



OPSEC
for Control Systems Engineers & Operators
Alpha

Introduction

This lesson defines OPSEC.

Enabling Learning Objective: Learn what OPSEC is, why it is important, and the Department of Homeland Security's purpose.

Pages in this lesson:

1. What is OPSEC?
2. Why Do It?
3. The Department of Homeland Security's Purpose

Presentation to the Control Systems Security Outreach Coordination Meeting

Mark P. Morgan
Lori Ross O'Neil
July 24, 2007

Cyber Security
for Control Systems Engineers & Operators

The Attack Process

This lesson discusses how vulnerabilities are exploited and the consequences of threats to the control system. Click the **PLAY** button below to watch a simulation of a cracker attacking a network.

PLAY

Cracker Employee

Internet Corporate Network Process Control Network

Slave Database Master Database HMI PLC SCADA



Areas to be addressed

- Current CSSP control systems security training
 - Online
 - Instructor Led
- Other Control System Security Training
- Training Ready for Transition to Industry
- Capabilities available for Industry Utilization

Current Training: Idaho National Lab

Instructor Led http://www.us-cert.gov/control_systems/cstraining.html

- *Control Systems Cyber Security – Who Needs It?* (1 hour)
- *Control Systems Security for Managers* (1 hour)
- *Intermediate Solutions for Process Control Security* (4 hours)
- *Introduction to Control Systems Security for the IT Professional* (8 hours)
- *Intermediate Control Systems Security* (8 hours)
- *Advanced Control Systems Cyber Security and Hands-on Workshop* (2 to 4 days)

Online Control System Security Training

Cyber Security
for Control Systems Engineers & Operators

LESSONS

- Threats and Risks
- Specific Risks to Control Systems
- Cyber Attacks
- Risk Assessment Overview
- Mitigation for Control Systems

Welcome to Cyber Security for Control Systems Engineers & Operators

Terminal Learning Objective

Cyber Security
for Control Systems Engineers & Operators

Current Lesson: 3

LESSONS

- Threats and Risks
- Specific Risks to Control Systems
- Cyber Attacks
- Risk Assessment Overview
- Mitigation for Control Systems

The Attack Process

This lesson discusses how vulnerabilities are exploited and the consequences of threats to the control system. Click the **Play** button below to watch a simulation of a cracker attacking a network.

PLAY

Cracker Employee Internet Corporate Network Process Control Network PLC HMI

Contact Us
Privacy Notice

Page updated: 02/09/2009
Course version: 1.1
Last reviewed: 2/8/2009

Contact Us
Privacy Notice

Course updated: 03/05/2009

▶ **Cyber Security for Control Systems Engineers and Operators** (~1 hour)

<http://cssptraining.labworks.org/training/lms/>

▶ **OPSEC for Control Systems Engineers and Operators** (~1 hour) 3 months until deployment

OPSEC
for Control Systems Engineers & Operators
Alpha

LESSONS

- Introduction
- Five-Step OPSEC Process
- Your Information: Who Wants It and How They Get It
- Information Protection
- Physical Protection

Introduction

This lesson defines OPSEC.

Enabling Learning Objective: Learn what OPSEC is, why it is important, and the Department of Homeland Security's purpose.

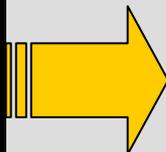
Pages in this lesson:

1. What is OPSEC?
2. Why Do It?
3. The Department of Homeland Security's Purpose

Profile of Online Learners Taking *Cyber Security for Control Systems Engineers and Operators*

240 students since February 2007

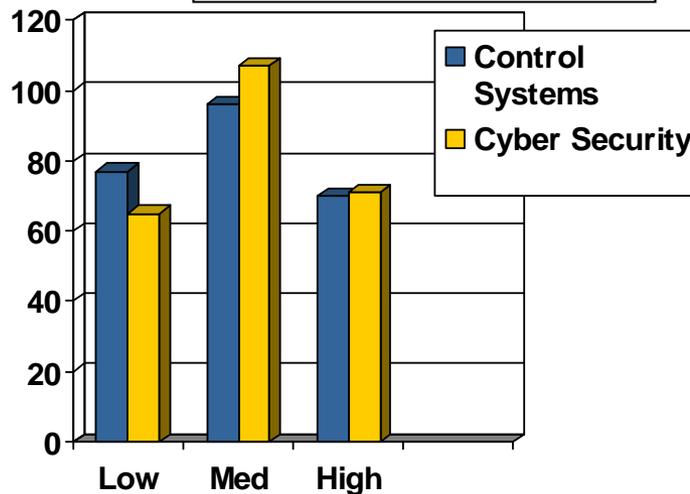
Totals by Industry:	100%
Electric	25%
Other	23%
Oil/Gas	18%
Nuclear	17%
Chemical	6%
Water	6%
Manufacturing	2%
Transportation/Shipping	2%
Natural Gas	1%



Totals by Job:	100%
Control Systems	36%
Other	15%
IT	45%
Training	4%



Experience Levels



Profile of Online Learners Taking continued Cyber Security for Control Systems Engineers and Operators

- ▶ Who visits?
- ▶ From where?

