*!!!RELEASED UNDER **EMBARGO** (UNTIL **FEB 18, 3 pm US/Eastern time**)!!!*

Invisible Things Lab presents the "Press Cheat Sheet" for the Attacking Intel® Trusted Execution Technology presentation at the Black Hat DC conference, Washington, DC, Feb 18, 2009.

Feb 16, 2009 — In this press release we share the details of our upcoming Black Hat DC presentation about Attacking Intel® Trusted Execution Technology. The amount of technical details have been significantly reduced in this press release in order to make it more accessible to a broader audience. People with technical background are encouraged to take a look at the conference paper and slides, in addition to this release.

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).

The Attack Details

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:

1. First an attacker is required to get access to a so called **SMM memory**. The code within SMM memory (also called SMRAM) is executed with the highest privileges on PC platforms.

   SMM is more privileged than the kernel-mode code (Ring 0), and even more privileged than a hardware hypervisor code, often referred to as "Ring -1". SMM code can be thought of as if executing in "**Ring -2**"[1].

2. Once the attacker got access to the SMM memory, the attacker can inject a special *shellcode*[2] into the SMM. The payload of the shellcode will depend on the circumstances. In our attack we use a shellcode that adds a simple backdoor to a Xen hypervisor (consult our prior research on Xen subversions presented at Black Hat USA 2008 for more details).

   The whole point about using a shellcode located inside SMM is that **Intel® TXT doesn't validate the SMM memory** during the trusted launch process. Consequently, the attacker might be able to survive the TXT trusted launch, if and only if, he or she, decides to shelter themselves inside the SMM memory.

SMM Attacks Details

The above TXT attack scenario presents one **non-trivial challenge for the attacker: how to get access to the SMM memory**. Today, modern systems do pretty well job on protecting the SMM memory, not only from write- but even from read-accesses from the OS. Even though there have been several presentations about SMM security-related issues in the past 2-3 years, none of the research considered how to bypass system-level protection of the SMM memory. That was because a few years ago it was trivial for an attacker to get access to the SMM; today the SMM memory is much better protected by a CPU and a chipset.

---

[1] Both "Ring -1" and "Ring -2" terms are colloquialisms and are not 100% technically correct. They are used to give reader a better intuition about which code is more privileged. x86/x86_64 processors "officially" only support 4 rings: 0, 1, 2 and 3, with #0 being the most privileged mode used by OS kernels, while #3 the least privileged execution mode, used by applications. Rings 1 and 2 are usually unused by most OSes.

[2] Shellcode is a special term used in computer security to describe a piece of code, injected by an attacker to target application or OS, that does something useful for the attacker.

During our presentation **we present two distinct attacks** that allow an attacker **to get access to the SMM memory** on the latest Intel® systems. Our work is applicable to the latest systems like e.g. those based on the Q35 chipsets, and most likely to those based on the Q45 chipsets[3].

Intel® requested we do not publish the details for our latest SMM exploit as Intel® is currently still working on fixing the issue. Moreover, Intel® believes similar issue affects also other vendors. Consequently, Intel® has notified CERT CC about the problem. CERT has assigned a vulnerability tracking number VU#127284 to this issue. We plan to present the details of this attack at Black Hat USA 2009 in July. Nevertheless, at the Black Hat DC on February 18, we plan to demonstrate our attack against TXT using an earlier bug in Intel® BIOS that we found last year and that has already been patched by Intel® a few months ago.

TXT Design Problem

While Intel® does indeed have plans to patch the SMM-implementation bugs we have exploited in our attack, the correct and generic solution to protect TXT against SMM-originating attacks is supposed to be provided by a software component called **SMM Transfer Monitor (STM)**.

Unfortunately, no STM is currently available. According to Intel®, STM is supposed to be provided by OEMs/BIOS vendors.

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 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®.

The situation looks different with the SMM vulnerabilities. Virtually every modern PC-based computer does make use of an SMM. Ability to infect SMM might give an attacker a huge advantage. Last year other researchers have presented working examples of rootkits that reside in SMM[4]. Such SMM-based malware might turn out to be extremely annoying, since the A/V programs would have to use so called "0day exploits" in order to read and scan the SMM memory.

vPro vs. TXT

We should stress that, while TXT is a part of the Intel® vPro™ brand, our research does not affect other technologies that are also part of the vPro, like e.g. Intel® AMT™.

---

[3] We haven't tested a Q45 chipset-based system, as such systems have been available in shops for just a few months now. We believe our recent SMM attacks apply to those chipsets as well, because of the nature of the vulnerability. Intel® has not denied, but also not confirmed the vulnerability in Q45-based systems.

[4] Although no method have been presented of how to infect the SMM. Our research makes SMM rootkits now a reality even on the latest systems.

About Rafal Wojtczuk

Rafal Wojtczuk, Principal 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/