South-Eastern Finland
University of Applied Sciences

INTRODUCTION TO CYBER SECURITY

Extent 3 ECTS Credits
Responsible teacher Dr. Hoda Mehrpouyan, Boise University, USA
Course contact person Ulla Vuorinen
Seats 30
Duration 19. - 30.7.2021
Application period: 1.-31.3.2021

COURSE INFORMATION

Course objectives

Students are introduced to the key principles of secure software development, including:

- Explain how software/hardware security should be addressed in rigorous development processes
- Apply methods for documenting the security requirements and secure design of a software/hardware system
- Apply methods for documenting security threats and mitigations
- Demonstrate knowledge of secure programming
- Identify appropriate activities for verification and validation of software security

Content

Week and Dates	**Topics**	**Project**
Day 1 (July 19th)	Secure Software Processes and Introduction to Industrial Control Systems (ICS) Security with case studies and discussion	
Day 2	Security Goals, Access Control, ICS Kill Chain and Attack Steps	HM1 Due
Day3	Secure Design: Control Systems I - *Lab1-Programmable Logic Controller (PLC)*	HM2 Due
Day 4	Control Systems II – *Lab2-PLC Hacking*	HM3 Due
Day 5 (July 25th)	Exam I – C-Strings	
Day 6 (July 26th)	Control Protocols – *Lab3 - Endpoint and Flow Analysis*	HM4 Due
Day 7	Integer overflows, Unknown Control Protocols	HM5 Due
Day 8	Assessing and Exploiting Embedded Electronics I	HM6 Due
Day 9	Assessing and Exploiting Embedded Electronics II	HM7 Due
Day 10 (July 30th)	**Exam II – Student Presentation**	

South-Eastern Finland
University of Applied Sciences

Prerequisities

Programming experiences with Java and C

Grading

Pass/fail or 0-5

Excellent (5)
Good (3-4)
Satisfactory (1-2)
Fail (0)

Assessment

Assignments	40%
Presentation/survey paper	15 %
Exam 1	20 %
Exam 2	25 %

Lecturer of the course

Hoda Mehrpouyan

Dr. Mehrpouyan's research focuses on ensuring privacy, security, and robustness of mission-critical cyber-physical systems. In May 2019, she was awarded a National Science Foundation CAREER Award from the Secure and Trustworthy Cyberspace (SaTC) program. The proposal titled "Formal TOols foR SafEty aNd Security of Industrial Control Systems (FORENSICS)" will develop a multi-layer security framework to provide control technicians and engineers with far superior mechanisms to address the increasing risk of cybersecurity attacks on vulnerable systems. In addition, in Aug. 2016, she was awarded an NSF CISE Research Initiation Initiative

(CRII) grant based on the proposal that was submitted to the Secure and Trustworthy Cyberspace (SaTC) program.

For her work on cybersecurity of the election process in Idaho, she has received funding from the Idaho Secretary of State and for her outreach efforts, she received funding from the National Security Agency (NSA), GenCyber Teacher program in 2017 and 2019.

Her main areas of interest are in requirement analysis and formal verification, compositional modeling and reasoning, safety and failure resilience modeling applied to complex engineering systems such as water treatment plants, smart manufacturing, automobiles, smart grid, and smart cities. To address these objectives, her research explores techniques and tools from different disciplines, i.e., model-based design from the system design community, model checking and formal verification from the software engineering community, and resilience analysis from the complex network theory.