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

Mismorphism: a Semiotic Model of Computer Security Circumvention

Sean Smith
Dartmouth College

Ross Koppel
University of Pennsylvania

Jim Blythe
Univ. of Southern California

Vijay Kothari
Dartmouth College

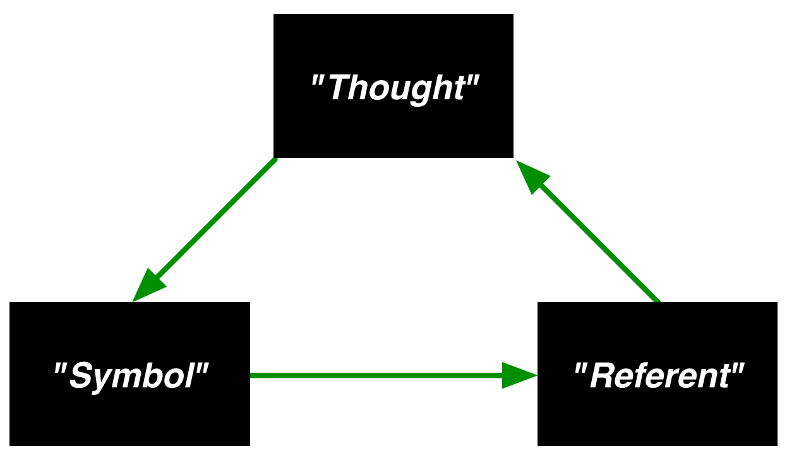
www.cs.dartmouth.edu/reports/TR2015-768.pdf

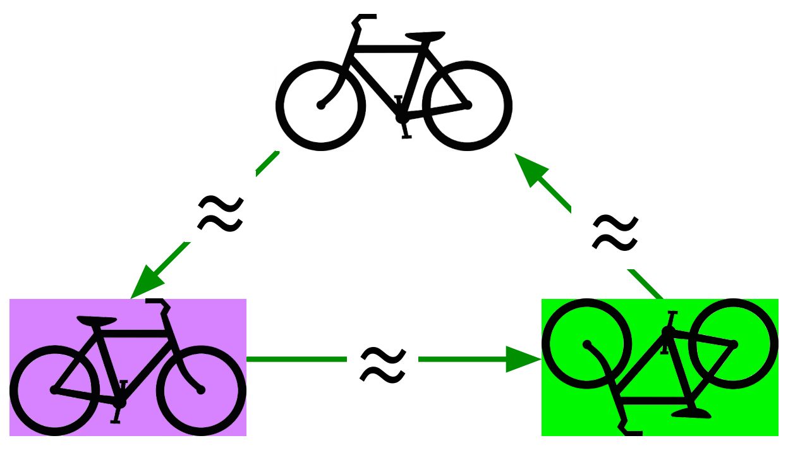
Introduction

Users systematically work around security controls. We can pretend this doesn't happen, but it does. In our research, we address this problem via observation and grounded theory (Bernard and Ryan, 2010; Charmaz, 2003; Pettigrew, 2000). Rather than assuming that users behave perfectly or that only bad users do bad things, we instead observe and record what really goes on compared to the various expectations. Then, after reviewing data, we develop structure and models, and bring in additional data to support, reject and refine these models.

A Semiotic Model for IT Usability Trouble

In their seminal work on the meaning of language, Ogden and Richards (1927) constructed what is sometimes called the ***semiotic triad***. The vertices are the three principal objects: what the speaker (or listener/reader) ***thinks***; what ***symbol*** they use; and the actual item to which they are ***referring***.

