PUZZLE BASED CYBER SECURITY LEARNING TO ENHANCE DEFENSIVE SKILLS OF FRONT-LINE TECHNICIANS

Collaborative Project:

Jackson State Community college and

The University of Memphis

NSF- ATE Award Numbers 1406992/ 1406853

Annual Evaluation Report 2017

Prepared by John Sands

Project Evaluator

Jackson State Community College

THE UNIVERSITY OF MEMPHIS Center for Information Assurance

Projection Context

Cyber-enabled devices are becoming more and more complex with integration of new capabilities and functionalities, both in software and hardware, making it very difficult for users to realize that they are under cyber-attacks or the cause of data breach, etc. It is also well-known fact that vulnerabilities at one component can affect other components in any computing device. But it is hard to realize the interdependencies of various components in order to secure the entire path to in and out of a cyber system. Puzzle-based Learning (PBL) approach proved to have improved STEM learning environment including mathematics, physics and computer science, however, there has been very little work done in computer and cyber security education. We propose to introduce PBL to basic cyber security education to help students better understand complex attack paths and countermeasures for fraud detection, cybercrime, and advanced persistent threats (APTs).

Principal Investigators

Principal Investigators - Professor Thomas L. Pigg Dean of Allied Health and CIS/Professor of CIS Jackson State Community College (JSCC) Email: tpigg@jscc.edu Prof.

Co-Principal Investigators - Dipankar Dasgupta Director, Center for Information Assurance the University of Memphis in Memphis, TN 38152-3240 Email: dasgupta@memphis.edu

Project Description

The project team will design and develop interactive, multi-level puzzles both for students who have limited knowledge of computers, networks, and cybersecurity and for students who have a moderate to high level of expertise. The complexity of the developed puzzles will be varied based on the target audience. Puzzle-based learning addresses two issues:

(1) It places emphasis on developing critical thinking skills instead of simply covering content.

(2) It promotes and builds mathematical and logical reasoning skills.

Many institutions have already used puzzles in their STEM curricula successfully. Puzzles have been introduced in introductory computer science courses. However, no significant work has been done on introducing puzzles into cybersecurity curricula. The project team will design scenario-based security puzzles that explore a range of topics (such as identifying and neutralizing malicious software, deploying a secure wireless network, and detecting e-mail spam) using logical decision trees, truth tables, and directed graphs.

At the end of each exercise, participants will be able trace back their decisions and analyze how an incorrect decision stem can lead to the exploitation of a vulnerability and how correct actions can prevent it. The investigators will phase in the use of these puzzles so as to:

i) examine how to effectively integrate such puzzle-based learning technology with instructional content of community college courses to improve the skill sets of front line cyber defenders

ii) ii) better identify and understand the circumstances under which success occurs. The project team will also conduct a small-scale efficacy study by having students participate in cyber "capture-the-flag" competitions to determine if the new enhanced courseware enables increased learning compared to the existing instructional methodology.

Project Goals

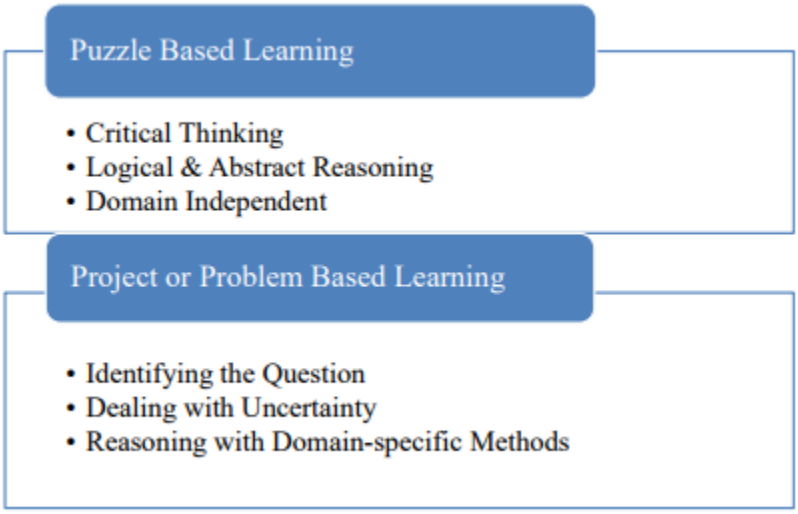
The goal of this project is to improve the effectiveness of cyber security education through puzzle-based learning (PBL), expanding student knowledge and problem solving skills through the stimulation of their cognitive abilities. PBL has already proven effective in many STEM learning environments including mathematics, physics, and computer science as an interesting and effective way of learning complex logic and abstract concepts. Cyber security has increasingly become important due to the escalating sophistication and frequency of online attacks, as well as the consequences of these attacks for various organizations and their infrastructures. This PBL project utilizes various approaches (simulations, interactive graphics, games, etc.) to improve defensive skills that will not only teach students how to protect specific systems, but also how to protect entire classes of systems that provide similar services, but with differing hardware/software components and architectures.

