Chapter 2
A New Meta-Heuristics for Intrusion Detection System by Scenario Inspired From the Protection System of Social Bees

Ahmed Chaouki Lokbani
Dr. Tahar Moulay University of Saida, Algeria

Mohamed Amine Boudia
Dr. Tahar Moulay University of Saida, Algeria

ABSTRACT

In this paper, the authors propose a meta-heuristic for intrusion detection system by scenario, inspired by the protection system of social bees to their hive. This approach is based on a specialized multi-agent system where the authors give limited responsibility to each guard bee agent: to secure only one port. This specialization aims to better exploit the training set and the hardware and software performance. The authors start this paper with a short introduction where they show the importance of IT security. Then they give a little insight into the state of the art, before starting the essential part of a scientific paper: "Our Approach," where they explain the natural model. Finally, they simplify their model in a modelling table to share their vision and philosophy to switch from natural model to artificial model.

INTRODUCTION AND PROBLEM

After that people realized that the "war: a massacre of people who don't know each other for the profit of people who know each other but don't massacre each other" Paul Valery. They have decided to change the field of wars form reality to virtual world. today the development of science gives birth to an electronic war. we can even predict that World War III will be purely electronic.

A proverb known and recited in the area of intelligence and espionage issues: "Who has information wins the war". The human had known lot of wars. The development of wars and strategies are based on the sensible information of the enemy and gives a favour to the camp that holds the last update of

DOI: 10.4018/978-1-5225-3004-6.ch002

information. In the history the data holder was always leaking under attack to intercept, modify or destroy information.

Nowadays everything, is computerized, personal information from birth to death: name, address, weight, height, date of birth, CV, health.... Are computerized and stored in servers and even money and fortune became as property files or tuples in a databases for mayor or numbers to the bank. It will not stop there, the arrival social networks and computerized our personal lives, opinions and feelings. We the IT professionals, aims to replicate the world in virtual mode. What makes servers and computer systems have become targets of attacks and crime.

This also leads us to predict the end of the old-style crime where robbers have to be writer and director and main actor, the end of improvisation as well, and the end of exposing the victim and criminal's life at risk. At present, The robber must have a great knowledge of computer science, he must write an algorithm instead of scenario, it must be implemented his computer programs and skipping all the security protocols. Now, robbers are able to work from a warm office listening to a Mozart symphony and drinking a cup of coffee. the challenge is big!!!!!

Electronic crime generally begins as a trend and a challenge between young and novice hackers, but it is rapidly evolving to the point where it becomes the subject of secret international tenders for large institutions and even countries. Companies and countries are under attack which can result in significant losses. The establishment of IT security has become more important than the establishment of the internal security for the place and people (scanner, metal detector, door guard,, weapon, intelligence ...). Must control the input data stream and the output data stream of the telephone cable, or fiber optic and wireless connections that the company spend a large sum to get them, for the installation and maintain them; all that with their total grateful(company), more than that, that she considers it like a pride and added value in its performance.

A good IT security is based on the robustness of the implementation of security policy, it is designed and defined by a number of characteristics: it occurs when the levels, the objectives of this polished and finally tick the tools used to ensure safety.

To ensure a protection of company data, different tools are available. They usually used together, in order to secure the various existing flaws in a system. But the first and the most important tools in the security system is the IDS (intrusion detection system); firstly because the majority of attacks are made after an intrusion or by introducing a malicious program and secondly because the IDS is the only tool that ensures permanence. It is responsible for start or stop strategies and response in case of attack.

IDS stands for Intrusion Detection System. It is an equipment that ensures on-the activity of a network or a given host to detect intrusion attempts and possibly react to this at-tempt. There are different kinds of IDS in the literature, it differs in the area of monitoring, operating mode or answer mode.

The theory cites two response mode: where the passive save attack in a log file that will be analysed by the security manager. And active response: rather aim is to stop an attack at the time of detection: by interrupting a connection where even against attack. We can classify the IDS by the response mode: passive IDS where IDS save intrusion and communicates it to the manager of IT security, and Active IDS that make an action when an intrusion is detected. While re-looking scientific and the software industry there are only passive IDS answer.

The approach of the security of information systems that prevails today is too passive. We expect to detect an attack while we trust the multiple protection tools that we have developed and which are not infallible.