Center for Curriculum and Transfer Articulation

Embedded Systems Security

Course: **CIS275DC**	Lec + Lab **3** Credit(s) **4** Period(s) **3.7** Load
	Course Type: **Occupational**
First Term: **2014 Fall**	Load Formula: **S- Standard**
Final Term: **Current**	

Description: In-depth overview of embedded systems used in power system utility environments and their underlying infrastructure. Provides understanding of what embedded systems are, how they are implemented and the security risks that are associated with them. Focuses on conducting reconnaissance activities from untrusted networks to identify weaknesses in control system networks. Describes how execution of attacks can be used to gain unauthorized access, creating impacts on embedded systems including the effects that they create. Actions that mitigate or reduce the risk of attacks to embedded systems that support grid operations are stressed. Partial preparation for certifications such as the International Council of Electronic Commerce Consultants (EC-Council) Certified Ethical Hacker (CEH) with a concentration in embedded systems security.

Requisites: Prerequisites: CIS274DA or permission of Instructor.

MCCCD Official Course Competencies

1. Describe the overall structure of embedded systems and how they support industrial control systems (I, III, IV).
2. Demonstrate impacts of advanced threats to industrial control systems (II).
3. Explain passive penetration testing its importance in assessing risks to embedded systems in support of industrial control systems (V, VI).
4. Discuss the impacts that affect the bulk electric system as it relates to compromise of embedded systems within the power utility core infrastructures such as Power Plant, SCADA, Smart Meters, Transmission and Distribution systems (VII).
5. Describe strategies which can be applied to embedded systems in order to secure them against emerging threats and to secure the industrial control systems (VIII).
6. Explain the evolution of successful attacks on embedded systems; how they work and how to protect against them (IX).

MCCCD Official Course Outline

I. Industrial Control System (ICS)
A. Supervisory Control and Data Acquisition (SCADA)
1. SCADA Telecommunications
2. Legacy SCADA Protocols
3. Enhanced SCADA Protocols
B. Energy Management Systems
C. Distributed Control System (DCS)

1. Programmable Logic Controllers (PLC)
2. Single Loop Controllers
3. Smart Field Devices
4. Communications Processor
5. Relays
6. Phasor Measurement Units
7. Smart Meters
8. Smart Collectors
9. Head end Systems

D. Industrial Control System Characteristics

II. Advanced Cyber Threats to the Electric Grid

A. United States Computer Emergency Readiness Team (US-CERT)

B. Industrial Control System Computer Emergency Readiness Team (ICS-CERT)

III. Embedded Systems Overview

A. Programmable Logic Controllers

1. Ladder Logic

B. Remote Terminal Units

C. Human/Man Machine Interfaces

D. Transformers

E. Generators

F. SCADA

1. VAX
2. Windows
3. Linus
4. Unix

IV. Building Embedded Devices

A. Configuration Setup

B. Network Setup

V. Passive Penetration Testing

A. Reconnaissance

B. Scoping

C. Network Perimeter Identification

1. Firewalk
2. Hping
3. Nmap
4. ARP Poisoning

D. External Network Host Identification

1. Historian
2. Operational Support Systems
3. Control System Support Systems
4. Corporate Support Systems

E. External Vulnerability Identification

F. Trusted Path Identification

1. Corporate Assets
2. Operations Assets
3. Control System Assets

G. Trusted Path Exploitation

1. Operating attacks

1. Operating attacks
2. Network attacks
3. Application attacks
4. SQL Injection attacks
5. User based attacks
6. Social Engineering

H. Control System exploitation do?s and don?ts

VI. Hacking the Embedded System

A. Hacking Industrial Control System Protocols

1. MODBUS
2. DNP
3. IEC 61850
4. Proprietary Protocols

B. Control System Network Traffic Analysis

1. Normal Control System Traffic
2. Unusual Control System Traffic

C. PLCs and ladder logic

D. RTUs and Telemetry

E. Phasor Measurement Units and the Reliability Coordinator

F. The Independent System Operator

G. Smart Meters and the ANSI protocols

VII. Creating Impacts with Embedded Systems

A. Process Control Impacts

1. Mechanical Process Disruption
2. Mechanical Process Modification

B. Plant Shutdown Impacts

1. Power Plant Revenue
2. Power Plant Safety
3. Grid Stability
4. Spinning and Contingency Reserve

C. SCADA Impacts

1. Grid Stability
2. Grid Reliability
3. Rolling Blackouts
4. Outage Detection Capabilities

D. Substation Impacts (Transmission and Distribution)

1. Breaker Failure
2. Transformer Malfunctions
3. Substation Safety

E. Residential Metering Impacts

1. Revenue Impacts
2. Power Outage
3. Privacy Impacts
4. Reputational Damage

VIII. Securing Embedded Systems

A. Defense in Depth

1. Proper Firewall Configuration
2. Data Diodes
3. Alerts

3. Alerts
4. Detecting Malicious Control System Activity
5. Responding to Control System Events
6. Security Awareness and Training
7. Wireless and Mesh Network Security
8. Vendor approved patches
9. Configuration Management
10. Unauthorized Connectivity
11. Network Segmentation
12. User/System Access

IX. Control System Incidents

A. Stuxnet
B. Night Dragon

Last MCCCD Governing Board Approval Date: **June 24, 2014**
