Chapter 4

TRUSTED VIRTUALIZATION-BASED PROGRAMMABLE LOGIC CONTROLLER RESILIENCE USING A BACKFIT APPROACH

James Cervini, Daniel Muller, Alexander Beall, Joseph Maurio, Aviel Rubin and Lanier Watkins

Abstract Industrial control systems perform vital cyber-physical functions in critical infrastructure assets. Programmable logic controllers, which are prominently found in industrial control environments, execute the operational control logic of cyber-physical systems. Due to the continued escalation of cyber attacks targeting industrial control systems and programmable logic controllers, strengthening the trust and resilience of these systems is paramount.

This chapter proposes an approach that leverages virtualization, cryptographic attestation, software-defined networking, security orchestration and a proprietary programmable logic controller runtime application to advance programmable logic controller trust and resilience while facilitating integration in deployed systems. A proof-of-concept capability demonstrated on a physical industrial control system testbed validates the approach. The experimental results confirm that the approach is viable for industrial control applications.

Keywords: Industrial control systems, virtualization, security

1. Introduction

Programmable logic controllers (PLCs) are real-time systems that receive inputs from sensors, execute pre-programmed logical routines and produce outputs that ultimately drive physical actuators. These devices and their control loops operate diverse physical processes, supporting industrial control systems in critical infrastructure assets in the energy, chemicals, manufacturing, water and wastewater sectors. Given the con-

Published by Springer Nature Switzerland AG 2022
J. Staggs and S. Shenoi (Eds.): Critical Infrastructure Protection XVI, IFIP AICT 666, pp. 103–117, 2022.
https://doi.org/10.1007/978-3-031-20137-0_4

stant targeting of these vital systems and processes, there is a compelling need to research methods that increase their resilience against cyber attacks. Additionally, cost and uptime requirements often result in sparse upgrade cycles of programmable logic controllers in the operational technology domain. Therefore, research must investigate the applicability of security approaches for deployed proprietary systems. This chapter proposes an approach that leverages virtualization and trusted computing to enhance operational technology systems. The enhancements enable these systems and the processes they control to be more resilient, flexible, secure and cost-effective.

Virtualization provides a guest environment segmented from host machine hardware by using a hypervisor to interpret and allocate the available computing resources. The segmentation provides several benefits. The lack of reliance on a specific host contributes to a dynamic virtual environment that can rapidly change hosts as needed to ensure maximum uptime. Also, the isolation between guest and host can mitigate malicious processes from spreading to host hardware. Additionally, the hardware abstraction provided by virtualization is cost effective compared with installing and maintaining dedicated hardware for each process that could be virtualized. Indeed, the ability to virtually test and seamlessly merge software updates and configuration changes with little or no downtime is highly desirable for operational technology systems.

This research has three principal contributions. It is first to cryptographically attest a virtualized programmable logic controller using a trusted platform module (TPM). Additionally, it proposes a virtualized programmable logic controller environment generation approach that leverages existing system hardware and software artifacts to streamline backfit deployments. Also, it is the first to engage automated security orchestration to respond to failures of programmable logic controllers in performing cryptographic attestation.

2. Related Work

The hard and soft real-time performance requirements imposed in operational technology environments clash with added layers of software complexity introduced by virtualization. As additional software processes are introduced to support programmable logic controller virtualization, the ability to guarantee real-time control loop performance is reduced. Previous research has attempted to address this problem by utilizing a real-time optimized environment and highlighting virtual programmable logic controller feasibility [3]. In contrast, this work explores the trust and resilience functionality enabled by the proven virtual pro-