# Teaching Industrial Control System Security Using Collaborative Projects

Thuy D. Nguyen, Mark A. Gondree, David E. Reed

## Conference on Cybersecurity of Industrial Control Systems

September 2015

# Motivations

- The insecurity of ICS is a pressing problem
  - 400+ ICS-CERT Advisories on ICS vulnerabilities and exploits

    - ICSA-15-239-01 : Moxa SoftCMS Buffer Overflow Vulnerabilities
    - ICSA-15-239-02 : Siemens SIMATIC S7-1200 CSRF Vulnerability
    - ICSA-15-239-03 : Innominate mGuard VPN Vulnerability
    - ICSA-15-237-01 : Endress+Hauser HART Device DTM Vulnerability
    - ICSA-15-225-01 : OSIsoft PI Data Archive Server Vulnerabilities
    - ICSA-15-223-01 : Schneider Electric IMT25 DTM Vulnerability

    [snip]

- ICS security is different from IT security
  - ICS has unique performance, reliability, safety requirements

- Need to prepare our students for proficiency in ICS security

*The views expressed in this material are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*

# Topics

- Course description
- Course format
- Project description
- Discussion and conclusions

# Cyber Systems and Operations (CSO) Curriculum

- 18-month graduate program focusing on cyber operations
  - Cyber operations requires both defensive and offensive skills
  - Graduation requirements include a capstone course and a thesis

- Technical emphasis
  - Computer network attack, defense, and exploitation
  - Cyber analysis, operations, planning and engineering
  - Cyber intelligence operations and analysis

- Practically-focused
  - Site visits, wargaming exercises, seminars, guest speakers and practical workshops

# CSO Capstone Course

- Follow *collaborative learning* and *problem-based learning* teaching methodologies
- Students work in small groups to solve real-world problems
  - Utilize previously-learned knowledge and skills
  - Have completed most of CSO program requirements
- Involve participation of an ICS system owner and ICS subject matter experts (SME)
- Focus on shipboard ICS because of its relevance to our school's mission

# Learning Objectives

- Student teams develop courses of action (COA) for specific ICS problems provided by the stakeholders
  - ICS is an unfamiliar technical domain for students
- Overall objective – can demonstrate in-depth understanding of project-related material
- Specific objectives – be able to
  - collaborate on research in self-directed teams
  - communicate in-progress research results to a technical audience
  - interpret and respond to outside technical feedback
  - prepare COA design alternatives
  - evaluate alternatives from an operational perspective
  - synthesize final technical recommendations
  - communicate technical recommendations to a stakeholder

# Topics

- Course description
- Course format
- Project description
- Discussion and conclusions

# Course Schedule

- Delivery method
  - Resident course format with in-class meetings each week
  - Out-of-class expected time commitment is ~8 hours per week

- Instructor and SME work together to guide students in research and COA development

| Phase | Purpose | Primary Participants |
|---|---|---|
| Phase 0 | Project creation | SME, instructor |
| Phase 1 | Technology familiarization | Students, instructor |
| Phase 2 | Initial engagement with SME | SME, students, instructors |
| Phase 3 | Interim progress review | SME, students |
| Phase 4 | Final progress review | SME, students |
| Phase 5 | Project conclusion | Students |

# Project Creation & Technology Familiarization

- **Phase 0** – occurs ~3 months before class begins
  - Instructor solicits real-world ICS problems from stakeholders and SMEs
  - Instructor and SME iteratively refine scope of work
    - Must align with students' technical background and course timeframe
  - Final outcome is a detailed project assignment

- **Phase 1** – students learn about ICS basics

| Lecture | Homework | Laboratory |
|---|---|---|
| ICS technology | Academic papers | ICS vulnerabilities |
| ISA/IEC-62443 | SME-provided materials | |
| ICS vulnerabilities | Videos on ICS security research | |

# SCADA-in-a-box Lab Exercise

- Simulate a realistic natural gas compression system
- Kit includes a PLC, HMI software, an industrial firewall, malware demonstrating a ModBus-based PLC exploit
- Two activities
  - Conduct an attack on unprotected PLC using malware delivered via opening a PDF on HMI system
  - Add and configure a firewall for the system to block unauthorized traffic

# Initial Engagement with SME & Interim Review

- **Phase 2** – research begins
  - First meeting with SME
    - Clarify assumptions, collect information, clarify project scope
    - SME can gauge students' technical strengths
  - SME-guided ship tour
    - Gain insights on ICS equipment, operational procedures

- **Phase 3** – research continues
  - Iterative COA development
    - Develop, deliberate, refine working versions cyclically
    - Discuss weekly accomplishments in class
  - Progress review with SME
    - Students present emerging ideas and potential approaches
    - SME provides guidance on challenges encountered

# Final Review & Project Conclusion

- **Phase 4** – research ends
  - COA refinement
    - More focused analyses based on SME's feedback
    - Demonstrate working prototypes for hands-on projects
  - Final review with SME
    - SME examines validity and feasibility of recommended COAs
    - Recommendations with solid technical analysis or prototypes will be considered for implementation

- **Phase 5** – project wraps up
  - Finalize project reports

# Topics

- Course description
- Course format
- Project description
- Discussion and conclusions

# Project Summary

| Project | Scope |
|---|---|
| Software subversion | Analysis of existing systems |
| Network security | Analysis of existing systems |
| Protection of multicast messages | Design |
| Smart card authentication | Design |
| Code repository security | Design |
| Continuous monitoring | Prototyping |
| Backplane intrusion detection | Tabletop vulnerability assessment |