Targeted Audience

Community College educators and students pursuing careers in computer networking and security fields.

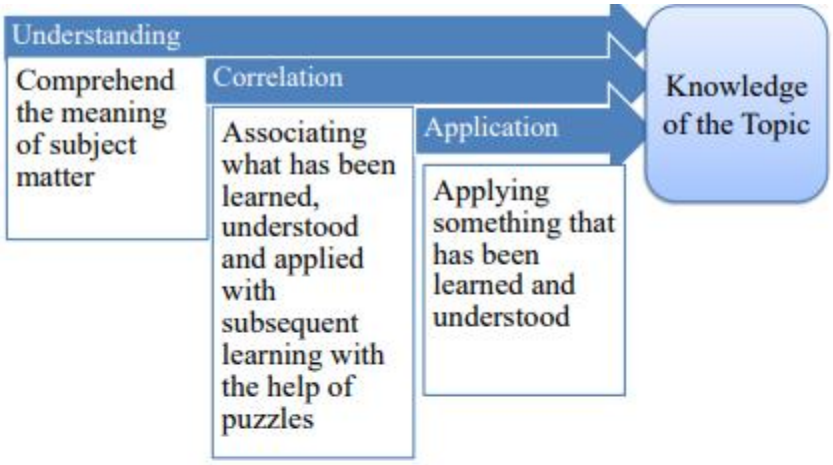
Summary of Products Produced

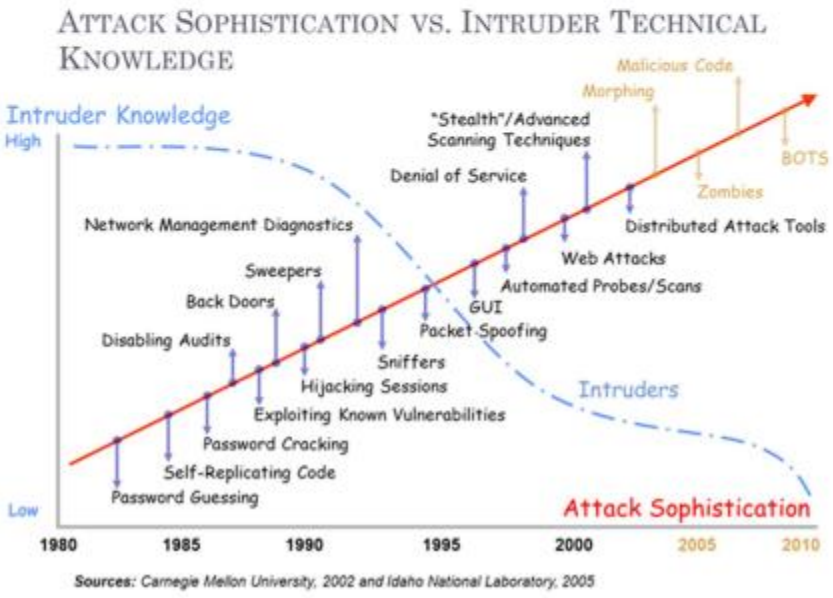
This research project – developed with "Unreal Engine" (UE4) – introduces novice users to abstract security concepts, enabling critical thinking through the solving of complex puzzles. Therefore, this research project will play a significant role in improving the critical thinking skills for next generation cyber security professionals.

Why Puzzles


Puzzle Based Learning	
Steps	Learning
• Introduction to the topics through lectures • Interactive Story with problems • Story can be led different directions in accordance to feedback to the problems	• Participants interact with the story and also the problem • Participants use logical reasoning and knowledge obtained from classes • Participants become aware of the consequences of their responses as the responses leads the story ahead

Learning Process





Implementation

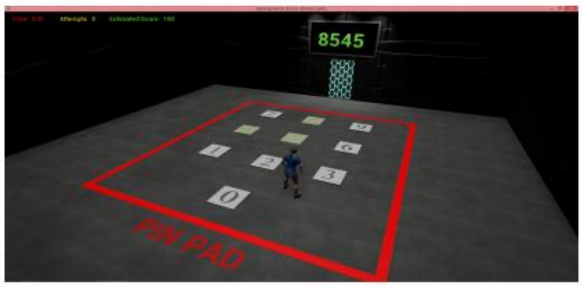
Unreal Engine

- Participants solve puzzles in a 3D gaming environment.
- Allows the participants to interactively engage with the puzzle.
- Score successful completion of different levels of the 3D game.

