October 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

LOG MANAGEMENT: USING COMPUTER AND NETWORK RECORDS TO IMPROVE INFORMATION SECURITY

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The information that is routinely collected about specific events occurring within information technology (IT) systems and networks can be used by organizations to improve the security of their operations. This information is recorded as an entry in a log, and each log entry can be linked to a particular event. Log entries, which can be analyzed when organizations need to identify security incidents and operational problems, provide valuable information to managers who are responsible for the operations and security of systems.

Log entries are recorded by the systems' software and applications. The entries containing information related to system security are produced by several sources. Some log entries are created by security software, such as antivirus software, firewalls, intrusion detection systems, and intrusion prevention systems. Other sources of security-related log entries are the operating systems on an organization's servers, workstations, and networking equipment, and the applications on the systems.

Guide to Computer Security Log Management

NIST's Information Technology Laboratory recently issued Special Publication (SP) 800-92, *Guide to Computer Security Log Management*, by Karen Kent and Murugiah Souppaya, to help organizations develop, implement, and maintain effective processes for managing logs with security-related information. The guide explains how sound log management practices can support the overall security of an organization's systems and information.

NIST SP 800-92 begins with basic information about computer security logs, the usefulness of these logs, and the challenges of managing them. Topics covered in depth in the guide include the components of the log management infrastructure, including the hardware, software, networks, and media that are used to generate, transmit, store, analyze, and dispose of log information; the planning processes that enable the organization to carry out consistent, reliable, and efficient log management practices; and the operational processes that aid organizations in successfully managing logs.

In the appendices to the guide, you will find a glossary of terms used, a list of acronyms, and an extensive listing of tools and resources that should be helpful in understanding and implementing log management in your organization. Both in-print and online resources are included. NIST SP 800-92 is available from NIST's web pages at:

http://csrc.nist.gov/publications/nistpubs/index.html.

Logs and Their Uses

Logs are records of many different, specific events that occur within an organization's systems and networks. In the past, the information recorded in logs was used primarily to identify operational problems. Today, the information provided by logs is used for many purposes:

* optimizing system and network performance; to record the actions of users;

continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since November 2005:

* identifying security incidents, policy violations, fraudulent activities, and operational problems;
* performing audits and forensic analyses;
* supporting internal investigations;
* establishing baselines; and
* identifying operational trends and long-term problems.

NIST's guide focuses on helping organizations manage the use of logs to improve IT security. While many logs are created by IT systems and could provide data that is useful for security, NIST SP 800-92 focuses on the logs that are closely related to computer security. For example, audit logs track user authentication attempts, and security device logs record possible attacks on systems. In managing computer security-related log data, organizations have to create, transmit, store, analyze and dispose of the data correctly. The computer security records should be stored in sufficient detail for an appropriate period of time and be available for routine log analysis. Federal organizations have to take into account the requirements of laws, regulations, and organizational policies. For example, federal organizations may need to analyze the log information for compliance with federal legislation and regulations, including:

* Federal Information Security Management Act of 2002 (FISMA) - requires federal agencies to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets.

* Health Insurance Portability and Accountability Act of 1996 (HIPAA) - mandates safeguarding the confidentiality, integrity, and availability of electronically protected health information.

* Sarbanes-Oxley Act of 2002 (SOX) - applies to financial and accounting practices and the IT functions that support these practices.

* Gramm-Leach-Bliley Act (GLBA) - requires financial institutions to protect their customers' information against security threats.

Managing Computer Security Logs

One of the challenges to the effective management of computer security logs is balancing the availability of large amounts of log information with the limited availability of organizational resources for analysis of the data. A large amount of information is collected daily by a large number of logs, and there are increasing threats to networks and systems. Organizations could realize benefits in using the data to reduce risks, but the staff time and resources needed to perform the analyses and to manage the log information have to be taken into consideration.

The large number of log information sources may produce inconsistent and incompatible content, formats, and time stamp information, making it difficult for analysts to understand the meaning of the data collected. Organizations may have to utilize automated methods to convert logs with different content and formats to a single standard format with consistent data field representations.

Another challenge is protecting the confidentiality, integrity, and availability of log information. Information such as users' passwords and the content of e-mails may be captured by logs. This raises security and privacy concerns involving both the individuals that review the logs and others that might be able to access the logs through either authorized or unauthorized means. Logs that are secured improperly in storage or in transit might also be susceptible to alteration and destruction by both intentional and unintentional techniques. As a result, malicious activities might go unnoticed and evidence could be manipulated to conceal the identity of a malicious party.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

Log information should be analyzed on a regular basis and in a timely fashion by security, system, and network administrators. These staff members need support for their exacting tasks. They especially need training on how to carry out the log analysis procedures and how to prioritize their activities effectively. They should also be provided with tools that can automate portions of the analysis process, such as scripts and security software tools. These tools can be helpful in finding patterns that humans cannot easily perceive, such as correlating entries from multiple logs that are related to the same event. Analysis of logs by staff members has to be an ongoing activity so that organizations can predict future problems and prevent them. In the past, many logs have not been analyzed in a timely manner. When organizations do not institute sound processes for analyzing logs, the value of the logs is significantly reduced.

