MUUGLines

The Manitoba UNIX User Group Newsletter

Editor: Katherine Scrupa

Next Meeting: April 9, 2019 7:30pm

Presentation: WINE with Kevin McGregor

Kevin McGregor will cover the state of the WINE project, software which enables you to run Windows software unaltered on Linux-based systems.

RTFM: xargs with Adam Thompson

Adam will demonstrate scripting techniques that allow parallel processing using nothing but standard UNIX tools.

Crontab

7:30pm: Meeting begins (init)

7:40pm – 8:15pm: Announcements/Roundtable, RTFM

8:15pm - 8:30pm: Break – eat and socialize

8:30pm - 9:45pm: Presentation & questions

9:46pm – 9:59pm: (sigterm)

10:00pm: Room must be empty (*sigkill*)
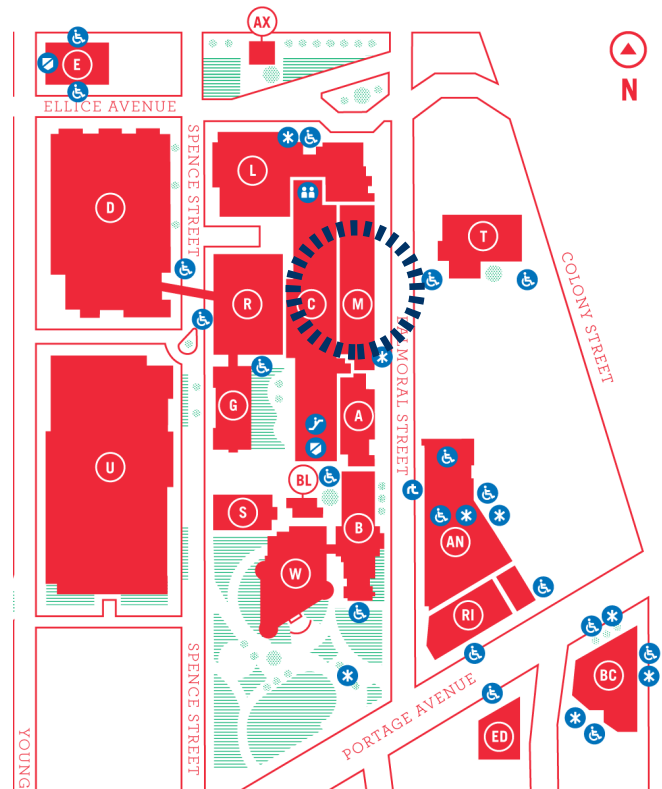
Nova Scotia Government Wins Cybersecurity "Award"

In 2018, a 19-year-old man was arrested for "unauthorized use of a computer." The charges have since been dropped.

The files were downloaded from Nova Scotia's freedom-of-information portal. Information consisted of birth dates, social insurance numbers, addresses and government-services client information. The information could be access by changing a number in the URL.

In March 2019, The Electronic Frontier Foundation awarded the unwanted "What the Swat?" award, notably for targeting the individual who brought the issue to their attention, and poor incident handling.

https://www.thechronicleherald.ca/news/local/privacy-breach-leads-to-embarassing-award-for-nova-scotia-292244/

Where to Find the Meeting: 2M67 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, or the bus terminal parkade. Please see http://www.uwinnipeg.ca/maps for further information about parking and access to the campus.

ICANT

ICANN is responsible for gTLD and DNS root zones, so they have been a big proponent for DNSSEC. Unfortunately, ICANN had misconfigured DNSSEC for https://www.icann.com

The DS record was missing, which is a common mistake. The misconfiguration has since been resolved.

ICANN owns both the .org and the .com. The .org was and is correctly configured.

https://twitter.com/__agwa/status/1099782458046705669?s=03

"Right to Repair" bill Submitted in Ontario's Legislative Assembly

In February, MPP Michael Coteau put forth a "right to repair" bill for electronic devices, an Amendment to the Consumer Protection Act. From the bill:

"At the request of a consumer or consumer electronics repair business, a brand holder shall provide them with the most recent version of the documents, replacement parts, software and other tools that the brand holder uses for, or provides to others for,

(a) diagnosing, maintaining or repairing the brand holder's branded electronic products; or

(b) resetting an electronic security function of the brand holder's branded electronic products if the function is disabled during diagnosis, maintenance or repair..

