MUUGLines

The Manitoba UNIX User Group Newsletter

September 2009 Volume 22 No. 01

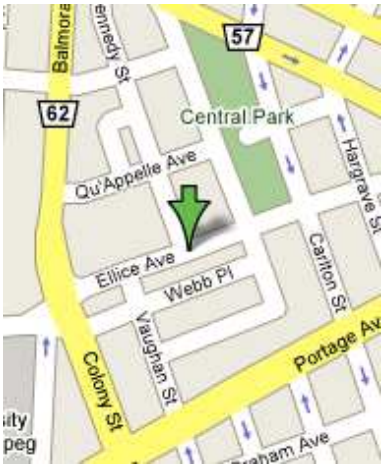
Next Meeting: September 8th, 2009

Connecting your Computer to the Real World

This month, Adam Thompson will be covering the dizzying array of I/O ports and technologies available for making connections to (or from) your computer. There's at least three ways to hook up a monitor; at least three ways to connect a keyboard and mouse; at least five ways to hook up a printer or scanner... Do you actually know what all those ports on the back do? What plugs into where? Does UNIX support them all equally? Which one is best (in any given circumstance)? We'll attempt to answer these questions for you. Adam Thompson will be the presenter.

Where to find the Meeting

Meetings are held at the IBM offices at 400 Ellice Ave. (between Edmonton and Kennedy). When you arrive, you will have to sign in at the reception desk, and then wait for a jackalope to take you (in groups) to the meeting room. Please try to arrive by about 7:15pm, so the meeting can start promptly at 7:30pm. Don't be late, or you may not get in. (But don't come too early either, since security may not be there to let you in before 7:15 or so.) Non-members are welcome, but may be required to show photo ID at the security desk.



Limited parking is available for free on the street, either on Ellice Ave. or on some of the intersecting streets. Indoor parking is also available nearby, at Portage Place, for $5.00 for the evening. Bicycle parking is available in a bike rack under video surveillance located behind the building on Webb Place.

Upcoming Meetings:

October 13th, 2009: TBA

MUUG Board Elections - Call for Nominations

Every October the Manitoba Unix User Group holds its Annual Meeting, the main goals of which are to elect a new Board of Directors and to pass any special resolutions. (Aside from that, it is a regular meeting)

Any MUUG member in good standing can be nominated to run for a position on the Board.

As of this writing, the following members of the current Board have let their names stand for re-election:

Sean Cody
Senior System Administrator - Prime Focus VFX Services

Gilbert Detillieux
Systems Analyst - University of Manitoba

Michael Doob
Professor - University of Manitoba

Kevin McGregor
Network Analyst - City of Winnipeg

Montana Quiring
Systems Administrator - University of Manitoba

Doug Shewfelt
Systems Specialist - City of Winnipeg

Adam Thompson
Consultant - athompso.net

Of course, this list is just a starting point. Any member in good standing of the group can be nominated simply by getting the support of one other member. If you feel you would like to contribute to the group by running for a board position, please don't hesitate to do so. (In fact, we'd like to see the number of board members increase.)

If you want to be nominated, or to nominate someone else, send a letter to the group's postal box or deliver it in person to a current board member. The letter must contain the name, title, and employer of the nominee, along with a short (100 word or so) biography, and must contain the signatures of the nominee and one other member. The letter must be received no later than September 29, 2008, which is 14 days prior to the October 13 meeting.

Although the by-laws require that the nominations be done in writing, with signatures, you can speed up the process by sending e-mail to **election@muug.mb.ca**, with the above information, and sending the signed paper copy later. In this case, please include the e-mail address of both the nominee and the supporter on the CC: list of the message, so that all parties concerned have a record of the communication.

Nominees should familiarize themselves with the MUUG bylaws, found here:

http://www.muug.mb.ca/pub/bylaws/

If you have any questions about the election or the nomination process, please contact Gilbert Detillieux, either by phone (474-8161) during business hours, or by e-mail to **election@muug.mb.ca** anytime.

Gilbert Detillieux
Election Committee Chair

Linux Kernel Null-Pointer Vulnerability

A Linux vulnerability has been found that affects all 2.4 and 2.6 series kernels released since 2001. This was reported in a recent issue of the SANS newsletter (**www.sans.org**) and many other sources. The vulnerability is locally exploitable, meaning that a user would have to run exploit code locally on a host with a vulnerable kernel. Because of the number of affected kernel versions, as well as a widely-published exploit, this flaw could lead to serious problems if not dealt with promptly.

In an item dated August 17, 2009, SANS reported "Linux developers have released versions 2.6.27.30 and 2.6.30.5 of the kernel to address a critical flaw disclosed last week. The flaw affects all 2.4 and 2.6 series Linux kernels released since 2001 on all architectures. An exploit for the flaw has been released and could be used to gain root privileges on vulnerable systems."

SANS included links to related articles at **ZDnetAsia.com** and **H-Online.com**, the latter which also provided links to workarounds provided by Red Hat and CentOS for their respective releases of Enterprise Linux. (As of the article's date, only Fedora and Debian had issued update packages to patch the vulnerable kernel versions in their supported distributions.)

