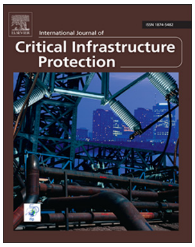
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Vulnerability modeling and analysis for critical infrastructure protection applications

Stefano Marrone[a,*], *Roberto Nardone*[b], *Annarita Tedesco*[b], *Pasquale D'Amore*[b], *Valeria Vittorini*[c], *Roberto Setola*[d], *Francesca De Cillis*[d], *Nicola Mazzocca*[c]

[a]*Seconda Universita di Napoli, Dipartimento di Matematica e Fisica, viale Lincoln, 5, 81100 Caserta, Italy*
[b]*Ansaldo STS, Innovation and Competitiveness Unit, Via Argine 425, Naples, Italy*
[c]*Universita di Napoli Federico II, Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione, Via Claudio 21, 80125 Naples, Italy*
[d]*Faculty of Engineering, Universita campus Bio-Medico di Roma, via Alvaro del Portillo 21, 00128 Rome, Italy*

ARTICLE INFO

Article history:
Received 18 January 2013
Available online 14 October 2013

Keywords:
Railway infrastructure
Physical vulnerability assessment
UML profiles

ABSTRACT

Effective critical infrastructure protection requires methodologies and tools for the automated evaluation of the vulnerabilities of assets and the efficacy of protection systems. This paper presents a modeling language for vulnerability analysis in critical infrastructure protection applications. The language extends the popular Unified Modeling Language (UML) to provide vulnerability and protection modeling functionality. The extended language provides an abstract representation of concepts and activities in the infrastructure protection domain that enables model-to-model transformations for analysis purposes. The application of the language is demonstrated through a use case that models vulnerabilities and physical protection systems in a railway station.

1. Introduction

The impact of the terrorist attacks on September 11, 2011 dramatically underscored the fragility of the critical infrastructure and its importance to modern society. This is especially true of critical infrastructure assets such as railway systems. Indeed, the number of attacks on railway assets during the past decade demonstrates the attractiveness of the infrastructure as a target for criminals and terrorists [6]. The massive crowds, potentially high fatality rates, societal reliance and open and accessible designs are all factors that contribute to the railway infrastructure being considered a soft target for assailants.

Physical protection systems incorporating people, policies and equipment are used to secure critical infrastructure assets from malevolent acts. Despite the increase in threat awareness and published best practices, organizations lack formal approaches for evaluating the effectiveness of decisions regarding the implementation of physical protection systems. Indeed, current assessment practices rely on compliance-based approaches (i.e., presence of appropriate components) and performance-based approaches (i.e., evaluation of the consequences of successful attacks).

This paper describes the results of research conducted under the ongoing EU co-funded project, Methodological Tool for Railway Infrastructure Protection (METRIP) [15], which is focused on developing a decision-making system for physical protection system design. The decision-making system is intended to: (i) suggest the types and dispositions of devices that maximize protection effectiveness; and (ii) help evaluate

[*]Corresponding author.
E-mail address: stefano.marrone@unina2.it (S. Marrone).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.10.001

the effectiveness of a given physical protection system against attacks.

A model-driven framework is presented that enables quantitative evaluations of asset vulnerability. The framework is based on a modeling approach that specifies the three main aspects involved in effective physical protection system design [5]: (i) attacks; (ii) assets; and (iii) protection technologies and devices. The approach extends the popular Unified Modeling Language (UML) by applying profiling techniques [13] to express vulnerabilities and protection schemes. Model-to-model transformations [3] are employed to generate formal analysis models from UML artifacts. The framework for critical infrastructure protection vulnerability analysis and modeling (CIP_VAM) satisfies three main requirements that enable its application in industrial settings: (i) the use of domain-specific terminology and concepts; (ii) the use of standardized techniques and tools; and (iii) the ability to strike the right balance between the desired level of protection and the associated costs.