The bill also stipulates costs for materials should be reasonable, and for items such as digital documentation, free."

If passed, bill 72 would be the first Right-to-Repair law for electronic devices in North America.

https://www.ola.org/en/legislative-business/bills/parliament-42/session-1/bill-72

Cisco RV-series Routers with strcpy Oversight Results in Buffer Overflows with Password Field

Cisco's RV-series routers which use embedded Linux, uses the strcpy function to handle login authentication.

Strcpy has an unfortunate behaviour of copying its data into a buffer without checking the length of the other buffer. This can allow a malicious actor to overwrite data, or redirect program execution. Because of this, strcpy is a well-known function to look for in an audit.

Security patches are available and free from Cisco (you don't need a support contract). As of March 1, 2019, the current patched versions are:

RV110W Wireless-N VPN Firewall: 1.2.2.1

RV130W Wireless-N Multifunction VPN Router: 1.0.3.45

RV215W Wireless-N VPN Router: 1.3.1.1

https://www.theregister.co.uk/2019/03/01/cisco_cve_2019_1663_strcpy_login_authentication/
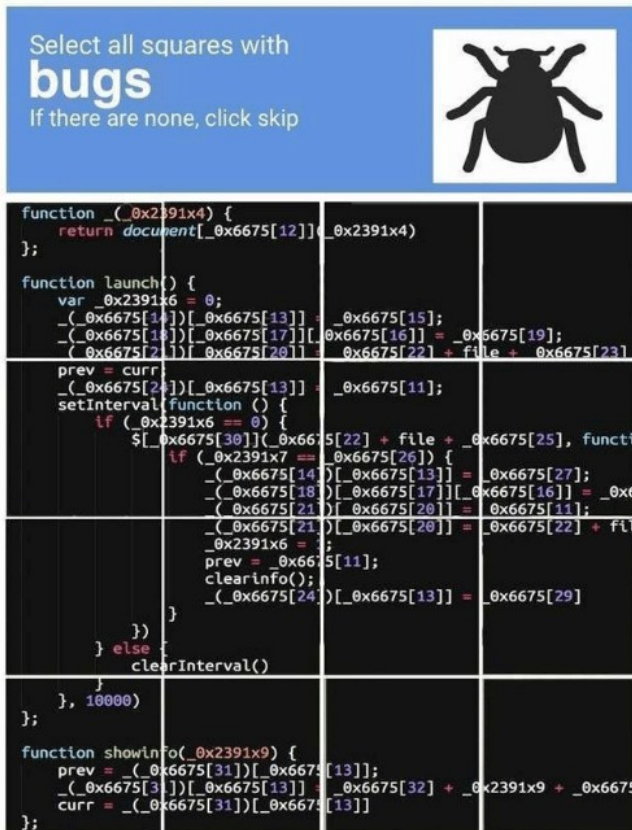
[Citation needed] \\TODO

Ever take a closer look for the man page for gcc? You know, the manual you use to look for the options of the tool you are using?

"Other options are passed on to one or more stages of processing.

Some options control the preprocessor and others the compiler itself.

Yet other options control the assembler and linker; most of these *are not documented here* [ed. note: emphasis ours], since you rarely need to use any of them."