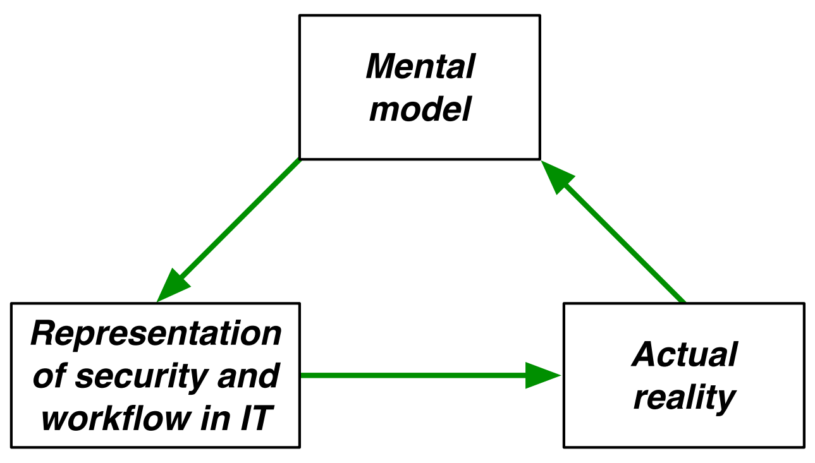


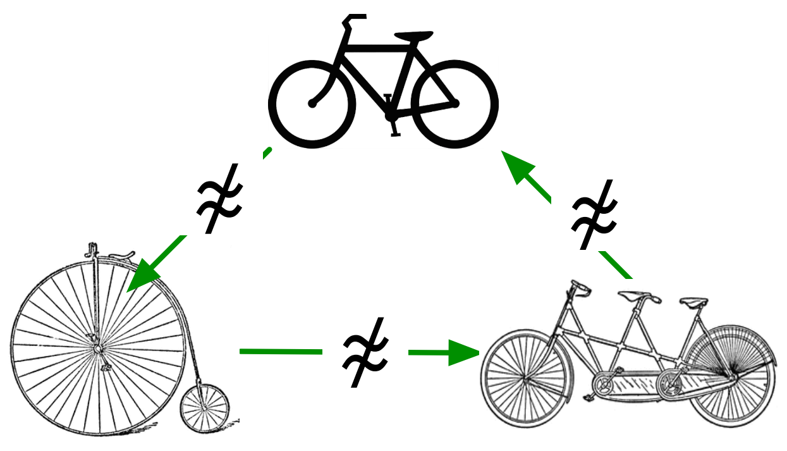


Regular semiotics: ***morphisms.***
Mappings ***preserve*** structure

Extending this Model to Security Circumvention

Smith and Koppel (2014) created a new triad for health IT.





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

We now extend to security:

- *Referent* → *thought*: the admin constructs a mental model of what she imagines is the actual enterprise workflow requirements.
- *Thought* → *symbol*: the admin reasons about security and work goals and construct a system configuration that she believes achieves these goals.
- *Symbol* → *referent*: this configuration in practice then generates some actual reality.

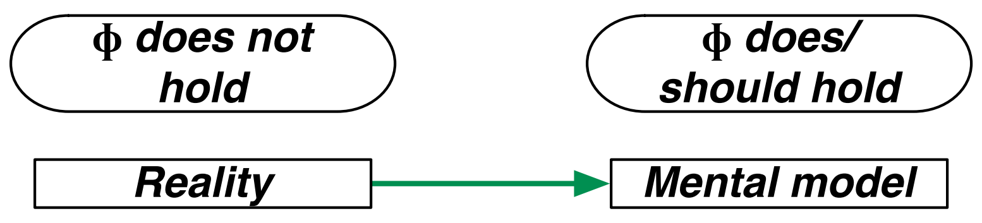
Policy creation:

- *Referent* → *thought:* Admin perceives risk from unattended computers in hospital
- *Thought* → *symbol*: Admin adds proximity detectors and automatic logout after timeout.
- *Symbol* → *referent*: Machines timeout when clinician turns away or detector is pointed wrong.

Policy circumvention:

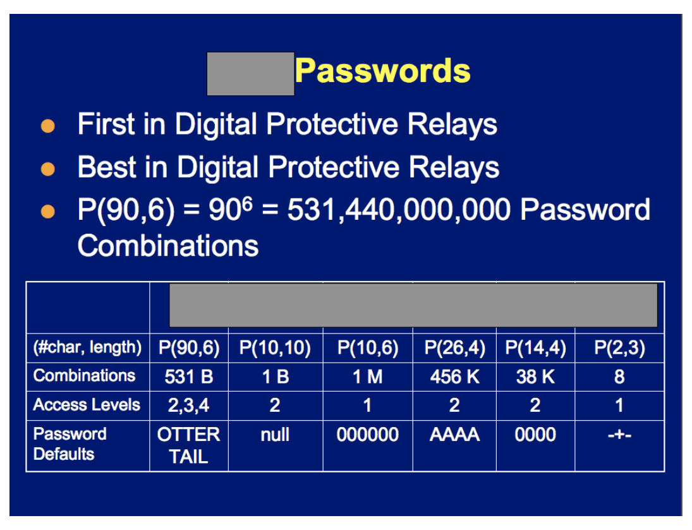
- *Referent* → *thought:* Clinicians perceive this system as not matching their desired workflow
- *Thought* → *symbol*: Clinicians place inverted styrofoam cups over detectors
- *Symbol* → *referent*: Net exposure is even worse

Loss of Static Properties



Lost Workflow Properties

- Electronic health records (EHRs) list oldest tests dfirst
- Computer physician order entry (CPOE) imposes "linear workflow" (Harrison et al., 2007)
- EHR limits box to N chars; no way for reader to know there's another box
- IEEE editing portal does not allow summary rejection
- Network flow anomaly tool fails to recognize only abuse
- Bona fide user cannot authenticate to credit bureau—because it uses knowledge-based authentication, based on data corrupted by id theft
- Policy requires nurses witness disposal of extra meds before disposal can happen.