Rank	Who?
1	Various ISPs
2	British-energy.com
3	Shell.com
4	Military
5	Education

Rank	Country
1	United States
2	United Kingdom (.uk)
3	Australia (.au)
4	Singapore (.sg)
5	Canada (.ca)
6	Germany (.de)
7	New Zealand (.nz)
8	France (.fr)
9	Netherlands (.nl)
10	Switzerland (.ch)
11	Ghana (.gh)
12	Pakistan (.pk)

Profile of Online Learners Taking continued *Cyber Security for Control Systems Engineers and Operators*

▶ What are they saying about the training?

77% who completed it would like additional training

▶ Comments from the post-training survey:

Recommended by a colleague - very good.

...more advanced online training would be useful.

..quick way to learn the basics of cyber attack and damage.

LIQUIDMATRIX SECURITY DIGEST

SCADA (in)Security Training

Author: Dave Lewis

May 15, 2007 at 3:24 pm · Filed under [Web Security](#), [SCADA Security](#)

Digital Bond: SECURING THE CRITICAL INFRASTRUCTURE

HOME

CONSULTING

RESEARCH

SCADA Security Training

Other Control System Security Training

- ▶ *Introduction to Control Systems* (~3 days)
 - Provided for Federal Law Enforcement and Other Agencies
 - Hands-on Exercises
 - Field Trips
- ▶ *NRC Inspectors Cyber Security (NICSec) Training* (4 day on-site) 6 months until deployment



U.S. NRC *Protecting People and the Environment*
UNITED STATES NUCLEAR REGULATORY COMMISSION

About NRC	Nuclear Reactors	Nuclear Materials	Radioactive Waste	Nuclear Security	Public Meetings & Involvement
-----------	------------------	-------------------	-------------------	------------------	-------------------------------

Training Ready for Transition to Industry Easily Modified for Control Systems

▶ Currently Internet Accessible:

<http://cybertrain.labworks.org/>

- *Computer Sanitization Awareness Training (DOE M205.12)*
- *Online Computer Forensics Awareness Training*

▶ *CyberCIEGE*- Learners construct and defend a cyber network in online game.

▶ *SAST Systems Administrator Simulation Trainer* - online real-world experience in identifying, responding to, and recovering from cyber attacks.



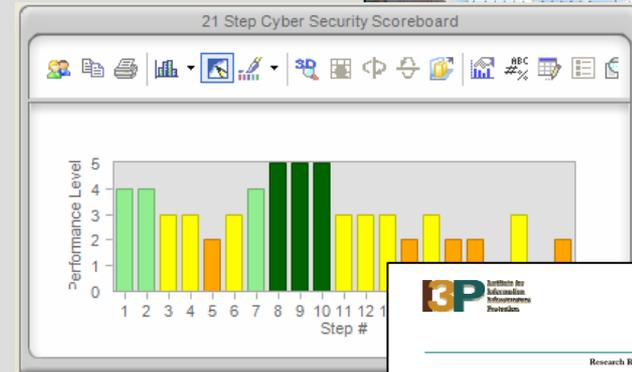
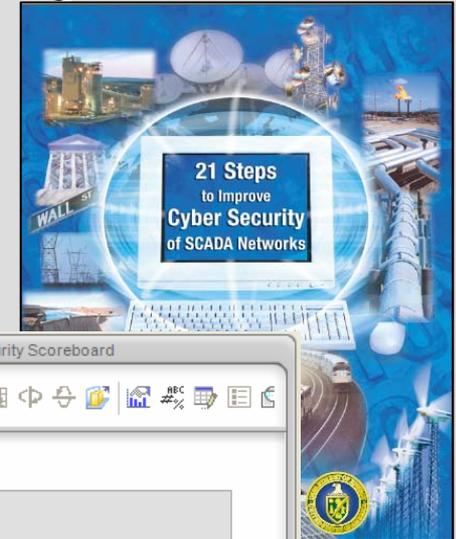
Capabilities available for Industry Utilization

- ▶ CIPAL Critical Infrastructure Protection Analysis Laboratory
<http://homeland-security.pnl.gov/cipal.stm>
- ▶ Electricity Infrastructure Operations Center (EIOC)
- ▶ Power Systems Communication Laboratory



I3P Products Potentially Available for Transition to Industry

- ▶ SHARP *Security Hardened Attack Resistant Platform* – approach to securing the control system.
- ▶ Cyber Security Metrics for Control Systems automated decision tool – based on *DOE 21 Steps to Improve Cyber Security of SCADA Networks*
- ▶ Control Systems Security Metrics Starter Kit – utilize existing tools for holistic control system metrics view



Process Control Systems Security Metrics – State of Practice

Conclusions

- ▶ Actively involved in CSSP training support
 - Niche: on-line training
 - Memorable and valuable
- ▶ Other control system security training is available to be leveraged by CSSP
- ▶ Other training capabilities that could be modified for control system security
- ▶ Physical capabilities exist for CSSP use
- ▶ Tech Transfer opportunities currently exist through coordination with other agencies

Contact Information

Mark P. Morgan m.morgan@pnl.gov 509/372-4128

Lori Ross O'Neil lro@pnl.gov 509/375-6702

For more information:

<http://cssptraining.labworks.org>

<http://www.pnl.gov/coginformatics>