Abstract
Cyber security has increasingly become important due to the escalating frequency and sophistication of on-line attacks, as well as the consequences of these attacks for various organizations and their infrastructures. This is an emerging field which requires real life experience to solve on going security challenges. Demand for cyber security professionals is ever increasing, and by 2019 the demand is reported to increase to 6 million, with a projected shortfall of 1.5 million. 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. 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?

- Critical Thinking
- Logical & Abstract Reasoning
- Domain Independent

Project or Problem Based Learning

- Identifying the Question
- Dealing with Uncertainty
- Reasoning with Domain-specific Methods

Learning Process

- Understanding
  - Comprehend the meaning of subject matter
- Correlation
  - Associating what has been learned, understood and applied with subsequent learning with the help of puzzles
- Application
  - Applying something that has been learned and understood

Unreal Engine

PIV-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).

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 increase awareness.
- 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.

Conclusion & Future Works

- 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.

Acknowledgements

This research project is funded by National Science Foundation, NSF- ATE Award Numbers 1406992/ 1406853.