[redacted] Passwords

- First in Digital Protective Relays
- Best in Digital Protective Relays
- P(90,6) = 90^6 = 531,440,000,000 Password Combinations

	[redacted]					
(#char, length)	P(90,6)	P(10,10)	P(10,6)	P(26,4)	P(14,4)	P(2,3)
Combinations	531 B	1 B	1 M	456 K	38 K	8
Access Levels	2,3,4	2	1	2	2	1
Password Defaults	OTTER TAIL	null	000000	AAAA	0000	-+-

Invariants made false

- "EHR reflects needed dose, not lethal dose"
- "IT system reflects actual IV dosage patient has received."
- "smart pump IT represents actual drug, dose, patient weight"
- "EHR reflects actual diagnosis, not insurance trick"
- "the EHR record's *author* field indicates the author"
- "'university travel portal for user A records only A's travel"

Provisioning

- Unix sysadmins confidently creating wrong access controls
- users at universities, govt, and P2P accidentally making private files world readable (Maxion and Reeder, 2005)
- investment bank employees unable to understand their own entitlements
- barrier to automated *role mining* is "interpretability" (Xu and Stoller, 2012)

Circumvention as Compensation

Adding functionality:

- Sticky notes, shared passwords
- US nuclear missiles had launch code "00000000" (Nichols, 2013)
- Using cred of authorized but deceased
- Rogue access points
- Bridging air gap
- Well-known defaults

Removing functionality:

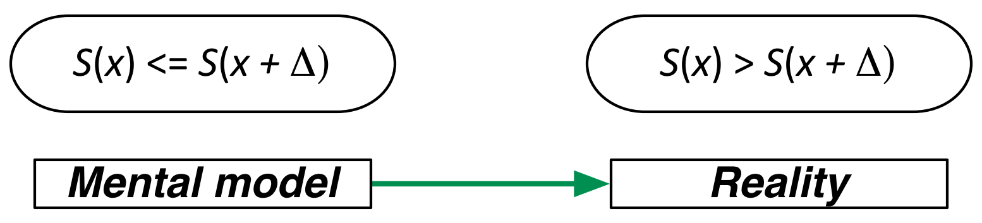
- disconnecting during remediation
- smart key in Faraday foil (Paul and MacNaughton, 2014)
- code silently removed by compilers (Wang et al., 2013)

Shadow systems:

- password-free telephone instead of online (Heckle, 2011)
- exfiltration by turning docs into images
- screen-scraping images into PowerPoint
- Dropbox instead of official Sharepoint
- work docs sent to home email
- govt IT going offsite to test porn filter
- govt users tunneling to university system
- govt users working from Starbucks

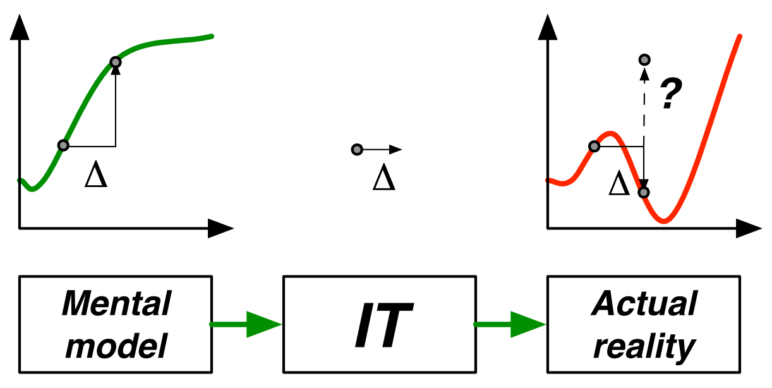
Loss of Monotonicity

We implicitly have some numeric function *S* taking a tunable parameter (e.g., password length) to the level of security achieved. The intention of the human is to tune the parameter *x* so as to maximize *S(x)*. However, if the mappings across the triad nodes fail to preserve crucial properties of this *x* vs *S(x)* curve, unfortunate things can happen.



