

PCSRF Conference Call Meeting Notes

Friday, February 11, 2005 1:30 PM – 3:00 PM EST

Hosted by National Institute of Standards and Technology

Participants

Peter Sargent, PreVal Specialist, Inc.
Dale Peterson, DigitalBond
David Thompson, Ashton Security Laboratories, LLC
Coleman, Clayton, Invensys
Tom Kropp, EPRI
Tom Good, DuPont
Tom White, Honeywell
Paul Blomgren, Mykotronx
Joe Steller, NIBS
Bill Miller, MaCT
Patrick Miller, PacifiCorp
Donna Post Guillen, INL
AJ Price, Georgia Pacific
Martin Delson, KEMA
Holly Beum, Interface-Technologies
Tim Shaw, SWANTECH
Richard Combs, Premcor
Jeff Mantong, Western Area Power Administration
Benjamin Church, Burns & McDonnell
Kyle Danilson, Securenetrics
Jon Saito, Seattle Public Utilities
Wei Huang, Florida Atlantic University
Andrew Hildick-Smith, Massachusetts Water Resources Authority
Rhodenizer Elizabeth, Public Safety and Emergency Preparedness Canada (PSEPC)
Betty Pierce, Secure Network Systems
Martin Naedele, ABB
John Reinkens, Lakehaven Utility District
Em delaHostria, Rockwell
Tom Phinney, Honeywell
Charles Hoover, Rockwell
Dave Teumim, Teumim Technical
Martha Sproul, Westinghouse Savannah River Company
David Saunders
Kevin Staggs, Honeywell
Mary S. Hester, Intelligent System Solutions
Bob Timpany, INL
Ron Sielinski, Microsoft
Dennis Holstein, OPUS Publishing
Joe Weiss, KEMA
Ernie Rakaczky, Invensys
Tom Donahoe, Areva
Joe Falco, NIST
Keith Stouffer, NIST

Agenda

The main objectives of the conference call were to discuss PCSRF objectives for the year, review activities in industrial controls security, review news and status, and determine the date and location of the next face-to-face meeting.

Objective - Develop a SCADA Protection Profile

A plan was proposed to focus the PCSRF effort on the development of a SCADA Protection Profile. The experiences learned in the development of the SPP-ICS will be applied as much as possible to the development of a SCADA PP.

In the development of the SCADA PP, the security requirements defined by the group would be organized into sections that can be met by specific functions which may then be mapped to specific components and/or vendors. This will allow vendors to concentrate on the requirements that they can meet and develop a product for, rather than trying to decipher the big picture and determine what requirements that they can address. This could provide a path for quicker vendor adoption and backing of the effort.

There are several PPs that currently exist that we may be able to reference for certain components in the SCADA PP. These PPs include switches and routers, wireless, firewalls, remote access, access control, operating systems and intrusion detection systems. These PPs will have to be examined to determine their relevance to this effort. Many of these PPs are available on the IATFF website: http://www.iatf.net/protection_profiles/

The goal of this plan would be to organize the security requirements that PCSRF defines around the components that could meet the requirements, not to write requirements around existing products. The goal of PCSRF is and has always been to move industry in a direction of better security by defining security requirements for new industrial control systems.

From the previous meeting, there was discussion as to what systems will be addressed since SCADA has different meanings in different industries. It was suggested that it may be more beneficial to address systems where SCADA refers to geographically distributed systems such as Water, Oil, Gas, Transportation (Railroads). The Electric industry has a different definition of what a SCADA systems is and seems to have more of a focused group addressing the issues. Keith Stouffer (NIST) asked Joe Weiss (KEMA) to clarify the significant properties of a typical Electric SCADA system.

Joe Weiss stated that SCADA has moved from being a Substation controller to a hybrid “mainframe.” What used to be SCADA is now an RTU/IED. Now SCADA is a higher level of control bringing other things together. Communications are heading towards Ethernet-IP although all the protocols are being used. Also, the power plant DCS talks to the SCADA system.

It was suggested and agreed that we create a specific work group to develop the SCADA PP. A small working group of experts would be the most productive approach to this effort and progress will be reported back to the overall PCSRF for review and comment. This group will develop the detailed functional and assurance requirements for a SCADA System Protection Profile, therefore knowledge with SCADA systems is nearly a necessity and knowledge with the Common Criteria is preferred. Please volunteer for this effort by emailing Keith Stouffer (keith.stouffer@nist.gov) by Friday February 25, 2005. The kick-off meeting (conference call) for this working group will be in early March.

Joe Weiss asked how these efforts are related to the standard currently being developed by ISA-SP99. Keith responded that Part 4 of the ISA-SP99 standard focuses on Specific Requirements for Manufacturing and Control Systems. Keith has been working with Bryan Singer (ISA-SP99 Chair) and there is agreement that the specific security requirements that PCSRF develops will feed into Part 4 of the standard. Part 4 of the standard is scheduled to start development in 2006.

Keith also mentioned that a few PCSRF members that have been developing component level Protection Profiles. Dale Peterson previously developed a Control Center PP and there are others including Protection Profiles for an HMI Sever and HMI Client that will be presented for review and comments at the next PCSRF face-to-face meeting.

