Title: Improving risk assessment model of cyber security using fuzzy logic inference system

Author: Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab A.L. Rassan, Md. Zakirul Alam Bhuiyan

PII: S0167-4048(17)30200-6
DOI: https://doi.org/doi:10.1016/j.cose.2017.09.011
Reference: COSE 1207

To appear in: *Computers & Security*

Please cite this article as: Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab A.L. Rassan, Md. Zakirul Alam Bhuiyan, Improving risk assessment model of cyber security using fuzzy logic inference system, *Computers & Security* (2017), https://doi.org/doi:10.1016/j.cose.2017.09.011.

Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System

Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab AL Rassan and Md. Zakirul Alam Bhuiyan*

[1]College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

[*]Department of Computer and Information Sciences, Fordham University, New York, USA

Email: {434910564, ahalmogren, mmhassan, irassan}@ksu.edu.sa, mbhuiyan3@fordham.edu

Abstract. This paper describes the impacts of criminal activities based on the nature of the crime, the victim, and the basis (whether short-term or long-range/term) of the impacts of cybercrime on Internet. Recently many countries are facing numerous cyber threats including DoS (and DDoS), malware, website defamation, spam and phishing email attacks. Due to these cybercrimes evolution, identifying and assessing security risk is crucial to access data from new technologies, and also trying to understand how technologies can be abused. Therefore, there is a need to develop a special cyber security risk assessment model to tackle over these cyber threats. In this paper, we propose to utilize Fuzzy Inference Model (FIS) to produce risk assessment result based on the four risk factors which are: vulnerability, threat, likelihood and impact to specify the range of risks that can threaten any entity and try to solve such issues to proposed entities. We have performed various analysis on this factors and finally, our evaluation results show the viability of our proposed approach.

Keywords: Cyber security, Cybercrime, Risk assessment model, Fuzzy logic inference, Risk factors evaluation.

1 Introduction

The modern technology is undergoing undisputed evolution and this can cause more challenging cyber vulnerabilities. Nearly 40% of states throughout the globe are expecting cyber-attacks, and this makes cyber security a global matter demanding integral efforts at all levels [1-3]. Cyber security is a global issue that, according to Information Systems Audit and Control Association (ISACA), can only be faced when all join efforts in closing the global skill gap and prepare cyber security experts with the guidance and knowledge they require [3].

The problem seems somewhat exaggerated in the Middle Eastern regions where cybercrime has been on a notable rise over the last two decades. Experts have predicted a continuous increase of cyber insecurities with regional disturbances such as the Arab Spring that target government websites [6]. The argument gains momentum as regional studies have set off to determine cyber vulnerabilities at a state level and suggest counter strategies to support the power of the global movement to attain higher cyber infection [4].

Risk analysis utilizes techniques that help people to manage uncertain events [50-52]. It is a method that is used to assess factors that lead to a loss or that hinder the success of a project of business. Organizations employ it to decide whether to proceed with a particular decision or not. Through the process of risk estimation, support is provided to help in making decisions [53-55].