Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency

Ron Trellue, Project Lead
Process Control Systems Forum
June 7, 2006

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.
Project Summary

This project was funded by the I3P starting in March 2005

The project is a 24-month, $8.5M effort by an 11 institution research and engineering team

Stakeholders are industry, government, and research community

Information and publications can be found at www.thei3p.org
Approach

- Assemble a research team of nationally recognized experts in cyber security and PCS security
- Build on the strengths of the team researchers to address six specific PCS security problems
- Focus on the oil and gas sector by partnering with industry – primarily the refinery and pipeline segments
- Develop tools and technology which could enhance the robustness of critical interdependent infrastructure process control systems
- Communicate and demonstrate results of the research
- Influence owner/operators/vendors and policy decision makers to increase PCS security robustness
Project Team Members - 50 total

- Dartmouth College – George Cybenko
- Institute for Information Infrastructure Protection (I3P) – Pat Erwin
- MIT/Lincoln Laboratory – Rob Cunningham
- MITRE – Michelle Gosselin
- New York University – Rae Zimmerman
- Pacific Northwest National Laboratory (PNNL) – Martin Stoddard
- Sandia National Laboratories (SNL) – Ben Cook
- SRI International – Ulf Lindqvist
- University of Illinois Urbana/Champaign (UIUC) – Bill Sanders
- University of Tulsa – Sujeet Shenoi
- University of Virginia – Yacov Haimes
Research Approach

Understand vulnerabilities, characterize the risk, analyze the consequences of disruption (Teams 1 and 2)

Understand and develop metrics that can be used to measure improvement (Team 3)

Research technical solutions (Teams 4 and 5)

Work with customers to transfer the knowledge gained and technology developed (Team 6 with the support of the other 5 teams)
Project Organization

Research Teams

Team 1
Risk Characterization
SNL

Team 2
Interdependencies
UVa

Team 3
Metrics
PNNL

Team 4
Security Tools
MIT/LL

Team 5
Information Sharing
MITRE

Team 6
Tech Transfer
SRI

Oil and Gas Industry
Requirements, Information
Workshops, Demonstrations
Technology Transfer
2nd Industry Workshop
June 8, 2006

- Focused on presentation and demonstration of research results in action-ready format

Understanding The Problems
- Vulnerabilities
- Metrics
- Interdependencies
- Risk Analysis

Understanding The Solutions
- Secure Design
- Security Monitoring
- Information Sharing
- Future Trends

- We will collect stakeholder feedback
Project has six goals
1. Increase awareness of Process Control System security risks
1. Increase awareness of Process Control System security risks

- Host industry/government workshops
  - Kickoff at Houston workshop June 2005
  - Metrics workshop in Washington State November 2005
  - Presentations and demonstrations workshop in La Jolla coming up June 8, 2006
  - Planning for at least one more at the end of year 2
- Present at PCS related conferences
  - (PCSF, NPRA, ISA, Infragard, EISAC, KEMA,…)
- Conduct site visits for in depth industry interaction
  - (Ergon, CITGO, Williams, Chevron, Symantec, …)
1. Increase awareness of Process Control System security risks

- Publications – can be found at www.thei3p.org
  - Process Control Systems Security Metrics – State of Practice – I3P Report # 1
  - National Cyber Infrastructure Bulletin no. 1, published by I3P
  - Requirements for Cross Domain Information Sharing Within SCADA Environments – I3P Report #4
  - Houston Workshop Risk Characterization Analysis Report (draft)
  - “Architecture for SCADA Network Forensics” – Tulsa
  - “Securing Control Systems in the Oil and Gas Infrastructures” – SRI (Oil and Gas Processing Review, Dec 2005)
2. Develop programs to educate students and stakeholders on PCS security
2. Develop programs to educate students and stakeholders on PCS security

- PCS Security Awareness taught at Sandia in April 2005 with industry guests
- PCS Security Class being taught at the University of Tulsa this Spring
- PCS sessions taught at CMI and soon at NYU
- Developing a new PCS security seminar specifically for the gas and oil sector
- Students from project’s institutions are graduating with expertise in PCS security
3. Recommend mitigation strategies for operators and policymakers
3. Recommend mitigation strategies for operators and policymakers

- “Best Practices” for the Oil and Gas Sector book is being written for ISA
- RiskMAP tool for decision makers business case
- Interdependencies models being developed to:
  - Construct realistic cyber-intrusion scenarios
  - Map specific cyber attacks into corresponding likely product disruption magnitude and duration
  - Map likely product disruption to commodity distribution network and economic impacts (both direct and indirect)
    - On a regional and interregional basis
    - Accounting for dynamics of recoveries from attacks
  - Conduct key cost-risk-benefit tradeoff analyses in risk management, addressing both direct and indirect impacts, to achieve enhanced system protection and resilience
3. Recommend mitigation strategies for operators and policymakers

- **Publications**
  - Trends for Oil and Gas Terrorist Attacks – NYU - I3P Report # 2
  - “Application of the Inoperability Input-Output Model for Systematic Risk Assessment of Interdependent Infrastructures” - UVa
  - “The next step: quantifying infrastructure interdependencies to improve security” - NYU
4. Develop and prototype technology and tools for PCS security
4. Develop and prototype technology and tools for PCS security

The following tools are under development and prototype testing:

- DEADBOLT – source code checking
- HSMTU – highly secure master terminal unit
- SecSS – Security Services Suite
- RiskMap – build business case for security
- APT – Access Policy Tool
- EMERALD – intrusion detection and correlation
- CDIS prototype – information sharing
5. Advance basic research in inherently secure PCS security
5. Advance basic research in inherently secure PCS security

Key research areas are:

- Developing infrastructure interdependency models that include PCS
- Developing cost/risk/benefit models
- Developing inherently secure design tools
- Developing cross domain solutions
6. Gain national recognition as a leading center of research, knowledge, and expertise in PCS security
6. Gain national recognition as a leading center of research, knowledge, and expertise in PCS security

- Team has been invited to present at many PCS related conferences including PCSF
- Work is recognized in DOE funded Energy Sector Roadmap
- Efforts being coordinated with other DHS and DOE programs
- I3P has established a PCS Knowledge Base and Digital Library
Results and next steps

- January mid-year Program Review resulted in approved year 2 funding – review by I3P Executive Committee, DHS PM, and industry panel

- February “reboot” meeting realigned tasks with a more stakeholder/industry focus

- Communications Plan and Marketing Plan under development to organize outreach communications and tech transfer

- June 8 Workshop will be a showcase for demonstrating some of the technology and getting feedback from the stakeholder community
Project Success

- Demonstrated improved cyber security in the Oil & Gas infrastructure sector
  - New research findings
  - New technologies
- Significantly increased awareness of
  - Security challenges and solutions
  - The capabilities of the I3P and its members