Comparing Learning Gains in Cryptography Concepts Taught Using Different Instructional Methods and Measuring Cognitive Processing Activity of Cryptography Concepts

Joseph Beckman (beckmanj@purdue.edu, Melissa Dark, Ph.D. – Primary Investigator

Problem
“...[a] desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate, and reconstitute systems after an attack.” (Evans and Reeder, 2010) and the difficulty of building experts through education in complex mathematical concepts such as those underlying cryptography (Sims & Chi, 2011).

Goal
Cybersecurity experts with not only deep technical skills, but also the capabilities to recognize and respond to complex and emergent behavior, as well as a “security mindset”, which includes mastery in using abstractions and principles, assessing risk and handling uncertainty, problem-solving, and reasoning; coupled with facility in adversarial thinking. This study focuses on the instruction of cryptography principles.

Research Questions
1. When cryptography instruction is delivered to students using instructional methods focused on representational understanding and representational fluency, does the order of use of these methods in instruction matter? That is, does learner expertise in the representational forms used in instruction support learning through translation among representational forms, does translation support expertise in representational forms, or neither?
2. Does prior knowledge of mathematics impact cryptography learning? If so, how?
3. Can processing cryptography concepts be measured in cognitive performance using fMRI and is cognitive processing of cryptographic concepts influenced by instructional method?

References