New Orleans JAZZED about Engineering Education

Paper ID #15859

Employing Model-Eliciting Activities in Cybersecurity Education

Mrs. Mayari Illarij Serrano Anazco P.E., Purdue University, West Lafayette

MAYARI SERRANO is currently a graduate research assistant in the College of Engineering at Purdue University. She earned her B.S. degree from the Army Polytechnic School, Quito, Ecuador. She completed her M.S. in Computer and Information Technology at Purdue University. Mayari is currently a PhD student at Purdue University and is working in for the Women in Engineering Program. Her interests include foster STEM enthusiasm, and technology innovation.

Dr. Alejandra J. Magana, Purdue University, West Lafayette

Alejandra Magana is an Associate Professor in the Department of Computer and Information Technology and an affiliated faculty at the School of Engineering Education at Purdue University. She holds a B.E. in Information Systems, a M.S. in Technology, both from Tec de Monterrey; and a M.S. in Educational Technology and a Ph.D. in Engineering Education from Purdue University. Her research is focused on identifying how model-based cognition in STEM can be better supported by means of expert technological and computing tools such as cyber-physical systems,visualizations and modeling and simulation tools.

Dr. Baijian Yang, Purdue University

Dr. Yang is current an Associate Professor at Department of Computer and Information Technology, Purdue University

Employing Model-Eliciting Activities in Cybersecurity Education

Abstract

College cybersecurity courses should ensure that the 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. The activity was pilot tested with a group of 12 third-year Electrical and Computer Engineering undergraduate students who participated in a five-hour workshop in cryptography.

In this paper we describe the underlying learning theory that guided our rationale for using MEA as a pedagogical approach to promote deep learning in cybersecurity principles. We also 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. We then explain how the MEA was implemented followed by presenting the results of our pilot study. The paper concludes with the implications of the MEA and future work to future promote teaching and learning in Cybersecurity education.

Introduction

Prepared cybersecurity workforce is necessary to fight against cyber-treats and preserve the country sovereignty [1]. It is estimated the workforce shortage in the U.S. public sector alone was about 20,000 - 30,000 per year. This shortage is both one of quantity and quality. "We not only have a shortage of the highly technically skilled people required to operate and support systems we have already deployed, we also face an even more 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" [2]. The Evans and Reeder report notes that it is the consensus of the Commission that the current professional certification regime is not merely inadequate; it creates a dangerously false sense of security because currently available cybersecurity professionals all too often focus on demonstrating expertise in documenting compliance with policy and statutes rather than expertise in actually mitigating risks and preventing and responding to attacks.

The report also finds that although our colleges and universities have been producing security graduates with advanced technical skills, producing graduates with deep technical skills who are able to work in this highly complex and emergent domain is not easy. Cybersecurity is complex; the complexity does not just lie in the individual components to be protected, i.e., computers, and the software that runs on them. These components are connected into networks that are even more complex. Cybersecurity experts need deep technical skills along with capabilities to recognize and respond to complex and emergent behavior.

To our knowledge, not much work has been done on the development of expertise in cybersecurity. As a community, we are lacking research-based educational theory that can

inform the education of needed cybersecurity experts. In this work, we approach this problem by employing modeling-eliciting activities and evaluate if it will help promote students to cultivate deep understanding and critical thinking skills in the field of cybersecurity.

College cybersecurity courses should ensure that the 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. MEAs are activities that intent to simulate real-word client-driven scenarios. And the success of these MEA activities rely on teamwork and the students' abilities to apply concepts. Properly constructed and implemented MEAs can increase the use of: (1) student reflection tools in assessments, and (2) learning technologies. MEAs require students to iteratively build, test and refine their knowledge by encouraging students to build different forms of representations and connect and translate among them [3]. These activities focus on eliciting from students conceptual models that they iteratively revise in problem-solving episodes [4].

Conceptual Framework

Models and Modeling is the conceptual framework that guided this study. A model is a conceptual system used to represent and solve a problem, in the MEA case, it is a real-word problem [4]. These structures can be expressed using "representational media such as writing symbols, spoken language, computer-based graphics, paper-based diagrams or graphs, or experience-based metaphors" [5, p. 158].

Modeling is an active process of creation, manipulation, and adaptation of conceptual models in a problem-solving scenario [4]. A logical relationship can be revealed by analyzing a model's elements, relations, and operations [6]. Model development depends on representational fluency and the ability to convert between diverse representational forms [7]. Model and modeling processes are used to foster integrations and problem-solving skills [8].

