Chapter 9
Dynamic Risk Assessment in IT Environments: A Decision Guide

Omid Mirzaei
Universidad Carlos III de Madrid (UC3M), Spain

José Maria de Fuentes
Universidad Carlos III de Madrid (UC3M), Spain

Lorena González Manzano
Universidad Carlos III de Madrid (UC3M), Spain

ABSTRACT

Security and reliability of information technologies have emerged as major concerns nowadays. Risk assessment, an estimation of negative impacts that might be imposed to a network by a series of potential sources, is one of the main tasks to ensure the security and is performed either statically or dynamically. Static risk assessment cannot satisfy the requirements of real-time and ubiquitous computing networks as it is pre-planned and does not consider upcoming changes such as the creation of new attack strategies. However, dynamic risk assessment (DRA) considers real-time evidences, being capable of diagnosing abnormal events in changing environments. Several DRA approaches have been proposed recently, but it is unclear which technique fits best into IT scenarios with different requirements. Thus, this chapter introduces recent trends in DRA, by analyzing 27 works and proposes a decision guide to help IT managers in choosing the most suitable DRA technique considering three illustrative scenarios – regular computer networks, internet of things, and industrial control systems.

DOI: 10.4018/978-1-5225-4763-1.ch009

INTRODUCTION

Information Technology (IT) deals with the use of computers to store, manipulate and retrieve any kind of data, ranging from business to personal, and in most cases, sensitive data. This field is receiving more attention in recent years due to the emergence of computer networks, wireless networks, and interconnected smart devices also known as the Internet of Things (IoT). In particular, Industrial IoT (IIoT), known as 4th Industrial Revolution (4IR), has received significant attention. In 4IR, real and virtual capabilities are merged into Cyber-Physical Production Systems (CPPS) through extensive usage of cloud services and applications, and, also, big data analytics (Sadeghi, Wachsmann, & Waidner, 2015).

In order to make sure that 4IR helps in achieving both economic and social improvements, authorities must anticipate and cover all involved security risks. Particularly, security of information needs to be addressed in order to provide a satisfying degree of reliability, confidentiality, integrity, and availability (Gehling & Stankard, 2005). It must be noted that numerous threats may affect these four factors. Thus, passive attacks (e.g. eavesdropping) or active ones (e.g. packet injection) may harm this environment (Deka, Kalita, Bhattacharya, & Kalita, 2015), (Nadeem & Howarth, 2013).

Regardless the type of threat or attack, they impose a magnitude of unreliability to information which is commonly known as "risk". Speaking more precisely, the term "risk" is an estimation of the degree of exposure to a threat that may occur on one or more assets causing damage to an organization (Awan, Burnap, & Rana, 2016). In a computer network scenario, an asset may be any of its components (e.g. hardware devices or their software) as well as other related elements such as the network users.

Managing risks is critical to ensure the overall corporate security. For this reason, information security governance is already assumed to be an integral part of the corporate IT governance (Von Solms, 2005). In particular, Wilkin et al. highlight that risk management forms this process along with other corporate aspects such as strategic alignment, value delivery, resource management and performance measurement (Figure 1) (Wilkin & Chenhall, 2010). Thanks to risk management, it is possible to properly handle risks as it serves to identify, assess, prioritize, mitigate and track them (Garvey, 2008). Among these steps, risk assessment deserves special attention since it involves measuring an intangible factor – the degree of risk posed by an action (S. Fu & Zhou, 2011), (Benini & Sicari, 2008). This complex task is essential for responding to the threat (Shoemaker & Conklin, 2011).

Currently, there are two major risk assessment approaches, namely static and dynamic ones (Alireza Shameli-Sendi, Naser Ezzati-jivan, Masoume Jabbarifar, & Michel Dagenais, 2012). In a static system, risks are evaluated based on static values of factors related to risks, including assets, threats, and vulnerabilities. Today, with the dynamicity of threats, there is an urgent need for Dynamic Risk Assessment (DRA) processes. Particularly, choosing an appropriate risk assessment method in IIoT systems is challenging since they provide different attack surfaces at multiple abstraction layers ranging from electronic devices (e.g. processors and memories to process data and sensors and actuators to control physical processes) to software (e.g. operating systems and applications), humans, and, last but not least, network connections (e.g. WiFi). In such a context, adapting classic static risk assessment methods is not straightforward, and, thus, requires another method, at an additional cost, which allows systems to update the risk level at real-time, as well as dealing with the changing nature of security threats (Holgado, Perez, Perez, & Villagra, 2015) and various abstraction layers which are usually involved.

Due to the importance of risk assessment process, several surveys have been published dealing specifically with security risks in information systems and computer networks. For instance, information security risk assessment concepts are presented in (Zhiwei & Zhongyuan, 2012), (Behnia, Rashid, &