Matthew E. Luallen
cybati.org

CybatiWorks Mini Kits Kickstarter

37
backers

$31,291
pledged of $30,000 goal

0
seconds to go

Funded!

This project was successfully funded on October 17.

Our Agenda

- What is the CybatiWorks platform?
- Building and using the Mini-Kit Edition
- CybatiWorks Missions version 1

What is it?

- The CybatiWorks® scalable academic and professional control system and internet of things cybersecurity platform enables educational institutions, industrial asset owners / operators and supporting entities to quickly understand control system environments and cybersecurity risks. The portable and complete training platform has been validated by hundreds of industry practitioners and educators.

- Grows with you, your educational and laboratory testing needs
  - Mini Kits
  - Missions
  - Courseware
  - Industrial Edition
  - Kinetic Models

Where did it come from?

- Built laboratory to achieve CCIE status in 1998-1999
- Long time instructor for Cisco Systems and SANS Institute
- 802.11 wireless at substations in 2005
- ICS cybersecurity conversion year 2006.
- NERC CIP / Transportation / Water control system control interpretation and integration world tour 2007-2010
- Cybati formed to build education to expand workforce and family home turned in to living laboratory
- Back injury, healing and ICS cybersecurity education world tour 2011 – today

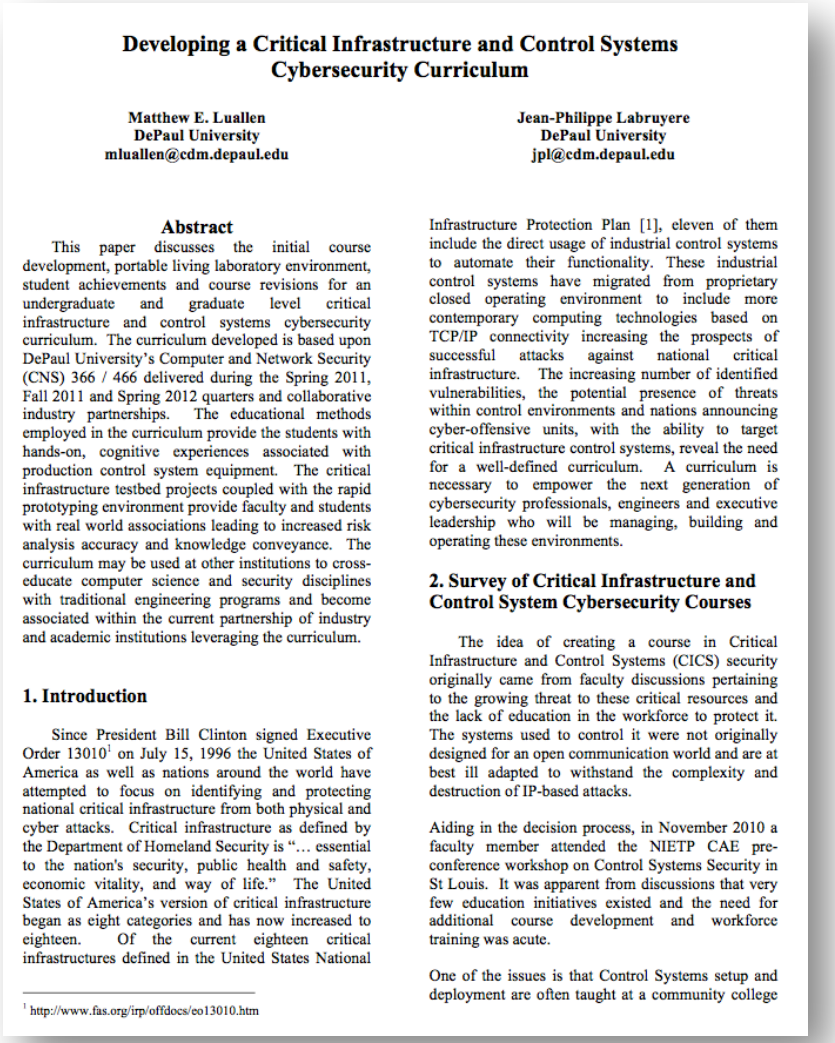
CybatiWorks-1

- **CybatiWorks® Educational Platform Supported Learning Outcomes**

  - History of critical infrastructure and control systems
  - Cyber-physical security risk management
  - Vulnerability assessment and penetration testing
  - Attack surface analysis
  - Exploit code analysis
  - Secure coding
  - Logic analysis and physical I/O control
  - Industrial and building automation protocols
  - Engineering workstation and server operating systems
  - Engineering workstation and server operating systems
  - HMI screens points, tags and design
  - OLE for Process Control
  - Cryptography
  - Kinetic model analysis
  - Wireless analysis
  - Application security (e.g. web, database)
  - Intrusion detection and visualization
  - Incident response and active defense

Accepted Conference Paper

- HICSS 46, January 2013
- Developing a Critical Infrastructure and Control System Cybersecurity Curriculum
- Identifies student projects, successes, failures and path forward



Developing a Critical Infrastructure and Control Systems Cybersecurity Curriculum

Matthew E. Luallen
DePaul University
mluallen@cdm.depaul.edu

Jean-Philippe Labruyere
DePaul University
jpl@cdm.depaul.edu

Abstract

