Invisible Things Lab to present two new technical presentations disclosing system-level vulnerabilities affecting modern PC hardware at its core.

July 27, 2009 — Invisible Things Lab's Rafal Wojtczuk and Alexander Tereshkin will present two new technical presentations at this year's Black Hat Conference in Las Vegas, NV, in July. The first presentation will talk about a new type of stealth malware, that potentially could be more powerful than kernel-mode, hypervisor-mode, and even SMM-based rootkits, while the second presentation will focus on bypassing the re-flash protections found on mainstream Intel® desktop systems.

Introducing "Ring -3" Rootkits (Compromising the Chipset)

In this presentation we will present the results of our research on how malware can potentially abuse the Intel® AMT technology (part of the vPro™ brand) in order to stealthy take control over the machine. The Intel® AMT technology offers attractive features for the attacker — AMT's code is executed by an *independent* processor that is located in the chipset (a vPro-compatible MCH), AMT's memory is separated from the host memory (isolation enforced by the chipset), AMT code has a dedicated link to the network card (independent of the host OS and drivers), and, last but not least, the AMT is active even if the computer is put into a sleep mode (S3 state).

We show how malware can bypass the AMT's dedicated memory protection, and consequently compromise the AMT code executing on the chipset. Additionally we discuss tricks we used for reverse engineering the AMT code, that were needed in order to create meaningful rootkits that can have access to the host memory (rootkit executes on the chipset, but has full access to the host OS, e.g. Windows).

The research stresses the need for better review of the security of the core system components, including the firmware and hardware.

Attacking Intel® BIOS

In this presentation we will discuss and demonstrate how to permanently re-flash Intel BIOSes on the latest Intel® Q45-based desktop systems. In contrast to a previous work done by other researches a few months earlier, who targeted unprotected low-end BIOSes, we focus on one of the most secure, vPro-compatible, BIOSes, that normally only allow a vendor's digitally signed firmware to be flashed. We demonstrate how to bypass this verification scheme, using a very sophisticated heap overflow exploit. The attack requires administrator-level access, and also requires one reboot to succeed, albeit doesn't require any user consent or cooperation, nor any physical access to the machine — thus it is well suited for use by malware.

The attack stresses the importance of other means for ensuring trusted boot process, like e.g. TCG's TPM-aided ones, as well as the importance of better review of the core system software and firmware.

About Chipsets

In our research we focused on two popular Intel desktop vPro-compatible chipsets: Q35 (released Q3 2007) and Q45 (released Q3 2008). Variants of those chipsets are also available for mobile computers (e.g. PM45, GM45) — we haven't tested those though.

Our test systems were based on Intel-branded motherboards, equipped with either Q35 or Q45 chipsets (DQ35JO, DQ45CB, respectively) and Intel BIOS.

Affected Systems

In order to install an AMT rootkit one needs to find a way to break into the AMT memory. We have successfully tested our memory attack on Intel Q35 chipset. We however noticed that Intel used additional protection in its new Q45 chipset, in which our attack doesn't work anymore.

We have verified the BIOS re-flashing attack works on Intel Q45-based system with Intel BIOS, but likely the attack affects many other Intel-based systems as well (i.e. with Intel BIOS) — please refer to the Intel advisory for details.

Working With Vendor

We have been in touch with Intel regarding the mentioned issues for several months and Intel representative told us they were planning to release the appropriate patches a day before our first presentation at Black Hat (July 28th).

Additional Questions & Answers

Q: Didn't you already break vPro earlier this year?

At Black Hat DC, in February 2009, ITL researchers, Rafal Wojtczuk and Joanna Rutkowska, have demonstrated an attack that allowed to bypass Intel Trusted Execution Technology (TXT), that also is part of the vPro™ brand. However Intel TXT and Intel AMT are independent technologies, and have different goals.

Q: How does the "Attacking Intel BIOS" presentation relates to the "Introducing Ring -3" one?

The attack presented in the "Attacking Intel BIOS" presentation could potentially be used to compromise AMT on Q45-based systems (that are otherwise immune to AMT compromise), as the AMT code is also stored on the SPI-flash chip, together with the BIOS code. We have, however, not verified this possibility yet, and some of the Intel specs suggest that the chipset performs additional verification on the AMT code retrieved from the SPI-flash, before executing it.

Q: Can a user disable AMT in BIOS?

Yes, but our rootkit would still be active. We have determined that some AMT code is still being executed, regardless of whether AMT is disabled in BIOS or not. In our proof of concept rootkit we decided to subvert this very AMT code.

Q: Why do you focus on such deep-level system security, isn't it more important, from the user's perspective, to look for bugs in Web browser and Web applications, after all?

We believe that security should be built on solid foundations. Consequently, we focus in our research on the core system technologies, that, we hope, could be used to build secure computer systems in the near future.

Q: What is the difference between a chipset and an MCH?

MCH stands for Memory Controller Hub, sometimes referred as "North Bridge". MCH's primary task is to connect the CPU with the memory (DRAM) and other I/O devices via an ICH (also called "South Bridge"). The term "chipset" refers to both the MCH and ICH considered together, but is also used to refer to the MCH alone.

Q: Intel latest Nehalem processors have integrated memory controller — does it change anything?

We haven't looked at the Nehalem systems yet. However, If they support Intel AMT technology, then they should have a similar functionality as the one used on Q35 and Q45 chipsets. Whether this additional "chipset processor" is physically located on the processor die, or inside the chipset (which is still there, just without the memory controller), should be irrelevant.

About Alexander Tereshkin

Alexander Tereshkin, Principal Researcher, is an experienced reverse engineer and an expert into Windows® kernel and hardware virtualization, specializing in rootkit technology and kernel exploitation. He is known for his research on sophisticated ideas for novel rootkit creation and personal firewall bypassing in the past years. Recently he has done significant work in the field of virtualization based malware and Microsoft® Vista™ kernel security. He is a co-author of "Understanding Stealth Malware" course. Alex holds the Russian equivalent of a Master's Degree in Applied Mathematics, and also the Russian equivalent of a PhD degree in Information Security from Taganrog State University Of Radioengineering (Southern Federal University).

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 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`

Relevant Links

- http://blackhat.com/html/bh-usa-09/bh-usa-09-speakers.html#Tereshkin
- http://blackhat.com/html/bh-usa-09/bh-usa-09-speakers.html#Wojtczuk
- http://www.intel.com/technology/vpro/index.htm
- http://www.intel.com/technology/platform-technology/intel-amt/
- http://security-center.intel.com/
- http://invisiblethingslab.com/