Mismorphism: a Semiotic Model of Computer Security Circumvention (Poster Abstract) *

S.W. Smith
Dartmouth College
sws@cs.dartmouth.edu

R. Koppel
University of Pennsylvania
rkoppel@sas.upenn.edu

J. Blythe
University of Southern California
blythe@isi.edu

V. Kothari
Dartmouth College
Vijay.H.Kothari.GR@dartmouth.edu

ABSTRACT

In real world domains, from healthcare to power to finance, we deploy computer systems intended to streamline and improve the activities of human agents in the corresponding non-cyber worlds. However, talking to actual users (instead of just computer security experts) reveals endemic circumvention of the computer-embedded rules. Good-intentioned users, trying to get their jobs done, systematically work around security and other controls embedded in their IT systems.

This poster reports on our work compiling a large corpus of such incidents and developing a model based on *semiotic triads* to examine security circumvention. This model suggests that *mismorphisms*—mappings that *fail* to preserve structure—lie at the heart of circumvention scenarios; differential perceptions and needs explain users' actions. We support this claim with empirical data from the corpus.

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 [1, 2, 4]. 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.

Over the last several years, via interviews, observations, surveys, and literature searches, we have explored the often tenuous relationship among computer rules, users' needs, and designers' goals of computer systems. We have collected and analyzed a corpus of hundreds of circumvention and unusability scenarios.

Semiotic triads, proposed almost a century ago (e.g., [3]), offer models to help understand why human agents so often circumvent computer-embedded rules. We suggest that these triads provide a framework to illuminate, organize, and analyze circumvention problems.

In our poster, we present these ideas and support them with examples from our corpus. Our longer technical report provides a far more exhaustive presentation of examples (including many from interviews with parties who wish to remain anonymous). As we are working on developing a typology rather than supporting a hypothesis, many of the usual factors in confirmation bias to do not apply.

The Semiotic Triad.

In a previous paper [5], we organized an earlier corpus of usability problems in health IT according to mismatches between the expressiveness of the representation "language" and the details of reality– between how a clinician's mental model works with the representations and reality.

Somewhat to our chagrin, we discovered we were scooped by almost a century. In their seminal 1920s work on the meaning of language, Ogden and Richards [3] constructed what is sometimes called the *semiotic triad*. The vertices are the three principal objects:

- What the speaker (or listener/reader) *thinks*
- The *symbol* they use
- The actual item to which they are *referring*

Much of Ogden and Richards' analysis stems from the observation that there is not a direct connection from symbol to referent. Rather, when speaking or writing, the referent maps into the mental model of the speaker and then into the symbol; when reading (or listening), the symbol maps into the reader's (listener's) mental model, which then projects to a referent, but not necessarily the same one. For example, Alice may think of "Mexico" when she writes "this country," but when Bob reads those works, he thinks of "Canada"—and (besides not being Mexico) his imagined Canada may differ substantially from the real one.

As we now consider a new corpus of scenarios in security circumvention and other authentication misadventures, we realize that this framework will also apply. We have a set of IT systems. Each system serves a set of users, and mediates access between these users and a cross-product of actions and resources. Each system has an IT administrator who

*A full version of this paper is available at
www.cs.dartmouth.edu/reports/abstracts/TR2015-768/

HotSOS '15 Apr 21-22, 2015, Urbana, IL, USA
ACM 978-1-4503-3376-4/15/04.
http://dx.doi.org/10.1145/2746194.2746219

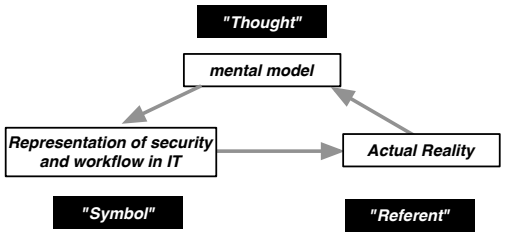

Figure 1: The basic Ogden-Richards triad, moved into 21st-century IT; the arrows indicate the main direction of mappings.

