Reasons for Cybersecurity Circumvention*

A Study and a Model

Sean Smith
PhD
Department of Computer Science
Dartmouth College
sws@cs.dartmouth.edu

Ross Koppel
PhD, FACMI
Department of Sociology
University of Pennsylvania
rkoppel@sas.upenn.edu

Jim Blythe
PhD
Information Sciences Institute
University of Southern California
blythe@isi.edu

Vijay Kothari
PhD Student
Department of Computer Science
Dartmouth College
vijayk@cs.dartmouth.edu

* This poster is an adaptation of an earlier paper: Mismorphism: a Semiotic Model of Computer Security Circumvention, Smith et al., HAISA 2015

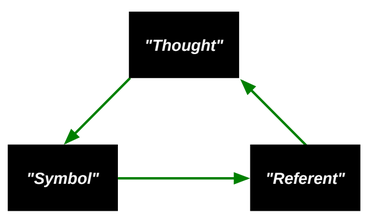
Introduction

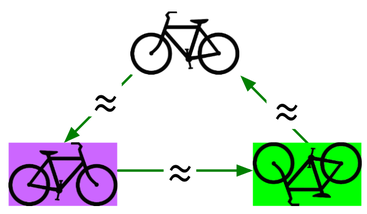
Users often work around security controls. We can pretend this doesn't happen, but it does.

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***.

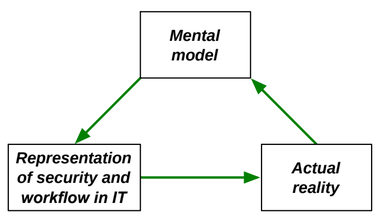


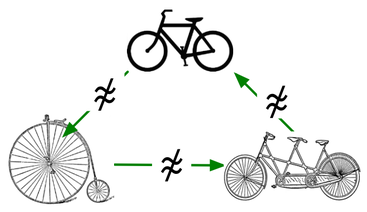


Regular semiotics: ***morphisms.***
Mappings ***preserve*** structure

We Ask Why Circumvention Occurs and How It Can Be Reduced

We extend the Ogden and Richards (1927) semiotic model to examine reasons for workarounds.





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 are the actual enterprise workflow requirements.
- *Thought → symbol*: the admin reasons about security and work goals and constructs a system configuration that she believes achieves these goals.
- *Symbol → referent*: this configuration in practice then generates some actual reality.

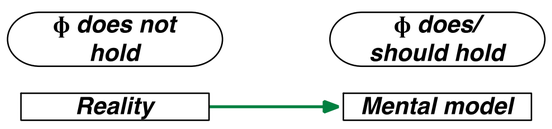
Policy creation:

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

Policy circumvention:

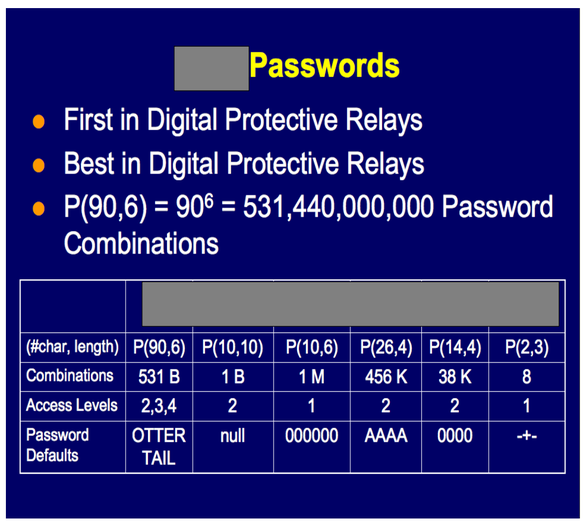
- *Referent → thought*: Clinicians perceive this system as not matching their desired workflow.
- *Thought → symbol*: Clinicians place inverted styrofoam cups over detectors.
- *Symbol → referent*: Net exposure is even worse.