This paper discusses the initial course development, portable living laboratory environment, student achievements and course revisions for an undergraduate and graduate level critical infrastructure and control systems cybersecurity curriculum. The curriculum developed is based upon DePaul University's Computer and Network Security (CNS) 366 / 466 delivered during the Spring 2011, Fall 2011 and Spring 2012 quarters and collaborative industry partnerships. The educational methods employed in the curriculum provide the students with hands-on, cognitive experiences associated with production control system equipment. The critical infrastructure testbed projects coupled with the rapid prototyping environment provide faculty and students with real world associations leading to increased risk analysis accuracy and knowledge conveyance. The curriculum may be used at other institutions to cross-educate computer science and security disciplines with traditional engineering programs and become associated within the current partnership of industry and academic institutions leveraging the curriculum.

1. Introduction

Since President Bill Clinton signed Executive Order 13010[1] on July 15, 1996 the United States of America as well as nations around the world have attempted to focus on identifying and protecting national critical infrastructure from both physical and cyber attacks. Critical infrastructure as defined by the Department of Homeland Security is "… essential to the nation's security, public health and safety, economic vitality, and way of life." The United States of America's version of critical infrastructure began as eight categories and has now increased to eighteen. Of the current eighteen critical infrastructures defined in the United States National Infrastructure Protection Plan [1], eleven of them include the direct usage of industrial control systems to automate their functionality. These industrial control systems have migrated from proprietary closed operating environment to include more contemporary computing technologies based on TCP/IP connectivity increasing the prospects of successful attacks against national critical infrastructure. The increasing number of identified vulnerabilities, the potential presence of threats within control environments and nations announcing cyber-offensive units, with the ability to target critical infrastructure control systems, reveal the need for a well-defined curriculum. A curriculum is necessary to empower the next generation of cybersecurity professionals, engineers and executive leadership who will be managing, building and operating these environments.

2. Survey of Critical Infrastructure and Control System Cybersecurity Courses

The idea of creating a course in Critical Infrastructure and Control Systems (CICS) security originally came from faculty discussions pertaining to the growing threat to these critical resources and the lack of education in the workforce to protect it. The systems used to control it were not originally designed for an open communication world and are at best ill adapted to withstand the complexity and destruction of IP-based attacks.

Aiding in the decision process, in November 2010 a faculty member attended the NIETP CAE pre-conference workshop on Control Systems Security in St Louis. It was apparent from discussions that very few education initiatives existed and the need for additional course development and workforce training was acute.