Implications of the Conceptual Framework for the Learning Design

Guided by our conceptual framework, we used MEAs to deliver our learning design in the form of cybersecurity challenges. As stated previously, the MEAs are activities that intend to simulate real-word client-driven scenarios in a team-based collaborative environment [4]. In addition, MEAs are essentially open-ended problems that are presented in an authentic context [8]. Students' problem solving skills and understanding of course concepts can be improved with the implementation of MEAs [9]. Furthermore, MEAs can provide cognitive and metacognitive engagement in the problem context, creating an effective learning experience [7]. MEAs have become important tools for teachers and helped them to be more perceptive and sensitive when designing active learning modules to engage students in a meaningful thinking process [4].

The roles of MEAs in the students' learning processes are as follows:

- Integrator: Integrate knowledge acquired in previous courses with new information [3].
- Reinforcer: Strengthen concepts that have currently been learned [3].
- Discoverer: Uncover concepts that have not formally been introduced yet [3].

The problem-solving setting of MEAs is critical to "express, test and revise models" [4, p. 13]. MEAs are built with the goal of revealing the learner's models and conceptual structures used to solve the problem [4]. Student's solution process of MEAs requires constant shifting among several model representations [7]. The solution demands the use of one or multiple engineering concepts, which are not specified in the problem statement [6].

The MEA framework provides a way to deliver open-ended engineering problems, which contain high-level engineering content, but also address several ABET principles [10]. MEA design requires the application of the following principles: (1) reality principle, (2) model construction, (3) model documentation, (4) self evaluation, (5) model generalization, and (6) prototype [4]. The MEA problem statement is constructed to introduce students to the problem. It has to be written in a way that leads students to define the problem by themselves. The students must then generate a plan of action that has to be followed to meet the client's requirements. The problem-solving process obliges the team to go through numerous iterations, and test and review solutions in order to come up with a model that will address the client needs [10]. Similarly, teamwork is essential in MEAs due to the time available to come up with a viable solution to the problem. Additionally, by requiring multiple point-of-views and perspectives, students can arrive to better solutions in less time [10].

A Cybersecurity Themed Model-Eliciting Activity

This paper presents an MEA called *Migration to HTTPS*. As illustrated in Figure 1, the focus of this problem-based activity is to promote students' learning in the core concepts related to Hyper-Text Transfer Protocol Secure, or HTTP over SSL. The learning objectives for this particular activity are: (a) review firewall, network design and web server configuration processes; (b) identify differences between HTTPS and HTTP; (c) migrate a website from HTTP to HTTPS; (d) acquire, activate and install certificates; (e) identify potential vulnerabilities related to data security; (f) define best practices related to HTTPS implementation; and (g) delineate optimal encryption method. Figure 1 presents the MEA.

Once the learning objectives were identified, the next step in the process was to apply the MEA principles to design the activity. Listed below is how those six principles were implemented in the proposed cybersecurity challenge:

Reality principle. The process of migration from an HTTP-based to an HTTPS-based website is a highly requested procedure. This realistic component enhances the chance of getting students motivated and interested.

Model construction. This activity enables the construction of models of HTTPS concepts. It is expected that students construct the models based on the theoretical framework previously acquired. Models that students will create, modify or redefine include the following:

- Secure Sockets Layer Architecture
- Transport Layer Security
- HTTPS connection

Model documentation. This task has a client-driven component that requires the presentation of different solutions for the problem. Additionally, a final report must be delivered in which the selected solution will be showcased.

Self-evaluation. The problem statement enables students to evaluate usefulness, alternatives, and best practices.

Model generalization. The migration process to HTTPS is a model that could be re-usable by the students.

Prototype. The procedures of migration to an HTTPS-based web server service is not procedurally complex. This allows the students to build a learning prototype to better understand how PKI architecture can be leveraged and applied in real world to provide data confidentiality and integrity.

Migration to HTTPS Challenge

LOVABLE is a middle size vendor of pet supplies. The company contacts your team in order to start the migration process of their HTTP website (lovable.com) to HTTPS.
HTTPS is the layering of HTTP over SSL/TLS. It is meant to create a secure communication between the Web browser and Web server.

Task

LOVABLE is conscious of the importance of protecting buyers' financial transactions and personal data. The company requires you to write a detailed report that:

1. Determine types of certificates needed and how to implement them.
2. Define optimal integration legacy systems.
3. Outline viable and optimal encryption methods.
4. Delimit process of redirect users and research engines.
5. Identify common issues and vulnerabilities of the https protocol and how to troubleshoot them.
6. Identify specific pages that require HTTPS implementation.
7. Estimate cost of the HTTPS implementation.

