MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 27 No. 3, November 2014 Editor: Adam Thompson

Next Meeting: October 14th, 2014

RTFM and presentation:

In the RTFM segment this month, Wyatt Zacharias will explore the differences between `wget(1)` and `curl(1)`.

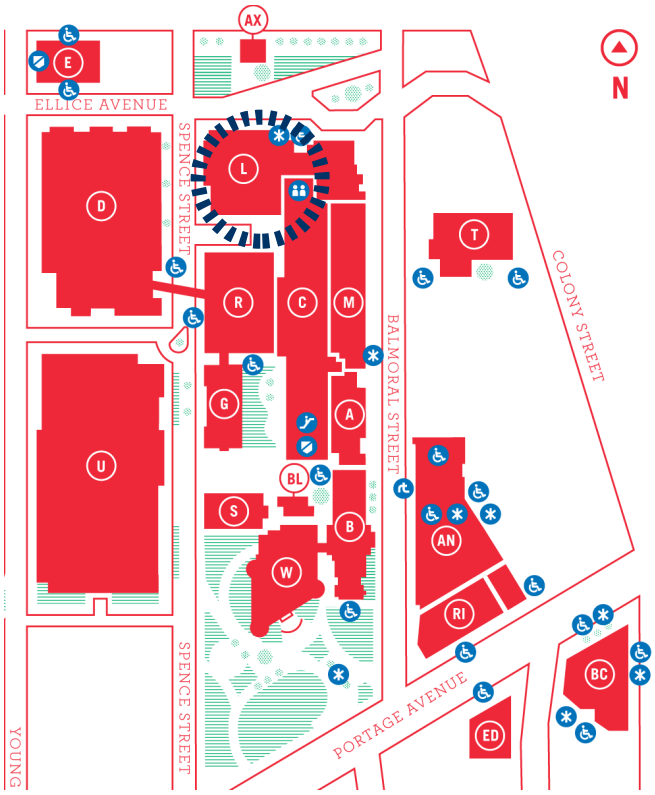
Then for this month's presentation, Brad Vokey will give a demonstration of LiveCode: an open source, cross-platform, rapid application development language. LiveCode evolved from MetaCard (the original Unix HyperCard clone) into becoming a true cross-platform IDE capable of running on iOS, Android, OS X, Windows, and several variations of Unix including Linux, Solaris, and BSD. It can be used to write mobile, desktop and server/CGI applications and is the most widely used HyperCard/HyperTalk clone.

LiveCode uses a high level, English-like programming language that is dynamically typed and tightly integrated to your program's interface. The language and compile-free work flow generate code that is self-documenting and very easy for casual programmers to comprehend.

MUUG Mugs!

Back by popular demand! MUUG now has new coffee mugs, cobalt blue and deep laser-etched with our age old, lovable logo for sale for $15 cash. They are quality mugs, made in the USA, and have a fairly large volume capacity. Want a mug but can't make meetings? Ask on the mailing list and most likely a board member can deliver one within Winnipeg.

Where to Find the Meeting



Meetings are held in the University of Winnipeg's Lockhart Hall (marked "L" on the map), at the south-east corner of Spence Street and Ellice Avenue. We can normally be found in room 1L08, but occasionally get relocated to nearby rooms. If there is a change, it should be conveyed via a sign on the door to 1L08. Parking is available on the surrounding streets. Please see `http://www.uwinnipeg.ca/maps` for further information about parking and access to the campus.

Those who do not understand UNIX are condemned to reinvent it, poorly.
—Henry Spencer

A (very slightly) New Look

Adam Thompson, Newsletter Editor

Fonts

As free and open-source software waxes in the UNIX® world, and PostScript® wanes, I've taken the opportunity to extend some recent discussions at the Board level into the newsletter: new fonts are used in this newsletter.

The masthead and header use the Droid family of TrueType fonts, which were released by Google and Ascender under the Apache license. The entire Droid family of fonts is freely available in the Android SDK and/or from Google Fonts; your distribution likely has a package that installs them automatically for you. They can also be retrieved from .https://code.google.com/p/google-fontdirectory/. Note that Ascender Corporation licenses the Droid Pro series of fonts for commercial users.