Uncanny Descent: dialing security ***up*** can make the reality ***worse***

- requiring strong passwords leads to writing them down or relying on security questions
- adding computerized controls to medicine hurts patients by disrupting workflow (many examples)
- adding S/MIME led to worse trust decisions (Masone, 2008)
- adding effective security controls led to them being disabled by default
- limiting message size led to accidental exfiltration



Uncanny Ascent: dialing security ***down*** can make the reality ***better***

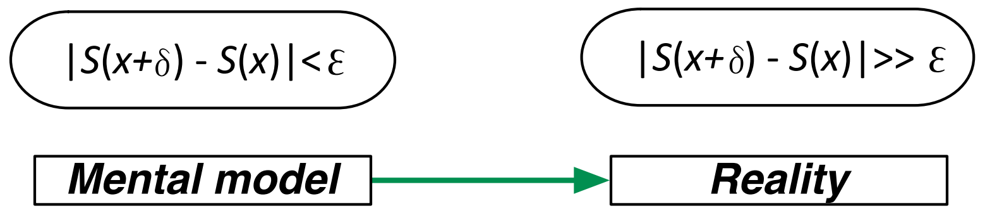
- eliminating unique passwords led to reduction in sharing
- shortening Gmail passwords can make them more secure
- having browser remember critical site password stopped phishing

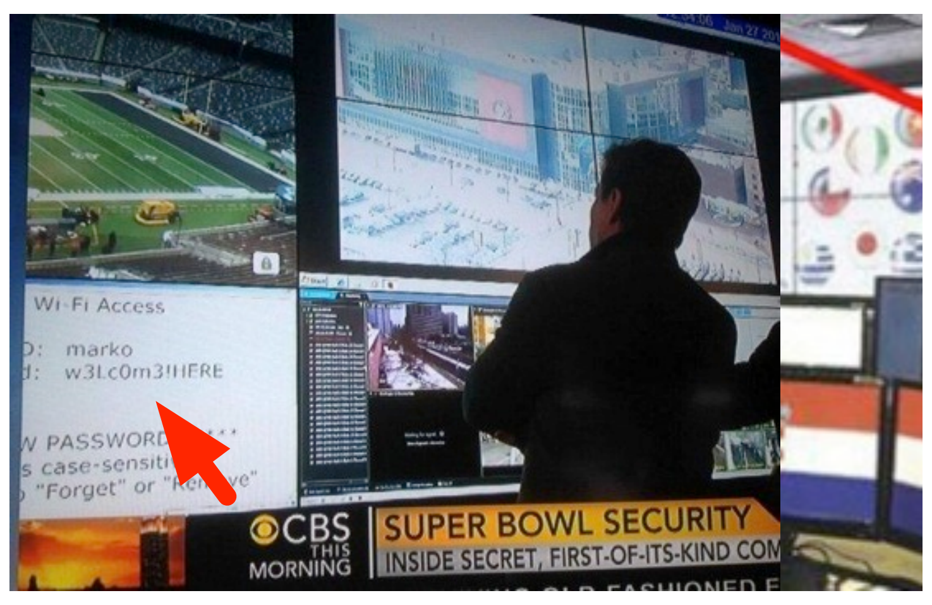
Uncanny Nop

- passwords must be distinct from last *N*—but users knew they checked via hash
- adding privileged secure WiFi—but users all use the public one
- educating users about good behavior doesn't change behavior (e.g., Riley, 2006; Yan et al., 2005; Dhamija and Perrig, 2000; Heckle, 2011).
- deleting material by deleting link

Loss of Continuity

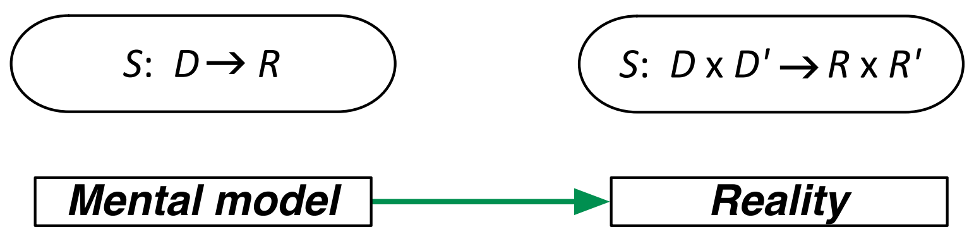
Small changes in configuration can yield surprisingly big changes in security reality





