Introduction to Robotic AI Security Module

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

Camp Learning Outcomes

1. Demonstrate substantial understanding of the cybersecurity First Principles.

Numbers four, five, six and seven

2. Explore the use of basic operating systems commands on different platforms.

All robot OS can be compromised to alter what they were originally intended for

3. Explain different types of attacks on computing systems.

Robots can be attacked both physically and through cyber

4. Experiment with basic tools and techniques used to attack and/or defend systems.

Firewalls on robots defend them from vulnerabilities

5. Realize the importance of password and username management and apply effective approaches to increase their security.

iPhone and Android both control robots so their passwords can b compromised

6. Understand the basics of computer programming and experiment with simple programs.

Computer programming runs robots

7. Realize the importance of secure coding and apply effective techniques to improve security.

If trap doors or backdoors left in code than can be used maliciously

8. Engage in scenario-based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place.

Use black tape versus white tape on Cublets robots to show wrong and right code

9. Uncover their own digital footprint and learn how to give themselves an “online make-over.”

See what other robots are available and what else these robots can do

10. Exemplify the ability to identify the authenticity and credibility of access requests.

Ask robots to play games

11. Develop skills needed to defeat various mal- and social engineering attacks.

Try to run robot without my phone. Will it work on theirs if download the app?

12. Apply the knowledge gained in solving real-world, scenario-based problems.

Interactive physical security with robots (diffuse a bomb)

13. Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

Robots are not charged or app is not available

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

- #4: Domain Separation area of control of robots
- #5: Layering of computer security in both the robot and the control mechanism
- #7: Modularity or separation of the functionality of the robot into modules
- #6: Abstraction of the toy robot into a full scale physical security model

Description:

This module presents an easy-to-understand introduction to fundamentals of robotics, AI and security. The participants will be introduced to Cozmo, Cublets and the DJI drone. The robots will provide input, process and output examples of cybersecurity such as disarming a potential bomb, distinguishing between right and wrong security paths and aerial surveillance. Cybersecurity threats to both the control mechanisms and the actual robots will be explained, explored and demonstrated. Pattern recognition will be utilized to find a potential terrorist among a mountain of surveillance data.

Learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include basics of AI, robotics and security applications. Participants will be encouraged to take the learning with them and apply the principles to their home networks and daily life. They will be encouraged to troubleshoot and secure their robotics for optimal performance.

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. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

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 AI security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as robotic co-existence with the human world. The contents will also advance in the level of detail when being presented to the Middle school group compared to when being presented to the High school students.