November 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

USING STORAGE ENCRYPTION TECHNOLOGIES TO PROTECT END USER DEVICES

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

End user devices, such as personal computers, portable electronic devices, and removable storage media, are vulnerable to many threats that can endanger the confidentiality of the information stored on the devices and enable unauthorized persons to gain access to the stored information. The threats can be both unintentional, such as the loss of a portable device, and intentional, such as directed attacks that result in disruption, identity theft, and other fraud.

End user devices include:
* personal computers - desktop or laptop;
* consumer devices - personal digital assistants (PDAs), smart phones; and
* removable storage media - Universal Serial Bus (USB) flash drives, memory cards, external hard drives, writeable disks (CD or DVD).

Security controls can be effectively applied to protect the sensitive information and particularly the personally identifiable information (PII) stored on end user devices. The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued a new guide to help organizations secure their end user devices and deter unauthorized parties from accessing the stored information. The guide focuses on the application of encryption and authentication techniques, which are the primary security controls for restricting access to sensitive information.

Guide to Storage Encryption Technologies for End User Devices

NIST Special Publication (SP) 800-111, *Guide to Storage Encryption Technologies for End User Devices*, was written by Karen Scarfone and Murugiah Souppaya of NIST, and by Matt Sexton of Booz Allen Hamilton. The publication addresses the basic concepts of storage encryption for end user devices, providing information that enables organizations to plan, implement, and maintain effective storage encryption solutions. Topics discussed include the three classes of storage encryption techniques (full disk encryption, volume and virtual disk encryption, and file/folder encryption), the protections provided by the three classes of techniques, and the role of cryptography and authentication in implementing storage encryption solutions.

The appendices to the guide include a description of the some of the alternate methods available for protecting stored information on end user devices, a glossary, an acronym list, and a reference list of online tools and resources. These references provide useful information to help organizations gain a better understanding of the use of storage encryption for protecting end user devices.

NIST SP 800-111 is available at http://csrc.nist.gov/publications/PubsSPs.html.

Storage Devices and the Need for Security Controls

One of the many threats to the confidentiality of information stored on end user devices is the insertion of malicious code or malware, which includes viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware. Malware attacks compromise the confidentiality, integrity, or availability of the organization's data, applications, or operating system, and give attackers unauthorized access to a storage device.

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 2006:

They can then transfer information from the device to the attacker's system and carry out other actions that jeopardize the confidentiality of the information on a device.

Another common threat is loss or theft of an end user device. Someone with physical access to a lost or stolen device has many options for viewing the information stored on the device. Insider attacks are also a concern. For example, an employee may attempt to access sensitive information stored on another employee's device or access another user's files on a device that the two users share.

These threats, as well as threats to other aspects of information system operation and management, should be addressed by the implementation of appropriate controls that are managed within a comprehensive information security program. Federal agencies are directed by the Federal Information Security Management Act (FISMA) to develop, document, and implement agency-wide information security programs and to provide information security for the information and information systems that support the organization's operations and assets.

Standards and guidelines developed by NIST help federal agencies meet their responsibilities under FISMA. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, helps agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, guides agencies in determining minimum security requirements for seventeen security-related areas and in selecting an appropriate set of security controls to satisfy the minimum requirements.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides information about recommended security controls, including controls related to storage security, such as controlling access through encryption of stored information, restricting access to mobile computing devices and information system media, and storing media in physically secure locations.

In addition to FISMA, federal agencies are also required by Office of Management and Budget (OMB) Memorandum M-06-16 to protect agency information that is either "accessed remotely or physically transported outside of the agency's secured, physical perimeter." M-06-16 specifically requires that agencies encrypt all data stored on mobile computing devices, such as laptops and personal digital assistants (PDAs), unless the data has been determined by the designated agency official to be nonsensitive. Additional requirements for federal agencies to protect sensitive personal information are included in the Privacy Act of 1974, the Gramm-Leach Bliley Act, and the Health Insurance Portability and Accountability Act of 1966 (HIPAA).

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.

Storage Encryption Solutions

Encryption and authentication methods are the primary security controls for restricting access to sensitive information stored on end user devices. FIPS have been issued specifying methods for encryption, message authentication, and security requirements for cryptographic modules. See the More Information section at the end of this bulletin for access to NIST resources on security-related FIPS and guidelines.

