Process Control/SCADA system vendor security awareness and security posture.

A starting point for the adequate security of process control/SCADA systems is the security awareness and security posture by the manufacturers, vendors, system integrators, and service organisations. The results of a short set of questions indicate that major security improvements are required in this area.

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands. Member of the NICC team.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl

Dr. Stefan Lüders

As deputy computer security officer, Stefan is responsible for the security of the process control systems at CERN, Switzerland.
Phone +41 22 767 4841
e-mail: Stefan.Lueders@cern.ch

The third Dutch Process Control Security Event was held in Amsterdam, on June 4th 2009. The event, organised by the Dutch National Infrastructure against Cybercrime (NICC), attracted both Dutch process control experts and members of the European SCADA Security Information Exchange (Euro-SCSCIE). A set of plenary sessions and parallel workshops addressed a wide range of topics. These included the control systems security program in the United States, the first industrial cyber security vulnerability database, vendor requirements, ownership in process control security, and the development of the Dutch national roadmap to secure process control systems.

„There is no market demand for process control/SCADA security".

Another topic which we will describe here in detail was the EuroSCSIE questionnaire on the security awareness and security posture of process control/SCADA manufacturers, vendors, system integrators, and third party service organisations.

EuroSCSIE

Stefan Lüders presented the background on EuroSCSIE. To better understand and control threats and vulnerabilities in process control/SCADA systems and networks, several nations and organisations started the EuroSCSIE in 2005. Its objective is „*to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions in the SCADA and Control Systems environment...*" with *"... those European Governments, Industry and research institutions that are dependent upon and, or whose responsibility it is to improve the security of SCADA and Process Control Systems.*"

Currently, EuroSCSIE has 19 members from 13 European nations representing users from various sectors as well as key government agencies.

Scary security tests

Stefan continued by showing the results of a 2005-2007 CERN study on the inherent security of 31 process control/SCADA devices from seven different vendors. Using the standard Nessus vulnerability scanner 17% of the process control devices crashed and required a full restart.15% failed partially, i.e. some communication services (e.g. FTP, Telnet, HTTP) hang up. The system vendors were rather clueless on how to react as "*There is no market demand for security".*

The setup of a questionnaire

Based upon a discussion within the EuroSCSIE about these and equivalent types of results in other organisations, an initiative was started to ask manufacturers, vendors, system integrators, and service organisations about their process

control/SCADA security awareness and security posture.

In a quick approach, a simple questionnaire with open questions was developed by the EuroSCSIE members comprising four topic areas:

- General Security Aspects (security policies, standards, good practices),
- Device Security (robustness, system hardening, testing, certification, documentation),
- Software and Firmware Security (software development life-cycle, authentication & authorisation, patching & compliance, configuration),
- Support (technical assistance, confidentiality, vulnerability disclosure, trustworthiness of personnel).

Each of these areas contained three to ten topics. For each topic, a couple of open sub questions were asked. For instance: "Which general security standards is your company following?", "Which control system security standards is your company following?", or "Is your company involved in developing standards?"

Some manufacturers and vendors ducked specific security questions.

The questionnaire, supported by 93 different utilities and bodies such as the EuroSCSIE, the Dutch ISACs, Swedish FIDI-SD, Swiss MELANI, and the U.K. SCSIE, was mailed by these bodies to a large set of Process Control/ SCADA manufacturers, vendors, and system integrators.

Analysis of the responses

Only nine process control/SCADA system manufacturers, vendors, and system integrators returned the questionnaire. The NICC took the responsibility to analyse the results in an anonymised way. The full, detailed information has been provided to the EuroSCSIE members on basis of non-disclosure.

