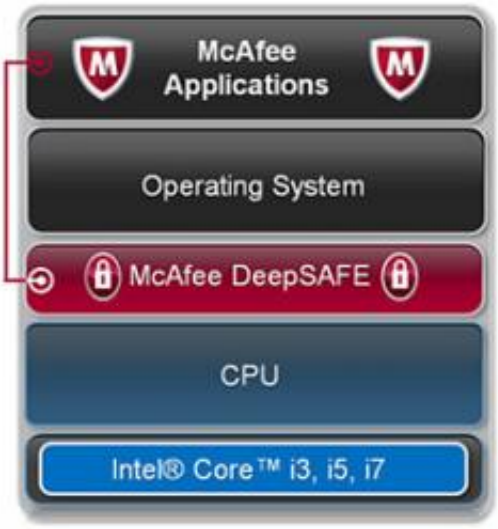
Intel-McAfee preview new rootkit weapon

September 16 2011, by Nancy Owano



(PhysOrg.com) -- Letting everyone know that today's computing is no longer about running good anti-virus software, McAfee this week presented a new technology approach in computer protection called DeepSAFE, designed to combat the newer forms of deeply-rooted malware that embed themselves outside the operating system and go undetected. What is special about DeepSAFE is that it goes beyond the operating system to do "kernel-mode rootkit prevention," according to McAfee, making the announcement at this week's Intel Developer Forum in San Francisco.

Unlike installed anti-virus software, the new layer of protection will sit

below a PC's operating system, to detect modifications attempted by hidden malware, according to George Kurtz, McAfee's CTO and executive vice-president. In sitting outside the operating system, the new software approach uses Intel's "chip-level hooks" to look for the presence of malicious software such as rootkits.

According to McAfee Labs, more than 1200 new rootkits are detected every day around the world, or 50 per hour every day. This is a security burden because of their ability to load and embed themselves at the kernel level of the operating system and they are difficult to spot. McAfee spokesmen said DeepSAFE veers from those current approaches that are actually based on "20+ year old techniques."

The technologies are becoming increasingly less effective, and "novel approaches are needed to effectively manage the increase in malware and other attacks."

DeepSAFE is designed to detect and block suspicious behaviors that are characteristic of many of those rootkits in real-time before they have a chance to spread.

The future of security technology is going to have to move beyond the operating system, says a McAfee video presentation, in no uncertain terms, and should not be bound by the same OS rules as today, because rootkits are designed to hide themselves away from the OS.

DeepSAFE is in beta. Products employing DeepSAFE technology are expected later this year. DeepSAFE is designed to work with Windows 7; McAfee anticipates DeepSAFE will work with Windows 8 on its release; McAfee is evaluating bringing the technology to Android mobile devices.

The McAfee preview at this week's Intel Developer Forum represents a

significant show as well as to how the two companies will work together following Intel's acquisition of McAfee for $7.68 billion in February.

More information: www.mcafee.com/us/resources/fa … psafe-technology.pdf
www.mcafee.com/us/solutions/mcafee-deepsafe.aspx