ITL BULLETIN FOR JUNE 2011

GUIDELINES FOR PROTECTING BASIC INPUT/OUTPUT SYSTEM (BIOS) FIRMWARE

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Modern personal computers (PCs) rely on the Basic Input/Output System (BIOS) to perform fundamental systems functions when the computer is turned on. The first software program executed on the main central processing unit (CPU) at startup, the system BIOS is stored in non-volatile memory and is called boot firmware. It initializes and tests hardware components, such as the keyboard, the screen, and the mouse, and it loads the PC's operating system. In addition, the system BIOS loads and initializes important systems management functions, including power and thermal management.

The system BIOS, which may be developed by original equipment manufacturers (OEMs) or by independent BIOS vendors, is distributed to end-users with computer hardware. The system BIOS is usually stored on electrically erasable programmable read-only memory (EEPROM) or other forms of flash memory, and can be modified and updated by end users, using a utility or special program. Manufacturers of BIOS firmware frequently provide updates for the system firmware to fix bugs, patch vulnerabilities, and support new hardware.

There are several different types of system BIOS firmware. The most widely used in desktop and laptop systems are the conventional BIOS and the Unified Extensible Firmware Interface (UEFI), a more recent industry specification, used in newer systems.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently issued guidelines to assist organizations in protecting the security of their systems and in preventing the unauthorized modification of system BIOS firmware on PC client systems. The new publication, NIST Special Publication 800-147, *BIOS Protection Guidelines: Recommendations of the National Institute of Standards and Technology*, focuses on current and future x64 and x86 client platforms. The recommended controls and procedures are applicable to most system designs, and are oriented toward enterprise-class platforms. The technologies discussed are also expected to be part of consumer-grade systems in the future.

NIST Special Publication (SP) 800-147, *BIOS Protection Guidelines: Recommendations of the National Institute of Standards and Technology*

Written by David Cooper, William Polk, Andrew Regenscheid, and Murugiah Souppaya of NIST, SP 800-147 provides technical recommendations for BIOS and platform vendors, and for information system security professionals who are responsible for managing the security of PC systems, secure boot processes, and hardware security modules. The guidelines assist organizations in developing procurement and deployment strategies for new systems.

NIST SP 800-147 provides background information on BIOS and its role in the boot process, and identifies potential attacks against the BIOS in operational environments. Diagrams depict the boot process for conventional BIOS and UEFI systems. A section of the guide presents security guidelines for BIOS implementations and recommended practices for managing the system BIOS. The guidelines for the secure updating of BIOS assist platform vendors in their processes of designing, implementing, or selecting a system BIOS implementation. Organizations developing procurement strategies for secure BIOS systems can use the recommended product features in their plans to acquire new, secure commercial products as they become available.

In addition, NIST SP 800-147 addresses BIOS management issues in enterprise operational environments. The focus is on the key activities that organizations should carry out related to provisioning, deploying, managing, and decommissioning the system BIOS as part of the overall platform life cycle. The recommendations focus on preventing the unauthorized modification of the BIOS. Organizations can also use the recommended BIOS management practices when developing their plans for future systems.

The appendices to NIST SP 800-147 include a summary of the security guidelines for system BIOS implementations, definitions of the terms used, a list of acronyms and abbreviations used, and a list of references.

NIST SP 800-147 is available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

Security Concerns and Threats to BIOS

Because of the key role of the BIOS in the PC architecture, unauthorized modification of BIOS firmware is a significant threat to system security. Modification could result in the insertion of malicious software as part of a sophisticated, targeted attack on an organization or denial of service of the computer systems with the targeted BIOS.

The system BIOS is a potentially attractive target for attack. The move from conventional BIOS implementations to implementations based on the UEFI, a common specification, may make it easier for attackers to target the BIOS with malware.

Malicious code running at the BIOS level could exert control over a computer system. It could be used to compromise components that are loaded later in the boot process, including the System Management Mode (SMM) code, boot loader, hypervisor, and operating system. Because the BIOS runs early in the boot process with very high privileges on the machine, malware running at the BIOS level may be difficult to detect. Because the BIOS is loaded first, there is no opportunity for anti-malware products to scan the BIOS.

