Accepted Manuscript

Dynamic risk management response system to handle cyber threats

G. Gonzalez-Granadillo, S. Dubus, A. Motzek, J. Garcia-Alfaro,
E. Alvarez, M. Merialdo, S. Papillon, H. Debar

PII: S0167-739X(17)31143-3
DOI: http://dx.doi.org/10.1016/j.future.2017.05.043
Reference: FUTURE 3491

To appear in: *Future Generation Computer Systems*

Received date : 31 October 2016
Revised date : 26 May 2017
Accepted date : 31 May 2017

Please cite this article as: G. Gonzalez-Granadillo, S. Dubus, A. Motzek, J. Garcia-Alfaro, E. Alvarez, M. Merialdo, S. Papillon, H. Debar, Dynamic risk management response system to handle cyber threats, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.05.043

Dynamic Risk Management Response System to Handle Cyber Threats

G. Gonzalez-Granadillo[a], S. Dubus[b], A. Motzek[c], J. Garcia-Alfaro[a], E. Alvarez[a], M. Merialdo[d], S. Papillon[b], H. Debar[a]

[a] *Institut Mines-Telecom, Telecom Sudparis, CNRS SAMOVAR UMR 5157*
9 rue Charles Fourier, 91011 EVRY, France
[b] *Bell Labs, NOKIA Route de Villejust, 91625 NOZAY, France*
[c] *Universität zu Lübeck, Institute of Information Systems,*
Ratzeburger Allee 160, 23562 Lübeck, Germany
[d] *RHEA Group, Avenue Pasteur 23, 1300 Wavre, Belgium*

Abstract

Appropriate response strategies against new and ongoing cyber attacks must be able to reduce risks down to acceptable levels, without sacrificing a mission for security. Existing approaches either evaluate impacts without considering missions' negative-side effects, or are manually based on traditional risk assessments, leaving aside technical difficulties. In this paper we propose a dynamic risk management response system (DRMRS) consisting of a proactive and reactive management software aiming at evaluating threat scenarios in an automated manner, as well as anticipating the occurrence of potential attacks. We adopt a quantitative risk-aware approach that provides a comprehensive view of the threats, by considering their likelihood of success, the induced impact, the cost of the possible responses, and the negative side-effects of a response. Responses are selected and proposed to operators based on financial, operational and threat assessments. The DRMRS is applied to a real case study of a critical infrastructure with multiple threat scenarios.

Keywords: Dynamic System, Automated Response, Risk Assessment, Graph Attack, Security Assurance, Cybersecurity

1. Introduction

In cyber security domains, attack scenarios are frequently represented by the use of attack graphs. Various kinds of attack graphs have been proposed in the scientific literature in order to represent at an abstract level (i.e., not a specific occurrence of an attack scenario, but a template of a possible multi-steps attack) scenarios composed of several elementary attack steps[1, 2, 3, 4]. However, in order to compute the most exhaustive list of possible attack scenarios, attack graphs must rely on algorithms that base their processes on an up-to-date knowledge of the network

Email addresses: gustavo.gonzalez_granadillo@telecom-sudparis.eu (G. Gonzalez-Granadillo), samuel.dubus@nokia-bell-labs.com (S. Dubus), motzek@ifis.uni-luebeck.de (A. Motzek), joaquin.garcia_alfaro@telecom-sudparis.eu (J. Garcia-Alfaro), ender.alvarez@telecom-sudparis.eu (E. Alvarez), m.merialdo@rheagroup.com (M. Merialdo), serge.papillon@nokia-bell-labs.com (S. Papillon), herve.debar@telecom-sudparis.eu (H. Debar)