Along with the occasional smattering of Droid Sans Mono, the body of the newsletter now uses Linux Libertine and Linux Biolinum OpenType fonts, released by the Libertine Open Fonts Project under both the GPLv3 and the OFL. These fonts provide excellent typographic results both on screen and on paper, excellent UNICODE coverage, a wide variety of styles, and are freely available from http://www.linuxlibertine.org/.

Once the appropriate files have been positively identified, they'll get uploaded to the MUUG FTP server alongside the newsletter. As a bonus, using freely-distributable fonts instead of PostScript® standard fonts should make the job of producing and editing the newsletter easier, as not everyone has access to the original "Adobe 35" fonts.

Logo

Wyatt Zacharias has kindly undertaken the job of reworking our old logo into a modern format, and fixed up some long-standing issues with it at the same time. The original logo was hand-coded in Encapsulated PostScript (as far as I can tell, anyway) and it didn't scale as well as we wanted it to.

You can see the new logo on the front page, in the header. The improvements are subtle, but they're there.

MUUG Board Election – Nominees

Adam Thompson, Nomination Committee Chair

(Ed. note: I forgot to get updated bios for most of these nominees – the stale bios are my fault, not the nominee's fault!)

The current nominees who have agreed to stand for election to the MUUG Board of Directors are:

Trevor Cordes: Owner, Tecnopolis Enterprises

Trevor Cordes has owned and operated Tecnopolis Enterprises – a computer VAR, programming and consultancy company – since 1999. Linux and open source have been the keystone of Tecnopolis since 2000 with the introduction of Linux-based appliances which today are critical to the operation of over 20 local small businesses. Trevor was President of the Atari ST User's Group in 1995 and 1997-1999, and also holds a B.Sc. (CompSci) from the University of Manitoba. His main workstation runs Fedora.

Gilbert Detillieux: Systems Analyst, University of Manitoba

Gilbert Detillieux has been working with UNIX as a programmer, system administrator, and trainer since 1980. He worked as a computer consultant specializing in UNIX, from 1983 to 1989, and is currently working as a Systems Analyst for the University of Manitoba's Department of Computer Science, where's he's worked since 1989, installing, supporting and upgrading the department's network and UNIX server infrastructure. He was co-founder and past president of the Technical UNIX User Group (now MUUG), and has been an active member of the MUUG board ever since.

Michael Doob: Professor, University of Manitoba

Michael Doob is a member of the Mathematics Department at the University of Manitoba. He has been using UNIX since 1990, primarily as a working environment for mathematical

publishing. He has been a member of MUUG for over a decade and has given a number of presentations to that group.

Robert Keizer: Owner, Argyle Machine

Robert Keizer is a Systems Administrator and Developer. Apart from his full time position as a Systems Administrator, Robert is interested in visualization, statistical analysis, and music.

Kevin McGregor: Systems Specialist, City of Winnipeg

Kevin McGregor provides server, platform and infrastructure support in the City of Winnipeg's Information Systems Department. After having briefly used UTS on an Amdahl mainframe in university in the mid-80s, he dabbled in Coherent and then converted to Linux and OpenBSD. He has been a member of MUUG since the early 90s, edited the group's newsletter for a number of years, presented various topics at MUUG meetings and has served on the board for the majority of his membership.

Katherine Scrupa: St. John's Ravenscourt School

Katherine is a I.S. Service Desk Technician at St. John's-Ravenscourt school. Katherine has been using Linux exclusively at home for five years, during which she has also been a member of MUUG. Promoting her learning experiences and solutions to benefit others, her blog can be located at http://uniquegeek.blogspot.com. Her educational pursuits in Computer Science at U of M led her to a Network Technology CCNA program (Hons.) at Red River College in 2010, with emphasis on working with Linux, cabling, and network equipment.

Adam Thompson: Proprietor, CustomHosting.ca

Adam first unknowningly used UNIX in 1988 while playing NetHack on the QNX BBS in Ottawa, which gave him a huge advantage the first time he encoutered `vi(1)`! He first ran into UNIX professionally in 1990, and started using Linux in 1991. Adam is the author of several `termcap(5)` and `terminfo(5)` entries, deployed the first cross-platform, public, networked instant-messaging system in Manitoba, and installed the first UnixWare system in Manitoba. He has developed several UNIX/Linux courses, and has also taught RDBMS administration. Adam has been a member of MUUG since 1995, and a board member for a decade.

