September 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

FORENSIC TECHNIQUES: HELPING ORGANIZATIONS IMPROVE THEIR RESPONSES TO INFORMATION SECURITY INCIDENTS

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

Digital forensic techniques involve the application of science to the identification, collection, examination, and analysis of data in ways that preserve the integrity of the information and maintain a strict chain of custody for the data. Organizations have the means to collect growing amounts of data from many sources. Data is stored or transferred by standard IT systems, networking equipment, computing peripherals, personal digital assistants (PDAs), consumer electronic devices, and various types of media. When information security incidents occur, organizations that have established a capability to apply digital forensic techniques can examine and analyze the data that they have collected, and determine if their systems and networks may have sustained any damage and if sensitive data may have been compromised. Digital forensic techniques can be used for many purposes, such as supporting the investigation of crimes and violations of internal policies, analyses of security incidents, reviews of operational problems, and recovery from accidental system damage.

Guide to Integrating Forensic Techniques into Incident Response

NIST's Information Technology Laboratory recently issued Special Publication (SP) 800-86, *Guide to Integrating Forensic Techniques into Incident Response*. Written by Karen Kent and Tim Grance of NIST, and by Suzanne Chevalier and Hung Dang of Booz Allen Hamilton, the guide provides detailed information on how an organization can establish a forensic capability and develop the needed fundamental policies and procedures that will guide the use of forensics. The focus is on helping organizations use forensic techniques to aid in the investigation of computer security incidents and in troubleshooting other information technology (IT) operational problems.

The publication describes the processes for performing effective forensics activities and recommends ways to use the many data sources that are available for collection, examination, and analysis. Forensic techniques are discussed from the IT perspective, rather than from the law enforcement standpoint. While it is not an all-inclusive step-by-step guide for executing a digital forensic investigation or a source of legal advice, the publication is a useful source of information on applying forensic technologies within the context of performing incident response or troubleshooting activities.

Issues covered in the guide include the need for computer and network forensics; how to establish and organize a forensics capability; and the basic steps of data collection, examination, analysis, and reporting. Case studies are provided to illustrate how data analyses can correlate events among several data sources. The appendices summarize the major recommendations in a convenient format and provide scenarios in which the application of forensics techniques might be appropriate. Also included in the appendices are a glossary, an acronym list, a list of in-print references, online tools, and other resources that support the establishment of a forensics capability and awareness of forensics tools and techniques.

The guide is available at http://csrc.nist.gov/publications/nistpubs/.

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 October 2005:

Why Forensics Techniques Are Needed for Information Security

Forensic science is generally defined as the application of science to the law. Over the last decade, the number of crimes that involve computers has grown, spurring an increase in companies and products that assist personnel in using computer-based evidence to determine the details of computer-related incidents. As a result, digital forensic tools and techniques have evolved to enable organizations to properly provide computer crime data to courts. In addition to assisting with criminal investigations and the handling of computer security incidents, digital forensic tools and techniques are valuable for many other organizational and security-related tasks, such as:

* troubleshooting operational issues: finding the virtual and physical location of a host with an incorrect network configuration; resolving a functional problem with an application; and recording and reviewing the current operating system (OS) and application configuration settings for a host.

* log monitoring: analyzing log entries and correlating log entries across multiple systems; assisting in incident handling; identifying policy violations; and auditing and other related efforts.

* recovering lost data from systems, including data that has been accidentally or purposely deleted or otherwise modified.

* acquiring data, for possible future use from hosts that are being redeployed or retired: acquiring and storing the data from a user's workstation when the user leaves the organization. The workstation's media can then be sanitized to remove all of the original user's data.

* protecting sensitive information and maintaining certain records for audit purposes: enabling organizations to notify other agencies or individuals when protected information is exposed to other parties.

The Forensic Process

NIST SP 800-86 describes a four-step process for applying digital forensic techniques in a consistent manner:

Collection. Data is identified, labeled, recorded and acquired from all of the possible sources of relevant data, using procedures that preserve the integrity of the data. Data should be collected in a timely manner to avoid the loss of dynamic data, such as a list of current network connections, and the data collected in cell phones, PDAs, and other battery-powered devices.

Examination. The data that is collected should be examined using a combination of automated and manual methods to assess and extract data of particular interest for the specific situation, while preserving the integrity of the data.

Analysis. The results of the examination should be analyzed, using well-documented methods and techniques, to derive useful information that addresses the questions that were the impetus for the collection and examination.

Reporting. The results of the analysis should be reported. Items to be reported may include: a description of the actions employed; an explanation of how tools and procedures were selected; a determination of any other actions that should be performed, such as forensic examination of additional data sources, securing identified vulnerabilities, and improving existing security controls; and recommendations for improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

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.

Forensics in the Information System Development Life Cycle

Many computer incidents can be handled more efficiently and effectively if forensic considerations have been incorporated into the information system life cycle. NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, presents a framework for incorporating security into all phases of the life cycle, and for selecting appropriate, cost-effective security controls. NIST SP 800-64 is available at: http://csrc.nist.gov/publications/nistpubs/.

