Journal of King Saud University – Computer and Information Sciences (2015) 27, 386–392

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

# Optimization of rootkit revealing system resources – A game theoretic approach

K. Muthumanickam *, E. Ilavarasan

*Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry 605 014, India*

Received 22 January 2014; revised 10 June 2014; accepted 23 October 2014
Available online 10 September 2015

**KEYWORDS**

Computer security;
Non-cooperative game theory;
Rootkit;
Resource optimization;
Windows OS

**Abstract** Malicious rootkit is a collection of programs designed with the intent of infecting and monitoring the victim computer without the user's permission. After the victim has been compromised, the remote attacker can easily cause further damage. In order to infect, compromise and monitor, rootkits adopt Native Application Programming Interface (API) hooking technique. To reveal the hidden rootkits, current rootkit detection techniques check different data structures which hold reference to Native APIs. To verify these data structures, a large amount of system resources are required. This is because of the number of APIs in these data structures being quite large. Game theoretic approach is a useful mathematical tool to simulate network attacks. In this paper, a mathematical model is framed to optimize resource consumption using game-theory. To the best of our knowledge, this is the first work to be proposed for optimizing resource consumption while revealing rootkit presence using game theory. Non-cooperative game model is taken to discuss the problem. Analysis and simulation results show that our game theoretic model can effectively reduce the resource consumption by selectively monitoring the number of APIs in windows platform.



## 1. Introduction

Today, approximately 90% of the operating systems in the Internet run windows operating system (W3Schools). This enables the remote attacker to easily damage many computer systems after getting an entry point in a victim computer. Malicious rootkits refer to a collection of software routines designed to hide their presence and other malicious activities and enable the attacker to take control of the victim computer (Emigh, 2006). Moreover, rootkits can also be used as backdoor to spy user or system's activities (Quynh and Take Fuji, 2007). The attacker can then capture sensitive information about either end-user or computer. As 85% of malicious software is being developed today with the intention of affecting windows operating system to harvest money (Wang and Dasgupta, 2007), we focus on the area of windows rootkit detection. In order to launch malicious activities, windows rootkits adopt a mechanism called 'hooking' which can modify the predefined execution path of a system call. However,

* Corresponding author.
E-mail addresses: kmuthoo@pec.edu (K. Muthumanickam), eilavarasan@pec.edu (E. Ilavarasan).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.10.004

rootkits need to access Native APIs to accomplish their tasks. There have been many approaches proposed in the past which rely on signature-based method. There were some effective anti-rootkit tools also available to dynamically analyze the behavior of Rootkit Malwares. However, they failed to detect native API hooks dynamically. Therefore, finding a mechanism that is capable of detecting malicious Native API hook rootkits to prevent both user-space and kernel-space is a challenging problem. To analyze the economic aspects of windows malicious rootkit activity and optimize the resource to be monitored, we investigate a game theoretical approach that models the relationship between the defender and the attacker. Our game theoretic approach will guide the defender to have optimal resources to reveal the presence of a rootkit. In order to attain the ultimate goal, an attacker might maximize his protection by utilizing maximum resources in the worst case whereas the defender's goal might be to optimize rootkit detection by resource consumption, i.e., by monitoring minimal number of APIs. When a Rootkit Revealing Module (RRM) is running on a host computer, it is necessary to continuously monitor more number of user-space objects and kernel-space objects, regardless of the possibility of an attack. To deal with this issue, we propose a game theoretical approach to reduce the monitoring APIs being monitored by RRM without loss of its detection accuracy. The monitored APIs are chosen according to the amount of resource consumed and the expected largest probability to attack. A game theoretic model to the Intrusion Detection System assists in the decision process of allocating limited resource for detecting significant threats in a large network in linear time. So, we have chosen a game theoretic approach to model the interaction between RRM and Rootkit Malware (RM) API hook attack to find the optimal number of APIs to be monitored. Here the two players are: the RRM and the RM. In this model, the RRM can choose to monitor the system or not, and for how long to monitor. On the other hand, the RM can choose to attack or not, or delay the attacking time to evade the RRM. As computer attacks are launched repeatedly, we select a repeated non-cooperative game model. The final outcome guides the RRM to use minimal number of APIs with respect to the attack scenarios.