https://linux.die.net/man/1/gcc

```
function _(_0x2391x4) {
    return document[_0x6675[12]](_0x2391x4)
};

function launch() {
    var _0x2391x6 = 0;
    _(_0x6675[14])[_0x6675[13]] = _0x6675[15];
    _(_0x6675[18])[_0x6675[17]][_0x6675[16]] = _0x6675[19];
    _(_0x6675[21])[_0x6675[20]] = _0x6675[22] + file + _0x6675[23]
    prev = curr;
    _(_0x6675[24])[_0x6675[13]] = _0x6675[11];
    setInterval(function () {
        if (_0x2391x6 == 0) {
            $[_0x6675[30]](_0x6675[22] + file + _0x6675[25], functi
                if (_0x2391x7 == _0x6675[26]) {
                    _(_0x6675[14])[_0x6675[13]] = _0x6675[27];
                    _(_0x6675[18])[_0x6675[17]][_0x6675[16]] = _0x6
                    _(_0x6675[21])[_0x6675[20]] = _0x6675[11];
                    _(_0x6675[21])[_0x6675[20]] = _0x6675[22] + fil
                    _0x2391x6 = ;
                    prev = _0x6675[11];
                    clearinfo();
                    _(_0x6675[24])[_0x6675[13]] = _0x6675[29]
                }
            })
        } else {
            clearInterval()
        }
    }, 10000)
};

function showinfo(_0x2391x9) {
    prev = _(_0x6675[31])[_0x6675[13]];
    _(_0x6675[31])[_0x6675[13]] = _0x6675[32] + _0x2391x9 + _0x6675
    curr = _(_0x6675[31])[_0x6675[13]]
};
```

Having Fun with MicroTik

Want to play around with MicroTik? Their RouterOS ISOs are available online, so you can run them as a VM, and extract system files.

The shell is only a command line interface for simple router commands. However, for further fun, you can root it and get a UNIX shell.

Follow this tutorial from Jacob Baines for some additional fun.

https://medium.com/tenable-techblog/
make-it-rain-with-mikrotik-c90705459bc6

Silly and Not-Silly Favourites

Find a physical server among servers:

  cat /dev/random | /dev/audio

Per-directory bash history:

  http://dieter.plaetinck.be/post/
per_directory_bash_history/

e: the bash script exits as soon as any line fails
x: prints each command that is going to be executed with a + in front of it

  set -ex

Last argument of command:

  Alt+.

Bonus: turn your Hyper terminal into nyancat while typing:

https://www.npmjs.com/package/hyper-cat

Play Nearly any Kind of Media on Chromecast

Cast All The Things (CATT) is a command-line tool that allows you to scan your network for Chromecast devices and to send media with simple one-liners:

catt cast ./mygif.gif

catt cast "https://www.youtube.com/watch?v=dQw4w9WgXcQ"

catt cast -s ./Demo.srt ./yourvideo.mp4

catt cast_site https://null-byte.wonderhowto.com

https://null-byte.wonderhowto.com/how-
to/hijack-chromecasts-with-catt-display-
images-messages-videos-sites-more-
0192834/

Control Android Devices from a Desktop with scrcpy

scrcpy is a tool launched from the command line that allows you to control an Android device from your desktop, or record its screen. It's lightweight, and focuses on performance with reasonable quality, offering 30~60 FPS, with a resolution of 1920x1080 or more. It also has a low latency (70 - 100 ms).

scrcpy's features:

"Control Android devices from a desktop (with a mouse and keyboard) running Linux, Windows or macOS

Works over USB or WiFi (though the performance decreases when using it over WiFi)

Allows recording the Android screen while mirroring

Limit the Android mirroring resolution width and height

Change the video bit-rate

Device screen can be cropped

Mirror multiple devices in the same time

scrcpy can be started directly in full screen

For presentations, scrcpy can show physical touches on the Android device (only physical touches, with finger on the device!)

Install APK by dragging and dropping it onto the scrcpy window, or push a file to the device /sdcard by dragging and dropping a non-APK file

Read-only mode to disable interacting using input keys, mouse events and drag&drop"

https://www.linuxuprising.com/2019/03/control-android-devices-from-your.html

Door Prize Books This Month:

Bash Pocket Reference

O-Reilly Media, March 2016

You'll quickly find answers to the annoying questions that generally come up when you're writing shell scripts: What characters do you need to quote? How do you get variable substitution to do exactly what you want? How do you use arrays? Updated for Bash version 4.4, this book has the answers to these and other problems in a format that makes browsing quick and easy.
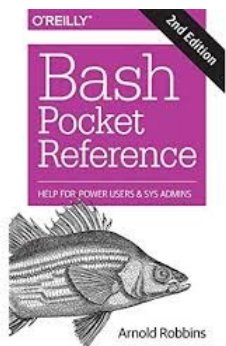
MUUG has gone social!

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/

Creative Commons License