The integrity of the system BIOS can be threatened as the system moves through the supply chain. Management procedures discussed later in this bulletin can help to identify and remedy systems that have an unapproved system BIOS.

Systems installed with the manufacturer's intended system BIOS are vulnerable to threats such as:

• **User-initiated installation of a malicious system BIOS**. User-initiated BIOS update utilities are often the primary method for updating the system BIOS. Technical guidelines alone will not prevent users from installing unapproved BIOS images if they have physical access to the computer system. Organizational security policies and procedures are needed to monitor, detect, and remediate the unapproved system BIOS, or initiate a recovery process to restore an approved BIOS.

• **Malware attacks.** Malware could leverage weak BIOS security controls or exploit vulnerabilities in the system BIOS itself to reflash or modify the system BIOS. General-purpose malicious software is unlikely to include this functionality, but a targeted attack on an organization could be directed towards the organization's standard system BIOS. The malicious BIOS could be delivered to the system either over a network or using media.

• **Organization-wide attacks.** Network-based system management tools could also be used to launch an organization-wide attack on the system BIOS. For example, an organization-maintained update server for the organization's deployed system BIOS could be compromised and could push a malicious system BIOS to computer systems across the organization. This is a high-impact attack that requires either an insider agent or a compromise of an organization's update process.

• **Rollback to a vulnerable system BIOS.** Any of the preceding mechanisms could be used to roll back to an authentic but vulnerable system BIOS. This is a particularly insidious attack, since the vulnerable BIOS is authentic and had been shipped by the manufacturer. Organizational security controls are needed to verify the source and integrity of the system BIOS.

Security Guidelines for System BIOS Implementations

NIST recommends the following practices to provide for a secure BIOS update process that includes a process for verifying the authenticity and integrity of BIOS updates, and a mechanism for ensuring that the BIOS is protected from modification outside of the secure update process.

These security guidelines, which assist platform vendors in designing, implementing, or selecting a system BIOS implementation, do not prevent all risks, such as individuals with physical access to systems from modifying the system BIOS. Organizational security policies and procedures are essential.

• **BIOS Update Authentication.** The authenticated BIOS update mechanism employs digital signatures to ensure the authenticity of the BIOS update image. NIST standards and guidelines specifying the application of digital signatures, key sizes, and encryption algorithms are listed in the **For More Information** section below. The authenticated update mechanism may be designed so that organizations can control the update process by permitting updates to the BIOS or rollbacks of the BIOS to an earlier version only if the update or rollback has been authorized by the organization.

• **Secure Local Update.** An optional secure local update mechanism requires a physical presence to authorize the installation of BIOS update images. BIOS implementations may optionally include a secure local update mechanism that updates the system BIOS without using the authenticated update mechanism. The secure local update mechanism, if it is implemented, should be used only to load the first BIOS image or to recover from a corruption of a system BIOS that cannot be fixed using the authenticated update mechanism. A secure local update mechanism should ensure the authenticity and integrity of the BIOS update image by requiring a physical presence. Further protections may be implemented in the secure local update mechanism to require the entry of an administrator password or the unlocking of a physical lock (e.g., a motherboard jumper) before permitting the system BIOS to be updated.

• **Integrity Protection.** Integrity protection features are used to prevent unintended or malicious modification of the BIOS outside the authenticated BIOS update process. The protection mechanism should be protected from unauthorized modification. The protection mechanism should protect relevant regions of the system flash memory containing the system BIOS prior to executing firmware or software that can be modified without using an authenticated update mechanism or a secure local update mechanism. Protections should be enforced by hardware mechanisms that are not alterable except by an authorized mechanism.

• **Non-bypassability.** Non-bypassability features ensure that there are no mechanisms that allow the system processor or any other system component to bypass the authenticated update mechanism. The authenticated BIOS update mechanism should be the exclusive mechanism for modifying the system BIOS when there is no physical intervention through the secure local update mechanism. The design of the system and accompanying system components and firmware should ensure that there are no mechanisms that allow the system processor or any other system component to bypass the authenticated update mechanism, except for the secure local update mechanism.

