COMPUTERS & SECURITY 39 (2013) 268–288

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

SHADuDT: Secure hypervisor-based anomaly detection using danger theory

*Reza Azmi, Boshra Pishgoo**

Operating System Security Laboratory (OSSL), Alzahra University, Tehran, Iran

ARTICLE INFO

Article history:
Received 17 May 2013
Received in revised form
19 July 2013
Accepted 8 August 2013

Keywords:
Intrusion detection system
Anomaly detection
Artificial immune system
Danger theory
Hypervisor technology
System call interception

ABSTRACT

Intrusion Detection based upon learning methods is an attractive approach in research community. These researches have two critical concerns: secure information gathering and accurate detection method. Here we used system calls together with their arguments as a suitable pattern for describing behavior of each process. In security applications, these patterns must be collected safely, so we proposed SHADuDT, a secure and robust hypervisor-based architecture for system call intercepting and information gathering that utilizes the second generation of Artificial Immune Systems (AIS) as intrusion detection method. Generally intrusion detection based on AISs fall into two categories. The first generation of AIS is inspired from adaptive immune reactions but the second one that is called danger theory focuses on both of these reactions to build a more biologically-realistic model of Human Immune System.

Here we presented a novel Algorithm in Danger Theory field as SHADuDT detection method (SHADuDT_DM) for anomaly detection and utilized hypervisor architecture for SHADuDT secure auditor (SHADuDT_SA) to guarantee the safety of information gathering. We evaluated SHADuDT architecture through several criteria and compared its detection method with classic AIS methods for anomaly detection. These Evaluation results show considerable improvements in terms of detection performance and false alarm rates while keeping low overheads in execution time and memory by using the advantages of both hypervisor technology and Artificial Immune Systems.

1. Introduction

By looking back at intrusion history, we perceive that detecting and countering subversive actions is one of the most necessary steps for system immunization. In general, Intrusion Detection Systems (IDS) fall into two main categories according to the location they put in it, namely i) Network-based IDS (NIDS) and ii) Host-based IDS (HIDS). NIDSs (Heady et al., 1990) place in another computer or a network device and evaluate network traffic for intrusion detection. In contrast, HIDSs (Vokorokos and Balaz, 2010) reside inside operating systems and evaluate their behaviors. These IDSs have better system view, so higher detection power and lower false alarm than NIDSs, but they are not completely robust and might be vulnerable against rootkits that exist in the system. Isolation is a practical approach to protect HIDS against rootkits. Thus, HIDS can be a suitable option for system protection if it is isolated from monitored operating system.

HIDSs can be implemented in different layers of software system. User level solutions (Snort: open source intrus) have low ability to detect malfunctioning processes because they

* *Corresponding author*. Tel.: +98 09127079969.
E-mail addresses: azmi@alzahra.ac.ir (R. Azmi), boshra.pishgoo@student.alzahra.ac.ir, boshra.pishgoo@gmail.com, boshra.pishgoo@yahoo.com (B. Pishgoo).
0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.08.005

have limited view of the system and can be bypassed easily by processes which have higher privilege. In contrast, kernel level IDSs (Onoue et al., 2008) have complete view of the whole kernel subsystems and get protection against malignant user level processes, but they are still vulnerable against kernel level rootkits. Due to kernel-level attacks and the requirement of high level privilege access right to the kernel's memory and its internal structure, our defense system is implanted in hypervisor layer to provide tamper resistance. Here, we put our HIDS into a small hypervisor that communicates with other layers by a known interface namely x86 ISA. This hypervisor will be more trustworthy container for an IDS because of its smallness and definitive interface and makes IDS more robust by completely isolating it from the other software layers (Sielken, 1999).

For building an HIDS, one needs to consider many issues such as data collection, feature extraction, intrusion recognition and reporting (Wu and Banzhaf, 2010). For data collection, IDSs can use different methods such as profiling and feature vise analysis to have a view of running processes. System calls auditing is an approach for feature vise analysis of a process to present a suitable pattern of its behavior. Here we utilize hypervisor layer for auditing system calls and their arguments to collect data safely and create secure log files. Then we can select and extract some suitable features among these files to form behavioral patterns.

