smh.com.au
The Sydney Morning Herald

Security conference to debut Windows firewire crack

PATRICK GRAY
September 19, 2006
Next

Locking your firewire-equipped Windows PC while you pop out for lunch won't keep it secure, thanks to a new hack developed by a New Zealand-based security consultant.

The new attack, which unlocks Windows workstations in 20 seconds by manipulating firewire ports, will be demonstrated at Sydney's Ruxcon security conference on September 30.

"It's generally well known in the forensics community that you can do this; it's just not been done against Windows as far as I know," says the creator of the hack, Adam Boileau, a consultant with Security-Assessment.com. "If you see an exposed firewire port, chances are that dude's got a problem."

By attaching a Linux-based computer running Mr Boileau's software to a locked Windows workstation, the target machine is tricked into allowing the attacking system to have read and write access to its memory, he says. After 20 seconds or so, the software fiddles with Windows' password protection code in the memory of the target machine, rendering it useless.

"You have read and write access to main memory, which means you can overwrite something that's about to be executed with your own code," he says.

The only reliable way to protect a computer against the unlocking technique is to disable its firewire port.

Similar attacks were demonstrated years ago on Mac and BSD systems but this is the first time it has worked against a Windows PC, Mr Boileau says. "All previous public discussion has said that Windows systems aren't vulnerable, which is false. I'll disclose the 'special sauce' that makes it work against Windows (at Ruxcon)." The special sauce, Mr Boileau adds, involves "tricking" Windows into believing the computer attached to it via firewire is a peripheral that requires read and write access to the system's memory in order to function. Unlike USB connections, "firewire is essentially an expansion bus, like a PCI slot", making the manipulation of the target system's memory fairly straightforward, he says.

Most corporate workstations aren't affected because they're usually not equipped with firewire ports, but Mr Boileau says most notebook computers are vulnerable to the attack.

Microsoft was unable to comment at the time of writing.

The Ruxcon conference will be held at Sydney's University of Technology. The offbeat event is put together "by the security community, for the security community", says organiser Chris Spencer. The non-profit conference draws about 300 attendees each year.

Mr Spencer says this year's line-up of speakers draws heavily on experts from Australia and New Zealand. "It shows the growing strength of the local community."

He says Mr Boileau's firewire presentation won't be the only world-first at Ruxcon this year.

"Ben Hawkes' presentation, Exploiting OpenBSD, will take a look at some new techniques to bypass the security protection technologies present in OpenBSD."

Other presentation topics will include Radio Frequency Identification security, web-services security and forensics.

Conference entry is $60.