

6 January 2009

By: Marius Oiaga, Technology News Editor



Intel vPro

[Intel vPro Hacked](#)

Allows for attacks against Xen and Linux

Intel vPro, a technology developed by the chip maker and applauded for delivering robust hardware-based security, has been hacked. InvisibleThings' Joanna Rutkowska, founder and CEO, and Rafal Wojtczuk, principle researcher, are getting ready to demonstrate the hack at Black Hat DC 2009, this February. According to the security researchers, they have put together the proof-of-concept for the hack, and will demo practical attacks on Intel Trusted Execution Technology at next month's Black Hat.

The Intel Trusted Execution Technology (Intel TXT) was especially designed in order to provide an additional layer of hardware security for virtual environments and operating system kernels. The additional protection tier is available on PCs with Intel vPro technology, the company revealed.

"Our research shows how an attacker can compromise the integrity of a software loaded via an Intel TXT-based loader in a generic way. We have created a proof-of-concept code that demonstrates the successful attack against tboot — Intel's implementation of the trusted boot process for Xen and Linux. Our attack comprises two stages. The first stage requires an implementation flaw in a specific system software. The second stage of the attack is possible thanks to a certain design decision made in the current TXT release," Rutkowska and Wojtczuk stated.

Rutkowska explained that the Intel TXT technology was set up to guarantee a trusted way for system software (this implied both a Virtual Machine/Hypervisor and an actual OS kernel) to load and to execute. The security researchers claimed that the attack would permit the system to be infected with malware from BIOS rootkits to boot sector viruses, and the Intel TXT technology would still allow the operating system or virtual machine to load.

"While evaluating the effectiveness of the Intel TXT technology, as part of a work done for a customer, we have identified several implementation flaws in the Intel's system software, which allowed to conduct the above mentioned stage-one attack. We have provided Intel with extensive description of the flaws in December 2008, and Intel is currently working on fixing those vulnerabilities," Rutkowska and Wojtczuk added.