Critical Infrastructure and Control System Cybersecurity Course

What are the security risks of Control System components, communication protocols and operations?

Whether the Control System is automating an industrial facility or a local amusement park roller coaster, the system was designed to operate in a physically, cyber and operationally secure domain. This domain extends throughout the facility using a combination of Programmable Logic Controllers, Programmable Automation Controllers, embedded logic controllers, Remote Terminal Units, as well as Human Machine Interfaces interlinked with one or a variety of SCADA systems and communication protocols across local and long distance geographic regions. The risks vary from simple eavesdropping or electronic denial of service to more sophisticated asset misuse and destruction. To further compound the challenge, today there are not enough professionals with security skills to sufficiently deter, detect and defend active threats against our critical infrastructure's control systems.

How can we progress from Control System security policy development to design, deployment, and assessment?

This course was designed to help organizations struggling with control system cybersecurity by equipping personnel with the skills needed to design, deploy, operate, and assess a control system's cybersecurity architecture. The course begins by quickly describing the risks and then introducing the participants to a customizable actuator and sensor control system trainer and programmable logic environment. This automation programming analysis creates the platform to identify logic flaws that combined with active cyber, physical, and operational procedures may lead to increased risk. The participants then utilize this knowledge to analyze the control system architecture through cyber, physical and operational risks including:

- Control System component engineered, programmed and firmware logic flaws
- Wired and wireless communication protocol analysis
- Physical, cyber and operational procedures
- Deterrence, detection and response to threats

The participant's knowledge is challenged through non-kinetic and kinetic analysis associated with common industry components as well as red team/blue team exercises of both physical and simulated control system environments such as Traffic Lights, Chemical Storage and Mixing, Pipelines, Robotic Arms, Heavy Rail and Power Grids.

What is critical infrastructure Control System cybersecurity?

Control Systems (Local, Distributed and SCADA systems) are used throughout the world to automate common processes. These systems need to provide reliable and safe automation for such critical infrastructures as the Bulk Electric System (BES), natural gas, oil, transportation, chemical, mining, fresh water/waste water, manufacturing, food, and defense. The critical necessities for both government and its people to survive are automated using industrial control systems. In the past decade, advances in technology have added automation that has intertwined of these systems with the Internet, wireless, business networks and traditional hardware and communications protocols. Many Control Systems (CSs) are in some way electronically connected to networks of less trust, potentially even a slight distance away from the Internet. These CSs typically use vulnerable communication protocols. Many even use TCP/IP and in specific situations, common off-the-shelf hardware and chipsets. It is paramount to the safety of our society to sufficiently understand the architecture of and protect these critical systems.

Who should attend this critical infrastructure Control System cybersecurity course?

The class establishes a high-level understanding of Control System cybersecurity valuable to a wide-range of professionals, whether directly in the field or responsible for compliance. The class also dives into a great deal of real-world cybersecurity applications and satisfies those who need or want to understand the inner-workings of the systems as well as the programming behind industrial automation. Therefore, the class is applicable to:

- Security personnel whose job involves assessing, deploying, or securing control system components, communications and operations
- Programmers, network and system administrators supporting control systems
- Process engineers and field technicians
- Operations and plant management personnel
- Control System vendor personnel
- Penetration testers
- NERC CIP, DHS CFATS and other Auditors who need to build deeper technical skills
- Computer emergency response teams

What are some of the topics covered?

- Introduction to programmable logic controllers, function block diagrams, ladder logic, communications and OLE for process control (OPC) / Human Machine Interface (HMI) programming
- Surveying your attack surface; Fingerprinting Control System components and communications inside your organization
- Security Assessments of PLCs/PACs
- Sensor and actuator design analysis using the customized control system trainer units
- Control system cyber case study review and analysis
- Reviewing and analyzing CERT and ICS-CERT vulnerability notifications through the establishment of a vulnerability assessment process
- Kinetic and non-kinetic control analysis using physical and simulated control system scenarios
- Hardware hacking HMIs with a Teensyduino++
- AB PCCC, Ethernet/IP, DNP3, IEC Variants, ICCP, Modbus communication protocol analysis
- Industrial wireless (IEEE 802.11, 900 Mhz, GPRS and IEEE 802.15.4/Zigbee) analysis
- Communication exploit analysis, protocol spoofing and fuzzing
- OLE for process control attack surface, exploitation and mitigating controls
- Performing physical-cyber-operational assessments and penetration tests
- Analyzing and developing Control System oriented Metasploit modules
- Understanding open source intelligence (OSINT) mechanisms used in control system social engineering operations
- Secure remote access solutions; Architecture and operations for administrative and operations remote access
- Integrating and monitoring layered operational, cyber and physical controls

Participant Requirements

Each team of two participants (a Pod) are provided training kits containing all hardware and software necessary for the course: a laptop, PLC programming software, HMI software, customizable actuator/sensor training unit, communications network and cabling, external wireless card, teensyduino++, customized Backtrack platform. The participant is not required to bring any technology to the class; however, the participant may use their own analysis tools.

What material is covered during each course day?

Day 1 (9am – 5pm), Lunch (12:15 – 1:30p)

- Roadmap and overview
- Course ethics and general security awareness
- Brief history of critical infrastructure and control systems
- Control system risk management (Threats, Vulnerabilities and Exploits)
- Surveying your attack surface; fingerprinting control system components and communications inside your organization
- Introduction to programmable logic controllers, function block diagrams, ladder logic, points/tags, communications and OLE for process control (OPC) / Human Machine Interface (HMI) programming
- Sensor and actuator design analysis using customizable I/O control system trainer units

Day 2 (9am – 5pm), Lunch (12:15 – 1:30p)

- Case study review and analysis
- Control system Open Source INTelligence (OSINT) and social engineering
- Control system cyber asset vulnerability assessments and penetration testing (supply chain, communications, firmware, operations and logic)
- Security assessments of PLCs/PACs
- Performing physical-cyber-operational assessments and penetration tests

Day 3 (9am – 5pm), Lunch (12:15 – 1:30p)

- Reviewing and analyzing CERT and ICS-CERT vulnerability notifications through the establishment of a vulnerability assessment process
- PLC configuration panel analysis and mitigating controls
- Hardware hacking control systems with a Teensyduino++, Arduino and Netduino Plus
- Host server (DCS, SCADA, OPC) and HMI protection and controls
- Analyze small scale mock kinetic environments

Day 4 (9am – 5pm), Lunch (12:15 – 1:30p)

- AB PCCC, Ethernet/IP, DNP3, IEC Variants, ICCP, Modbus communication protocol analysis
- Traditional and industrial wireless (IEEE 802.11, 900 Mhz, GPRS and IEEE 802.15.4/Zigbee) analysis
- Communication exploit analysis, protocol spoofing and fuzzing
- Analyzing and developing control system oriented Metasploit communication modules
- Network infrastructure protection and controls
- Secure remote access solutions; Architecture and operations for administrative and operations remote access

Day 5 (9am – 4pm), Lunch (12:15 – 1:30p)

- Integrating and monitoring layered operational, cyber and physical controls
- Situational awareness, assessment and incident response
- Intrusion detection and prevention using network signatures and host-to-host communications analysis
- Forensics and attribution in control systems
- Simulated power grid control system red team / blue team exercise

Author Statement

I wrote this class so that people could understand the elements of, ethically hack and proactively defend our control systems. This course will help the participants figuratively and literally get their hands around the challenges of protecting local and geographically dispersed control environments.