When analysing the completed questionnaires, it immediately became obvious that using open questions does not help to obtain answers that one can compare easily. Some respondents replied with half a page text per topic. One had to make educated guesses in which way the text answered to the stated questions. In some cases, it was obvious that the respondent deliberately wanted to avoid answering a detailed question. In other cases, it turned out that the stated questions were ambiguous. It did not help either that some questions seemed to be replicated where a strict delineation between hardware, software, and services was intended. Above all, open questions allow for vague and foggy answers. For example, the answers to one particular question ranged from a discussion of the availability of a non-disclosure agreement to the description of burning a CDROM of the complete software installation. Moreover, some vendors offer different product lines with different security characteristics.

In hindsight, some important questions were not asked for and therefore not addressed, e.g. software escrow, non-disclosure with 3rd party personnel and protection of customer data, information to customer when malware is detected in the service/maintenance organisation, audit trail of remote 3rd party activities, and secure disposal of failing storage devices.

For the aforementioned reasons, a future follow up of the questionnaire will mostly contain closed questions with some open boxes for additional remarks or explanations. Nevertheless, some conclusions based upon the limited set of returned questionnaires could be drawn and are discussed in the following.

General security aspects

The security policies of the respondents show a large variety in the level of maturity: from a formal global security policy to the reply that security is the issue of the end-user, not that of the PCS/SCADA manufacturer.

The questionnaire asked for the used of standards. Apart from ISA SP99, the ISO/IEC 17799:2005/27000 series, and ISO/IEC15408), some respondents comply with a large set of other (de facto) standards such as CIP 002-009, IEC 62351, IEEE 1711, NIST SP 800-82, CIGRE, …. Larger manufacturers support more standards and often co-operate in the development of industry standards.

Five of the respondents engage the Cyber Security Procurement Language for Control Systems (CSPL) in a positive way and regard it as the basis for security requirements of the customers. However, one respondent replied that the CSPL is used by end users in the wrong way, but did not explain what is wrong. Three respondents never heard about the CSPL, another one did not answer this question at all.

Device security

Five respondents have a formal development process in place, including code review and formal quality management processes. Three respondents trust the good craftsmanship skills of their personnel, but lack a formal process. One respondent outsourced this issue to 3rd party network security.

Systems can be hardened at additional costs by some of the respondent organisations, and three respondents have their systems externally certified or independently tested. One respondent pointed to external parties which offer

verification; device security is not of their concern.

In order to assess whether the systems are robust, six respondents use common test tools such as Nessus and NMAP. Three use other tools such as Metasploit, Achilles test box, and protocol fussers. Since the 2005-2007 experiences by CERN, which we discussed before, the industry has moved. None of the respondents wants to publically disclose their test results. However, in a confidential setting, most customers will be allowed to take a look at the test results.

Regarding the support for secure IP- protocols in the process control/ SCADA environment, four respondents use and support protocols such as SSH, SSL/TLS and IPSec. Four respondents do not support them and one uses a proprietary protocol.

"Information security is an issue of the end-user, not of the PCS/SCADA manufacturer"

The support of the end users by providing security documentation varies a lot with respect to the document quality and information content. It ranges from installation notes to a complete system security manua1. One respondent even offers a security test plan. Three vendors do not provide much security documentation but advertised the service of their in-house security consultants.

Only five of the respondents have a formal process for providing security advisories. Some of the others consider this. One manufacturer/vendor does not plan for providing security advisories.

PCS/SCADA software security

Access control and authentication most often depends on Microsoft Active Directory, others support mechanisms based on Kerberos, Radius, and LDAP. On the other hand, one respondent stated that they support only simple passwords and another respondent proudly mentioned the use of a **single unchangeable password**.

Patching is another hot topic in the process control security environment. The responses were quite diverse. One respondent does not support patching but issues a new release every six months. Another respondent verifies and officially supports a MS released patch within three to four days on average, and seven days maximum. Six respondents have patch verification and patch support processes in place. Nevertheless, most respondents state that their process control software is independent of the operating system. One respondent requires hardening of the underlying operating system and network software.

Transferability of the process control software and its licenses to another platform in case of hardware failure is supported by all manufacturers/ vendors, either by supplying new license keys, by moving a dongle, or by support via telephone.

