UDC 004.056.2

INFORMATION INTEGRITY MONITORING AS A PART OF HOST INTRUSION DETECTION SYSTEM

KANSTANTSIN HALAVAN, EVGENIJ SUHAREV
Polotsk State University, Belarus

The article describes the concept of the information integrity, control information integrity and the relevance of integrity. Providing classification and comparison of modern information integrity software.

In the context of the deep distribution of information technology in all human activity fields, the reliability of the identification information and the control of its integrity become important issues, all scientific, technological, and social. The scientific and technological problems include creating mathematical approaches, algorithms, software and hardware to solve these problems. The social aspect of the problem is the need to create a public accessible, convenient and secure system with the reliable data identification, an adequate level of development of information technologies.

Information integrity control has significant impact in various fields of human activity. In the financial area a large number of financial transactions is carried out every day on the Internet in which integrity control of the processed, transmitted and stored information is an important part.

Creating a secure system is a complex problem, and it is solved by using of software and hardware, as well as organizational measures. The real protection system is built based on possible threats and the chosen security policy.

The main information security threats depend on the aspects on which these threats are directed. They are:

- privacy threats;
- integrity threats;
- availability threats;
- authenticity threats;
- safety threats.

Information protection system ensures the information integrity, if it provides the accuracy, completeness and security of information from unintentional and intentional distortions in storage, transmission and processing.

One way to ensure the information integrity is to use software (file) integrity monitor tools and to process information, including its recovery.

The main objective of information integrity monitoring tools is to provide such a state of the system when it is impossible to hide the fact any unauthorized modification of information.

File integrity monitor (FIM) is one of the security tools that can be implemented in a host environment as a part of a host based intrusion detection system (HIDS). Information integrity monitor plays a big role in monitoring the integrity of the files in the event of any changes to the files or their content, access control, privilege, group and other properties either by authorized or unauthorized users. The main goal of related integrity tools is to notify system administrator if any changes have been made, deleted, or added on the monitored system. Basically, file integrity tools measure the current checksum or hash value of the monitored.

As part of the HIDS functions, file integrity monitoring can be classified as off-line (on request) and on-line (on real time) integrity monitoring [1].

Tripwire [2] is a well known file integrity monitoring tool that motivates other researchers to develop more powerful IIM tools. Tripwire works are based on four processes: init, check, update and test. Comparison of the current hash values of the files with the baseline values is the main principle of the FIM tools like Tripwire.

Inspection frequency and the modification detection effectiveness is the main issue in the off-line FIM. In order to maintain the effectiveness of the FIM, high frequency inspection is needed at the cost of system performance, and vice versa. In order to overcome this issue by proposing a dynamic inspection schedule by classifying related files to certain groups and the inspection frequency will vary between the groups of files [1].

On-line FIM is proposed to overcome the delay detection in off-line IIM approach by monitoring the security event involving system files in real-time. However, in order to work in real-time, it requires the access of low level (kernel) activities which require kernel modification. When kernel modification is involved, the solution is kernel and platform-dependent, and therefore incompatible with other kernels and platforms.

As an example, I3FS [3] proposed a real-time checking mechanism using system call interception and working in the kernel mode. However this work also requires some modifications in protected machine's kernel.

In addition, whole checksum monitoring in real time affects performance degradation. I3FS offers a policy setup and update for customizing the frequency of integrity check.

There are various on-line FIM and other security tools using the virtual machine introspection (VMI) technique to monitor and analyze a virtual machine state from the hypervisor level.

On the other side, virtualization based file integrity tools (FIT) has been proposed by XenFIT [4] to overcome the privileged issue on the previous user mode FIT. XenFIT works by intercepting system call in monitored virtual machine (MVM) and sent to the privileged virtual machine (PVM). However, XenFIT requires a hardware virtualization support and only can fit with the Xen virtual machine, not other virtualization software. Another Xen based FIT is XenRIM [5] which does not require a baseline database. NOPFIT [6] also utilized the virtualization technology for their FIT using undefined opcode exception as a new debugging technique. However, all those real-time FIT only works on the Linux based OS [1].

Centralized management of the file integrity monitoring is the main concern of those tools, and in order to develop this need one should take it as the fundamental features for this type of system and need to focus more on the checking scheduling concern on the multi-platform host. The other security tools also implement a centralized management for their tools, such as anti-malware and firewalls, FIM as part of HIDS also needs that kind of approaches to ensure the ease of administration and maintenance.

FIM tools, Samhain [7], and OSSEC[8] come with centralized management of the FIT component in their host based intrusion detection system which allow multiple monitored systems to be managed more effectively. Monitoring the integrity of files and registry keys by scanning the system periodically is a common practice of the OSSEC.

Combining the on-line and off-line integrity monitoring with centralized management is to maintain the effectiveness of the FIM and to reduce the performance overhead.

Conclusion. The integrity threat is one of the main information security threats. Unauthorized changes of the information may be caused by accidental or premeditated actions. One way to ensure the information integrity is the use of software integrity controls and processes information, including its recovery.

In general, data integrity control is provided by pre-determining characteristics of the information integrity, called a message authentication code [9].

Among the considered software should note the client / server structure of the program with a centralized management, including the administrative console to collect information, the set up time of the integrity check for each agent and configuration. As a method for the modificationdetection used hashes comparisonmethod.

REFERENCES

1. Towards a Dynamic File Integrity Monitor through a Security Classification / Zul Hilmi Abdullah [et al.] // International Journal on New Computer Architectures and Their Applications (IJNCAA). – 2011. – Vol. 1, № 3. – P. 766–779.
2. Kim, G.H. and E.H. Spafford, The design and implementation of tripwire: a file system integrity checker, in Proceedings of the 2nd ACM Conference on Computer and communications security. - 1994, ACM.
3. Patil, S. I3FS: An In-Kernel Integrity Checker and Intrusion Detection File System, in Proceedings of the 18th USENIX conference on System administration / S. Patil. – USENIX Association: Atlanta, GA, 2004.
4. Junghan, K. NOPFIT: File System Integrity Tool for Virtual Machine Using Multi-byte NOP Injection. in 2010 International Conference on Computational Science and Its Applications / K. Junghan. – Fukuoka, Japan, 2010.
5. Quynh, N.A. A novel approach for a file-system integrity monitor tool of Xen virtual machine, in Proceedings of the 2nd ACM symposium on Information, computer and communications security / N.A. Quynh, Y. Takefuji. – ACM: Singapore, 2007.
6. Quynh, N.A. A Real-time Integrity Monitor for Xen Virtual Machine, in Proceedings of the International conference on Networking and Services / N.A. Quynh, Y. Takefuji. – IEEE Computer Society, 2006.
7. Wotring, B. Samhain, in Host Integrity Monitoring Using Osiris and Samhain / B. Wotring, B. Potter. – Syngress: Burlington, 2005. – P. 241–305.
8. System Integrity Check and Rootkit Detection, in OSSEC Host-Based Intrusion Detection Guide / A. Hay, [et al.]. – Syngress: Burlington, 2008. – P. 149–174.
9. Петров А.А. Компьютерная безопасность. Криптографические методы защиты информации / А.А. Петров. – М. : ДМК, 2000. – 448 с.