Loss of Static Properties Result in Greater Vulnerabilities



Lost Workflow Properties:

•Electronic health records (EHRs) list oldest tests first.
•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 identity theft.
•Policy requires nurses witness disposal of extra meds before disposal can happen.



	[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 make 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)

User Circumvention of Authentication Protocols

Users are often obliged to work around authentication protocols to perform their tasks.

Adding Functionality:
•Sticky notes, shared passwords.
•US nuclear missiles had launch code "00000000" (Nichols, 2013).

Removing Functionality:

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

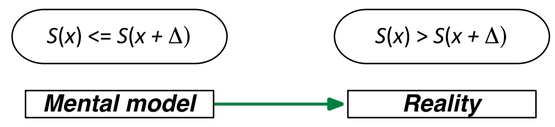
Shadow systems:

- 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.
- Government users tunneling to university system.
- Government users working from Starbucks.

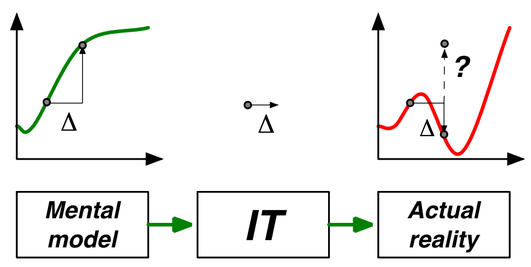
Turning Security Knobs Has Unintended Consequences

When security rules tighten, users who view them as incongruent with workflow needs are obliged to circumvent them, thereby creating a dip in actual security.

Loss of Monotonicity



We implicitly have some numeric function *S* that maps 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 leads to them being disabled by default.
- limiting message size leads to accidental exfiltration.

Uncanny Ascent: Dialing security ***down*** can make the reality ***better***.

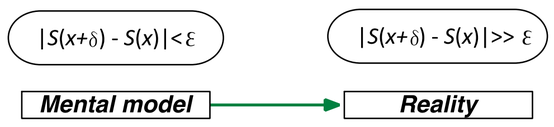
- eliminating unique passwords led to reduction in sharing.
- shortening Gmail passwords can make them more secure.
- having browser remember critical site password stopped phishing.

Uncanny nop: Dialing security ***up*** **or** ***down*** has ***no effect*** on the reality.
•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.

The system is as weak as its weakest link. With greater complexity, there are more vulnerabilities.

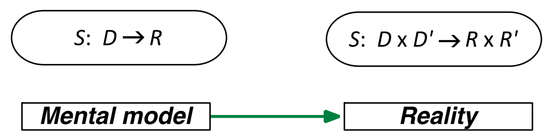
Loss of Continuity

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



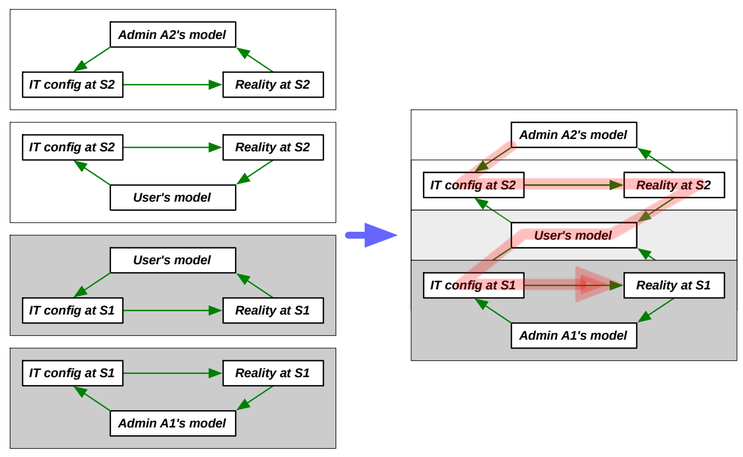
Domain and Range Trouble

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 reuse + leak.
- training users to accept self-signed SSL certificates.
- training users to accept basic authentication.
- requiring users to change passwords.



For more information on this and our other project work, visit http://shucs.org

Visit shucs.org to learn more about the Science of Human Circumvention of Security

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141.

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATIONTRUST INSTITUTE