Support organisation

The support/ maintenance organisations of the respondents have a quite diverse policy when hiring personnel. It ranges from a formal vetting procedure to trust on 'blue eyes'. Some respondents have a 'secrecy' paragraph in the contracts with their personnel.

However, strong guarantees on the confidentiality the customers' data were lacking in many cases, especially when that sensitive data is located at the manufacturer/vendor premises.

The laptops and other systems in use by the support/maintenance personnel are provided with a decent antivirus tool with up-to-date signatures. However, seven respondents do not have a policy or guarantees that their software patch level is up to date. Only one support organisation has a strict policy for their support people: "*Thou shall not connect to an end-user network of a customer*".

Conclusions

Despite the limited set of responses, a number of security issues to be worked on by process control/SCADA manufacturers, vendors, system integrators, and third party service organisations stand out from the analysis:

- Industry good practices are required to guarantee business continuity in case of device failure. Licensing issues shall not block/delay the business continuity.
- Customers shall not drop security demands from quotations to reduce acquisition cost.
- The delivery of hardened system shall become industry standard.
- Access rights shall default to DENY. Default installation passwords shall not exist.
- Industry good practices are required for publishing patches and advisories, and to communicate vulnerabilities.
- Strong guarantees (industry good practices) have to be developed for the trustworthiness of support and maintenance personnel (and the full 3rd party chain) as well as their maintenance procedures.

The dialogue about security between end users and the process control/SCADA manufacturers, vendors, system integrators, and third party service organisations need to be intensified. The questionnaire has been a good start. A next, fully developed, more framed questionnaire may help to stimulate this dialogue and professionalism in securing process control/SCADA systems.

Critical Financial Institutions: Business Continuity Scenarios and Costs

This is the second article in a series of three on how a good practice in software engineering, Test Driven Development (TDD), could become also a good practice for BCP writing at CFIs. First article showed how compliance with the ECIP Directive requires strong BC management at CFIs. This article focuses on how to deal with high costs of some BC crisis scenarios. Last one will show how TDD could help.

Prof. César Pérez-Chirinos
Business Continuity Unit Manager
Banco de España
cepeche@gmail.com

Abstract

This article is the second in a series of three. The series summarises author's experience of successful application of Test Driven Development (TDD) principles in the implementation of the Business Continuity Management (BCM) System in a Critical Financial Infrastructure (CFI): a central bank. This approach has been also useful in other central banks, both in Europe and Latin America.

The full series includes: (i) a Context section, explaining why CFI should have a strong BCM Programme if they want to assure compliance with future revisions of the ECIP Directive[1], (ii) a BC Plan (BCP) Maintenance Issues section –this article-, showing common problems arising to keep the BCP updated, (iii) a TDD of BCPs section, showing how to use TDD-like approach to solve issues in section (ii); and a Conclusions section.

Costs of resilience are virtually unlimited. This article shows a possible approach to delimitate responsibilities for bearing these costs. CFIs top managers require such a clarification to avoid either overinvestment or becoming scapegoats.

The Limits of Security Oriented Business Continuity Management

After the September 11 attacks on the World Trade Center complex, focus of BCM changed from technology oriented Disaster Recovery Plans (DRPs) to a wider scope centred on safety of people running critical processes.

We can summarise this change of paradigm saying that top managers at that time could think something like: *We already know how to have IT continuity. Let's work on how to assure people's continuity for highly disruptive scenarios, protecting them (and us) against any threat*. This way of thinking had the benefit to bring to the toolbox of business continuity management some classical techniques of security officers, like threat intelligence, people oriented crisis management, and so on. But it had the collateral damage of some degree of self-deception: there are business continuity disruption scenarios (earthquakes, pandemics, etc) that can't be mitigated no matter how much you spend on classical security measures.

And then, Katrina destroyed New Orleans.

And business continuity main word changed from "full protection" to "resilience". This was a wise move of

1 "Critical Financial Institutions, OSPs and Business Continuity Plans". ECN Vol. 5, No. 1, pp. 21-23; April / May 2009