2. Motivation

There is a significant shortfall of methods for analyzing and enhancing railway security. With regard to the evaluation of vulnerabilities, a crucial requirement is the classification of attack scenarios. To this end, during the first phase of the METRIP Project, we created a database of criminal incidents and terrorist attacks that occurred worldwide from 1970 to 2011. We analyzed 541 incidents in an attempt to correlate the incidents with the primary features of railways (e.g., number of tracks, daily numbers of trains and passengers, station extensions, and numbers and types of implemented protection systems) [4].

Our analysis revealed that the attacks over the last few years have been more lethal. Starting in 2000, the number of attacks and the number of victims per attack have increased steadily. The findings indicate a change in terrorist tactics with an increased emphasis on killing people as opposed to causing economic harm or destroying iconic monuments. The most commonly used weapon type was a bomb, with suicide bombers accounting for the majority of the victims. Medium to small railway stations were targeted most frequently while the most lethal attacks were perpetrated against larger stations. Cameras were found to be the most commonly used protection system; however, security guards proved to be the most effective at preventing attacks and fatalities.

An interesting finding that emerged from the study was that the selection of security systems was usually more directly related to station attributes than to security requirements. To ensure effective protection, it is important to develop better selection criteria based on limiting vulnerabilities while considering station attributes. The CIP_VAM framework described in this paper considers attacks, threats and protection systems to address this limitation and to apply protection measures more effectively.

3. Overview of the approach

Several approaches have been proposed for modeling vulnerabilities and evaluating the effectiveness of security measures. However, the vast majority of traditional models focus specifically on cyber systems or introduce frameworks that can be extended to account for physical protection. For example, LeMay et al. [10] have developed the ADVISE Framework, which employs attack graphs to express and analyze attacker behavior and goals. Similarly, Kotenko and Stepashkin [8] use model checking to conduct cyber security evaluations. However, in the case of physical protection system modeling and evaluation, it is imperative to express all the attributes associated with the underlying framework in a holistic manner.

The proposed CIP_VAM profile facilitates the generation of quantitative models (e.g., Petri nets, Bayesian networks and localization models) for evaluating physical protection system configurations and vulnerabilities. Model-driven engineering and model-to-model transformations are employed very effectively to develop the formal representations.

Fig. 1 shows the METRIP modeling and analysis schema. In general, physical protection system designers and evaluators

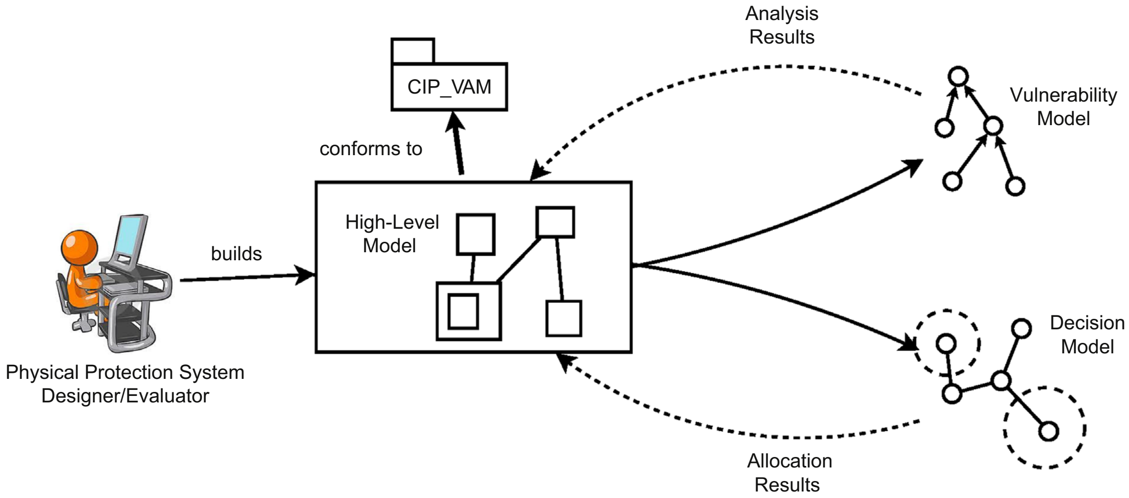


Fig. 1 – METRIP modeling and analysis.