

## **PCSRF Conference Call Meeting Notes**

**Tuesday, September 7, 2004 1:30 PM – 3:00 PM EDT  
Hosted by National Institute of Standards and Technology**

### **Participants**

Marty Robbins, Georgia Pacific  
Joseph D. Steller, American Lifelines Alliance, National Institute of Building Sciences  
Jim White, WiredCity  
Ted Ripp, BP  
Charles Hoover, Rockwell  
Tony Haynes, NCMS  
Al Cooley, Verano  
Dave Teumim, Teumim Technical, LLC  
Stan Scown, INEEL  
Geoff French, General Dynamics  
Tim Shaw, Cyber SECURITY Consulting  
Ernest Rakaczky, Invensys  
Perry Pederson, TSWG  
Martin Naedele, ABB  
Murray Donaldson, Decisive Analytics  
Bill Miller, MaCT  
Tom Phinney, Honeywell  
David Saunders  
Dale Peterson, DigitalBond  
Robert O'Brien, Secure Controllers LLC  
Tom Good, DuPont  
Dan Hoffman, University of Victoria  
Paul Short  
Art Wilson, Tresys Technology  
Mike Hale, Tresys Technology  
Joe Weiss, KEMA  
Holly Beum, Interface-Technologies  
Bill Rush, GTI  
Kevin Staggs, Honeywell  
Dick Oyen, ABB  
Keith Stouffer, NIST

### **Purpose**

The main objective for the meeting was to discuss a plan to move the PCSRF effort forward, share news and status updates and determine the date and location of the next face-to-face meeting.

### **Agenda**

- Discuss plan for SCADA Protection Profile
- Direction and next steps
- News and status updates

## Opening Remarks

Keith Stouffer (NIST) started off the meeting and stated that the main topic for this conference call was to discuss a plan to move the PCSRF effort forward, review status, and determine the date and location of the next face-to-face meeting.

To help answer the question "What does/doesn't a Common Criteria evaluation mean?" a link to a document that Stu Katzke (NIST) wrote is included below. This document has not been published and is not an official NIST position, but rather this "Truth in Evaluation" Statement is intended to help consumers understand the meaning of a CC evaluation and the resultant CC certificate issued for a vendor's product. CC certificates are issued by the NIST and NSA or by equivalent government organizations participating in the Common Criteria Recognition Arrangement (CCRA).

[http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/7-Sep-2004/CC\\_evaluation.doc](http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/7-Sep-2004/CC_evaluation.doc)

## Proposed Plan – Develop a SCADA Protection Profile

Keith Stouffer proposed a plan 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 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/](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.

## SCADA Protection Profile Discussion

Bill Miller (MaCT) suggested that the HMI be one of the components that we develop a PP for. There are several existing PPs for components that make up an HMI, such as Database and OS PPs, that could possibly be leveraged.

Tim Shaw (Cyber SECURITY Consulting) asked which components would be addressed and that is the Database PP is relevant since he thought it was develop for Federal databases.

Murray Donaldson (Decisive Analytics) added that the Database PP should be able to address any database including Federal and non-Federal.

Tom Phinney (Honeywell) added that most databases used in control systems are not relational databases.

Tim Shaw noted that a possible way to address several components at once is to form committees that are interested on defining the requirements for each component. This would be a good idea if we can get enough people to volunteer their time to the effort. This will be discussed further at the next meeting.

Holly Beum (Interface-Technologies) added that it will be very important to get concise definitions as to what each component of the system is and what its interfaces are. KS – If the proposed plan is accepted, clearly defining the components and interfaces of the system will be paramount to its success.

Tom Good (DuPont) added that it would not be a good idea to write PPs to get existing products certified, but to move in a direction of better security. KS - This is a very important issue and one that is core to this group and effort. The goal of PCSRF is to move industry in a direction of better security by defining specific security requirements for new industrial control systems.

Dale Peterson (DigitalBond) added that the Control System PP that he has been working on could also be good candidate for the group to address. The Draft Control Center PP can be reviewed here [http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/Control\\_Center\\_PP.pdf](http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/Control_Center_PP.pdf)

Tom Phinney (Honeywell) mentioned that they have a new product that uses a DMZ to separate the process control network. Honeywell will make information on this product available within the next few weeks. Kevin Skaggs (Honeywell) also mentioned the use of shadow servers in their upcoming product.