One of the issues is that Control Systems setup and deployment are often taught at a community college

[1] http://www.fas.org/irp/offdocs/eo13010.htm

Cybati Critical Infrastructure and Control System Cybersecurity Course

- Academic and Professional
- Educated over 1,000 participants
- 5-day hands-on course covering ICS/SCADA/ Plant attack surface and mitigating controls
- Designed with a portable, living laboratory of real applications, hardware and protocols
- 85% rate of identifying new vulnerabilities during the course week

RECENT ADVISORY (ICSA-14-254-02)

OVERVIEW

This advisory was originally posted to the US-CERT secure Portal library on September 11, 2014, and is being released to the NCCIC/ICS-CERT web site.

Independent researcher Matthew Luallen of CYBATI has identified a denial-of-service (DoS) vulnerability to the DNP3 implementation of the Allen-Bradley MicroLogix 1400 controller platform. Rockwell Automation has produced a firmware revision that mitigates this vulnerability.

This vulnerability could be exploited remotely.

CYBATI CICS Cybersecurity Industrial Edition Training Kit (version 1)

- Customized, portable kit to augment the course content

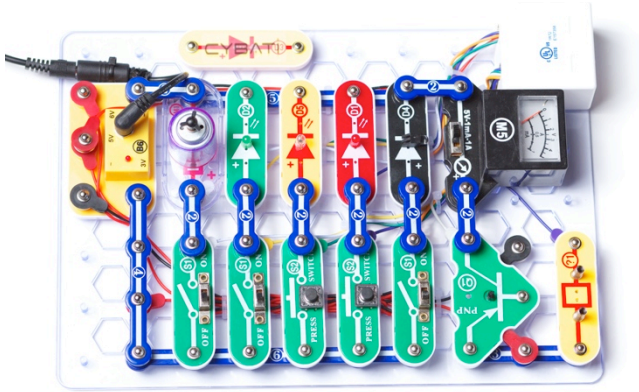
- Control System Portable Laboratory and Research Kit (Allen Bradley MicroLogix and Siemens Programmable Logic Controllers)
- PLCtrainer.net static trainer
- HMI, PLC, Manual Controls, CS Network, CYBATIFIED Backtrack

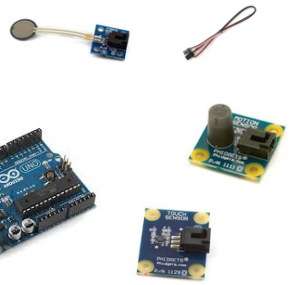
CYBATI CICS Cybersecurity Industrial Edition Training Kit (version 2)

- Similar to IPv5, CYBATI's version 2 training kit lasted for about 4 months
  - Attempted several new designs of quick connect sensors, kinetic modeling and associated cybersecurity learning methods

CYBATI CICS Cybersecurity Training Kit (version 3)

