Invisible Things Lab to demonstrate practical attacks on Intel® Trusted Execution Technology at the upcoming Black Hat conference in Washington, DC, Feb 2009.

Jan 05, 2009 — Invisible Things Lab's Rafal Wojtczuk and Joanna Rutkowska will present results of a new research on security of Intel® Trusted Execution Technology at the Black Hat conference in Washington, DC, on February 18-19, 2009.

What is TXT?

Intel® Trusted Execution Technology (TXT), formerly code named LaGrande, is currently part of the Intel® vPro™ brand and is a key component of the Intel®'s Safer Computing Initiative. Intel® TXT comprises a set of extensions to the CPU, as well as the chipset, and also makes extensive use of the Trusted Platform Module 1.2 (TPM).

Our attack

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.

Working with vendors

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.

We have also been in touch with Intel® about the possibility of conducting the second-stage attack since November 2008. In December, after providing Intel® with the details about the first-stage attack, Intel® promised to release, in the coming weeks, an updated TXT specification for developers that would explain how to design their TXT-based loaders in such a way that they are immune to our attack. Intel® claims the current Intel® TXT release does contain the basic building blocks that could be used to prevent our second-stage attack and the release of the additional specification would make it feasible in practice.

Affected users

Intel® TXT is a very new technology — the TXT/vPro™ compatible hardware has been available on the market for only about a year now. Consequently, Intel® TXT is currently not a widely deployed technology. The Xen hypervisor is one of the few popular products that can make use of it, via the above-mentioned Intel® tboot module. However, we believe, Intel® TXT, due to its unique features, has a great potential to positively impact computer security in the near future, assuming potential vulnerabilities, like the one mentioned here, will be resolved by Intel®.

About Rafal Wojtczuk

Rafal Wojtczuk, Principle Researcher, has over 10 years of experience with computer security. Specializing primarily in kernel and virtualization security, over the years he has disclosed many security vulnerabilities in popular operating system kernels (Linux®, SELinux, *BSD, Windows™) and virtualization software (Xen®, VMWare® and Microsoft® virtualization products). He is also well known for his articles on advanced exploitation techniques, including novel methods for exploiting buffer overflows in partially randomized address space environments. He is also the author of libnids, a low-level packet reassembly library. Rafal holds a Master's Degree in Computer Science from University of Warsaw. He is based in Warsaw, Poland.

About Joanna Rutkowska

Joanna Rutkowska, Founder and CEO, is a recognized researcher in the field of system-level security. Over the past several years she has introduced several breakthrough concepts and techniques on both the offensive and defensive side in this field. Her work has been quoted multiple times by international press and she is also a frequent speaker at security conferences around the world. In 2007 she founded Invisible Things Lab, a boutique security consulting company focusing on OS and virtualization systems security. Joanna holds a Master's Degree in Computer Science from Warsaw University of Technology. She is based in Warsaw, Poland.

About Invisible Things Lab

Invisible Things Lab focuses on cutting-edge research in computer security, specializing in system-level security. We are well known for our pioneering research in the areas of kernel security, virtualization security and system/firmware-level security. Our work has been widely quoted by international press and the members of our team often speak at industry conferences around the world. The unique skills of our team allow us to analyze complex new technologies and point out design- and implementation-level security flaws and recommend how to fix them, before the "bad guys" can exploit them.

Contact

For press inquiries, Invisible Things Lab can be contacted via email:
`contact@invisiblethingslab.com`

Links

- http://www.intel.com/technology/security/
- http://www.intel.com/technology/vpro/index.htm
- http://www.blackhat.com/html/bh-dc-09/bh-dc-09-speakers.html#Wojtczuk
- http://invisiblethingslab.com/