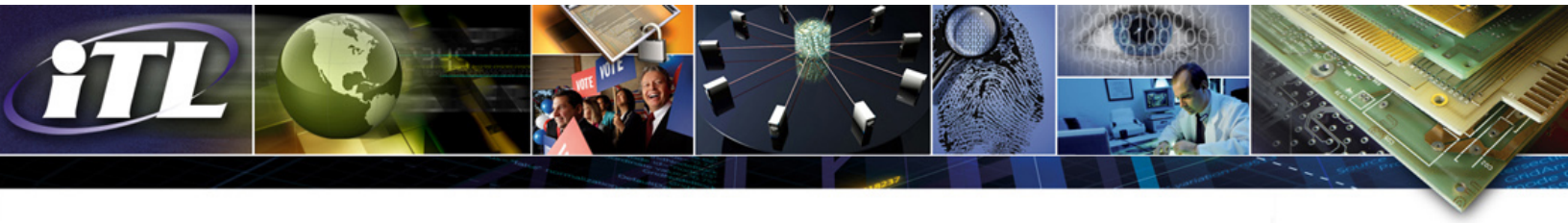


ITL BULLETIN FOR OCTOBER 2014

RELEASE OF NIST SPECIAL PUBLICATION 800-147B, BIOS PROTECTION GUIDELINES FOR SERVERS

Andrew Regenscheid, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

Modern computers rely on fundamental system firmware, commonly known as the Basic Input/Output System (BIOS), to enable system components to communicate and work together. The BIOS is typically developed by both original equipment manufacturers and independent BIOS vendors. Manufacturers frequently update system firmware to fix bugs, patch vulnerabilities, and support new hardware, but an unauthorized update constitutes a significant threat because of the BIOS's unique and privileged position within the computing architecture. Intentionally damaging the BIOS could prevent a computer from booting, perhaps permanently damaging the device. Similarly, inserting malicious software into the BIOS could be very difficult to detect or correct, since the BIOS runs before most anti-malware countermeasures. In such a case, even reformatting or replacing hard drives wouldn't clean it, since the BIOS is stored on flash memory on the motherboard. These concerns have been demonstrated in actual attacks on real-world systems: the CIH virus wiped BIOS contents, essentially destroying systems in the late 1990s, and the Mebromi Trojan horse virus injected malicious code in BIOS firmware in 2011.

BIOS protections can significantly mitigate these threats by attempting to block attackers from tampering with the BIOS. A protected BIOS can serve as an important root of trust from which to gain more confidence in the security of the rest of the system. This is especially important for server computing systems.

Introduction to NIST Special Publication 800-147B

To provide guidance on securing BIOS on server-class systems, ITL produced a new publication, NIST Special Publication (SP) 800-147B, *BIOS Protection Guidelines for Servers*. This publication joins NIST SP 800-147, *BIOS Protection Guidelines*, released in April 2011, that provided guidelines for desktop and laptop systems deployed in enterprise environments.

Compared to client systems, the design of servers can vary significantly, with many servers offering remote management capabilities and multiple BIOS update mechanisms. SP 800-147B includes BIOS protections for basic, managed, and blade servers. These types of servers often contain Service Processors – specialized microcontrollers that provide administrators with an interface to manage the host server. SP 800-147B guidelines are intended to help secure BIOS update mechanisms so that only authentic, authorized BIOS images are written to BIOS flash memory. While client systems typically have

only one path for updating the BIOS, server systems may implement several update mechanisms to allow administrators to update the BIOS from different environments. SP 800-147B provides detailed recommendations on how the BIOS protections could be implemented with one or more of the following general types of authenticated update mechanisms:

- Authenticated BIOS update that can occur anytime;
- Authenticated BIOS update on reboot; or
- BIOS update at runtime and verification of BIOS on reboot.

The security guidelines in SP 800-147B do not attempt to prevent installation of inauthentic BIOS through the supply chain, by physical replacement of the BIOS chip, or through secure local update procedures, as administrators may have a need to customize BIOS on their systems. The foundation for the BIOS protections is the Root of Trust for Update (RTU). This trusted component, a combination of hardware and firmware, is responsible for verifying and performing updates and for enforcing write protections to block unauthorized BIOS tampering. SP 800-147B details requirements for performing secure BIOS updates and maintaining BIOS integrity through the RTU.

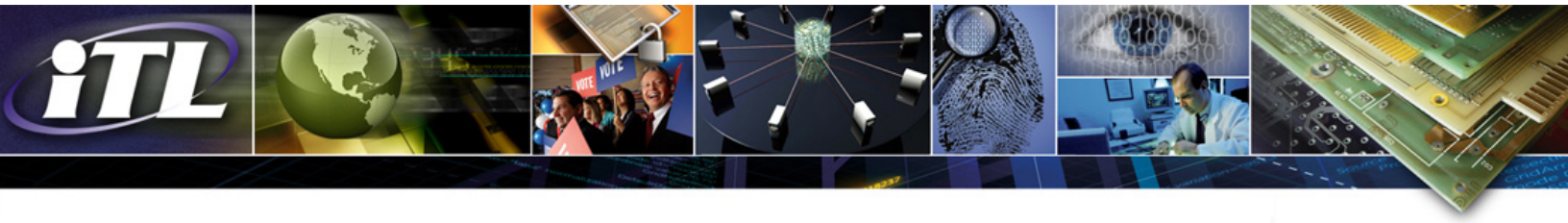
BIOS Security Principles

The security principles presented in SP 800-147 for client systems – update authentication, flash region integrity, and non-bypassability—apply directly to server-class machines. The complexity of server architectures and the multiple update paths for BIOS on servers require the extension of the guidelines in SP 800-147. SP 800-147B provides guidelines for servers to protect BIOS and the process used to update it. The publication describes authorization and authentication in the context of BIOS updates, supporting secure update mechanisms including:

