

PCSRF Face-to-Face Meeting Notes

Wednesday, February 18, 2004 8:30 AM – 5:00 PM ET
Hosted by National Institute of Standards and Technology
Gaithersburg, Maryland

Agenda and Participants

The agenda from the meeting and attendees list are available on the PCSRF website:

<http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/Agenda18-Feb-2004.pdf>

Purpose

The main objective for the meeting was to review/discuss the System Protection Profile for Industrial Control Systems (SPP-ICS) document. There were also several presentation that discussed documents and ongoing work that lead to the development of the SPP-ICS document.

Opening Remarks

Keith Stouffer (NIST) started the meeting with a review of recent events and roadmap for future activities. The short-term roadmap is to get to a Version 1.0 of the SPP-ICS document and to distribute the document to a wider audience for review. To achieve this goal, there are several issues that need to be addressed. These issues are listed below, with the bolded items, the most critical. We are asking the group to provide feedback on these issues by March 12, 2004.

Overall comment on the SPP-ICS from the group

CHAPTER 2

Scope of STOE definition needs to be verified

Diagram of STOE needs to be refined/verified

Further development on distinguishing the physical and logical scope of the STOE, including those parts of the external operating environment not addressed by the STOE.

CHAPTER 3

The specification of sources or categories of ICS vulnerabilities need to be refined/confirmed

Application guidance for the refinement of vulnerabilities, attacks, assets and ultimately threats to be included

Further development of environmental assumptions and OSPs to be performed

CHAPTER 4

Specification of risk categories to be confirmed

Application guidance for the refinement of risk categories into specific risks relevant to the STOE

Develop risks to be mitigated by the external operating environment

CHAPTER 5

Security objectives wording to be further developed

CHAPTER 6

Selection of SFRs and SARs still to be finalized

Functional Security Requirements to be reorganized into class/family groupings

CHAPTER 7

Comment on basic outline/structure

Application notes under development

CHAPTER 8

Comment on the skeleton of the rationale

Mapping and sufficiency arguments under development

APPENDIX A

List of acronyms to be completed

Supporting Presentations

The first presentation was by Stu Katzke (NIST) on the system certification and accreditation work ongoing at NIAP and an overview of federal guidance documents that were referenced in the development of the SPP-ICS document. The presentation is available on the PCSRF website:

<http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/FISMA.ppt>

Murray Donaldson (Decisive Analytics) then gave a brief presentation on the ongoing work to extend the ISO 15408 Common Criteria to address system-level security requirements. This effort within ISO 15408 is benefiting directly from the work in PCSRF to define system-level security requirement for industrial control systems. The presentation is available on the PCSRF website:

http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/System_CC.ppt

Ron Sielinski (Microsoft) then gave a presentation on Microsoft products and their use in manufacturing environments. One of the issues addressed was security patch management. The presentation is available on the PCSRF website:

<http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/MSFT.ppt>

SPP-ICS Review

Ron Melton (Decisive Analytics) presented a review of the development and refinement of the SPP-ICS document from Version 0.88 to 0.91. The presentation included a review on how to use the document, the basic security approach, and a review of the document. The presentation is available on the PCSRF website:

<http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/SPP-ICS.ppt>

During the SPP document discussion, the group thought that confidentiality should be an objective. Confidentiality was mentioned early in the document, but only as an indirect objective in support of safety. Several in the group gave examples where confidentiality was important to prevent industrial espionage, market exploitation or the timing of attacks. Another objective that came up was the need for logged information that supports forensics.

The Common Criteria process continues to baffle some members. During discussions at the break, some of us thought that providing a concrete example of the CC in action would clear up a lot of the confusion. We considered using something like a hardware firewall, something everyone understands, and describing scenario-style what is meant by the Target of Evaluation, the Security Target, what a Protection Profile would be, what a buyer would specify in a procurement request, what a vendor would respond with, etc. Stu Katzke noted that the NIAP site has a list of Security Targets for commercial products, and these could be used in the example.

Additional Presentations

After some discussion on the SPP-ICS document, several other items were discussed.

Department of Homeland Security (DHS) Overview

Mike Lombard (DHS) gave an overview of the organization of DHS, including where critical infrastructure security is addressed in the Information Analysis Infrastructure Protection (IAIP) Directorate. The physical aspect of critical infrastructure protection falls with the Protective Security Division (PSD) and the cyber aspect of infrastructure protection falls within the National Cyber Security Division (NCSD).

HMI antivirus testing update

Joe Falco (NIST) gave a presentation on the effects of antivirus software on the operation of PC based HMI software. These results were derived from some initial testing on the NIST Testbed. The presentation is available on the PCSRF website:

<http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/Antivirus.ppt>

Tom Good (DuPont) noted that they have been running antivirus software on hundreds of HMIs with no adverse affects. Joe's testing confirms this, showing that at the usual low priority, the virus scanning only increases the nominal 150 millisecond HMI update intervals to 250 milliseconds. Tom didn't think any more antivirus testing with HMIs would be beneficial. The impact on soft PLCs would be the next step.

Draft Control Center Protection Profile

Dale Peterson (Digital Bond) presented a Protection Profile for Control Centers to the PCSRF that includes the systems used to manage an industrial control system. These systems typically include real time control servers, historian servers, HMI, network operating systems, and control center infrastructure equipment. The Protection Profile does not include PLCs, RTUs, and other field devices, nor the communications to the PLCs, RTUs, and other. The Protection Profile is available on the PCSRF website:

http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/18-Feb-2004/Control_Center_PP.pdf

ISA-SP99 WG7 subgroup 2 work

Dave Teumim (Teumim Technical LLC) presented the work that is ongoing in ISA-SP99 WG7 subgroup 2 which is mapping security requirements from different sectors (defense, electric, process control).

Roadmap

Group provide feedback on SPP-ICS issues by March 12, 2004

Version 1.0 SPP by March 31, 2004

Conference call to discuss SPP week of April 5, 2004

Workshop on using the SPP-ICS within the acquisition and procurement process - ???

Next Meeting

The next PCSRF meeting will be a conference call the week of April 5, 2004. Additional information, including agenda will be posted in the future.