PHYS.ORG

Build safety into the very beginning of the computer system

April 29 2011

A new publication from the National Institute of Standards and Technology (NIST) provides guidelines to secure the earliest stages of the computer boot process. Commonly known as the Basic Input/Output System (BIOS), this fundamental system firmware—computer code built into hardware—initializes the hardware when you switch on the computer before starting the operating system. BIOS security is a new area of focus for NIST computer security scientists.

"By building security into the firmware, you establish the foundation for a secure system," said Andrew Regenscheid, one of the authors of BIOS Protection Guidelines (NIST Special Publication 800-147). Without appropriate protections, attackers could disable systems or hide malicious software by modifying the BIOS. This guide is focused on reducing the risk of unauthorized changes to the BIOS.

Designed to assist computer manufacturers writing BIOS code, SP 800-147 provides guidelines for building features into the BIOS that help protect it from being modified or corrupted by attackers. Manufacturers routinely update system firmware to fix bugs, patch vulnerabilities and support new hardware. SP 800-147 calls for using cryptographic "digital signatures" to authenticate the BIOS updates before installation based on NIST's current cryptographic guidelines.* The publication is available just as computer manufacturers are beginning to deploy a new generation of BIOS firmware. "We believe computer manufacturers are ready to implement these guidelines and we hope to see them in products soon," said Regenscheid.

The publication also suggests management best practices that are tightly coupled with the security guidelines for manufacturers. These practices will help computer administrators take advantage of the BIOS protection features as they become available.

BIOS Protection Guidelines, NIST SP 800-147, is available at csrc.nist.gov/publications/nis … 00-147-April2011.pdf .

* See Digital Signature Standard (FIPS 186-3, June 2009) at csrc.nist.gov/publications/fip … 186-3/fips_186-3.pdf ,

Recommendation for Key Management – Part 1: General (NIST SP 800-57, March 2008) at csrc.nist.gov/publications/nis … ised2_Mar08-2007.pdf , and

Recommendation for Obtaining Assurances for Digital Signature Applications (NIST SP 800-89, November 2006) at csrc.nist.gov/publications/nis … -89_November2006.pdf

Provided by National Institute of Standards and Technology

Citation: Build safety into the very beginning of the computer system (2011, April 29) retrieved 2 May 2024 from https://phys.org/news/2011-04-safety.html