http://shucs.org

Modeling Human Security Behavior
Recent Results on Understanding Compliance

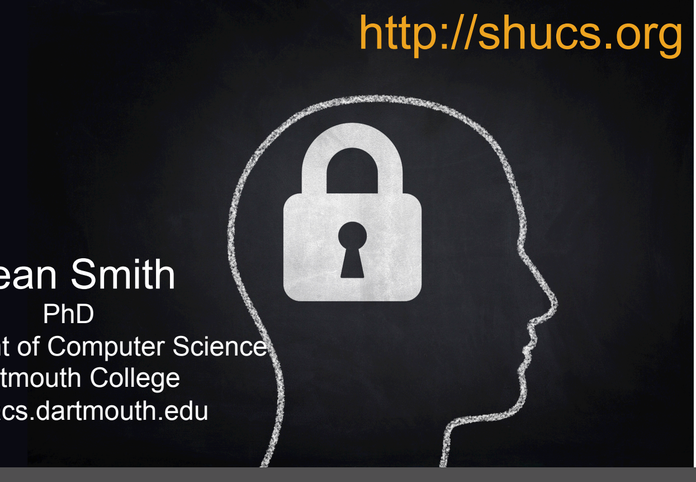
Jim Blythe
PhD
Information Sciences Institute
University of Southern California
blythe@isi.edu

Christopher Novak
Undergraduate Student
Department of Computer Science
Dartmouth College
novak.17@dartmouth.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



WHAT WE DID

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.

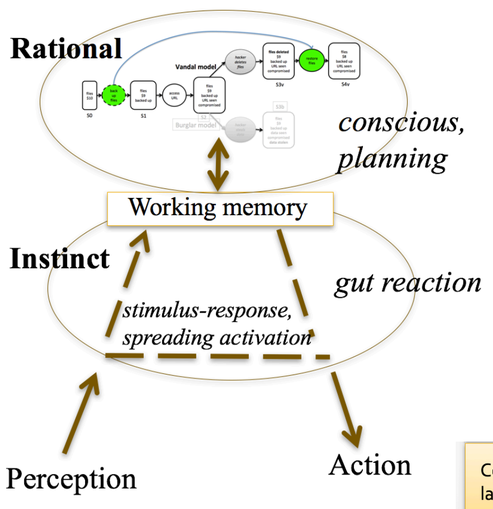
This approach makes experimental data more useful to practitioners. Our platform for building agent models, below, also provides a repository where this data can be available in an easily extensible, plug-and-play for for practitioners.

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

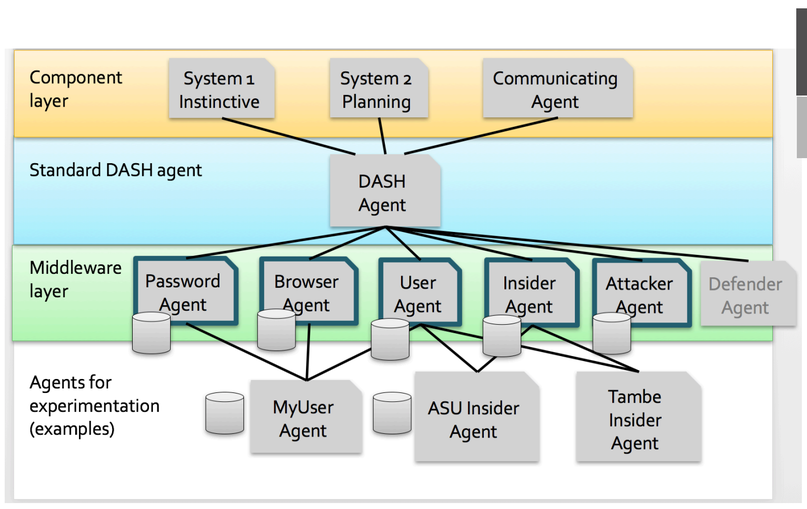
Reactive planning models human ability to adapt and re-plan.

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 improvements:

- Easier modeling language based on python
- Support for multi-agent models and experiment management
- Discrete-event model supporting telescoped time
- Use in human subject experiments mixing DASH agents and subjects:

Current Experimental Work

Pilot testing a behavioral experiment 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.

