Introduction to Database Systems and Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #1: Demonstrate substantial understanding of the cybersecurity first principles.
- #2: Explore the use of basic operation systems commands on different platforms.
- #3: Explain different types of attacks on computing systems.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #7: Realize the importance of secure coding and apply effective techniques to improve security.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #1: Domain Separation
- #2: Process Isolation
- #3: Resource Encapsulation
- #4: Least Privilege
- #5: Layering
- #6: Abstraction
- #7: Information Hiding
- #8: Modularity

Description:

This module presents an easy-to-understand introduction to fundamentals of database systems and database security. Includes topics of information models, database schemas, basic CRUD operations, and SQL. Various database architectures from desktop only to multi-tier will be presented. Both graphical user interface and command line will be used to define, populate, query, and maintain a database. Security measures to define users and grant/revoke privileges on database objects will be covered along with roles of various users of database systems. SQL injection will be demonstrated together with a discussion of proper countermeasures. Includes a cursory discussion on stored procedures.

Learner-centered classroom:

This module is designed to be taught in an interactive environment in which all attendees will be active participants in the learning process. This module will first have the students implement a cash register system using MS-Access. After creating the system and populating the system with data, students will experiment with generating queries. All interactions with the system will use the graphical user interface of access. Subsequently, attendees will be introduced to Oracle using the command line interface. Pre-built SQL scripts will be used to build and populate a small database. Students will experiment with generating queries. The module will conclude with a hand-on demonstration of a web based database system which is vulnerable to SQL injection. Throughout the module security first principles will be emphasized.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. At the beginning of the module, attendees will asked as group to enumerate as cyber security first principles in general. At the end of the module attendees will be asked to again enumerate the cyber security principles, only this time emphasizing the relation to database systems. Both times this will be performed orally as a group. Experiments with database queries a means to explore use of basic operation systems commands on different platforms, and applying knowledge gained in solving real-world, scenario-based problems. Experiments with the vulnerable database system will realize the importance of secure coding and need for effective programming techniques to improve security A few pre/post camp questions will provide a degree of formal assessment.

Suitability to various groups:

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the database systems can be integrated into the K-12 curriculum with emphasis on securing information stored in databases. The contents will also advance in the level of detail when being presented to the high school group compared to content being presented to the middle school students.

How the Teachers and Students groups will be interacting:

This module will not have explicit interaction amongst the three groups. Contents covered in the teachers group will primarily focus of how to integrating these security concepts in the K-12 curriculum, while those to students will focus on kindling their interest in the area of cybersecurity. Also, input from the teachers will be sought on how to better deliver the module contents to the other two students groups.