



Institute for
Information
Infrastructure
Protection

www.thei3p.org/

PROCESS CONTROL SYSTEMS SECURITY RESEARCH PROJECT

Developing Security Solutions for the Oil and Gas Sector

PROGRESS SUMMARY FEBRUARY 2007

The Process Control Systems (PCS) Security Research Project is focused on improving the robustness of the information infrastructure in the oil and gas sector. Phase I of the project began in March of 2005 and concluded in February 2007. This fact sheet summarizes the status and availability of the project's major tools and products.

OUTREACH

The I3P has hosted three security workshops to engage oil and gas infrastructure owners, operators, vendors, and the research team. The final workshop was held February 15-16, 2007 in Houston. Workshop presentations can be requested from the I3P. The team has also presented project results at over twenty process control systems related conferences, and they have participated in numerous site visits for in-depth industry interaction. The team has published a substantial number of journal articles, technical reports, and conference papers, many of which are available at the I3P web site. PCS security classes have been developed and are being taught at several of the participating universities such as the University of Tulsa.

Contact: Eric Goetz, I3P, research@thei3p.org, (603) 646-0692

I3P PCS Project Web Site: <http://www.thei3p.org/projects/pcs.html>

RISK CHARACTERIZATION

An I3P technical report on characterizing risk in oil and gas process control systems was published along with a related article in the Oil and Gas Journal. A one-day security training course was developed and given at the February 2007 workshop. This course could be offered again upon request.

Contact: Annie McIntyre, Sandia National Laboratories, amcinty@sandia.gov, (505) 284-0968 or Jason Stamp, jestamp@sandia.gov, (505) 284-6797

I3P report on PCS risks: <http://www.thei3p.org/repository/researchreport6.pdf>

SITUATIONAL AWARENESS/BUSINESS CASE TOOLS AND SERVICES

RiskMAP, the proven Risk-to-Mission Assessment Process, provides decision support information tailored to company needs. RiskMAP translates between the technical terms of network risk and the business terms of corporate risk so that all can understand and decide on risk mitigation strategies. Negotiations are underway to transfer the product to a commercial company.

Contact: Peter Kertzner, MITRE Corporation, kertzner@mitre.org, (781) 271-2286

Interdependency models have been developed to assess the economic consequences of cyber disruption in the oil and gas sector at the facility, regional, and national scale. Publications are available on the I3P website describing the results of the analysis from the models.

Contact: Yacov Haimes, University of Virginia, haimes@virginia.edu, (434) 924-3803

METRICS

Two prototype security metrics tools have been developed and are available for beta-testing. One is based on the *DOE 21 Steps for Improving Cyber Security of SCADA Networks* and it provides a security metrics dashboard for assessing the status of security efforts. The other, P-STET, evaluates and compares the costs and benefits of new security products. In addition, three reports are being produced focusing on the state of practice, requirements, and available tools for PCS security

metrics. Information on all of these products is available on the I3P website (www.thei3p.org).

Contact: Cliff Glantz, Pacific Northwest National Laboratory, cliff.glantz@pnl.gov, (509) 375-2166

SECURE DESIGN TOOLS

DEADBOLT is an effective, scalable and practical automated testing framework that facilitates the discovery of buffer overflows in C and C++ software before deployment. A prototype version is being tested at a PCS vendor's site and plans are underway to make the software available.

Contact: Michael Zhivich, MIT/Lincoln Laboratory, mzhivich@ll.mit.edu, (781) 981-4761

SecSS. The Security Services Suite is intended to serve as a technical solution for securing communications networks used in industrial control systems with five approaches: message monitoring, protocol-based solutions, tunneling services, middleware components, and key management. The tools are being demonstrated to potential customers and vendors in hopes of finding a partner to help make the tools more readily available.

Contact: Mauricio Papa, University of Tulsa, Mauricio-papa@utulsa.edu, (918) 631-2987

SHARP. The Security-Hardened Attack Resistant Platform (SHARP) provides an infrastructure independent, high-security environment for networked process control systems. SHARP is intended to be a drop-in component that can work with existing process control systems. SHARP limits access to sensitive data, decreases the likelihood of a successful attack, and reduces interruptions to operations even if an attack succeeds. Licensing opportunities will soon be available.

Contact: Ron Pawlowski, Pacific Northwest National Laboratory, ron.pawlowski@pnl.gov, (509) 372-4116

APT. The Access Policy Tool assesses a system of firewalls and their rule-sets and host policy enforcement mechanisms to determine whether the rule-sets accurately implements the desired policy. APT can be run offline or online. A prototype version is available today for customer evaluation. Testing is currently in progress at a vendor site and discussion is underway for commercializing the tool.

Contact: David Nicol, University of Illinois Champaign/Urbana, nicol@crhc.uiuc.edu, (217) 244-1925

Emerald. Emerald is a system for intrusion detection and alert correlation that has been adapted from enterprise systems for use in control systems. Emerald itself is available today from SRI. Emerald's correlation and alert systems takes input from several of the other tools developed by this project.

Contact: Al Valdes, SRI International, valdes@csl.sri.com, (650) 859-4976

SECURE INFORMATION SHARING

Cross Domain Information Sharing (CDIS). Cross Domain Information Sharing is a proof-of-concept capability for analyzing PCS incident data. The team has developed a working prototype that illustrates PCS incident reporting and statistical and trend analyses.

Contact: Chris Eliopoulos, MITRE Corporation, celiopou@mitre.org, (781) 271-3625

Anonymous Authentication Technology. This technology is being used as a component of the CDIS prototype. Sandia hopes to make a software package available (likely for no cost) to entities involved in information sharing seeking additional anonymity protection. The underlying cryptographic protocol is patent pending.

Contact: Tim Draelos, Sandia National Laboratories, tjdrael@sandia.gov, (505) 844-8698

Information about the project may be found at
<http://www.thei3p.org/projects/pcs.html>

I3P Publications may be found at
<http://www.thei3p.org/publications>

Points of Contact:

Project Director: John Cummings,
jccummi@sandia.gov (505) 845-9937

Project Leader: Ben Cook,
bkcook@sandia.gov (505) 844-3795

I3P Assistant Director for Research & Analysis :
Eric Goetz, egoetz@thei3p.org (603) 646-0692

This work was produced under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College, and 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 [site and documents] are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security, the Science and Technology Directorate, the I3P, or Dartmouth College.