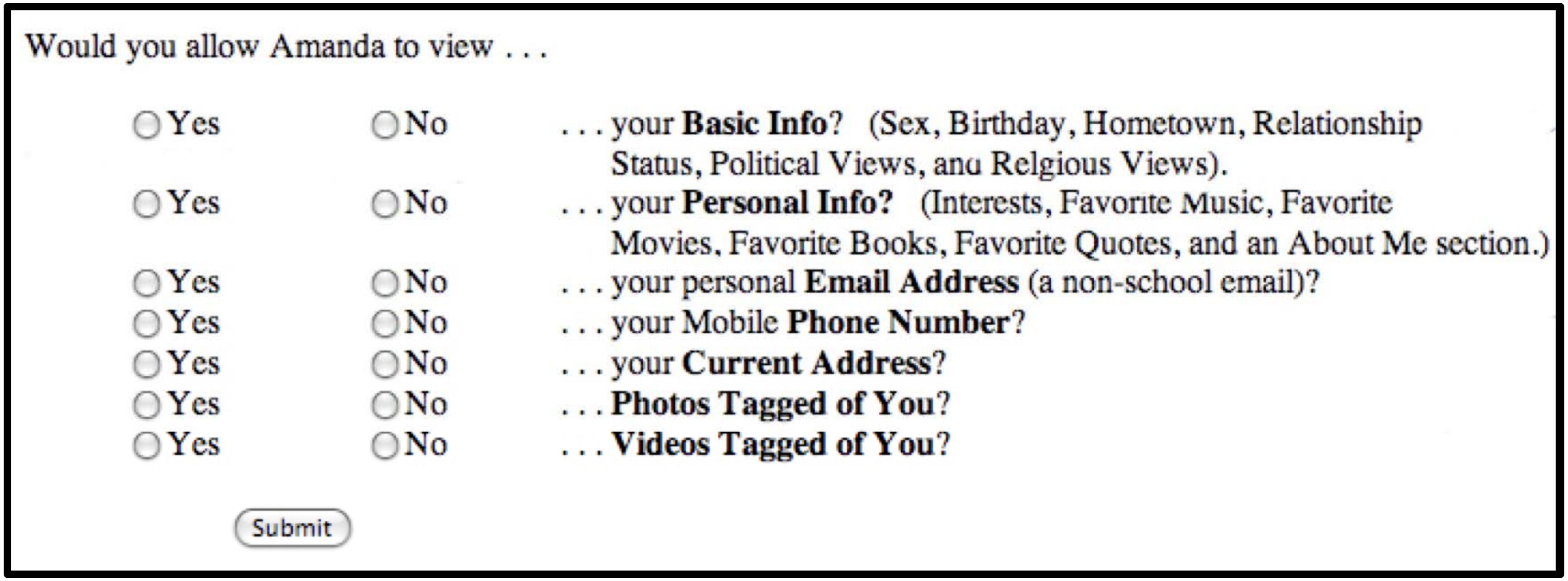
Groups 28 groups

Dartmouth for XKCD!, Admirers of Mister Darcy, Extraordinaire, NASA Langley LARSS/USRP Summer 2008, 01101100001100110011001100110111, 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, ...

Profiles

			common friends	common tags	last time talked	distance
1	***Wade Spurlock***	lived on freshman floor; haven't talked since	16	18	infinite	0
2	***Chathum Nielsen***	randomly sat at your table in food court	0	0	infinite	0
3	***Arthur Patterson***	dated in 18 months in HS	23	88	9 months	126
4	***Danny Wilson***	uncle	9	0	9 months	587
5	***Jake Mehrens***	danced with once at Thu Night Salsa	1	3	1 month	656
6	***Andrew Van Winkle***	HS friend, family connections	35	5	1 month	3000
7	***Amanda Hartley***	same Greek house, but don't know well	36	0	6 months	0
8	***Phil Sanders***	met at a party; sketchy	26	0	infinite	0
9	***Beth Franz***	friend of older sister	1	3	infinite	2946
10	***Andrew Parrish***	met at party last term; funny	23	0	3 months	0
11	***Samantha Miller***	same camp in HS; used to hang out	14	18	5 months	2364
12	***Michael Holloway***	boss last summer	1	3	3 months	656
13	***Darcy Shapiro***	same top 5 favorite movies	0	0	infinite	0
14	***Megan Lundeby***	best friend since preschool	24	82	0	2719
15	***Maddie Petrin***	track teammate first 2 years of college	35	2	0	2997
16	***Colleen Kirsten***	both like Queen	0	0	infinite	361
17	***Peggy Clark***	camp director; you worked; family went	44	87	12 months	2688
18	***Cam Schnur***	met in a hostel in Prague during LSA	0	0	12 months	256
19	***Kate Farrington***	friend of roommates	13	2	infinite	0
20	***Sarah Watkins***	hung out at conference	0	0	2 months	126

Access Control Decisions



Would you allow Amanda to view . . .

○ Yes ○ No . . . your **Basic Info**? (Sex, Birthday, Hometown, Relationship Status, Political Views, anu Relgious Views).

○ Yes ○ No . . . your **Personal Info?** (Interests, Favorite Music, Favorite Movies, Favorite Books, Favorite Quotes, and an About Me section.)

○ Yes ○ No . . . your personal **Email Address** (a non-school email)?

○ Yes ○ No . . . your Mobile **Phone Number**?

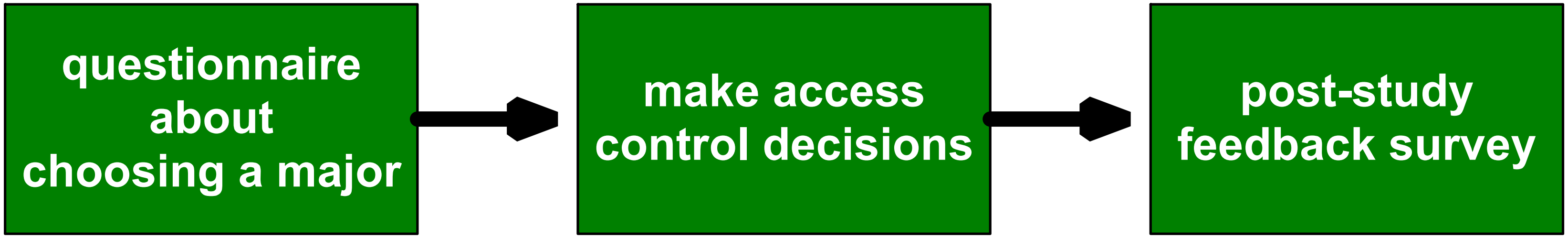
○ Yes ○ No . . . your **Current Address**?

○ Yes ○ No . . . **Photos Tagged of You**?

○ Yes ○ No . . . **Videos Tagged of You**?

Methodology

Control group:

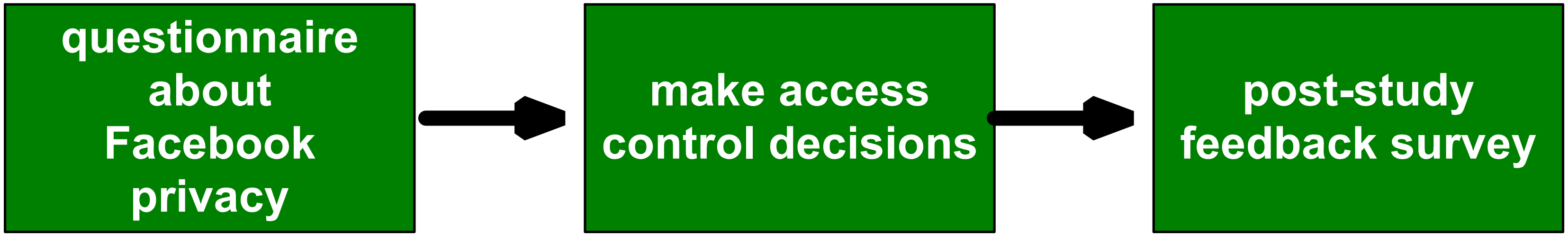


questionnaire about choosing a major

make access control decisions

post-study feedback survey

Introspective group:



questionnaire about Facebook privacy

make access control decisions

post-study feedback survey

Results

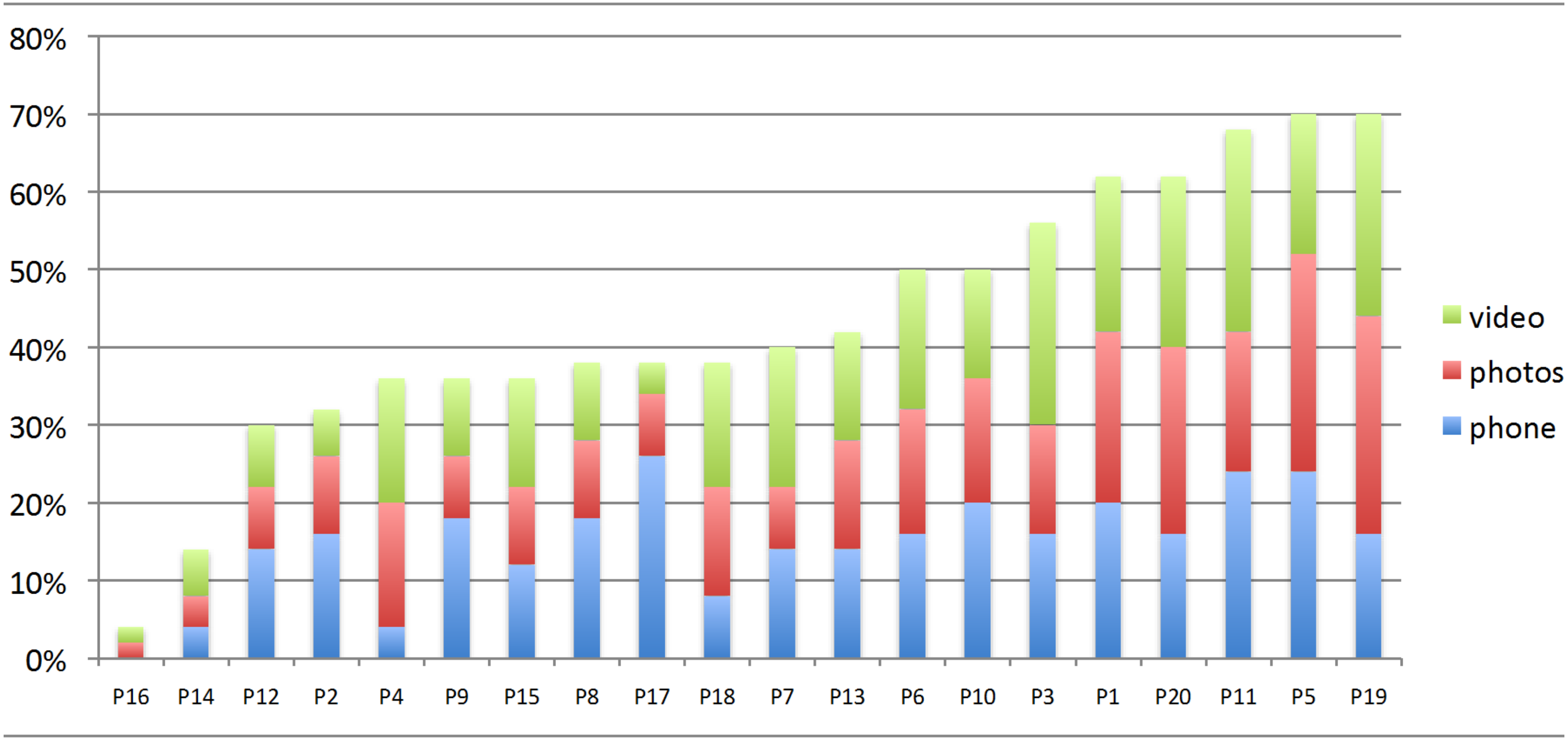
$\boldsymbol{P_C \not\approx P_I}$

Results

$\boldsymbol{P_C \not\approx P_I}$ The introspective group was ***significantly more likely to share sensitive information!***

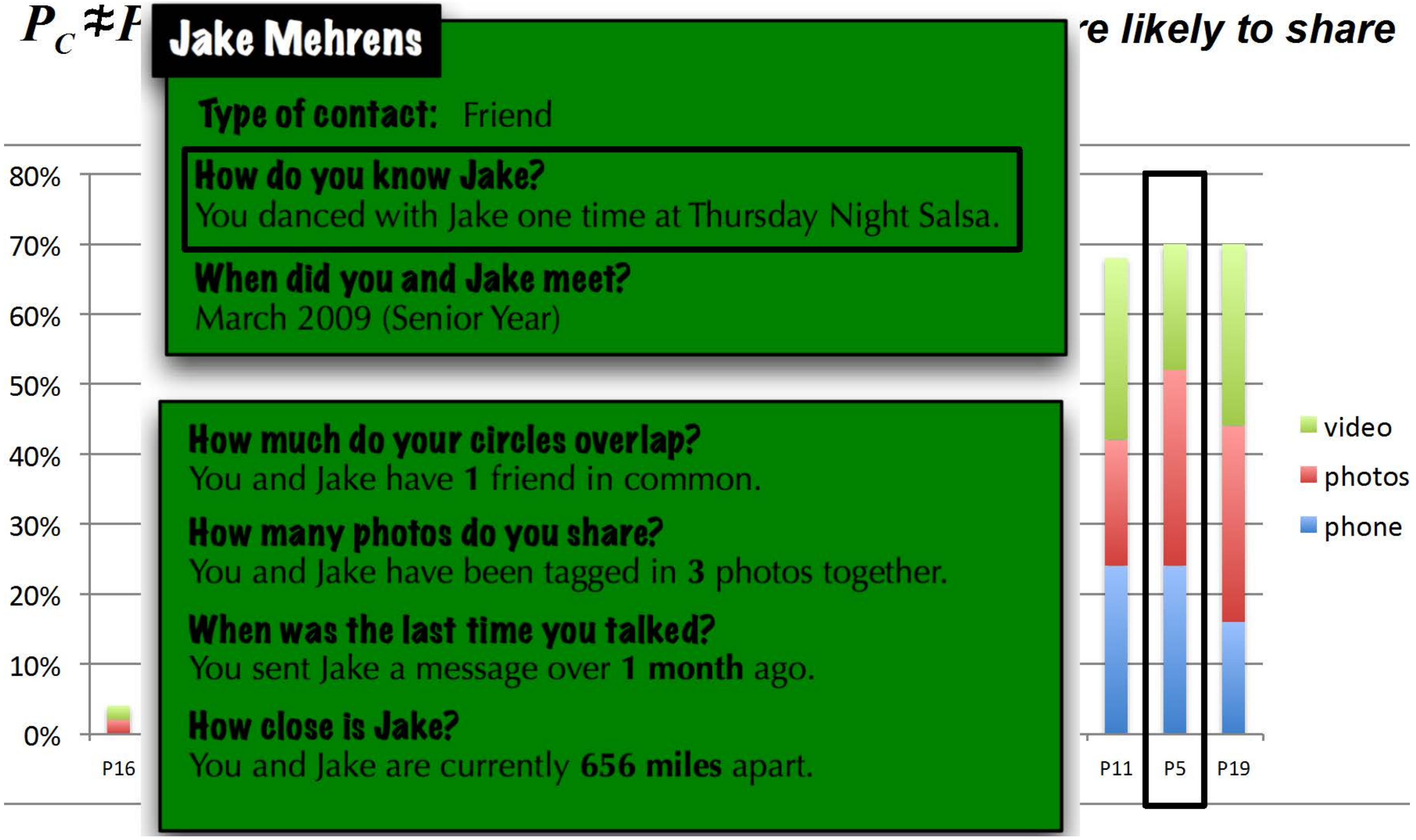
Results

$P_C \mp P_I$ The introspective group was ***significantly more likely to share sensitive information!***



Results

$P_C \mp F$ … re likely to share



Jake Mehrens

Type of contact: Friend

How do you know Jake?
You danced with Jake one time at Thursday Night Salsa.

When did you and Jake meet?
March 2009 (Senior Year)

How much do your circles overlap?
You and Jake have **1** friend in common.

How many photos do you share?
You and Jake have been tagged in **3** photos together.

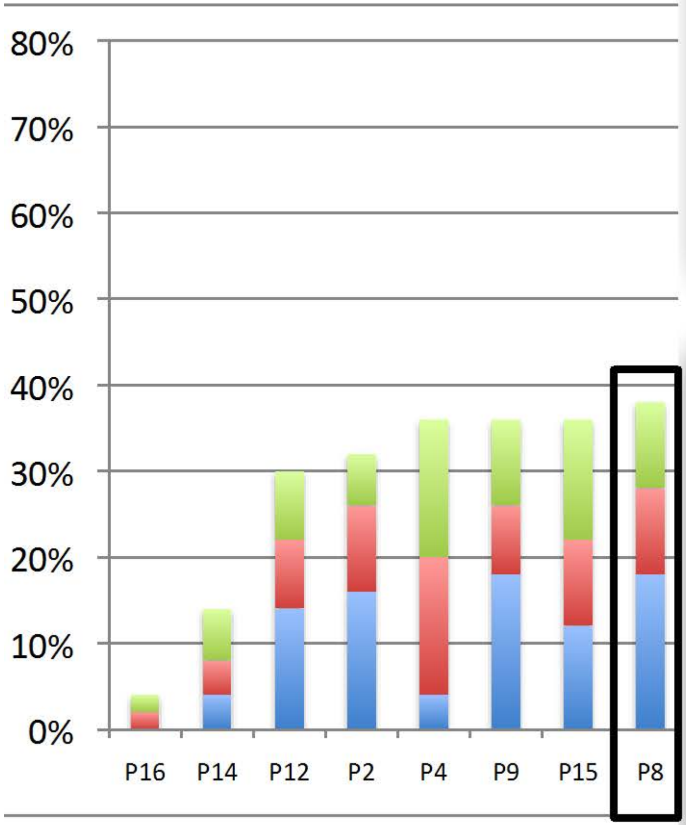
When was the last time you talked?
You sent Jake a message over **1 month** ago.

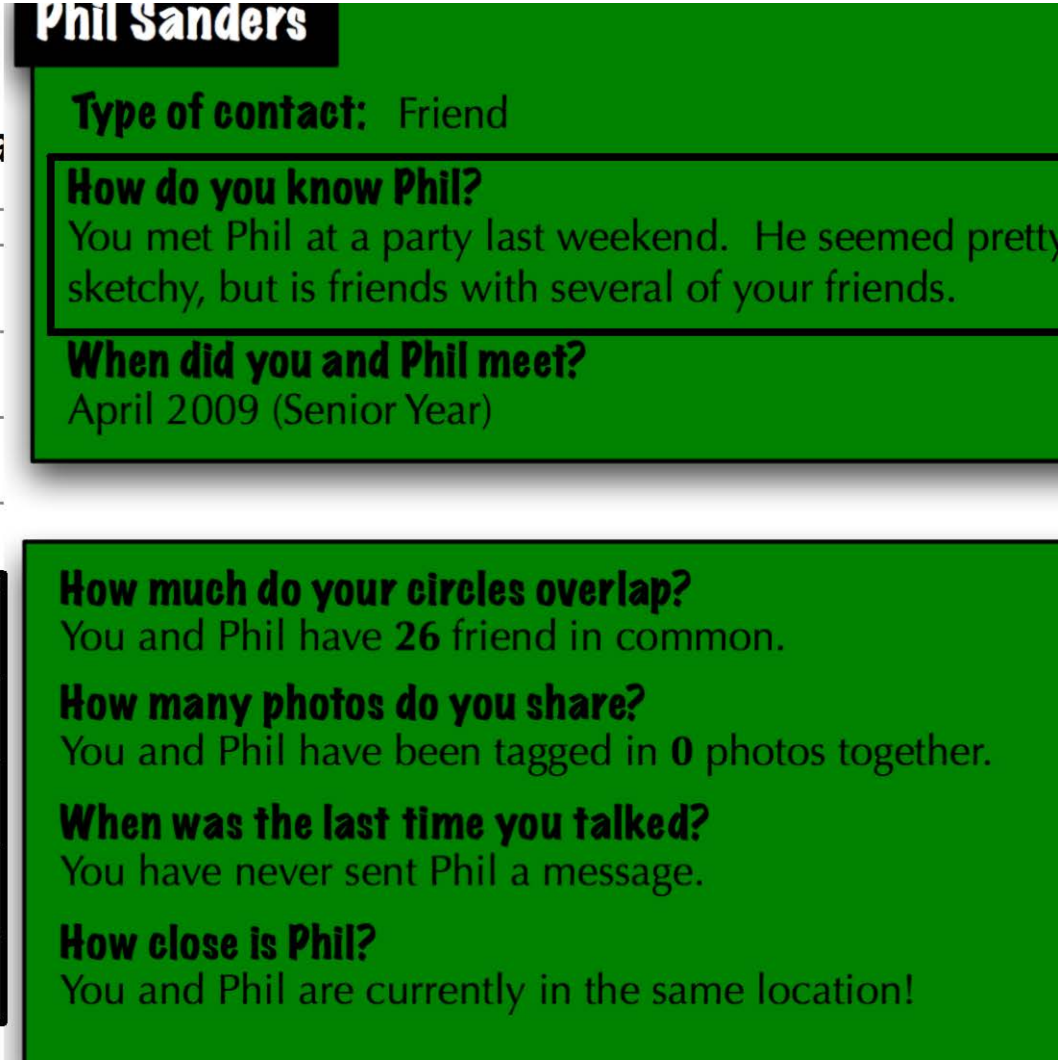
How close is Jake?
You and Jake are currently **656 miles** apart.

Results

$P_C \neq P_I$ The introspective

sensitive informa





Phil Sanders

Type of contact: Friend

How do you know Phil?
You met Phil at a party last weekend. He seemed pretty sketchy, but is friends with several of your friends.

When did you and Phil meet?
April 2009 (Senior Year)

How much do your circles overlap?
You and Phil have **26** friend in common.

How many photos do you share?
You and Phil have been tagged in **0** photos together.

When was the last time you talked?
You have never sent Phil a message.

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

Results

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

Results

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

- ***educating*** users about privacy issues

Results

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

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

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!***

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

PDF Box

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!***

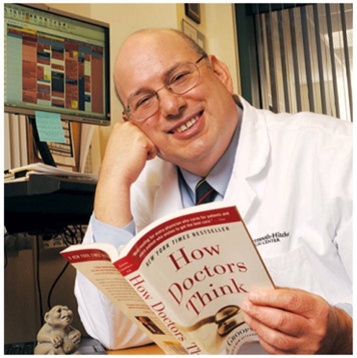
Wilson Schooler led to this.
What ***else*** can we find?

