PENNSTATE

Technology Available for Licensing
Office of Technology Management-The Pennsylvania State Univ.
113 Technology Center, University Park, PA 16802
814.865.6277 phone; 814.865.3591 fax

Non-Confidential Description - PSU No. 3571
"Rootkit-Resistant Disks for Preventing Persistent Malware from Installing Itself on an Operating System"

Keywords:

Computer security, malware, storage, rootkits, disks, disk processor, hard drives

Links:

Inventor Website
Related Article

Inventors:

Patrick McDaniel, Kevin Butler, Stephen McLaughlin

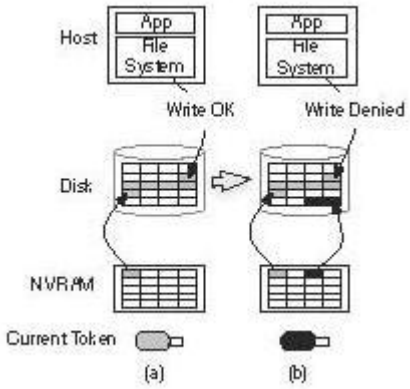

Figure 1. Use of tokens in a rootkit-resistant disk (RRD). Blocks written to disk using the gray token are labeled as such; attempts to write gray-labeled data are denied as long as the gray token is not present.

Background

A rootkit is an invasive computer program or combination of programs that exploits operating system (OS) vulnerabilities by obscuring evidence that the computer is compromised. Rootkits avoid operating system detection by subverting or evading standard security measures, often disguising themselves as harmless software programs. Once a rootkit infects a computer, it may hide files or create a backdoor login for hacking, compromising system-wide security. Rootkit malware can be persistent (survives system reboot) or non-persistent (does not survive across reboots). The only known method for removing a persistent rootkit is by reformatting the computer hard drive.

Invention Description

The disclosed invention is a read-only rootkit-resistant disk (RRD) that protects against persistent malware. Because the security operations of the RRD are enforced at the level of the disk processor—rather than by the host operating system—there is no room for rootkits to mask their presence by exploiting OS vulnerabilities or insinuating themselves into other programs. Preliminary tests have shown that the disclosed RRD can fully suppress rootkit virulence even if the operating system is infected, eliminating the need to wipe the hard drive.

Advantages/Applications

- Capable of intermixing mutable and immutable data, thereby offering more flexible and robust protection
- Avoids high-storage overhead of many read-only devices
- Permits essential upgrading and patching
- Operation of the RRD is transparent and runs independent of the user

Contact: **Bradley A. Swope**
Sr. Technology Licensing Officer
The Pennsylvania State University

Phone: (814) 863-5987
Fax: (814) 865-3591
E-mail: bradswope@psu.edu