Object Oriented Programming Game Module

Module Learning Outcomes:

Primary:

- #1: Demonstrate substantial understanding of the Cybersecurity First Principles.
- #2: Understand the basics of computer programming and experiment with simple programs.

Secondary:

- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.
- #13: Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module Addresses the following Cybersecurity First Principles:

- Encapsulation
- Abstraction
- Information Hiding
- Modularization
- Least Privilege
- Domain Separation
- Process Isolation

Description:

This module will exploit student's interest in computer games while laying a rudimentary understanding of Object Oriented Programing. Students will experiment with several games implemented in the Java programming language and make small modifications in logic and the instantiation of objects within each game. Emphasis will be placed on principles of abstraction, encapsulation, modularization, information hiding as applied to object oriented programming. In addition to the basics of object oriented programming, the danger of installing games from unknown sources will be made evident in a demonstration of covert interrogation of a computer and stealing of digital content. Through this demonstration students will recognize the importance of least privilege, domain separation, and process isolation.

Upon completion of the module students will:

- ❖ Gain further understanding of programming basics including variables, assignments, operators, loops, conditionals, and functions.
- ❖ Gain a cursory understanding of object oriented principles including class, encapsulation, inheritance, polymorphism, instance variables, methods and instantiation.

- Gain understanding of the risks of installing games and improve judgement on what and what not to install.

- Gain understanding of techniques to minimize risk in executing games.

Hands-On Classroom:

In this module students have hands on access to several games written in the Java programming language through the use of the Eclipse development environment. Following a short presentation on object oriented programming in relation to game design, instructor will lead examination and execution of several games. Students will modify constructor parameters of objects within each game and observe the results. Other instructor led modifications include instantiation of further objects within games and small changes to logic involving loops and conditionals. To minimize errors, most changes will be performed by uncommenting pre-supplied lines of code within each game. Students may perform their own experimental changes. While leading the students through the modifications, cybersecurity first concepts of abstraction, modularization, information hiding and encapsulation will be referenced and discussed.

Included in the module is a demonstration of covert interrogation and stealing of digital media. The demonstration involve having students create a few files on their computer's desktop folder prior to the presentation on object oriented games. One of the games when executed will in the background steal the files the student created and send them to a server. This action will only be revealed at the end of the object oriented programming presentation. While this demonstration is benign, the point will be made that games could behind the scenes perform malicious activities that could have drastic consequences. Students will then be asked for steps they could take to minimize the risk. In the course of this discussion cybersecurity first principles of least privilege, domain separation, and process isolation will be injected into the discussion.

Assessment:

This module will be assessed by the pre/post test for the camp. In addition reaction to the covert interrogation and digital stealing demonstration will be noted in the instructor's post camp report which will include a list of actions suggested by the students to reduce the risk in executing games.

Suitability to various groups:

The principles introduced in this module are applicable for both the middle school and high school as the modifications to the programs will primarily be accomplished through uncommenting lines, copy/paste, and change of very limited text. It is anticipated that high school students may proceed at a quicker pace. In the event the primary content is complete, secondary examples may be used. Both groups will experience the covert interrogation and digital stealing.

How the Teachers and Students groups will be interacting:

This module is targeted for the student groups. Teachers may be invited to observe the presentation. The content will be available to teachers following the camp to use in their own demonstrations.