NYU | TANDON SCHOOL OF ENGINEERING

ECE-GY 9463: Security Architectures for Industrial Control Systems

Description:
This course introduces basic and advanced topics on security architectures for Industrial Control Systems (ICS). A comparative analysis between traditional information technology (IT) and operational technology (OT) is presented, along with security vulnerabilities and mitigation strategies assuming real-time requirements and focus on availability. Case studies, current trends, threats, and vulnerabilities will be discussed, as well as attacking and defending methodologies for ICS.

Rationale:
Many cyber security attacks nowadays target critical infrastructure (power grid, water treatment, intelligent transportation, etc.). Cyber security experts should be well informed of the unique challenges of protecting critical infrastructure against cyber threats.

Learning objectives:
1. Understand the differences between IT Security & OT Security
2. Ability to perform effective threat modeling for critical infrastructures
3. Ability to perform effective OT security risk management
4. Ability to design effective ICS security architectures

Tentative course schedule:
1. Introduction / Terminology: This module will serve as the introduction to the course. It will discuss a brief overview of the prerequisites and ICS, will introduce the terms used, and discuss the need for specialization on OT security instead of simply porting IT approaches.

2. Historical events / Current trends: This module will discuss historical events and current malware trends for critical infrastructure, such as Stuxnet, NotPetya, the attack on the Ukrainian power grid, etc.

3. Differences between Information Technology Security and Operational Technology Security: This module will revisit everything discussed in Information and Network Security from an OT perspective. Topics include: Timeliness and Performance requirements, Availability requirements, Risk Management requirements, Physical Effects, System Operation, Resource Constraints, Communication, Change Management, Managed Support, Component Lifetime, Component Location.

4. OT threat modeling: This module will perform threat modeling for OT security, and will also discuss OT-specific attack trees.

5. OT security abstraction layers / Testbeds: This module will abstract OT in distinct layers (hardware, firmware, control, software, network, process) and will discuss the threats for each layer as well as cross-layer threats. Finally, it will introduce the concept of testbeds, which are lab environments suitable for cybersecurity assessment.

6. Anatomy of an OT attack / Case studies: This module will discuss the anatomy of an OT attack using real case studies. It will introduce the cyber kill chain, with discussion on reconnaissance, weaponization, delivery, exploitation, and command-and-control. Real case studies include Stuxnet, the Ukraine power grid attacks, and the Mirai botnet. The module will also introduce the concepts of vulnerability measurements (CWEs, CVEs, CVSS, etc.).

7. Student presentations: Presentation of the assignments.

8. OT Security Risk Management: This module will introduce the risk management process for ICS, and will discuss special considerations for doing an ICS risk assessment, such as: Safety, potential physical impacts, impact of physical disruption, incorporating non digital aspects on ICS into impact evaluations, etc. It will discuss risk analysis as well as methods to address risk. Application of security control to ICS will also be discussed.

9. Industrial protocols: This module will also discuss industrial protocols, ports and services (Modbus, BACnet, DNP3, IEEE 802.x, ZigBee, etc.)

10. ICS Security Architecture 1: This module will discuss approaches to ICS Security architecture. They will discuss network segmentation and segregation, boundary protection, logically separated control networks, and network segregation.

11: ICS Security Architecture 2: This module will continue the discussion of approaches to ICS Security architecture. They will discuss defense-in-depth architectures, general firewall policies for ICS, recommended firewall rules, specific ICS firewall rules, and unidirectional gateways.

12. OT Security Certifications / Standards: This module will discuss existing certification and standards with regards to security of critical infrastructure. It will introduce and discuss in depth the NIST guidelines and cybersecurity frameworks.

13. Emerging approaches: This module will also discuss emerging approaches towards Ot security, such as OWASP security recommendations, ISO standards, ISA standards, etc.

14. State-of-the-art research in OT security: This module will discuss state-of-the-art research in OT security appearing the top security conferences.

15. Student presentations: Presentation of the final project.

Course material:
NIST Guide to Industrial Control Systems (ICS) Security (PDF available online for free)

Grading criteria:
Participation: 20%, Assignments: 30%, Project: 30%, Presentations: 20%

Course requirements:
Assignment 1 [Due: Week 3] [10%]: Understand current threat landscape (malware, ransomware, etc). Students will be asked to find information about the prevalence of threats, historical data, current trends, and future predictions, and then present their findings in a 4-page PDF report.

Assignment 2 [Due: Week 5] [10%]: Students will be asked to use the Shodan search engine in order to understand the threat landscape in terms of publicly accessible devices, in a 4-page PDF report.

Assignment 3 [Due: Week 7] [10%]: Reconnaissance of a specific industry (healthcare, transportation, etc.), across various countries. Students will focus on one critical infrastructure and find information about current landscape, analyze, and suggest solutions and ways forward in a 4-page PDF report.

Presentation 1 [Due: Week 7] [10%]: Present the combination of all assignments during class.

Project [Due: Week 14] [30%] (will be split in milestones, students can work in groups): For a specific critical infrastructure sector (could be the one used in the assignments), students are required to come up with a full risk assessment/management plan to protect it, followed by a thorough security architecture. Students should also prove that their approach meets all required certification standards.

Presentation 2 [Due: Week 14] [10%]: Project presentation during class (allocated time depends on the number of students).