Journal of Network and Computer Applications 32 (2009) 721–732

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation ☆

Li Feng [a,c,*], Wei Wang [b], Lina Zhu [a], Yi Zhang [a]

[a] Center of Dependable and Secure Computing (CDSC) of WuHan Digital Engineering Institute, WuHan, Hubei Provence 430074, China
[b] French National Institute for Research in Computer Science and Control (INRIA) Sopia antipolis, France
[c] State Key Laboratory for Manufacturing Systems (SKLMS) and MOE Key Lab for Intelligent Networks and Network Security (KLINNS), Xi'an Jiaotong University, Xi'an, China

ARTICLE INFO

Article history:
Received 2 March 2008
Received in revised form
21 May 2008
Accepted 13 June 2008

Keyword:
Intrusion prediction
Plan recognition
Dynamic Bayesian network
Transfer probability estimation
System call sequences

ABSTRACT

Predicting the intentions of an observed agent and taking corresponding countermeasures is the essential part for the future proactive intrusion detection systems (IDS) as well as intrusion prevention systems (IPS). In this paper, an approach of dynamic Bayesian network with transfer probability estimation was developed to predict whether the goal of system call sequences is normal or not, with early-warnings being launched, so as to ensure that some appropriate countermeasures could be taken in advance. Since complete set of system call state transfer can hardly be built in real environments, the empirical results show that the newly emerging system call transfer would have great impact on the prediction performance if we straightly use dynamic Bayesian network without transfer probability estimation. Therefore, we estimate the probability of new state transfer to predict the goals of system call sequences together with those in conditional probability table (CPT). It surmounts the difficulties of manually selecting compensating parameters with dynamic Bayesian network approach [Feng L, Guan X, Guo S, Gao Y, Liu P. Predicting the intrusion intentions by observing system call sequences. Computers & Security 2004; 23/3: 241–252] and obviously makes our prediction model more applicable. The University of New Mexico (UNM) and KLINNS data sets were analyzed and the experimental results show that it performs very well for predicting the goals of system call sequences with high accuracy and furthermore dispenses with much more manual work for selecting compensating parameters.

1. Introduction

Computer security is a rapidly developing and extremely important research domain. Hackers use various attacking skills to intrude or crash the targets to achieve their goals. Thus, predicting the hackers' goal becomes very vital for a proactive intrusion prevention system. Intrusion detection must turn to predict the future actions of attackers from detecting the attacks already happened. Geib and Goldman (2001) first proposed a model based on plan recognition to predict the goals of hackers, which depends on a hierarchical plan library that provides recipes for achieving goals. Huang and Wicks (1999) addressed a conceptual architecture about identifying the attack strategy, which aims to drive various intrusion detection systems (IDS) components to work together.

Some audit information such as system logs of host, traffics of network or IDS alarms can trace the hackers' behavior in various viewpoints. In our work, we choose system call sequences as observation data. Each operating system has its own inner functions built in kernel. The functions are used for each calling from user space of system. In UNIX-like systems, the functions that used are called system calls, which represent the transitions from user space to kernel space. Accordingly, to most extent, sequences of system calls in kernel space represent a plan of user or hacker in user space to achieve a certain goal. In general, it can be classified into two main types: normal and abnormal. Anomaly system call transfer can be regard as the wrong or malicious action planning of an observed process reasonably. Therefore, it can be great beneficial to block the malicious action through examining the plan or goal of a calling sequence of kernel functions.

In recent years, a lot of research activities for the intrusion detection used system call sequences as valuable data sources. In 1996, Forrest et al. (1996) initially introduced a simple anomaly detection method called time-delay embedding (tide), based on

☆ The research presented in this paper was supported in part by 863 High Tech Plan (No. 2007AA01Z464) of China and the Defense Pre-Research Projects of the 'Eleventh Five-Year-Plan' of China (Nos. C0820061362-06 and A1420080183).

* Corresponding author at: Center of Dependable and Secure Computing (CDSC) of WuHan Digital Engineering Institute, WuHan, Hubei Provence 430074 China. Tel.: +86 2787787006.

E-mail addresses: fengli_xjtu@163.com (L. Feng), wei.wang.email@gmail.com (W. Wang), an235000@163.com (L. Zhu), zhangyi98@sohu.com (Y. Zhang).