The rest of the paper is aligned as follows: Section 2 discusses related work. Section 3 defines the problem statement. We explain a game theory model in Section 4. Furthermore, a case study is presented in Section 5. Section 6 presents the simulation results. Finally, in Section 7 we conclude the proposed work.

## 2. Related works

As malware writers have devised new methods to violate computer security policies, many researchers focused developing a new technique to combat them. An intrusion system based on Bayesian probability has been proposed (Altwaijry and Algarny, 2012) in which naïve Bayesian classifier is mainly used to identify four different classes of attacks. The system was trained using KDD data set to achieve better detection rate. The authors of Abdullah Al-Kadhi (2011) proposed an assessment report on spam in the Kingdom of Saudi Arabia. The study paper also discussed about anti-spam efforts in different countries and emerging anti-spam technologies. The paper provides a basis for researchers who look for knowledge in spam type of attack. Another approach (Alfantookh, 2006), particularly for detecting DoS attacks was proposed. Their system used the idea of neural network to classify known and unknown attacks from network traffic packets and achieved better results. In this context, only few works addressed the issue of resource optimization. Today, game theory is being effectively applied to address many real world issues. There have been plenty of ideas proposed in the field of computer security especially in the area of Intrusion Detection Systems (IDS). But limited methods existed to model malicious rootkit detection in windows platform using game theory. Game theory gained authenticity because of John Von Neumann and Morgenstern and they published a book in 2004 (Neumann et al., 2004). Thereafter, it has been applied in the fields of biology, economics, sociology, etc (Game theory). A game is played between two or more players with different strategies. A payoff/reward has been awarded to the player for each and every action within the game. The payoff may be either positive or negative value. The game solution guides each player to know their optimal strategy against the opponent.

Intrusion detection has long been an active research topic in the detection of potential attacks. There have been limited approaches addressing the use of game theory to improve the performance of the detection module. Liu et al. (2002) presented a game model to optimize intrusion detection strategies in a closed network. In Liu (2005), authors discussed a game theoretic approach to predict cyber attacks. In Kodialam and Lakshman (2003), authors developed a game theoretic framework to formulate the game interaction between the intruder and the service provider. The optimal strategy of the intruder is to minimize the probability of being detected and the service provider's objective is to maximize the detection probability. In Alpcan and Baskar (2004), the authors modeled a non-cooperative and non-zerosum game to discuss continuous-kernel version. The authors proved the existence of the Nash Equilibrium and discussed the dynamics of the game. Few approaches (Pacha and Park, 2006; Liu et al., 2006) have been proposed over ad-hoc networks. Liu et al. (2008) proposed a non-cooperative game model to enable the Host Intrusion Detection System to optimize the resources to be monitored. Also, a multi-stage buffer overflow attack was taken as a case study and it was concluded that their model utilizes minimal objects. In Chen and Leneutre (2009), authors addressed the intrusion detection problem in heterogeneous networks using game theoretic approach. They discussed the problem as a non-cooperative game between the attacker and the defender. To achieve optimal system value, they derived optimal strategy for the defender and minimal resource consumption. Otrok et al. (2008), presented game theory model to discuss the issues of detecting intrusions in wired network. A sampling strategy has been derived to reduce the success rate of the defender. From the literature survey, we ensure that none of the work addresses the problem of optimizing the number of system resources especially the number of APIs to be monitored while revealing a rootkit presence. Motivated by this, we propose a game theoretic model to detect rootkit presence by monitoring minimal number of APIs in windows operating system.

Reference Luo et al. (2010) discussed a non-cooperative, non-zero sum game which is played between the administrator and the attacker in a network of computers. The authors stated