PCSRF Conference Call Meeting Notes

Wednesday, October 13, 2004 1:30 PM – 2:30 PM EDT
Hosted by National Institute of Standards and Technology

Participants

Keynon Basinger, Invensys
Martin Naedele, ABB
Tom Kropp, EPRI
Perry Pederson, TSWG
Kevin Staggs, Honeywell
Bill Miller, MaCT
David Saunders
Alan Gunnerson, US Army
Ernest Rakaczky, Invensys
Tom Phinney, Honeywell
Kyle Danilson, Securenetrics
Charles Hoover, Rockwell
Tom Good, DuPont
Jeff Dagle, PNL
Dick Oyen, ABB
Tom Kerestes, EMA Inc
Stan Scown, INEL
Bob Evans, INEL
Jeff Mantong, Western Area Power Administration
Dave Teumim, Teumim Technical
Joe Weiss, KEMA
Dale Peterson, DigitalBond
Holly Beum, Interface-Technologies
Joe Falco, NIST
Keith Stouffer, NIST

Purpose

The main objective for the meeting was to discuss the comments received and make a decision on 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.

Agenda

- Discuss comments received on SCADA Protection Profile plan
- Direction and next steps

Opening Remarks

Keith Stouffer (NIST) started off the meeting and stated that the main topic for this conference call was to review and discuss the comments received on 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.

Proposed Plan – 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 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.

SCADA Protection Profile Comments

Comment:

During the meeting there was a discussion about how to measure compliance. Since there will be multiple components (e.g. OS, HMI application, IDS, etc.) just certifying compliance with one element may be meaningless. That is, if I have a SCADA solution with a secure operating system that meets the requirements for OS certification, but not anything else, is the solution compliant or not? I think the discussion was left that providing some sliding scale of compliance might be the way to go, encouraging users and vendors to include compliance with as many elements as possible.

Discussion:

Keith Stouffer (NIST) stated that although components of a system could comply to a set of security requirements, this does not imply that the overall system is secure.

Dick Oyen (ABB) was not clear how a system with a combination of certified components could not add up to a secure system. He thought the system approach would take care of this.

Keith Stouffer responded that system level issues must be addressed in order to have a secure system.

Joe Weiss (KEMA) brought up the topic of secure real-time operating systems (RTOS) as a component of a system that must be addressed. He asked if there was a protection profile available for an RTOS.

Keith Stouffer replied that there is a protection profile available for a generic OS but not a RTOS.

Joe Weiss stated that this should be identified as a problem that needs to be addressed. He asks if a secure RTOS offered by a company called Greenhill could somehow be used as a starting point for a PP.

Keith Stouffer responded if it is kept generic and not vendor product specific, it may be possible to use the vendors current implementation as a starting point to aid in the development of a PP.

Comment:

You asked for comments and input regarding the proposal to create a SCADA PP by taking "components" of typical SCADA system and looking at the protection and security requirements for each.

One comment I would like to start with is that we probably need to look at "functions" rather than at particular pieces of software. A SCADA/HMI software vendor like Wonderware (or Intellution and "the FIX") breaks their overall software offering into "modules" for the purpose of generating license fees, not because their "modules" represent logical separation by priority or role. You can buy a "basic" graphics package, or the fancy one with lots of wizards and shape libraries. But both are for developing operational displays. A vendor of complete, integrated SCADA/DCS systems may just offer graphical display creation as part of an overall HMI configuration toolkit, which may also include report generation and alarm management features. So the modularization offered by particular SCADA/HMI vendors probably isn't directly relevent to our task.

The second comment I offer is that many times a general term (like HMI) is used to encompass several hardware and software components and a wide range of functionality. Ask a SCADA system operator about his HMI and he will point at a physical console with one or more CRTs and keyboards and pointing devices. Depending on the "mode" of that HMI (and the authority of the user) it might be in use for system configuration and application development, or for process monitoring and control. So, in that case, the "HMI" is really a platform for supporting several distinct and separate functions.

I view SCADA (and DCS systems) as having "functions" (typically tied to specific system utility and operational software) such as system configuration development and modification, application program development and modification, operating system administration, user operational environment development and modification (including displays, reports, logs and alarming functions), historical data collection and administration and of course, the real-time operational monitoring and control environment for the operational personnel. I may have missed one, or combined a couple, but you get the idea. Usually different people, with different skill sets and different access rights, are assigned to each of these functional areas. (Yes, we all know the system where one guy does it all. He just wears a lot of functional hats.)

If we deal in functions (eg. Database configuration and maintenance) then we should be able to avoid the problem of how vendor "A" deals with that task, versus vendor "B". I also think that functional separation will make us "generic" in regards to any vendor's offering seeming to be favored.

Discussion:

There was a general discussion of the above concept of functionality vs. components when considering the development of protection profiles. The group agreed that a functional approach should be taken.

Keith asked if there is any indication of where vendors are currently heading with the implementation of security into their products? Is there a way to find out what their planned security enhancements to their products are prior to their release?

Consensus was that these features are typically not revealed until they are first successfully developed.

Comments:

Here are some comments on the SCADA PP plan of the 7 Sept 2004 meeting, but really they are questions.

