Protecting computers at start-up: New NIST guidelines

December 21 2011

A new draft computer security publication from the National Institute of Standards and Technology (NIST) provides guidance for vendors and security professionals as they work to protect personal computers as they start up.

The first software that runs when a computer is turned on is the "Basic Input/Output System" (BIOS). This fundamental system software initializes the hardware before the operating system starts. Since it works at such a low level, before other security protections are in place, unauthorized changes—malicious or accidental—to the BIOS can cause a significant security threat.

"Unauthorized changes in the BIOS could allow or be part of a sophisticated, targeted attack on an organization, allowing an attacker to infiltrate an organization's systems or disrupt their operations," said Andrew Regenscheid, one of the authors of BIOS Integrity Measurement Guidelines (NIST Special Publication 800-155). In September, 2011, a security company discovered the first malware designed to infect the BIOS, called Mebromi.* "We believe this is an emerging threat area," said Regenscheid. These developments underscore the importance of detecting changes to the BIOS code and configurations, and why monitoring BIOS integrity is an important element of security.

SP 800-155 explains the fundamentals of BIOS integrity measurement—a way to determine if the BIOS has been modified—and how to report any changes. The publication provides detailed guidelines to hardware and software vendors that develop products that can support secure BIOS integrity measurement mechanisms. It may also be of interest to organizations that are developing deployment strategies for these technologies.

This publication is the second in a series of BIOS documents. BIOS Protection Guidelines (NIST SP 800-147) was issued in April, 2011.** It provides guidelines for computer manufacturers to build in features to secure the BIOS against unauthorized modifications. The detection mechanisms in SP 800-155 complement the protection mechanisms outlined in SP 800-147 to provide greater assurance of the security of the BIOS.

NIST requests comments on draft SP 800-155 by January 20, 2012. Copies of the publication can be downloaded from csrc.nist.gov/publications/dra … P800-155_Dec2011.pdf . Please submit comments to 800-155comments[at]nist.gov with "Comment SP 800-155 in the subject line.

More information: * Information on Mebromi: www.symantec.com/security_resp … =2011-090609-4557-99
** See the May 10, 2011, Tech Beat article "Build Safety into the Very Beginning of the Computer System" at www.nist.gov/public_affairs/te … /tb20110510.cfm#bios

Provided by National Institute of Standards and Technology

Citation: Protecting computers at start-up: New NIST guidelines (2011, December 21) retrieved 24 April 2024 from https://phys.org/news/2011-12-start-up-nist-guidelines.html