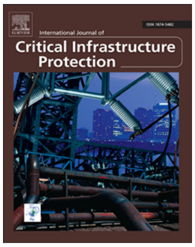
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



A multi-layered and kill-chain based security analysis framework for cyber-physical systems

Adam Hahn[a,*], *Roshan K. Thomas*[b], *Ivan Lozano*[b], *Alvaro Cardenas*[c]

[a]*School of Electrical Engineering and Computer Science, Washington State University, Pullman, Washington 99164, USA*
[b]*The MITRE Corporation, MS T340, 7515 Colshire Drive, McLean, VA 22102, USA*
[c]*Erik Jonsson School of Engineering and Computer Science, University of Texas at Dallas, 800 West Campbell Road, EC31, Richardson, TX 75080, USA*

ARTICLE INFO

Article history:
Received 13 January 2015
Received in revised form
9 August 2015
Accepted 15 August 2015

Keywords:
Cyber-physical system security
Kill-chain
Cyber reconnaissance
Controllability
Observability

ABSTRACT

This paper introduces a novel framework for understanding cyber attacks and the related risks to cyber-physical systems. The framework consists of two elements, a three-layered logical model and reference architecture for cyber-physical systems, and a meta-model of cyber-physical system attacks that is referred to as the cyber-physical system kill-chain. The layered reference architecture provides a systematic basis for studying how the causal chain associated with cyber perturbations can be traced all the way to physical perturbations. The cyber-physical system kill-chain describes the progressive stages of attacks to illuminate the steps required for an attacker to launch a successful attack against a cyber-physical system. The proposed framework offers a novel approach for comprehensively studying the elements of cyber-physical system attacks, including the attacker objectives, cyber exploitation, control-theoretic properties and physical system properties. The framework is evaluated using a simulated unmanned aerial system and the results of the evaluation are discussed. The longer-term goal is to use the framework as a means to deduce cyber-physical system security properties and to enumerate the principles for designing systems that are resilient to cyber attacks.

1. Introduction

Attacks on cyber-physical systems (CPSs) have been observed with increasing frequency and have attracted the attention of the research community and industry. However, a common attack analysis framework and related design principles for resilient cyber-physical systems have not yet emerged. Organizations such as NIST have emphasized that accurate security threat models are critical to designing secure cyber-physical systems [17].

This paper introduces a novel framework for analyzing cyber attacks against cyber-physical systems. The framework provides a foundation for understanding cyber attacks and the related risks to cyber-physical systems, and for articulating design principles that will help engineer resilient cyber-physical systems.

The framework incorporates two elements. The first element comprises a logical system model and reference architecture that express the architectural composition of cyber-physical systems in terms of three interrelated layers. The bottom physical layer models the physical dynamics and properties of a control system, including its sensors and actuators. The middle control layer embodies a mathematical model of the control logic and various control algorithms, state

[*]Corresponding author.
E-mail address: ahahn@eecs.wsu.edu (A. Hahn).

http://dx.doi.org/10.1016/j.ijcip.2015.08.003
1874-5482/© 2015 Elsevier Ltd All rights reserved.

estimators, error correction and sensor feedback mechanisms that are used to observe and manipulate the physical system. Finally, the top cyber layer expresses the control system in a computerized platform, such as a programmable logic controller. The cyber layer utilizes the Architecture Analysis and Design Language (AADL) to model communications buses, data, messages, processes and systems.

The second element of the framework is a cyber-physical system kill-chain for analyzing attacks and threat models in the cyber-physical system domain. This meta-model of cyber attacks helps understand the various lifecycle phases that make up an attack. It is analogous to the cyber kill-chain originally proposed by Hutchins et al. [10]. It clarifies the value of intelligence-driven defenses that emphasizes an understanding of adversarial tactics, techniques and procedures as the basis for designing system defenses. The intelligence-driven defense approach has been used to predict the vulnerabilities that could be exploited to launch attacks [8]. Meanwhile, the U.S. Department of Defense has used the kill-chain to design cyber security testing and evaluation activities [18].

