Abstract

Algorithms for computer program infection detection inspired by biological immune mechanisms

mgr inż. Patryk Widuliński

Computer systems are very popular these days. Unfortunately, with their increased popularity has come the emergence of actors who, for different purposes, often seek unauthorized access to user data. IDS (intrusion detection systems) have been developed to address these threats. In recent years, researchers have been inspired to find modern solutions to detect intrusions. Researchers have noticed some parallels between the goals of IDS and biological immune systems. This has led to the development of artificial immune systems (AIS). The aim of the thesis was to analyze existing and develop my own algorithm for detection of computer program infections, inspired by defense mechanisms of living organisms. The thesis states that it is possible to implement algorithms for detection of computer program infections with properties comparable or better than known solutions, including solutions using AIS known from the literature. In this dissertation, a comprehensive review of the literature on IDS and AIS, and in particular the most popular AIS algorithm, the negative selection algorithm (NSA), has been conducted. A custom intrusion detection system was then proposed to detect infections in the operating system. A random method and a template method were implemented in the system, and a proprietary improvement of these methods using an additional set of intercellular receptors was presented. The system was thoroughly tested for a wide range of receptor generation input parameters, and performance was compared with other solutions known from the literature. The experimental studies showed that the IDS system achieves comparable or better results than those known from the literature. Based on the experimental studies, it was concluded that the goal of the thesis was achieved and the thesis was proven. Further research may consider the ability of the IDS to repair infected files in the operating system.