MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 31 No. 7, March 2019

Editor: Trevor Cordes

Next Meeting: March 12th, 2019

OpenBGPD

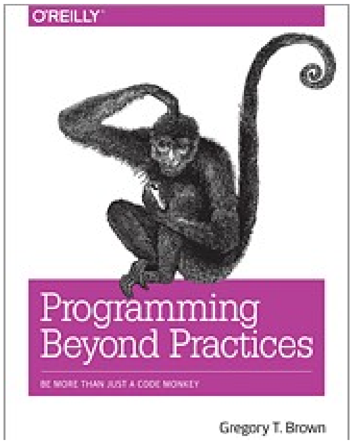
Adam Thompson will talk about setting up a BGP Looking Glass server quickly using OpenBSD and OpenBGPd, as well as how he used the UNIX "toolkit" to solve some BGP analysis & visualization problems.

The latest meeting details are always here:
`https://muug.ca/meetings/`

Creative Commons License

Door Prizes! Not-Old Book!

A special treat this month, we will be door-prizing an O'Reilly book from late 2016 entitled Programming Beyond Practices. Readers will be blessed with the magical ability to "Be More Than Just a Code Monkey".



A short easy read at 132 pages, PBP is language-agnostic and provides a high-level overview of what boils down to what everyone but this author calls software engineering. It uses a narrative style where you are the main character working through a fictional greenfield project. Initial impressions are positive.

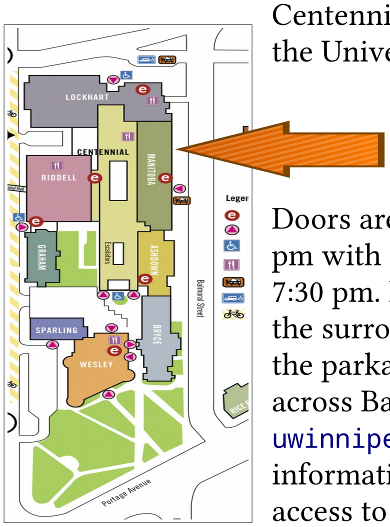
In addition, this month we'll have a smattering of various semi-archaic dead trees to give away courtesy of Adam Thompson. Add in the usual e-book and magazine assortment and you have a recipe for some crazy fun.

Remember, only dues-paying MUUG members get entered in the first draw, so join today! Subsequent draws will include non-members. Good luck to all!

Where to Find the Meeting

University of Winnipeg, Room 1M28

Meetings are held in the University of Winnipeg's Centennial Hall, in the middle of the University Complex.



We can be found in room 1M28.

Doors are usually open by 7:00 pm with the meeting starting at 7:30 pm. Parking is available on the surrounding streets and in the parkade above the bus depot across Balmoral Street. See `uwinnipeg.ca/maps` for further information about parking and access to the campus.

Meetup != Member

We love Meetup members! But Meetup causes some confusion. When you join MUUG on Meetup, you are merely telling Meetup you are interested in MUUG; you are not actually becoming a dues-paying member of MUUG. To become a full member of MUUG you must sign up at a meeting, via mail, or via email using one of our sign-up forms. You can obtain one via the following link.

`https://muug.ca/pub/forms/memform.pdf`

When you sign up, you must pay $20 in yearly dues. Memberships and dues are important to MUUG as they provide one metric of success of our outreach efforts, and dues are the group's predominant source of income. That income is used to buy and maintain the mirror server, increase outreach via outlets such as Meetup, print and mail out newsletters, and provide for meeting expenses.

We encourage everyone to attend meetings, whether they are paying members or not. Check us out to see how MUUG can help you enhance your UNIX experience! But when you see how MUUG is worthwhile to you, please sign-up as a dues-paying member and help us continue in our mission. $20 a year is only $2 a meeting! What a bargain!

Help us promote this month's meeting, by putting this poster up on your workplace bulletin board or other suitable public message board:

https://muug.ca/meetings/MUUGmeeting.pdf

Hi rasdaemon; Bye-bye edac-utils

Have a system with ECC memory? You probably know about edac-utils. That's the old way to monitor and interrogate the ECC data collected by supported hardware. If you got hit with a cosmic ray, it'll tell you.

Unfortunately, edac-utils is abandonware as of around 2011. Luckily, a replacement is available in the form of rasdaemon; and it's superior in that it is designed to deal with all RAS events, not just ECC ones. RAS stands for "reliability, availability and serviceability" and has its roots at IBM.

