

Agenda

5th Annual I3P Process Control Systems Security Workshop

The Future of PCS Security: Where Are We Going and How Do We Get There?

8:00	Registration and Continental Breakfast	<i>Room 335 B</i>
8:30	Welcome Robert K. Cunningham, MIT Lincoln Laboratory and Team Leader	<i>Room 335 A</i>
8:40	Keynote: The Wrath of Mother Nature: Implications for Cyber Security David Batz, Cyber Security Risk Manager for Alliant Energy Security & Facility Services Catastrophic flooding that swept the Midwest in June 2008 disrupted operations at a large electric utility. The cause may have been environmental, but the consequences were comparable to a major cyber attack. What were the lessons learned about recovery and restoration of an affected electric utility? And how do those lessons translate to cyber security?	<i>Room 335 A</i>
9:20	PCS Security: Progress on the Horizon Robert K. Cunningham, MIT Lincoln Laboratory There is a growing understanding of how to secure PCS—the NERC Critical Infrastructure Protection standards and the recent release of the API 1164 2.0 standard show this, but challenges remain. The I3P has developed and commercialized some of the first tools to address the remaining challenges. In this brief introduction, you'll learn what others have found challenging, how some tools can address these challenges, and questions you should be asking about your business, your network, and your vendors' equipment.	<i>Room 335 A</i>
9:35	PCS (and Corporate) Risk: It's Not Just about Availability Jim Watters, MITRE Corporation Confidentiality, Integrity and Availability concerns can vary within a plant, affecting corporate risks. Learn how the Risk-to-Mission Assessment Process (RiskMAP) handles all three concerns as it translates between the techno-speak of PCS network risk assessments and the corporate language of business risks.	<i>Room 335 A</i>
9:50	Software Errors: Critical Oversights in Critical Infrastructure Protection Michael Zhivich, MIT Lincoln Laboratory Critical infrastructure operators depend on SCADA and process control systems to deliver accurate, real-time data for analysis and to relay control requests promptly. Errors in the software that runs these systems can result in transmission of stale or incorrect data, or in the loss or modification of control requests. Such failures impede the operator's ability to assess the state of the system and to control it reliably. Finding and eliminating errors in software therefore plays an essential role in ensuring that PCS operations remain robust and secure. At this session, you will learn about DEADBOLT, an I3P tool that improves PCS vendors' ability to discover and address software errors before deployment.	<i>Room 335 A</i>
10:05	Break	

10:20	<p>Location-Based Access Control of PCS Operators Sam Clements, Pacific Northwest National Laboratory</p> <p>Access control is a key challenge in process control system security. Non-obtrusive Authentication of Critical Infrastructure Operators (NACIO) utilizes commercially available technologies to provide operator authentication without impacting operational constraints. Learn how to detect an insider issuing unapproved commands, how to identify the issuer of a critical command, retain an audit trail of such commands, and detect unapproved remote access to critical workstations.</p>	<i>Room 335 A</i>
10:35	<p>Best Practices in Firewall Configuration: Checking for Compliance David Nicol, University of Illinois</p> <p>Studies show that firewall misconfiguration is common, permitting traffic that was not intended or expected. Learn about Access Policy Tool (APT), which utilizes configuration best-practice recommendations from NIST (and others) to check against the rules that govern traffic in a control system. APT was developed to meet the needs of a stakeholder whose PCS system involves over 50 firewalls.</p>	<i>Room 335 A</i>
10:50	<p>Monitoring PCS Networks: a Sound Strategy for Enabling and Maintaining Security Mauricio Papa, University of Tulsa</p> <p>Interconnectivity between business and process control networks exposes control systems to serious attacks. Learn about a distributed monitoring architecture (SecSS) for control protocols that offers a successful counter-strategy to such attacks. The architecture employs a distributed network of sensors that relay field protocol data to a central database, and is scalable and distributable. The tool, which currently supports the Modbus and ROC protocols, is capable of building communication profiles and uses a graphical interface to notify operators of various abnormal events that might indicate malicious activity.</p>	<i>Room 335 A</i>
11:05	<p>Motivated Adversaries: What Operators Need to Know Bryan Richardson, Sandia National Laboratory</p> <p>Motivated adversaries, like skilled chess players, watch how their opponents react before making the next move. They understand their opponent's control system and the key processes it controls. As a critical element of defense against a cyber attack, operators need to understand not only how such adversaries work, but also how to troubleshoot and respond to such attacks with minimal operational impact. The Operator Response Training Simulator (OPSIM) helps operators develop an instinctive response to a disruption so that a cyber adversary can be quickly identified and a response plan initiated.</p>	<i>Room 335 A</i>
11:20	<p>Technology Demonstrations:</p> <ul style="list-style-type: none"> • RiskMAP. Talk over the importance of considering not just Availability and Integrity, but also Confidentiality when it comes to protecting your PCS network. • DEADBOLT. Learn how resource exhaustion and memory corruption errors in process control software can affect operations and what DEADBOLT can do to help software vendors find and address such errors before deployment. • NACIO. See how this system uses non-obtrusive methods to authenticate users issuing critical commands on control center workstations based on proximity and network traffic. This implementation is transparent to the user and requires no modification to the existing workstation configuration. See how this system helps meet regulatory requirements without affecting operational requirements. 	<i>Room 335 C</i>

