MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 30 No. 10, June 2018
Editor: Wyatt Zacharias

Next Meeting: June 12, 2018 7:30pm

RTFM: Pioneer

Pioneer - A game of lonely space adventure - will be demonstrated by Trevor Cordes. Not just a game, Pioneer is a full-blown space simulator with realistic Newtonian physics. After you figure out how to not crash into planets or overshoot space stations by mega-kms; explore the planets and other star systems, work as a trader to make a few bucks, or arm up and become a pirate or assassin. Beautiful spacescapes make this a demo worth seeing!

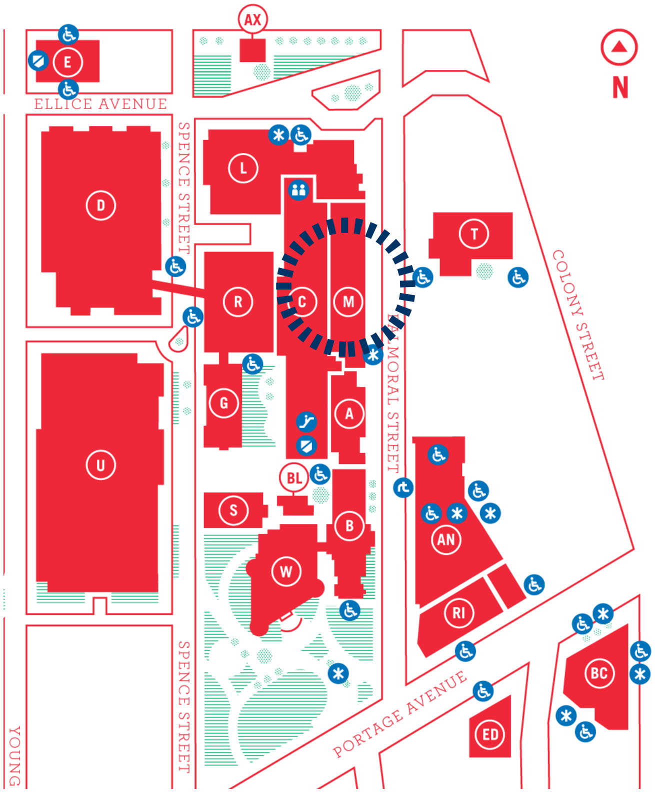
Presentation: Perl PDF::Reuse

Brad Vokey will give a brief demonstration of how to mass produce similar (but not identical) PDF documents in Perl by re-using a starting PDF file as a template. Perl::Reuse is very fast, and gives you the capacity to produce many PDF pages per second creating very big PDF documents if necessary.

Door Prize Book This Month: WebSocket

Until recently, creating desktop-like applications in the browser meant using inefficient Ajax or Comet technologies to communicate with the server. With this practical guide, you'll learn how to use WebSocket, a protocol that enables the client and server to communicate with each other on a single connection simultaneously. No more asynchronous communication or long polling!

Where to Find the Meeting: 1M28 Manitoba Hall, U of W



Meetings are held in the University of Winnipeg's Manitoba Hall (marked "M" on the map), along Balmoral St. We can normally be found in room 1M28, but occasionally get relocated to nearby rooms. If there is a change, it should be conveyed via a couple signs around the halls. Parking is available on the surrounding streets. Please see `http://www.uwinnipeg.ca/maps` for further information about parking and access to the campus.

Notepad Now Supports LF

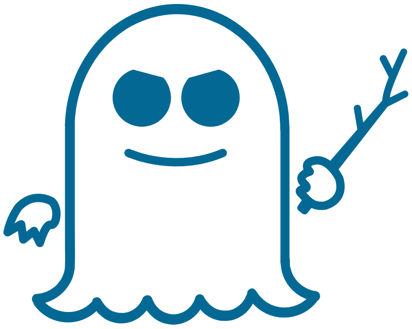
Until now the Windows Notepad application has only supported the Windows style newline, which uses a CR and LF symbol (carriage return,

and line feed), at the end of each line. Linux and macOS, however, only use a LF to denote a new line. This would be unrecognized by Notepad, and any Unix document opened by it would have all its contents on a single line. Notepad will now be able to open and edit Unix files and continue using the correct newline. Although, it does not sound like new documents created with Notepad can be made to use the Unix newline.

https://bit.ly/2K4z3qk

Spectre 2.0

Microsoft and Google have announced that they have found a fourth variant of the Spectre/Meltdown speculative execution vulnerabilities disclosed several months ago, which has been assigned CVE-2018-3639. Just like the Spectre variants before it, all major CPU architectures including Intel/AMD x86, ARM, and IBM Power are affected. The variant is similar to the other Spectre vulnerabilities in that it relies on the speculative execution features of the CPU to fill the cache with private information that can later be read.



Intel says that new patches are being developed for the new variant, however, those who have already installed the patches for variant 1 are fairly safe, as those patches make the other variants much more difficult to exploit.

https://bit.ly/2KFFIHR

GPG Plugins Vulnerable to Data Leak

On May 15th, security researchers disclosed a new set of vulnerabilities discovered in OpenPGP and S/MIME when used for end-to-end email encryption, which enables an attacker to disclose the entire plain text contents of the encrypted email. The first flaw comes from the way that email clients in combination with PGP plugins handle the decrypted message contents, the PGP encryption itself is still considered strong. When an email client receives an S/MIME encoded message, which can include a combination of unencrypted and encrypted elements, it will first decrypt the appropriate portions of the message, and then process any rich-text elements from all sections, including those in the unencrypted sections. When processing the HTML in the email the client does not perform any boundary checking on the HTML in the now decrypted message. This means that malformed HTML code contained in the unencrypted portion of the email can be interpreted by the client to include contents of the encrypted message in its decrypted form. For example, an `img` tag lacking a closing quote in the `src` field will include the entire message contents after it inside the URL request.

