Chapter 40
An Approach based on Social Bees for an Intrusion Detection System by Scenario

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

Ahmed Lehireche
University Djillali Liabes of Sidi Bel Abbes, Algeria

Reda Mohamed Hamou
Dr. Moulay Tahar University of Saïda, Algeria

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

ABSTRACT

The aim of the authors' work is to model the intrusion detection system by scenario with a bio-inspired method in this case the system of protection of social bees. The natural pattern of social bees produces security efficiency by its three filters. In this paper, the authors focus on scenario approach they chose as a strategy to intrusion odor recognition of bees. They propose a new philosophy based on limited responsibility for each agent. This proposition aims to better exploit the performance of their hardware, and to use intelligently a kddcup'99 corpus.

INTRODUCTION AND PROBLEMATIC

The human being, during the history, had known lot of wars. The development of wars and strategies gives a favour to the camp that holds the last update.

After the two world wars and the Cold War, today the development of science gives birth to an electronic war, even it is predicted that World War III will be purely electronic. In the story the data carrier was leaking under attack to intercept, modify or destroy information. Nowadays everything, especially in the developed countries, everything is computerized, personal information from birth to death: name,

DOI: 10.4018/978-1-5225-9866-4.ch040

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 personal lives, opinions and feelings. We are IT professionals; we aim to replicate the world in virtual mode. What makes servers and computer systems have become targets of attacks and crime.

Electronic crime is a mode and a challenge between young hackers, but do not neglect it gets a nerve of the competition between companies and secret services of the countries. Companies are under attack which can result in significant losses. The need for companies in IT security is becoming increasingly important. The implementation of a comprehensive security policy is difficult enough, essentially, by the diversity of aspects to consider. A security policy can be 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 proper protection of company data, different tools are available. They usually used together, in order to secure the various existing flaws in a system. The centre piece of a security system is the IDS (intrusion detection system); it is the only tool that ensures permanence. It is responsible for start or stop strategies and response tools 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 IDS: where passive IDS save detected intrusions in a log file that will be analysed by the security manager. And active response: The active response rather aim is to stop an attack at the time of detection: by interrupting a connection where even against attack. 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 (blindly) the multiple protection tools that we have developed and which are not infallible.

It is necessary to change our assumptions and our security models of information systems. For this, a new proactive approach is essential. The active response, also called offensive defence, is legal according to the law made in 2011. The US Department of Defence of the United States (DoD) published its strategy for operating in cyberspace. They announced to set up Active defence capabilities to block intrusions to its computer networks and systems.

If you back up toward the end of the second paragraph of this introduction, you will find a striking sentences: “We are IT professionals, we aim to replicate the world in virtual mode” we are computer scientists and we adhere and contribute to this goal too. We had searched in nature a strong security system having an offensive defence. We were attracted by a quote from Albert Einstein that “if bees disappear, mankind has for four years to live,” how social bees can protect themselves and their honey facing the law of the strongest?

None of us have little reason not dare to approach an unprotected hive, because not only will not but it will be pursued and attacked hundreds of meters by the inhabitants of this hive who sacrifice themselves for the safety of their hive. This inspired us to model an intrusion detection system based on a meta-heuristic, in this case the system of protection of social bees.

In this paper we propose a theoretical model modelling a new intrusion detection system based on bio-inspired metaheuristic namely “social bees” that we nicknamed it “IDSbee” having an active response mode; and we propose dubbed the given computer system of this IDSbee a “hive” system.