- Customized, portable kit to augment the course content

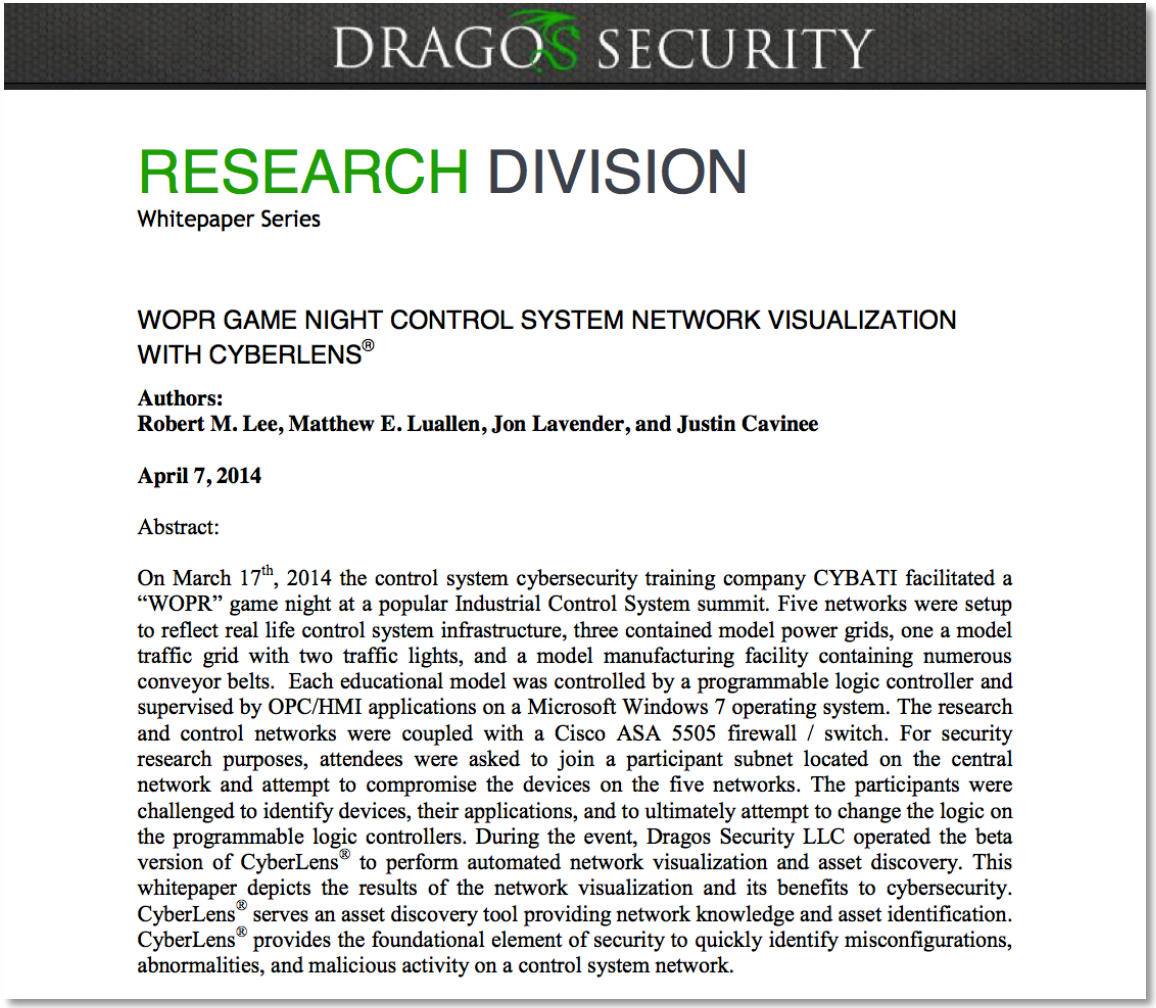




- Modifications
  - Customizable I/O trainer
  - Quick connect PLC I/O
  - Phidget™, Arduino™ and other 3-5 vdc sensors and actuators
  - More protocols (DNP3, Modbus)
  - Small scale environments

CYBATI CICS Cybersecurity Mastery Stations (version 1)

- WOPR Event
- Mission assignments
- Participant driven
- Skill assessment through risk identification and penetration



DRAGOS SECURITY

RESEARCH DIVISION

Whitepaper Series

WOPR GAME NIGHT CONTROL SYSTEM NETWORK VISUALIZATION WITH CYBERLENS®

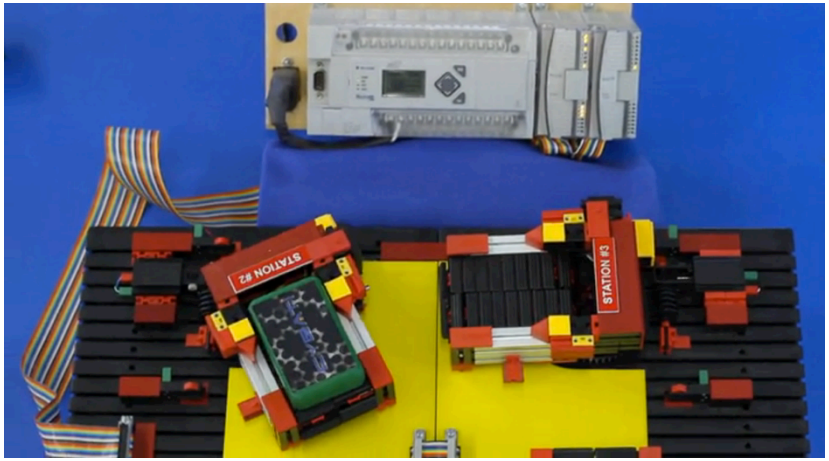
Authors:
Robert M. Lee, Matthew E. Luallen, Jon Lavender, and Justin Cavinee