- **Authenticated BIOS update mechanisms**, where digital signatures prevent the execution of BIOS update images that are not authentic;
- An optional **secure local update mechanism**, which requires that an administrator be physically present at the machine in order to install BIOS images without signature verification;
- **Firmware integrity protections**, to prevent unintended or malicious modification of the BIOS outside the authenticated BIOS update process; and
- **Non-bypassability** features, to ensure that there are no mechanisms that allow the main processor or any other system component to bypass the BIOS protections.

BIOS Update Authentication

SP 800-147B describes methods to implement authentication for updates, leveraging digital signatures to ensure the authenticity and integrity of update images. The use of a Verification Component within the RTU helps prevent insertion of a malicious update. The process is supported by other NIST cryptographic standards and guidance including digital signature applications and recommendations for security key lengths. SP 800-147B includes guidance regarding prevention of unauthorized BIOS update to an earlier authentic version. Appropriate rollback protections will depend upon the environment in which the server is used and the security and availability needs of the organization operating the server.



Secure Local Update

The new publication describes methods to optionally include a secure local update mechanism that updates the system BIOS without using the authenticated update mechanism. For example, requiring an administrator to be physically present at the server to conduct the update mitigates the risk of a remote attacker conducting a malicious update. The secure local update mechanism could also be used by a physically present administrator to update to an earlier BIOS version on a system that does not allow rollback. However, SP 800-147B notes that systems that implement the secure local update mechanism are potentially vulnerable to attacks by rogue administrators or other attacks with physical access to the server.

Firmware Integrity Protection

To prevent the execution of inauthentic or malicious BIOS code, SP 800-147B recommends verification methods to protect the integrity of the system BIOS during the boot process. It points out that system flash memory containing BIOS, excluding configuration data stored in nonvolatile memory, should be protected from modifications outside the authenticated BIOS update mechanisms. If implemented, BIOS flash protections could be further enforced by system hardware mechanisms. The publication also describes automatic recovery mechanisms that initiate recovery to a protected authentic BIOS, reducing the likelihood of a successful denial-of-service attack.

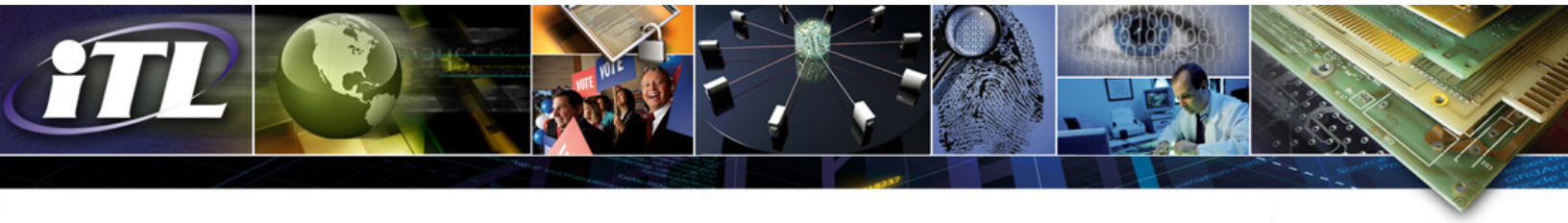
Non-Bypassability

SP 800-147B reminds readers that the design of the system (and accompanying system components and firmware) must ensure that there is no means to bypass the secure update and integrity verification methods described above. It points out that there should not be mechanisms to install or execute unauthenticated BIOS code, except through physical intervention, nor should there be an update path except through the RTU.

A modern platform includes design features that give system components direct access to the RTU or system BIOS for performance and management improvements, such as shadowing the BIOS in RAM or for system management mode operations. A system component may have read access to system flash memory, but it should not be able to directly modify the RTU in an unauthorized manner.

Conclusion

As cyber attacks become more sophisticated, the potential for BIOS or other firmware attacks is growing. Providing BIOS protection can improve security by making such an attack more difficult to implement. The guidelines in SP 800-147B provide server-specific recommendations such as those to help guard against remote exploits where an attacker is able to gain access to a server, attacking the BIOS to strengthen their position. The protections described reduce that threat by making it difficult to tamper with BIOS. Such protections may also guard against attackers with physical access to the box. The protections should be weighed against the potential legitimate needs of system administrators to be able to manage BIOS as needed, which could include flashing their own BIOS images. The guidelines in SP 800-147B provide flexibility for vendors and users to do just that.



Additional Resources

David Cooper, William Polk, Andrew Regenscheid, Murugiah Souppaya, NIST SP 800-147, *BIOS Protection Guidelines*

Andrew Regenscheid, NIST SP 800-147B, *BIOS Protection Guidelines for Servers*

Dan Goodin, *Malware burrows deep into computer BIOS to escape AV*, 14 Sep 2011

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov