Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Virtualization of SCADA testbeds for cybersecurity research: A modular approach

Thiago Alves, Rishabh Das, Aaron Werth, Thomas Morris*

Department of Electrical and Computer Engineering, University of Alabama in Huntsville, 301 Sparkman Dr. Huntsville, AL 35899, United States

ARTICLE INFO

Article history:
Received 29 December 2017
Revised 2 April 2018
Accepted 6 May 2018

Keywords:
SCADA
Cybersecurity
Modular testbed
OpenPLC
Simulink

ABSTRACT

SCADA systems were made robust to sustain tough industrial environments, but little care was taken to raise defenses against potential cyber threats. With time, the threats started pouring in and eliciting major concerns in the research community. The extremely high cost and critical nature of SCADA Systems has made it nearly impossible for researchers to perform experiments with live cyber-attacks. Hence, replicating the behavior of these complicated systems by developing high-fidelity testbeds and testing the vulnerabilities on them provides researchers with the necessary workspace to combat the threats currently haunting these legacy systems. However, high-fidelity testbeds like Deter and NSTB are not portable and are hard to replicate. Even though it was possible to identify some portable testbeds, they all have poor support on the virtualization of the SCADA controller or use hardware-in-the-loop, which affects portability. In this research, a novel-modular framework is proposed to replicate complex SCADA Systems entirely on a virtual simulation, which makes them very low cost and portable. The process of virtualizing each major component is discussed. Finally, the success of this methodology is demonstrated by replicating real world critical infrastructures, which are presented as case studies as well as cyberattacks to demonstrate the use of the framework for cybersecurity research.

1. Introduction

A Supervisory Control and Data Acquisition system (SCADA) manages and monitors critical infrastructures such as power plants and water distribution systems. These legacy systems were designed to work in isolation from normal communication networks, and therefore considered secure. However, it has become established that these systems are vulnerable to cyber-attacks as can be seen by some of the well-known examples: Maroochi attack (Slay and Miller, 2008) (in Queensland, Australia), nuclear power plant in Oak Harbor, Ohio compromised by the SQL Slammer worm (Moore et al., 2003). Also, there are a few other noteworthy attacks, such as Stuxnet (Langner, 2011) and Havex (ICS-CERT 2014), which further demonstrated the potential of destructive cyber-attacks on SCADA systems. Given that SCADA systems are also part of critical infrastructure such as electric energy systems, nuclear energy systems, water and sewage treatment plants, gas/oil energy systems, and transportation systems, attacks on those systems can lead to catastrophic consequences for the nation. The work put forth by Alcaraz and Lopez (2012) identifies five requirements of Critical Control Systems that, if tampered, can cause impact on services, resources, operational control and sensitive information of the control system environment.

* Corresponding author.
E-mail addresses: tra0006@uah.edu (T. Alves), rd0029@uah.edu (R. Das), aww0001@uah.edu (A. Werth), tommy.morris@uah.edu (T. Morris).

https://doi.org/10.1016/j.cose.2018.05.002
0167-4048/© 2018 Elsevier Ltd. All rights reserved.

To counter these attacks, researchers have put their efforts in finding defense mechanisms that can protect the SCADA network and the Programable Logic Controllers (PLCs). The literature is rich in providing information about vulnerabilities and threats of SCADA systems. Alcaraz and Zeadally (2013) explore vulnerabilities and threats on SCADA systems and propose protection mechanisms on four areas: governance (security policies and standards), robust network design, self-healing, and modeling and simulation. A better way to build defense mechanisms for SCADA systems is by understanding the behavior of the entire system in a modular way so that the vulnerability associated with each segment can be studied for cybersecurity research.

The SCADA community has seen ample research that involves paradigms for replication of the physical processes. Little efforts have been made to make the virtualization framework modular that could be used by SCADA researchers. Alves et al. took the pioneering step to create a gas pipeline SCADA system in a modular paradigm (Alves et al., 2016). The characteristics of the modeled testbed were compared with the actual physical testbed, and the success of the modeling approach was demonstrated through experiments. Although the modular approach exhibits high fidelity with the physical-gas pipeline, the framework was not generic enough to model different SCADA systems.

This paper demonstrates a novel modular approach to virtualize SCADA systems for research in Cybersecurity. A modular virtualization framework enables SCADA researchers and experts from each domain to create a better replica of the actual counterparts and facilitates the analysis of vulnerabilities associated with each element. For the purpose of this paper, virtualization is defined as a computer-generated simulation of reality. Therefore, a virtualized item must correspond to its real-life counterpart with maximum fidelity, while being enclosed on a virtual environment. The proposed framework is generic enough to model a wide variety of SCADA systems with required high fidelity to test the effect of cyber-attacks on the system's different modules.

The contributions of this paper are (1) the design and detailed description of the novel and modular SCADA virtualization framework, (2) the application of the virtualization principles in each SCADA component, and (3) three use cases applying the virtualization framework to create a virtual water storage tank testbed, a virtual gas pipeline testbed and a virtual refrigerated liquefied petroleum gas pipeline testbed. These testbeds allow for cyber security research, which may include experimentation with cyber-attacks and SCADA Systems. The paper is organized as follows for the remaining sections: 2 related works, 3 SCADA components overview, 4. SCADA virtualization, 5. Case studies, 6. Usage scenarios, 7. Conclusion, and the last section is Acknowledgment.

2. Related works

Foreseeing the advantages offered by virtual testbeds for research in SCADA security, many researchers have created testbeds to accurately mimic those systems. Siaterlis and Genge (2014) compared the features of recent virtual and physical SCADA testbeds and devised several metrics (fidelity, repeatability, measurement accuracy and safety) to measure the effectiveness of a virtual SCADA testbed. The work put forth by Vaughn and Morris (2016) highlights the need for high-fidelity testbeds for SCADA cyber security research. Several testbeds (Deter Benzel et al., 2006, NSTB Kenneth Barnes, 2009) did have high-fidelity to the physical system but the portability, repeatability and cost of the testbeds were unacceptable. The novel-modular architecture for SCADA testbed development put forth in this paper is designed specifically to address these issues, thereby providing high-fidelity testbeds at a very low cost that are highly portable and easily repeatable by end users.

Another notable survey by Holm et al. (2015) compares the performance of thirty testbeds mimicking different industrial processes. This study analyzed the shortcomings of each testbed approach, and it was observed that in the testbed development, repeatability by the end user is a major concern. Secondly, most of the testbeds were crafted for a specific industrial process and were not generic to model other systems. Siaterlis et al. (2013) addressed the second research problem and proposed a modular approach with high fidelity in the network side, but the architecture that virtualizes the SCADA system did not have programmable logic controllers and the logic controlling the virtualized industrial process were executed by servers.

Similarly, a python script was used by Reaves and Morris (2012) to mimic the function of a PLC in the industrial process. Although multiple metrics were used to ascertain considerable fidelity, the system is not generic enough to model different industrial processes.

PowerCyber testbed developed by Iowa State university (Hahn et al., 2010) with simulated industrial protocols like DNP3 and IEC 61850 was specifically designed to model power systems. This architecture does not have virtualized PLCs and hence industrial programming languages for implementing the logic of the system like ladder logic, structured text, etc. are not supported.

Another approach to create a framework for SCADA simulations is SCADASim (Queiroz et al., 2011), which is basically an extension of the OMNET++ network emulator (Varga and Hornig, 2008) that allows it to communicate with external SCADA devices. Although this approach enables the development of complicated SCADA networks, it lacks the modeling of the physical plant and requires hardware-in-the-loop for high-fidelity simulation of SCADA controllers. Another example of an OMNET++ based testbed is the work put forth by Queiroz et al. (2009), which has the same limitations of SCADASim.

Therefore in this paper, a scalable low-cost solution for modeling multi-domain heterogeneous physical processes with high fidelity is proposed. Researchers can replace any module with a different implementation for that module to potentially improve the fidelity of the testbed. It is also possible that a virtual module may be replaced by an actual counterpart without affecting the response of the testbed. Additionally, it is not necessary for the end user to be proficient with the exact technology used to model each module of the testbed, thereby bolstering the reproducibility of the testbed. Secondly, the modular design will facilitate SCADA researchers to identify vulnerabilities on specific parts of the