# Linux beats Windows for kiosk security, says developer

**'Hardening' Windows for kiosk use is difficult, says Netstop**

BY ULRIKA HEDQUIST | AUCKLAND | MONDAY, 1 DECEMBER, 2008

EMAIL PRINT

Kiosks running Linux are more secure than those running Windows, says one local developer after *Computerworld*'s report on attack code targeting Windows kiosks last week.

Mac Jones, of Whangarei-based Netstop, says public-facing kiosks running Windows-based software are hard to "harden". The Windows operating system was designed for people at home and in offices, who, naturally, wouldn't try to hack their own computers. But now, most 15-year-olds can pull up information on the internet and hack a Windows computer, he says.

To Jones, it proved too hard to make kiosks safe using Windows and he switched to the Linux operating system, which, thanks to its kernel-based model, can be built in a very safe manner, he says.

Linux machines only have the applications that the machine needs to use running on it. In addition, its security model only allows privileged users to install software, meaning that malicious software won't be installed on the machine by, for example, clicking a dodgy link in an email, he says.

On top of the security model, most exploits today are aimed at Windows machines, mainly because there are more people using Windows than Linux, he says.

Is Linux more secure than Microsoft for kiosk software? That "old chestnut" has been around for at least a decade, says Brett Roberts, national technology officer of Microsoft New Zealand, "but it is not born out of facts or research by independent security researchers", he says.

Last week, *Computerworld* reported that an attack tool, targeting internet kiosks and terminals running Windows, had been released by a New Zealand security researcher, Paul Craig, who works for consultancy Security-Assessment.com. Craig released his findings at the world's largest hacking conference, DEF CON, in Las Vegas in August.

The toolset, called iKAT (interactive kiosk attack tool), produces a command shell that allows the user to compromise a terminal by by-passing the security access controls.

Microsoft supports and advocates the ethical release of security information, says Roberts.

"Responsible disclosure is a good thing," he says. "All software has bugs and vulnerabilities. We make it very easy for people to provide disclosure information to us and we act on each and every approach."

The reason so many kiosks run Windows is that manufacturers want a user interface that users are familiar with, says Roberts.

After last week's story stated there are no kiosk software developers in New Zealand, a reader email informed *Computerworld* about Netstop.

Kiosk software developers are scarce in New Zealand, but Whangarei-based Netstop has been thriving since 1998.

The company started out developing for kiosks running Windows, but switched to Linux in 2003 — primarily because of security issues — and hasn't looked back since, says Jones. Netstop's software is installed on around 180 kiosks for internet use around the country.

Jones welcomes research like Craig's, saying it can only serve to make things more secure for the public when using kiosks for internet access. Usually, researchers will give the software manufacturer some notice before publishing their findings to the world, he says.

In his paper, Craig listed around 30 ways of getting around security controls when hacking a kiosk, and Jones reckons this is going to be very hard for the software manufactures to fix.

Jones recommends avoiding typing in sensitive information when using a public kiosk, but if you have to type in, for example, your bank account number, it is a good idea to open up a word processor and type in the number in a different order and then copy and paste the number into a website. A keylogger would then record the wrong number. Another tip is to keep URLs, such as your bank website or other sensitive sites, in an email or notepad file, and then cut and paste them into the browser, and so avoiding typing in the URLs.

He also recommends getting down on the floor and following the computer cable to the wall; there are keylogging hardware devices that connect to the cable.

If you have typed in a URL for a bank and then an account number, this will be recorded on the device and ready for the criminal to pick up, he says.

Jones also warns that some kiosks overseas run pirated software, and therefore, no security updates will have been being applied. These kiosks are in a vulnerable state, he says.

EMAIL
PRINT
SHARE THIS STORY WITH:

LATEST NEWS

- Sinclair to leave Renaissance
- Telecom result helped by $27m compensation payment
- Gen-i awarded datacentre contract with Air New Zealand
- FRY UP: They may be watching you
- Five govt agencies engage with Public Records Act
- Telecom revenue down, but some improvement seen









MOST POPULAR
READ | COMMENTED | EMAILED | SHARED

- Netbook failure rate disappoints major user
- Google Wave code to live on
- Govt plans hinder FX Network sales
- File-sharing bill could extend surveillance culture - Bott
- Surveillance Bill amendments reassure telcos
- HP researcher cracks conundrum









MOST POPULAR STORIES FROM FAIRFAX BUSINESS MEDIA GROUP WEBSITES

CIO
- The Mad Mouse Challenge: Four crossings in one day
- Your workplace in 2020: Gartner's predictions
- Tech-savvy staff willing to buy their own work tools
- 'Reputation is crucial'
- Five Advantages of unified information access

PCWorld
- Breathe new life into your laptop's battery
- Kiwis may be eligible for iPhone 4 refunds
- Press F1: Where's the power?
- 2 degrees launches 3G services
- HP Mini 210 (Vivienne Tam Edition)
- Apple confirms iPhone 4 refund policy

Reseller news
- Comworth signs disty deal with Zultys
- Red Hat takes cloud on the road
- New winners join veterans as Microsoft awards expand
- Cisco APAC posts 23 percent YOY growth
- MYOB: Recession over for most businesses

Unlimited
- Change agents
- Sun sets on the Bill Day Show
- One man's battle with Fisher and Paykel
- Is our national airline going off brand?
- Please turn on your cellphones