Sample Produces

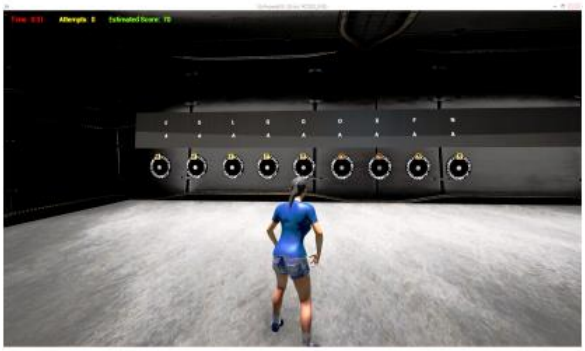
PIN-PAD Puzzle

- The user figures out the PIN using discrete mathematics in order to advance to the next level.
- There are a number of different permutations depending on the total number of smudges.
- The user brute forces the correct PIN by entering the different permutations from the previous step.



Encryption and Decryption Puzzle (Ceaser Cipher)

- Encryption and decryption of random strings with given hints.
- The user rotates each wheel to the correct character (clockwise or counter clockwise).
- Upon selecting all the correct characters the user submits their solution by pressing enter, green lights (win) and red lights (try harder).



Result Score

- User score displayed after completing each level.
- Scores are calculated by number of tries and total time spent on each level.
- The scores will be saved in an encrypted file for the course administrator to grade the participants.
- The scoring mechanism can be updated according to instructor's choice.

Potential Applications
• Simulation of Multi-factor authentication. Starting with passwords, security questions, biometrics and then integrate different combinations of them. • Simulation of Phishing attacks, how it's done and how to discern Phishing attempts from legitimate communication. • Puzzle based game to introduce different system vulnerabilities, attack vectors, and ways to mitigate possible exploitation of vulnerabilities.

Focus of Evaluation

The focus of this report is to determine the overall effectiveness quality and impact of the learning base puzzles produced by the partnership between Jackson State Community College and University of Memphis. The report combined several different methods of data collection and assessment. The data collection methods used in this project evaluation included online surveys, interviews and the measurement of puzzle utilization and adoption. The results of this report will be used to identify the quality of the current products, measure the effectiveness of the development and dissemination processes and attempt to measure the impact of the overall project. The following is a summary of the data collection and analysis.

Evaluation Instruments

Over the last two years the project principal investigator (PI) and external evaluator and collaborated to develop several evaluation and data collection instruments. These instruments were published and disseminated through an online survey system (survey monkey). The type of question used were designed to collect demographic information, identify the targeted education level and measure the impact and quality of the puzzles. The following are examples of the question used:

Which of the following best describes your institution?
How many years have you taught?
Which of the following best describe your students?
How many students are enrolled in your typical class?
Puzzle-based learning is an instructional method I am interested in adopting in my IT and Cyber Security courses.
How well do our puzzles meet the needs of your curriculum?
How well do the puzzles you reviewed align to your curriculum?
How responsive are the puzzles performance on your computer or device?

How accurate are the puzzles you experienced?
How likely are you to use any of our puzzles in your class on a regular basis?
How would you rate the overall quality of the beta puzzles you used?
How likely is it that you would recommend our cybersecurity puzzles to a friend or colleague?
Overall, how satisfied are you with the cybersecurity puzzles?
Which of the following words would you use to describe the cybersecurity puzzles at this point? Select all that apply.
Do you have any other comments, questions, or concerns related to the cybersecurity puzzles you reviewed?
What institution are you from?

The instruments also provided for open ended comments, suggestions and complaints. The puzzles and survey were used at targeted workshops and conferences including the Midwest Cisco Academy Conference, and the Community College Cyber Summit (3CS). Several participants were also interviewed after taking the survey in order to delve deeper into survey findings.