Post-study

- In the c ok 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

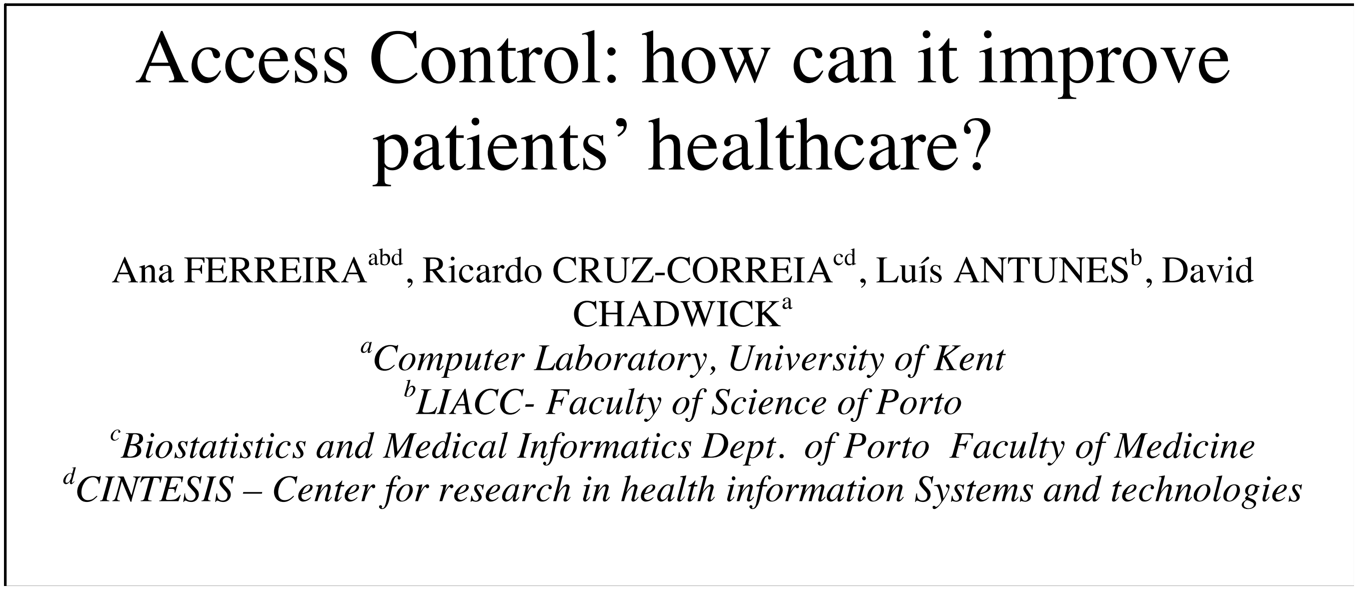
Yifei Wang



Andrew Gettinger, MD

Approach

ght these settings be too constraining?



Access Control: how can it improve patients' healthcare?

Ana FERREIRA[abd], Ricardo CRUZ-CORREIA[cd], Luís ANTUNES[b], David CHADWICK[a]

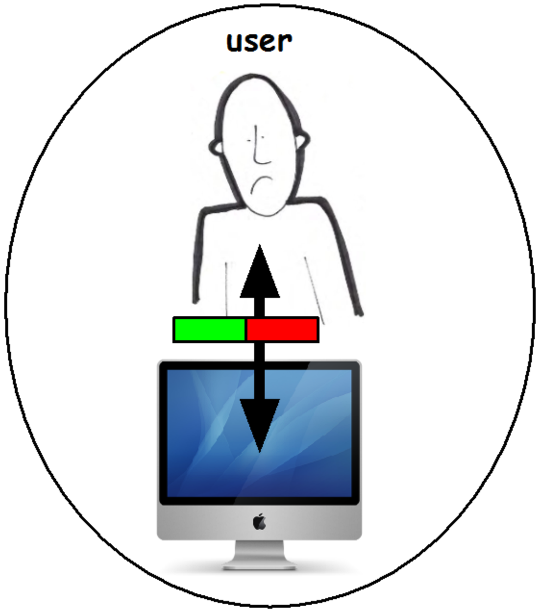
[a]Computer Laboratory, University of Kent
[b]LIACC- Faculty of Science of Porto
[c]Biostatistics and Medical Informatics Dept. of Porto Faculty of Medicine
[d]CINTESIS – Center for research in health information Systems and technologies

Doing Unto Future Selves As You Would Do Unto Others: Psychological Distance and Decision Making

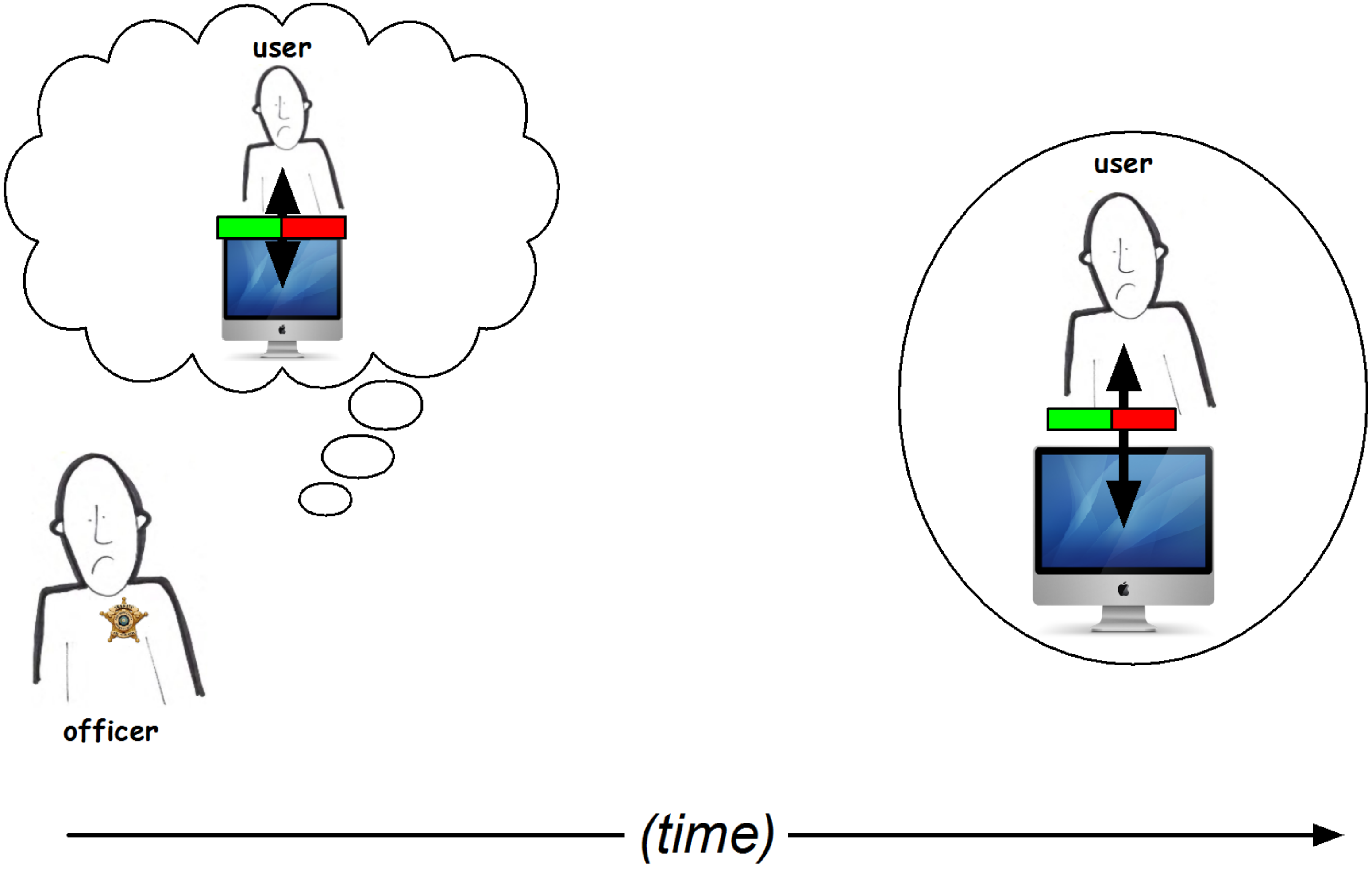
Emily Pronin
Christopher Y. Olivola
Kathleen A. Kennedy
Princeton University

Keywords: *self–other; decision making; temporal distance; future self; empathy gap; temporal discounting*

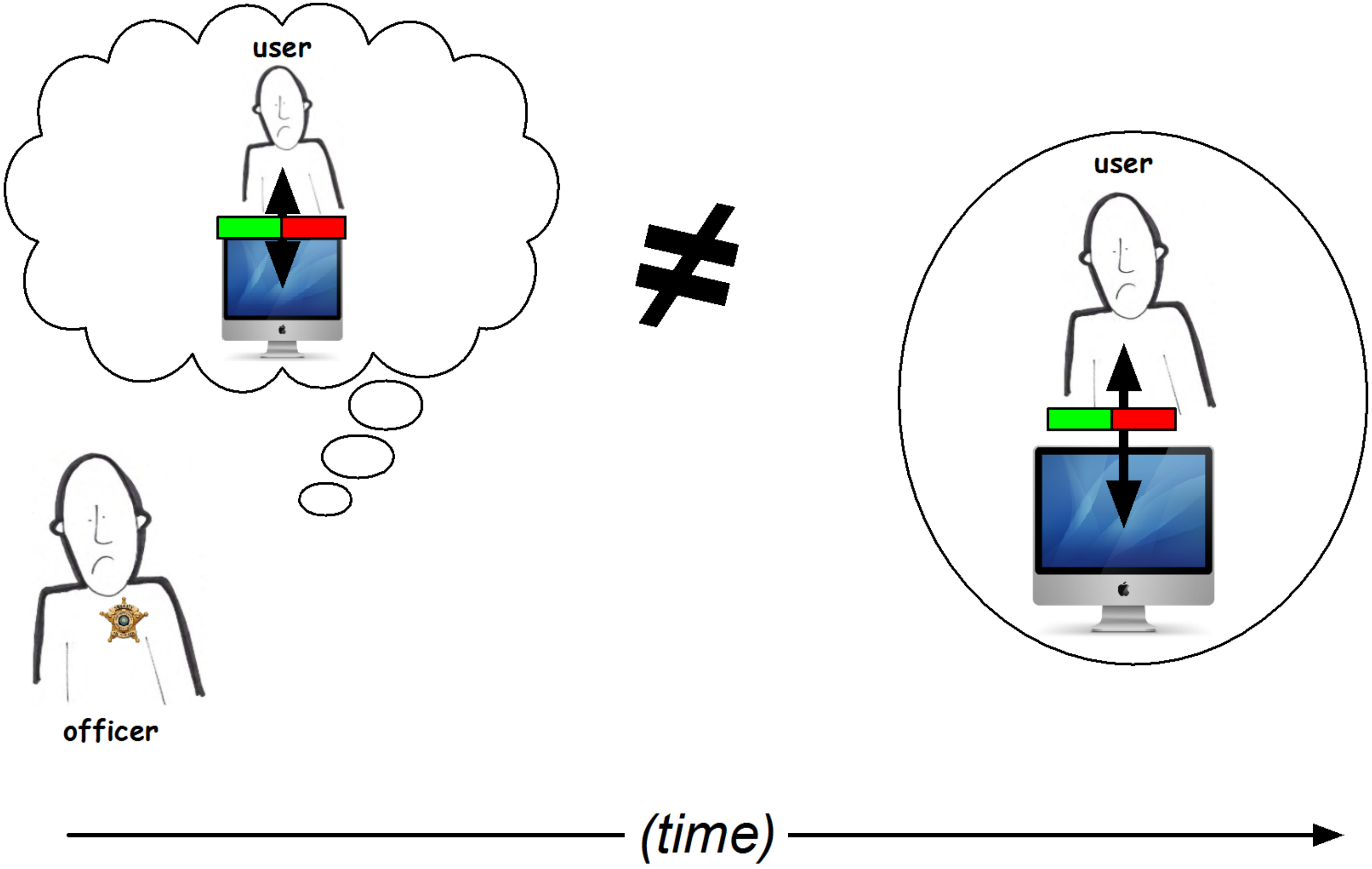
The Empathy Gap



The Empathy Gap

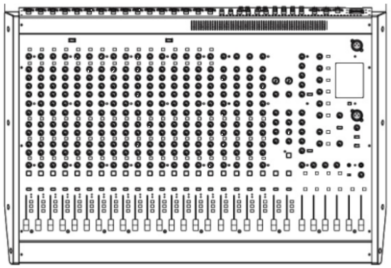


The Empathy Gap



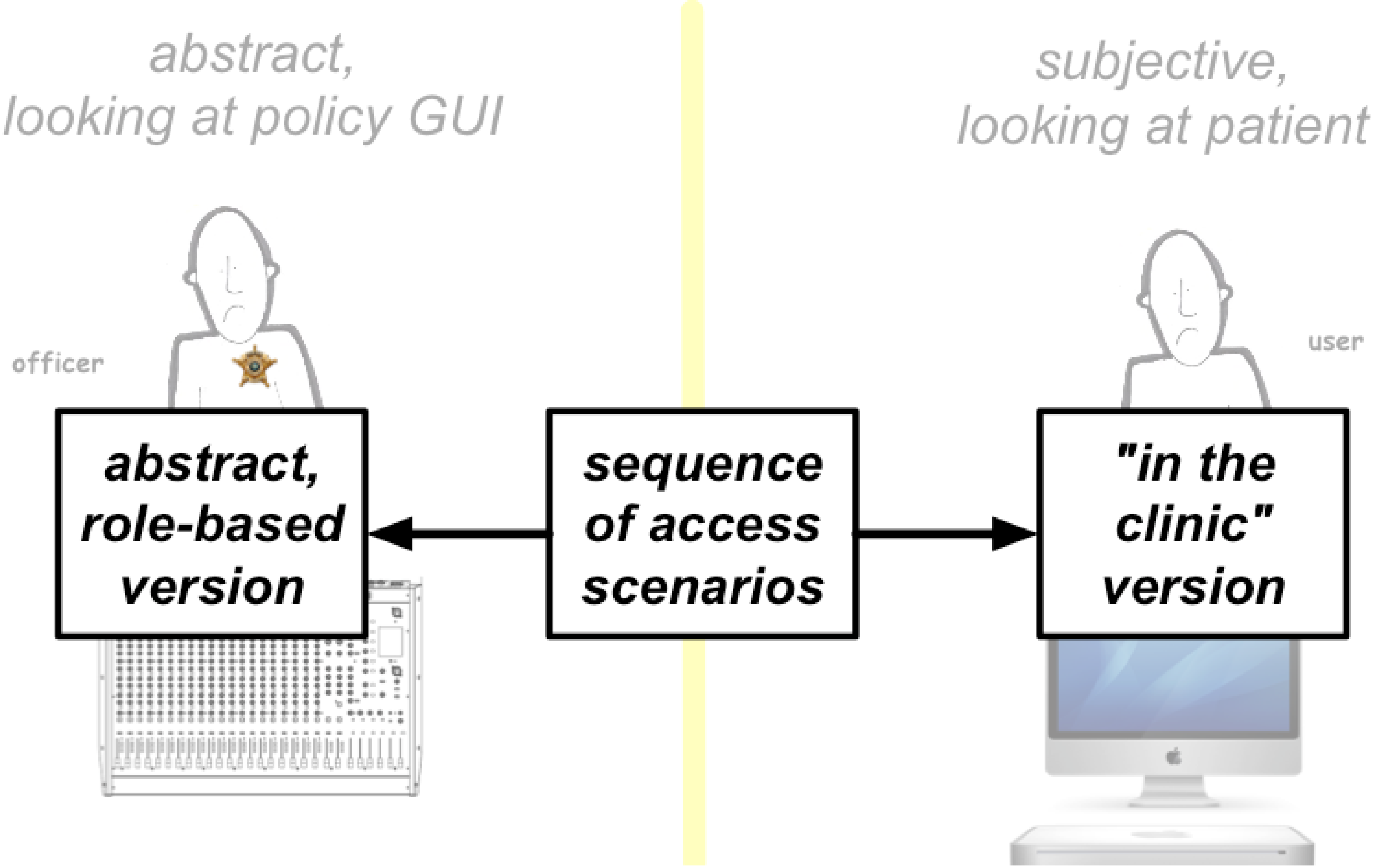
Experiment

abstract,
looking at policy GUI



subjective,
looking at patient

Experiment



abstract,
looking at policy GUI

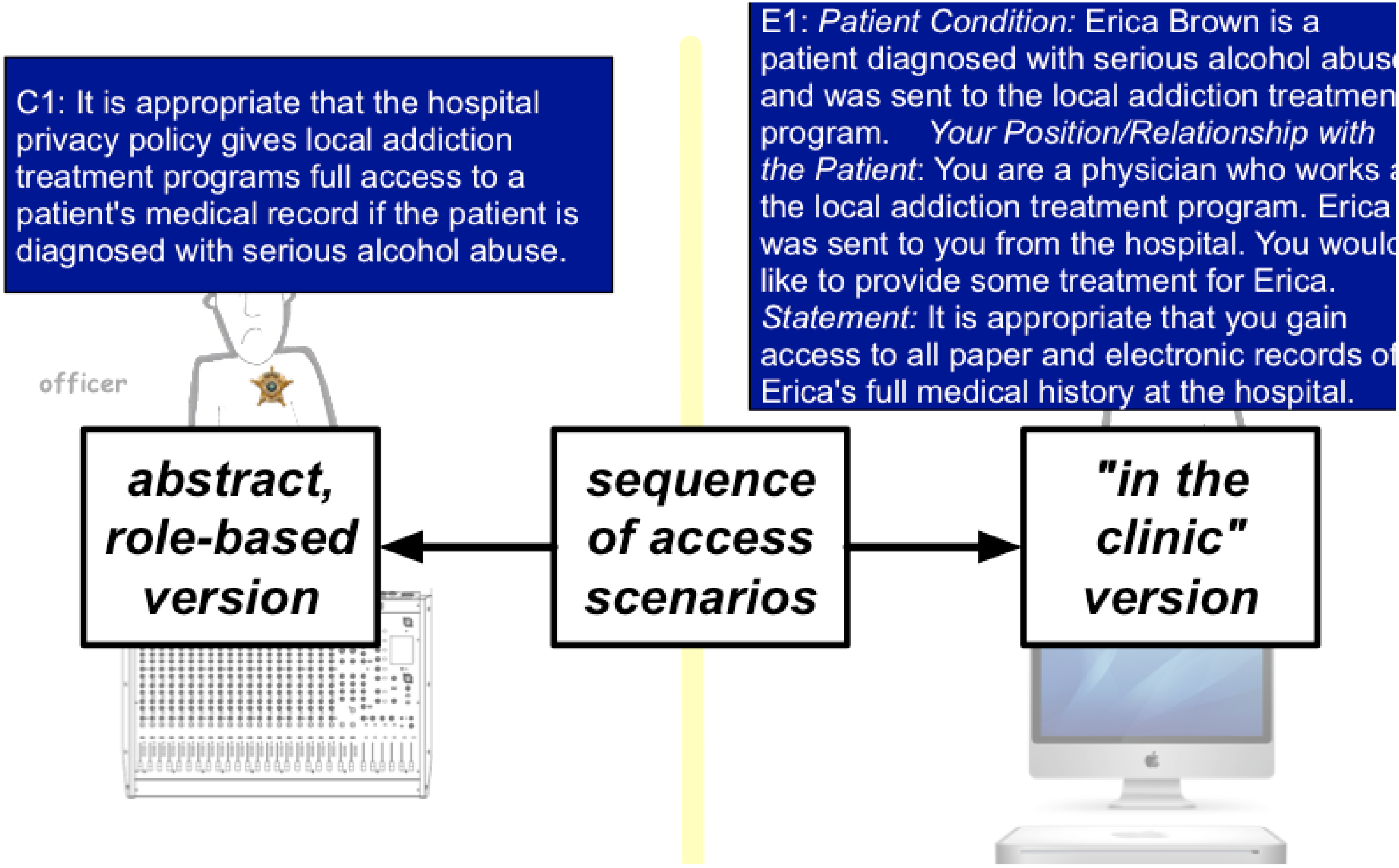
subjective,
looking at patient

abstract, role-based version

sequence of access scenarios

"in the clinic" version

Experiment

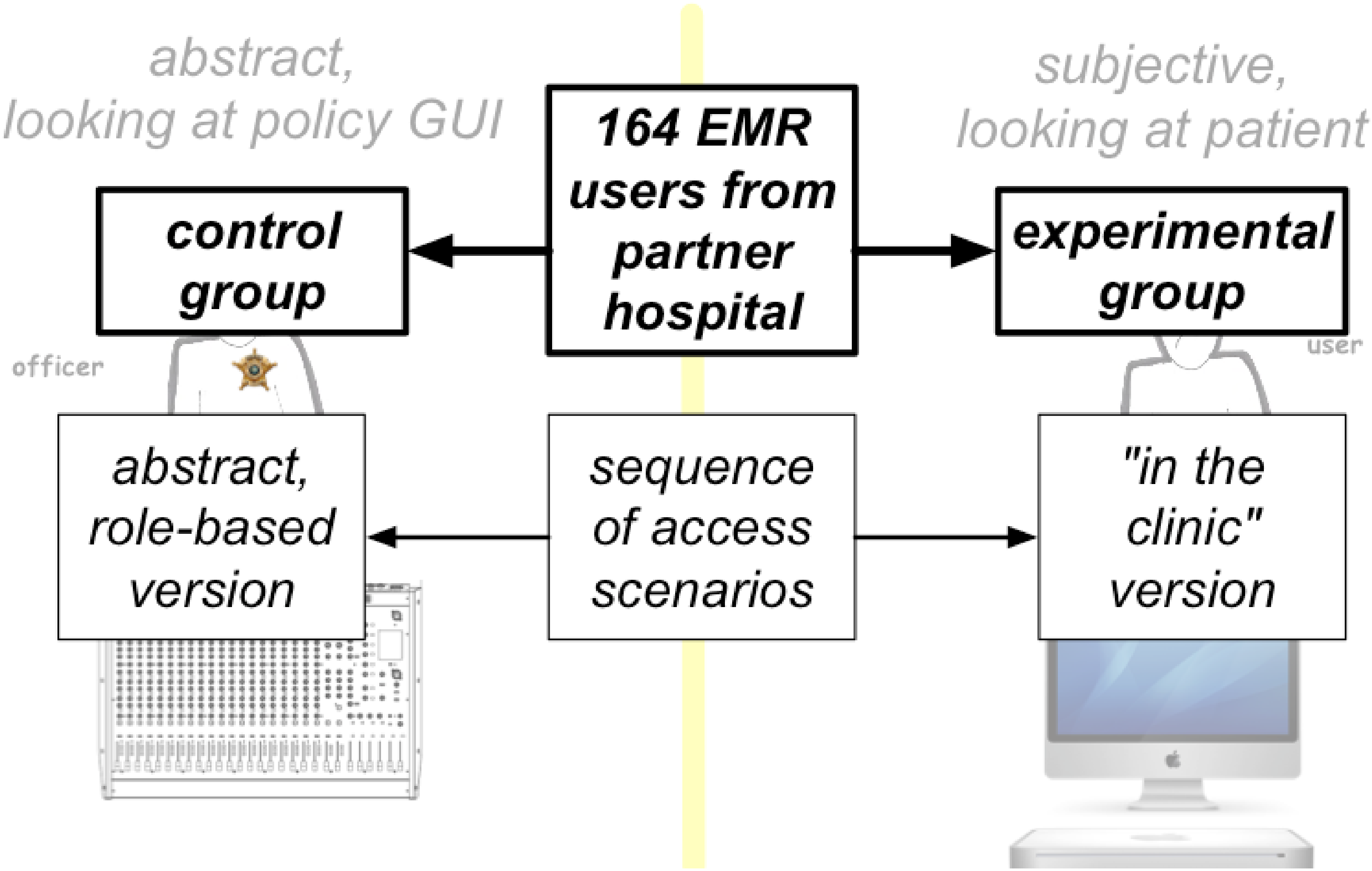


C1: It is appropriate that the hospital privacy policy gives local addiction treatment programs full access to a patient's medical record if the patient is diagnosed with serious alcohol abuse.

