TROIE

Testbench for the RObustness of Industrial Equipment

Sponsored by CERN openlab SIEMENS

Standards Based Measurable Security For Embedded Devices

Abstract

Industrial Control Systems (ICS) 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.
Defense 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 called TROIE (Testbench for the Robustness Of Industrial Equipment). TROIE builds on prior TOCSSiC [2] experience, but is updated to support more vulnerability scanning techniques and provide standards-compliant measurements. Such measurements can be employed to automatically evaluate device vulnerabilities and security policy compliance.

Project Objectives

o Investigate cyber security standards for Industrial Control Systems (ICS)

o Research Programmable Logic Controller (PLC) specific vulnerabilities

o Implement a vulnerability research environment, based on TOCSSiC [2]

o Assess the robustness of SIEMENS PLC products

o Determine the key aspects of cyber security in the CERN environment.

Testbench Technologies

The TROIE testbench employs the following open-source technologies :

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 scanning tools and supports the NASL vulnerability scripting language.

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

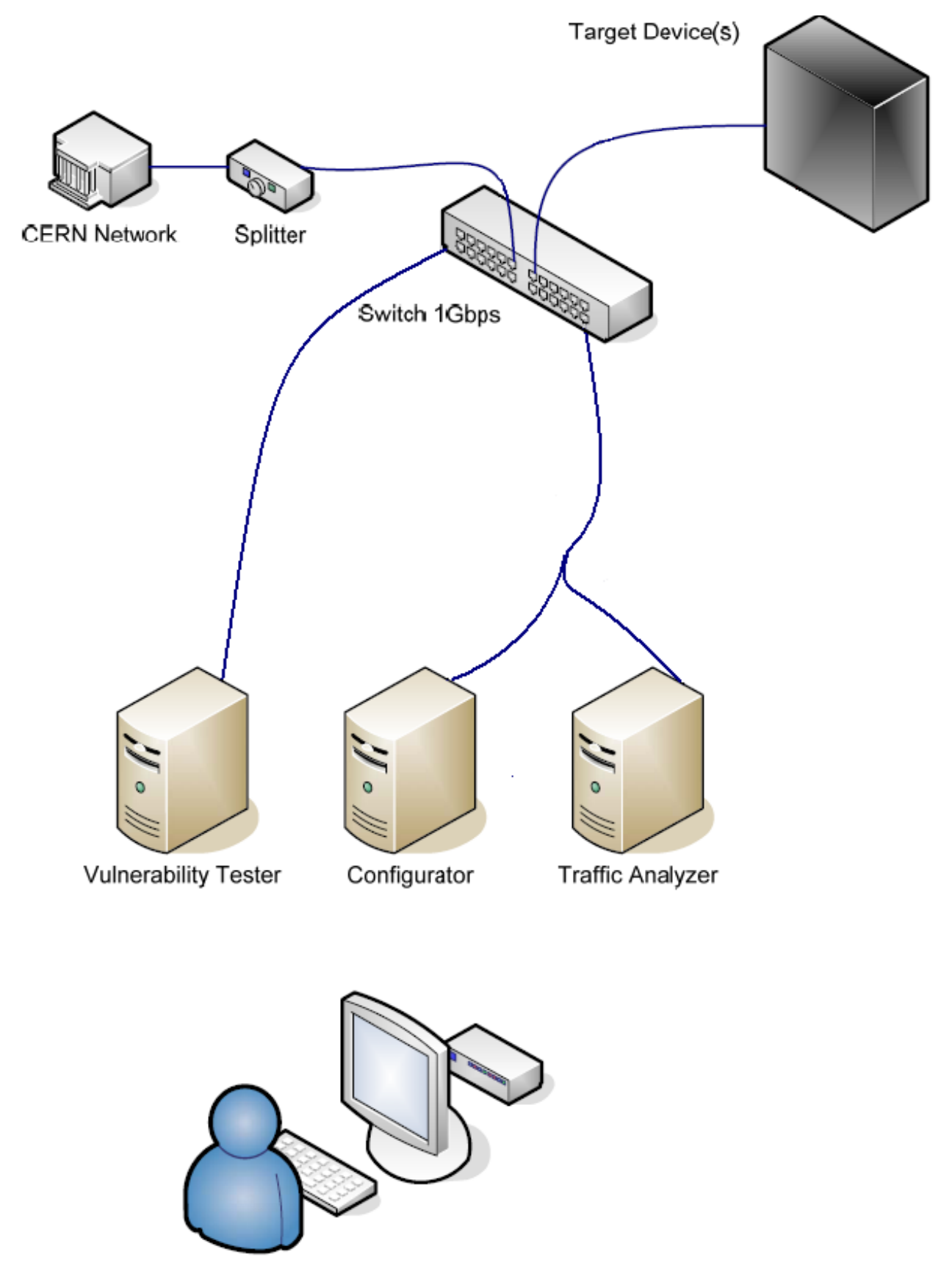

Figure 1 - TROIE Testbench Setup

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

As part of the project, a list of commercial testbenches has also been evaluated.

Wurldtech Achilles Satellite [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.

ICS Specific Standards

A large number of ICS specific cyber security standards exist but none of them has been identified to be complete or stable enough to be used as a basis for consistent security assessments and risk exposure measurements.

ISO/IEC 2700x
Aimed at securing traditional information systems, ISO/IEC 2700x standard documents were not designed with any input from the ICS community. While relevant in many of its aspects to control systems (insofar as they are partly built using off-the-shelf IT components), these documents do not specifically identify critical assets of such a system, nor do they cater for its operational lifecycle [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 Distributed Control Systems.
Despite its current draft status, 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 (Operational lifecycle, ICS specific risk analysis, defense-in-depth strategy).

Security Metrics

Security policy enforcement is a continuous improvement process. A. Jaquith [3] demonstrates that a mature process must be expressed by key performance indicators that are a factor of time and money, and must support business specific trending.
As an example, 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.

Cybersecurity enforcement can be understood from countless perspectives, equally as relevant. These perspectives must eventually be aggregated into a single scoreboard, and be universally understood by all members of the organisation, from the shopfloor to management teams alike.
In that respect, security metrics are an important part of ISA-99 standard proceedings, yet few industrial cybersecurity products are currently able to produce or leverage security metrics.

First Achievements

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 or SNMP and Step7 based monitoring, thereby 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 Satellite 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 ones being to :

o Further improve the integration of monitoring and vulnerability scanning techniques, in order to offer a feature complete test bench to the widest audience.
o Deliver structured and standard security metrics compatible vulnerability assessments, that are both familiar to PLC-based facility stakeholders and relevant to PLC technical personnel.
o 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/

2009 ICALEPCS
WEP110
Authors : Brice Copy (brice.copy@cern.ch)
Filippo Tilaro (filippo.tilaro@cern.ch)
14 October 2009

CERN EN Engineering Department