Technical Disclosure Commons

Defensive Publications Series

August 16, 2017

Method to query and determine if a storage device secure digital signature has been compromised

Richard J. Tomaszewski
Hewlett Packard Enterprise

Paul Kaler
Hewlett Packard Enterprise

Method to query and determine if a storage device secure digital signature has been compromised

In today's world the threat of cyber attacks is a serious threat to businesses and individuals. The number of cyber attacks and the sophistication of these attacks increase daily. Whether they are attempts to obtain confidential information or attacks to maliciously destroy or alter data these attacks are very real and a threat at a global scale. While there are multitude of security protection technologies and solutions implemented today there are still vulnerabilities within compute systems. One vulnerability which has a vulnerability is an attack vector via firmware. Specifically through storage devices such as disk drives and solid state drives. One could just read Kaspersky reports to see that malicious firmware attacks in drives has happened and is a vulnerability.

To address this best in class disk drives and solid state storage devices have implemented digitally signed firmware to protect against malicious firmware attacks. Typically in a digitally signed firmware implementation in a data storage device would validate the authenticity of the firmware during a firmware download operation. The storage device may or may not validate the authenticity of the firmware at each reboot or power cycle. Security should be a full time protection focus. A user may desire to query a data storage device at any time for security purposes to ensure that the firmware on the storage device has not been tampered with.

To achieve this one would implement a method to query a data storage device to validate that the authenticity of the secure digitally signed firmware has not been compromised on demand. A storage device would be asked through a specific security command to 're-check' the validity of the firmware and return a status indicating whether the firmware is still authentic. A newly defined security storage device command when issued to a data storage device would instruct the storage device to perform the firmware digital signature authentication algorithms that were performed at either firmware download or in some cases also at reboot or power cycle of the device. If the digital signature authentication algorithms complete successfully the device would return a status indicating that firmware is still secure. If the digital signature authentication algorithms complete unsuccessfully the device would return a status indicating that firmware authentication has failed and the firmware is no longer considered authentic.

This solution provides an advantage over only validating authenticity at firmware download, reboot, or power cycle of a data storage device in that a user or application

can monitor and validate the integrity of the data storage device firmware at any time. As part of an overall security solution it provides protection validation at the lowest level within your storage device firmware.

Disclosed by Richard Tomaszewski and Paul Kaler, Hewlett Packard Enterprise