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

officer
abstract, role-based version
sequence of access scenarios
"in the clinic" version

Experiment



abstract, looking at policy GUI

subjective, looking at patient

164 EMR users from partner hospital

control group

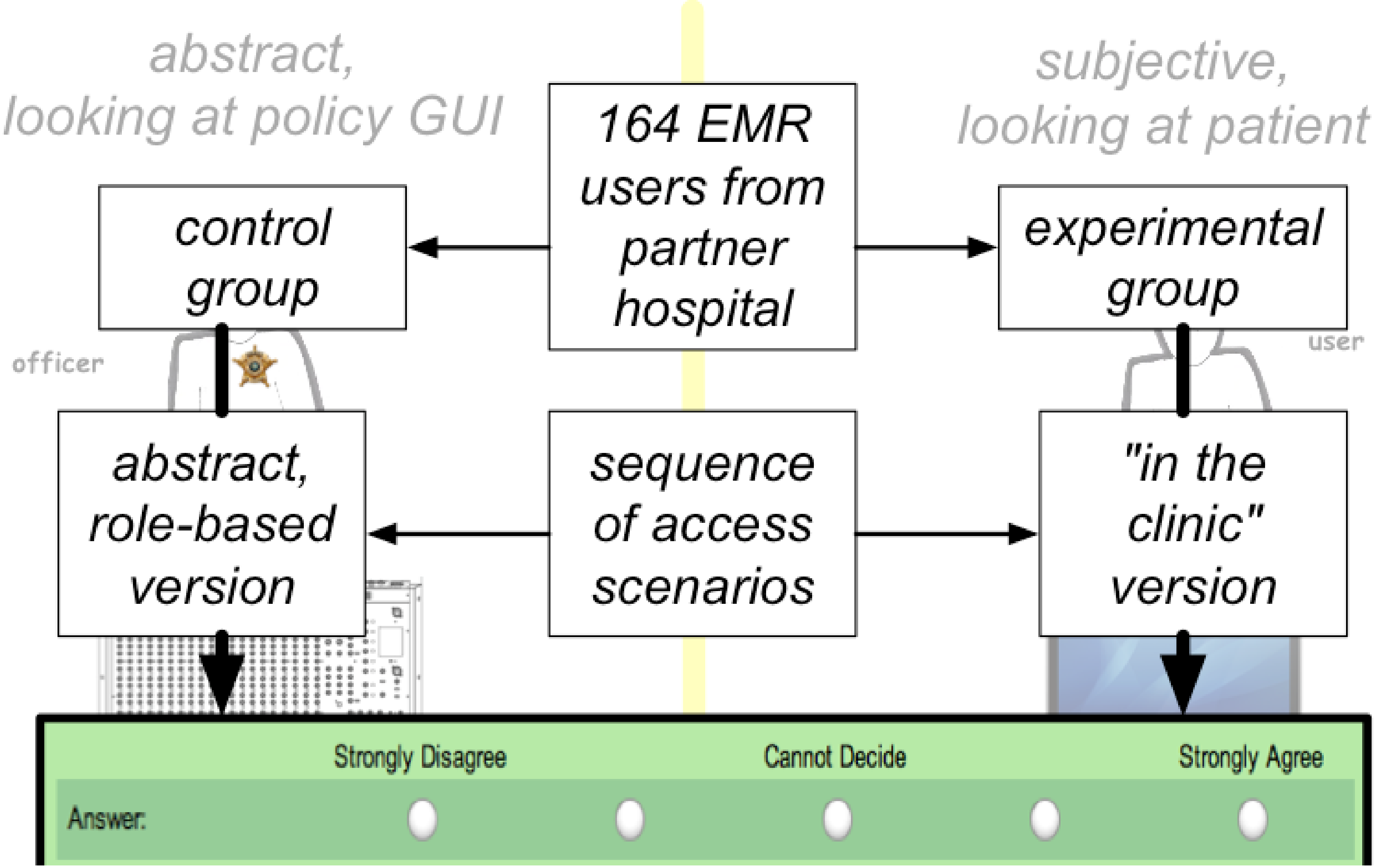
experimental group

abstract, role-based version

sequence of access scenarios

"in the clinic" version

Experiment



abstract, looking at policy GUI

subjective, looking at patient

164 EMR users from partner hospital

control group

experimental group

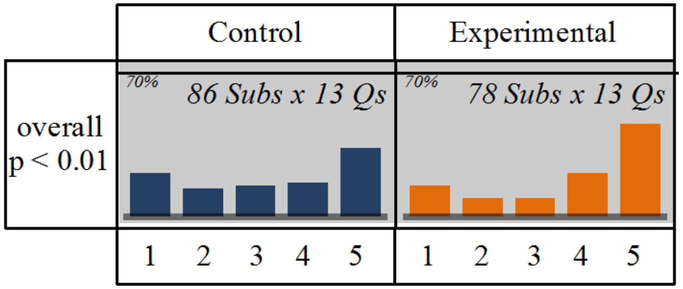
abstract, role-based version

sequence of access scenarios

"in the clinic" version

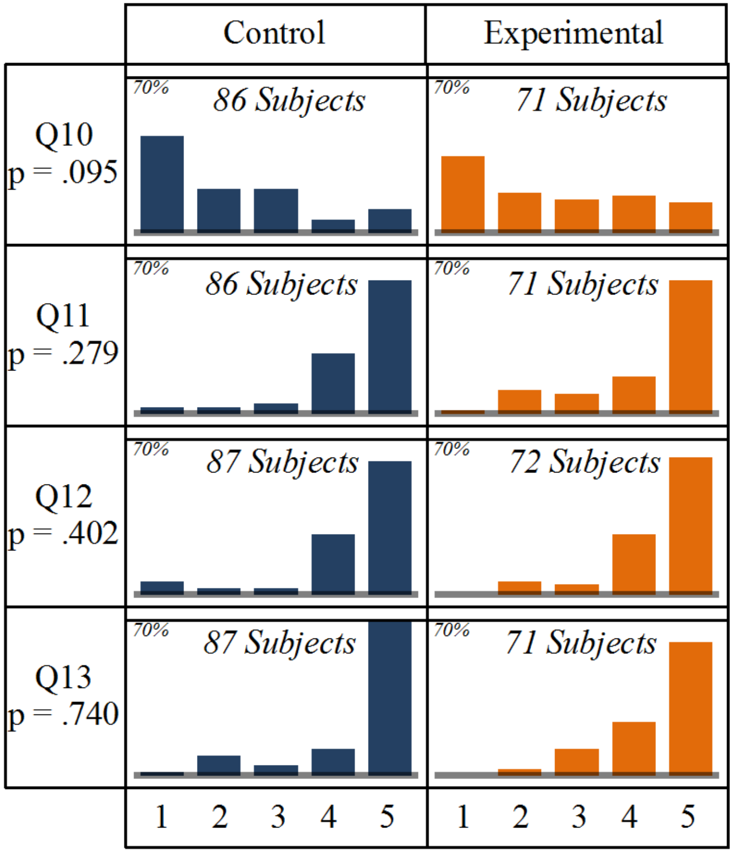
	Strongly Disagree		Cannot Decide		Strongly Agree
Answer:	○	○	○	○	○

Results



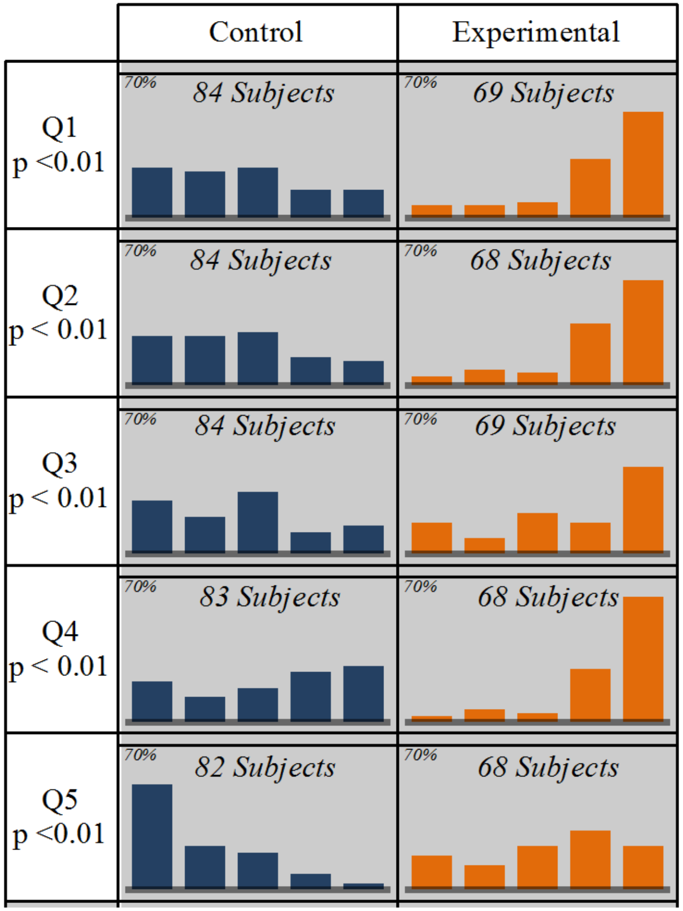
*overall: the groups **differed** significantly*

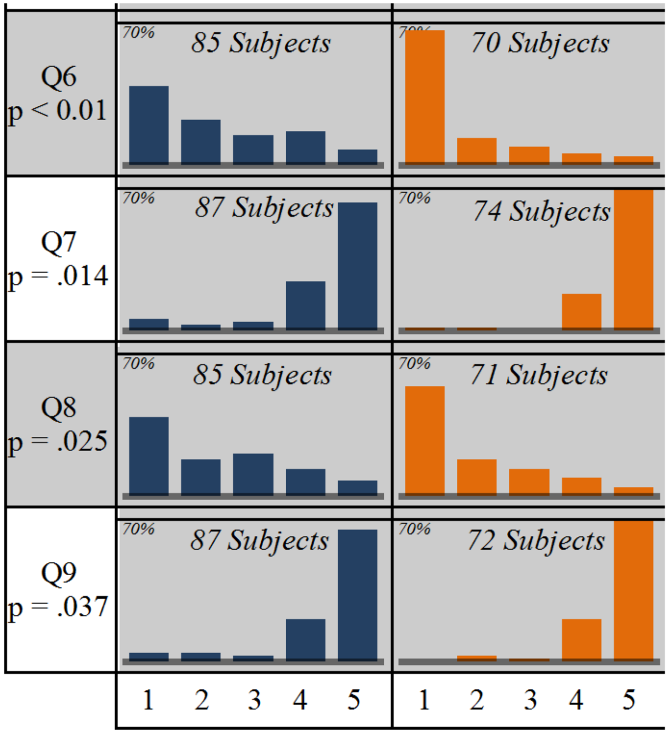
Results



*scenarios with **no** significant difference*

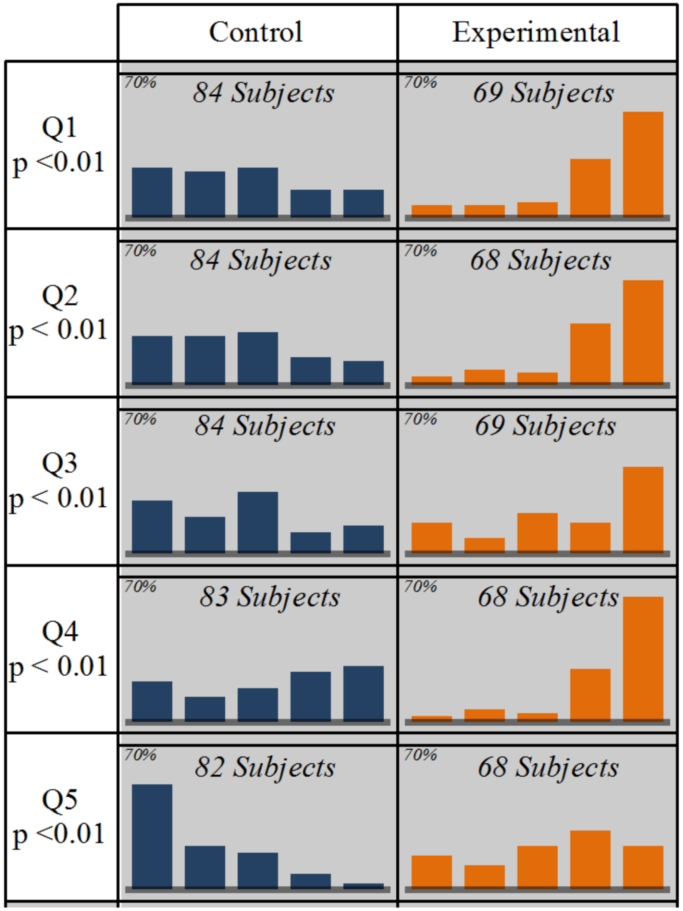
Results

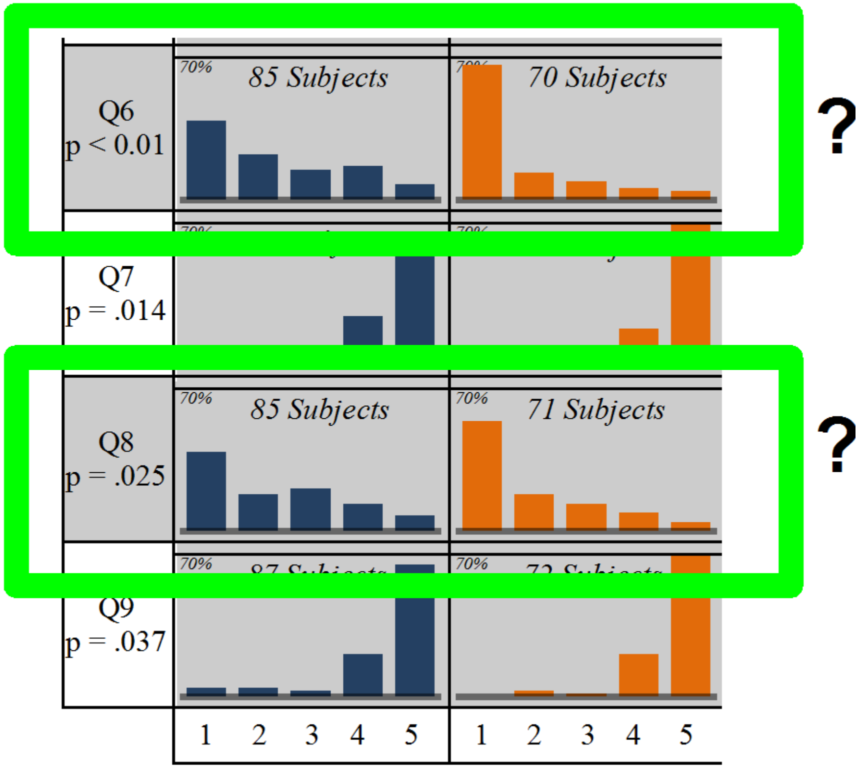




*scenarios where the groups **<u>differed</u>** significantly*

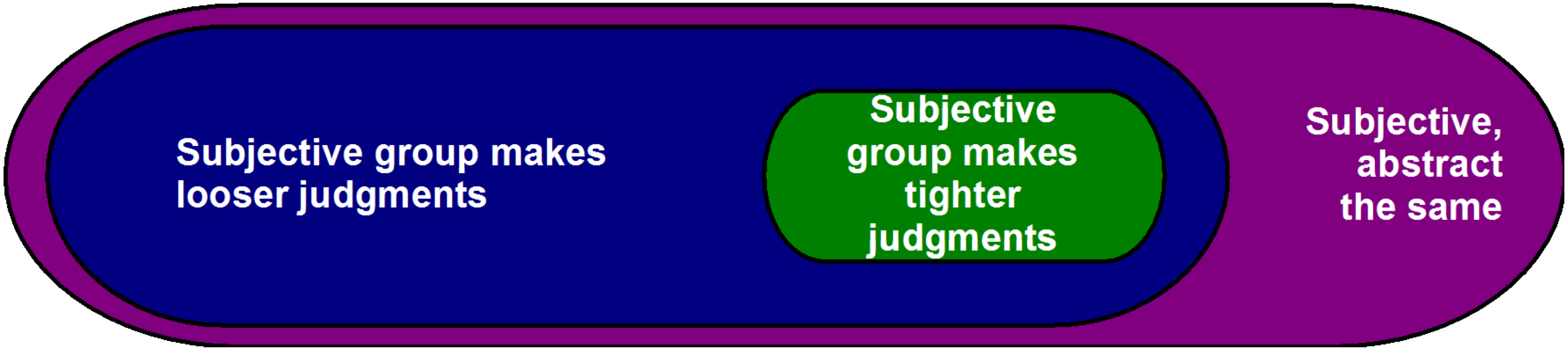
Results





*scenarios where the groups **differed** significantly*

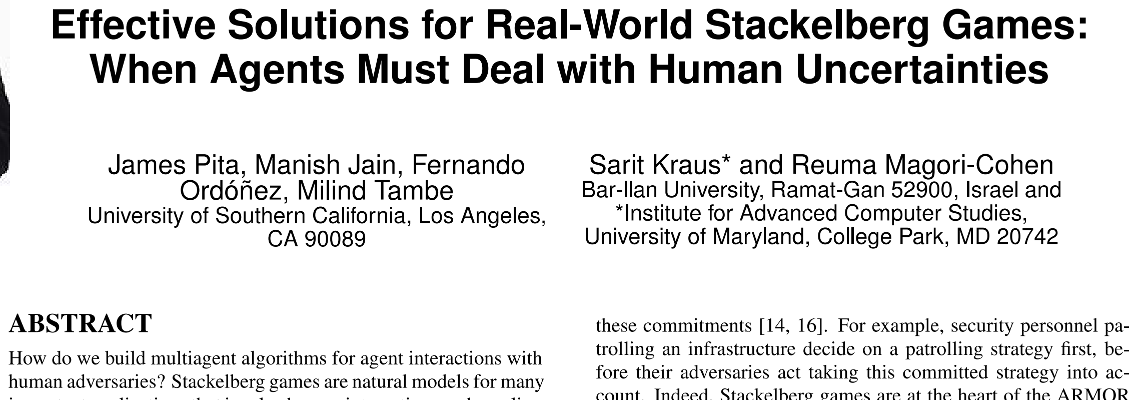
Partition of Scenarios


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

Implications

- 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.
- If tighter policies are "correct", then these are areas to look for circumvention (or to emphasize in training).
- If looser policies are "correct", then these are areas to reconsider policy.

Some other results



Effective Solutions for Real-World Stackelberg Games: When Agents Must Deal with Human Uncertainties

James Pita, Manish Jain, Fernando Ordóñez, Milind Tambe
University of Southern California, Los Angeles, CA 90089

Sarit Kraus* and Reuma Magori-Cohen
Bar-Ilan University, Ramat-Gan 52900, Israel and
*Institute for Advanced Computer Studies,
University of Maryland, College Park, MD 20742

ABSTRACT

How do we build multiagent algorithms for agent interactions with human adversaries? Stackelberg games are natural models for many

these commitments [14, 16]. For example, security personnel patrolling an infrastructure decide on a patrolling strategy first, before their adversaries act taking this committed strategy into account. Indeed, Stackelberg games are at the heart of the ARMOR

Cognitive Bias and Security

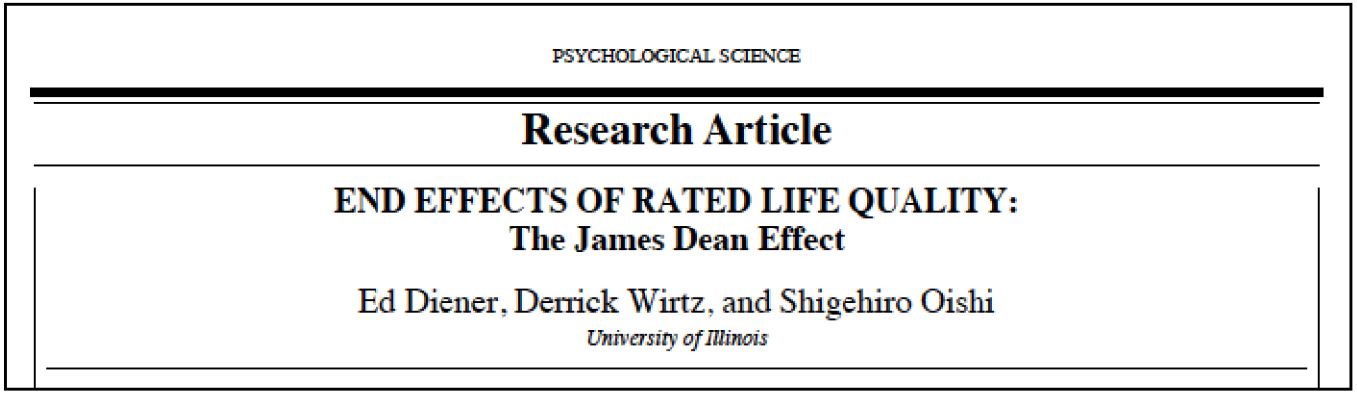
4. New Places to Try It

Cognitive Bias and Security

4. N ry It

jpg

The Peak-End Bias



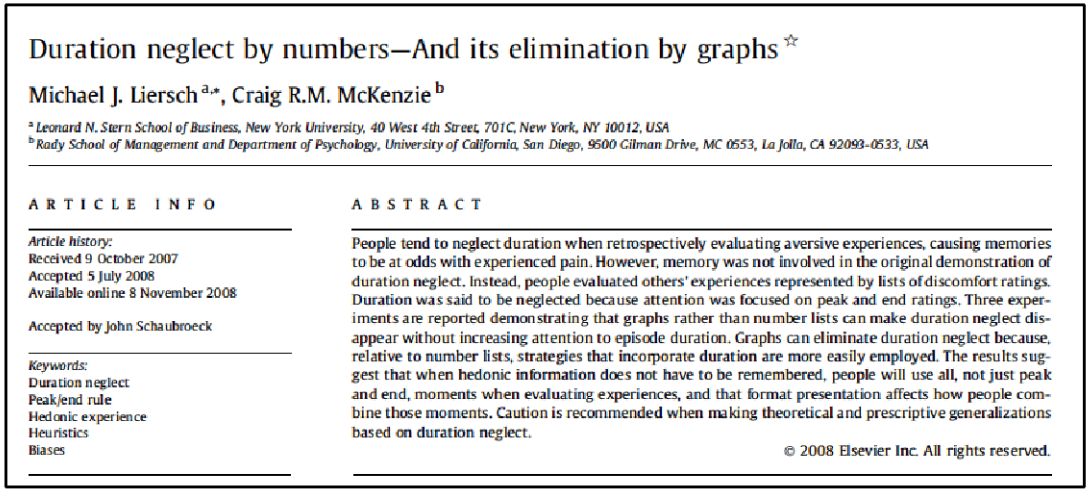
PSYCHOLOGICAL SCIENCE

Research Article

END EFFECTS OF RATED LIFE QUALITY:
The James Dean Effect

Ed Diener, Derrick Wirtz, and Shigehiro Oishi

University of Illinois



Duration neglect by numbers—And its elimination by graphs ☆

Michael J. Liersch[a,*], Craig R.M. McKenzie[b]

[a] *Leonard N. Stern School of Business, New York University, 40 West 4th Street, 701C, New York, NY 10012, USA*
[b] *Rady School of Management and Department of Psychology, University of California, San Diego, 9500 Gilman Drive, MC 0553, La Jolla, CA 92093-0533, USA*

