STANDARDS BASED MEASURABLE SECURITY FOR EMBEDDED DEVICES*

B. Copy, F. Tilaro, CERN, Geneva, Switzerland

Abstract

Control systems are now routinely connected with enterprise networks and even wide area networks, opening their components to a large array of cyber security threats. Facing threats on such a large scale can now longer solely be done through ad-hoc incident response and post-mortem activities. Defence in depth strategies are being widely adopted and advocated through emerging control systems specific cyber security standards [1]. With these strategies comes the need to accurately prioritise risks and manage system assets, in order to implement measured, tailored security restrictions and automatically assess damages to provide efficient and precise incident response. Eventually, an organization must be able to measure incidents trends and evaluate business impact to feed constant security policy reviews. CERN has implemented a control device cyber security test bench, entitled TOCSSiC [2], updated to provide standards-compliant measurements. Such measurements can be employed to automatically evaluate device vulnerabilities and security policy compliance.

CYBER SECURITY AND CONTROL SYSTEMS

In the recent years, an increasing number of cyber security related incidents affecting industrial control systems (ICS) have been reported [4] [7], resulting in dire consequences both to operating personnel, the systems' respective stakeholders and the environment as a whole. Vendors of critical infrastructure equipment have become more responsive to cyber security related requirements and have started to integrate them more actively in their product life cycle, with their primary focus lying in stability and robustness.

Programmable Logic Controllers (PLC) are the cornerstone of countless systems both in the industry and in the world of high energy physics. As thus, they are an essential link in any defence-in-depth strategy and must be considered as first class citizens in the chain of control.

The Openlab SIEMENS PLC Security project was initiated at the beginning of 2009 as a direct response to the market demand for more stable and cyber security related risk resilience.

PROJECT OBJECTIVES

A SIEMENS funded research project, hosted by CERN Openlab, the “PLC Security” project aims at :

- Investigating cyber security standards relevant to PLC equipment operation.
- Establishing a working environment tailored for ICS, built upon prior TOCSSiC [2] experience, to enable the discovery of new security vulnerabilities.
- Assessing the robustness of SIEMENS Programmable Logic Controller (PLC) products.
- Performing automated security assessments of industrial control equipment.
- Determining which are the key aspects of cyber security in the CERN environment.

A prototype working environment, based on TOCSSiC [2] and tentatively entitled “Testbench for the Robustness Of Industrial Equipments” (TROIE) has been assembled to act as an umbrella for the validation of existing and emerging vulnerability scanning techniques.

SECURITY METRICS

Security policy enforcement is a continuous improvement process. A. Jacquith [3] demonstrates that, like all maturing processes, it may well first be initiated by measuring discrete event occurrences and comparing year to year baselines. In the long run however, a mature process must eventually end up being expressed by a series of key performance indicators that are a factor of time and money, and a set of heuristics that support trending. As an example, while an organization may tally up the number of unwanted “spam” emails it receives each day. A more significant measurement could be “the proportion of unwanted emails that were not filtered out by our anti-spam implementation”, a number which results in wasted time, and therefore resources, for the organization's personnel.

Numerous goal oriented organizational structures, from hospitals to military operations, from multi-national businesses to premier league football teams, make near to daily usage of comparable key performance indicators.

The outcome of a football match can be interpreted from a large number of perspectives, ranging from in-match statistics, players' recent physiological assessments, players' dietary regimen or even supporting spectators' headcount on the day. Most people like to see all these factors summarized for all to see on the football stadium's scoreboard and weekly league table updates, before possibly diving into the causes of these results.

Like the outcome of a football match, cyber security can be understood from numerous viewpoints, which are equally as relevant. These perspectives must eventually be aggregated into a single scoreboard, and be universally understood by all members of the organisation, supporters and players, shop floor and management teams alike.

In that respect, security metrics are an important part of ISA-99 standard proceedings, yet few industrial cyber

*Work supported by SIEMENS through CERN Openlab

# brice.copy@cern.ch

security products are currently able to produce, aggregate or leverage security metrics.

INDUSTRIAL CONTROL SYSTEMS CYBER SECURITY STANDARDS

National and international standards play as a general rule a key role in ensuring cohesion amongst equipment vendors, promoting interoperability and minimizing costs for asset owners. Major government agencies in northern America and Europe have assembled testimonies [4] and mandated the introduction of cyber security standards, guidelines or regulations in order to better protect their critical infrastructures.

ISO/IEC 2700x

Aimed at securing traditional Information System, ISO/IEC 2700x standard documents were not designed with any input from the Industrial Control Systems community. While relevant in many of its aspects to control systems (insofar as they are partly built using off-the-shelf IT components), they do not specifically identify critical assets of such a system, nor do they cater for its operational life cycle [5].

NERC CIP

Mandated by the USA federal government and aimed at securing electrical grid operation from cyber security related threats, NERC standards CIP 02 to CIP 09 act as a minimal legal set of requirements for grid operators. The applicability and relevancy of this standard has been disputed [6] and it is currently under review.

ISA-99

An international standard, designed from the ground up for industrial control systems, which specifically targets SCADAs, PLCs and DCS, it is consistently supported and updated by technical reports providing an updated view of current cyber security practices and market offerings.

ISA-99 features a document (ISA-99 Part 4 standard) specifically targeted at technical requirements for industrial automation and control systems, which is due to reach completion in 2012 [7].

