Modeling Human Security Behavior
Recent Results on Understanding Compliance

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

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

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

Why Do We Need to Model Human Behavior?

Understanding human behavior to critique and suggest better security policies.

Security practitioners must make decisions that reflect the interplay between human behavior and systems. As our other posters show, this can be significant and complex. How can we predict it well enough to test or discover better, human-aware policies and security tools?

The role of human subject experiments.

Our understanding of human behavior in security must be rooted in observation and experimental work. However:

Human subject experiments are too expensive to use in every case, to test every potential solution.

This is particularly true for teams, or more than a few individuals, or organization-wide effects or the interplay between a number of organizations.

Models based on experimental data.

When it is infeasible to test security decisions with human participants before going live, a valuable approach is to build models of human behavior, allowing better informed decisions.

To develop models that are useful in practice, we focus on modeling real-world scenarios and ensuring that the models capture the relevant facets of human behavior.
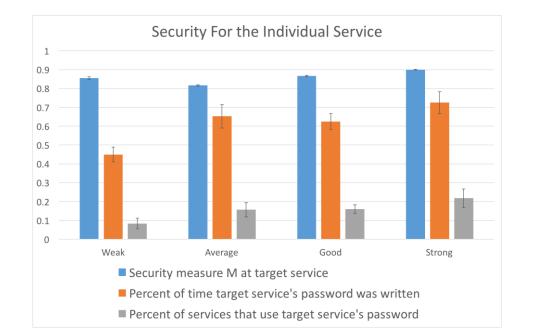
We aim to base each model on relevant experimental data, by our group or others, and to validate any extensions required to fit .

Platform for reuse of experimental data.

This approach makes experimental data more useful to practitioners. Our platform for building agent models, below, also provides a repository where this data can be available in an easily extensible, plug-and-play for for practitioners.

DASH: Dual-Process Modeling Toolkit

Our platform for agent-based modeling of security decisions is DASH: Deter Agents Simulating Humans.

DASH is inspired by work in cognitive science that models some distinguishing features of humans:
• **Dual process**: We sometimes think carefully about our next action, but more often simply follow routine.
• **Mental models**: When we think about security issues, most people do not have a good understanding of the situation but reason from analogy with physical security, or use models like healthcare (e.g. 'virus').
• **Bounded rationality**: we are affected by cognitive load, deadlines, fatigue and emotion.
• **Replanning:** When we follow a plan, we continually check that it is working and can re-plan on the fly.

A dual process model combines thoughtful and instinctive behavior

Mental models capture approximate reasoning

Reactive planning models human ability to adapt and re-plan.

Effects of cognitive load, fatigue etc. typically based on experimental data.

Plug-and-play module reuse
• of experimentally validated data
• of fragments of agent behavior, *e.g.* attacker, password user etc.
• of world models

Further simplifies agent modeling while supporting best practices

Recent and current work on DASH:
• Easier modeling language based on python
• Support for multi-agent models and experiment management
• Compositional reuse of agent fragments
• Discrete-event model supporting telescoped time
• Use in human subject experiments mixing DASH agents and subjects

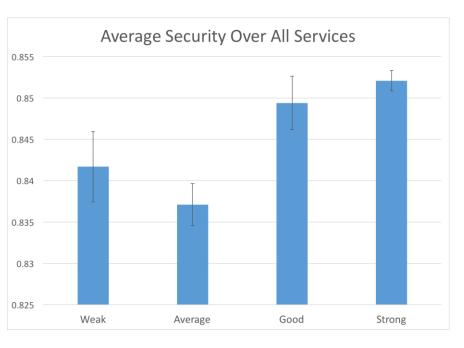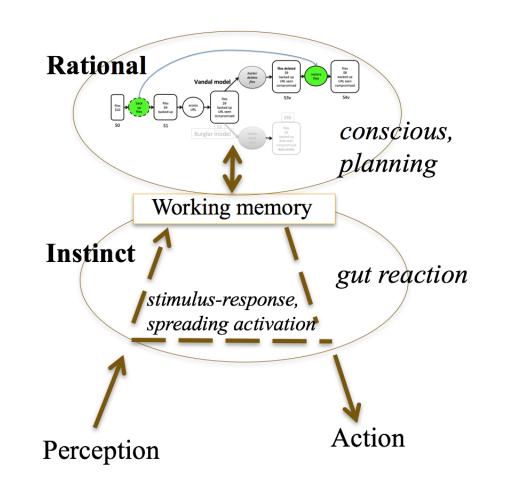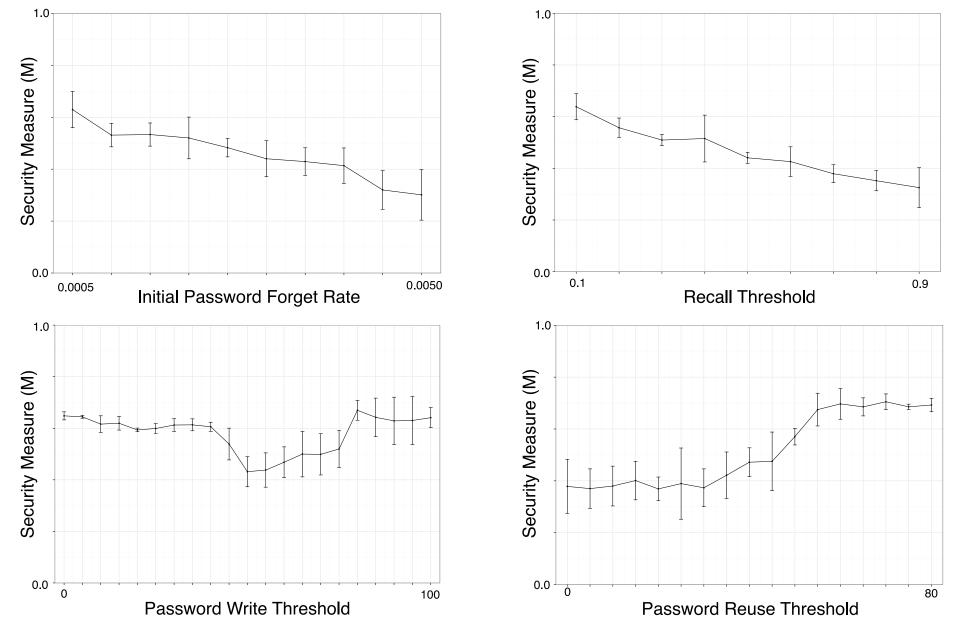For more information on this and our other project work, visit http://shucs.org

