Computers and Electrical Engineering 47 (2015) 275–285

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

On synergies of cyber and physical security modelling in vulnerability assessment of railway systems ☆

Stefano Marrone [a,*], Ricardo J. Rodríguez [b], Roberto Nardone [c], Francesco Flammini [d], Valeria Vittorini [c]

[a] Dip. di Matematica e Fisica, Seconda Università di Napoli, Caserta, Italy
[b] Research Institute of Applied Sciences in Cybersecurity, University of León, Spain
[c] DIETI, Università di Napoli "Federico II", Naples, Italy
[d] AnsaldoSTS, Naples, Italy

ARTICLE INFO

Article history:
Received 30 September 2014
Received in revised form 4 July 2015
Accepted 10 July 2015
Available online 12 August 2015

Keywords:
Cyber-physical systems
Vulnerability assessment
UML profile
Bayesian networks
Generalized stochastic Petri nets

ABSTRACT

The multifaceted nature of cyber-physical systems needs holistic study methods to detect essential aspects and interrelations among physical and cyber components. Like the systems themselves, security threats feature both cyber and physical elements. Although to apply *divide et impera* approaches helps handling system complexity, to consider just one aspect at a time does not provide adequate risk awareness and hence does not allow to design the most appropriate countermeasures. To support this claim, in this paper we provide a joint application of two model-driven techniques for physical and cyber-security evaluation. We apply two UML profiles, namely SecAM (for cyber-security) and CIP_VAM (for physical security), in combination. In such a way, we demonstrate the synergy between both profiles and the need for their tighter integration in the context of a reference case study from the railway domain.

1. Introduction

Cyber-physical systems emerged as a branch of the embedded systems research specifically focused on the interaction between the computational elements and the physical entities [1]. When research on cyber-physical systems overlaps with the emerging paradigms of smart-cities, Internet-of-Things and intelligent transportation, to name a few, then security issues become critical whereas distributed systems can be exposed to both physical and cyber-threats. It is a matter of fact that while researchers seem to be well-aware of the physical effects of cyber-threats, much of the research on information, on "logical", or on "cyber" security are not related to physical sensing. However, many threats to cyber-physical systems (especially when they are isolated from the Internet) are also originated from physical intrusions, e.g., intruders accessing control terminals in technical rooms. This kind of information should be fused with the one coming from logical intrusion detection to provide a superior situation awareness and early warnings; thus, merging physical with logical access control allows to recognise otherwise undetectable identity frauds.

Many safety–critical systems, as the ones used for railway control, are unreachable from the Internet but have technical equipment located in geographically distributed shelters and used for actuation, power, and telecommunications. This

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. J. Garcia-Alfaro.

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

http://dx.doi.org/10.1016/j.compeleceng.2015.07.011
0045-7906/

equipment is normally used by maintainers and other authorised personnel, but can be potentially targeted by unauthorised personnel through the same physical access points. Since trackside shelters and technical rooms are nowadays equipped with physical security and environmental monitoring devices, security threat analysis can be advantageously fed with both physical and logical elements [2].

Nowadays, holistic modelling of complex systems is still a challenging research issue, being largely accepted that the more promising and scalable approaches focus on modularity and composability (both in modelling and solving). Another promising research effort aims at using as much as possible *de facto* standards in systems modelling, as the Unified Modelling Language (UML) together with its extensions and Domain Specific Modelling Languages (DSMLs), in order to provide a modeller with easy-to-use, reusable tools. This enables to build cohesive system views while hiding the underlying complexity of the analysis process, often based on model-to-model (M2M) transformations and orchestration of different solvers for different formalisms biased on the evaluation objectives.