Despite its ISA-99 remains at this stage the favourite route to follow, as it was designed as a general purpose cyber security standard with a close attention to ICS specific issues such as :

- Role based access control
- Operational life cycle of a control system
- Asset criticality assessment and risk analysis methods
- Defense-in-depth strategy
- Continuous policy auditing and review

On Standards

To this stage, no cyber security standard has been identified to be complete or stable enough to be used as a basis for consistent security assessments and risk exposure measurements. Relevant measurements can still be expressed using ad-hoc vulnerability classifications [8] or diagnostic metrics [3] (such as perimeter security or availability and reliability) but no unified, shop-floor to top-floor standard metrics hierarchy exists yet to underpin the project's efforts.

TEST BENCH TECHNOLOGIES

Multiple technologies were evaluated as part of the project's activity. While no definitive architecture has been specified for the TROIE testbench, the following technologies have been short-listed and employed to perform initial security assessments of PLC or other network enabled control equipments :

Openvas [9] is an open-source network vulnerability scanner which originated as a branch of the popular Nessus 2 vulnerability scanner. It integrates a large range of other tools and supports the NASL vulnerability scripting language. Its plugin-centric architecture provides a flexible environment for the development and deployment of new vulnerability scanning techniques.

Wireshark [10] (previously known as Ethereal) is a popular open-source network sniffer which features built-in support for numerous industrial protocols.

Peach Fuzzer [11] is an open-source protocol fuzzer written in Python which implements a wide array of data protocols and encoding schemes. It can be used in conjunction with Wireshark to capture network packet sequences and apply advanced mutating algorithms in order to unravel protocol implementation vulnerabilities.

Cacti [12] is an open-source SNMP monitoring tool which can be used to monitor PLC communication processing units that support this management protocol.

Wurldtech Achilles [13] is a commercial all-in-one vulnerability scanning solution which combines advanced protocol fuzzing techniques with PLC specific monitoring and offers a comprehensive alternative to existing open-source solutions. Wurldtech Inc. also plays a major role in the preparation of industrial cybersecurity standards, such as ISA-99.

ACHIEVEMENTS

After two yearly quarters of research efforts, the Openlab PLC security project has allowed to gather the required expertise to :

- evaluate existing cyber security standards and their respective state of readiness,
- inventory and leverage relevant vulnerability discovery techniques in order to compose a working test bench,
- establish contacts both in the industry and with other European government agencies and ICS users.

In terms of technical outputs, TROIE produces testing results consistent with TOCSSiC findings, with the addition of new vulnerabilities and support for new vulnerability scanning technologies such as OVAL [14], thanks to Openvas.

TROIE leverages a larger range of monitoring techniques, such as communication round-trip times, SNMP based monitoring and Step7 protocol-based polling, exposing a finer granularity of vulnerabilities (such a partial loss of control or partial loss of visibility, which despite their seeming innocuity may have a strong impact on critical control processes).

Our Wurldtech Achilles evaluation demonstrates the considerable potential of protocol fuzzing in finding new low level vulnerabilities, even in the most robust, modern and hardened equipments.

PERSPECTIVES

The Openlab PLC security project still has significant milestones to achieve, the most important being to :

- Further improve the integration of monitoring and vulnerability scanning techniques, in order to offer a feature complete test bench to the widest audience.
- Deliver structured, standard security metrics compatible, vulnerability assessments, that are both familiar to PLC-based facility stakeholders and relevant to PLC technical personnel.
- Adopt a cyber security standard against which CERN assets can be measured, thereby steering equipment vendor choices.

REFERENCES

[1] F. Tilaro, "Control system cybersecurity standards, convergence and tools", CERN technical report, April 2009.

[2] S. Lueders, "Control systems under attack !?", ICALEPCS 05, Geneva, October 2005.

[3] A. Jaquith, "Security Metrics : Replacing Fear, Uncertainty, and Doubt", Addison-Wesley Professional, March 26, 2007, ISBN-10: 0-321-34998-9.

[4] J. Weiss, “Control Systems Cyber Security—The Need for Appropriate Regulations to Assure the Cyber Security of the Electric Grid”, U.S. Congress Testimony, October 2007; http://www.controlglobal.com/industrynews/2007/168.html.

[5] L. Pietre-Cambacedes et al., "Cybersecurity Standards For The Electric Power Industry – A Survival Kit " - CIGRE 2008 proceedings.

[6] S. Katzke, K. Stouffer, M. Abrams, D. Norton, J. Weiss, “Applying NIST SP 800-53 to Industrial Control Systems“, ISA Expo 2006, Houston, TX, October 2006.

[7] T. Angraave, "WIB Minimum Vendor Requirements", 4 June 2009, Amsterdam.

[8] National Cyber Security Division, U.S. DHS, “Common Attack Pattern Enumeration and Classification”, August 2009; http://capec.mitre.org/.

[9] T. Brown, W. Anderson, “Openvas : The Open Vulnerability Assessment System”, June 2007; http://www.openvas.org/.

[10] A. Orebaugh, G. Ramirez and J. Beale, “Wireshark & Ethereal Network Protocol Analyzer Toolkit”, Syngress Publishing, 2006, ISBN 1-59749-073-3.

[11] M. Eddington, “Peach Fuzzing Platform”, 2009; http://peachfuzzer.com/.

[12] I. Berry et al., “Cacti, the complete network graphing solution”, June 2009; http://www.cacti.net.

[13] N. Kube et al., “The Achilles Testing Methodology”, Achilles Satellite sales brief, Wurldtech Inc., 2009; http://www.wurldtech.com/products/achilles_how.html.

[14] National Cyber Security Division, U.S. DHS, “Open Vulnerability And Assessment Language”, February 2009; http://oval.mitre.org/.