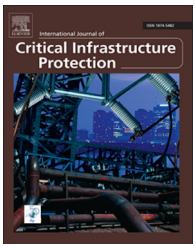
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 8 (2015) 40–52

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



A language for describing attacks on cyber-physical systems

Mark Yampolskiy[a,*], *Péter Horváth*[b], *Xenofon D. Koutsoukos*[c], *Yuan Xue*[c], *Janos Sztipanovits*[c]

[a]*School of Computing, Shelby Hall, University of South Alabama, 150 Jaguar Drive, Mobile, Alabama 36688, USA*
[b]*Department of Broadband Communications and Electronics, Budapest University of Technology and Economics, Egry József utca 18, 1111 Budapest, Hungary*
[c]*Institute for Software Integrated Systems, Vanderbilt University, 1025 16th Avenue South, Suite 102, Nashville, Tennessee 37212, USA*

ARTICLE INFO

Article history:
Received 16 May 2013
Received in revised form
22 September 2014
Accepted 23 September 2014
Available online 11 October 2014

Keywords:
Cyber-physical systems
Security
Cross-domain attacks
Taxonomy
Attack description language

ABSTRACT

The security of cyber-physical systems is of paramount importance because of their pervasiveness in the critical infrastructure. Protecting cyber-physical systems greatly depends on a deep understanding of the possible attacks and their properties. The prerequisite for quantitative and qualitative analyses of attacks is a knowledge base containing attack descriptions. The structure of the attack descriptions is the indispensable foundation of the knowledge base.

This paper introduces the Cyber-Physical Attack Description Language (CP-ADL), which lays a cornerstone for the structured description of attacks on cyber-physical systems. The core of the language is a taxonomy of attacks on cyber-physical systems. The taxonomy specifies the semantically distinct aspects of attacks on cyber-physical systems that should be described. CP-ADL extends the taxonomy with the means to describe relationships between semantically distinct aspects, despite the complex relationships that exist for attacks on cyber-physical systems. The language is capable of expressing relationships between attack descriptions, including the links between attack steps and the folding of attack details.

1. Introduction

Cyber-physical systems (CPSs) have become increasingly pervasive in modern society. They are used in all kinds of unmanned vehicles and automated manufacturing plants, but more importantly, they are used in the critical infrastructure – electrical power grids, transportation systems and healthcare systems. At this time, only a handful of attacks on cyber-physical systems have been detected "in the wild." Nevertheless, it is reasonable to assume that attacks on cyber-physical systems will rapidly escalate with increasing connectivity and evolving business models. The means of attacks on cyber-physical systems are essentially similar to those used to target information technology and communications systems. However, the goals of

*Corresponding author.
E-mail address: yampolskiy@southalabama.edu (M. Yampolskiy).

http://dx.doi.org/10.1016/j.ijcip.2014.09.003
1874-5482/

cyber-physical attacks and the propagation of their effects are considerably different. The analysis – and ultimately the understanding – of attacks on cyber-physical systems depends on the ability to describe the attacks in a systematic and comprehensive manner.

According to Byres and Lowe [3], attacks on industrial control systems and critical infrastructure assets can be traced as far back as 1995. Currently, the most famous attack is Stuxnet [1,5]. Discovered in 2010, it supposedly operated undetected for more than three years [11]. The most notable aspect of the Stuxnet attack is that it inflicted physical damage to an industrial infrastructure (i.e., uranium hexafluoride centrifuges) via the cyber domain. The March 2000 attack on Maroochy Water Services in Queensland, Australia is another prominent example of an attack on an industrial infrastructure. The attack disrupted pumping operations and suppressed alarms, resulting in the release of untreated sewage into local waterways [17]. The possibility of similar cross-domain attacks on modern automobiles has been reported. Several researchers (see, e.g., [4,10]) have shown that elaborate cyber-attacks can lead to physical consequences, including disabling the brakes of an automobile, killing the engine while the automobile is moving at high speed, permanently locking the doors and manipulating the speed indicator. Other researchers [6,19] have demonstrated the ability to compromise quad-rotor unmanned aerial vehicles (UAVs) and microsatellites.