11:20	Technology Demonstrations (Cont.): <ul style="list-style-type: none"> • APT. Using a network topology that is inspired by our work with industrial partners, step through various visual components of APT: network visualization, inspection of policy rules and global access policies, reporting of access paths that violate the policy. Find the rules that contribute most to non-compliance, and experiment with changes that fix the problems. • SecSS. See how sensors can monitor a PCS network and report back to a central location. The main components of the architecture are on display, including the actual output produced by the remote sensors as well as a front-end GUI that shows status and topology information in real-time. • OPSIM. Understand, with the help of this operator-response training simulator, how motivated adversaries approach an attack, from design to execution, and how they can use troubleshooting heuristics to their advantage. Learn how to respond to an attack with minimal operational impact. 	<i>Room 335 C</i>
12:30	Lunch Technology demonstrations will continue in Room 335 C.	<i>Room 335 B</i>
1:15	Today's Technology Launching Tomorrow's Solutions Greg Vaughn, President of Entelec Greg Vaughn, president of ENTELEC, will briefly discuss the role of ENTELEC's members and conference attendees in helping industry develop "tomorrow's solutions today."	<i>Room 335 A</i>
1:30	The Future of PCS Security: Technological Challenges Ron Trelue, Trelue Consulting What are the big unsolved PCS security problems? How can the I3P research team best work towards finding solutions? Analysis of security needs expressed by the community has led the team to focus on five top areas for further research.	<i>Room 335 A</i>
1:45	The Future of PCS Security: Technological Prospects Moderated by I3P PCS Advisory Board Members This will be a one-hour breakout session, with five tables, each devoted to a prospective R&D path. <ul style="list-style-type: none"> • Trustworthy Communication: How can we ensure reliable communication with physically insecure components? Can we improve security assurances through hardware-based techniques? <i>Moderators: Apu Kapadia, MIT/LL, team lead and Bob Huba, Advisory Board</i> <i>Room 335 A</i> • Actionable Security Metrics: Can we identify the key security goals and develop "actionable metrics"? <i>Moderators: David Nicol, UIUC, team lead and Charles Palmer, I3P Chair</i> <i>Room 335 B</i> • PCS Simulation and Emulation: Does the tight interplay between the human, physical, and cyber aspects of these systems compound the complexity of defending them? Can simulation close the gap? <i>Moderators: Bryan Richardson, Sandia, team lead and Steve Elwart, Advisory Board</i> <i>Room 335 B</i> 	

1:45	<p>The Future of PCS Security: Technological Prospects (Cont.)</p> <p>Moderated by I3P PCS Advisory Board Members</p> <ul style="list-style-type: none"> Digital Forensic Tools: When something goes wrong with your PCS, what are the key things to investigate? Do you have all the information you need? Can tools help? <i>Moderators: Mauricio Papa, University of Tulsa, team lead, and Scott Crane, Advisory Board Room 335 B</i> Cyber Security Standards: What has been added to API 1164 and SP99? What is being done and what should be done in the future for standards? <i>Moderators: Morgan Henrie and Eric Cosman, Advisory Board Room 335 C</i>
2:45	<p>The Future of PCS Security: National R&D Priorities <i>Room 335 A</i></p> <p>Robert K. Cunningham, MIT Lincoln Laboratory</p> <p>In October 2008, the I3P convened a Forum to address the cyber security challenges facing process control systems and the nation's cyber physical infrastructure. US Senators Joseph Lieberman and Susan Collins, Chair and Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs served as honorary co-chairs of the event. Results from that session, which brought experts from industry, government and academia together are presented by the Forum's moderator and placed in the context of other important government efforts.</p>
3:15	<p>Discussion: How Do We Get There? <i>Room 335 A</i></p> <p>Ulf Lindqvist, SRI</p> <p>Drawing on the topics and information discussed during the breakout sessions, participants will examine technological prospects for the future as well as immediate security needs on the control side. What are the greatest security challenges? Is there a best path forward? How should the various technological prospects be prioritized?</p>
4:30	<p>Wrap Up: What Next? <i>Room 335 A</i></p> <p>Robert K. Cunningham, MIT Lincoln Laboratory</p>
5:00	<p>Adjourn <i>Room 335 A</i></p>
6:00	<p>ENTELEC Welcome Reception <i>Room 339 A/B</i></p>