Encryption can be used to encrypt an individual file containing sensitive information or to encrypt all stored data. Three types of encryption methods are available: full disk encryption, volume and virtual disk encryption, and file/folder encryption. Issues to be considered in selecting the appropriate encryption solution for a particular situation include the type of storage, the amount of information that needs to be protected, the environments where the storage will be located, and the threats that need to be mitigated. A chart in NIST SP 800-111 compares the protections and other characteristics of the different storage encryption technologies.

Full disk encryption (FDE). Also known as whole disk encryption, full disk encryption is the process of encrypting all the data on the hard drive used to boot a computer, including the computer operating system (OS), and permitting access to the data only after successful authentication to the FDE software product.

Most FDE products are software-based and are mostly used on desktop and laptop computers. The requirement for pre-boot authentication means that users have to be able to authenticate their identity using the fundamental components of a device, such as a standard keyboard. Since the OS is not loaded, OS-level drivers are unavailable. For example, a PDA or smart phone could not display a keyboard on the screen for entering a password because that is an OS-level capability.

Protection Offered: For a computer that has not been booted, all the information encrypted by FDE is protected, assuming that pre-boot authentication is required. When the device is booted, then FDE provides no protection; once the OS is loaded, the OS becomes fully responsible for protecting the unencrypted information. However, when the device is in a hibernation mode, most FDE products can encrypt the hibernation file.

Virtual disk and volume encryption. Virtual disk encryption involves encrypting a file called a *container*, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided. In this case, the container is typically mounted as a virtual disk. Virtual disk encryption is used on all types of end user device storage. The container is a single file that resides within a logical volume. Examples of volumes are boot, system, and data volumes on a personal

computer and a USB flash drive formatted with a single filesystem. Volume encryption involves encrypting an entire logical volume and permitting access to the data on the volume only after proper authentication is provided. Volume encryption is most often performed on hard drive data volumes and volume-based removable media, such as USB flash drives and external hard drives.

Protection Offered: When virtual disk encryption is employed, the contents of containers are protected until the user is authenticated for access to the containers. In the case of a single sign-on being used for authentication, the containers are usually protected until the user logs onto the device. If a single sign-on is not used, then protection is typically provided until the user explicitly authenticates to a container. Virtual disk encryption does not provide any protection for data outside the container, including swap and hibernation files. These files could contain the contents of unencrypted files that were being held in memory. Volume encryption provides the same protection as virtual disk encryption, but for a volume instead of a container.

File/folder encryption. This method consists of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. Folder encryption is very similar to file encryption, but addressing individual folders instead of files. Some OSs offer built-in file and/or folder encryption capabilities, and many third-party programs are also available for this encryption process. Folder encryption and virtual disk encryption differ in that virtual disk encryption involves a container, which is a single opaque file. No one can see what files or folders are inside the container until the container is decrypted. File/folder encryption is transparent, making it possible for anyone with access to the filesystem to view the names and possibly other metadata for the encrypted files and folders, including the files and folders within encrypted folders, unless they are protected through OS access control features. File/folder encryption is used on all types of storage for end user devices.

Protection Offered: File/folder encryption protects the contents of encrypted files, including the files in encrypted folders, until the user is authenticated for the files or folders. When a single sign-on is used, the files are normally protected until the user logs onto the device. When a single sign-on is not used, protection is typically provided until the user explicitly authenticates to a file or folder. File/folder encryption does not provide any protection for data outside the protected files or folders, including swap and hibernation files, which could contain the contents of unencrypted files that were being held in memory. File/folder encryption software also cannot protect the confidentiality of filenames and other file metadata. This situation can result in attackers getting access to valuable information such as files that are named by Social Security number.

NIST Recommendations

NIST advises that organizations implement the following recommendations to facilitate more efficient and effective design, implementation, and management of storage encryption solutions for end user devices:

Consider solutions that use existing system features and infrastructure when selecting a storage encryption technology. Organizations have many factors to consider when they are selecting storage encryption solutions, including the platforms they support, the data they protect, and the threats they mitigate. Some solutions involve deploying various servers and installing software on the devices to be protected, while other solutions can use existing servers, as well as software built into the devices to be protected, such as FIPS-approved encryption features built into the devices' operating systems. When the changes to the infrastructure and devices are more extensive, it is more likely that the storage encryption solution will cause a loss of functionality or other problems with the devices. When evaluating solutions, organizations should compare the loss of functionality with the gain in security capabilities and decide if the trade-off is acceptable. Solutions that require extensive changes to the infrastructure and end user devices should generally be used only when other solutions cannot meet the organization's needs.