Joe Weiss (KEMA) expressed concern over using the term SCADA since the term can mean different things in different industries. This is something that will need to be addressed in the next meeting.

## **Direction and next steps**

The proposed plan to develop a SCADA PP, organizing the security requirements defined by the group into sections that can be met by specific components and/or vendors, will be reviewed by the PCSRF and is open for comment. Comments will be accepted until September 24, 2004. All comments on the proposed plan will be collected and made available to the PCSRF group. If you would like to provide a comment on the proposed plan and do NOT want your comments shared, you must make note of this in your response. Please direct all comments to Keith Stouffer [keith.stouffer@nist.gov](mailto:keith.stouffer@nist.gov)

The comments collected on the proposed plan will be sent to the PCSRF group the week of September 27, 2004 and a conference call will be held during the week of October 11, 2004 to review the comments and make a decision on the proposed plan.

## **News and status updates**

Joe Weiss provided some information on the KEMA conference that was held at INEEL. The INEEL staff demonstrated two control system attack scenarios. The first was an attack from a PC located locally by a person with cyber security, but not control system knowledge. The second attack utilized a recently identified system vulnerability to attack a typical substation SCADA system. The second attack was initiated remotely by Sandia National Laboratory (SNL) personnel from Albuquerque. The remote computer was connected to the local corporate LAN via a VPN connection. The attack was directed at a simulated, mocked-up substation SCADA system at INEEL in Idaho Falls (approximately 800 miles away). The exploit was sent through the VPN connection between the corporate LAN and SCADA LAN, and then through the firewall protecting the substation SCADA. The attackers were able to perform the following functions:

- Open a breaker at the substation
- Open and close all breakers at the substation
- Change the SCADA HMI breaker status representation on the operator's console display to indicate that a breaker was open while in reality it was not
- Open a breaker at the substation while completely hiding the actual status of the breaker from the operator's displays

KS - I believe that this demonstration strengthens the proposed case to develop an HMI PP.

Bill Miller provided some information on an assessment that was performed at Fairfax Water Authority. There was a fair amount of effort put into defining policies and procedures, especially when contractors were involved. The SPP-ICS was not used directly in the assessment.

Murray Donaldson provided information on a training course that DAC is offering. The course, titled *System Security Engineering and Efficiently Safeguarding Your Business* will be held November 30 - December 2, 2004 at the Sheraton Columbia Hotel in Columbia, Maryland. Additional information can be found on the following website: <http://www.commoncriteria.com/Seminar.htm>

## **NIST Industrial Control System Security Testbed**

Keith Stouffer provided some background information on the NIST Industrial Control System Security Testbed for the new members and solicited ideas for testing that the members view as beneficial.

The NIST ICS Security Testbed provides an industrial setting in which to validate standards for process control security and develop performance and conformance test methods.

The testbed contains several implementations of typical industrial control and networking equipment including relevant sensors and actuators. The Testbed has a water distribution system designed to resemble a SCADA system and a factory control system designed to resemble a bottling plant. Detailed information on the testbed can be found here: [http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Equipment\\_list\\_small.ppt](http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Equipment_list_small.ppt)

Currently, testbed activities are focused on the development of performance metrics and tests to provide industry with procedures, and guidance with accompanying generic data to illustrate potential problems and solutions when deploying security software with industrial control systems.

As a starting point, NIST has been conducting HMI software performance testing with concurrently executing anti-virus software on the Water distribution system including:

- Monitor system resources and communication packets between HMI and PLC
- Inject test viruses from available access points.
- Perform virus definition updates

NIST will extend this work to include other security software applications (e.g. personal firewalls) and time critical control applications (e.g. software based PLCs).

DOE is working to establish the NIST ICS Security Testbed as an integral part of the National SCADA Testbed with NIST providing expertise in standards and performance metrics.

## **Next Meeting**

The next meeting will be a conference call during the week of October 11, 2004 to review comments and make a decision on the proposed plan. Additional information, including a request for available dates will be sent out shortly to the group.