Flawed Mental Models Lead to Bad Cyber Security Decisions: Let's Do a Better Job

Sean Smith, Vijay Kothari,* Jim Blythe,† Ross Koppel‡*

** Dartmouth College, † ISI, University of Southern California,, ‡ University of Pennsylvania*

Conventional computer security wisdom implicitly assumes models about humans and human organizations such as:

- Only bad people circumvent security controls. (Corollary: good users never share passwords.)
- It's actually possible for organizations to create and maintain a perfect electronic representation of the access control policies they need.

These models then translate into practices that conventional wisdom blesses as good. For just two examples:

- To make a system more secure, the security administrator should require stronger passwords and frequent password changes.
- To reduce inadvertent exposure of data from semi-public workstations, it's good to have user sessions automatically time out.

Unfortunately, fieldwork (by us[1] and many, many others) shows that these models are not necessarily true, and that the practices resulting from them do not necessarily make things better---and can in fact make things worse. If we blindly apply conventional wisdom without validating the assumptions upon which it is based, we don't see the security gains that we might expect. This gives rise to *uncanny descents*, scenarios where we turn up security knobs with the expectation that aggregate security will improve, but we instead observe that things get worse.

We posit that these problems all result from the same underlying cause: flawed models of the interaction of humans and technology. Security policies, mechanisms, and recommendations are designed according to a human-conceived model of security, whether designed directly by the policy designer (e.g., by following tradition) or indirectly by the utilization of risk assessment or other security tools that are created by humans.

In previous work, we've characterized these causes as *mismorphisms*, ``mappings that fail to preserve structure"---especially mismatches between the security practitioner's mental model, the user's mental model, the model arising from system data, and the reality.

This situation gives rise to a grand challenge: how do we unravel this problem? Flawed models lead to bad decisions. We need a way to make better decisions.

This poster explores this problem, and presents both our current work as well as where we plan to go next. A solution would likely have several components: effective ways to talk about aggregate security in practice, effective ways to discover and correct flaws in mental models, and effective ways to make better security decisions despite such flaws.

[1] E.g., S.W. Smith, R. Koppel, J. Blythe, V. Kothari. "Mismorphism: a Semiotic Model of Computer Security Circumvention." *International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015).* July 2015