Use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments. Centralized management, which is an effective and efficient practice for policy verification and enforcement, key management, authenticator management, data recovery, and other management processes, is also recommended for most storage encryption deployments. Centralized management can also be an effective practice for automating the deployment and configuration of storage encryption software to end user devices, for distributing and installing updates, for collecting and reviewing logs, and for recovering information from local failures.

Ensure that all cryptographic keys used in a storage encryption solution are secured and managed properly to support the security of the solution. Storage encryption technologies use one or more cryptographic keys to encrypt and decrypt the data that they protect. When a key is lost or damaged, organizations may not be able to recover encrypted data from the computer. Therefore, organizations should carefully plan their key management processes, procedures, and technologies before implementing storage encryption technologies. This planning should include all aspects of key management, including key generation, use, storage, recovery, and destruction. Organizations should carefully consider how key management practices can support the recovery of encrypted data if a key is inadvertently destroyed or otherwise becomes unavailable. Organizations planning on encrypting removable media also need to consider how changing keys will affect access to encrypted data stored on removable media. They should develop feasible solutions, such as retaining the previously used keys in case they are needed.

Select appropriate user authenticators for storage encryption solutions. When storage encryption solutions are employed, users must authenticate successfully before accessing the information that has been encrypted. Common authentication mechanisms are passwords, personal

identification numbers, cryptographic tokens, biometrics, and smart cards. Instead of adding new authenticators for their users, organizations should consider leveraging existing enterprise authentication solutions, such as Active Directory and public key infrastructure (PKI) techniques. This practice is generally acceptable when two-factor authentication is used. However, using the same single-factor authenticator for multiple purposes, such as operating system (OS) authentication and storage encryption authentication, significantly weakens the protection that the authentication process provides. For example, an attacker who learns a single password could gain full access to the device's information. Organizations should carefully consider the security implications of using the same single-factor authenticator for multiple purposes. In particular, organizations should not use email passwords and other passwords, sometimes transmitted in plaintext, as single-factor authenticators for storage encryption.

Implement measures that support and complement storage encryption implementations for end user devices. Since storage encryption alone cannot provide adequate security for stored information, additional security controls are needed. Federal organizations categorizing their systems according to FIPS 199 should select and deploy the necessary controls based on the potential impact of a security breach involving a particular system. Management, operational, and technical controls are explained in NIST SP 800-53.

Some examples of supporting controls are:

* Revising organizational policies as needed to incorporate appropriate usage of the storage encryption solution;
* Securing and maintaining end user devices properly to reduce the risk of compromise or misuse. This includes securing device operating systems, applications, and communications, and physically securing devices; and
* Making users aware of their responsibilities for storage encryption, such as encrypting sensitive files, physically protecting mobile devices and removable media, and promptly reporting loss or theft of devices and media.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. For information about NIST standards and guidelines that are referenced in NIST SP 800-111 and other security-related publications, covering related topics, such as protecting active content, electronic mail, and servers, see http://csrc.nist.gov/publications/index.html Selected publications specifically related to the guide include:

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for federal information and information systems in seventeen security-related areas that represent a broad-based, balanced information security program.

NIST SP 800-21, Second Edition, *Guideline for Implementing Cryptography in the Federal Government*, helps agencies select, specify, employ, and evaluate cryptographic protection mechanisms for federal information systems.

NIST SP 800-53, *Minimum Security Controls for Federal Information Systems*, provides guidance in selecting, specifying, and tailoring security controls that will provide an appropriate level of security, based on the organization's assessment of mission risk.

Draft NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, will assist organizations in developing an effective assessment plan.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, assists organizations in identifying information types and impact levels, and assigning impact levels for confidentiality, integrity, and availability.

NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, summarizes the HIPAA security standards and explains the structure and organization of the Security Rule.

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.