1084-8045/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2008.06.002

monitoring system calls invoked by active and privileged processes. Profiles of normal behavior were built by enumerating all fixed length of distinct and contiguous system calls that occur in the training datasets and unmatched sequences in actual detection are considered anomalous. In subsequent research, the approach is extended by various methods. For example, (Lee and Stolfo, 1998) explored data mining approach to study a sample of system call data and characterize the sequences contained in normal data by a small set of rules. The sequences violating those rules were then treated as anomalies for monitoring and detection purpose. Warrender et al. (1999) proposed a Hidden Markov Model (HMM) based method for modeling and evaluating invisible events. Yeung and Ding (2003) and Lee and Xiang (2001) used information-theoretic measures for anomaly detection. Liao and Vemuri (2002) used K-nearest neighbor (K-NN) classifier and (Hu et al., 2003) applied robust support vector machines (SVM) to model program behavior and classified each process as normal or abnormal based on system call data. Sharma et al. (2007) adopted kernel based similarity measures to detect anomaly events. In our previous work, we also employed non-negative matrix factorization (NMF) (Wang et al., 2004), self organizing maps (SOM) (Wang et al., 2006) and principal component analysis (PCA) (Wang et al., 2008) to profile program and user behavior using system call sequences. These existing methods (Forrest et al., 1996; Lee and Stolfo, 1998; Warrender et al., 1999; Yeung and Ding, 2003; Lee and Xiang, 2001; Liao and Vemuri, 2002; Hu et al., 2003; Sharma et al., 2007; Wang et al., 2004, 2006, 2008) based on system call data are shown as effective for detecting malicious actions. However, they are only able to detect intrusions after attacks have occurred, either partially or fully, which makes it difficult to block the attack in real time. Therefore, it is most desirable to incorporate a prediction function into system call based IDS for predicting the type of goals so that the proper response can be taken before substantial damage harms the systems.

Plan recognition is the process of inferring the goals of an agent from observations of an agent's action, which is considered as an inference problem under uncertain conditions (Robert et al., 1999; Charniak and Goldman, 1993). Current related research mainly focuses on: (1) predicting plans or goals during cooperative interactions; (2) understanding stories (natural language processing); (3) recognizing the plans of an agent that is unaware of the plans being monitored, known as keyhole plan recognition (Albrecht et al., 1997; Wærn and Stenborg, 1995). There are two main features of the keyhole plan recognition: (1) the monitored agent is not aware of that its behavior is monitored and analyzed; (2) the observed data is incomplete. In the traditional plan recognition methods, the plan library is built manually, which greatly hinders the wide application of the plan recognition method. To overcome this obstacle, machine-learning approaches are applied to collect information about the plans and to make decisions. Being capable of modeling a time-varying system, dynamic Bayesian network (DBN) is one of the few methods that enables us to develop effective methods for recognizing and monitoring the time-varying plans (Charniak and Goldman, 1993; Nicholson and Brady, 1994; Friedman et al., 1997). DBN-based plan recognition is first proposed by Albrecht et al. (1997) for predicting the goals of multiple players in multi-user dungeon (MUD) game with good experimental results.

In this paper, we proposed an approach on DBN with transfer probability estimation (DBN with TPE) to predict the goals of intruders by observing the system call sequences. The domain of goal states for observed agents includes normal and anomalous goals. The normal denotes a kind of goal with which normal user completes specific daily tasks, while the anomalous represents a kind of goal of malicious users or hackers exploiting the vulnerable target host. Through building the structure of DBN and condition probability table (CPT) by training data, system call sequences can be modeled to predict their intentions. Theoretically, Bayesian formula is based on the total probability theorem and exclusive partition of event space. However, in reality, it is difficult to have ideal partition of system call transfers in normal and anomalous sequences sets. There exists those sequences with different types of goals but have the same sub-sequences or it may also be true that certain parts of an anomaly system call sequence can be the same as that of a normal sequence. To mitigate the impact from prediction errors, we proposed an approach on parameter compensation to condition probability distribution of normal system call sequences and successfully predict the goals with good accuracy (Feng et al., 2004). However, the approach of parameter compensation introduced much more unnecessary manual selection in trials and errors and can hardly choose the ideal compensating parameters. The defects hamper its wide application in real environments. To efficiently solve the above problem, we propose an approach on TPE based on DBN. Since the Bayesian theory needs some priori information about observed agents, the complete information about the system call transfers is hard to be obtained totally. In experiments, we discover that the newly emerging transfer states that are not included in CPT have bad impact on the prediction performance. The approach in Feng et al. (2004) only simply specifies a very small fixed value to the probability of newly emerging transfer states. In this paper, we estimate the probability of newly emerging system call transfer that are not included in CPT to greatly reduce the computation cost for manual selection of compensating parameters.

In the reminder of this paper, we will organize the paper as follows. Section 2 clarifies how to model an intrusion goal prediction system by DBN with TPE . In Section 3, the contrastive experimental results are given based on DBN without TPE and the model with TPE. Section 4 draws some conclusion about our approach and outlines the future work.

2. The model for predicting the goals based on DBN with transfer probability estimation (TPE)

2.1. Structure and condition probability table (CPT)

To discover the irregularity of the system call sequences and detect intrusions, the following state variables are defined (Feng et al., 2004).

(1) *System call* (S): represents all possible calls in a system call sequence. The size of state space of system calls is $|S|$, which is the total number of possible calls in an operating system.
(2) *Goal* (Q): being a set of state variables describing the goal of a sequence as normal or abnormal. Goal Q consists of two classes of states: normal and abnormal. The normal goal denotes that normal users or processes want to accomplish normal tasks. The abnormal goal is what intruders or hackers intend to reach by exploiting the vulnerabilities of the system.

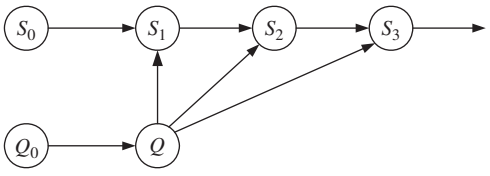

Fig. 1. DBN for predicting the goal of a system call sequence.