After data collection and feature extraction phases, we must construct a detection model using our secure patterns for intrusion recognition. In this area, IDSs fall into two main categories according to the detection approaches they employ, namely i) Misuse detection and ii) Anomaly detection. Misuse detection identifies intrusions by matching observed data with pre-defined descriptions of intrusive behavior. This approach can detect well-known intrusions efficiently with a very low false alarm rate, but it will fail easily when facing unknown intrusions. At the other hand, anomaly detection is orthogonal to misuse detection and hypothesizes that abnormal behavior is rare and different from normal behavior. Hence, it builds models for normal behavior and detects anomaly in observed data by noticing deviations from these models. This approach has the capability of detecting new types of intrusions and only requires normal data when building profiles.

There are different methods in computational intelligence field which have been frequently used for anomaly detection up now (Wu and Banzhaf, 2010). In this paper, we employ artificial immune systems for anomaly detection. This approach is inspired from Human Immune Systems (HIS) and is a suitable option for intrusion detection because of its distributed, self-organized and lightweight nature. All AIS methods can be divided into two main categories. The first one is inspired from adaptive immune system which is a complex of a great variety of cells. Among its cells, two lymphocyte types, T cells (TC) and B cells (BC), cooperate to distinguish self from non-self antigens. Negative selection (Hofmeyr, 1999), Clonal selection (De Castro and Timmis, 2002; Watkins and Timmis, 2004) and immune network (Jerne, 1974) are three important branches of this category.

In the other side, the second category is new generation of AIS and is inspired from both innate and adaptive immune systems. A type of cells known as Dendritic Cells (DC) act as important medium between innate and adaptive immune system (Wu and Banzhaf, 2010). Danger theory methods fall into this category. In the fundamental idea of the first generation of AIS, Immune responses are triggered when the body encounters non-self antigens; but Matzinger proposed the Danger Model (Matzinger, 1994, 2001), and claimed that immune responses are triggered by the unusual death of normal tissues, not by non-self antigens.

Aickelin and his research group applied Danger Theory to intrusion detection systems as a project called "Danger Project" (Mutz et al., 2006) in 2003. The results of their works can be summarized as one innate immunity architecture, and two danger theory based algorithms namely the Dendritic Cell Algorithm (DCA) (Greensmith, 2007; Greensmith and Aickelin, 2006, 2007; Greensmith et al., 2004, 2005, 2006, 2010) and TLR algorithm (Twycross et al., 2007; Twycross and Aickelin, 2007, 2008). Both DCA and TLR employ the model of DCs but the implementation of them focuses on different aspects of the DC model. The DCA relies on the signal processing aspect by using multiple input and output signals, while the TLR emphasizes the interaction between DCs and T cells, and only uses danger signals (Wu and Banzhaf, 2010). In this paper, our proposed detection method falls into danger theory field too. Like TLR, our algorithm emphasizes the interaction between DCs and T cells but it utilizes an advanced signal processing similar to DCA. Unlike DCA and TLR that require external danger signals, our algorithm generates these signals through structure of normal and abnormal training data and doesn't require any external source for signal generation. Due to the use of training data structure, our method has lower false alarm and higher detection performance than previous methods and can be used as an appropriate classifier.

In order to collect all mentioned features in a single framework, here we propose a novel architecture which is called SHADuDT. SHADuDT is a secure and robust hypervisor-based architecture that intercepts and audits system calls in hypervisor layer utilizes the second generation of AIS as intrusion detection method to separate normal and abnormal behaviors.

The remainder of this paper is organized as follows. Section 2 describes some related researches in different aspects of our work. The biological inspiration from HIS that is base of our algorithm is introduced briefly in Section 3. SHADuDT architecture and its implementation are explained in Section 4 by details. Section 5 evaluates our model at different views like execution time, memory consumption and detection performance. In this part, we investigate the experimental results of our proposed danger theory method and compare it with classic AIS methods like negative selection and previous danger theory algorithms like DCA and TLR. Finally, Section 6 concludes all topics and indicates our future works in this field.

2. Related works

As mentioned in previous section, SHADuDT_SA and SHADuDT_DM are two main parts of our proposed architecture. So in the following subsections, we introduce some researches in