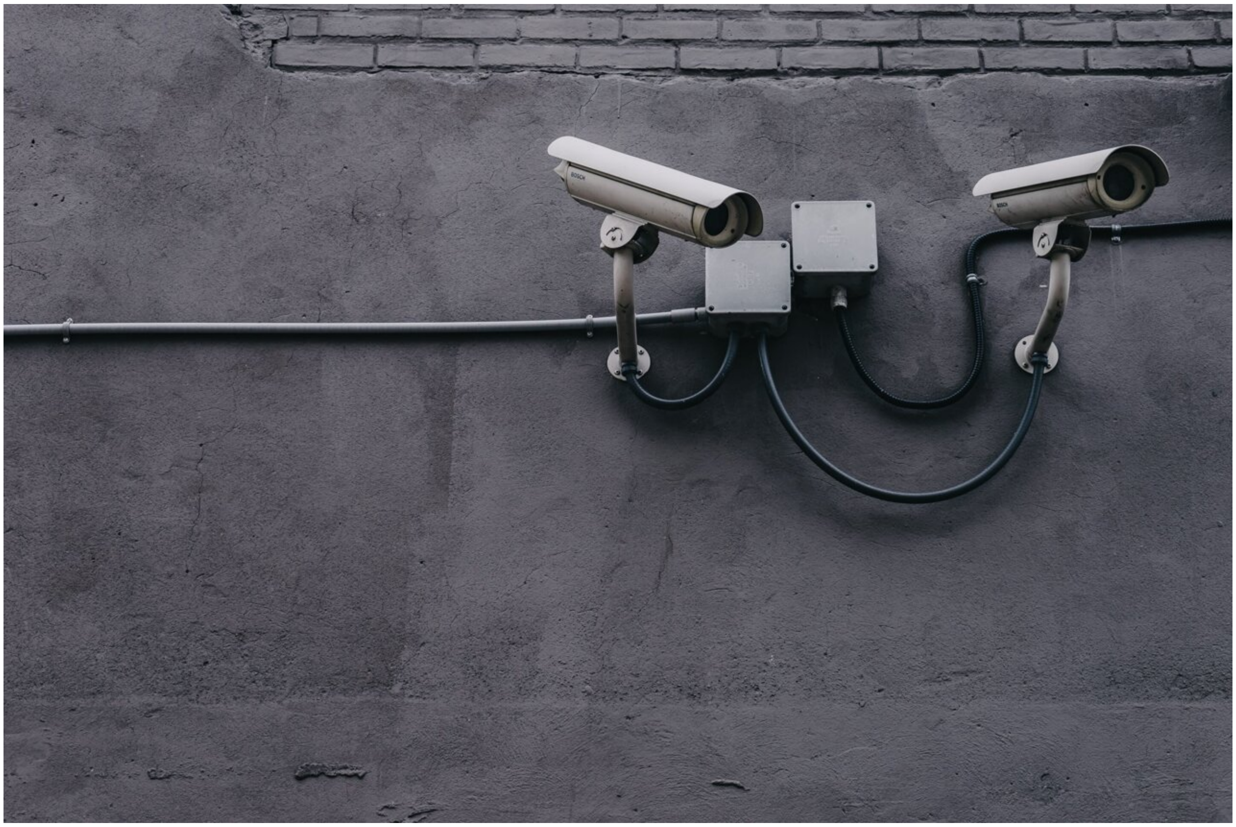
PHYS.ORG

Security first: New NIST guidelines on securing BIOS for servers

August 22 2012



Credit: Unsplash/CC0 Public Domain

The National Institute of Standards and Technology (NIST) is requesting comments on new draft guidelines for securing BIOS systems for server computers. BIOS—Basic Input/output System—is the first major software that runs when a computer starts up. Both obscure and fundamental, the BIOS has become a target for hackers.

Server manufacturers routinely update BIOS to fix bugs, patch vulnerabilities or support new hardware. However, while authorized updates to BIOS can improve functionality or security, unauthorized or malicious changes could be part of a sophisticated, targeted attack on an organization, allowing an attacker to infiltrate an organization's systems or disrupt their operations. BIOS attacks are an emerging threat area. In September, 2011, a security company discovered the first malware designed to infect the BIOS, called Mebromi.*

An important mechanism for protecting BIOS in servers is to secure the BIOS update process, guarding against unauthorized BIOS updates. NIST's 2011 publication on BIOS security** provided instructions for protecting BIOS in desktops and laptops. The guidelines focused on the core principles of authenticating updates using digital signatures, BIOS integrity protection and "non-bypassibility" features that ensure that no mechanisms circumvent the BIOS protections.

BIOS Protection Guidelines for Servers addresses BIOS security in the varied architectures used by servers. "While laptop and desktop computers have largely converged on a single architecture for system BIOS, server class systems have a more diverse set of architectures, and more mechanisms for updating or modifying the system BIOS," says author Andrew Regenscheid. In addition, many servers contain service processors that perform a variety of management functions that may include BIOS updates, and this document provides additional security guidelines for service processors.

Servers require more flexibility, according to Regenscheid, because in addition to having different architectures, they are almost always managed remotely. BIOS Protection Guidelines for Servers is written for server developers and information system security professionals responsible for server security, secure boot processes and hardware security modules. The draft publication BIOS Protections Guidelines for Servers, (NIST Special Publication 800-147B), is available at csrc.nist.gov/publications/dra … 00-147b_july2012.pdf .

More information: NIST requests comments on this draft by Sept. 14, 2012. Please email all comments to 800-147comments@nist.gov.

* Information on Mebromi: www.symantec.com/security_resp … =2011-090609-4557-99
** D.A. Cooper, W.T. Polk, A.R. Regenscheid and M.P. Souppaya. BIOS Protection Guidelines (NIST SP 800-147) is available at www.nist.gov/manuscript-public … ch.cfm?pub_id=908423

Provided by National Institute of Standards and Technology

Citation: Security first: New NIST guidelines on securing BIOS for servers (2012, August 22) retrieved 11 July 2024 from https://phys.org/news/2012-08-nist-guidelines-bios-servers.html