Brad Vokey: Owner, Fortresss Software

Brad Vokey is the owner of Fortress Software Inc. and the creator of the Matchmaker Fundraiser (a fundraiser that "matches up" over 1 million high school students across Canada and the US. during Valentine's). Brad started the company in 1985 using Apple II computers writing the original program entirely in 6502 machine language. The program migrated to 68000 machine language (on Atari ST computers) in 1986 and then eventually to C (and Atari TT computers) soon after. The original C program is still very much alive to this day and is constantly being tweaked and added to every year. Brad has served on the board of the Atari ST Users Group (STUG) until its dissolution in 2000 and has been a member of MUUG since 2006. He was first exposed to Linux in 1999 with Mandrake 6.0, uses Linux on a daily basis on his company's firewalls, and is looking forward to converting his entire office to Linux "sometime" in the future.

Wyatt Zacharias: Unix/Linux Administrator, Manitoba Blue Cross

Wyatt Zacharias graduated from Red River College in computer networking, and now works at Manitoba Blue Cross supporting a mixture of HP/UX and Linux. His interests include micro controllers and robotics.

MUUG Mirroring Requests

As you may know, MUUG mirrors several Linux distributions (such as Fedora and Ubuntu) for the benefit of members and geographically (networkally?) close members of the public. Your Linux install may be using MUUG's server, lisa.muug.mb.ca, without even knowing it, as most package managers now determine the fastest (usually closest) mirrors automatically.

MUUG will be expanding disk capacity in the near future and we are soliciting requests for additional things to mirror. "More distros" is an obvious candidate, but other non-distro ideas have been bandied about, such as Wikipedia. If you

have a favourite mirror you would like to see mirrored on lisa, let us know at meetings, on the mailing list, or directly at board@muug.mb.ca.

First priority will go to suggestions by members.

MUUG Server Update

Speaking of that new disk capacity...

The board approved the purchase of a new server to provide FTP, WWW and e-mail services. An ASUS RS300-H8-PS12 was acquired, along with CPU, RAM and storage for the OS. Adam Thompson is currently working on configuring the server. The spinning-rust storage is expected to arrive and get installed over the next couple of weeks.

Once configured, the server will be hosted by a friendly network. The board's goals at the moment are to be connected to MBIX and CA*Net, via both IPv4 and IPv6. Negotiations for server colocation are ongoing at this time with potential bandwidth donors.

POODLE

Why SSL needs to die

From US-CERT:

> All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable. However, the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack demonstrates this vulnerability using web browsers and web servers, which is one of the most likely exploitation scenarios.

CVE-2014-3566 has been allocated for this vulnerability.

Google's paper on the bug provides for some bed-time reading:
https://www.openssl.org/~bodo/ssl-poodle.pdf

In summary:

SSL v1 was hopelessly inadequate (from a cryptographic standpoint) almost from the day it was deployed.

SSL v2 has multiple weaknesses, and is no longer considered secure against brute-force attacks in a reasonable time frame.

And now SSL v3 has proven to have a gaping flaw that affects nearly all users.

SSL isn't even standardized – RFC 6101 finally documented the last-known state of SSL v3 when it became clear that an official standard was needed for reference.

SSL v2 only made it as far as Internet Draft stage in 1995 before dying in committee due to multiple technical problems with the standard. That's the same year Windows 95 was released, neither Ubuntu nor CentOS existed yet, and OS/2 and VMS were still considered viable operating systems!

Meanwhile, Transport Layer Security was first defined in RFC 2246, published in January of 1999. Version 1.1 followed in RFC 4346, in April of 2006. Another update, version 1.2, was published in RFC 4492 in April 2008, and extensions continue to be published periodically – the most recent work is from last October in RFC 7027.

SSL has lived on for over 15 years through a combination of ignorance, apathy, and a desire for backward compatibility at all costs.

Thanks to the security risks demonstrated by POODLE, Google has disabled (or is about to disable) all SSL support in all their products and platforms, and rely exclusively on TLS.

Who's left behind? Internet Explorer 8 users on Windows XP. It's time to at least switch to a newer browser, folks: IE8 just got left in the dust.

Book & User Group Discounts

No Starch Press

No Starch Press has established a discount for user group members. It's valid for 30% off everything they publish, and it doesn't expire. Use "MUUG" as the discount code when ordering from their website.