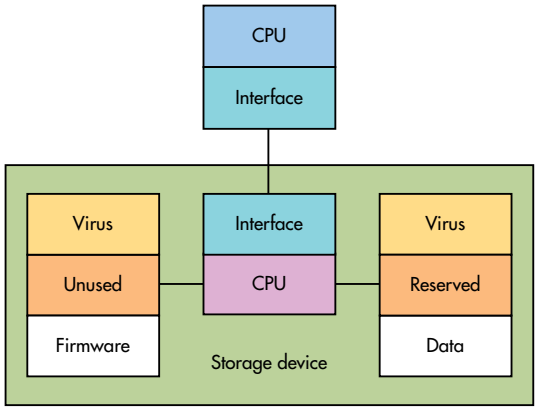
BILL WONG | Embedded/Systems/Software Editor
bill.wong@penton.com

Hacking Hard Drives and Other Nasties

Securing your system is harder than you think when it is possible to hack a hard drive so that the virus cannot be detected and removed.

The Catch-22 quote, "Just because you're paranoid doesn't mean they aren't after you," seems tame these days as revelations from Edward Snowden (*see "Prism, Big Data and Double, Secret Probation" on electronic design.com*) and Kaspersky Labs continue to emerge. One of the latest from Kaspersky Labs is that a very advanced group of hackers called the Equation Group could be an organization like the NSA (*see "Kaspersky Lab Discovers Equation Group: The Crown Creator of Cyber-Espionage" on electronic design.com*).



1. Researchers at Kaspersky Labs have discovered hard drives that had a virus in firmware that allowed another part of the virus to be hidden on a hard disk.

Tracking down and dealing with nebulous attackers is no easy chore. It is hard enough for the Global Research and Analysis Team (GReAT) at Kaspersky Labs—and they know what to look for. In this instance, one of the attacks was via hard disk drives that had their firmware hacked (*see the figure*). Essentially the firmware was replaced so a virus was included in addition to providing the normal drive functionality. The additional changes to the firmware allow data to be hidden in the main storage area. This can be accomplished easily, since the drives are already set up with spare sectors to be remapped in the event of another sector going bad.

This finding resulted in an ominous warning from GReAT director Costin Raiu, who noted, "Another dangerous thing is that once the hard drive gets infected with this malicious payload, it is impossible to scan its firmware. To put it simply: for most hard drives, there are functions to write into the hardware firmware area, but there are no functions to read it back. It means that we are practically blind, and cannot detect hard drives that have been infected by this malware."

The hacked drive can essentially store a copy of a virus or even a hacked operating system in the main storage area of the device that survives a format request since the firmware is the program that performs the formatting. This information can replace a newly installed system and this is completely transparent to the rest of the system, including any antivirus or disk-checking software. A secure boot system may be able to detect a problem, assuming it is not spoofed as well. That can be a much harder job, but not impossible especially given the difficulty in hacking the hard drive in the first place. The approach works regardless of whether a drive is a hard disk or a solid-state disk. Its approach can even work on encrypted disks.

AN IoT CHALLENGE

The approach of hiding malicious code in a way that it cannot be detected is not new. It is also an approach that is becoming more of an issue with the rise of the Internet of Things (IoT), which offers even fewer mechanisms to analyze and detect problems that arise within a network.

Embedded developers need to understand the security threat issues and build secure systems that will not inadvertently be employed in compromising situations. This can be challenging, since building the application alone is usually hard enough--but it cannot be overlooked, because a majority of systems are connected in some fashion. Even air-gap computer security measures can be overcome using USB flash drives if systems are not configured properly.

This issue also relates to counterfeits and the gray market. More intelligent devices have more places to hide nefarious software, and it is much easier to insert software into a device in hand rather than via remote means.

It is all a matter of who, or what, you can trust.