Data Collection

Nine college and a handful of high schools were selected to pilot the initial product. As the produce became more refined other schools were encouraged to pilot the puzzles. The puzzles were demonstrated and disseminated to numerous faculty over the last two years. In total 72 faculty participated in the evaluation of the puzzles. Several of the faculty were interviewed. Students were also encourage to complete an evaluation survey of the PBLs. The PI and External evaluator developed and disseminated the following data collection instruments:

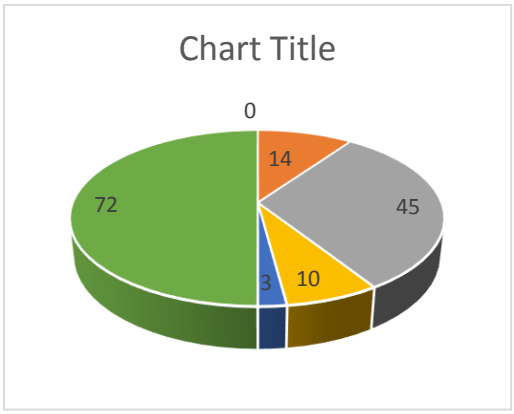
Instrument Description	Date Created	Responses
Teacher Survey - Puzzle Based Cyber Security Learning Project	10/12/2016 11/17/2017	12 17
Student Survey - Puzzle-Based Learning for Cyber Security	10/12/2016	82
Teacher Interviews - Puzzle-Based Learning for Cyber Security	02/17/2017	5
Students Interviews - Puzzle-Based Learning for Cyber Security	04/21/2017	4
Puzzle-Based Cybersecurity Learning Product Review	05/09/2016	21
Puzzle-Based Cybersecurity Learning to Enhance Defensive Skills of Front-Line Technicians	05/09/2016	23

Results

The results revealed that the majority of participants were community college teachers, some high school and 4-year colleges.

ANSWER CHOICES–	RESPONSES	Percentage
6th - 8th Grade (Middle School)	0	0.00%

9th-12th Grade (High School)	14	19.44%
Community College / Technical College / Two-year College	47	62.50%
Four Year College	9	13.89%
University	2	4.17%
Total	72	100.00%



The results of the data collection and analysis also reveal several trends, successes and challenges. Every participant expressed an interest in adopting (60%) or consider adopting (40%) the puzzles as part of their cyber security programs. The data also exposes several opportunities in the future utilization of learning-based puzzles. A large percentage of the instructors did NOT feel the puzzles directly aligned to the content they teach. The development team understands that future puzzles development will need to spend more attention to content alignment rather than student engagement and design characteristics.

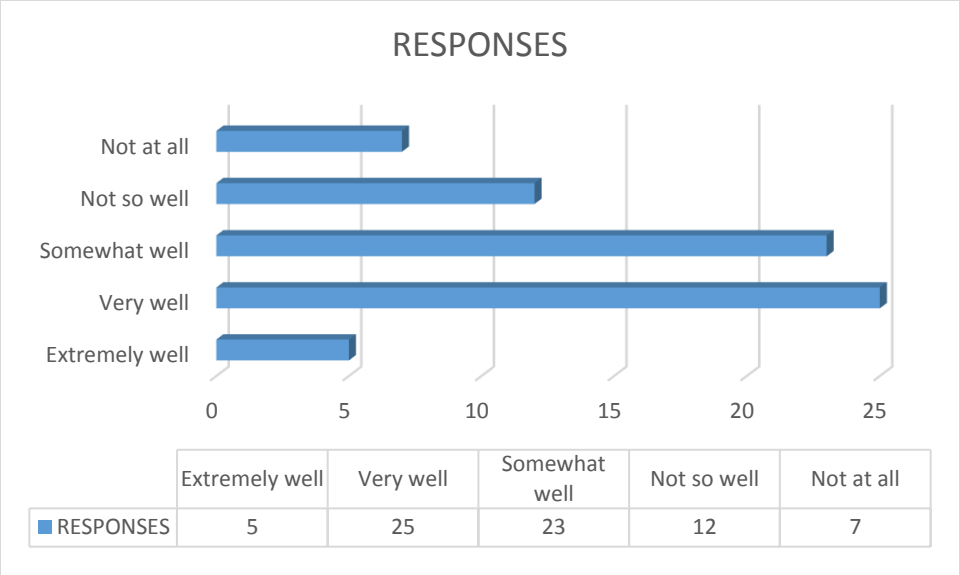
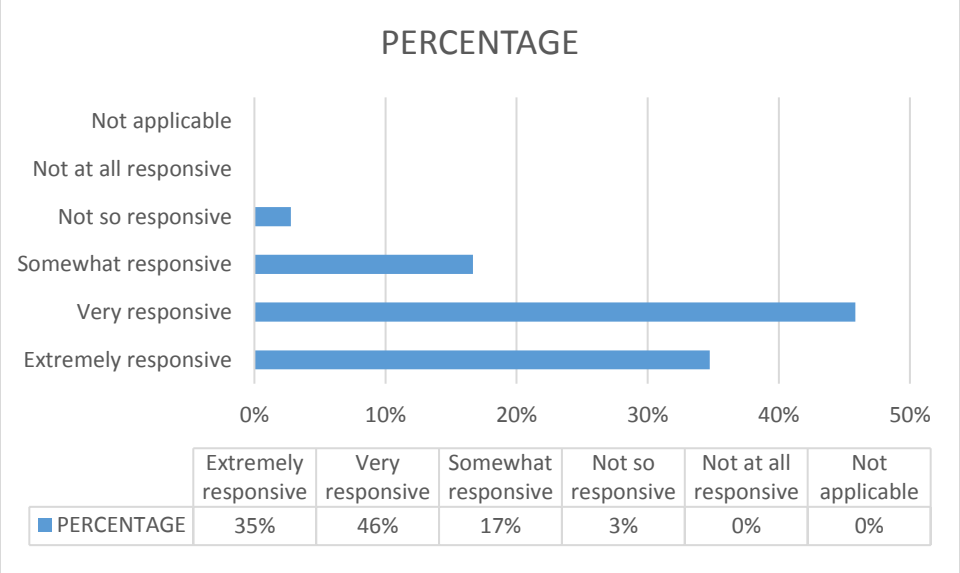