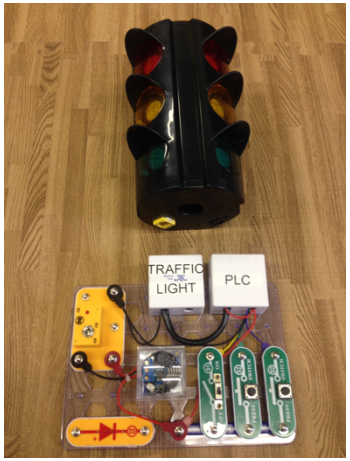
April 7, 2014

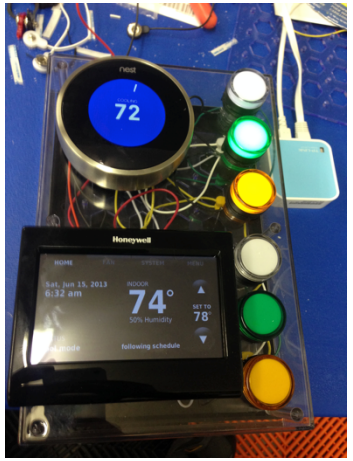
Abstract:

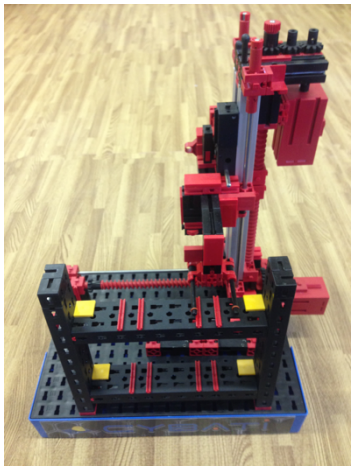
On March 17th, 2014 the control system cybersecurity training company CYBATI facilitated a "WOPR" game night at a popular Industrial Control System summit. Five networks were setup to reflect real life control system infrastructure, three contained model power grids, one a model traffic grid with two traffic lights, and a model manufacturing facility containing numerous conveyor belts. Each educational model was controlled by a programmable logic controller and supervised by OPC/HMI applications on a Microsoft Windows 7 operating system. The research and control networks were coupled with a Cisco ASA 5505 firewall / switch. For security research purposes, attendees were asked to join a participant subnet located on the central network and attempt to compromise the devices on the five networks. The participants were challenged to identify devices, their applications, and to ultimately attempt to change the logic on the programmable logic controllers. During the event, Dragos Security LLC operated the beta version of CyberLens® to perform automated network visualization and asset discovery. This whitepaper depicts the results of the network visualization and its benefits to cybersecurity. CyberLens® serves an asset discovery tool providing network knowledge and asset identification. CyberLens® provides the foundational element of security to quickly identify misconfigurations, abnormalities, and malicious activity on a control system network.

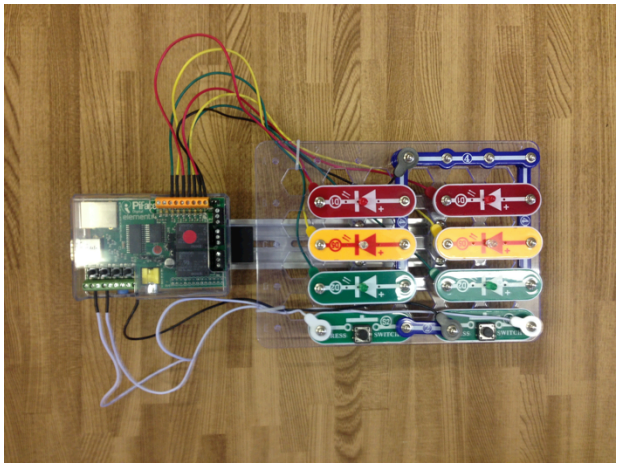
Sample Kinetic Models (Mastery Stations)