Huang et al. [8] emphasize that attacks on industrial infrastructures can have economic consequences. Moreover, the attack consequences can be amplified by the interdependencies existing within a single cyber-physical system as well as those existing between multiple cyber-physical systems. Rinaldi et al. [16] specify four types of interdependencies: physical, cyber, geographical and logical. Because of the interdependencies, the effects of an attack can propagate through multiple domains and inflict secondary damage to other cyber-physical systems and infrastructures. Specifically, attacks on cyber-physical system – even attacks executed in cyberspace – can cross domain boundaries, propagating and amplifying the effects in the domains and causing damage in multiple domains.

This paper describes the Cyber-Physical Attack Description Language (CP-ADL), which is based on a taxonomy specified in [20]. The language can express conventional cyber attacks as well as cross-domain attacks on cyber-physical systems. CP-ADL provides a structure for describing a variety of attacks, an important prerequisite for qualitative and quantitative analyses of attacks on cyber-physical systems. These analyses provide valuable knowledge and understanding of the structural properties and probabilities of attacks. Furthermore, the analyses can help identify the degrees to which functionally equivalent architectural elements are vulnerable to various types of attacks. As such, the resulting knowledge and understanding are vital to improving cyber-physical system security and dependability.

2. Related work

In previous work [20], we analyzed the sufficiency of several cyber security taxonomies for describing attacks on cyber-physical systems. Because cyber security focuses only on attacks that execute in and influence the cyber domain, these taxonomies are unable to express cross-domain effect propagation that is characteristic of attacks on cyber-physical systems. To address this deficiency, we created a novel six-dimensional taxonomy for describing cross-domain attacks on cyber-physical systems; Section 3 provides a brief overview of this taxonomy. Since the current knowledge and understanding of cyber-physical attacks are somewhat limited, the taxonomy only defines the dimensions (i.e., the aspects to be described), not the values corresponding to the dimensions. This approach has, in fact, been adopted in the cyber security domain. An example is the taxonomy of Hansman and Hunt [7], which supports structured human-readable descriptions of newly discovered attacks and is used by major entities such as US-CERT.

Although taxonomies specify structures and, in some cases, support elements of the structures, the definition of a description language based on a taxonomy can be a challenging task. The primary purpose of a description language based on the taxonomy defined in [20] is the structured expression of human-readable attack descriptions. Therefore, the description language should support variable-length descriptions in every dimension.

The importance of a description language goes beyond the mere specification of a data format for a taxonomy. Especially important is that a description language provide the capability to express metadata such as the relationships between the elements of various dimensions. As will be discussed in Section 3, this is a critical property for describing attacks on cyber-physical systems, especially if multiple elements must be specified for every dimension of an attack step.

As in the case of taxonomies, the absence of cross-domain considerations in cyber attack description languages hinders their application to the cyber-physical domain. Nevertheless, these languages can provide valuable guidance in developing CP-ADL. Of special interest are the language used to specify US-CERT alerts [18] and the Common Vulnerabilities and Exposures (CVE) description language [12] used in the National Vulnerability Database [15]. Both the languages uniquely identify attacks and describe them in the form of human-readable free text that is separated into semantically distinct sections. A US-CERT alert contains sections that provide the affected systems, attack overview, description, impact, solution, references and revision history. The CVE format provides a structured means to exchange information about security vulnerabilities [9]; a CVE description includes the standard identifier number with a status indicator, a brief description and references to related vulnerability reports and advisories. The Open Vulnerability and Assessment Language (OVAL) uses the publicly released vulnerabilities identified in the CVE list as the basis for most vulnerability definitions [2,13]. An important point is that all the