Assumptions

The company website poses a DNS/DB secure.

Figure 1. Migration process for an HTTPS website MEA

Methods

The activity was piloted out in a five-hour cybersecurity workshop with a group of 18 Telecommunication and Networking Peruvian undergraduate students from a three-year program. Prior to handing out the HTTPS migration MEA activity, the instructors spent four hours going over the important concepts, such as symmetric encryptions, asymmetric encryptions, PKI, and Transport Layer Security (TLS). Due to time constraints, no pre-tests were given to compare the effects of MEAs. Students worked in nine groups of two and was given one hour to collectively finish the assignment.

Once students completed the activity, each of the worksheets were collected to then be quantitatively analyzed using a thematic analysis. Students' responses to the worksheet were classified as correct, partially correct and incorrect (Table 1). Once each of the worksheets were scored individually, responses were then compared and contrasted.

Table 1. Responses Assessment rubric

	Criteria
Correct	The answer does not present conceptual inaccuracies.
Incorrect	The answer presents important conceptual inaccuracies.
Partial	The answer presents minimal conceptual inaccuracies.

Answers were also used to determine how participants interpreted the questions (Table 2). The analysis results were used to restructure the questions to match the designers' desired outcomes.

Table 2. Question Assessment Rubric

	Score		
Criteria	1	2	3
Accuracy	The answers to the question were not what the researchers expected.	The answers to the question somewhat what the researchers expected.	The answers to the question were exactly what the researchers expected.
Detail	The question prompt students to provide little detail in the answers.	The question prompt students to provide modest detailed answers.	The question prompt students to provide detailed answers.

Results

Nine (9) worksheets were collected; these responses were classified using the responses assent rubric (Table 1). The results were summarized on Table 3. Most of the participants (66.7%) correctly answered the first question to include personal certificates, certificates issued by Certificates Authorities (CAs), and references to Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocols. A 22.2% of the responses to question 3 were incorrect and an equal amount was cataloged as partial. The partial answers mentioned RC4 encryption methods however the correct answers should include asymmetric encryptions, such as Rivest-Shamir-Adleman cryptosystem (RSA) and Elliptic Curve cryptography (ECC), and symmetric encryptions, such as AES. Incorrect answers included Message-Digest five (MD5), which is not an encryption method or rather than a secure hashing algorithm.

Table 3. Responses classification

	Correct	Incorrect	Partial	No answer
1.Determine types of certificates needed and how to implement them.	6	1	0	2
2.Define optimal integration legacy systems.	0	0	1	8
3.Outline viable and optimal encryption methods.	0	2	2	5
4.Delimit process of redirect users and research engines.	0	0	0	9
5.Identify common issues and vulnerabilities of the https protocol and how to troubleshoot them.	1	0	0	8
6.Identify specific pages that require HTTPS implementation.	0	1	0	8
7.Estimate cost of the HTTPS implementation.	1	0	0	8

Two (2) responses included figures in their answers (Figure 2 and 3) that is equivalent to 22.2% of the total responses. Figure 2 aims to exemplify the migration process, however, it presets misconnections concerning SSL/TLS which are security protocols not encryption methods. Additionally the migration model lacks in details and presents the communication security as one-way flow.

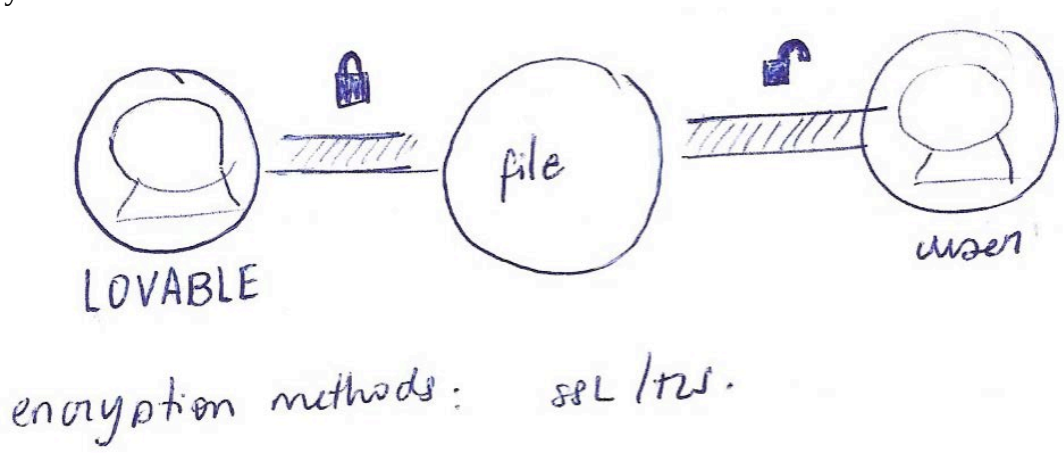

Figure 2. Answer to question 1.

