A Hybrid Intrusion Detection and Visualization System

J. Peng, C. Feng, J.W. Rozenblit
Department of Electrical and Computer Engineering
The University of Arizona
Tucson, AZ 85721-0104, USA
jr@ece.arizona.edu

Abstract

Network attacks have become the fundamental threat to today's largely interconnected computer systems. Unauthorized activities and unauthorized access account for a large proportion of these networks. Unauthorized accesses and misuse of critical data can be catastrophic to businesses, emergency services, and even threaten the defense and security of a nation. Intrusion detection system (IDS) is indispensable to defend the system in the face of increasing vulnerabilities. This paper proposes a hybrid intrusion detection and visualization system that leverages the advantages of current signature-based and anomaly detection methods. The hybrid instruction detection system deploys these two methods in a two-staged manner to identify both known and novel attacks. When intrusion is detected, autonomous agents that reside on the system will automatically take actions against misuse and abuse of computer system, thus protecting the system from internal and external attacks.

1. Introduction

The essential part of an intrusion detection system is the detector and its underlying principle of operation, which is based on the belief that an intruder's behavior will be measurably different from that of a legitimate user so that many unauthorized actions can be detected. Typically, IDSs employ statistical anomaly and rule-based misuse models in order to capture the drifting of normal behaviors. Intrusion detection can be categorized into three types: signature detection, anomaly detection and hybrid detection. Signature detection is conducted by signature matching of known attacks. For example, internet worm attacks can be detected by signature detection because of the explosive usage of specific network services. The major limitation of signature-based detection method is that it cannot detect novel attacks. Anomaly detection, on the other hand, models normal behaviors and attempts to identify anomaly activities of computer system performance metrics such as I/O activity, CPU usage. Because intrusions can deviate significantly from the ordinary profile maintained by the IDSs, it is possible that many new intrusions can be detected. Hybrid detection is a method that leverages the advantages of both anomaly and signature based methods.

In an intrusion detection system, some sort of security audit should be performed in order to get a security audit data. This data is then stored and processed in real-time by the detector. Autonomous agents on the system take the processed results and check for anomalies. If any suspicious behavior is detected, these agents will report to the site security officer (SSO) who then takes further action such as denying the intruder's access.

There are two mechanisms for handling specific events sent by security audit -- programmed and adaptive learning. Programmed mechanism refers to a stack of rules pre-defined by domain experts. It is relatively simpler to implement, hence it has been applied in almost all of the signature detection systems and some of anomaly detection systems. The learning mechanism is a more complicated approach that observes traffic for a period of time and models the underlying process.

2. Hybrid system framework

Our research aims to design a systematic and intelligent hybrid intrusion detection and visualization system. The system introduces a two-stage intrusion detection technique. Host system calls are monitored as audit data source. Current research is conducted on a standalone host only. However, the system can be migrated to distributed systems in the future with ease.

The first stage is the misuse detection stage that employs the signature-based detection method. A database of known detection behaviors has been developed and updated over the time. Data mining is an effective technique of discovering knowledge from voluminous data sets to assist in building such database. In this stage, the system compares system audit data with

Proceedings of the 13th Annual IEEE International Symposium and Workshop on Engineering of Computer Based Systems (ECBS'06)
0-7695-2546-6/06 $20.00 © 2006 IEEE

intrusion behavior database in real time. If any intrusion is detected, the autonomous agents will start to intervene and take precautions according to the event handling mechanisms. After the signature detection stage, a graph of system call information should be generated. Knowledge is usually presented in the form of decision rules easy to be used in the future.

The second stage is the anomaly detection stage. This stage can overcome the shortcoming of the first stage and is able to detect novel attacks. It can provide additional detection such as misuse of confidential data by internal users. An anomaly-based IDS achieves this by identifying program behaviors that deviate from the known normal behavior. It monitors a program by observing event traces and comparing those traces to some expected behavior.

Our approach uses sequences of system calls as a characterization of program behavior. We use a software program to capture the "normal" program traces and generate a "safe" range of system calls. Figure 1 shows a simple example of "normal" sequences of system calls during a day's operation. The decision engine uses the fuzzy inference approach. In the fuzzy inference module, input variables can be obtained from the system event traces and the output variable RESULT is generated. The fuzzy inference module then uses the inference rules to detect anomaly system behaviors. The rules are constructed on the basis of empirical prior knowledge about system processes like following: IF Syscall1 ValueIS VERY High AND Syscall2 ValueIS VERY High, THEN RESULT is Abnormal. Learning method such as neural network can be applied to get the prior knowledge. If any anomaly has been detected, automatic agents will report the event to site security officer to take further actions.

In both stages, there are large amount of data that need to be analyzed. It is difficult for the security officers to get a quick understanding of the data without having digging into the numbers. Thus, a visualization system is needed to give security officers an intuitive representation of such information as normal range of system calls.

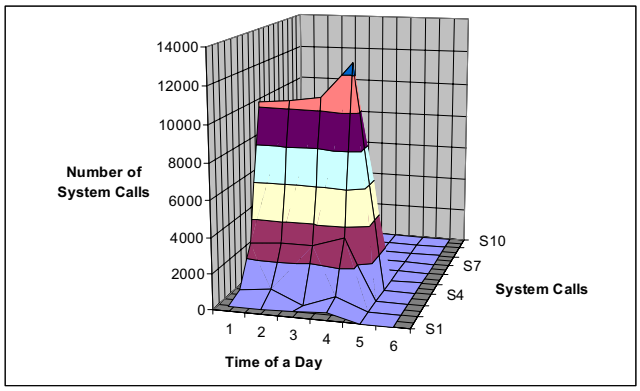

Figure 1 Statistics of System Calls

References

[1] B. Mukherjee, L. T. Heberlein, K. N. Levitt, "*Network Intrusion Detection*", IEEE Network, May/June 1994

[2] Z. Li, A. Dad, J. Zhou, "*Theoretical Basis for Intrusion Detection*", Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY

[3] Q. Xue, J. Sun, Z. Wei, "*TJIDS: an intrusion detection architecture for distributed network*", Proc. of the Canadian Conference on Electrical and Computer Engineering (IEEE CCECE 2003), pp.709-712, May 2003.

[4] J. Xin, J.E. Dickerson, J.A. Dickerson, "*Fuzzy feature extraction and visualization for intrusion detection*", Fuzzy Systems, 2003. FUZZ '03. The 12th IEEE International Conference on Volume 2, 25-28 May 2003 Page(s):1249 - 1254 vol.2

[5] S. Axelsson, "*Intrusion detection systems: A survey and taxonomy*", Technical Report 99-15, Department of Computer Engineering, Chalmers University, March 2000.

[6] W. Lee, S. J. Stolfo, K. W. Mok, "*A data mining framework for building intrusion detection models*", Proceedings of the 1999 IEEE Symposium on Security and Privacy, May 1999.

[7] W. Lee, S. J. Stolfo, "*Data Mining Approaches for Intrusion Detection*", Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998

[8] Leandro N de Castro, J. Timmis, "*Artificial Immune Systems: A Novel Paradigm to Pattern Recognition*", Artificial Neural Networks in Pattern Recognition, University of Paisley (2002)

[9] S. Kumar, E. H. Spafford, "*A software architecture to support misuse intrusion detection*", Proceedings of the 18th National Information Security Conference, pages 194-204, 1995.

[10] B. Schneier, "*Attack Trends 2004 and 2005*", Counterpane Internet Security Inc. http://www.acmqueue.org/modules.php?name=Content&pa=showpage&pid=316