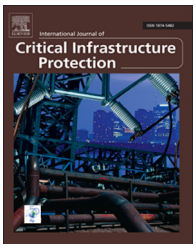
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Experimental assessment of network design approaches for protecting industrial control systems

*Béla Genge**, Flavius Graur, Piroska Haller*

Department of Informatics, Petru Maior University of Tîrgu Mureş, Nicolae Iorga, No. 1, Tîrgu Mureş, Mureş, 540088 Romania

ARTICLE INFO

Article history:
Received 3 July 2014
Received in revised form
11 June 2015
Accepted 28 July 2015
Available online 8 August 2015

Keywords:
Industrial control systems
Network security
Defense-in-depth
Software defined networking
Stuxnet

ABSTRACT

This paper surveys and provides experimental results related to network design techniques focused on enhancing the security of industrial control systems. It analyzes defense-in-depth strategies, network segmentation, network firewall configurations and the role of intrusion prevention systems, intrusion detection systems and anomaly detection systems. The paper also studies the applicability of emerging technologies in the area of IP networks, including software-defined networking, network functions virtualization and next generation firewalls in securing industrial control systems. The main contribution of this paper is the experimental assessment of existing and future network design approaches in the presence of real malware (e.g., Stuxnet) and synthetic attacks (e.g., denial-of-service attacks). The experimental results confirm the importance of defense-in-depth strategies and also highlight the embryonic state of software-defined networking security, which requires profound transformation and validation in order to be embraced by the industrial control system community.

1. Introduction

The pervasive adoption of commodity, off-the-shelf information and communications hardware and software in modern industrial control systems has led to significant cost reduction as well as greater efficiency, flexibility and interoperability between components. At the same time, it has enabled the implementation of new services and features such as remote monitoring and maintenance, energy markets and the emerging smart grid. However, the technological shift from completely isolated environments to "system of systems" integration has had a dramatic impact on industrial control system security [3]. By leveraging attack vectors that are commonly used to compromise traditional computer systems (e.g., phishing and USB infections), malware aimed at disrupting critical infrastructure systems have become effective cyber weapons [13,50].

Industrial control systems are also subject to a new breed of cyber-physical attacks. These attacks, which are more complex and sophisticated than traditional cyber attacks, can exploit the cyber and physical dimensions of industrial control systems to significantly impact their normal functioning. Stuxnet [13] is believed to be the first malware that was specifically designed to attack industrial control systems. Its ability to rewrite the control logic of industrial hardware and, more importantly, to hide its presence from system engineers, showcased a new class of threats in which disturbances originating in the cyber dimension propagate to the physical dimension. Stuxnet's follow-ups, Duqu [58], Flame [50] and Dragonfly [59] (reported in June 2014), have revealed

*Corresponding author.
E-mail address: bela.genge@ing.upm.ro (B. Genge).

http://dx.doi.org/10.1016/j.ijcip.2015.07.005
1874-5482/

the true dimension of cyber espionage where specially forged malware can strategically compromise significant organizations and, if needed, cause damage in various industrial sectors, including defense, aviation and energy.

Given the escalating threats, this paper provides an experimentation-based survey of existing network design techniques aimed at enhancing industrial control systems security. The main goal is to experimentally evaluate the impact of network design choices on the successful outcome of cyber attacks on industrial control systems. The paper starts with an overview of the main approaches, including well-established techniques such as network segmentation, firewall-based traffic filtering and the deployment of intrusion prevention systems (IPSs), intrusion detection systems (IDSs) and anomaly detection systems (ADSs). Next, the importance of defense-in-depth strategies is emphasized and the applicability of emerging IP network technologies such as software-defined networking (SDN), network function virtualization and next generation firewalls to securing industrial control systems are discussed. This discussion is followed by experimental evaluations of the principal security measures. The evaluation is conducted using real malware (Stuxnet) and a synthetic denial-of-service attack that causes severe disruptions to communications and services. The results confirm the importance of defense-in-depth strategies and highlight the applicability of novel IP network technologies to enhance the security of modern industrial control systems.

