Employing Model-Eliciting Activities in Cybersecurity Education

Mayari Serrano
Alejandra Magana
Baijian Yang
Department of Computer and Information Technology, Purdue University

INTRODUCTION

College cybersecurity courses should ensure that activities employed can engage students in learning and allow translation from conceptual knowledge to practice. We propose to use model-eliciting activities (MEAs) to develop students’ representational fluency in the cybersecurity domain. The cybersecurity topic chosen for the MEA implementation was Hyper-Text Transfer Protocol Secure (HTTPS). The MEA developed, “Migration to HTTPS”, comprises core concepts of HTTPS and their application on a real-world cybersecurity tasks.

OBJECTIVES

- Illustrate how design principles were applied to construct a “Migration to HTTPS” MEA, along with the justifications of how learning objectives were aligned with the assessment procedures.
- Explain how the MEA was implemented followed by presenting the results of our pilot study.
- Determine the implications of the MEA in teaching and learning in Cybersecurity education.

METHOD

The activity was pilot tested with a group of 18 students from a three-year program equivalent to a third-year Electrical and Computer Engineering, who participated in a five-hour workshop in cryptography.

RESULTS

ME implementation can be used as a new resource to enrich learning outcomes in cybersecurity education. Participants’ mental models of the topic show several misconceptions related to basic concepts of cybersecurity. Text-based answers, and graphic-based answers unveiled many conceptual gaps of between perceived concepts and the actual knowledge.