# Software Subversion & Network Security

- **Software subversion via portable memory devices**
  - Problem: Inappropriate use of portable memory devices to introduce malicious code into a shipboard ICS
  - Review existing policies and operational practices
  - Propose changes to allow the use of these devices
    - Case studies: list control system and ventilation system

- **Network security**
  - Problem: Unauthorized traffic between an ICS network and the external shipboard network
  - Investigate network isolation technologies
  - Propose ways to implement a DMZ and use perimeter control technologies in a shipboard ICS
    - Case studies: list control system and ventilation system

# Message Protection & User Authentication

- **Protection of multicast IPsec messages**
  - Problem: Messages between PLC and HMI systems are not authenticated
    - Current design uses IP multicast to conserve bandwidth
  - Investigate both BITW and BITS IPsec approaches
  - Propose an ICS design using IPsec to provide integrity and anti-replay protection

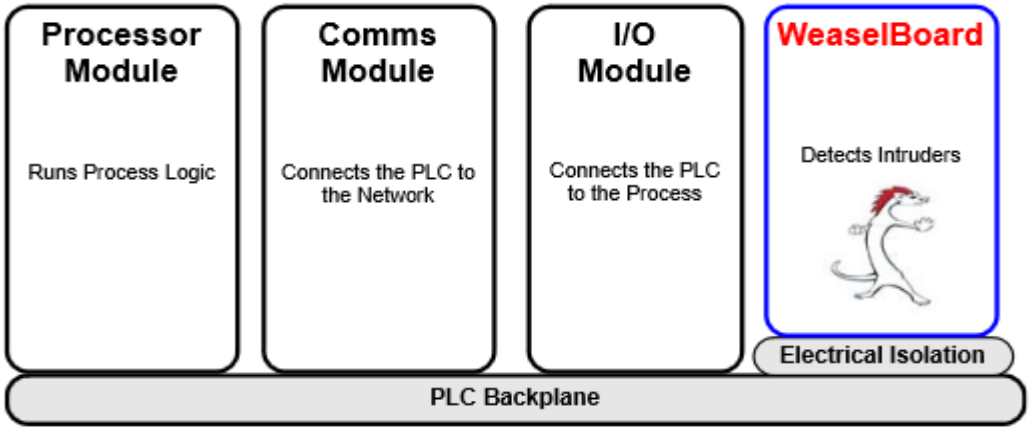
- **Smart card authentication**
  - Problem: User authentication is weak in ICS domain
  - Survey both contact and contactless smart cards for use in ICS
  - Develop a concept of operations for user authentication using smart cards in a typical shipboard ICS
    - Include system life cycle management—initial deployment through retirement or disposal

# Revision Control & Continuous Monitoring

- **Code repository security**
  - Problem: Unprotected revision control systems are easy targets
  - Survey known attacks against Apache Subversion (SVN) and Git
  - Investigate how to secure an SVN/Git server for use in ICS
    - Include eliciting functional and security requirements from SME
  - Recommend a revision control system and methods for hardening it for use in ICS

- **Real-time security monitoring**
  - Problem: Historians do not track security-relevant events
  - Examine open source tools for monitoring security events in an ICS
    - Security event management (aka SIEM): OSSIM
    - Network monitoring: Zabbix
  - Propose ways to integrate these tools in a shipboard ICS
    - Include identifying ICS-aware plugins that must be developed or customized

# PLC Backplane Intrusion Detection




- Problem: PLC backplane activities can be exploited to collect information about PLC design and software
- Perform tabletop vulnerability assessment of Sandia's WeaselBoard using a fictional ICS
  - WeaselBoard captures backplane traffic and forwards it to an external system for intrusion analysis
  - Develop potential attack scenarios that can bypass WeaselBoard's alarm generation mechanisms

# Topics

- Course description
- Course format
- Project description
- Discussion and conclusions

# Lessons Learned

- Successful ways to improve student understanding:
  - Direct instruction, field trips, ICS-relevant lab exercises
- Successful ways to increase student engagement:
  - Projects with hands-on experiments
  - Leverage student familiarity with the problem context
- Formulation of project assignments was difficult
  - Collective experience of a cohort was not fully understood when project assignment areas were developed
- Iterative research and design process was challenging
  - Many students viewed unanticipated problems as impediments, rather than opportunities for improvement

# Lessons Learned (cont.)

- Horizontal transfer of knowledge was challenging
  - Most students had problem applying prior knowledge in new and unfamiliar contexts
- Friendly team rivalry produced more complete and in-depth research results
- New project topics required lots of work
  - Steep learning curve for students
  - Time-consuming project refinement for instructor and SME
- A common perception: ICS-related projects were not relevant to students' course of study
  - Interaction with SMEs helped overcome this obstacle

# Conclusions

- Students were able to demonstrate understanding of ICS security issues successfully
  - SME feedback indicated student recommendations were sensible
  - Some recommendations were targeted for adoption
- Having SME support and field trips was imperative for reinforcing ICS concepts and technologies
- Improvements being considered:
  - Add a prerequisite course focusing on ICS security with hands-on exercises
  - Projects are built on previous findings
    - Allow tech transfer across cohorts

Thuy D. Nguyen

Department of Computer Science
Naval Postgraduate School
Monterey, CA 93943 U.S.A

tdnguyen@nps.edu