Organizations also need to protect the availability of their logs. Many logs have a maximum size; for example, the software is limited to storing the 10,000 most recent events, or keeping 100 megabytes of log data. When the size limit is reached, the log might overwrite old data with new data or completely stop collecting log information. Both of these outcomes result in the loss of availability of log data. To meet data retention requirements, organizations might need to keep copies of log files for a longer period of time than the original log sources can support. It may be necessary to establish processes to archive the log information.

Because of the volume of logs and the costs of archiving log data, it can be appropriate in some cases to reduce the logs by filtering out log entries that do not need to be archived. The confidentiality and integrity of the archived logs also need to be protected.

NIST Recommendations for Log Management

NIST recommends that organizations carry out the following actions for more

effective and efficient log management processes:

*** Establish policies and procedures for log management.** Organizations should develop standard processes for performing log management. In the planning process, logging requirements and goals should be defined. Based on those goals and requirements, an organization can then develop policies that clearly define mandatory requirements and suggested recommendations for log management activities, including log generation, transmission, storage, analysis, and disposal. An organization should also ensure that related policies and procedures incorporate and support the log management requirements and recommendations. The organization's management should provide the necessary support for the efforts involving log management planning, policy, and procedures development.

Policies and procedures help to assure a consistent approach and implementation of laws and regulatory requirements throughout the organization. Audits, testing, and validation procedures can help to assure that the logging standards and guidelines are being followed.

Requirements and recommendations for logging should be created in conjunction with an analysis of the technology and resources needed to implement the log management process. Generally, organizations should require logging and analyzing the data that is of the greatest importance, and should also have non-mandatory recommendations for the other types and sources of data that should be logged and analyzed if time and resources permit. In some cases, organizations can choose to have all or nearly all of its log data generated and stored for at least a short period of time in case it is needed. This policy gives greater weight to security considerations than to usability and resource usage. Also this policy can support better decision making in some cases. When establishing requirements and recommendations, organizations should strive to be flexible since each system is different and will log different amounts of data than other systems within the organization.

The organization's policies and procedures should also address the preservation of original logs. Many organizations send copies of network traffic logs to centralized devices. In addition, they may use tools that analyze and interpret network traffic. In cases where logs may be needed as evidence in proceedings, organizations may wish to acquire copies of the original log files, the centralized log files, and interpreted log data. This policy is useful in case there are any questions regarding the fidelity of the copying and interpretation processes. Retaining logs for evidence may involve the use of different forms of storage and different processes, such as putting additional restrictions on access to the records.

*** Prioritize log management appropriately throughout the organization.** After an organization defines its requirements and goals for the log management process, it should then prioritize its requirements and goals based on the organization's perceived reduction of risk and the expected time and resources needed to perform log management functions. An organization should also define roles and responsibilities for log management for key personnel throughout the organization, including establishing log management duties at both the individual system level and the log management infrastructure level.

*** Create and maintain a log management infrastructure.** A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data. Log management infrastructures normally perform several functions that support the analysis and security of log data. After establishing an initial log management policy and identifying roles and responsibilities, an organization should develop one or more log management infrastructures that can effectively support the policy and roles. Organizations should consider implementing log management infrastructures that includes centralized log servers and log data storage. When designing infrastructures, organizations should plan for both the current and future needs of the infrastructures and the individual log sources throughout the organization. Major factors that should be considered in the design include the volume of log data to be processed, network bandwidth, online and offline data storage, the security requirements for the data, and the time and resources needed for staff to analyze the logs.

*** Provide proper support for all staff with log management responsibilities.** To ensure that log management for individual systems is performed effectively throughout the organization, the administrators of those systems should receive adequate support. This should include disseminating information to log management staff, providing training, designating points of contact to answer questions, providing specific technical guidance, and making tools and documentation available.

*** Establish standard log management operational processes.** The major log management operational processes include configuring log sources, performing log analysis, initiating responses to identified events, and managing long-term storage. In addition, administrators have other responsibilities, such as:

* Monitoring the logging status of all log sources;

* Monitoring log rotation and archival processes;

* Checking for upgrades and patches to logging software, and acquiring, testing, and deploying them;

* Ensuring that each logging host's clock is synchronized to a common time source;

* Reconfiguring logging as needed, based on policy changes, technology changes, and other factors; and

* Documenting and reporting anomalies in log settings, configurations, and processes.

More Information

Other NIST publications that support log management processes include:

NIST SP 800-31, *Intrusion Detection Systems (IDS)*, provides information about hardware and software systems that

automate the processes of monitoring events occurring in computer systems and networks, and of analyzing them for signs of security problems.

NIST SP 800-40 version 2, *Creating a Patch and Vulnerability Management Program*, provides guidance on creating a security patch and vulnerability management program, and on testing the effectiveness of the program.

NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, provides guidance on the development of policies to guide the selection, installation and maintenance of firewalls that protect systems connected to the Internet and to other networks.

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, discusses how to protect the confidentiality, integrity, and availability of data, applications, and operating systems by preventing and handling incidents involving the insertion of malicious code and software into systems.

These and other NIST publications can help you in planning and implementing a comprehensive approach to IT security.

Information about the NIST publications that are referenced in this bulletin, as well as other security-related publications, is available at http://csrc.nist.gov/publications/index.html

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.