This paper also presents an approach for experimenting with the cyber and physical dimensions of large industrial control systems. The approach embodies software-defined network controllers based on Floodlight [46], real sensor networks, an implementation of the emerging Sensei/IoT* proposal [45] and the Mininet network emulator [26]. This is an important step in industrial control system security experimentation because it paves the way towards testing software-defined-network-enabled industrial control system configurations. In fact, software-defined networking leads to flexible and dynamic industrial control networks in which accidental failures and malicious attacks can be mitigated through dynamic network reconfiguration. However, throughout this work, it is noted that software-defined networking is an emerging technology, built on an architecture that does not embody security. Thus, while software-defined networking may bring certain advantages, the absence of security features requires profound research and extensive validation before it can be embraced by the traditional IP networking community, let alone the industrial control systems community.

This paper has three major contributions. First, it conducts an analysis of network design methodologies focused on securing industrial control systems, and experimentally tests the applicability of emerging networking paradigms to industrial control systems. Second, despite the many articles about Stuxnet [9,13,17,25,33], this paper is the first to describe systematic experiments that evaluate the effects of various network design strategies on Stuxnet's ability to propagate in an industrial control network. Third, the paper presents a novel approach for experimenting with software-defined-networking-enabled industrial control networks in order to provide laboratory-scale infrastructures for conducting security and resilience studies.

2. Related work

Securing industrial control systems used in the critical infrastructure is an important area of research [30,34,36,55]. A survey of the scientific literature reveals a large collection of articles dealing with security assessments of industrial control systems. Several guidelines and tools have been developed to assess the security risks in industrial control installations. The U.S. Department of Homeland Security guide, Cyber Security Assessments of Industrial Control Systems [61], provides an overview of the cyber security assessment process. It discusses typical cyber security assessment steps such as establishing an assessment team, creating a test plan, identifying attack vectors, executing the assessment and reporting the results.

The Cyber Security Evaluation Tool (CSET) provides a systematic approach for conducting cyber security assessments of industrial control systems [28]. CSET is a question and answer based tool that helps establish whether the configuration of a specific installation adheres to industry standards and best practices. It is currently available as a standalone software tool.

The InSAW tool provides an integrated approach for modeling actors, assets, relationships between assets and relationships with external entities [42]. InSAW helps construct dependencies and data-flow graphs that aid in the identification of possible vulnerabilities. The tool has been used extensively in recent assessment approaches proposed by Leszczyna et al. [34,36].

The aforementioned approaches are designed to conduct cyber security assessments of industrial control systems without interfering with the actual installations. In contrast, the work presented in this paper experimentally assesses the impact of different industrial control network configuration decisions on the outcomes of cyber attacks involving real and synthetic malware.

Several researchers have conducted experimental assessments using synthetic attacks against industrial control systems. Cardenas et al. [11] have studied various attacker models and their impacts on a simulated physical process. Other researchers [21,49] have investigated the impacts of attacks such as spoofing, replay and denial-of-service on the functioning of physical processes. Leszczyna et al. [36] have leveraged the MalSim agent-based architecture [35] to simulate the behavior of a wide range of malware.

Moving to large-scale infrastructures, Bilis et al. [8] have documented the impacts of deliberate attacks on the performance of electric power grids. The attacks, which modified parameters in a simulated electric grid, could be launched by an attacker after bypassing protective security measures to cause significant damage to the underlying physical infrastructure.

In contrast to the aforementioned assessments, this paper provides valuable insights on the impacts of industrial control network design decisions on the behavior and successful replication of real malware (i.e., Stuxnet). The paper does not focus on the actual impact of malware on the functioning of physical processes because this aspect has been covered extensively in previous studies [8,21,31]. The novelty and principal contribution of this paper is the experimental assessment of the impact of Stuxnet on a typical industrial