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

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

From Wikipedia, the free encyclopedia

Ethnography (from Greek ἔθνος ethnos "folk, people, nation" and γράφω graphō "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, communication studies, history—wherever people study ethnic groups, formations, compositions, resettlements, social welfare characteristics, materiality, spirituality, and a people's ethnogenesis.[5] The typical ethnography is a holistic study[6][7] and so includes a brief history, and an analysis of the terrain, the climate, and the habitat. In all cases it should be reflective, make a substantial contribution toward the understanding of the social life of humens, 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.
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
1. Annoyingly Hard Problems
Access Control
Access Control

"good"

officer

user

Access Control

"bad"

officer

user
Access Control
Access Control

policy!

officer

user

"good"
Access Control

policy!

officer

"good"

user
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?"
...in medical IT

View of passwords inside the supply room

Bob’s PW
wv2XXcym

Password for all smart pumps
Smtpum

Barb’s PW
omg2445

Len’s PW
IRT277cbm

Who drank my coffee?
Barb

Jon’s PW
9877cizbm

Andy’s PW

Sean’s PWs
IRT 445yti
IRK277c2m
Never 434

Med Rm PW
If you’re here you
know it already

My passwords
Hidden:
Lift to see

Suzzythe best223**2

Mike’s PW

Don’t look

“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 loç
  access-list 1 permit 333.041.18.0 0.0.0.255 loç
...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: 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.
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: pauletKuku@yahoo.com

Hi My Dear,
How are you?

This E-mail was sent from "RNP140088" (Aficio MP 4001).
Scan Date: 01.29.2013 19:04:21 (-0500)
Queries to: ricohdonotreply@dartmouth.edu

pauletKuku@yahoo.com
...in email

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

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

This E Scan Quer

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

File Type: pdf

http://www.xerox.com
Healthcare information technology’s relativity problems: a typology of how patients’ physical reality, clinicians’ mental models, and healthcare information technology differ

Sean W Smith, Ross Koppel

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 trade-offs that, if done profitably, can be dangerous. Reductionism extends to looking at effective access control, which must be considered in the context of an entire system.

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

officer
Secret Weapon

"Eppur si muove..."
Secret Weapon
Secret Weapon
Secret Weapon

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

- Reid K. Hastie, Robyn M. Dawes

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 :)

Unofficial, Psychology of Decision Making:
- Dan Ariely.
  *Predictably Irrational: The Hidden Forces That Shape Our Decisions.*
- Paul Coco and Scott Bates.
  *Methods in Behavioral Research.*
- Cordelia Fine
  *A Mind of Its Own: How Your Brain Distorts and Deceives.*
- Thomas Gilovich et al, editors.
  *Heuristics and Biases: The Psychology of Intuitive Judgment.*
- Daniel Kahneman et al, editors.
  *Judgment under Uncertainty: Heuristics and Biases.*

Summary of biases, recommended by Vijay:
- Daniel Kahneman, editor.
  *Choices, Values, and Frames.*
- Daniel Kahneman
  *Thinking, Fast and Slow.*
  Farrar, Straus and Giroux, 2011.
- D. Gilbert.
  *Stumbling on Happiness.*
- David Hardman
  *Judgment and Decision Making: Psychological Perspectives.*
- Pohl, Rudiger F.
  *Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory.*
- Plous, Scott
  *The Psychology of Judgment and Decision Making.*
Secret Weapon

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

- Reid K. Hastie, Robyn M. Dawes

Pohl's book below is also highly recommended; Hardman's book (below) also looks good—but may contain more "critical reviews of research papers" than an actual text...