What systems will be covered by the SCADA PP? It seems like this question is asked from time to time, but I do not think it has been answered within PCSRF. Is it intended to cover any plant that is so widely distributed that there are distances that cannot be physically guarded, or is it limited to a type of plant? Will it include pipelines and water treatment or just power transmission and distribution?

The "System" approach to PP and ST was intended to provide assurance that an overall system in a plant was protected. But the SCADA PP will be written without a SCADA SPP. How will the assurance of security over the overall system be maintained if we skip the SCADA SPP step? The cost of achieving the different EALs varies by a huge amount. There is a concern that EAL4 and below will only validate that security claims are met, but not that there are no other security defects. There is also a concern that EAL5 and higher are prohibitively expensive in a commercial market. There is also a concern that EAL5 and higher may require re-certification in different countries. What EAL levels will be expected? Who will determine what levels will be expected. Will this be a market issue or regulatory?

I really like the new direction.

I have a concern over using the term SCADA since the term can mean different things in different industries.

I agree with the comment at the end regarding use of the term SCADA. This needs to be clearly defined for the reasons stated – it means different things depending on the industry. Which reminds me, are electric, gas, and other public infrastructure SCADA systems included in the scope? If so, then this also needs to be clearly identified. These systems are quite a bit different from industrial SCADA systems and they use different equipment vendors and have different operating philosophies and requirements.

Discussion:

Bill Miller (MaCT) pointed out a good example of a protection profile representing the current PP writing practices: http://www.iatf.net/protection_profiles/single_level_web.cfm

This PP, written for a web server, uses the latest PP writing structure. The first 40 pages include the TOE and is a good example for group.

Bill Miller also suggested having PCSRF members submit ideas for what a SCADA system should include, including its architecture and associated equipment breakdown. Then, the group should look for commonalities to arrive at a direction for a SCADA PP and develop a statement of evaluation for a particular target.

The group asked what systems will be addressed since SCADA has different meanings in different industries?

Keith Stouffer responded 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 asked Joe Weiss 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.

Keith asked Joe if he could explain the difference between the NERC 1200 and 1300 standards. Joe replied that 1200 was geared towards SCADA and EMS while 1300 expands that area of influence. See: ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf

Keith asked do vendors of SCADA systems develop products that are geared toward one industry?

Dick Oyen responded that ABB has a particular product line "Ranger" that deals strictly with electrical. But they also have derivatives of this product that support other industries.

The group asked if the core of definition of a SCADA system should mean geographically distributed. Keith responded that this is what he suggests.

Dick Oyen stated that the earlier PCSRF plans showed a SCADA System PP (SPP) and are we skipping that now?

Keith responded we would not really be skipping it. The system requirements need to be defined, but may not need to be defined in Common Criteria language since systems may never be certified. Components, however, would need CC specification for certification.

Tom Phinney (Honeywell) added that at an IEC meeting, there was a strong favor for an easier language than CC for industry to use. Of course formal CC is needed for certification.

Bill Miller added that the Security Capabilities Profile (SCP) document is a pretty much English version of the information contained in the SPP-ICS.

Keith added that he will make members aware of SCP again, especially those that are new to the group and don't know about the document. The Security Capabilities Profile document is available on the PCSRF site at: http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/SCP-17-Sep-03.doc

Bill added that the SANS document that was distributed to the group is good to review. This paper focuses on reviewing a key area of data network theory - The Open Systems Interconnect (OSI) Seven Layer Model, and how the model's concepts can be applied in the context of information security. The paper is available on the PCSRF site at: http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/7-Sep-2004/OSI.pdf

The group asked what's the EAL level for SPP-ICS. Keith Stouffer responded that it is an EAL 3.

Bill Miller added that labs do not evaluate at levels above 4 (NSA does this). Typically a vendor starts off with a 1 or 2 and goes higher at the request of a user.

Dale Peterson (DigitalBond) suggested that the group needs to get down to defining the functional and assurance requirements and move on from the defining the TOE. Tom Phinney agreed with this.

Tom Good (DuPont) was concerned with all outside activities (SP99, PCSRF, others) how can we get additional resources to help with these efforts? Would it be possible to get some help from INEL?

Bob Evans (INEL) said that they are pushing SP99 and PCSRF, and if they get funding they will strive to get PCSRF and SP99 some resources, however, resources are unknown at this time.

Keith asked the group if the proposed plan to develop a SCADA PP is the direction that we want to go. The group agreed.

Direction and next steps

It was agreed upon to move on to develop a SCADA PP. Keith Stouffer will develop a project plan and task list and send it to the group for review during the week of October 25, 2004. Comments on the project plan and task list will be accepted until November 5, 2004. All comments on the proposed plan will be collected and made available to the PCSRF group the week of November 8, 2004. 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

The comments collected on the proposed plan will be sent to the PCSRF group the week of November 8, 2004 and a conference call will be held during the week of November 15, 2004 to review the comments.

Next Meeting

The next meeting will be a conference call the week of November 15, 2004 to review comments on the proposed plan and task list. Additional information, including a request for available dates will be sent out shortly to the group.