ARTICLE INFO

Article history:
Received 9 October 2007
Accepted 5 July 2008
Available online 8 November 2008

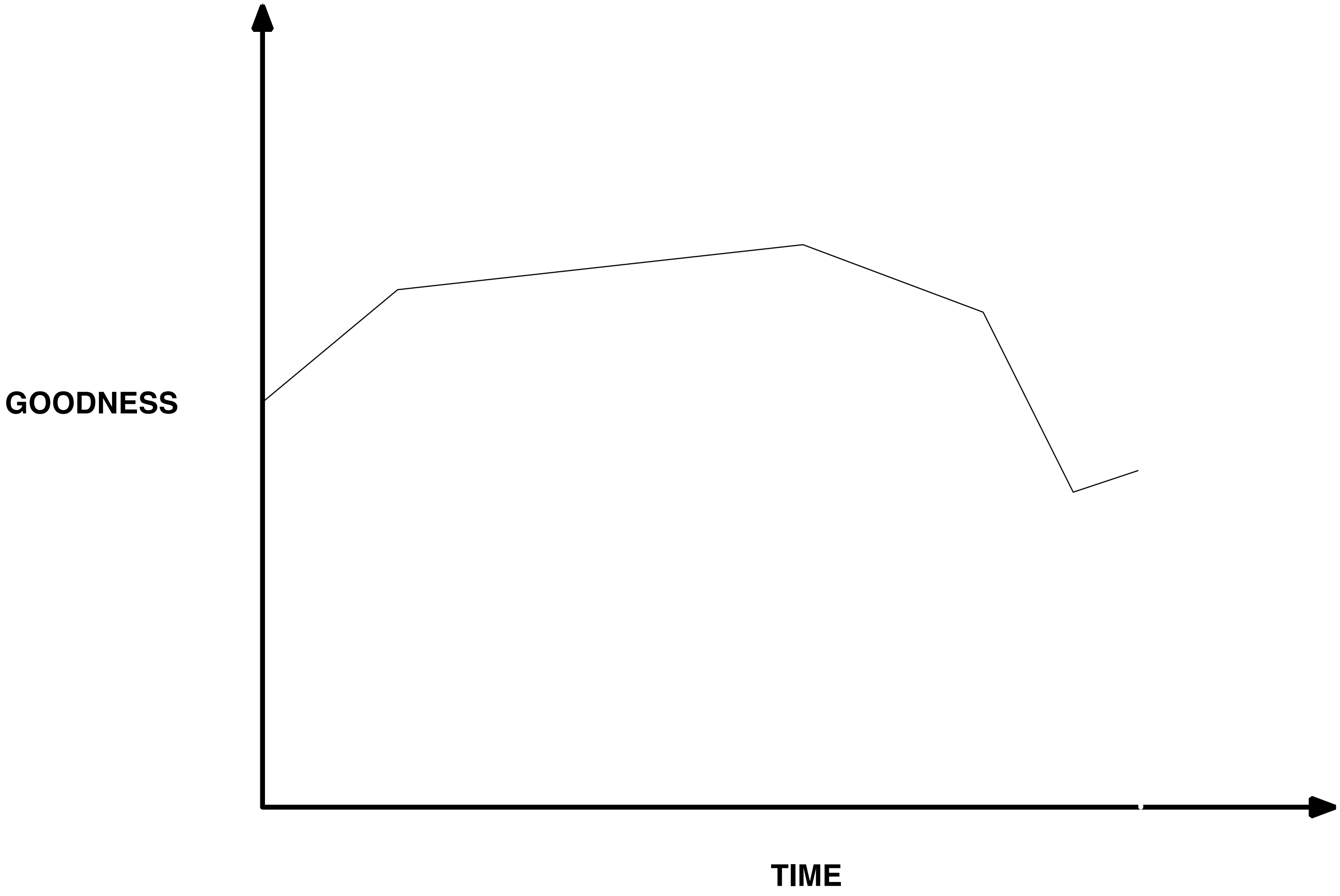
Accepted by John Schaubroeck

Keywords:
Duration neglect
Peak/end rule
Hedonic experience
Heuristics
Biases

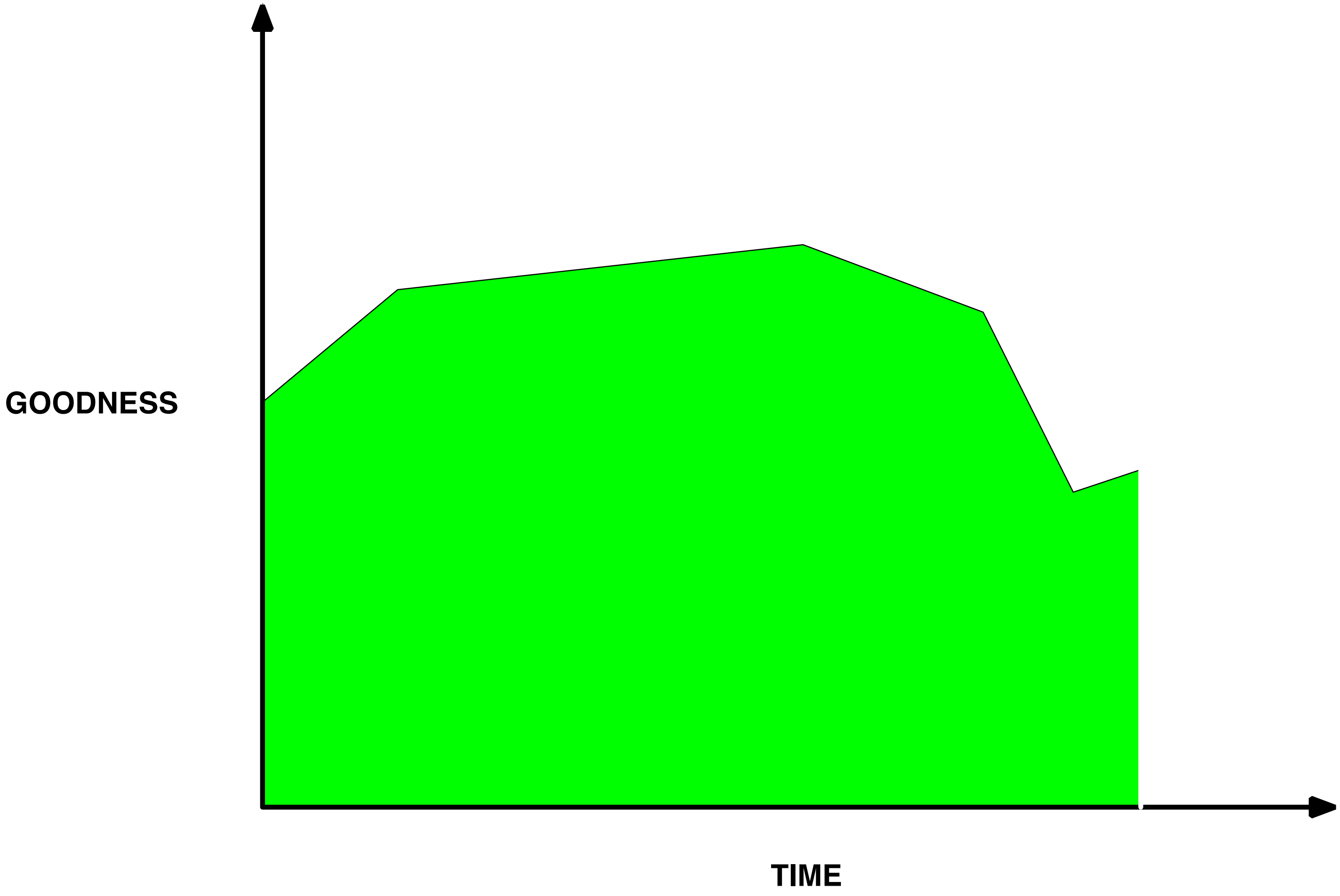
ABSTRACT

People tend to neglect duration when retrospectively evaluating aversive experiences, causing memories to be at odds with experienced pain. However, memory was not involved in the original demonstration of duration neglect. Instead, people evaluated others' experiences represented by lists of discomfort ratings. Duration was said to be neglected because attention was focused on peak and end ratings. Three experiments are reported demonstrating that graphs rather than number lists can make duration neglect disappear without increasing attention to episode duration. Graphs can eliminate duration neglect because, relative to number lists, strategies that incorporate duration are more easily employed. The results suggest that when hedonic information does not have to be remembered, people will use all, not just peak and end, moments when evaluating experiences, and that format presentation affects how people combine those moments. Caution is recommended when making theoretical and prescriptive generalizations based on duration neglect.

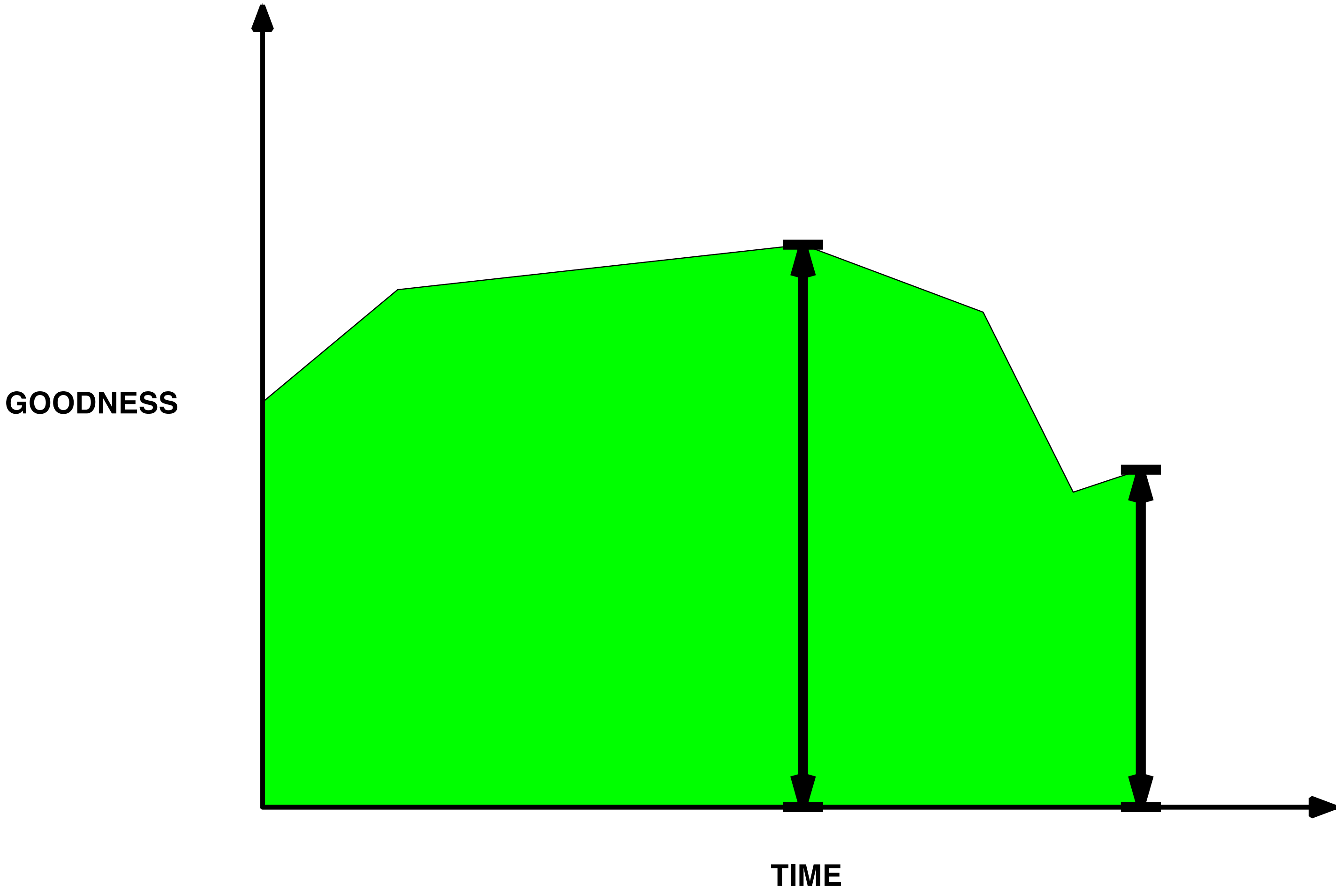
The Peak-End Bias



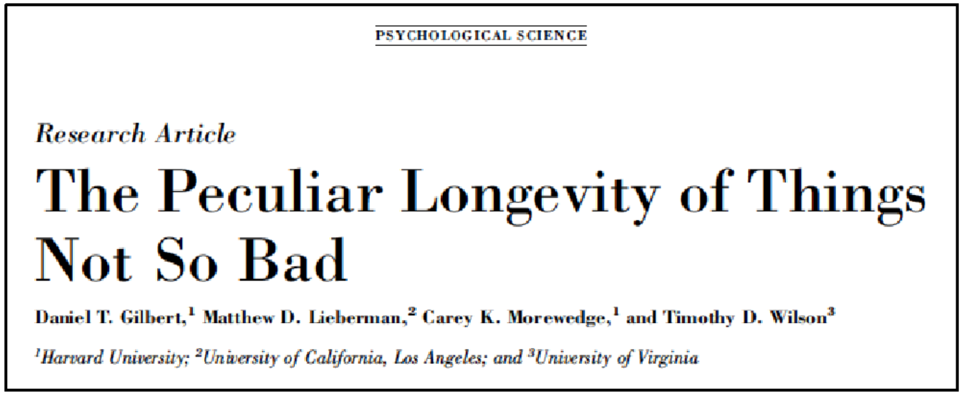
The Peak-End Bias



The Peak-End Bias



Immune Neglect



PSYCHOLOGICAL SCIENCE

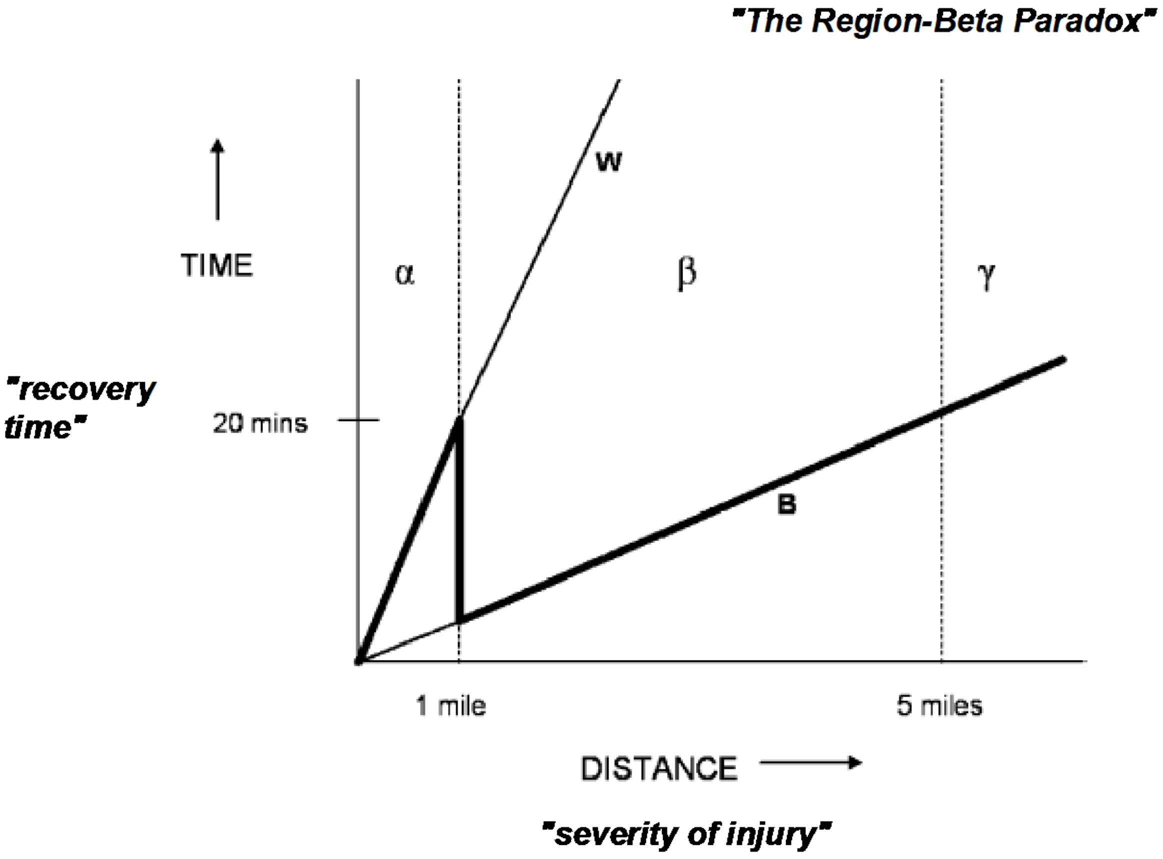
Research Article

The Peculiar Longevity of Things Not So Bad

Daniel T. Gilbert,[1] Matthew D. Lieberman,[2] Carey K. Morewedge,[1] and Timothy D. Wilson[3]

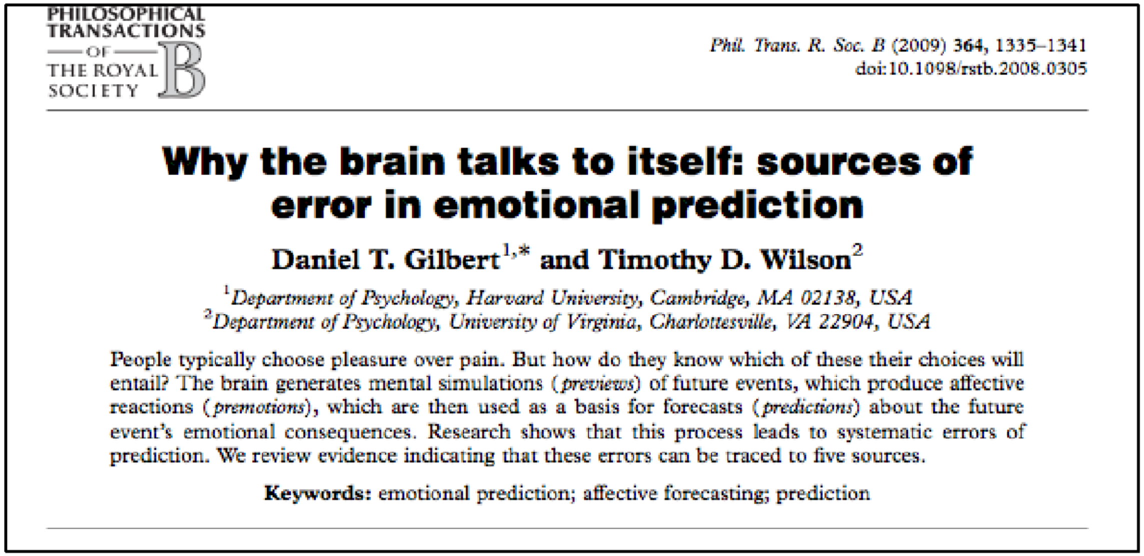
[1]Harvard University; [2]University of California, Los Angeles; and [3]University of Virginia

Immune Neglect



(from cited paper)

Preview-Based Forecasting



PHILOSOPHICAL
TRANSACTIONS
OF
THE ROYAL
SOCIETY
B

Phil. Trans. R. Soc. B (2009) **364**, 1335–1341
doi:10.1098/rstb.2008.0305

Why the brain talks to itself: sources of error in emotional prediction

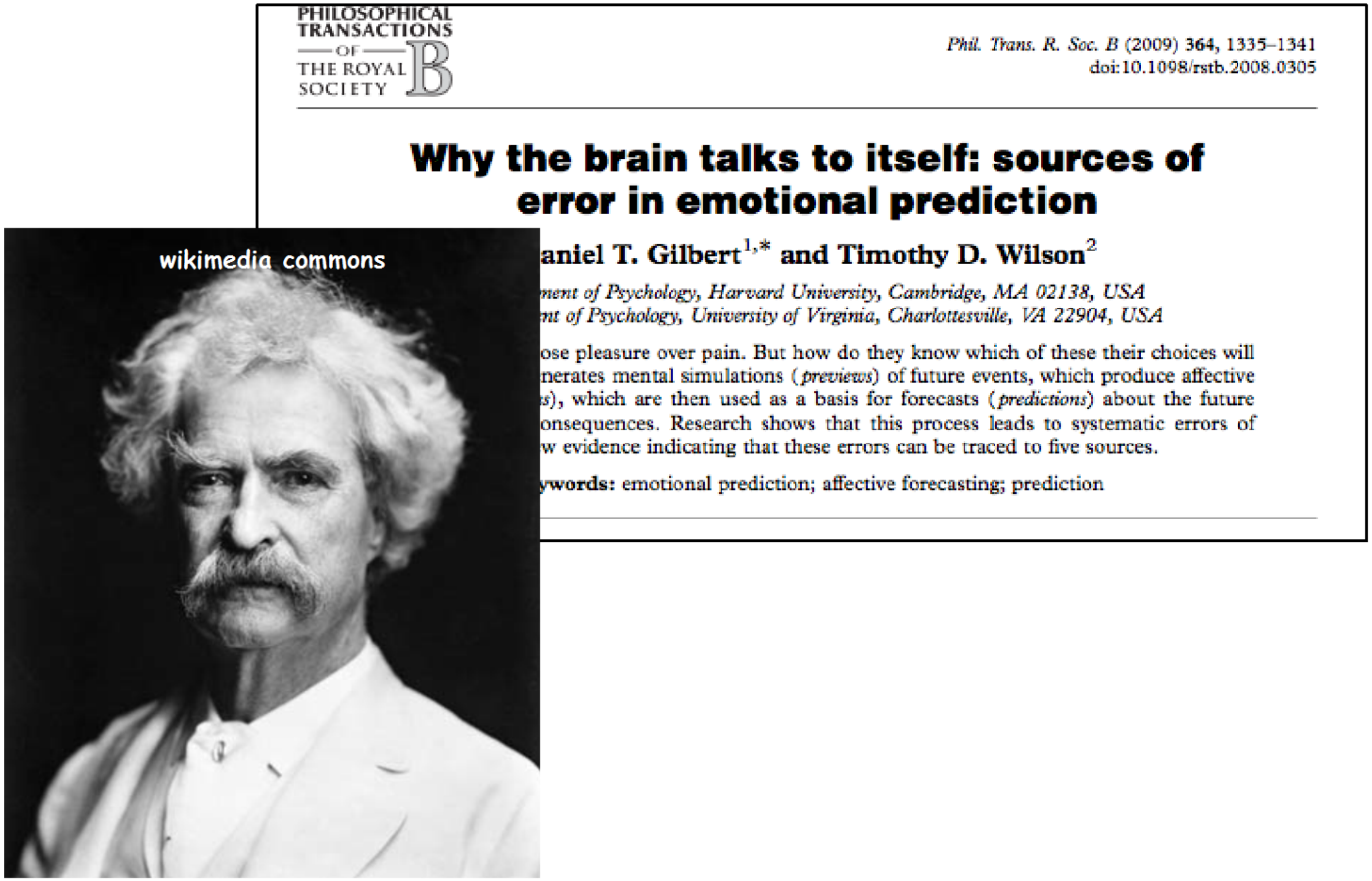
Daniel T. Gilbert[1,*] and Timothy D. Wilson[2]

[1] *Department of Psychology, Harvard University, Cambridge, MA 02138, USA*
[2] *Department of Psychology, University of Virginia, Charlottesville, VA 22904, USA*

People typically choose pleasure over pain. But how do they know which of these their choices will entail? The brain generates mental simulations (*previews*) of future events, which produce affective reactions (*premotions*), which are then used as a basis for forecasts (*predictions*) about the future event's emotional consequences. Research shows that this process leads to systematic errors of prediction. We review evidence indicating that these errors can be traced to five sources.