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:

- Daniel Kahneman
  *Thinking, Fast and Slow*
  Farrar, Straus and Giroux, 2011.
- D. Gilbert.
  *Stumbling on Happiness.*
- Daniel Kahneman
  *Choices, Values, and Frames*
- David Hardman
  *Judgment and Decision Making: Psychological Perspectives*
- Pohl, Rudiger F.
  *Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory*
- Plous, Scott
  *The Psychology of Judgment and Decision Making*
Secret Weapon

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

- Reid K. Hastie, Robyn M. Dawes

Pohl's book below is also highly recommended: it's not a "textbook" in the usual sense, but rather a collection 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 :)

Unofficial, Psychology of Decision Making:
- Daniel Kahneman
  *Thinking, Fast and Slow*
  Farrar, Straus and Giroux, 2011.
- D. Gilbert.
  *Stumbling on Happiness.*
- David Hardman
  *Judgment and Decision Making: Psychological Perspectives*
- Pohl, Rudiger F.
  *Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory*
- Plous, Scott
  *The Psychology of Judgment and Decision Making*

Summary of background essay:
Cognitive Bias and Security

3. Initial Results
How do we protect users from dangerous privacy spills?
From Psychology: Introspection Inhibits Intuition

Thinking Too Much: Introspection Can Reduce the Quality of Preferences and Decisions
[Attitudes and Social Cognition]

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?

$P_U \approx P_M$

$P_U \neq P_M$
Fake Social Network

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: 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!

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
- Dartmouth for XxCol: Admire of Mister Darcy

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

# Profiles

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

Would you allow Amanda to view . . .

- Yes  No  . . . your **Basic Info**? (Sex, Birthday, Hometown, Relationship Status, Political Views, and Religious 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**?

[Submit]
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

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

$P_c \neq P$

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 information

**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 friends 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
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
**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 control 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\textsuperscript{abd}, Ricardo CRUZ-CORREIA\textsuperscript{cd}, Luís ANTUNES\textsuperscript{b}, David CHADWICK\textsuperscript{a}
\textsuperscript{a}Computer Laboratory, University of Kent
\textsuperscript{b}LIACC- Faculty of Science of Porto
\textsuperscript{c}Biostatistics and Medical Informatics Dept. of Porto Faculty of Medicine
\textsuperscript{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

officer

subjective, looking at patient

user

The Science of Security initiative is funded by the National Security Agency.
http://hot-sos.org/
Experiment

abstract, looking at policy GUI

abstract, role-based version

sequence of access scenarios

"in the clinic" version

subjective, looking at patient

The Science of Security initiative is funded by the National Security Agency.
http://hot-sos.org/
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.
Experiment

- **control group**: abstract, role-based version
- **experimental group**: "in the clinic" version
- **164 EMR users from partner hospital**: sequence of access scenarios

- abstract, looking at policy GUI
- subjective, looking at patient

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

abstract, looking at policy GUI

control group

164 EMR users from partner hospital

sequence of access scenarios

subjective, looking at patient

experimental group

"in the clinic" version

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

overall: the groups differed significantly
Results

<table>
<thead>
<tr>
<th></th>
<th>Control</th>
<th>Experimental</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q10</td>
<td>70% 86 Subjects</td>
<td>70% 71 Subjects</td>
</tr>
<tr>
<td>p = .095</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q11</td>
<td>70% 86 Subjects</td>
<td>70% 71 Subjects</td>
</tr>
<tr>
<td>p = .279</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q12</td>
<td>70% 87 Subjects</td>
<td>70% 72 Subjects</td>
</tr>
<tr>
<td>p = .402</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q13</td>
<td>70% 87 Subjects</td>
<td>70% 71 Subjects</td>
</tr>
<tr>
<td>p = .740</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

scenarios with no significant difference
Results

<table>
<thead>
<tr>
<th></th>
<th>Control</th>
<th>Experimental</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>84 Subjects</td>
<td>69 Subjects</td>
</tr>
<tr>
<td>p &lt; 0.01</td>
<td>70%</td>
<td>70%</td>
</tr>
</tbody>
</table>