Red Hat's recommended fix for RHEL, until they release a patched kernel update, involves disabling some of the vulnerable kernel modules that are known targets of existing exploits, by adding lines such as these to `/etc/modprobe.conf` (for RHEL 4 and 5):

```
install pppox /bin/true
install bluetooth /bin/true
install sctp /bin/true
```

This workaround was first suggested in Bugzilla, then later published to their FAQ:

https://bugzilla.redhat.com/show_bug.cgi?id=516949
http://kbase.redhat.com/faq/docs/DOC-18065

CentOS recommends a slightly different approach to disabling the affected modules, by adding lines such as these to `/etc/modprobe.conf`:

```
alias net-pf-3 off # Amateur Radio AX.25
alias net-pf-4 off # IPX
alias net-pf-5 off # DDP / AppleTalk
alias net-pf-9 off # X.25
alias net-pf-10 off # IPv6
alias net-pf-23 off # IrDA
alias net-pf-24 off # PPPoE
alias net-pf-31 off # Bluetooth
```

Of course, these workarounds can only be used if the protocols in question are not required. A reboot may be required if any of the affected modules were already loaded.

The CentOS workaround was proposed on their mailing list:

http://lists.centos.org/pipermail/centos/2009-August/080663.html

US-CERT/NIST has catalogued this vulnerability as **CVE-2009-2692.**

More Kernel Capers…

This has been a rather stormy summer from a Linux kernel security perspective as well. In the past 3 months, Fedora has issued 6 separate kernel updates (2 in June, one in July and 3 in August). Granted, we're used to seeing some "churn" in Fedora, but many of these updates have been prompted by various security vulnerabilities.

In addition to the above vulnerability, there have been several other null-pointer related vulnerabilities reported and patched, including a gcc-optimization-related bug (**CVE-2009-1897**), `mmap_min_addr` security bugs (**CVE-2009-1895**), and most recently, a `clock_nanosleep` bug (**CVE-2009-2767**). A couple stack- and heap-based overflow issues in `eCryptfs` (**CVE-2009-2406** and **CVE-2009-2407**) round out the set of advisories.

Fortunately, most of these vulnerabilities showed up in recent 2.6 series kernel releases, and don't affect the more mature, stable Linux distributions.

In a BIND about DNS Security?

The summer also wouldn't be complete without another DNS-related security bug. While not as big an issue as last year's DNS flaw discovered by Dan Kaminsky (as we reported in the ***September 2008 issue of MUUGLines***), a new flaw was reported at the end of July this year (**CVE-2009-0696**) which "allows remote attackers to cause a denial of service (assertion failure and daemon exit)."

Affected versions are "ISC BIND 9.4 before 9.4.3-P3, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1." Most supported systems should have had updates issued by now. If you're running an Internet-visible and vulnerable version of ISC BIND that hasn't been updated or patched, you might want to look into updating it.

UNIX Turns 40

Born in 1969, and originally named "Unics" (a pun based on the name of an earlier operating system called Multics), the UNIX Time Sharing System is now 40 years old. First written in assembler for a Digital PDP-7 mini-computer at AT&T Bell Labs, by Ken Thompson and Dennis Richie, UNIX has provided a lasting legacy, with it's "less is more" philosophy, and simple set of command-line tools. It would take a few more versions and a total rewrite of the system in C before UNIX would provide us with possibly its greatest legacy: the concept of a portable, architecture-independent operating system.

The 40th birthday of this venerable old OS was noted, among others, by Computer World, in a rather substantial article:

http://www.computerworld.com/s/article/print/9133570/Unix_turns_40_The_past_present_and_future_of_a_revolutionary_OS

Softpedia also marked the event with a (shorter) article that includes a couple spiffy charts of the UNIX evolutionary tree:

http://news.softpedia.com/news/40-Years-of-Unix-119827.shtml

Even the BBC got in on the party, with a technology article:

http://news.bbc.co.uk/2/hi/technology/8205976.stm

Also Celebrating a Birthday…

Now more than a debutante, Debian turns sweet 16 this year:

http://www.h-online.com/open/Happy-Birthday-Debian--/news/114014

OpenSSH turns 10 this month, apparently without the press coverage its 5th birthday generated:

http://www.openssh.com/press.html

And it looks like our trusty old user group is now starting its 22nd year of MUUGLines publication!

SCO v. Novell Appellate Decision

IEEE Spectrum recently reported (on August 25) that the U.S. 10th Circuit Court of Appeals has reversed the 2007 summary judgment decision that found that Novell owned the *Unix* and *Unixware* copyrights.

http://spectrum.ieee.org/blog/computing/it/riskfactor/who-owns-unix

Expanded coverage at *Groklaw* shows that the news isn't as bad as one might first expect:

http://www.groklaw.net/article.php?story=20090824142203182

Linux Cold-Boot in One Second!

In the race for the fastest boot time, it looks like MontaVista Software has now taken a substantial lead, succeeding in booting their embedded Linux system in about one second.

http://blog.internetnews.com/skerner/2009/07/linux-achieves-1-second-boot.html

The news was picked up or linked to by various other sites, including this one that also features a video of the boot demo:

http://dvice.com/archives/2009/07/linux-booted-in.php

Sending Us E-Mail?

Due to the amount of e-mail MUUG receives, we've set up an auto-reply to give you jaunty feedback, and redirect some of the e-mail to the appropriate places. Why not look at **http://www.muug.mb.ca/about.html#contacts** first?

Share Your Thoughts

E-mail us with your comments on the newsletter, whether it's criticisms or commendations, and continue to send in articles or ideas for the same. Specifically, what sort of material you would rather see: Announcements, technical articles, new products, or…?

What Do You Think?

If you have a How-To or other idea, and aren't ready to give a presentation at MUUG, an article is a great alternative! If you can write better than the editor, that's terrific; if you can't, submit it anyway and we'll get it into shape for publication. We know that many of you have some great ideas and lots of knowledge. Why not share? Send Mail to: **editor@muug.mb.ca**.