Modeling Network Effects in Password Use

What is the best password policy for an organization? We have developed and are continuing to improve a password management simulation to uncover the likely consequences and value of a policy. The simulation is also used to estimate how a policy impacts the aggregate security of a group of services.

DASH agents create and use accounts on various services and manage their passwords. The cognitive burden associated with remembering many passwords, along with a tendency to forget over time, drives users to circumvent recommended password advice. Agents use coping strategies observed in human subjects (e.g., Florencio et al., 2014); they write passwords down and they reuse them between sites.

Security vs. Target Service's Password Composition Policy Strength

Validation and Sensitivity Analysis

To understand how our model may depend on assumptions, we conducted a sensitivity analysis. We also partially validated our model by comparing the outputs of simulation runs to empirical data from the literature. Korbar et al., 2016 provides an overview of a recent iteration of the password simulation along with discussion of validation attempts.

We are currently improving the faithfulness of user agent behaviors and building attacker agents that employ various attack strategies to replace a hard-coded security measure. For example, we model how an attacker might gain access to a password list and use it to access accounts on other services.

Effects of Workflow on Security: Resource Contention and Workarounds

Consider a clinical setting where clinicians must used shared resources (e.g. standalone computers, COWs) in order to perform their primary tasks. When a worker logs out another to access a resource, there is a danger that medications are recorded for the wrong patient.
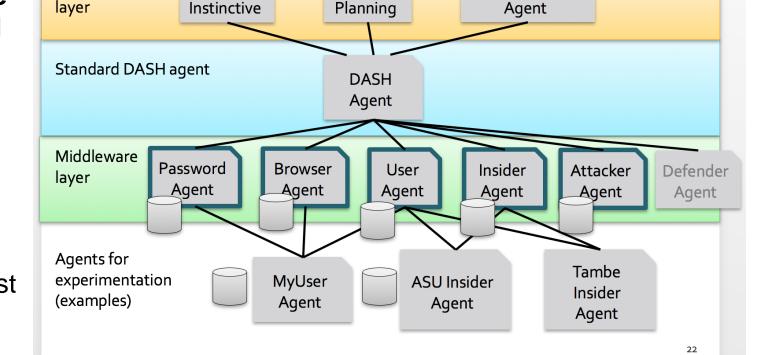
Auto-logout mechanisms (e.g. proximity or time-based) that reduce the danger are likely to be defeated by clinicians, because of the extra time demands on a busy workload (see our poster on reasons for circumvention).

Much of the information that could predict this circumvention, and hence the true value of a timeout policy, is about the workflow of the group, which is easier to measure than behavioral patterns.

Our multi-agent simulation helps predict the level of contention for shared resources based on task time and numbers of patients, workers and resources, and the probability of workarounds to auto-logout.

Our aim is to help configure existing technology so as to minimize workflow interference. For example, we can help estimate the optimal timeout threshold before auto-logout.

Current Work

In addition to development work on the DASH platform (see left) and on modeling scenarios (above):

Pilot testing a password behavioral experiment to run on Amazon Mechanical Turk to uncover circumvention behavior when humans manage passwords on multiple accounts under cognitive load and time pressure. We will explore the consequences of this behavior in our simulation.

Collaborating with researchers at the University of Pennsylvania to use the data to learn Markov models of password behavior that can be incorporated into DASH agents, improving the simulation.

Collaborating with researchers at Arizona State and USC to develop human subject experiments that combine humans and DASH agents networked on DETER, with humans alternately playing the roles of defenders or attackers, to understand human behavior in cyber attacks.

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

INFORMATION TRUST INSTITUTE