| Q2 | 84 Subjects | 68 Subjects |
| p < 0.01 | 70% | 70% |

| Q3 | 84 Subjects | 69 Subjects |
| p < 0.01 | 70% | 70% |

| Q4 | 83 Subjects | 68 Subjects |
| p < 0.01 | 70% | 70% |

| Q5 | 82 Subjects | 68 Subjects |
| p < 0.01 | 70% | 70% |

| Q6 | 85 Subjects | 70 Subjects |
| p < 0.01 | 70% | 70% |

| Q7 | 87 Subjects | 74 Subjects |
| p = .014 | 70% | 70% |

| Q8 | 85 Subjects | 71 Subjects |
| p = .025 | 70% | 70% |

| Q9 | 87 Subjects | 72 Subjects |
| p = .037 | 70% | 70% |

scenarios where the groups **differed** significantly
Results

<table>
<thead>
<tr>
<th>Question</th>
<th>Control</th>
<th>Experimental</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>84 Subjects</td>
<td>69 Subjects</td>
</tr>
<tr>
<td>p &lt; 0.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q2</td>
<td>84 Subjects</td>
<td>68 Subjects</td>
</tr>
<tr>
<td>p &lt; 0.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q3</td>
<td>84 Subjects</td>
<td>69 Subjects</td>
</tr>
<tr>
<td>p &lt; 0.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q4</td>
<td>83 Subjects</td>
<td>68 Subjects</td>
</tr>
<tr>
<td>p &lt; 0.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q5</td>
<td>82 Subjects</td>
<td>68 Subjects</td>
</tr>
<tr>
<td>p &lt; 0.01</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Ordoñez, 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 of 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. Not Security It
The Peak-End Bias

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 B553, La Jolla, CA 92030-0833, USA

ARTICLE INFO

Article history:
Received 5 October 2007
Accepted 5 July 2008
Available online 8 November 2008
Accepted by John Schaubroeck

Keywords:
Duration neglect
Peak-end rule
Hedonic experience
Hedonics
Bases

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.

© 2008 Elsevier Inc. All rights reserved.
The Peak-End Bias
The Peak-End Bias
The Peak-End Bias
Immune Neglect

Research Article
The Peculiar Longevity of Things
Not So Bad

Daniel T. Gilbert, Matthew D. Lieberman, Carey K. Morewedge, and Timothy D. Wilson

Harvard University; University of California, Los Angeles; and University of Virginia
Immune Neglect

"The Region-Beta Paradox"

TIME

DISTANCE

"recovery time"

"severity of injury"

(From cited paper)
Why the brain talks to itself: sources of error in emotional prediction

Daniel T. Gilbert¹,* and Timothy D. Wilson²

¹Department of Psychology, Harvard University, Cambridge, MA 02138, USA
²Department 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 (promotions), 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
Why the brain talks to itself: sources of error in emotional prediction

Daniel T. Gilbert¹,* and Timothy D. Wilson²

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

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

Keywords: emotional prediction; affective forecasting; prediction
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"
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?
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.
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?
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,
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]
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
• 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.

<table>
<thead>
<tr>
<th>use anti-virus-software</th>
<th>buggy</th>
<th>mischief</th>
<th>crime</th>
<th>vandal</th>
<th>burglar</th>
<th>big-fish</th>
</tr>
</thead>
<tbody>
<tr>
<td>use care visiting websites</td>
<td>n</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
</tr>
<tr>
<td>make regular packups</td>
<td></td>
<td></td>
<td>y</td>
<td></td>
<td>y</td>
<td>n</td>
</tr>
<tr>
<td>keep patches up to date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n</td>
</tr>
</tbody>
</table>
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]
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
• http://www.youtube.com/watch?v=6zHJoZqrCB0

• keylogger video

Access control -
http://www.youtube.com/watch?v=F9m6A4gWXX8

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

Phishing -
http://www.youtube.com/watch?v=4ZQ9pFTCdy4
Mental models in security interfaces
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

Semiotic Models
mental model

Representation in IT

Reality

Smith and Koppel 2014
Smith and Koppel 2014
Morphism

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

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

security

tunable parameter

Delta

?
Example:
Loss of locality of control

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

VNC access to same environment as humans

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

Tasks completed

% of sites blocked

- No replanning
- 1 alternate
- 2 alternates
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

[Graph showing cumulative web traffic of group]

Cumulative Web traffic of group

Recovery tails off under some conditions.

[Blythe et al. IAAI 11]
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

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

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

**System 2**

Pick action rationally: Explain all facts

**Working memory**
Looks good – sign off

From System 1:
- Over-pressurization: HPI is on
- PORV is closed
- Core temp. very high
- Turn HPI off

Spreading activation biases working memory

System 2

System 1

Over-pressurization: Loss-of-coolant
HPI-on
PORV-closed
Core temp. very high

Working memory
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