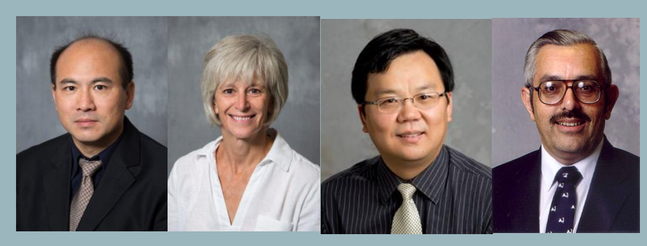
CybeRFM

-- Enhancing Cybersecurity Education Through a Representational Fluency Model

PIs: Dr. Baijian Yang, Dr. Melisa Dark, Dr. Victor Chen, and Dr. Sam Wagstaff

http://va.tech.purdue.edu/CyberFM



The 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).

The Goal

Create 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.

Hypotheses

- Representational Fluency can learners grasp complex cybersecurity concepts and principles
- Model Eliciting Activities (MEAs) can help build **more** robust mental models on cybersecurity

Approach

- Cryptography class split into control group and treatment group
- MEAs with Representational Fluency are designed for the treatment group
- Pretest and post test are evaluated using fMRI scans while subjects are responding to crypto questions with multiple representations

DESIGN AND METHODS:

Participants:

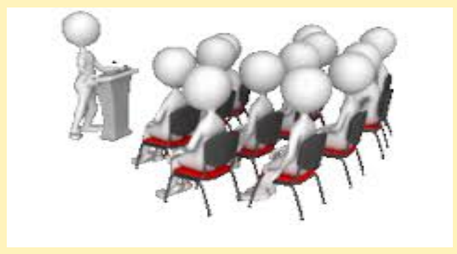
Control Group (N=31)

Treatment Group N=19

Comparison of coursework scores

fMRI Brain Pre Scan

Traditional Expository Teaching



MEA with Representational Fluency Teaching Method

fMRI Brain Post Scan

Outcomes:

1) *MEAs contextualized for cryptography*
2) *Between group comparative analysis of MEA and expository teaching in developing representational fluency*
3) *…and in students' executive function*

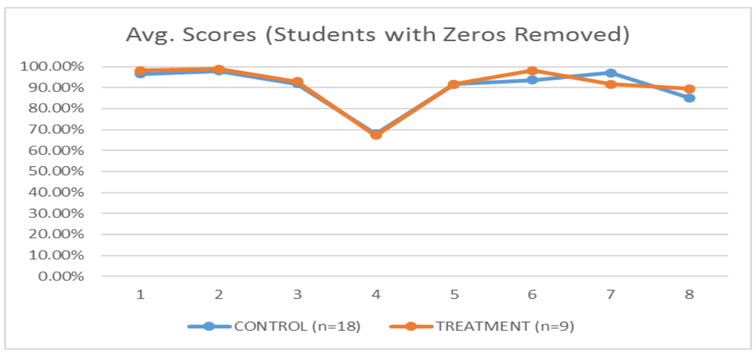
Artifacts Generated

- 5 MEAs designed for CS355
  - Cryptanalyses
  - Polyalphabetic Cipher
  - Key Exchange
  - Zero Knowledge Transfer
  - Digital Cache
- 4 MEAs designed for CNIT 555/370
  - Cryptanalyses
  - Cryptograph Principles
  - Symmetric Encryption
  - Public Encryption
- Abstract to ASEE 2017 accepted

Progress of the Current Study

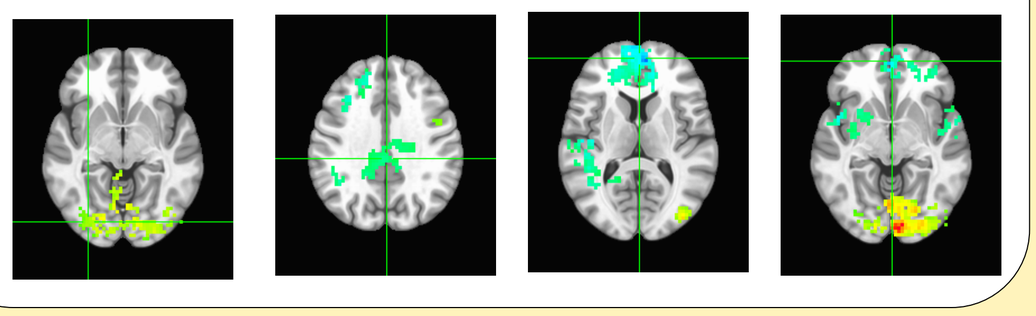
- *Collected Data:*
- Pre and Post Course fMRI Scans
- Scores on responses to questions given to subjects during fMRI scanning
- Score data for all graded course activities

Analysis – Classroom Grade Data



Analysis (In Progress) – fMRI Scan Data

Graphical Language Math Multiple



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

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

National Science Foundation
WHERE DISCOVERIES BEGIN

PURDUE UNIVERSITY