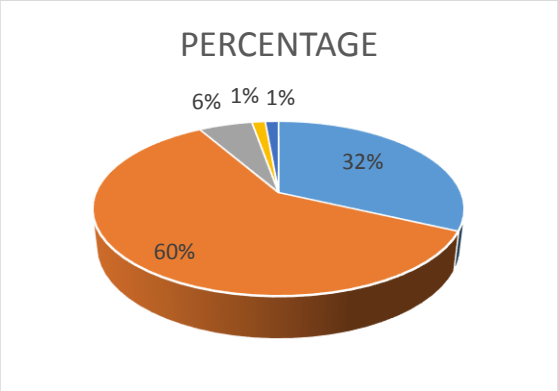
Figure 1 - How well do the puzzles you reviewed align to your curriculum?

Respondents were much more satisfied with the accuracy and responsiveness. These result have improved significantly over the last year and two revised versions of the puzzles.



ANSWER CHOICES	RESPONSES	PERCENTAGE
Extremely accurate	23	32%
Very accurate	43	60%
Somewhat accurate	4	6%
Not very accurate	1	1%
Inaccurate	1	1%
Total	72	100%

Findings



Teacher interviews reveal that cyber-security educators are very enthusiastic regarding the use of puzzle-based learning if the puzzles directly support the lessons they are teaching. Several teachers express a need to use the learning-based puzzles as a way to allow students to practice difficult skills or master difficult concepts. The majority of teachers expressed a need for puzzle like tools that allow students to work on skill building as part of in and out of class assignments.

The majority of teachers rated the puzzles as accurate and relatively simple to operate. The most common request was to have teachers more engaged in the selection of future puzzles. Most teachers would like to see puzzles able to randomly recreate the designed problems so students are required to solve a related but different variation problem each attempt. Good examples of new topics would include subnetting, access control list, hashing, risk calculations and identification common vulnerabilities with recommended countermeasures. Several teachers pointed out that PBL products would be especially useful and needed in delivering online classes. The participants were unanimous in voicing a need for continued research and development of additional cyber-security focused learning-based puzzles.

Student Interviews

The overall finding is that student enjoy puzzle-based learning as a method of instruction and developing new skills. Most student felt PBL could be more challenging and include multiple levels of difficulty. Student also commented that the puzzles be more game oriented. This format would require student to progress through levels.

Conclusion and Future Work

The development team has made great progress in develop more accurate and responsive products. It is obvious that future focus should be working closer with target faculty and students in aligning the product to curriculum elements and adding the ability to progress through additional levels and include the ability to generate more problems.

- Provokes the thinking process by providing challenges.
- Interactive process to engage participants in the story or the problem.
- Participants will able to see the future consequences of their actions, makes the learning process interesting.

- More enlarged versions with other development platforms are being developed as part of NSF grant.
- User study with two different controlled groups (one with traditional learning, other with Puzzle based learning) are going to be conducted in this semester