Understanding Human Cognition in Computer Network Defense

PI: David Schuster, PhD. San Jose State University

http://www.vectrlab.net/research.php?area=cybersecurity

VECTR Lab

Improving Human Decision Making in Network Defense

Effective decision making by cybersecurity professionals is a critical layer in network security. Mental models support situation awareness, but these cognitive factors are poorly understood in network defense contexts.

Challenges to cybersecurity professionals:

- Cost and frequency of attacks
- High workload among cyber defenders
- Rapidly evolving threat landscape
- Unmet cybersecurity professional workforce need

Our Objective: Inform assessment, training, selection, and development of next-generation tools for cybersecurity professionals by identifying the cognitive outcomes that predict successful threat response.

Leveraging cognitive outcomes of expert cyber defenders

↓

Informing assessment, training, selection, and next-generation defense tools

↓

Workforce development and a strategic advantage against novel threats

Scientific Approach

- Identifying content and structure of cybersecurity professionals' knowledge in computer network defense
  - Quantifying situation awareness
  - Identifying mental models
  - Iterative validation with experts
- Developing empirically derived assessments of mental models and SA for cyber security professionals
- Supporting new training techniques that transfer broadly to cyber security decision making

Background

- Mental models are internal representations of the task environment.
- Situation awareness is goal-relevant knowledge held during task performance.
- Both constructs have been applied to technology design and training across domains, but measures are task-specific.

Methods

- Cognitive task analysis
  - Cybersecurity professional survey
  - Knowledge elicitation methods (e.g., concept mapping, knowledge audit)
- Measure and assessment development informed by cognitive task analysis
- Measure validation using simulation

Progress to Date

- Bootstrapping and literature review: integration of published materials to support cognitive task analysis
- Draft cyber situation awareness model
- Cognitive task analysis protocol development

Next Steps

- Situation awareness model validation and iteration
- Knowledge elicitation for mental models
- Testbed development
- Increasing the number of expert participants

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

SJSU SAN JOSÉ STATE UNIVERSITY