Threat and Risk Assessment Using Continuous Logic

Aristides Dasso
Universidad Nacional de San Luis, Argentina

Ana Funes
Universidad Nacional de San Luis, Argentina

INTRODUCTION

The chapter presents a method to help assessing threats and their associated risks. Threat and Risk Assessment encompass a wide area, ranging from building construction to network and computer security through automotive design and construction, and many others such as Supervisory Control And Data Acquisition (SCADA), Energy Management System (EMS) systems among others, many of them closely associated with computer and networks systems.

Assessing threats and the risks associated to them implies several tasks such as identifying threat and risks, detecting them and their level of danger to a particular organization cybersecurity system, as well as to decide what to do with a specific threat, the costs of prevention or correction, the consequences of the actual risks occurring or, alternatively, not paying any attention to them, disregarding them.

Properly identifying, recognizing, making out a possible threat is the first step in this process; consequently, to have a list of characteristics, traits, attributes or requirements can be of help in that task. Therefore, it is necessary in first place to clearly define the set of requirements that can be of use in identifying threats and their related risks. Second, it is important to have a method that using those requirements eases the building of a model that assist people in charge with the job of assessing threats and risks in order to make well informed decisions on the matter.

The method proposed here is aimed at giving help in the area of cybersecurity and it is based on the Framework for Improving Critical Infrastructure Cyber security developed by the National Institute of Standards and Technology (NIST). The proposal integrates this framework with a quantitative method based on the use of a Continuous Logic, the Logic Scoring of Preference (LSP) method. LSP is a method suitable for decision making that provides the guidelines to produce a model/tool to assist the expert in the process of assessing how much a product or system satisfy a number of requirements, in this case associated to the identification, protection, detection, response and recovery of threat and risks in an organization. More specifically, the proposal is aimed to supplement steps 3 to 5 in the NIST program (NIST, 2018) with the necessary activities to develop a quantitative LSP model for assessing threat and risks in an organization. Therefore starting from a set of requirements taken from the NIST Framework, and applying the LSP method, a decision model can be developed. The resulting model can be used as an effective tool to assist professionals in the process of assessing potential threats and risks involved in any kind of organization, be it industrial, service, utilities, etc., providing a global indicator as well as a set of partial indicators, for each system under evaluation. These indicators are values in the interval [0; 100]; the global indicator represents the stage in which a system under evaluation is with respect to

DOI: 10.4018/978-1-7998-3473-1.ch083

the whole set of critical threat and risk requirements identified and, in the case of the partial indicators, to cohesive subgroups of requirements.

BACKGROUND

The next two subsections discuss related work on threat and risk assessment and introduce some concepts of the LSP method necessary to understand the rest of the work.

Threat and Risks Assessment

Threat and Risk Assessment is part of an ongoing process of identifying, assessing, and responding to risk. Threat and Risk Assessment in cyber security contexts is becoming more and more a concern for organizations of any kind, i.e. industrial, utilities, service oriented, etc., since computers and networks have penetrated nearly every activity. Organizations increasingly have the need to assess the potential threats and the risks involved in their processes and infrastructures. Not only commercial and government institutions but also utilities are aware of the potential threats to their infrastructures. Many open source and proprietary methods exist today to perform a risk and threat assessment, some focused on specific types of risk and some focused on specific business sectors. Of course the problem of threat and risk assessment is also considered in settings where security is a concern in a wider sense, for instance the threats and risks confronted in cyber terrorism, cyber war, and other similar scenarios; an overview of this can be found in Lewis, J. A. (2002). The threats and risks involved in unmanned aerial vehicles (UAVs) are also considered in Hartmann, K., Steup, C. (2013). In Ciapessoni, E. et al. (2018) the authors developed a method based on probabilities considering that threats can go from natural disasters to deliberate acts of sabotage.

There are also US patents on the subject such as Magdych et al. (2003), and Kelley, J. D., Lahann, J. S., Mackey II, D. H. (2006).

In Cherdantseva, Y. et al. (2016) there is a review of Threat and Risk assessment methods for Supervisory Control And Data Acquisition (SCADA) systems of great size and scope. It must be considered that SCADA systems are prone to attacks that can have serious consequences, e.g. Stuxnet malware (Zetter, K. 2019). Also Bayne, J. (2002) furnishes an overview of the whole process of Threat and Risk Assessment. There are also guides to risk management such as ISO 31000 (2018).

There is an extensive literature on security and network structure concerning smart grid environments, e.g. a Threat and Risk Assessment methodology, presented in Smith P. (AIT), Editor. (n.d.), where a "threat identification approach, based on attack graphs" is proposed. They use *Semantic Threat Graphs* (STGs) as "a tool to precisely determine the necessary countermeasures for the identified threats".

Also the European Network and Information Security Agency (ENISA) analyzes in ENISA (2010) the future risks in a scenario of future air travel, were Internet of Things (IoT) and Radio Frequency IDentification (RFID) technologies are used. The methodology employed is based on the standard ISO/IEC 27005:2008 Information technology — Security techniques — Information Security Risk Management. A very detailed "Vulnerabilities and Threats List" has been developed. A "Risk Identification and Assessment" is considered based on three elements, i.e. Risk = f(Asset, Vulnerability, Threat). A spread sheet was elaborated as part of the development (ENISA, n.d.).