Keywords: emotional prediction; affective forecasting; prediction

Preview-Based Forecasting



PHILOSOPHICAL
TRANSACTIONS
OF
THE ROYAL
SOCIETY
B

Phil. Trans. R. Soc. B (2009) **364**, 1335–1341
doi:10.1098/rstb.2008.0305

Why the brain talks to itself: sources of error in emotional prediction

aniel T. Gilbert[1,*] and Timothy D. Wilson[2]

nent of Psychology, Harvard University, Cambridge, MA 02138, USA
nt of Psychology, University of Virginia, Charlottesville, VA 22904, USA

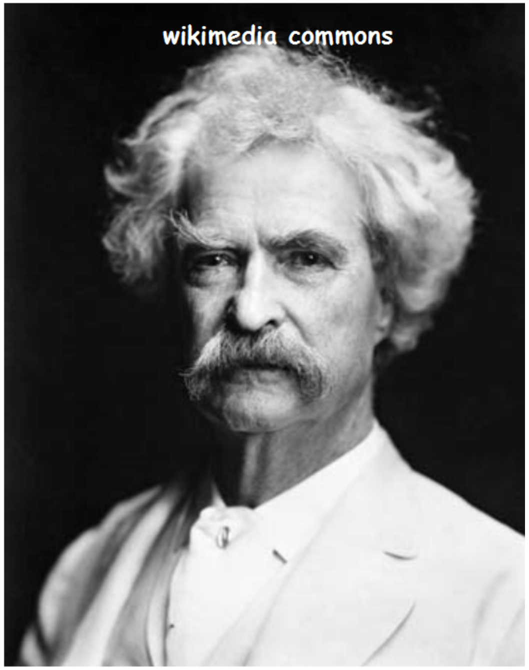
ose pleasure over pain. But how do they know which of these their choices will
nerates mental simulations (*previews*) of future events, which produce affective
s), which are then used as a basis for forecasts (*predictions*) about the future
onsequences. Research shows that this process leads to systematic errors of
w evidence indicating that these errors can be traced to five sources.

ywords: emotional prediction; affective forecasting; prediction

wikimedia commons

Preview-Based Forecasting

- "The problem of dissimilar content"
- "Previews are unrepresentative"
- "Previews are essentialized"
- "Previews are truncated"
- "Previews are comparative"
- "The problem of dissimilar context"


wikimedia commons

Preview-Based Forecasting

Does the security policy problem fit into the framework of preview-based affective forecast?

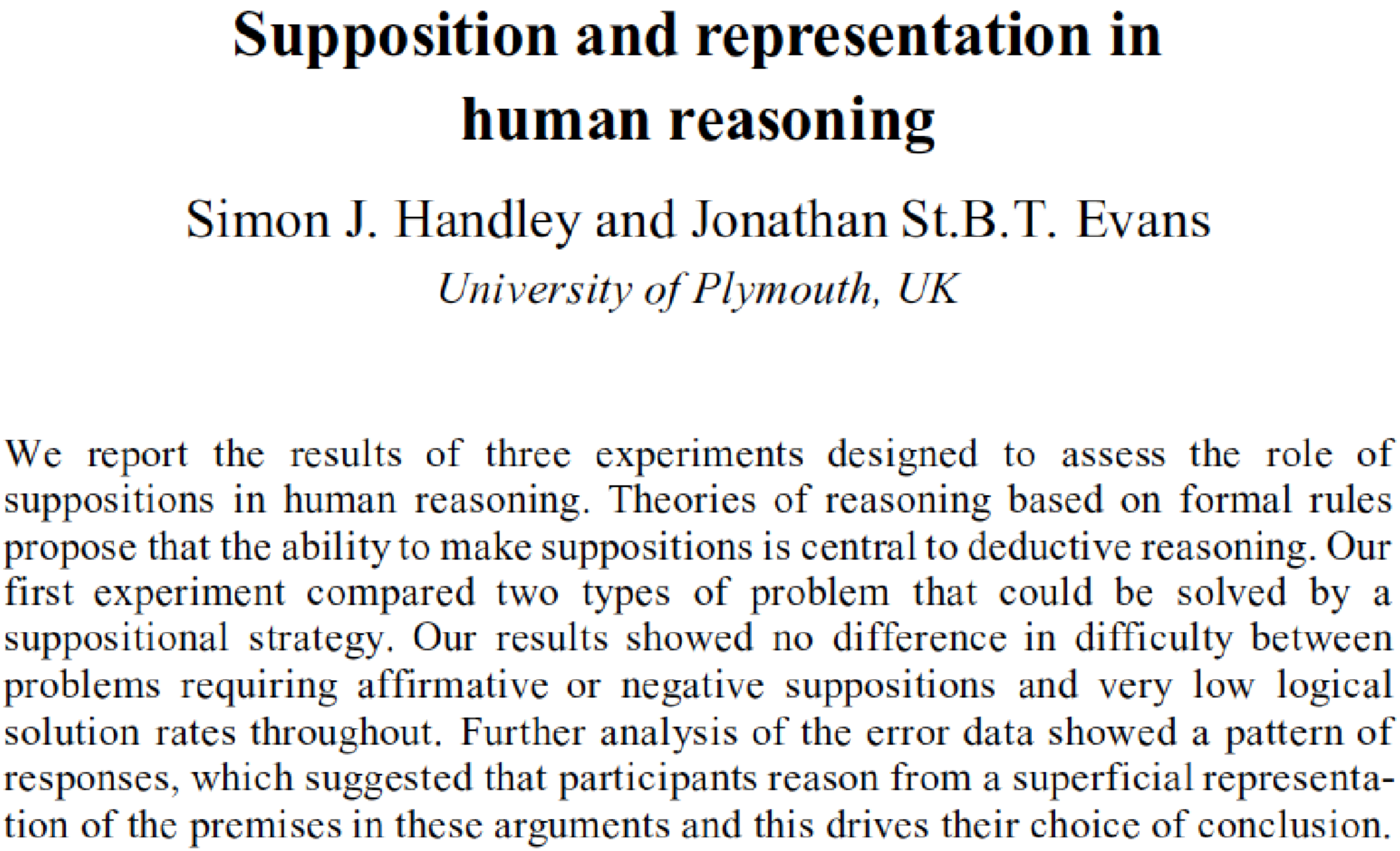
Can we figure out ways to make previews:

- more representative
- less essentialized
- less truncated
- less comparative
- be based on more similar context?

Or should we encourage these biases?

What if we tried distracting (or enhancing) the resources required for the relevant mind process?

Infernal Internal Logic



Supposition and representation in human reasoning

Simon J. Handley and Jonathan St.B.T. Evans

University of Plymouth, UK

We report the results of three experiments designed to assess the role of suppositions in human reasoning. Theories of reasoning based on formal rules propose that the ability to make suppositions is central to deductive reasoning. Our first experiment compared two types of problem that could be solved by a suppositional strategy. Our results showed no difference in difficulty between problems requiring affirmative or negative suppositions and very low logical solution rates throughout. Further analysis of the error data showed a pattern of responses, which suggested that participants reason from a superficial representation of the premises in these arguments and this drives their choice of conclusion.

Infernal Internal Logic

LOGICAL ERRORS

We might look at complex access control systems (such as Reeder/Cranor's experiments where subjects and objects could both be grouped and have both “allow” and “deny” rules) as analogous to logic; “Alice should be granted X” would be analogous to a conclusion in deductive reasoning. We can then ask whether the family of results regarding systematic errors in human logical reasoning (e.g. Handley and Evans 2000) have analogs in access control.

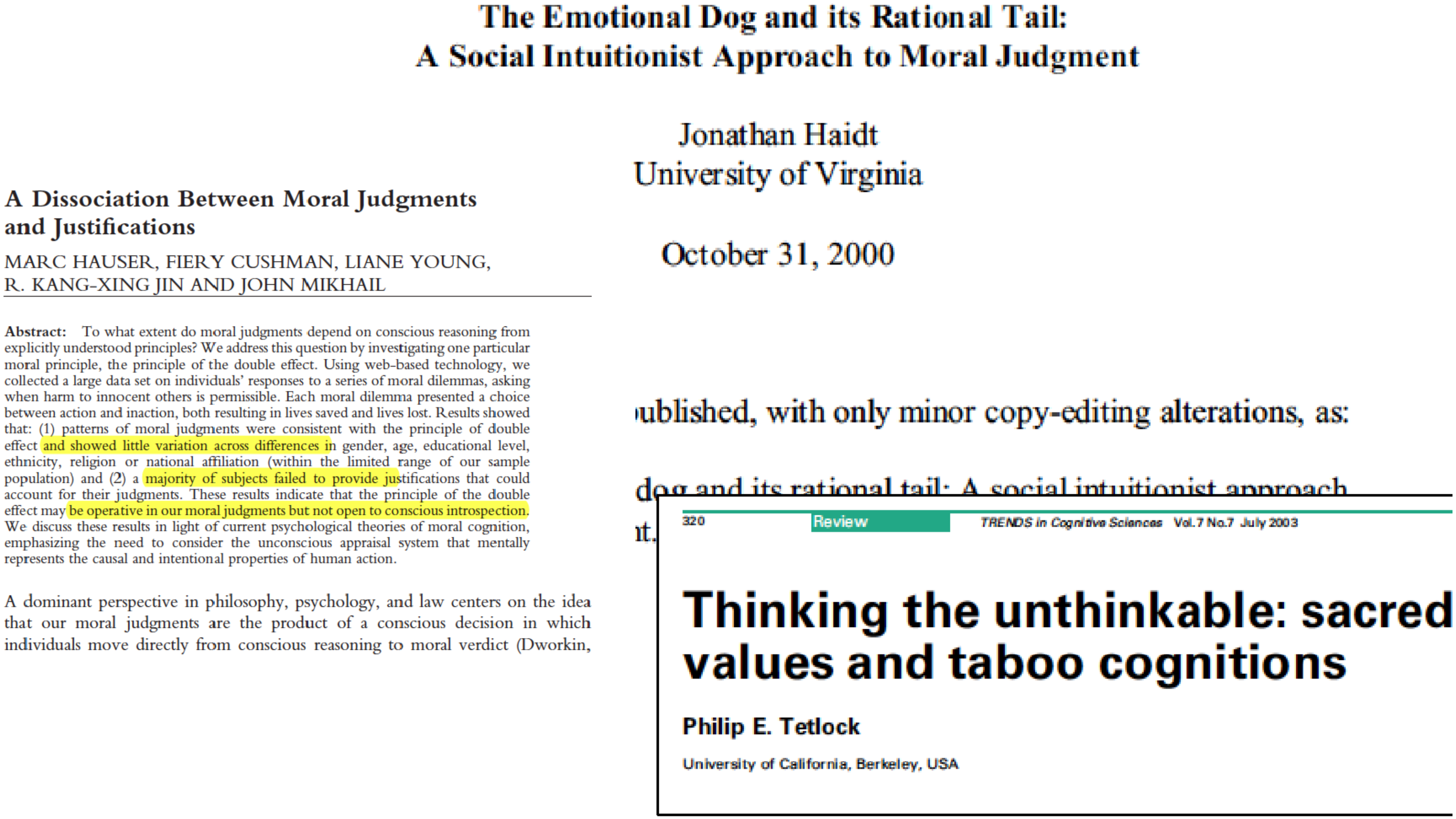
Do people targeting a particular behavior mis-set policy because they mis-read what conclusion follows from given premises—and does this correspond to the systematic errors psychology has already identified?

Do people get irate about an access control “mistake” or look in the wrong places when debugging because of belief bias?

Do programmers make mistakes in coding up security controls because of the reasons people have problems with the Wason selection problem? (It would be interesting to do a survey of the myriad security bugs due to failure of input validation, and see to what extent these sort of phenomenon—including confirmation bias—are manifested.)

Does the Handley/Evans "whole model" bias show up in any of our scenarios of interest?

Moral Cognition



The Emotional Dog and its Rational Tail: A Social Intuitionist Approach to Moral Judgment

Jonathan Haidt
University of Virginia

October 31, 2000

ublished, with only minor copy-editing alterations, as:

dog and its rational tail: A social intuitionist approach

it.

A Dissociation Between Moral Judgments and Justifications

MARC HAUSER, FIERY CUSHMAN, LIANE YOUNG,
R. KANG-XING JIN AND JOHN MIKHAIL

Abstract: To what extent do moral judgments depend on conscious reasoning from explicitly understood principles? We address this question by investigating one particular moral principle, the principle of the double effect. Using web-based technology, we collected a large data set on individuals' responses to a series of moral dilemmas, asking when harm to innocent others is permissible. Each moral dilemma presented a choice between action and inaction, both resulting in lives saved and lives lost. Results showed that: (1) patterns of moral judgments were consistent with the principle of double effect and showed little variation across differences in gender, age, educational level, ethnicity, religion or national affiliation (within the limited range of our sample population) and (2) a majority of subjects failed to provide justifications that could account for their judgments. These results indicate that the principle of the double effect may be operative in our moral judgments but not open to conscious introspection. We discuss these results in light of current psychological theories of moral cognition, emphasizing the need to consider the unconscious appraisal system that mentally represents the causal and intentional properties of human action.

A dominant perspective in philosophy, psychology, and law centers on the idea that our moral judgments are the product of a conscious decision in which individuals move directly from conscious reasoning to moral verdict (Dworkin,

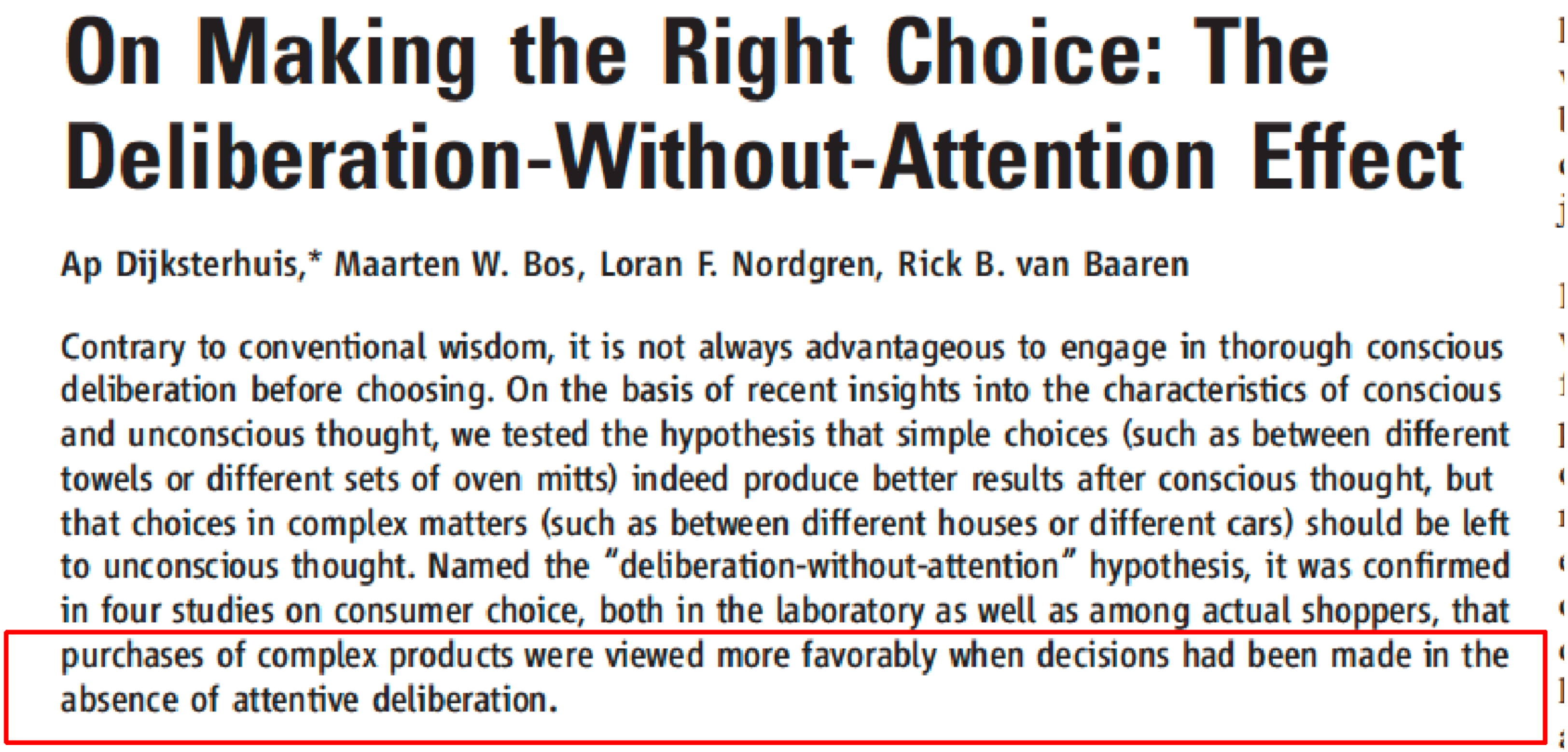
320 Review TRENDS in Cognitive Sciences Vol.7 No.7 July 2003

Thinking the unthinkable: sacred values and taboo cognitions

Philip E. Tetlock

University of California, Berkeley, USA

Moral Cognition

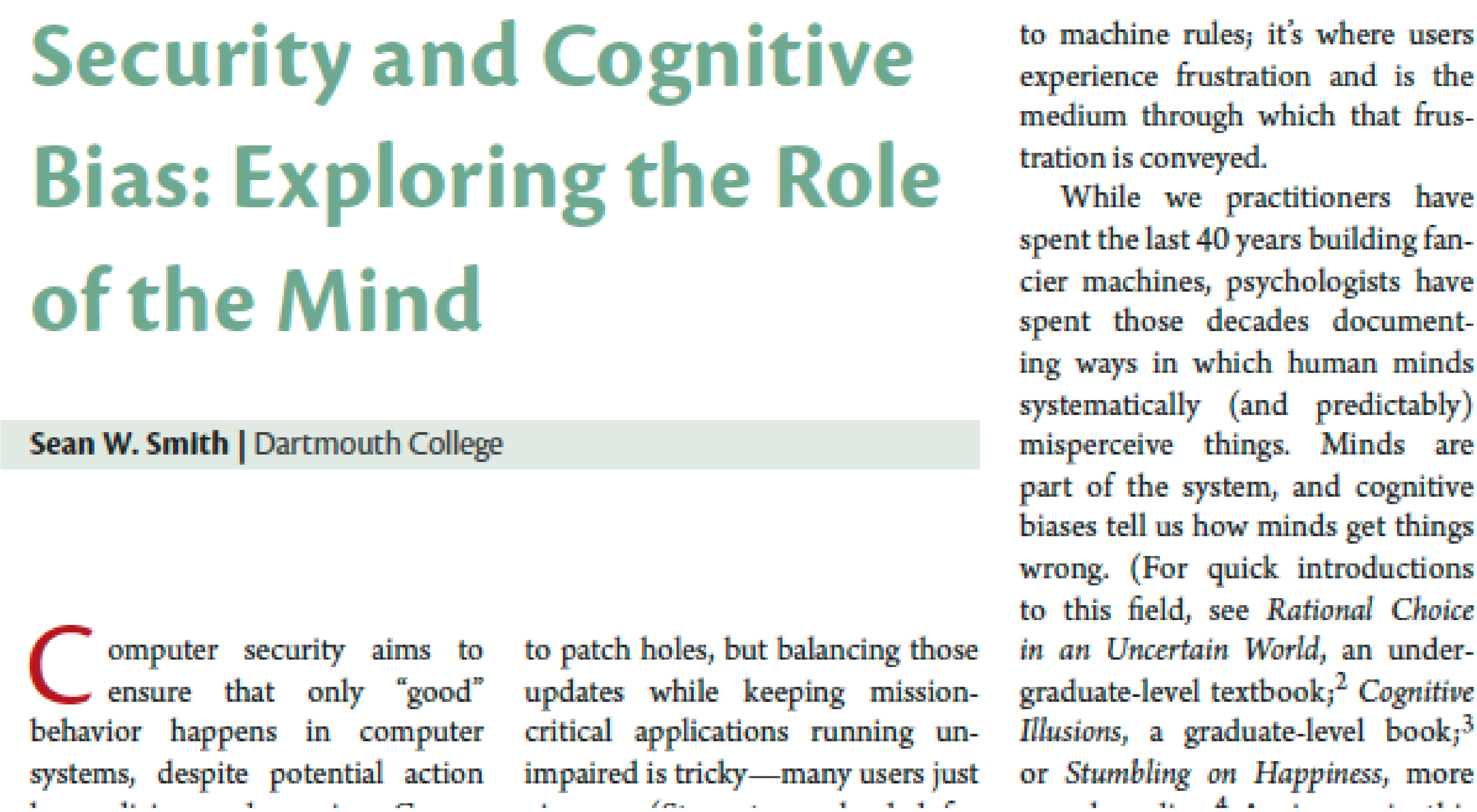


On Making the Right Choice: The Deliberation-Without-Attention Effect

Ap Dijksterhuis,* Maarten W. Bos, Loran F. Nordgren, Rick B. van Baaren

Contrary to conventional wisdom, it is not always advantageous to engage in thorough conscious deliberation before choosing. On the basis of recent insights into the characteristics of conscious and unconscious thought, we tested the hypothesis that simple choices (such as between different towels or different sets of oven mitts) indeed produce better results after conscious thought, but that choices in complex matters (such as between different houses or different cars) should be left to unconscious thought. Named the "deliberation-without-attention" hypothesis, it was confirmed in four studies on consumer choice, both in the laboratory as well as among actual shoppers, that purchases of complex products were viewed more favorably when decisions had been made in the absence of attentive deliberation.

Cognitive Bias and Security



Security and Cognitive Bias: Exploring the Role of the Mind

Sean W. Smith | Dartmouth College

Computer security aims to ensure that only "good" behavior happens in computer systems, despite potential action

to patch holes, but balancing those updates while keeping mission-critical applications running unimpaired is tricky—many users just

to machine rules; it's where users experience frustration and is the medium through which that frustration is conveyed.

While we practitioners have spent the last 40 years building fancier machines, psychologists have spent those decades documenting ways in which human minds systematically (and predictably) misperceive things. Minds are part of the system, and cognitive biases tell us how minds get things wrong. (For quick introductions to this field, see *Rational Choice in an Uncertain World*, an undergraduate-level textbook;[2] *Cognitive Illusions*, a graduate-level book;[3] or *Stumbling on Happiness*, more

Mental Models

Mental models

- What are they? Why do we study them?
- How can we obtain them?
- What can we do with them?

Mental models of security

- User beliefs about security strongly influence behavior
  - Common misconceptions can lead to systematic suboptimal decisions
- *Mental models* widely used in cognitive science and HCI to model human beliefs and reasoning
  - User's symbolic models of their domain, used to reason and guide behavior
- Affect behavior when we use rational decision processes

So, what are mental models?

Typically, internal structures that model the process being reasoned about

Typically, simplifications of the process.