It runs as a daemon, and major distros will have a systemd unit pre-made for you. No need to configure it, just start the unit! You get info from it by running commands such as the following:

ras-mc-ctl --mainboard: tells you your motherboard model if your hardware is supported.

ras-mc-ctl --layout: shows you your RAM layout in an ASCII graph by memory controller, channel and csrow.

ras-mc-ctl --summary: tells you if you've had any errors in ECC memory, PCIe, MCE, or Extlog.

CAA Beefs Up Web PKI

No, we're not talking boosting batteries in winter; we're talking solving one of the modern web's major flaws. In this instance, CAA stands for "Certification Authority Authorization" and comes from RFC 6844 from 2013. CAA finally came to town in late 2017 when CAs (the guys who issue SSL certificates) voted to mandate its support.

What does it do? It means no cooperating CA (which should be all of them, at least the big ones) will issue a cert without doing a quick DNS check. They look for a new DNS RR called "CAA" which simply lists all the CAs permitted to issue a cert for the domain in question.

So if you know you only get your certs from Let's Encrypt, make yourself a CAA record of "letsencrypt.org". That should preclude any malign actor from tricking any other CA into issuing a cert you didn't authorize.

It's not foolproof – unscrupulous CAs could easily ignore your CAA. However, such CAs would probably get exposed and have their root certs removed from web browsers.

For fun, see if CAA has a CAA: dig -t CAA caa.org

https://tinyurl.com/zf4btfj

O'Reilly E-Newsletters Return

After nearly a year's hiatus, book publisher extraordinaire's free online email newsletters are back! In August 2017 they vanished without a trace, with no word or warning. Poof!

Until in June 2018, without word or warning, they magically reappeared. As before, the newsletters are filled with (a bit of) original and (mostly) curated content and links. The editors do a really good job and they take very little time out of your day. Be prepared to be bombarded with ads for ORM's conferences though; *free* has to be paid for somehow, I guess.

https://tinyurl.com/y4cunh29

Screen Scraping Morphs Again

Those who recall the 2014 MUUG presentation “Dr. Scrapelove” on web crawling / screen scraping [1] may be interested in some modern updates.

First we had WWW::Mechanize::Firefox, which still works great if you don’t need JavaScript to access desired content; but that was starting to get rare even in 2014. So that presentation also showed you MozRepl; that worked great until 2016 when Firefox Quantum broke the required XUL infrastructure.

So it was off to PhantomJS, which was even better than MozRepl because it was “headless” – requiring no browser to function. Replacing MozRepl with PhantomJS required just a few new modules, quick doc reads, and about a dozen lines of code changed.

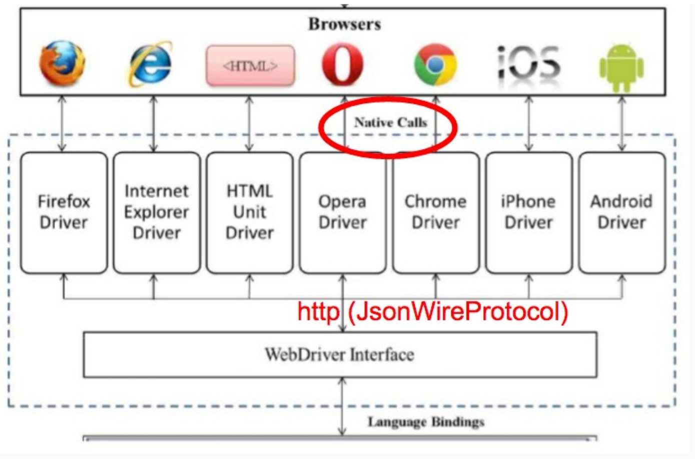
But a year later PhantomJS became abandonware, and it became evident that security could become a problem. Picture a modern browser that doesn’t receive security updates, and you’ll get an idea of what running PhantomJS would expose.

So it’s off to Selenium: modern and well supported. But it’s much more complicated than anything before it. It’s an entire web browser testing framework, as well as a remote controller. Entire 800 page books have been written about it.

Thankfully by 2018 another option appeared: WebDriver [2]! Selenium was a driving force behind the WebDriver concept, but it has since broken out into its own standard and you can use WebDriver without Selenium. Many major browsers, including Firefox, support WebDriver.

WebDriver can be headed or headless. In headless mode it works much like PhantomJS, except that it operates in your chosen browser’s binary environment and as such it becomes indistinguishable to web servers from the real-deal manually-operated browser. Better yet, the “rendered” page (CSS, JS and all) will be identical to what would result from a manual visit to that page in said browser.

