Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 95 (2016) 24 – 31

Procedia
Computer Science

Complex Adaptive Systems, Publication 6
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2016 - Los Angeles, CA

A Method for Revealing and Addressing Security Vulnerabilities in Cyber-Physical Systems by Modeling Malicious Agent Interactions with Formal Verification

Dean C. Wardell*, Robert F. Mills, Gilbert L. Peterson, Mark E. Oxley

Air Force Institute of Technology, 2950 Hobson Way, Dayton OH 45433

Abstract

Several cyber-attacks on the cyber-physical systems (CPS) that monitor and control critical infrastructure were publically announced over the last few years. Almost without exception, the proposed security solutions focus on preventing unauthorized access to the industrial control systems (ICS) at various levels – the defense in depth approach. While useful, it does not address the problem of making the systems more capable of responding to the malicious actions of an attacker once they have gained access to the system. The first step in making an ICS more resilient to an attacker is identifying the cyber security vulnerabilities the attacker can use during system design. This paper presents a method that reveals cyber security vulnerabilities in ICS through the formal modeling of the system and malicious agents. The inclusion of the malicious agent in the analysis of an existing systems identifies security vulnerabilities that are missed in traditional functional model checking.

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology

Keywords: vulnerability detection; model checking; malicious agents; industrial control systems

* Corresponding author. Tel.: 1-321-961-5009
E-mail address: dean.wardell@us.af.mil

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology
doi:10.1016/j.procs.2016.09.289

1. Introduction

Industrial control systems (ICS) have been "found to be rife with vulnerabilities"[1]. Researchers have put significant effort into developing security policies, practices and bolt-on security measures. The security measures have been primarily focused on intrusion detection, user authentication and countering malware. These multiple protective layers make up the 'Defense in Depth' strategy that is essential for system protection. Defense in Depth provides preventive measures, but more attention needs to be given to designing the systems to be more resilient to attacks if and when malicious actors do gain access.

A primary step in making these systems more resilient is identifying security vulnerabilities unique to the operational technology (OT) as opposed to those known to be in related IT systems. These vulnerabilities are usually inherent in the ICS design, but some are emergent from the combined system of systems that comprise so many ICS.

Once the vulnerabilities have been identified, steps can be taken to address them. The corrective actions can range from simple updates in the controller code, to redesigning portions of the system to add or change hardware. Depending on the criticality of the system, and the extent to which it is vulnerable to attack, an advanced fault tolerant or adaptive control strategy may be appropriate.

To begin the process of making a control system more resilient against a malicious agent that gains access to it, this paper proposes a novel application of formal system verification to identify cyber security vulnerabilities. This method is intended to be used as part of an overall risk management strategy and to assist those performing vulnerability analysis on ICS. We demonstrate this method on two different ICS controllers and then show how many of the vulnerabilities can be improved or even eliminated by making simple updates to the controller logic.

2. Related Work

Vulnerability assessments are used to identify where a system may be susceptible to attack. While primarily used on IT systems, cyber vulnerability assessments have also been advocated for use with ICS[2,3]. While useful, these are a manual processes requiring extensive system expertise.

In past work[4], the authors take steps to automate the vulnerability assessment of binary software programs (vs. source code) by enhancing traditional black-box fuzzing of the windows server with a genetic algorithm. A more recent example[5] uses fuzzing and an SMT solver to automate the vulnerability analysis of commercial binary programs. These programs have not been applied to ICS OT programs.

From a control theory perspective, research has been accomplished[6,7] in mathematically modeling control systems to better understand their functionality and improve their security. These models are used to produce simulations and conduct testing[8,9]. System testing is useful but suffers from the needle-in-a-haystack problem.

Unlike system testing, formal verification is a more complete solution. Formal verification of IT software and protocols has been well researched and some work has focused on modeling threats[10,11] and one specifically modeled and checked malicious interactions with the program[12].

The idea of formally verifying ICS through model checking has been explored to some extent since 2001. The research in this area has been focused on checking the functionality of the systems[13,14]. A lesser portion of the research has focused on verifying safety functions of control systems[15,16] and only recently have a few researchers considered model checking for security purposes[17].

Research in modeling human interactions with cyber-physical systems (CPS) has primarily considered correct user actions[18,19] with some consideration of the possibility of unintentional user errors[20,21]. None of these specifically model check malicious actions with the CPS.

It is at the intersection of 'model checking control systems for security' and 'modeling malicious agent interaction' that we focus our efforts.

Existing reference material[22,23,24] describes the different types of attacks that can executed against ICS and supervisory control and data acquisition (SCADA) systems. From these, the answer to the question 'what can a malicious agent do to the system once they gain access?' distils out to five general types of malicious interactions with a system:

Changing set points. Set points are used to set conditions under which the controller will start and/or stop particular functions. An authorized user/operator can change these set points by accessing the controller from an