Examples of these life cycle considerations include:

* Performing regular backups of systems and maintaining previous backups for a specific period of time;

* Enabling auditing on workstations, servers, and network devices;

* Forwarding audit records to secure centralized log servers;

* Configuring mission-critical applications to perform auditing, including recording all authentication attempts;

* Maintaining a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets;

* Maintaining records of network and system configurations; and

* Establishing data retention policies that support performing historical reviews of system and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed.

Summary of Recommendations for Using Forensic Techniques

NIST recommends that organizations carry out the following actions to establish, organize, and use forensic techniques effectively:

* **Develop organizational policies that contain clear statements** addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures.

High-level policies should allow authorized personnel to monitor systems and networks and to perform investigations for legitimate reasons under appropriate circumstances. Organizations may also adopt a separate forensic policy for incident handlers and others with forensic roles; this policy should provide more detailed rules concerning appropriate behavior. Forensic policy should clearly define the roles and responsibilities of all staff members and external organizations performing or assisting with the organization's forensic activities.

Organizations usually rely on a combination of their own staff and external groups to perform forensic tasks. Some organizations perform standard tasks themselves and use outside parties only when specialized assistance is needed for demanding tasks, such as sending physically damaged media to a data recovery firm for reconstruction, or having specially trained law enforcement personnel or consultants collect data from cell phones and similar sources. These tasks usually require the use of specialized software, equipment, facilities, and technical expertise that many organizations cannot afford to acquire and maintain.

The organizational policy should clearly indicate who should contact specified internal teams and external organizations, and the policy should clearly define the circumstances for making the contacts. When deciding which internal or external parties should handle each aspect of forensics, organizations should consider factors such as personnel and equipment costs for collecting data; the time needed for internal or external teams to respond to incidents; and data sensitivity and privacy issues.

*** Create and maintain procedures and guidelines for performing forensic tasks**, based on the organization's policies and all applicable laws and regulations. The procedures and guidelines should focus on general methodologies for investigating incidents using forensic techniques, since it is not feasible to develop comprehensive procedures tailored to every possible situation. Consideration should be given to developing step-by-step procedures for performing routine tasks. The procedures and guidelines should facilitate consistent, effective, and accurate actions. This is especially important for handling incidents that may lead to prosecution or internal disciplinary actions. When decision makers handle the forensic data evidence in a sound, thorough manner, they are in a position to take necessary follow-up actions with confidence.

The organization's procedures and guidelines should support the admissibility of evidence into legal proceedings, and should include information on gathering and handling evidence properly, preserving the integrity of tools and equipment, maintaining the chain of custody, and storing the evidence appropriately. Because electronic logs and other records can be altered or otherwise manipulated, organizations should be prepared, through their policies, guidelines, and procedures, to demonstrate the integrity of their records. The procedures and guidelines should be reviewed periodically and when any changes are made to the policies and procedures of the incident handling teams.

* Develop organizational policies and procedures that **support the reasonable and appropriate use of forensic tools.**

Organizational policies and procedures should clearly explain what forensic actions should and should not be performed under various circumstances, as well as describing the necessary safeguards for sensitive information that might be recorded by forensic tools, such as passwords, personal data, Social Security numbers, and the contents of e-mails. Legal advisors should carefully review all forensic policies and high-level procedures.

The organization's policies and procedures on the use of forensic tools should address the use of anti-forensic tools and techniques, which are designed to conceal or destroy data so that others cannot access it. There are many uses for anti-forensic software, such as removing data from computers and media that are to be discarded. Recently issued NIST SP 800-88, *Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology*, provides help to organizations in securely managing the information processed and stored on devices and media. The guide on media sanitization was discussed in the August ITL Bulletin and is available at: http://csrc.nist.gov/publications/nistbul/index.html.

* **Prepare IT professionals** to support and participate in forensic activities.

IT professionals throughout the organization, especially incident handlers and other first responders to incidents, should understand their roles and responsibilities for forensics. They should receive training and education on forensic–related policies and procedures, and be prepared to cooperate with and assist others when the technologies for which they are responsible are part of an incident or other event. IT professionals should also consult closely with legal counsel in general preparation for forensics activities to determine which actions IT professionals should and should not perform. The consultation with legal counsel should also take place on an as-needed basis to discuss specific forensics situations. The organizational management should be responsible for supporting forensic capabilities, reviewing and approving forensic policy, and approving certain forensic actions, such as taking mission-critical systems off-line.

Incident handlers performing forensic tasks should have a broad knowledge of forensic principles, guidelines, procedures, tools, and techniques, as well as anti-forensic tools and techniques that could conceal or destroy data. It is also helpful if incident handlers have knowledge of technical issues involving information security, operating systems, file systems, applications, and networks. Training courses help to build competence in forensics among technical support staff, system and network administrators, and other IT professionals. Interactions between incident handlers and IT

professionals can be effective in promoting the understanding of forensics tools and in identifying potential shortcomings in forensics capabilities.

For More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to IT security.

For information about NIST standards and guidelines that are referenced in the forensics techniques guide, as well as other security-related publications, see 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.