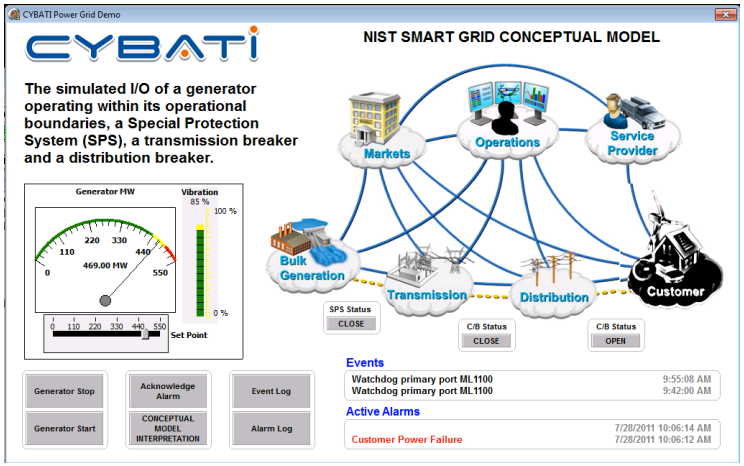












Sample Kinetic Models (Mastery Stations)

- Traffic Light
- Robotic Arm
- Train / Rail
- Manufacturing Line
- Amusement Park
- Pipeline / Fuel Operations
- Water Treatment Facility

CybatiWorks Mini Kits Kickstarter

- Hands-on Demonstration

SHA1 Fingerprints (USB Drive)

- SHA1 tools
  - **MAC OS / Linux** *openssl sha1 <file>*
  - **MS Windows** *FCIV –sha1 <file>*
- SHA1(CybatiWorksPI.img.zip)= 58507d2e7e9f07ad6673ca1c94ea2cfdf455b9a3
- SHA1(CybatiWorks-1.vmwarevm.zip)= ee5e425ac28d0c523fa37e14ad18df030026e617
- SHA1(Laboratory- CybatiWorks-1 Initial Setup.pdf)= 5c833ed5163e039b2b1b9762e823bdf54e71e4a9
- SHA1(Win32DiskImager-0.9.5-binary.zip)= 75e886d0941b0de14b463a55609125631b307398

ICS Security Goals through Missions

- Over 1,000 participants to date with cyber, operational and physical security skillsets
- Hands-on cybersecurity missions to achieve awareness during live-fire events
- Maintaining a trustworthy and accessible system
- An adversary must only successfully penetrate one pathway

- Missions and models devised to illuminate the risks and mitigating options

Mission Categories

- BLUE 
  - Personnel skills inventory, cyber asset discovery, change management, vulnerability assessment, incident response and forensics, operational procedures, technical mitigations
- RED 
  - See above (without authority)

Mission Notables

- RED
  - BAUD rate cycling of administrative serial port
  - All GREEN traffic light
  - Model train set derailed
  - Project file password extraction of protected ICS device used for engineering workstation control
  - New zero-days identified (Firmware, HTTP, Modbus, DNP3, Engineering workstation software …)
- BLUE
  - Functional process logic altered to defeat cyber attack
  - Labrea tar pit / honeypot systems
  - Forensics analysis of project file network exfiltration
  - Critical ICS/SCADA point analysis and monitoring

Mini Kit Missions!

- Participant Missions
- Exploratory to assess your skills
  - Applied research to support the community

- Win free access to the upcoming limited seat (limited to 6 participants) DL course
  - April 21, 22 and 27, 28
  - $3,995 including Mini Kit

THE ANSWER.
54:52:55:53:54

"I recognize that today is the smartest I will ever be for the remainder of my life. When I was a child I knew everything and now each day I learn of more that I do not understand."

We need volunteers

- Mission enhancements
- Kinetic models