Computers and Electrical Engineering 47 (2015) 286–298

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Assessing and managing the information and communication risk of power generation ☆

F. Baiardi [a,*], F. Tonelli [a], L. Guidi [b], D. Pestonesi [b], V. Angeletti [b]

[a] Dipartimento di Informatica, Università di Pisa, Italy
[b] ENEL Ingegneria e Ricerca SpA, Pisa, Italy

ARTICLE INFO

Article history:
Received 30 September 2014
Received in revised form 6 July 2015
Accepted 7 July 2015
Available online 5 August 2015

Keywords:
Risk assessment
Metric
Intelligent agent
Model based assessment
Monte Carlo method
Industrial control system

ABSTRACT

We describe a model-based assessment of information and communication technology (ICT) risk that produces statistical samples by simulating the attacks of intelligent agents. To support this assessment, we have developed an integrated set of tools, the Haruspex suite. Some of its tools build the models of the target system and those of the agents that other tools apply to simulate the agent attacks. Further tools analyze the output of the simulation. After outlining the proposed approach and the suite, we describe the assessments of two industrial control systems that supervise, respectively, a thermoelectric generation plan and a hydroelectric one. To simplify the presentation of the output of these assessments, we introduce the security stress, a synthetic measure of how a system resists to attacks.

1. Introduction

Intelligent agents are among the most dangerous threats of information and communication technology, ICT, systems because they escalate their privileges, i.e. access rights, through a sequence of attacks that uses the rights that an attack grants to execute the following ones.

To assess the risk due to these agents we propose a model based approach that collects statistical samples by applying a Monte Carlo method to a scenario where some agents attack the target system of the assessment. The method uses abstract models of an ICT system and of the agents in multiple step-by-step simulations of how each agent selects and executes its attacks. These simulations return a sample to compute the statistics to assess and manage the risk. Our approach does not need to collect historical data because it is model based.

The Haruspex suite is an integrated set of tools to support the proposed approach. These tools build the simulation models, apply the Monte Carlo method, and analyze the samples it returns. We describe how the suite assess two critical ICT systems, each acting as an Industrial Control System, ICS, of a power generation plan. Each assessment determines the probability that some attackers acquire the control of the plan and proposes cost effective countermeasures.

This paper is structured as follows. Section 2 briefly reviews works on security metrics, vulnerabilities, and attack simulation. Section 3 describes the Haruspex tools to build the models and simulate the agent attacks. After discussing the

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

[*] Corresponding author.

E-mail addresses: baiardi@di.unipi.it (F. Baiardi), tonelli@di.unipi.it (F. Tonelli), luca.guidi@enel.com (L. Guidi), daniela.pestonesi@enel.com (D. Pestonesi), valentino.angeletti@enel.com (V. Angeletti).

http://dx.doi.org/10.1016/j.compeleceng.2015.07.005
0045-7906/© 2015 Elsevier Ltd. All rights reserved.

selection of countermeasures, Section 4, introduces synthetic measures to simplify an assessment. Lastly, it discusses the validation of the suite. Both sections refer to the same running example to simplify the suite description. Section 5 describes the adoption of the suite to assess and manage the ICT risk of two industrial control systems, ICSs, that supervise and manage, respectively, a hydroelectric power generation plant and a thermoelectric one. After briefly resuming the lesson learned in these assessments, we draw some conclusions.

This work integrates the results outlined in [1,2] and presents them systematically. Furthermore, it applies the suite tools to assess and manage the ICT risk of two ICSs, each supervising a distinct power generation plant. Each assessment considers a scenario where attackers aim to control power generation by acquiring the proper access rights on some ICS components. Each assessment models both insider and external attackers. Lastly, the paper introduces the security stress, a synthetic measure to simplify the communication of the results of an assessment.

2. Related works

This section reviews previous works on the description and the simulation of attacks against ICT system as well as on metrics of ICT robustness. We also review some works on the impact of ICT risk on power generation and smartgrids. While a large number of works has addressed attack simulation, ICT risk assessment and management, just a few works propose an integrated approach to these issues. This integrated approach is the main original contribution of our work on the Haruspex suite.

Refs. [3–5] analyze the simulation of attacks against ICT systems. Ref. [6] discuss intelligent, goal oriented agents with reference to terrorism. Ref. [7] describes attack pre conditions and pairs an attack with the proper countermeasure. Ref. [5] models agents with partial information. These papers do not exploit attack simulation to produce data to assess a system. Furthermore, most tools to analyze privilege escalation do not discover attack sequences. The taxonomy in [8] introduces a classification of vulnerabilities. Ref. [9,10] discuss the modeling and the selection of countermeasures through attack graphs. Ref. [11] considers goal oriented attackers.

Refs. [12,13] review security metrics. Ref. [14–16] propose metrics of the robustness of an ICT system under attack by intelligent agents but they do not integrate these metrics with alternative attacks. The metric in [17] focuses on zero-day vulnerabilities. The one in [18] is similar to security stress as it considers the amount of work to attack a system. Ref. [19] computes the probability that an agent reaches a goal but it neglects alternative attacks for a goal.

Refs. [20–22] discuss the role and the assessment of ICT risk in power generation and smart grids.

3. The Haruspex suite: running experiments

For the sake of brevity, we use *risk assessment* as a synonymous of *probabilistic risk assessment* while *right* and *privilege* are shorthands for *access right*.

The Haruspex suite supports risk assessment and management of an ICT system with reference a scenario where it is the target of some agents that aim to reach their predefined goals. Some tools of the suite build the models of the target system and of the agents. Other tools use these models to implement independent simulations of the agent attacks. These simulations return a statistical sample with information on, among other, the attacks the agents have executed, the goal they have reached and the time this takes. The resulting approach supports a security-by-design strategy to assess an ICT system during its design and before its deployment.

This section briefly describes the *builder* and the *descriptor*, the tools to build the models of, respectively, the system and an agent. Then, it introduces the *engine*, a tool that applies the Monte Carlo method and simulate the agent attacks. The following section describes the tools of the suite that analyze the samples the *engine* returns.

Table 1 defines some abbreviations and the main parameters of the two models. In the following, we use the system in Fig. 1(a) as a running example to describe the tools and the information they return.

Table 1
List of abbreviations.

S	the target system
c	a component of S
ag	a threat agent
g	a goal of an agent
at	an elementary attack
v	a vulnerability
$v(at)$	the vulnerabilities enabling at
$pre(at)$	the set of rights an agent needs to implement at
$res(at)$	the resources to execute at
$post(at)$	the set of rights at grants if it succeeds
$succ(at)$	the success probability of at
$time(at)$	the execution time of at
$\lambda(ag)$	the look-ahead of ag