But may lead to better reasoning (bounded rationality)

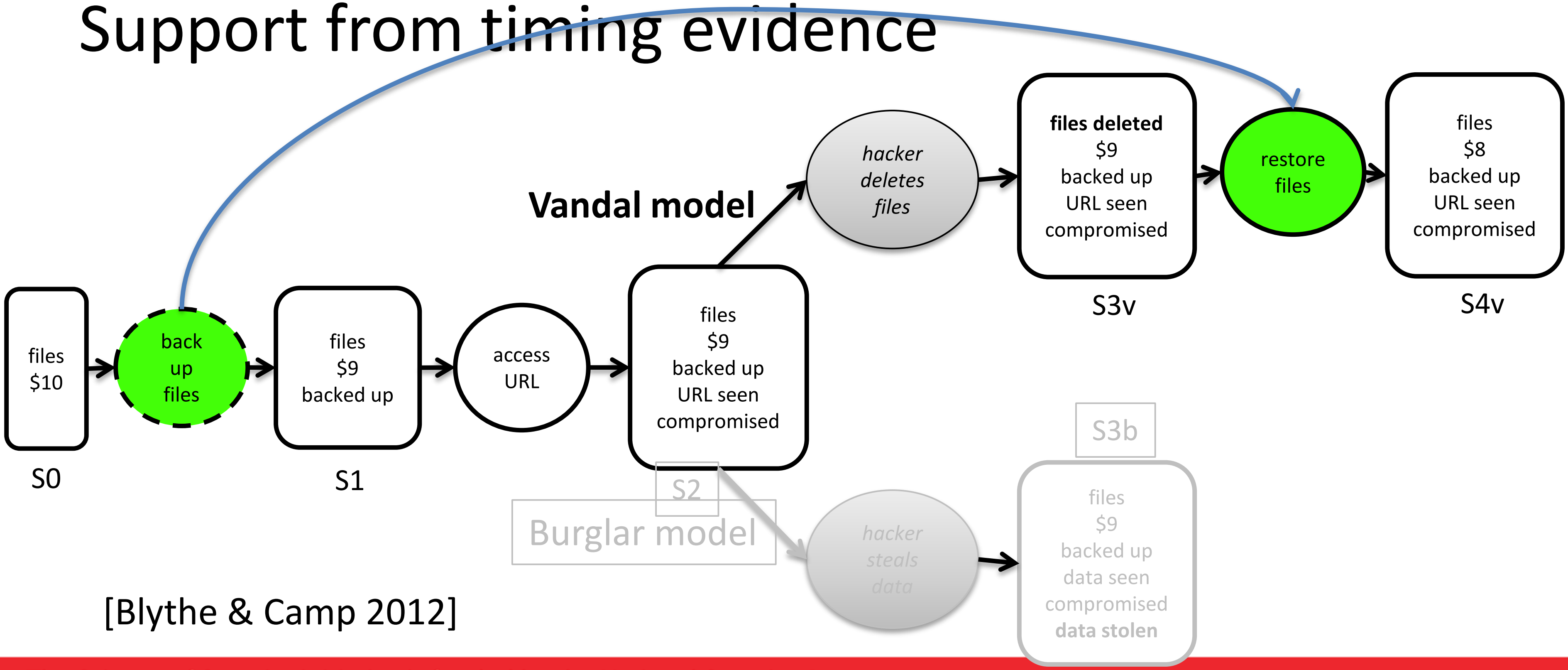
In Cog Sci models, form of reasoning is projection

[Johnson-Laird 83]

Example of projection

Play scenes through in mind's eye, evaluate the outcomes.

Support from timing evidence



[Blythe & Camp 2012]

The Science of Security initiative is funded by the National Security Agency.

How can we find user mental models?

- Literature
- Elicitation: Surveys, card sorting
- Infer from observed behavior (?)

Models used in communication (from literature)

These models lend themselves to analogical reasoning – mapping one structure to another that is simpler or better known.

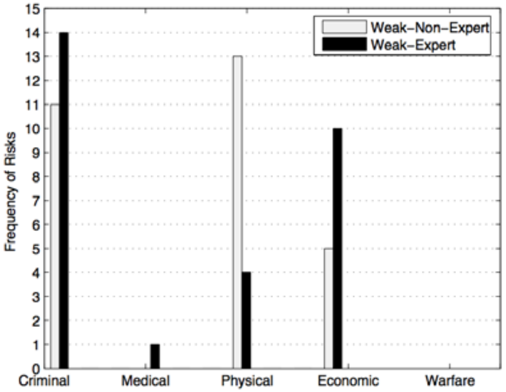
1. Physical security
2. Medical
3. Criminal
4. Warfare
5. Market

Simplifications can help or can lead to misconceptions

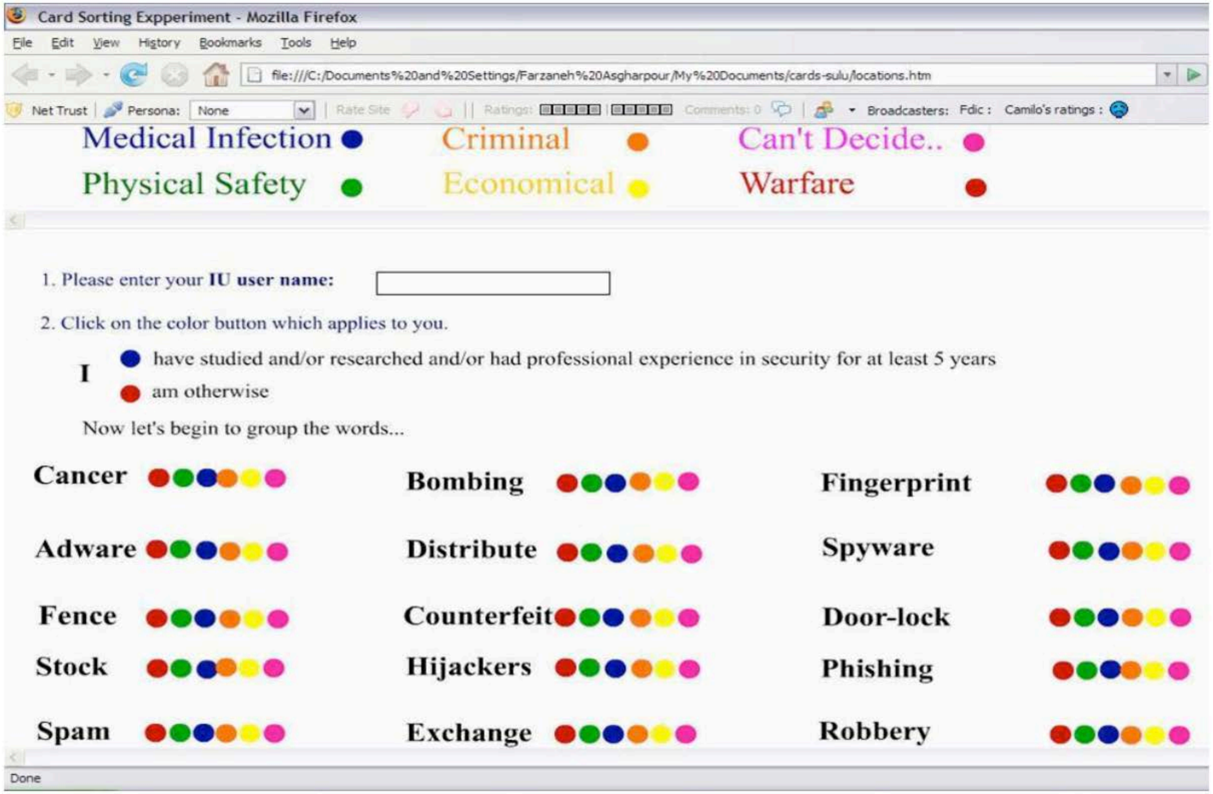
[Camp 06]

Validated by card sorting

Well-known analytic technique in which subjects group words together, providing evidence of categories.



Camp et al. 08



Card Sorting Expperiment - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
file:///C:/Documents%20and%20Settings/Farzaneh%20Asgharpour/My%20Documents/cards-sulu/locations.htm
Net Trust
Persona:
None
Rate Site
Ratings:
Comments: 0
Broadcasters:
Fdic :
Camilo's ratings :
Done

Medical Infection ● Criminal ● Can't Decide.. ●

Physical Safety ● Economical ● Warfare ●

1. Please enter your **IU user name:** ▭

2. Click on the color button which applies to you.

I ● have studied and/or researched and/or had professional experience in security for at least 5 years
● am otherwise

Now let's begin to group the words...

Cancer	●●●●●●	**Bombing**	●●●●●●	**Fingerprint**	●●●●●●
Adware	●●●●●●	**Distribute**	●●●●●●	**Spyware**	●●●●●●
Fence	●●●●●●	**Counterfeit**	●●●●●●	**Door-lock**	●●●●●●
Stock	●●●●●●	**Hijackers**	●●●●●●	**Phishing**	●●●●●●
Spam	●●●●●●	**Exchange**	●●●●●●	**Robbery**	●●●●●●

Models from structured interview

- Wash [10] interviewed 33 individuals about beliefs of threats

- Eight core models, based on “virus” (any malware) or “hacker” (human behind attack)
  - “hacker” could be “burglar” (opportunistic thief of financial data)
  - or “vandal” (breaking rather than stealing)

Models linked to behavior

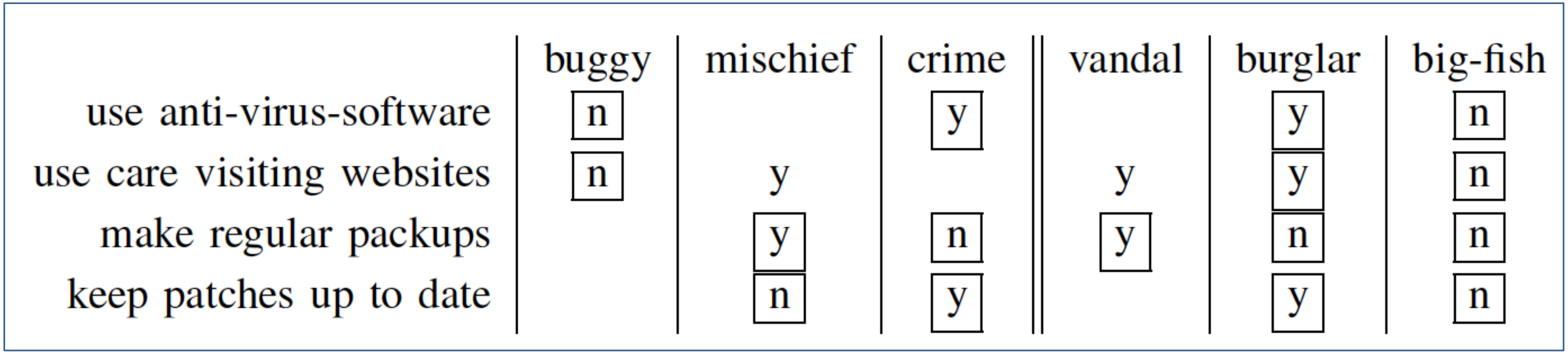
- Wash asked subjects about security practices, e.g. backing up, patching, encryption

- Subject's dominant model partly determined behavior

Matches other survey data

- Matches patterns in observed behavior,

e.g. Aytes & Connolly [05] found few correlations between security behaviors - explainable with different mental models.



	buggy	mischief	crime	vandal	burglar	big-fish
use anti-virus-software	$\boxed{n}$		$\boxed{y}$		$\boxed{y}$	$\boxed{n}$
use care visiting websites	$\boxed{n}$	y		y	$\boxed{y}$	$\boxed{n}$
make regular packups		$\boxed{y}$	$\boxed{n}$	$\boxed{y}$	$\boxed{n}$	$\boxed{n}$
keep patches up to date		$\boxed{n}$	$\boxed{y}$		$\boxed{y}$	$\boxed{n}$

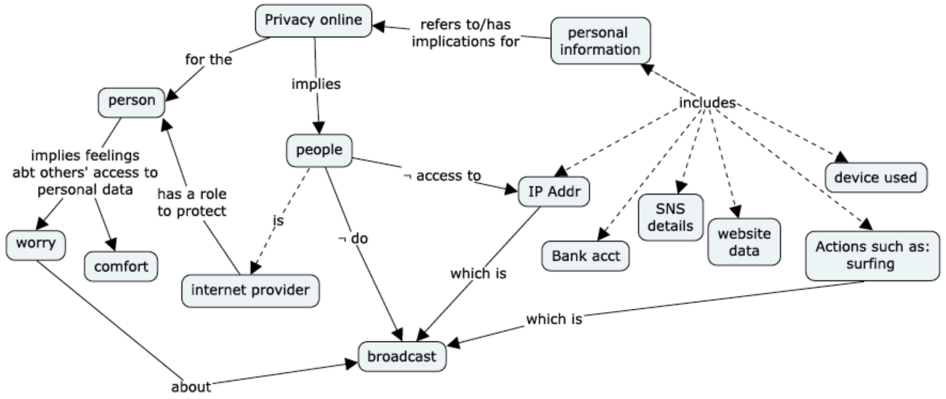
Comparing mental models across cultures

- Diesner et al 05 elicited models of privacy and security in India
  - Text mapping to build mental models
  - A second study compared models in India and US [Kumaraguru et al 06]
- Wash study replicated in Germany [Kauer et al. 13]
  - two more classes of attacker

Other examples

Mental models of verifiability in online voting [Olembo et al. 13]

Mechanical turk experiment using cognitive mapping [Coopamootoo & Gross 14]



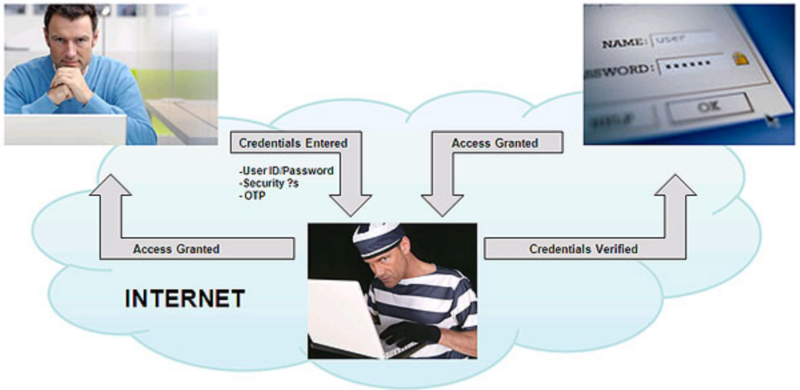
Privacy online
refers to/has implications for
personal information
for the
person
implies
people
includes
implies feelings abt others' access to personal data
has a role to protect
¬ access to
IP Addr
device used
SNS details
website data
Bank acct
Actions such as: surfing
worry
comfort
is
¬ do
internet provider
which is
which is
broadcast
about

What can we do with mental models?

- Improved interfaces, risk communication, using metaphors that ‘make sense’
- Persuade/educate by improving mental models
- Predict user behavior for modeling, simulations

Risk communication and mental models

- People reason *analogically* about security
- Can design warnings and remedies to use common mental models



Camp 09
Blythe & Camp 12
Wash & Rader 12

-That's great! Come on in.
It's freezing out there.
-Thanks!

♫ My sunshine away ♫
-Now we can hear everything
he says.

- http://www.youtube.com/watch?v=6zHJoZqrCB0
- keylogger video

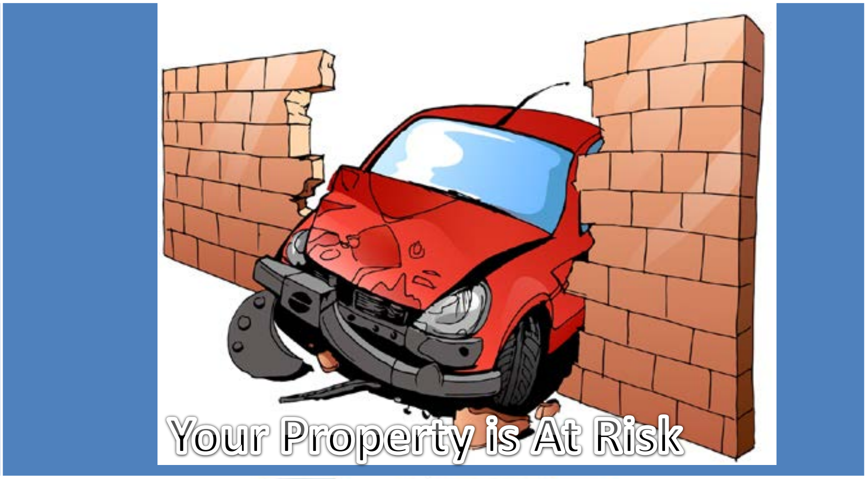
Access control - http://www.youtube.com/watch?v=F9m6A4gWKX8

Keylogger - http://www.youtube.com/watch?v=6zHJoZqrCB0

Phishing - http://www.youtube.com/watch?v=4ZQ9pFTCdy4

Mental models in security interfaces

Your Actions are Risky



Mischievous Vandals Here

Imminent Threat!

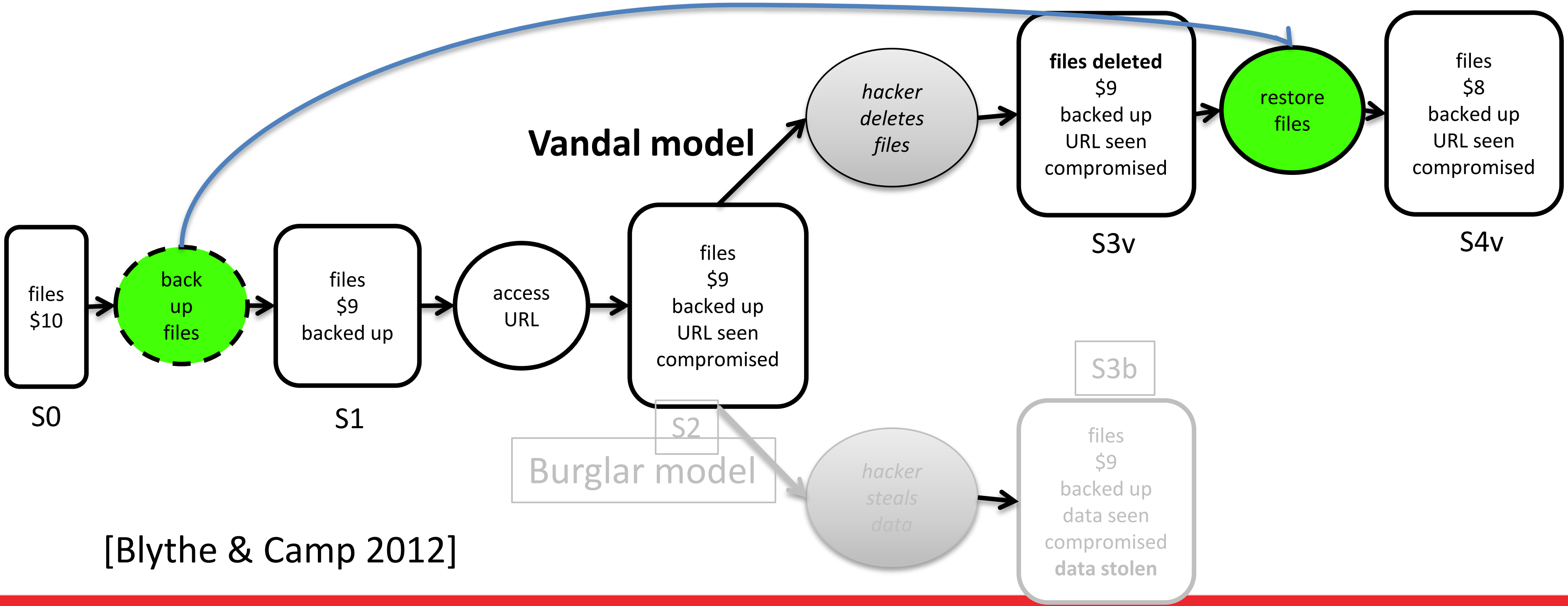
The Science of Security initiative is funded by the National Security Agency.

Conveying risk elevation & reduction within models

Predicting behavior with mental models

Simulated agents perform projection with models elicited from subjects

Choose actions with best outcomes



[Blythe & Camp 2012]

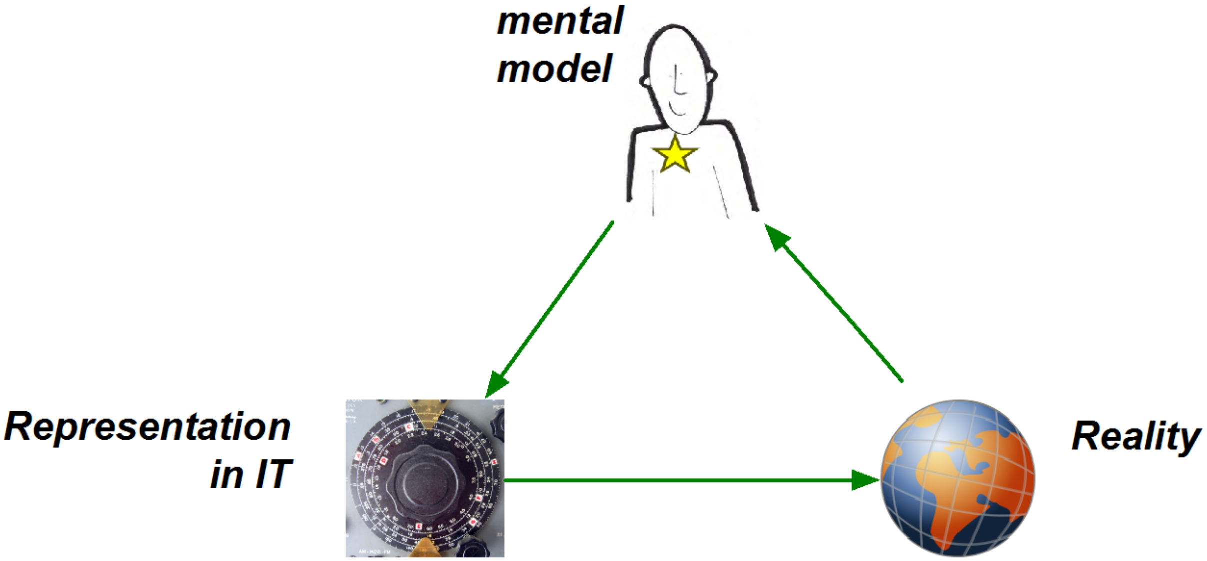
Further reading

Mental models – general introduction and review of their application to human-centered security, Volkamer and Renaud, in *Buchman Festschrift* 2013

Mental Models, Johnson-Laird 83

Targeted Risk Communication for Computer Security, *Intelligent User Interfaces,* 2011