To be exploited the vulnerability requires either that the sender's computer has been compromised and malicious email contents can be added at the time of sending, or that a man in the middle is able to intercept the email on the wire and add the malicious contents in transit. Initial mitigation steps include disabling HTML rendering, or decrypting message contents outside of an email client. Although clients are working on patches for this undesired behaviour, it is unclear whether it can be completely mitigated.

A second vulnerability comes in the exploitation of the cipher block chaining used by the plugin to encrypt the message contents. Since all standards compliant clients are supposed to insert specific headers into the message an attacker can use that content knowledge to generate legitimate CBC blocks that contain the malicious HTML code. This attack also relies on either a compromised source or man in the middle capability. Researchers also found that due to text compression and slight differences in standard compliance between clients this attack was on average only 30% effective.

https://bit.ly/2rHdC8b
https://mzl.la/2shGqo1

Google Crostini for ChromeOS

Announced at Google I/O 2018, a new feature called Project Crostini is coming to Google's ChromeOS. All of Google's chromebooks ship with their own version of Linux called ChromeOS, however, ChromeOS itself has never actually let you run applications built for Linux. Applications for the machine must come either from the Chrome app store, or more recently from the Google Play store, providing Android apps. Project Crostini uses Linux native KVM to create virtual Linux instances to run the applications in a containerized fashion. Google has designed the feature to be fully integrated within ChromeOS, allowing native ChromeOS apps and Linux apps running in the virtual container to be used simultaneously and switched between transparently. The first version of the Linux virtual container being developed by Google will be running Debian Stretch.

The feature will first be available to ChromeOS running on Google's self branded PixelBook, with plans to quickly add to the supported device list after that. Google claims that over half of the Chromebooks currently running have enough hardware capacity to support the new feature.

https://zd.net/2kzXTnm

Washington State Residents Up In Arms About Bitcoin Boom

The Chelan County Public Utility District is facing a unique challenge as demand for their very affordable hydro power has skyrocketed from bitcoin mining farms setting up shop in the county. A recent hearing held by Chelan PUD was overflowing with local residents, some concerned about the negative impact that the miners may bring, while others were promoting the boom, claiming it will bring economic improvement. According to Chelan PUD before now the typical power demand growth in a year would be around 4MW, enough for roughly 2,250 homes. Yet since 2017 alone over 200 megawatts have been requested by new mining operations.

The cost of electricity in Chelan Country averages around $00.03/Kwh or about one fifth the national U.S. average. The reason Chelan PUD is able to offer such cheap power is due to their abundance of hydro electric capacity which they are able to sell at premium rates to other electric markets, subsidizing their local customers rates. However, as local demand spikes less power is available for resale to other markets, and stresses on local power grids grow. Now Chelan PUD is left to decide whether they embrace the boom and build out capacity to support a volatile industry with an uncertain future, or clamp down on demand and stifle potentially beneficial growth.

https://bit.ly/2Jfj6kA

Fedora 28 Released

Fedora 28 released at the beginning of May, bringing a couple of interesting new features with it. Fedora now features modular repository functionality, allowing you to easily select different versions of software. It also adds new third party repository support, making it easier to add proprietary packages such as the Nvidia official drivers. ARM64 has been promoted to a primary architecture, which means it will received packages and updates on the same schedule as other main Fedora architectures.

Huawei to Cease Offering Bootloader Unlocking

For many years now, cell phone manufacturer Huawei, based out of Shenzhen China, has been extremely popular with those wanting run custom Android ROMs on their smartphone. This is because the manufacturer made it extremely easy to unlock the boot loader of their phones, allowing the custom software to be loaded, even offering a dedicated support page on the topic. Recently that support page disappeared, and shortly after Huawei publicly announced that they were ending support for boot loader unlocking and would not be providing the resources to do so anymore. Unlike PCs, where any capable software can be booted by the user, smartphones have tight integration between the BIOS and boot loader, and use digital signatures to only boot approved software. Without an official process to allow unsigned ROMs users are forced to "hack" their own phones using exploits and back door methods in order to boot their software. Huawei has responded to all of the confused and upset users, stating the following:

> *In order to deliver the best user experience and prevent users from experiencing possible issues that could arise from ROM flashing, including system failure, stuttering, worsened battery performance, and risk of data being compromised, Huawei will cease providing bootloader unlock codes for devices launched after May 25, 2018. For devices launched prior to the aforementioned date, the termination of the bootloader code application service will come into effect 60 days after today's announcement. Moving forward, Huawei remains committed to providing quality services and experiences to its customers. Thank you for your continued support.*

MUUG has gone social!

Twitter:
twitter.com/manitobaunix

Facebook:
facebook.com/ManitobaUnix

Meetup
meetup.com/Manitoba-UNIX-User-Group

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

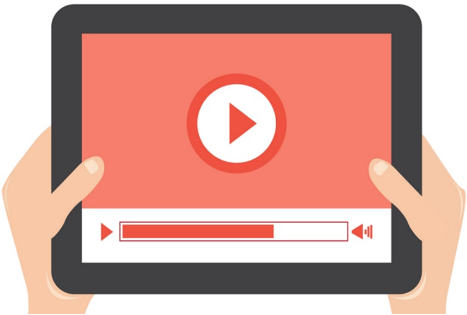
https://muug.ca/meetings/MUUGmeeting.pdf

Sponsors

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/

Watch MUUG Online



Missed a meeting, or want to follow along with a demo at home? Video recordings of the DaemonDash and presentations are now available on the MUUG website and on our YouTube channel.

https://muug.ca/meetings/video

https://www.youtube.com/channel/UCOhD-mKEXk9oUJActy_u4cUA/about

Creative Commons License