Real Time Detection Framework of Insider Threat Based Agent

Zhen-hui WANG
School of Technology and Engineering, Xi'an Fanny University, Xi'an, China

Keywords: Insider threat, Abnormal behavior, Identity authentication, Detect

Abstract. In view of the increasing internal threat behavior of enterprise information system, especially the internal user data corruption. A real time detection framework based on agent is proposed, and malicious insider threats are identified by comparing user identity and abnormal operation behavior. The framework makes a data acquisition module, a detection module, audit module and response module. The function of the detection system is explained from 4 aspects of identity authentication, access control, and operational audit and vulnerability detection. This framework implements the user real name login, behavior detection and post audit, fundamentally prevent malicious insiders to obtain illegal data and provide response and intervention capabilities, enhance the security of an information system.

Introduction

With the rapid development of Internet technology and communication technology, cases of internal personnel intentionally and unintentionally using information systems and database vulnerabilities to engage in forbidden activities are increasing year by year. In the face of various security threats faced by the information system, the internal threat is far less than the external attack, but it causes more losses and harms. In 2013, typical internal threats leaked by Snowden sounded the alarm of the internal threat again. Staff, partners, and third party companies providing data services are the main perpetrators of insider threats. Internal threats can cause reputation damage, economic loss, and even endanger national security for individuals and enterprises. The data leakage caused by the seven internal threats in 2014 caused incredible damage to business and related organizations [1].

IBM Security 2015 network indexes show that many types of attacks internal threat topped the list, 55% of the attacks are derived from the internal employees who are given access to the system [2]. In contrast to external workers, employees know more about what data is valuable, and what is stolen does not have any value. Malicious operation is easily ignored by the enterprise organization, so the internal threats, has gradually become the object of security experts on the domestic and abroad, back in 2011 the United States Department of defense proposed the establishment called ADAMS within the military threat detection system [3].

At present, with the continuous upgrade of Internet technology, communication technology, intelligent mobile phone technology, the diversification of enterprise information system access technology and facilitation trend, internal threats in the enterprise information system, especially the internal users of data destruction, the security problem has become the current enterprise information construction to be solved.

Design of Internal Threat Detection Framework

Design Principles

At present, technology for insider threat detection method used varied. The most frequently used method is based on artificial intelligence, such as statistical learning method, the method of system dynamics etc. In these studies, although the methods used are different, but with no exception for malicious internal users prior knowledge (such as: the attack ability, attack purpose, attack cost)
However, in practical applications, it is sometimes difficult to get the prior knowledge of the attacker before the successful detection, so the practicability of these methods is difficult to guarantee. The insider threat detection model has the problem of high false positive rate and false negative rate. Take into account this situation and in order to ensure the function and performance requirements, we analyzed the security requirements, the domestic and foreign internal threat detection technology and product function, put forward a kind of data detection module based on agent technology.

An agent is a software agent that can perceive the environment and take appropriate actions, draw up its rules of action, and can affect the environment. On the one hand, agent technology offers an effective way to solve the new network distributed application problems; on the other hand, agent technology provides a reasonable conceptual model for comprehensively and accurately studying the characteristics of distributed computing systems. Agent communication language can implement flexible and diverse interaction, and can achieve effective collaboration between Agents.

The specific design idea is that the user's identity and authority can be judged by the agent before the user access to the business data. Only authenticated users can access data. In the process of user processing authorization data, agent monitors the user's behavior in real-time, and registers the user's behavior into the log file. After processing, agent can call the corresponding signature mechanism according to the user's need to sign the processing part of the user, so that users cannot deny the data modification.

System Structure

Logical Structure. The logical framework of the insider threat detection system is divided into three layers: the first layer is the internal threat detection system and customer service host interface, realize the communication with the client and data collection; the second part is the internal threat detection system for internal security modules, realize detection, audit, response and other security control functions; the third part is the internal threat detection system and enterprise database server interface, realize the communication with the database and data collection. Figure 1 is a three layer logical structure diagrams.

![Figure 1. Logic structure of insider threat detection framework based on Agent.](image)

The data acquisition module is composed of the detecting system in an information gathering tool. The module has the characteristics of data needed for the collection of the detection module. User input is the type of operation, location, time, connection mode and connection protocol, host, operational data and results of operation data, the output is logged information, vulnerability scanning and other information, is the basic module support detection system.

The principal task of the detection module is to use the internal threat detection rules and knowledge base to compare and analyze the user behavior data, output the system alarm and suspicious event information.

The response module can make the alarm and interrupt service according to the judgment of the internal threat of the detection module and the system strategy analogous to the internal threat characteristic value, so as to eliminate or reduce the internal threat.
The audit module is post-hoc analysis and prevents omission of log information. Do further analysis, judgment and deep mining to user behavior or suspicious operation that cannot be detected by detection rules.