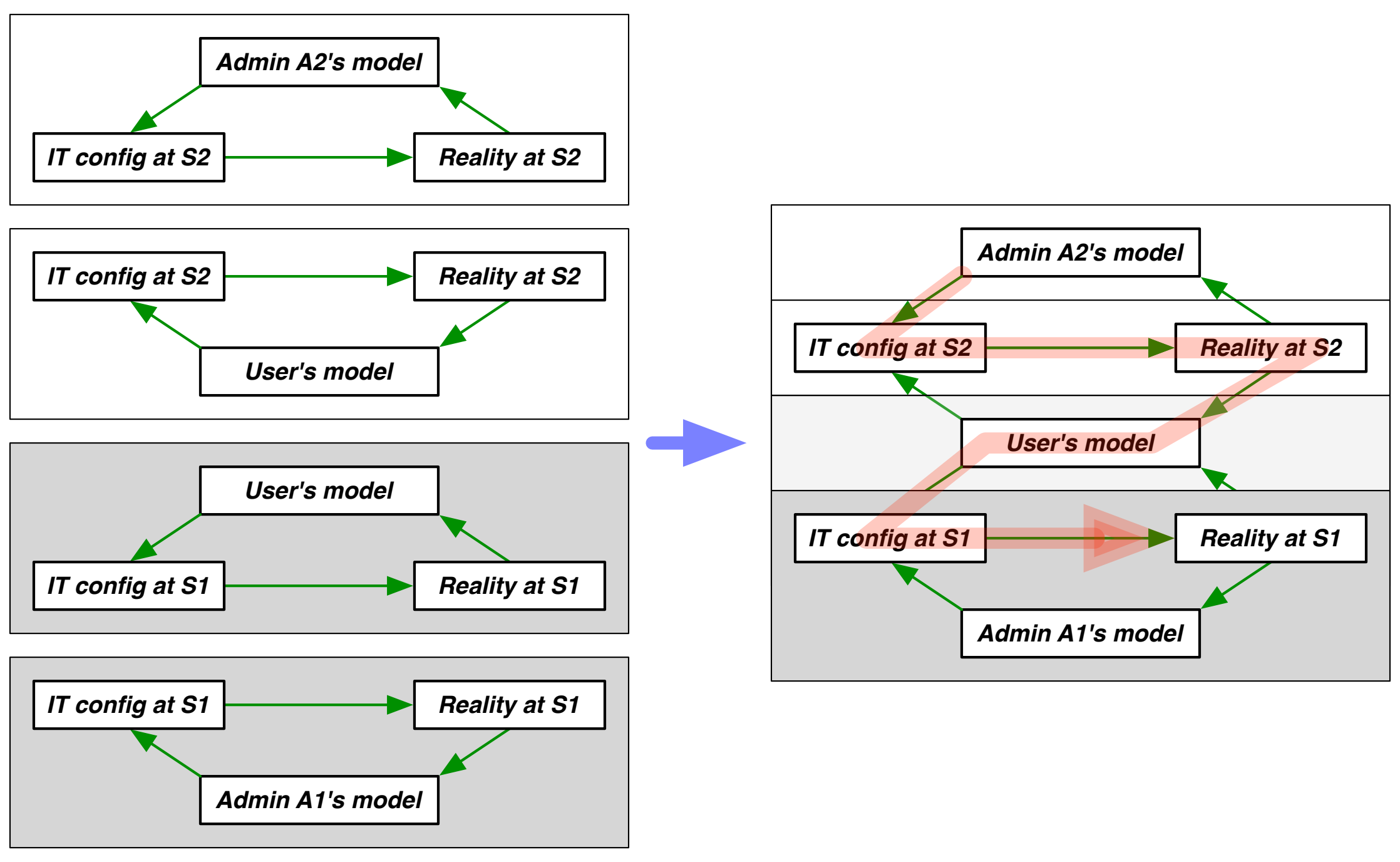
Domain and Range Trouble

Reality may have more parameters and consequences



Example: loss of locality of control. The actual security at S1 can change because of a policy change by the admin at a different S2!

- password re-use + leak
- training users to accept self-signed SSL
- training users to accept basic authentication
- requiring users to change passwords.



Next Steps

Mismorphisms lie at the heart of circumvention, because they characterize the scenarios that frustrate users—and often the resulting circumvention itself. In future work, we plan to distill this model into design principles for better security engineering, so that users can get their jobs done without working around the rules.

http://hot-sos.org/

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