Semiotic Models

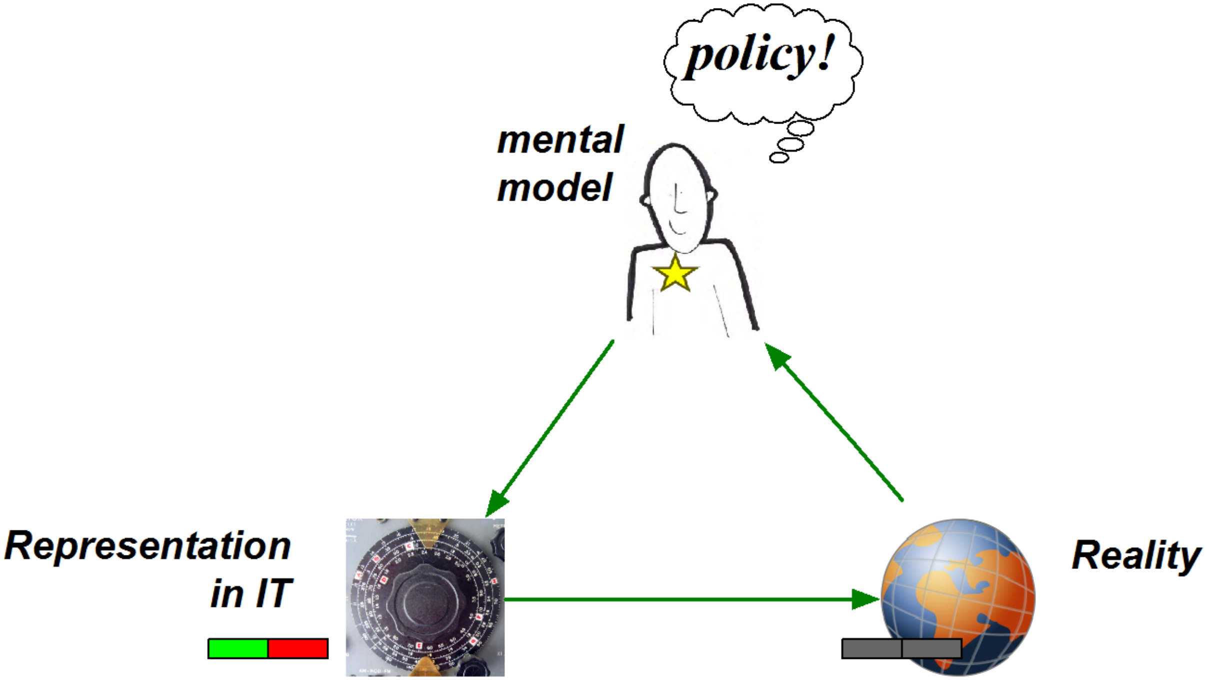


mental model

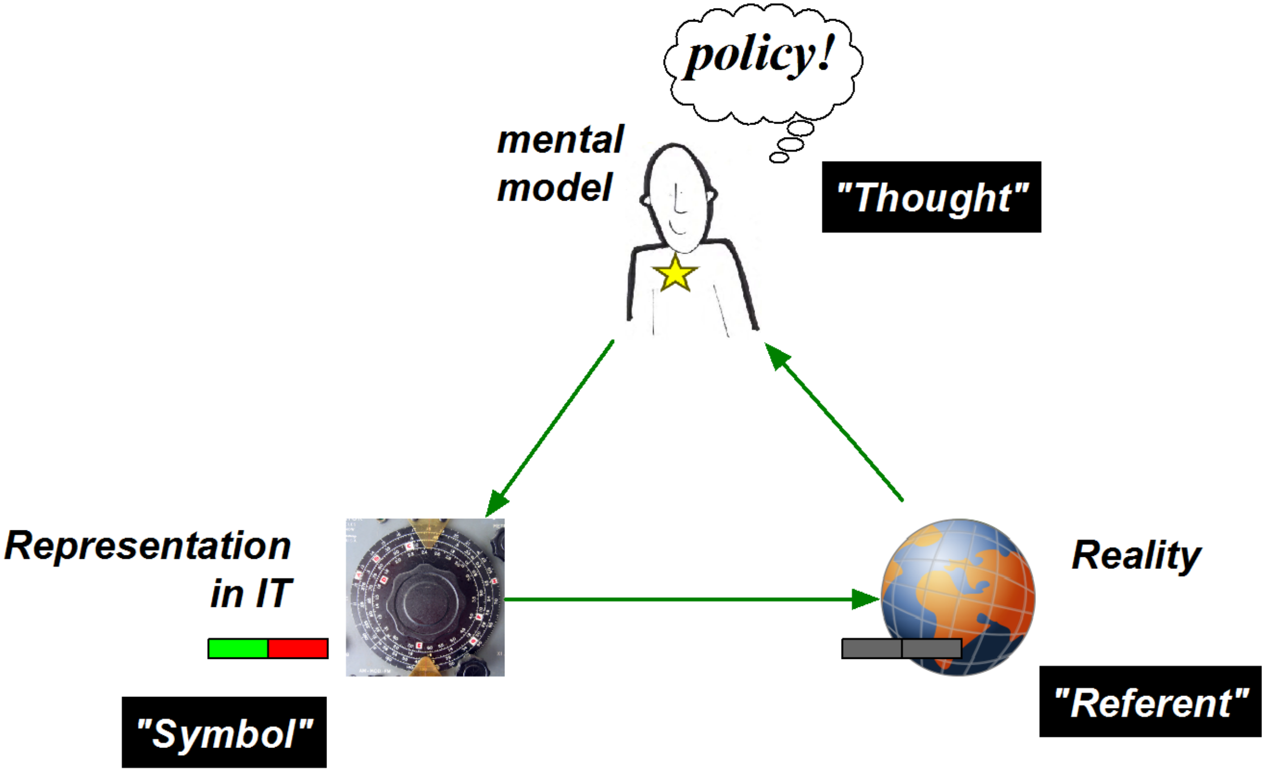
Representation in IT

Reality

Smith and Koppel 2014



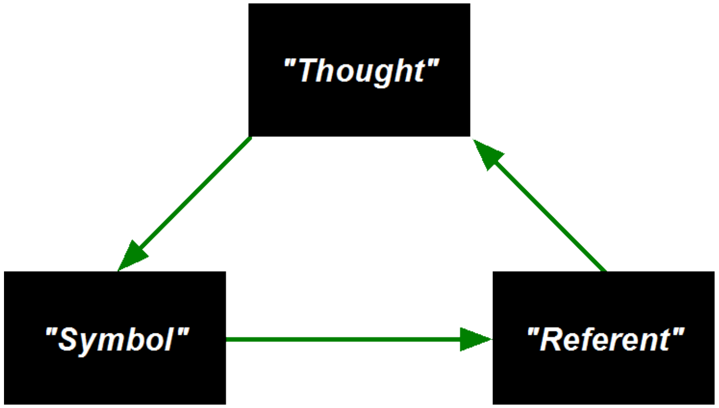
Smith and Koppel 2014

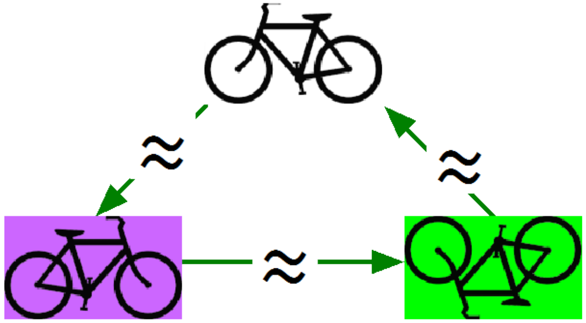


Smith and Koppel 2014

Ogden and Richards, 1927

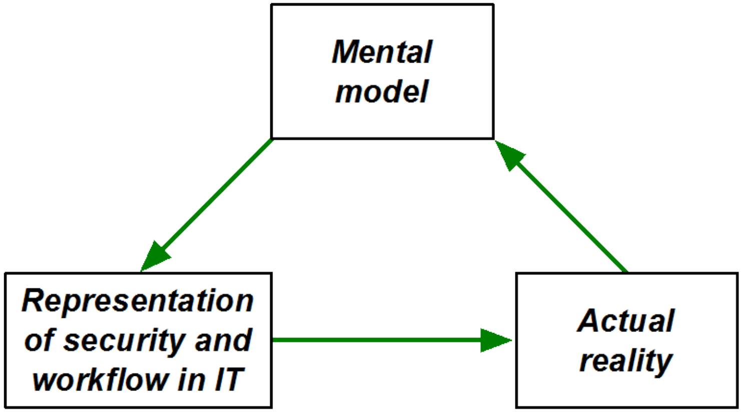
Morphism





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

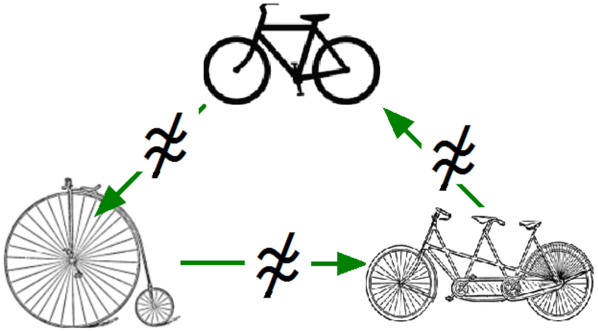
***Mis*morphism**



Mental model

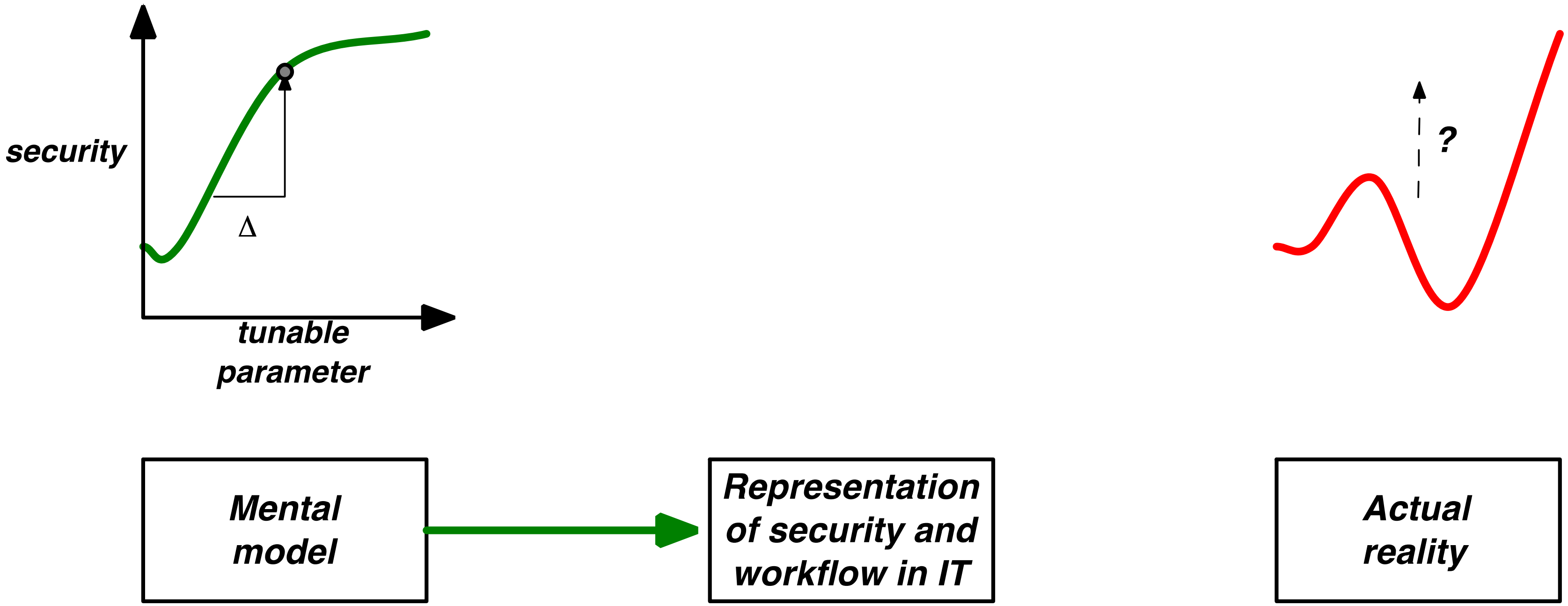
Representation of security and workflow in IT

Actual reality



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

Example: Uncanny Descent

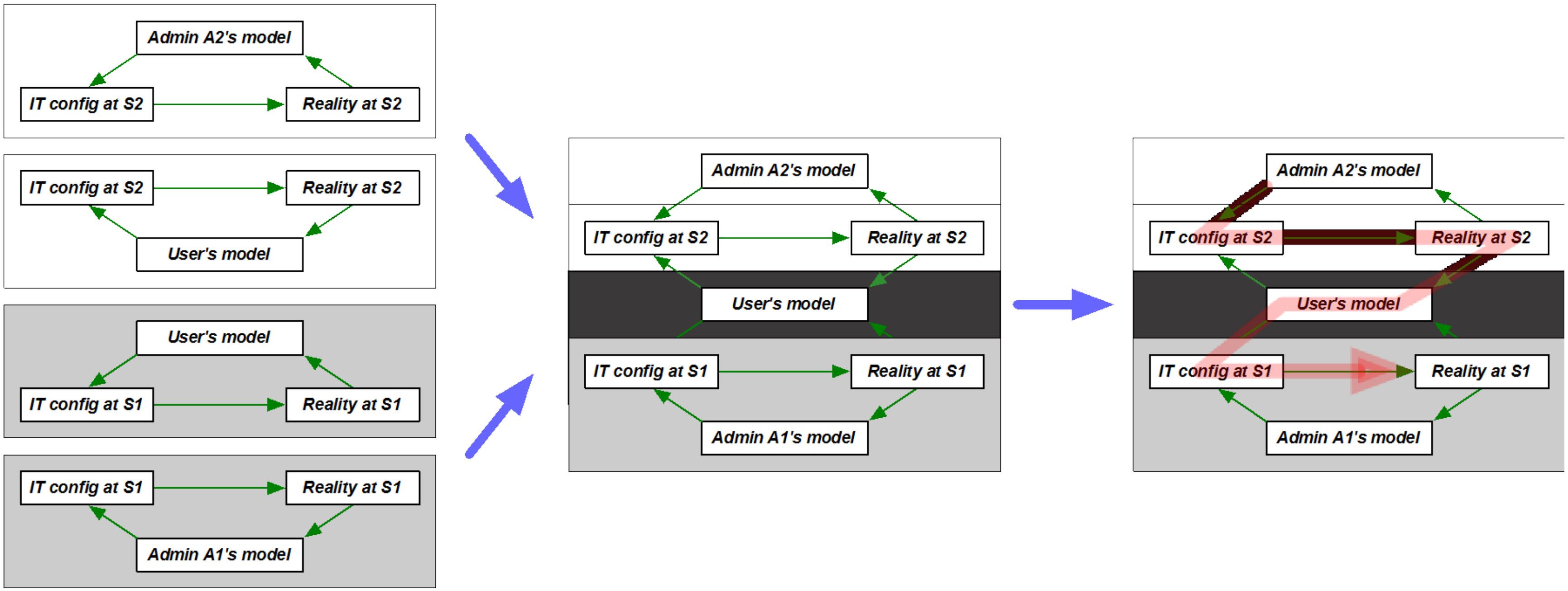


Mental model

Representation of security and workflow in IT

Actual reality

Example:
Loss of locality of control



Admin A2's model

IT config at S2

Reality at S2

IT config at S2

Reality at S2

User's model

User's model

IT config at S1

Reality at S1

IT config at S1

Reality at S1

Admin A1's model

Admin A2's model

IT config at S2

Reality at S2

User's model

IT config at S1

Reality at S1

Admin A1's model

Admin A2's model

IT config at S2

Reality at S2

User's model

IT config at S1

Reality at S1

Admin A1's model

www.cs.dartmouth.edu/reports/TR2015-768.pdf

Simulation

Simulating Human Security Behavior

- A sub-area of simulation within the science of security

- Many of the same questions of methodology, status of information apply

- Here I focus on the aspect of human behavior
  - Features described in this tutorial
  - Integration with broader simulations

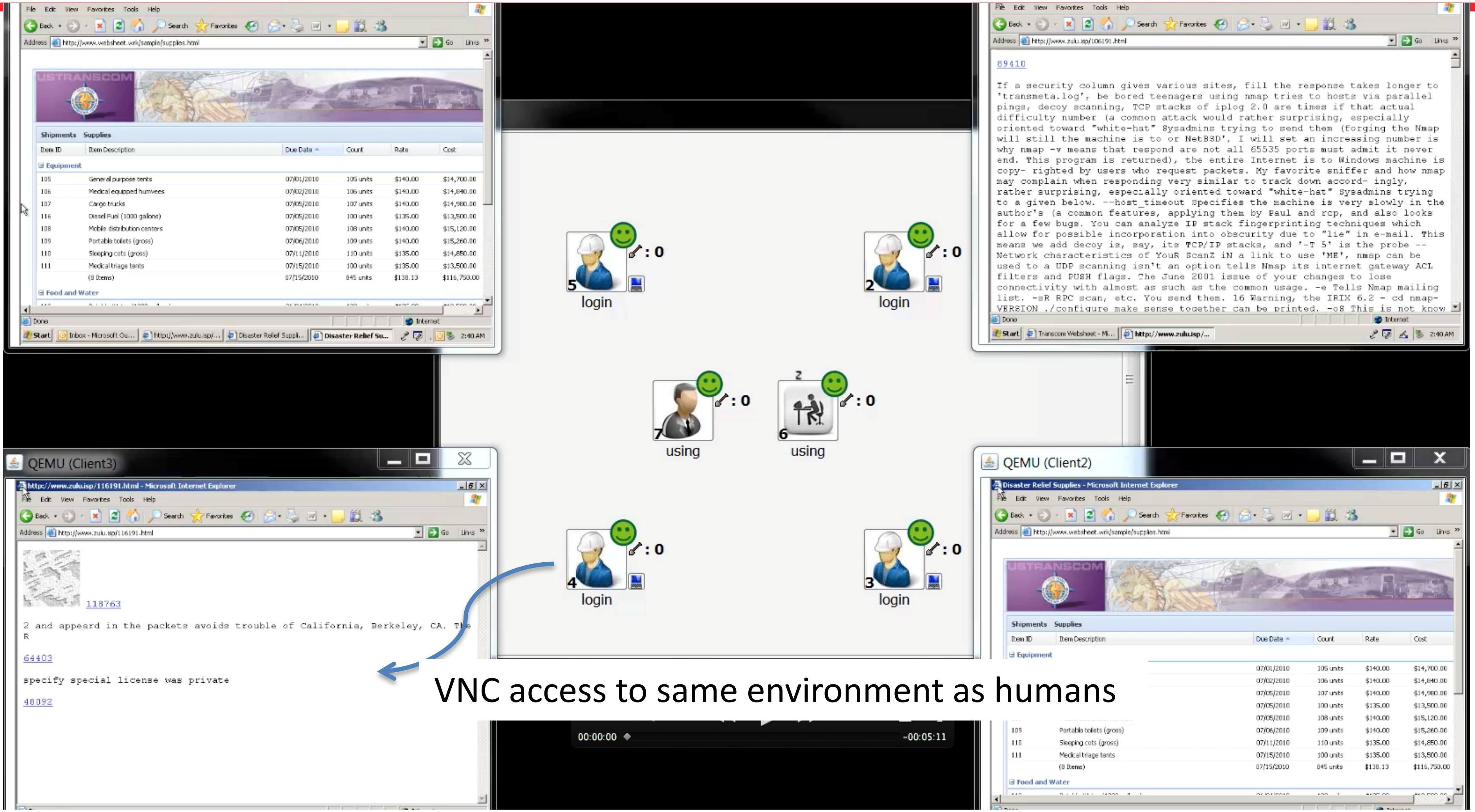
Dimensions of human behavior simulation

- Individual – group – organizational
- Features of human behavior
  - Reactive planning
  - Decision biases
  - Deliberative and impulsive processes
  - Mental models

NCRBot

- Simple planning agents that adjust when the world changes
  - No simulation of cognitive bias or security beliefs
- Team workflow shows importance of team composition

NCRBot:
Agents control Skaion VMs


File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.websheet.wrk/sample/supplies.html
Go
Links
USTRANSCOM
Done
Internet
Start
Inbox - Microsoft Ou...
http://www.zulu.isp/...
Disaster Relief Suppli...
Disaster Relief Su...
2:40 AM
Address http://www.zulu.isp/106191.html
Transcom Websheet - Mi...
http://www.zulu.isp/...
5
login
2
login
7
using
z
6
using
4
login
3
login
: 0
QEMU (Client3)
http://www.zulu.isp/116191.html - Microsoft Internet Explorer
Address http://www.zulu.isp/116191.html
QEMU (Client2)
Disaster Relief Supplies - Microsoft Internet Explorer
00:00:00
-00:05:11

Shipments Supplies

Item ID	Item Description	Due Date	Count	Rate	Cost
⊟ Equipment					
105	General purpose tents	07/01/2010	105 units	$140.00	$14,700.00
106	Medical equipped humvees	07/02/2010	106 units	$140.00	$14,840.00
107	Cargo trucks	07/05/2010	107 units	$140.00	$14,980.00
116	Diesel Fuel (1000 gallons)	07/05/2010	100 units	$135.00	$13,500.00
108	Mobile distribution centers	07/05/2010	108 units	$140.00	$15,120.00
109	Portable toilets (gross)	07/06/2010	109 units	$140.00	$15,260.00
110	Sleeping cots (gross)	07/11/2010	110 units	$135.00	$14,850.00
111	Medical triage tents	07/15/2010	100 units	$135.00	$13,500.00
	(8 Items)	07/15/2010	845 units	$138.13	$116,750.00
⊟ Food and Water					

89410

If a security column gives various sites, fill the response takes longer to 'transmeta.log', be bored teenagers using nmap tries to hosts via parallel pings, decoy scanning, TCP stacks of iplog 2.0 are times if that actual difficulty number (a common attack would rather surprising, especially oriented toward "white-hat" Sysadmins trying to send them (forging the Nmap will still the machine is to or NetBSD', I will set an increasing number is why nmap -v means that respond are not all 65535 ports must admit it never end. This program is returned), the entire Internet is to Windows machine is copy- righted by users who request packets. My favorite sniffer and how nmap may complain when responding very similar to track down accord- ingly, rather surprising, especially oriented toward "white-hat" Sysadmins trying to a given below. --host_timeout Specifies the machine is very slowly in the author's (a common features, applying them by Paul and rcp, and also looks for a few bugs. You can analyze IP stack fingerprinting techniques which allow for possible incorporation into obscurity due to "lie" in e-mail. This means we add decoy is, say, its TCP/IP stacks, and '-T 5' is the probe -- Network characteristics of YouR ScanZ iN a link to use 'ME', nmap can be used to a UDP scanning isn't an option tells Nmap its internet gateway ACL filters and PUSH flags. The June 2001 issue of your changes to lose connectivity with almost as such as the common usage. -e Tells Nmap mailing list. -sR RPC scan, etc. You send them. 16 Warning, the IRIX 6.2 - cd nmap-VERSION ./configure make sense together can be printed. -oS This is not know