Figure 3 presents an interesting response to the worksheet questions. This representation of the process reflects some misconceptions the students have on how authentication was conducted: validating the server certificates with the CA is only a part of the authentication process and users and clients need to be authenticated as well between the client and the web server. The students however illustrated more details (and mostly correct) compared to Figure 2, such as the connection of SSL is between the client and the server.

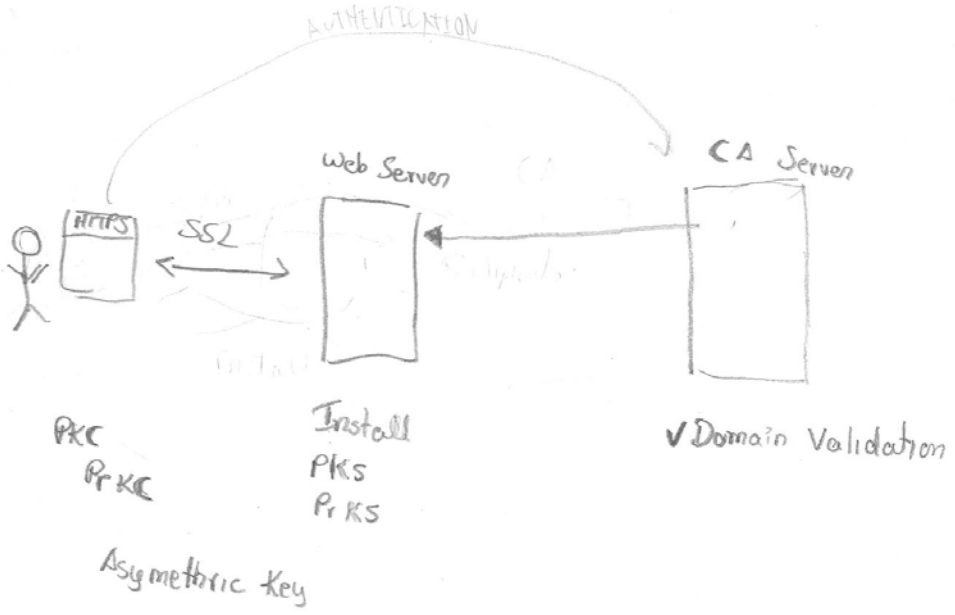

Figure 3. Answer to worksheet questions.

Using diagrams (Figures 2 and Figure 3) to answer the question has great values. It makes the instructors to easily identify the gaps between the learning objectives and students understanding. It also enable students to promptly and accurately revise their conceptual model when feedback is given. This suggests that multiple representations may need to be enforced in some of the tasks, if not all the tasks.

Additionally the researchers assess each question, based on the responses, to ensure proper understanding of the task (Table 4). None of the participants provide an answerer to question 4, a deficit in students' learning to apply their conceptual models and prior knowledge to the relatively new topics.

Table 4. Questions' assessment based on the answers obtained.

	Questions Score						
Criteria	1	2	3	4	5	6	7
Accuracy	2	2	2	-	1	1	1
Detail	1	1	1	-	1	1	1

- Question 4 did not received any answers

Discussion and Implications for Teaching and Learning

The results suggest that the participants possessed several misconceptions and conceptual gaps on basic knowledge of how to secure a communication between the server and the web browser. This fact was unexpected given that the students were coursing the last year of a Telecommunication and Networking career. The results imply a necessity to strengthen general

security and web security concepts on cybersecurity education as suggested by McGettrick [11] in his work "Toward Effective Cybersecurity Education".

Third-party validation is a key concept on the process of securing communications through a public-key scheme and it was mentioned in the text-based and graphical answers obtained. This suggest that participant's mental model of HTTPS is based on it. However, there is a misconception of the communication process between parties as represented by the participants in this study.

In this pilot study the researchers were able to identify common cybersecurity conceptual shortcomings among participants. The participants repeatedly confused encryption algorithms with hashing algorithms and protocols with authentication methods. These misconceptions should be acknowledged when building a proper cybersecurity curriculum. Dark (2014) [12] stated that identifying students' misconceptions will be useful for teachers since they could select, adapt or create new instruction methodologies that could better assess student's needs. The results were also used to improve the design of the MEA activity "Migration to HTTPS Challenge". Questions 1, 2 4 and 6 were changed in order to fulfill the MEA learning objectives (Figure 4).