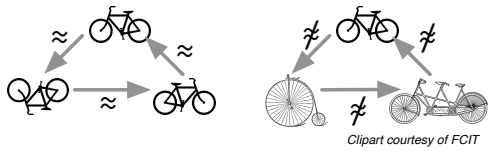

Figure 2: Standard semiotics considers structure-preserving mappings between the nodes of the triad (left); in circumvention semiotics, we think about mappings that fail to preserve structure (right).

worries about the security configuration—as well as users who worry about trying to use the resulting system for their actual work. For different systems, the user sets are not necessarily disjoint.

The interaction between the reality, the IT representation, and the mental models correspond to the vertices in Ogden and Richards' triad:

- *Thought*: the *mental model* a party has about the actions users can and cannot (or should and should not) do with resources.
- *Symbol* (i.e. *configuration*): the representation of security policy within the IT system itself; the built-in functionality of the IT system, intended to express the correct workflow. (Here, we mean policy as the actual machine-actionable expression of admin intention, not a published instructional document.)
- *Referent* (i.e. *reality*): the actions users can and cannot do with the resources, in reality; the de facto allowed workflow.

Figure 1 sketches this basic triad. In this framework, the primary mappings are counterclockwise: Thanks to the connection of IT and reality, we now have a direct symbol-referent connection, improving on (or at least complicating) the merely linguistic world Ogden and Richards explored. Note however, that ordinary users also participate in this triad, and that mappings in the other direction can also be interesting: e.g., investment bankers trying to infer which of their entitlements are actually necessary in their daily job (symbol → thought, then thought → referent).

Mismorphism.

The semiotics of language and the effective communication of meaning focus on *morphisms*—"structure-preserving mappings"—between nodes of the triad. However, with IT usability problems we are concerned instead with ineffective communication—and hence focus on what we call *mismorphisms*: mappings that *fail* to preserve important structure

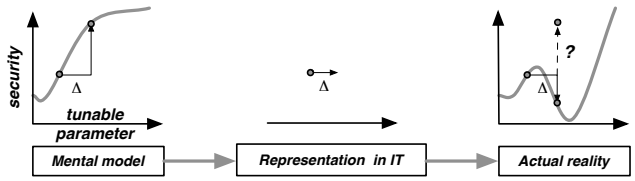

Figure 3: In what we call the uncanny descent, the mental model shows that dialing up security improves security; but when this change is mapped through the IT configuration into reality, security actually decreases.

when we go from z in one node of the triad to its corresponding z' in another (Figure 2).

Often, in questions of security design, implementation, and use, we implicitly have some function numerical $\mathcal{S}$ taking a tunable parameter (e.g., password length) to the level security achieved. The intention of the human is to tune the parameter x so as to maximize $\mathcal{S}(x)$. However, if the mappings across the triad nodes fail to preserve crucial properties of this x vs $\mathcal{S}(x)$ curve, unfortunate things can happen.

Catalog.

In the full paper, we explore this idea by identifying specific categories of mismorphism—including loss of monotonicity (e.g. Figure 3), loss of continuity, and loss of domain and range properties—and supporting them with items from our corpus.

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.

Acknowledgment.

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

References

[1] H. R. Bernard and G. W. Ryan. *Analyzing Qualitative Data: Systematic Approaches*. Sage Publications, 2010.

[2] K. Charmaz. Grounded theory. In *SAGE Encyc. of Soc. Sci. Research Methods*, pages 440–444, 2003.

[3] C. Ogden and I. Richards. *The Meaning of Meaning*. Harcourt, Brace and Company, 1927.

[4] S. F. Pettigrew. Ethnography and Grounded Theory: a Happy Marriage? In *NA - Advances in Consumer Research*, volume 27, pages 256 – 260. Association for Consumer Research, 2000.

[5] S. W. Smith and R. Koppel. Healthcare information technology's relativity problems: a typology of how patients? physical reality, clinicians? mental models, and healthcare information technology differ. *Journal of the American Medical Informatics Association*, 21:117–131, 2014.