

8 March 2008

By: Bogdan Botezatu, Hardware Editor



The FireWire port can grant intruders access to the computer's memory
Cables HQ

[Cold-Boot Reloaded: FireWire Tool to Bypass Windows Authentication](#)

The exploit has been alive and kicking since 2006

New Zealand hacker Adam Boileau has publicly released the source code of a tool that allows bypassing the Windows authentication via the computer's FireWire port. The tool has been written back in 2006, but its creator merely kept it for performing LanParty tricks. The cracking tool is written in Python and counts about 200 lines of code. It exploits a less documented feature in the FireWire port specifications that allows direct access to a computer's memory. In order to successfully accomplish the task, the cracker would target specific places where Windows uses to store its vital authentication routines, then overwrite original Windows routines with patches that skip the operating system's password check functions. Basically, the FireWire's possibility to access the memory directly (DMA) allows it to act more than a hardware debugger, which makes it immune to the refuse of miscellaneous applications to run when a software debugger is present. For instance, many commercial applications would refuse to start or would shut down immediately if they detect the presence of programs monitoring memory directly. According to Boileau, the FireWire trick allows the attacker to hack into Windows Vista's password-check code. The intruders could also use a laptop's PCMCIA port to plug in a Firewire card, then attack the operating system as soon as it has finished auto-installing the required drivers. FireWire ports can be used as high-speed debugging devices that can gain memory access and let hackers perform any patching operations where needed. They can either render a password check useless, or they can legitimately debug poorly-written applications. However, FireWire ports can be used in more than cracking passwords and hacking into users' computers. Hardware debuggers could be used in PC forensic investigations, that would allow authorized staff to snatch the HDD encryption key straight from the computer's memory. The bad news is that Microsoft's operating system is not the weak link: the OS code cannot be held responsible for the attack. The FireWire trick works on all the existing operating systems, including Mac OS X and Linux.