

Control Systems Security Program Education & Training Interest Group PCSF – June 7, 2006 La Jolla, CA

Brian Lopez (blopez@llnl.gov, 925 422 5839)

Lawrence Livermore National Laboratory (LLNL)

Control Systems Security Program (CSSP)

National Cyber Security Division (NCSD)



Homeland
Security

CSSP Education & Training Strategy

- Three Thrust Areas
 - Academic
 - Students & Professors engaged with CIP issues and careers
 - Across all relevant disciplines (engineering, computer science, public policy, management, etc)
 - Awareness
 - Industry Leaders, Managers, System Designers
 - Government Officials and Agencies
 - General Public
 - Operational
 - System Operators

CSSP Education & Training Strategy

Three Goals

1. Encourage and enhance teaching of control system security at the college and university level (inherently multi-disciplinary).
2. Promote general awareness, interest, and knowledge of the need for and means to achieve security in the control systems.
3. Enhance the availability and quality of operational control system security training.

1. Encourage and Enhance Teaching

- Support interested faculty for invited sabbaticals at National Laboratories with control system programs.
- Provide grants to faculty interested in teaching seminars/courses at universities and conferences.
- Provide scholarships to graduate students in programs related to cyber security of control systems.
- Provide internships to graduate students in programs related to cyber security of control systems.
- Support development of curricula related to security of control systems (and share that curricula freely).
- Other ideas?

2. Promote Awareness

Promote general awareness of the need for and means to achieve security in control systems (at both technical and leadership levels)

- General awareness of control systems security issues, measures and mitigations
- Training information on the use of control systems security tools, assessment approaches, and risk-based mitigation methodologies.
- Developing sector-specific training material based on sector security standards.
- Work with conference organizers to offer CSSP seminars.
- Faculty exchange with National Laboratories (provide speakers).
- Work with professional development vendors to offer CSSP seminars.
- Other ideas?

3. Operational Training

- Develop training for critical infrastructure protection which properly frames and elucidates control system issues.
- Incorporate policy and business/safety risk issues with technical concepts to provide a holistic understanding of security for control systems.
- Encourage the use of training packages by industry. Post them to website free of charge.
- Provide continued awareness and outreach efforts to operational community through attendance at and maintenance of information booths at relevant conferences and workshops.
- Support cyber security interns at National Laboratories that are engaged in control system security activities.
- Promote the establishment of fellowships and scholarships and assistantships from the vendors and principal critical infrastructure industries at the university level.
- Collaborate and develop strong partnerships with federal programs that promote cyber security in particular those that provide funding to education and training opportunities.
- Other ideas?

Targeted Outcomes

- Increased number of professionals engaged in cyber security of control systems within the critical infrastructure community.
- Increased awareness of control system security issues and solutions.
- Increased skills and skill development programs for operators of critical infrastructure control systems.
- Increased private sector partnerships.
- Develop the demand within the private sector for professionals with academic degrees and credentials in control system cyber security.
- Other ideas?

Example: Curriculum Development

- Target: Decision-makers Across Disciplines
- Expected Outcomes:
 - Understand basic concepts underlying the technical functions, vulnerabilities, and means of protection of control systems
 - Understand the drivers that lead to new and increasing levels of vulnerability
 - Be equipped to intelligently address policy development and decision making:
 - Industry: Advise leaders on relevant CIP issues, the value of control systems security, and practical strategies for doing so.
 - Government: Advise leaders on the relevant CIP issues and appropriate policies and programs to mitigate those issues.

Example Course Topics

- Critical infrastructures – What are they? Why critical?
 - Infrastructure facilities and services
 - Private vs public ownership
 - Criticality of services in times of disaster
 - Technical vulnerability examples (control system case studies)
 - Use of critical infrastructure as a weapon by terrorists
 - Interdependence (including shared control system vulnerabilities between sectors)
- Policy context:
 - Laws, Commissions, PDDs, role of DHS and other agencies
 - Role and structure of government (federal, state, city) in critical infrastructure security
 - Role of technical community – vendors, universities, national laboratories
 - Critical infrastructure as part of “all hazards” approach



Example Course Topics (cont.)

Technical problems and solutions

- Science and technology applied to reducing vulnerabilities
- Case studies
 - SCADA systems used in electric power industry
 - SCADA systems in chemical plants
 - Cyber threats and vulnerabilities; cyber attack as force multiplier
- Systems thinking and systems problems; testing and red-teaming

Managing high reliability organizations

- Experience from existing organizations
- Principals of management when facing terrorism, other disasters
- Business cases for investment in robustness and resilience

Creating a market for disaster preparedness investments

- Private risk management for terrorist attacks
- Role of insurance and re-insurance industries

Creating trust: information sharing, public-private partnerships

- Institutional proposals and solutions
- International issues
- Public-private collaboration – beyond regulation and subsidies



Very Interdisciplinary Team

- Engineering, Computer Science and Systems Analysis Departments
 - Control Systems critical to infrastructures
 - Underlying IT systems critical to all infrastructures
 - Systems Analysis Tools and Techniques
- Risk Management
 - Tools for vulnerability assessment and risk management
- Economics
 - Networked industries
 - Security externalities
- Business Analysis
 - Business Case Development
 - Insurance, reinsurance, and other options
- Management theory
 - Collaborative (public-private) governance
 - Managing robust and resilient industries



Project Leadership

Lewis Branscomb

- Harvard JFK School / University of California San Diego
- NSF, NIST, NAS, etc
- Author: *Making Our Nation Safer: the Role of Science and Technology in Countering Terrorism*

Philip Auerswald

- George Mason University
- Director, Center for Science & Technology Policy
- Editor: Book forthcoming this summer from Cambridge University Press focused on Critical Infrastructure Protection from multiple disciplines

Brian Lopez

- Lawrence Livermore National Laboratory
- Leader, Vulnerability & Risk Assessment Program (VRAP)
- Decade of experience leading vulnerability assessments against critical infrastructure, book forthcoming, lectured on vulnerability assessment and critical infrastructure issues at UC-Berkeley, Univ. of Washington, Microsoft.



Schedule - Distribution - Contact

Schedule

- Draft of the Curriculum: End of Summer
- Final Version: Christmas

Distribution

- Entire curriculum including reading lists and all supporting materials will be freely available and distributed via web site.

Contact

- Brian Lopez
 - Email: blopez@lhn.gov
 - Phone: 925 422 5839