Recommended Practices for BIOS Management

NIST recommends that organizations adopt the following management practices, which complement the security guidelines. The five phases of the platform life cycle to be addressed are:

• **Provisioning Phase,** which establishes configuration baselines identifying the approved BIOS version and configuration settings. It is important that the organization institute a mechanism for identifying, inventorying, and tracking the different computer systems across the enterprise throughout their life cycle.

Identifying and monitoring the BIOS image characteristics, such as manufacturer name, version, or time stamp, allows the organization to perform update, rollback, and recovery. The organization should maintain a “golden master image” for each approved system BIOS, including superseded versions, in secure offline storage.

Protection of keys and algorithms used in the authentication process depends upon the BIOS product that an organization uses. See the guide for details on the maintenance of keys. Private keys should be maintained under multiparty control to protect against insider attacks. For organizational keys, the corresponding public keys must also be maintained securely.

In addition, a common configuration baseline for each platform must be created to conform to the organization’s policy. The baseline should ensure that the integrity protection and non-bypassability features are enabled (if they are configurable), and that organization policies for password policy and device boot order are enforced. The BIOS image information and associated baseline of settings for each platform should be documented in the configuration management plan.

• **Platform Deployment Phase**, which establishes or verifies the configuration baseline using a secure local update mechanism. The secure local update process should be used to provision the approved BIOS for that platform from the golden master image; the corresponding authentication procedures should be installed; and BIOS-related configuration parameters established before computer systems are deployed. This will help the organization to maintain a consistent, known starting baseline. The organization should periodically perform assessments to confirm that the organization’s BIOS policies, processes, and procedures are being followed properly.

• **Operations and Maintenance Phase**, which provides that systems are monitored for unexpected changes, and planned BIOS updates are executed using the authenticated BIOS update mechanism. This phase includes the operations and maintenance activities that are important for maintaining BIOS security and reliability in the operational environment. System BIOS updates should be performed using a change management process, and the new approved version should be documented in the configuration plan, noting that the previous BIOS image has been superseded.

The BIOS image and configuration baseline should be continuously monitored. If an unapproved deviation from this baseline is detected, the event should be investigated, documented, and remediated as part of incident response activities. The incident response plan should document the process and set of authorized tools that can be used to capture the evidence to help determine the root cause. The secure local update mechanism should be used to recover from a BIOS image compromise.

When a new BIOS image is required to extend system capabilities, improve system reliability, or remediate software vulnerabilities, BIOS updates should be performed using the authenticated update process. When the organization participates actively in the update process, the multiparty control process must be executed to retrieve the private key from secure storage and generate the digital signature. The BIOS installation package should also be signed, and the digital signature should be verified before execution. Once the update has executed successfully, the configuration baseline should be validated to confirm that the computer system is still in compliance with the organization’s defined policy.

• **Recovery Phase**, which supports authorized rollback to an earlier BIOS version and recovery from a corrupted BIOS. In some circumstances, a BIOS update will be required that cannot be accomplished using the authenticated update process. In other cases, a BIOS update may have unintended consequences, forcing the organization to roll back to an earlier version. Extra steps may be required for an authenticated update to authorize a rollback, or the secure local update process may be required to reestablish a secure baseline. As with the Operations and Maintenance phase, it is essential to validate the configuration of the BIOS against the organization’s defined policy after BIOS rollback or reinstallation.

• **Disposition Phase**, which restores the BIOS and configuration data to their original settings to protect against accidental information leakage. Before the computer system is discarded by the organization, sensitive data from the system BIOS should be removed or destroyed. The configuration baseline should be

reset to the manufacturer's default profile, sensitive settings such as passwords should be deleted from the system, and keys should also be removed from the key store. If the system BIOS includes any organization-specific customizations, a vendor-provided BIOS image should be installed. This phase of the platform life cycle reduces chances for accidental data leakage.

For More Information

NIST publications that are cited in SP 800-147 include:

Federal Information Processing Standard (FIPS) 180-3, *Secure Hash Standard (SHS)*
FIPS 186-3, *Digital Signature Standard (DSS)*
NIST Special Publication (SP) SP 800-61 Rev1, *Computer Security Incident Handling Guide*
NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*
NIST SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*

For information about these NIST standards and guidelines, as well as other security-related publications, see the NIST Web page http://csrc.nist.gov/publications/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov.