Modern businesses and enterprises are dependent on information technology and systems (ITS), and they are developing into complex socio-technical systems comprised of human factors, ITS systems, and platform infrastructure. The complexity of modern systems and the forever improving computing capability creates an opportunity for attackers to exploit multiple vulnerabilities concurrently. To defend against attackers, risk managers need to predict possible attack vectors. For risk managers to combat attackers' activities, attack-defence trees are formalised as a tool to identify, model, and quantify complex attack scenarios (Fraile et al., 2016).

The importance of cyber and information security to modern enterprises has made them a fundamental part of the investment in information technology and systems. The reporting of successful attack cases against businesses and governments demonstrates the importance of providing and assuring adequate protection to the information and technology assets. A risk management process that enables security managers to be aware of possible risks by identifying, describing, and analysing the potential vulnerabilities that must be reduced or mitigated is required (Bistarelli et al., 2012). The ultimate goal of such a risk process is to guide towards the adoption of a set of countermeasures that may mitigate risk or reduce it to an acceptable level. The attack-defence tree provides risk managers with the capability to measure the impact of such countermeasures on the attacker's actions (Aslanyan et al., 2016).

Bibliography :

Aslanyan, Z., Nielson, F., & Parker, D. (2016). Quantitative verification and synthesis of attack-defence scenarios. *Proceedings - IEEE Computer Security Foundations Symposium*, *2016-August*, 105–119. https://doi.org/10.1109/CSF.2016.15

Bistarelli, S., Fioravanti, F., Peretti, P., & Santini, F. (2012). Evaluation of complex security scenarios using defense trees and economic indexes. *Journal of Experimental and Theoretical Artificial Intelligence*, *24*(2), 161–192. https://doi.org/10.1080/13623079.2011.587206

Fraile, M., Ford, M., Gadyatskaya, O., Kumar, R., Stoelinga, M., & Trujillo-Rasua, R. (2016). Using attack-defense trees to analyse threats and countermeasures in

an ATM: A case study. *Lecture Notes in Business Information Processing, 267,* 326–334. https://doi.org/10.1007/978-3-319-48393-1_24