In this paper, we take advantage of two novel UML profiles, namely *Security Analysis and Modelling* (SecAM) [3] and *Critical Infrastructure Protection – Vulnerability Analysis and Modeling* (CIP_VAM) [4], to address the modelling of digital and physical security in combination. The approach moves from separate usage of the two profiles, through a loosely coupled one, pointing towards a fully and strictly integrated profile including the modelling potential of both SecAM and CIP_VAM. Besides, we also show how each profile benefits by the information contained in the other in the formal models generated and used for quantitative security evaluations. We combine the usage of SecAM and CIP_VAM to exploit synergies in modelling and analysis of cyber and physical security aspects: from UML models annotated by both profiles, a cyber and physical security analysis can be performed coping with the complexity of critical infrastructure protection. We finally evaluate our approach in an intrusion scenario in railway trackside/lineside shelters.

The rest of this paper is structured as follows. Section 2 reviews the related work, introduces SecAM, CIP_VAM, and background needed to follow the rest of the paper. Section 3 describes the reference case study of the railway shelter used to motivate our research. Section 4 introduces the vulnerability modelling, considering separately physical and cyber security. Then, Section 5 considers them jointly, and proposes some modelling enhancements. Section 6 demonstrates the effectiveness of our approach by means of sensitivity analyses. Finally, discussion and conclusions are drawn in Section 7.

2. Related work and background

2.1. Related work

Model-based evaluation of computer and network security has a long story, dating back to the first techniques to model and evaluate system dependability [5]. Dependability and security model-based evaluation approaches encompass *combinatorial methods* (e.g., based on Reliability Block Diagrams, Fault Trees, or Attack Trees), *State-Based Stochastic Methods* (e.g., through Markov Reward Models or Stochastic Petri Nets), *Model Checking* (e.g., automatic attack graphs generation [6]), or a combined used of several methods and formalisms [7]. However, security of critical infrastructures like those for mass-transit transportation is a multi-facet problem that requires an integrated approach taking into account digital (i.e., cyber) security as well as physical security, which is strictly related to system protection against intentional threats of physical nature. In physical vulnerability assessment, a *quantitative* notion of vulnerability is used and commonly defined as the likelihood that an attempted attack is successful [8]. In this direction, practical applications for vulnerability analysis use statistical approaches and mathematical modelling [9,10]. Nevertheless, model-based approaches for cyber-security and physical security are separately considered and applied.

A recent trend in critical system modelling for security and dependability analysis envisions top-down model-driven approaches that automatically derive quantitative models. These approaches rely on DSMLs or UML profiles for specification and modelling of a kind of systems. Model-driven processes enable automated modelling and analysis of different solutions during the overall system development life-cycle (for instance, security solutions or design choices) and they maybe easily integrated in industrial settings. So far, few DSMLs or profiles exist specifically tailored for modelling security and vulnerability aspects of critical infrastructures. CORAS [11] assists in modelling and analysing the risk of changing systems in terms of their Quality of Service and fault tolerance characteristics. MARTE [12] is an OMG standard profile for modelling and analysing non-functional properties of real-time embedded systems. Similarly, Dependability Analysis and Modelling (DAM) [13] is a non-standard specialisation of MARTE that supports dependability analysis. Regarding UML profiles addressing security, UMLsec [14] allows to specify security information during the development of security-critical systems and provides tool-support for formal security verification. An UML extension is also proposed in [15] for model-based security assessment. UMLintr [16] is a further profile for specifying intrusion scenarios. Other UML profiles focus on security in grid computing [17] or distributed systems [18]. In this sense, CIP_VAM [4,19] is a recent UML profile that addresses physical protection of critical infrastructures and provides tool support for automatic generation of vulnerability models based on Bayesian Networks (BNs). However, it does not consider cyber-security issues. Another recent UML profile, SecAM [20,3], overcomes this issue since it allows specifying cyber-security aspects while enabling their assessment.

At the best of our knowledge, there are a lot of scientific works comparing UML profiles in different contexts but there are only few of them exploring the synergies of a joint use: in [21], MARTE, SysML, and UMLSec are used to model non-functional properties of telecommunication systems; in [22], MARTE and MARTE-DAM are mixed to allow evaluation of performance