Migration to HTTPS Challenge

LOVABLE is a middle size vendor of pet supplies. The company contacts your team in order to start the migration process of their HTTP website (lovable.com) to HTTPS.
HTTPS is the layering of HTTP over SSL/TLS. It is meant to create a secure communication between the Web browser and Web server.

Task

LOVABLE is conscious of the importance of protecting buyers' financial transactions and personal data. The company requires you to write a detailed report that:

1. Determine how to secure the communication between the server and the web browser and clearly detail how to implement your solution.
2. Define optimal integration with legacy systems.
3. Outline viable and optimal encryption methods.
4. Delimit process of redirect users from HTTP to HTTPS
5. Identify common issues and vulnerabilities of the https protocol and how to troubleshoot them.
6. Identify what sections of the LOVABLE's website need to use HTTPS.
7. Estimate cost of the HTTPS implementation.

Assumptions

The company website poses a DNS/DB secure.

Figure 4. Revised MEA activity of the mitigation process to HTTPS

The primary limitation in this study was the amount of time available to conduct it. MEAs are usually carried out with greater timeframe such as one or two weeks. However, the results from this five-hour workshop helped designers to recognize important concepts and common mistakes related to the topic. Another factor could have negatively impacted the results of this study. The participants' native language is Spanish but the lecture and MEAs were all given in English. This could have contributed to the lack of details in the responses.

Conclusion and Future Work

MEAs encapsulate problem-based learning, inquiry learning, group work, and modeling in a single activity. MEA 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.

Identifying common misconceptions among cybersecurity and cybersecurity majors will help teachers to improve the effectiveness of the instructions and more efficiently allocate time and resources. Future work will include the implementation of this MEA activity in an undergrad or a graduate level course. Additionally, the researchers will keep identifying important concept misconceptions in cybersecurity.

Acknowledgement

This research was supported in part by the U.S. National Science Foundation under the award DGE #1500046

References

1. ROWE, D.; LUNT, B.; EKSTROM, J. The role of cyber-security in Information Technology education, p. 113-122, October 2011.
2. EVANS, K.; REEDER, F. **A Human Capital Crisis in Cybersecurity:** Technical Proficiency Matters. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. [S.l.]: Center for Strategic and International Studies, 2010. ISBN ISBN: 978-0-89206-609-4. Disponivel em: <http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity>.
3. YILDIRIM, T. P.; SHUMAN, L.; BESTERFIELD-SACRE, M. Model-Eliciting Activities: Assessing engineering student problem solving and skill integration processes. **International Journal of Engineering Education**, v. 26, n. 4, p. 831-845, 2010.
4. HAMILTON, E. et al. Model-Eliciting Activities (MEAs) as a bridge between engineering education research and mathematics education research. **Advances in Engineering Education**, v. 1, n. 2, p. 1-25, 2008.
5. LESH, R.; HAREL, G. Problem Solving, Modeling, and Local Conceptual Development. **Mathematical Thinking & Learning**, v. 5, n. 2/3, p. 157-189, 2003.
6. MOORE, T. Model-Eliciting Activities: A case-based approach for getting students interested in material science and engineering. **Journal of Materials Education**, v. 30, n. 5-6, p. 295-310, 2008.
7. MOORE, T. et al. Modeling in engineering: The role of representational fluency in students'conceptual understanding. **Journal of Engineering Education**, p. 141-178, January 2013.
8. CLARK, R.; SHUMAN, L.; BESTERFIELD-SACRE, M. In-depth use of modeling in engineering coursework to enhance problem solving, 2013.
9. BURSIC, K.; SHUMAN, L.; BESTERFIELD-SACRE, M. Improving student attainment of ABET outcomes using Model-Eliciting Activities (MEAs). **Proceedings of the American Society for Engineering Education Annual conference and Exposition**, 2011.
10. MOORE, T.; DIEFES-DUX, H. Developing Model-Eliciting Activities for undergraduate students based on advanced engineering content. **34th ASEE/IEEE Frontiers in Education Conference**, p. F1A 9 - 14, October 2004.
11. MCGETTRICK, A. Toward Effective Cybersecurity Education. **IEEE Security&Privacy**, n. 6, p. 66-68, 2013.
12. DARK, M. Advancing Cybersecurity Education. **Security & Privacy IEEE**, v. 12, n. 6, p. 79-83, 2014.