Install the client agent in customer service and database server on the host machine, and capture internal staff input data and commands, and can lock screen and upload screenshots. To achieve real-time online monitoring and post audit through the dual role of a security detection system.

**Access Control Structure.** The internal threat detection system monitoring program receives the user issued by SQL request, analyzed SQL statement, found out the subject and object, check the subject and object access authorization, then analyzed the SQL statement intention, first check the sensitive words, avoid SQL injection, cross site scripting attack. Secondly, by matching the SQL operation and rules in action check the abnormal degree, according to the degree of deviation analysis, reasoning and detection behavior decision, when the operation behavior anomaly over a range of rules, the immediate alarm and provide relevant audit results. Figure 2 is the internal threat detection system access control logic diagram.

![Control logic of insider detection system based on agent.](image)

**Data Storage Design.** The data accessed by the internal threat detection system are logically divided into six types. The first is request data, that is, the SQL commands and consumer information submitted by the user to the database server. For example: host name, IP address, etc. The second type is used and authority data, which is user identity and access control information ACL. The third type is the user operation log, recording user behavior, used for operational audit. The fourth is knowledge base file, which saves the export data of Agent, which is convenient for reasoning and analysis of Agent. The fifth is the rule base, which establishes the standard of anomalous behavior for each class of authorized users. The sixth type is system configuration file, such as communication parameters, trust degree and so on. In order to decrease the system complexity and improve the scalability of the system, the six kinds of information are stored in XML mode.

**Internal Threat Detection Framework Function Design**

Depending on the demand for enterprise data security level the internal threat detection system function is different. However, each module function is defined according to the principle of component and reuse.

- The data acquisition module: data acquisition, vulnerability detection.
- The detection module: identity authentication, access control, rules management, security policy adjustment.
- The response module: Alarm system, denial of service.
- Audit module: log audit, event analysis, data mining.

The internal threat perception and detection technology activities can be divided into three parts: Blocking, detection and response according to the time sequence. Data packet filtering technology is used to realize identity authentication and role based data access control, and this function is processed by the authentication agent. Authentication Agent plays the role of software protection wall in software architecture, and performs security filtering and auditing for requests for various connection and operational databases. In addition, a lot of data leakage is the intramural personnel familiar with loopholes in the system to obtain, therefore, the use of Agent vulnerability detection, by detecting the database server vulnerabilities, assess the safety level of risk prevention. The operation audit is encapsulated into the operation audit agent, and the online real-time behavior detection or
ex-post data analysis is carried out according to the preset detection rules and security policies. Abnormal behavior detection will trigger response execution of Agent, thereby reducing the threat of internal damage. Each agent is through collaboration to complete the task of security, therefore, the communication security problem is very important; the user password hash value as the key research, based on the realization of secure communication mechanism of symmetric encryption algorithm.

Conclusions
According to the security requirements of the current enterprise information system to deal with internal threats, put forward a kind of internal threat detection of Agent framework based on this framework, including data acquisition, identity authentication, log management, vulnerability detection, and audit operation module. The construction of various functional modules for the intelligent agent, in the agent complete collaboration between abnormal behavior detection and identification task, in order to analyze the system operation logs dynamic, real-time detection and intervention operation for internal threats. With the flexibility of Agent and Agent trust base and identity authentication technology based on object serialization, improve the internal threat detection agility and reliability; enhance intelligence and adaptive ability of the enterprise internal threat detection system.

Acknowledgement
This research was financially supported by Scientific Research Program Funded by Shaanxi Provincial Education Department

Reference
[1] The seven data leakage events caused by insider threats in 2014, http://netsecurity.51cto.com/art/201501/462964.htm
[2] IBM Report: 55% attacks are from the enterprise internal!, http://www.ctiforum.com/news/baogao/467709.html
[3] “Anomaly Detection at Multiple Scales (ADAMS) Broad Agency Announcement DARPA-BAA-11-04 (PDF),” General Services Administration. 2011.
[4] Zhang H.B., Pei Q.Q., Wang C.et al. Insider threat based on access vector’s [J]. Journal of XiDian University, 2014,4 1(1): 110-115.
[5] Chen X.J., Shi J.Q., Xu F., et al. Algorithm of Optimal Security Hardening Measures Against Insider Threat [J]. Journal of Computer Research and Development, 2014, 51(7): 1565-1577.
[6] Singhal A. Data Warehousing and Data Mining Techniques for Computer Security [M]. New York: Springer-Verlag, 2006: 83-103.
[7] Ertoz L., Eilertson E, Lazarevic A., et al. MINDS-Minnesota Intrusion Detection System [C]//Next Generation Data Mining. New York: MIT/AAAI Press, 2004: 65-86.