By combining a layered reference model with the cyber-physical system kill-chain, the proposed framework supports the systematic analysis of causal chains and perturbations that emanate from the cyber layer all the way to the physical impact on the cyber-physical system. The utility of the framework is demonstrated using a case study involving the control system of a simulated unmanned aerial system (UAS). A number of cyber attacks were launched against various unmanned aerial system components and the resulting physical system impacts were evaluated. The simulations were then used to explore how the cyber, control and physical properties influence attack impacts. The analysis provides insights into defensive strategies that are effective during the various cyber-physical kill-chain phases.

2. Previous work

The last few years have seen the publication of numerous research papers that analyze cyber vulnerabilities in cyber-physical systems. Cardenas et al. [2] have demonstrated how attacks can impact different elements of a control loop in a cyber-physical system. Several research efforts have explored theoretical and real-world attacks against cyber-physical systems; these attacks have used a broad range of attack vectors and have targeted various elements of the control loop. Fig. 1 identifies the control loop components that can be impacted by cyber attacks, including measurements, actuator signals, controllers and reference signals.

By manipulating sensor signals, an attacker can corrupt the state estimates computed by a controller and then change the resulting control signals sent to actuators. Liu et al. [15] have shown that cyber attackers can manipulate power system state estimation algorithms by sending fraudulent measurements to state estimators. Other researchers have demonstrated that unmanned autonomous vehicles can be hijacked by spoofing GPS signals that cause controllers to send incorrect control actions [21]. Additionally, researchers have demonstrated that wireless signals can be used to manipulate medical devices and cause drug overdoses [14,19].

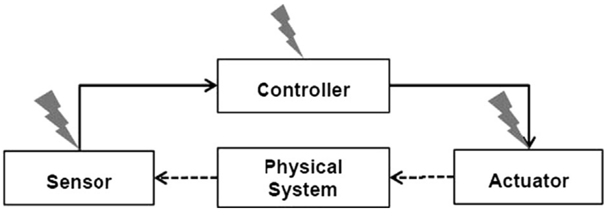


Fig. 1 – Cyber-physical system attacks.

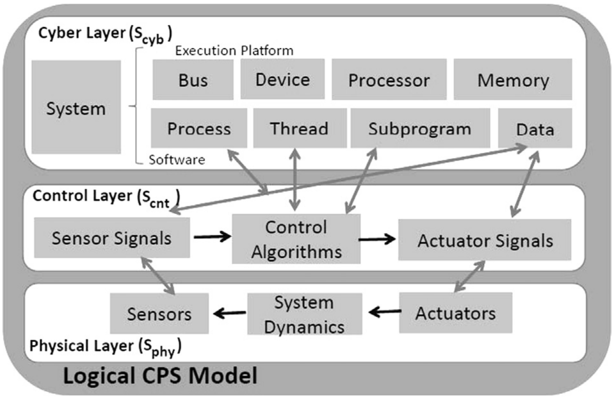


Fig. 2 – Logical cyber-physical system model.

Numerous attacks have demonstrated the ability to manipulate control algorithms executing on controllers by abusing administrative rights or exploiting software vulnerabilities. By manipulating a controller, an attack can directly influence the control signals sent to actuators. The Stuxnet worm is an excellent example of an attack on a controller – it manipulated ladder logic device configuration code in a programmable logic controller to send malicious commands to frequency converters that directly controlled centrifuge rotors [4]. Similarly, the Aurora attack demonstrated that electric power generators could be physically damaged if their frequency control is made out-of-sync with the frequency control of the power grid [22]. Additionally, Halperin et al. [9] have demonstrated that controllers in implanted cardiac devices can be remotely reprogrammed to cause incorrect treatments and/or dosages to be given to patients.

An attacker can manipulate control actions by directly sending commands to actuators. For example, researchers have directly injected packets into the CAN buses of modern automobiles, resulting in malicious control actions being sent to critical actuators (e.g., engines and brakes) [3,13].

3. Cyber-physical system model

This section introduces a three-layer representation of a cyber-physical system S as demonstrated in Fig. 2. The model layers include the physical layer S_{phy}, control layer S_{cnt} and cyber layer S_{cyb}. Each layer is defined in detail below.