Ministry of National Defence
Military Technical Academy „Ferdinand I”

THESIS SUMARRY

„ Contributions on Self-adaptive honeypot systems”

Author: Eng. Adrian PĂUNA
Email: adrian.pauna.ro@gmail.com
PhD. supervisor: prof. univ. dr. ing. Victor-Valeriu PATRICIU

In the current global economic context, where the impact of cyber attacks is exponentially increasing, it is critical to detect and particularly understand their nature. Therefore, honeypot systems are probably the most used mechanism for studying the elements of a cyber attack.

Due to their steady development over the past forty years, honeypot systems have evolved from simple computers exposed over the Internet with the purpose of being attacked and monitored simultaneously, up to the level where such systems can interact autonomously with attackers, using the current developments in the field of artificial intelligence.

Our paper presents a series of honeypot systems called self-adaptive, developed during our scientific research. Such systems are based on the use of reinforcement learning algorithms aiming to enable autonomous interaction with the attackers. The paper presents in each of the four chapters of contributions a theoretical description of the machine learning elements used, as well as the architecture of the honeypot systems developed, their implementation and a series of tests and results.

Chapter 1 Introduction presents a description of the modules making up the architecture of self-adaptive honeypot systems. Also, the chapter includes basic elements related to the machine learning algorithms used for developing each self-adaptive honeyot system.

Chapter 2 Honeypot Systems includes a brief presentation of the concepts related to honeypot systems. It also details the evolution of honeypot systems from the beginning of the 80's to nowadays' honeypots, including a classification of honeypot systems into six categories by different defining elements. The chapter continues with a presentation of the most commonly used types of honeypot systems, namely low-interaction and high-interaction honeypot systems, respectively. The chapter ends with a detailed presentation of self-adaptive honeypot systems modelling, taking into account the machine learning paradigm.

Chapter 3 RASSH - reinforcement learning self-adaptive honeypot system presents in the first part the theoretical elements related to the reinforcement learning algorithms used for modelling and implementation of the RASSH system. This chapter also describes general notions concerning the Markov decision process, Value functions and Action-Value functions, exploration / exploitation dilemma. Their

presentation is necessary for understanding how the machine learning algorithms work. We also detailed the SARSA (State-Action-Reward-State-Action) algorithm, as its implementation is used in the machine learning mode operated by RASSH.

The chapter continues with the presentation of the honeypot system modelling as a machine learning agent and its implementation details, with a few conclusions regarding the utility of the honeypot system implemented.

Chapter 4 QRASSH - self-adaptive deep-reinforcement learning honeypot system analyses the defining elements of Deep Reinforcement Learning (DRL) algorithms. DRL algorithms are basically an upgrade of the basic RL algorithms, by introduction of neural network elements. That significantly improves their performance, making them suitable for production implementations. The chapter continues with the presentation of the architecture and modelling of the QRASSH system, highlighting elements related to the DQN (Deep-Q-Learning) algorithm used to determine the actions performed by the honeypot system in contact with the attackers. We also included a series of tests performed on the honeypot system exposed over the Internet. Finally, the conclusions of the QRASSH implementation and testing are presented.

Chapter 5 CASSH - Self-adaptive honeypot system capable of reasoning describes in the first part a series of elements defining the Case Based Reasoning algorithms. The CBR cycle diagram is detailed, emphasizing the four R's: Retrieve, Reuse, Revise, Retain. The architecture and implementation of the self-adaptive CASSH honeypot system are further presented, followed by a detailed description of the paradigm of the belief-desire-intention (BDI) agents, in conjunction with the CBR algorithms. The chapter ends by highlighting certain elements regarding the results of the tests carried out.

Chapter 6 IRASSH - Self-adaptive honeypot system used to optimize reward functions begins by describing in detail the algorithms of Apprenticeship Learning via Inverse Reinforcement Learning. The task of such algorithms is to determine a reward function from an observed behaviour. The chapter continues with the mathematical modelling as well as the architecture and implementation of the IRASSH system. This self-adaptive honeypot system works based on a three-phase flow. In Phase 1, the self-adaptive honeypot system agent is manually trained. Basically, the honeypot system is presented the sequence of actions to be taken in different situations of interaction with the attackers. In Phase 2, based on a previously learned policy, a series of weights are generated for each feature, using inverse reinforcement learning algorithms. Based on such weights, the optimal reward function is generated. In Phase 3, the reward function obtained in Phase 2 is used by the IRASSH agent in production and thus verified. The chapter ends with a few conclusions and elements regarding the utility of the IRASSH system.

Chapter 7 Conclusions presents the final conclusions of our research paper, highlighting also the original contributions that have been made to the subject matters approached by the paper, the list of publications during the PhD training, as well as the bibliography consulted during the entire scientific research process.