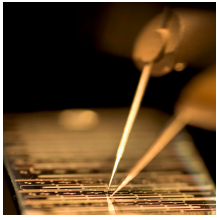


14 July 2008

By: George Craciun, Security News Editor



Kaspersky to demonstrate flaw in Intel CPU
Intel

[Kaspersky to Simulate Successful Hacking Attack on Intel CPU](#)

There are several security vulnerabilities to take advantage of

Kris Kaspersky, software engineering expert, security consultant and technical writer, will demonstrate at the upcoming HITB (Hack in the Box) Security Conference how an attacker can use JavaScript and TCP/IP packets to remotely exploit a flaw in the Intel processor. The conference will be held in Malaysia over a period of three days, from the 27th to the 30th of October. Kris is not to be confused with Eugene Kaspersky, the co-founder of the security software company Kaspersky Lab. "In this presentation, I will share with the participants the finding of my CPU malware detection research which was funded by Endeavor Security. I will also present to the participants my improved POC code and will show participants how it's possible to make an attack via JavaScript code or just TCP/IP packets storms against Intel based machine. Some of the bugs that will be shown are exploitable via common instruction sequences," says Kris Kaspersky. According to Kris, as long as an attacker is familiar with JIT Java-compilers and the way they work, that compiler can be "persuaded" to perform several actions, such as crashing the system. Basically, any hacker with a particular set of skills can take over the compiler. At the Malaysia security conference Kris will also let IT enthusiasts in on how a flawed CPU damages the HDD without the user even realizing it. Kris will also share info in regard to data recovery. Did you know that Intel Core 2 is plagued by as many as 128 flaws and that Intel Itanium by 230? These bugs can affect you in several ways, from crashing your system when certain conditions are met, to granting an attacker complete access to your machine. These security vulnerabilities can be exploited locally or remotely, no matter what OS you have installed, what programs you are running, and how recently you patched your operating system. The thing is that for the end-user there are no tools that one can use to check for these bugs, not to mention that even if there were such a tool, for numerous bugs there is no fix available. "Although CPU bugs are not something new in the security industry, nobody has come out with any proof-of-concept exploits and as it stands, there are no known malware that take advantage of these bugs, although some malware writers have actually used CPU bugs for targeted attacks. It is just a matter of time before we start seeing these sort [sic] of attacks used in more devastating ways over the Internet," says Kris Kaspersky.