We will use the data to learn Markov models of password behavior that can be incorporated into DASH agents, improving our simulation (collaboration with U Penn)

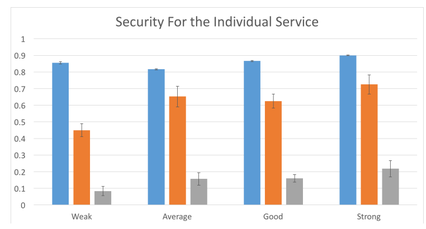
Human subject experiments with both humans and DASH agents networked on DETER, with humans alternately playing the roles of defenders or attackers, to understand human behavior in cyber attacks. (one completed in collaboration with Arizona State, one proposed with USC)

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.

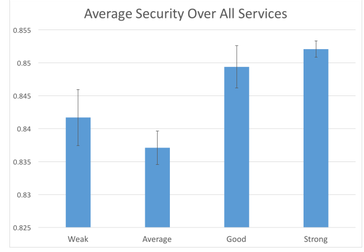
Security vs. Target Service's Password Composition Policy Strength



Security measure at service

Proportion of written passwords

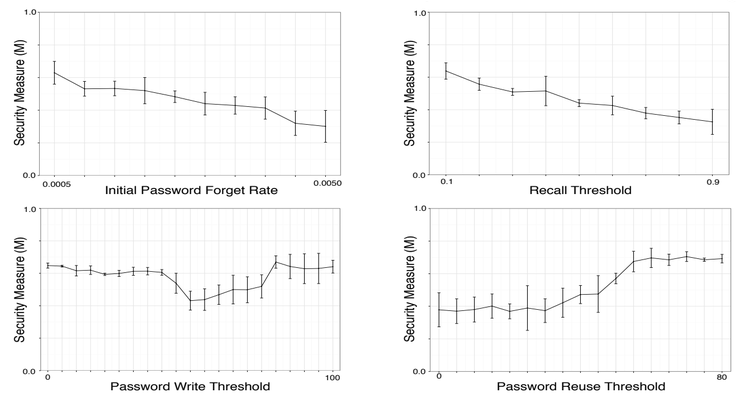
Proportion of reused passwords



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 have recently built 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.



WHAT COMES NEXT

Validation

Our simulations must match reality to be informative. As the quality and quantity of available data improves and expands, we continually refine our simulations. Our experimental work (see left) is aimed at validation.

Machine Learning to Validate and Improve Agent Simulations

Given data on human behavior we will tune agent and agent community behaviors through optimization of parameters to best match the data.
If our assumptions lead to agents that cannot match the data well, this indicates that something is missing in our model and the data can provide evidence of what is missing. We can also optimize the agent specification to find the *simplest* model that fits given data well.
Finally, components of behavior can be learned from data and used in agents in plug-and-play fashion, such as rules for predicting password reuse. This approach leads to *evidence-based agent-based models*.

Modeling New Aspects of Security in the Wild

Security Effects of Workflow: Resource Contention & Workarounds

Consider a clinical setting where clinicians must used shared resources (e.g. standalone computers) 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 [personal communication].

The true value of the timeout policy depends on this workaround, which largely depends on the stress produced on the workflow. This is often simpler to model 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. It can then help estimate the optimal timeout threshold before auto-logout.

Modeling and Understanding Social Engineering Attacks

Social engineering attacks exploit (and sometimes even create) human vulnerabilities unbeknownst to the victim. For example, a phishing email may dupe users (e.g., with a malicious "reply-to" field) or induce emotion (e.g., by telling the victim she won a prize) to persuade them to commit actions they would not otherwise perform.

We are beginning to model such attacks, building on existing literature that suggests impulsivity, emotion, fatigue, personality traits, and other factors affect user susceptibility to phishing.
DASH models can help us understand the contextual factors in susceptibility to phishing attacks, and provide insights that help security practitioners make sound decisions to mitigate phishing risks.

Tools for Making Better Decisions

With our simulations we aim to build insight into the complex effects of security policy in the real world that helps practitioners build more effective solutions in their context.

We will foster communication to build more realistic simulations, but more importantly bridge the gap with policy development and provide tools the practitioner can use to gain insight into their specific situation.

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