Activities in Industrial Controls Security

Security Configurations for Windows Systems

SANS is interested in working with the PCSRF members to develop security configurations for Windows systems used in the industrial control system domain. There is some activity underway between SANS and Idaho National Laboratory (INL) in this area. Keith has forwarded this information to PCSRF members that previously expressed interest in participating in this activity. If anyone else is interested in participating in the activity, the contact at SANS is Alan Paller and he can be contacted at AlanPaller@aol.com

INL and SANS have discussed a "Birds Of a Feather" session at upcoming SANS conferences. INL/SANS request feedback from PCSRF members on whether they, or their organizations, would participate. POC Bob Timpany, 208 526-6334 Robert.Timpany@inl.gov

INL and SANS have initially discussed co-developing SCADA/PCS courses for the SANS curriculum. POC Bob Timpany, 208 526-6334 Robert.Timpany@inl.gov

DHS's Control System Security Test Center (CSSTC), an effort involving multiple National Labs, will pursue further contact with SANS in reference to develop security configurations for Windows systems used in the industrial control system domain. POC for CSSTC, Bob Timpany, 208 526-6334 Robert.Timpany@inl.gov

Process Control Systems Forum (PCSF)

The Department of Homeland Security has established a Process Control Systems Forum (PCSF). The PCSF is a unified effort between the National Cyber Security Division and Science & Technology to form a natural bridge between Government and Industry.

The purpose of the Process Control Systems Forum is to accelerate the development of technology that will enhance the security, safety and reliability of process control and SCADA systems by providing a single venue for technologists from all user sectors, from all vendors, and from academia to work together in evaluating, specifying, developing, refining and testing new technologies.

The PCSF is an open, collaborative, voluntary forum that will leverage the experience and capabilities of stakeholders in the development and adoption of common architectures, protocols, and practices for next generation control systems. Innovations developed by the forum will guide requirement gathering, testing, retro-fit, development, and deployment strategies. The PCSF will leverage knowledge currently dispersed among sectors, and stimulate cross-functional discussions between Information Technology (IT) and Operations to strengthen communication and resolve issues inherent within their respective disciplines.

The PCSF is not a standards body and is not intended to replace any existing activities in the PCS and SCADA community. The PCSF will build upon the existing body of work in this subject area, and establish links with others in industry and government to arrive at a common underlying architecture for process control systems that offers security, reliability, resiliency, and continuity in the face of disruptions and major incidents.

The public kick-off meeting for the PCSF is May 17-18 in Dallas TX. For those that have additional questions on the PCSF, the contact at the DHS is Peter Miller (Peter.Miller@dhs.gov)

Keith Stouffer is on the Governing Body of the Forum to provide guidance on the issues to be addressed in the Forum and the strategy and direction of the Forum. Additional information on the PCSF is available at <http://www.pcsforum.org>.

News and Status

Bill Miller (MaCT) mentioned that he has set up Microsoft SharePoint to aid in collaboration among the PCSRF members. Currently there is a PCSRF SharePoint that also has pointer to useful sites such as Common Criteria, NIST, NSA, and Microsoft. Those interested in joining it can contact Bill at mact-usa@att.net The URL for the SharePoint is: <http://mactsp.wss.bcentral.com/PCSRF> Bill also said that a Share Point could also be created for the members of the SCADA PP working group once it is formed.

Bill Miller has also started an effort to develop 2 Protection Profiles for an HMI Server and HMI Client. The TOEs are written understandable English. Additional information on these PPs will be provided at the next face-to-face meeting.

Joe Weiss stated that the Technology Solutions for Security of SCADA and Process Control Systems KEMA conference will be held in Albuquerque, NM on August 22-24, 2005. Following this meeting on the August 25-26, there will be an International Standards Coordination meeting to address international control systems cyber security standards.

Bob Timpany (INL) gave an overview of efforts at the Idaho National Laboratory. They are addressing physical and cyber security using the Control Systems Security Test Center, a multi-lab cooperative effort between the National Labs. They are addressing test methods for SCADA and DCS components and are working with the PCSRF System Protection Profile for Industrial Control Systems (SPP-ICS) to develop a DHS Framework for control system security. They are also developing English level equivalents on the SPP-ICS for vendor use.

Direction and next steps

It was agreed upon to create a work group to develop the SCADA Protection Profile. This group will develop the detailed functional and assurance security requirements for SCADA systems, therefore knowledge with SCADA systems is nearly a necessity and knowledge with the Common Criteria is preferred. If you would like to participate in this work group, please contact Keith Stouffer (keith.stouffer@nist.gov) by Friday February 25, 2005. The kick-off meeting (conference call) for this working group will be in early March.

Next Face-to-Face Meeting

The next face-to-face meeting will be held on May 19, 2005 in Dallas, TX. This is the day following the DHS Process Control Systems Forum kickoff meeting. Specific information on the hotel will be sent to the group once the hotel has been confirmed for the PCSF meeting.

Action Items

Keith Stouffer will compile and distribute the meeting minutes by February 18, 2005

Joe Weiss will send Keith info on the KEMA workshop and standards meeting so that they can be put in the minutes

Keith Stouffer will send info to the group once the hotel has been confirmed for the PCSF meeting.