In Perl you use Selenium::Firefox, Selenium::Remote::Driver and good old WWW::Mechanize to program WebDriver. Doc reading and code changes are more than the switch to PhantomJS, but not as bad as you’d think, and not as bad as with full-blown Selenium.



WebDriver is supported by bindings, modules and APIs in every language that matters. Ditto regarding browser support.

Is WebDriver the final scraping panacea? As an actual W3C standard and widespread support, as well as a basis in industry-leader Selenium, it very well could be… Long live WebDriver!

[1] `https://muug.ca/meetings/screen-scraping-slides.pdf`

[2] `https://tinyurl.com/y7ohalsw`

Thunderclap Trounces Thunderbolt

Thunderbolt (peripheral connection technology spec) is fast. Makes sense when you learn it’s basically just DMA over the wire. As such, there’s plenty of room for error as sketchy peripherals can theoretically go to town on your memory.

A brand new flaw and PoC called Thunderclap was recently revealed. This flaw allows malicious Thunderbolt devices to gain access to unauthorized and privileged memory spaces, run arbitrary code, and the usual litany of nefarious activities.

It works because of flaws in the way IOMMUs are used (or not used) by modern OSs. This includes Windows 10, Linux, MacOS and FreeBSD.

Hackers produced a fake NIC that appeared as a real one to the host OS. The NIC received access to protected memory areas to conduct its packet flows. This was leveraged to access the plaintext version of encrypted network traffic, as well as UNIX domain socket traffic. Ultimately, on MacOS and FreeBSD they were able to get their faux-NIC to execute arbitrary programs as root.

You're only vulnerable if you plug in a malicious Thunderbolt device, but with nearly all hardware production taking place in China, who can really know what device is or is not malicious.

Luckily, more judicious use of the IOMMU may solve this problem. Linux is on the ball and should have the vulnerability closed(ish) by the time 5.0 rolls out. However, effects may linger as speed continues to trump security in the world of hardware.

https://tinyurl.com/y2qpr4a3

https://tinyurl.com/y46648s9

MUUG Mirror Gains Distros

Recent additions to your local MUUG mirror server include MX Linux:

> MX Linux is a cooperative venture between the antiX and former MEPIS communities, using the best tools and talents from each distro. It is a midweight OS designed to combine an elegant and efficient desktop with simple configuration, high stability, solid performance and medium-sized footprint.

And IUS:

> IUS is a community project that provides RPM packages for newer versions of select software for Enterprise Linux distributions.

IUS is extremely handy for users of RHEL and CentOS who want to create a blend of stable this and modern that. For instance, you can easily run PHP 7.2 on RHEL7.1, all without "rpm dep hell" or zillions of affected rpms.

Just another friendly service provided by your MUUG! Access the mirrors at muug.ca/mirror

SysAdmins Steam Over Spectre Stink

Performance-hungry admins are revolting! As Intel and Linux devs diligently try to solve the awful mess that is the Spectre-class of vulnerabilities, pushback is coming from an unlikely source: Linux SysAdmins.

For instance, STIBP, a Spectre-mitigating tweak added to the kernel, killed PHP server performance by 30%. So the kernel devs have started creating tunables to regain your performance.

4.15 allows a boot command line option called "nospectre_v2" which disables the fix for Spectre V2. 4.17 adds "nospec_store_bypass_disable" to un-mitigate Spectre V4. 4.19 lets you go even nuttier disabling V1 with "nospectre_v1". There's also a "nospectre_v2" and "spec_store_bypass_disable" that have been in since that fateful time a year ago.

The argument goes that some (many?) systems may be immune to some (all?) Spectre-type attacks because of perimeter defense and workload. For instance, a server that is secure, accessed by few, trusted people, and is known to never run untrusted user-supplied code, could theoretically disable Spectre protections. Single-task servers such as web servers are prime candidates. The choice is up to you... As Dirty Harry says: Do you feel lucky punk?

https://www.youtube.com/watch?v=8Xjr2hnOHiM

Our Sponsor

A big thanks to Les.net for providing MUUG with free hosting and all that bandwidth! Les.net (1996) Inc., a local provider of VoIP, Internet and Data Centre services, has offered to provide a 10% discount on recurring monthly services to MUUG members. Contact **sales@les.net** by email, or +1 (204) 944-0009 by phone, for details.

https://les.net/