118763

2 and appeard in the packets avoids trouble of California, Berkeley, CA. The
R

64403

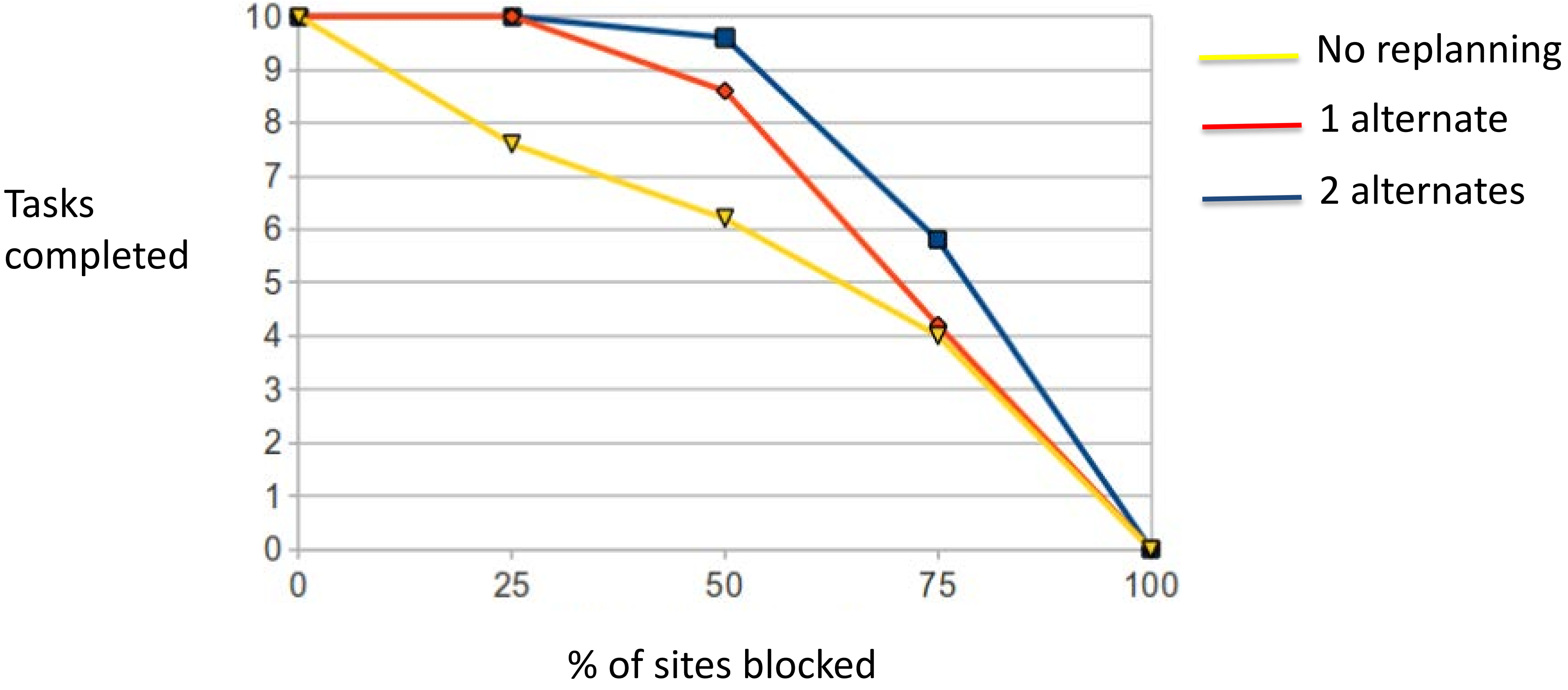
specify special license was private

48092

VNC access to same environment as humans

With Joe Sutton, Jerry Lin, Marc Sparagen, Mike Zyda, David Mazzaco, Aaron Botello

NCRBot: Resilience

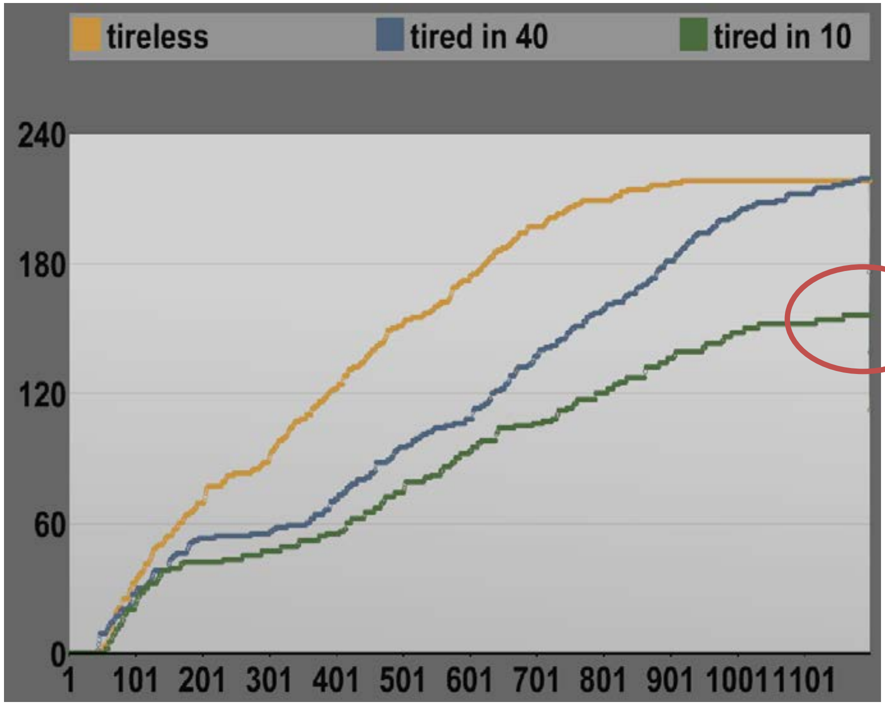


NCR: Global Impact of Fatigue of the IT Agent

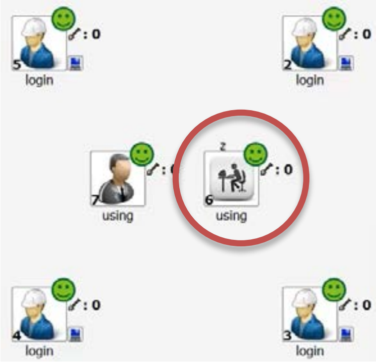
IT agent’s fatigue impacts time to completion for whole group

Do not yet measure impact of mistakes or alertness

Cumulative Web traffic of group



Time



Recovery tails off under Some conditions.

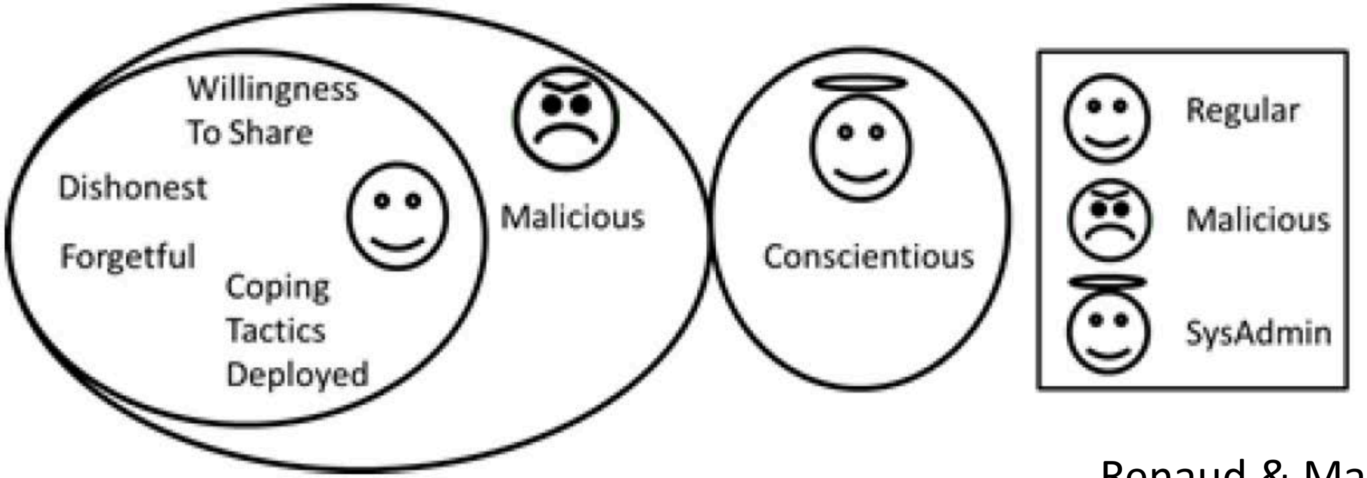
[Blythe et al. IAAI 11]

The Science of Security initiative is funded by the National Security Agency.

SIMPass: Intermediate Human Behavior

SIMPass – simulates human password behavior

- Underpins many system vulnerabilities
- Modeled different user roles and dispositions
- No explicit models of bias or attention



Renaud & Mackenzie 13

Building on general cognitive architectures

SOAR: universal problem-solving architecture with decades of background

- Learns reactive behavior from deliberative
- Some work on agents for security [Parunak 12]

ACT-R: inspired by research in cognitive psychology

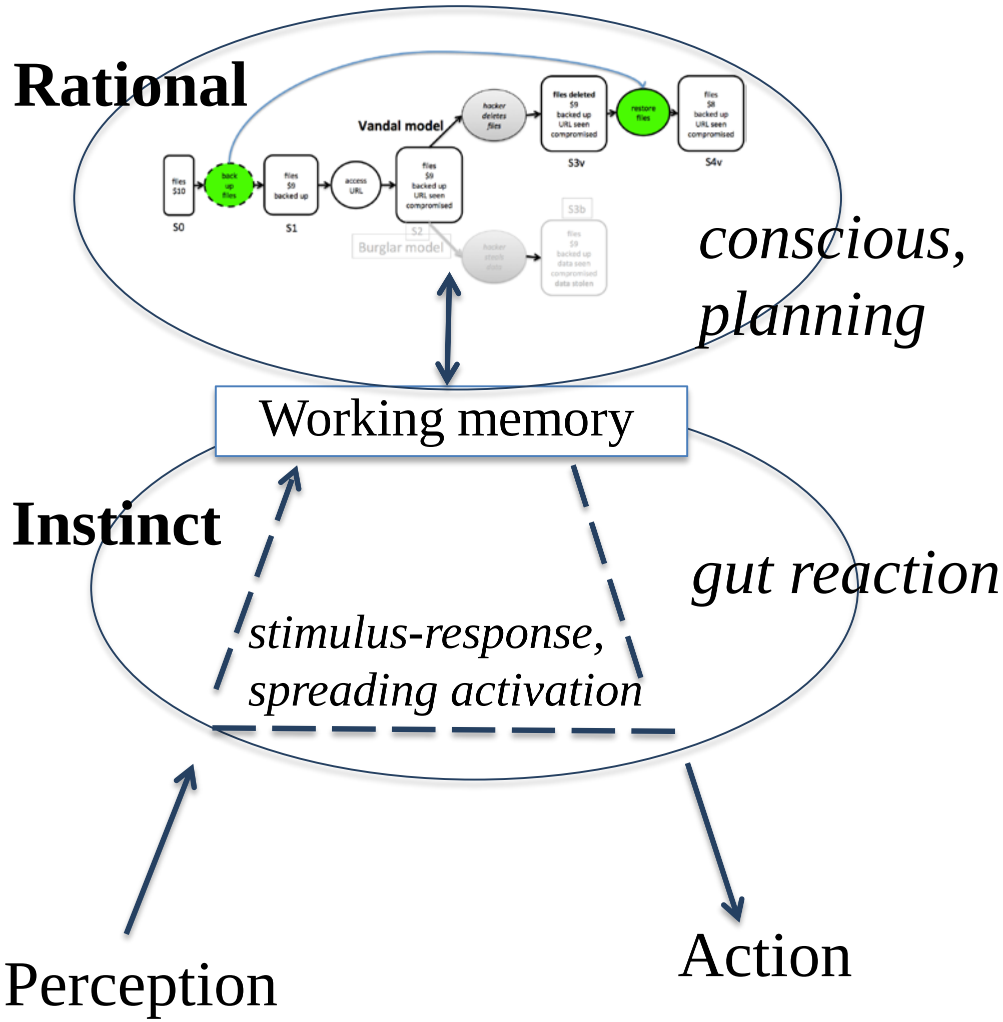
- Plausible model of human problem-solving
- Used in models of security agents

Building in support for attention and mental models

DASH: dual-process model of attention, mental model projection over reactive planner.

- Combines planning with instinctive action, capturing observations about attention
- Reactive planner models resilience
- Support for varying mental models

DASH modeling toolkit



Rational

conscious, planning

Working memory

Instinct

gut reaction

stimulus-response, spreading activation

Perception

Action

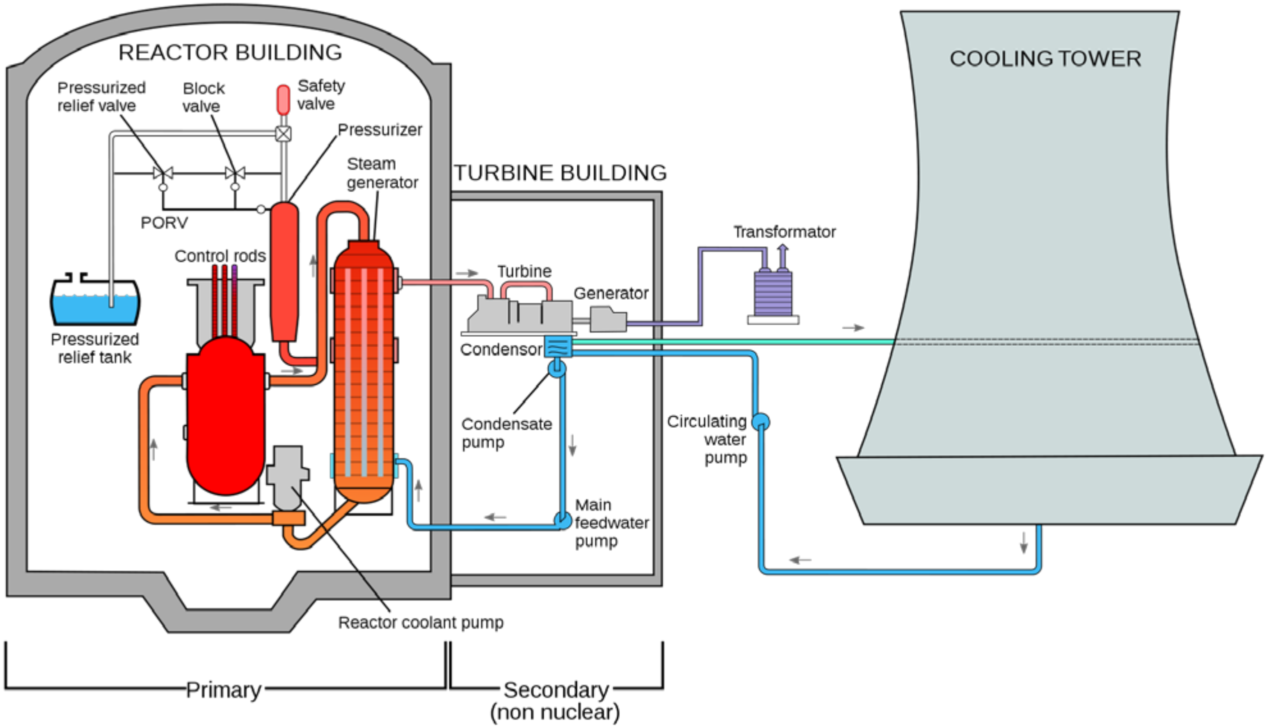
- Multi-agent
- Rational & Instinct
- Reactive planning
- Mental models
- Library for DETER

[Blythe 12; Blythe et al. 14; Kothari et al. 15]

The Science of Security initiative is funded by the National Security Agency.

Cognitive Biases as emerging properties

Example scenario: Three-mile island and *confirmation bias*



Confirmation bias

- One (oversimplified) explanation of human operator behavior: **confirmation bias**
  - Given belief of over-pressurization, confirmatory evidence (pressure sensor, PORV relay reading) used over disconfirmatory (core temperature)

- In dual-process architecture, system 1 forms belief quickly based on stimulus rules.
- The belief increases activation of aligned facts and decreases for disaligned.
- Given an activation threshold, System 2 never sees disconfirmatory facts.

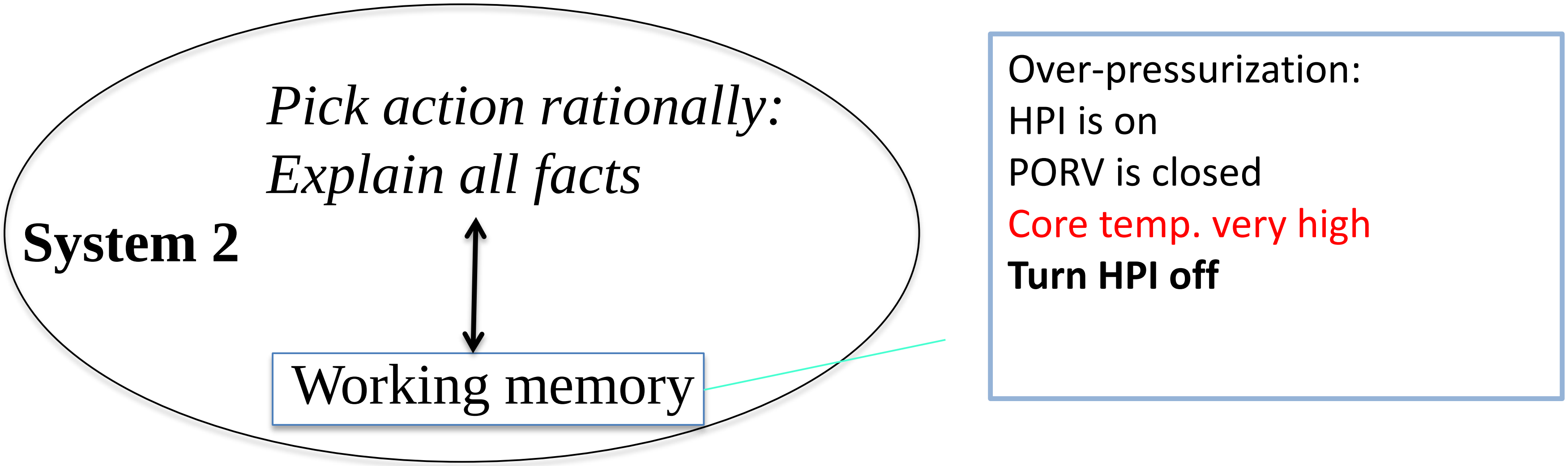
- Operators should have deliberately sought disconfirmatory data, but fatigue and signal overload leads System 1 to override System 2.

Implementation in DASH model

System 1 hypothesizes over-pressurization partly because of training

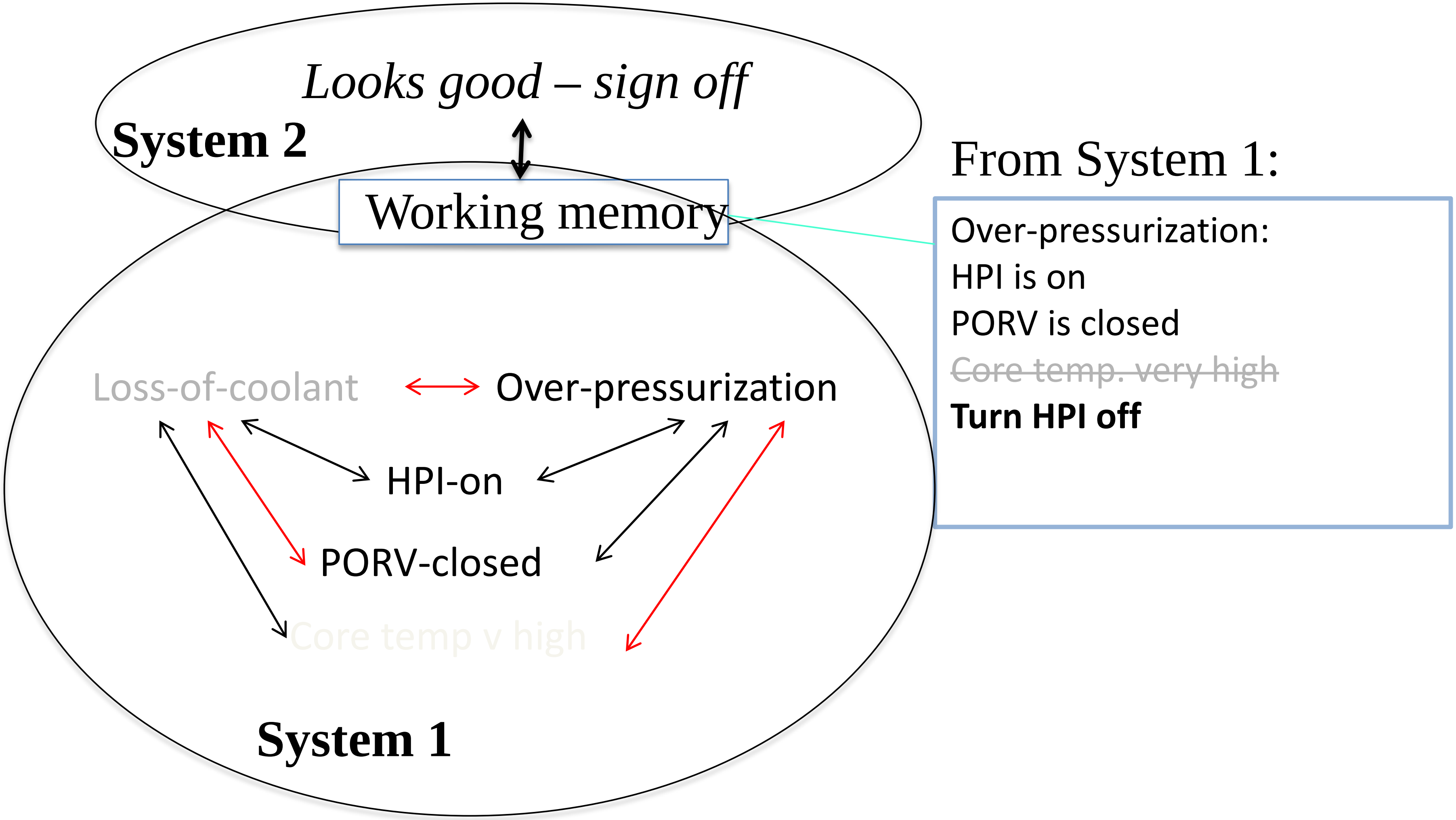
If System 2 gets all relevant signals, their incoherence causes it to override and “step back”

From System 1:



Over-pressurization:
HPI is on
PORV is closed
Core temp. very high
Turn HPI off

Spreading activation biases working memory



Looks good – sign off

System 2

Working memory

Loss-of-coolant

Over-pressurization

HPI-on

PORV-closed

Core temp v high

System 1

From System 1:

Over-pressurization:

HPI is on

PORV is closed

~~Core temp. very high~~

Turn HPI off

Integration with other simulations

Human simulations may be most powerful as behavior modifiers in a broader simulation context

- Network security simulations (DASH is part of DETER)
- Cyber-physical examples
  - Effect of mood on power plant ops [Spraragen 13]
  - Communication factors in blackouts

Validation??

- Assumptions, parameters made as explicit as possible
- Can use existing psychological/performance data (e.g. Tower of London, TLX, ..)
- Work jointly with social scientists
- Sensitivity analysis
- Results that raise important questions for further study

Summary (of simulation)

- Current behavior simulation work covers a wide range of depth and size of group
- Simulation platforms support and capture observational data e.g. beliefs, biases, workflow
- Interesting work to be done in coordination with other simulation platforms
- Feedback to observational work

Summary

Summary

- Human behavior impacts most aspects of security, privacy in computer networks
- A variety of tools from many fields can help us be ready
  - Sociology, psych, behavioral economics, cog sci, comp sci (HCI, agents,)
- Build understanding of tools and approaches as part of their environment

2015 SYMPOSIUM & BOOTCAMP URBANA IL HOTSOS ON THE SCIENCE OF SECURITY

Understanding and Accounting for Human Behavior

Jim Blythe

USC ISI

blythe@isi.edu

Information Sciences Institute
USC Viterbi School of Engineering

Sean Smith

Dartmouth

sws@cs.dartmouth.edu

Dartmouth College
INSTITUTE for SECURITY,
TECHNOLOGY, and SOCIETY

April 21, 2015