MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 33 No. 5, January 2021 Editor: Trevor Cordes

Next Meeting: January 12th, 2021 (Online Jitsi Video Meeting)

Feature Presentation: Open Source Solutions for Remote Work

Alberto Abrao and Troy Denton will give an overview of free and/or open source solutions for modern remote work needs.

Topics include:

- Video meetings – hosting your own with Jitsi. Existing free(!) services, and self-hosted installation
- VPN – how to host your own with wireguard
- Office 365 alternatives: NextCloud and Collabora Office. Overview and installation

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

Where to Find the Meeting:

`jitsi.merlin.mb.ca/muug.2021.01`

This month (just like last month) we are using our own online Jitsi meeting server hosted by merlin.mb.ca.

The virtual meeting room will be open around 7:00 pm, with the actual meeting starting at 7:30 pm.

You do not need to install any special app or software to use jitsi: you can use it via any modern webcam-enabled browser by going to the aforementioned link.

Thank you `MERLIN` *(the Manitoba Education Research and Learning Information Networks)* for providing the hosting and bandwidth for our meetings.

How's Your Jitsi?

MUUG wants to hear from you about your experiences with Jitsi, the open source software MUUG is using for its online meetings. Have you had any trouble or glitches? Has performance been OK? The MUUG board is here to help if you are still experiencing issues. Email the roundtable mailing list, or `board@muug.ca`.

Since the last meeting we have updated the Jitsi server and you may notice a few changes this month. For one, we've made it mandatory you enter a screen name in order to join the meeting.

New Distro Releases

Activity continues on the distro front. Some of the more notable releases are:

- CentOS 8.3: makes it easy to migrate from the legacy release paradigm to the new CentOS Stream "just ahead of RHEL" rolling release.
- FreeBSD 12.2: includes updated Intel wireless support, a Linux-in-jails feature, and newer OpenSSL, OpenSSH, clang, and more.

Notable Software Updates

- Firefox 84: WebRender is now on by default, if you use GNOME and X11, making things faster and smoother; Flash support goes the way of the dodo, but hardly anyone will notice; and Linux shared memory will be used for improved performance.

- Ruby 3.0.0: in progress since 2016, this major milestone focuses on performance, concurrency and typing. They claim 3X speed improvement in some benchmarks compared to 2.0!

- GnuCOBOL 3.1.2: Yes, you too can learn COBOL and become one of the most-direly-needed programmers! Surprisingly, this version gets support for modern things like JSON and XML generation. Yes, in COBOL.

- Xfce 4.16: 1.3 years in the making, this release includes the developers' switch to GitLab and other behind-the-scenes workflow enhancements. There are also tons of user-facing changes. As a small sample, Thunar can now pause copy/move operations and you can queue file transfers, and a new visually-consistent set of icons helps to define Xfce's new visual identity:

- GTK 4.0: is the result of four years of development. They have dropped the "+" from the GTK+ moniker. Highlights of 4.0 are built-in media playback, drag & drop support, improved accessibility, and more. It will be the basis for the upcoming GNOME 40 desktop. (Guess those Xfce people have to get back to work to migrate from GTK 3.)

Linux Random Never Blocks

This author got a big shock one day while reading random bits from /dev/random: the entropy pool wasn't decreasing after each read! 10 bytes read: hardly any change. 100 bytes read: hardly any change. 1000 bytes read (more than the pool indicated): hardly any change. Why was /dev/random behaving like /dev/urandom?

It turns out Linux 5.6 quietly removed the blocking-ness aspect from the LRNG system in a major revamp. From the patch submission:

> *The main improvements compared to the existing /dev/random is to provide sufficient entropy during boot time as well as in virtual environments and when using SSDs. A secondary design goal is to limit the impact of the entropy collection on massive parallel systems and also allow the use accelerated cryptographic primitives.*

For the compliance crowd, this new LRNG system is "SP800-90B" compliant and ships with the requisite assessment, as well as related test tools. Apparently SP800-90B does not permit using system interrupts (such has HID and disk events), which the old LRNG utilized, and as such this new one does not.

The new LRNG is also "about 50% faster in the performance critical interrupt handler code path". The only time this LRNG should block is before the CRNG (Linux crypto-strength RNG) is ready; something that occurs very early in the kernel boot process.

A new flag has been added to getentropy(), GRND_INSECURE, for when junky, "best effort" randomness is acceptable.

Interestingly, the following still reports a variable amount which changes continually over time, yet the LRNG is no longer constrained by it:

```
cat /proc/sys/kernel/random/entropy_avail
```

The kernel also makes more extensive use of in-hardware RNGs such as the quality (when the bugs have been fixed, see the Sept. 2020 issue of MUUGLines) ones found in the latest Ryzen and Intel CPUs. However, for the conspiratorial-minded, the increased reliance upon opaque CPU RNGs and elimination of HID/HDD "noise" as an entropy source may make it easier for a malefic entity to

control the quality of the world's cryptographic security.

For fun and laughs, boot your 5.6+ kernel with the kernel command line option:

```
dyndbg=file drivers/char/lrng/* +p
```

to view all the activity of the LRNG in dmesg.

https://www.phoronix.com/scan.php?page=news_item&px=Linux-5.6-Random-Rework

https://lwn.net/Articles/817575/

Proving Daemon File Access

We've all been there. You're editing some obscure conf file for a daemon. You reload the daemon but you swear it's ignoring what you've put in the conf file. Is it even reading the files you are editing?

Now you can easily prove the daemon (or other program) is using/ignoring your conf file so you can open up a bugzilla, or troubleshoot the chain of conf file reads: using inotifywait. Is BIND named really accessing all the zone files you think it is?

```
inotifywait -r -m -e access \
/var/named/data
```

This will show you every file the daemon accesses as you restart the daemon, in the order they are accessed. Very handy for troubleshooting complex daemons with long conf file include chains. inotify is the gift that keeps on giving.

CentOS "Forked" Already

Well that didn't take long! Those at the last MUUG meeting will recall the discussion regarding Red Hat's changes to CentOS where they are basically turning it into not-so-bleeding-edge-Fedora, thus making it useless for its sole purpose for many people: being a drop-in, free, exact replacement for RHEL.

Enter CloudLinux, who recently announced it was investing over a million dollars into making a CentOS (the original paradigm) clone.

> *Red Hat's announcement has left users looking for an alternative with all that CentOS provides and without the disruption of having to move to alternative distributions. We promise to dedicate the resources required to Project Lenix that will ensure impartiality and a not-for-profit community initiative. CloudLinux already has the assets, infrastructure, and experience to carry out the mission, and we promise to be open about the process of developing Project Lenix.*
>
> *– Igor Seletskiy, CloudLinux CEO*

> *Project Lenix will be a free, open-source, community-driven, 1:1 binary compatible fork of RHEL 8 (and future releases). For CentOS users, the company promises Lenix will provide an uninterrupted way to convert existing CentOS servers with absolutely zero downtime or need to reinstall anything.*
>
> *– Anonymous on ZDNet*

Apparently *Lenix* is just a placeholder name for the time being.

In addition to *Lenix*, CentOS's original co-founder Gregory Kurtzer also announced he will create his own RHEL clone: *Rocky Linux*. So there is a lot of movement in the community to counter Red Hat's somewhat controversial move. It hearkens back to prehistoric times when Red Hat ditched the free RHL and created RHEL and left the free-as-in-beer crowd in the lurch for about a year until Fedora was created. (Much to the delight of Debian, et al.)

https://www.zdnet.com/article/cloudlinux-to-invest-more-than-a-million-dollar-a-year-into-centos-clone/

Linux On Apple's M1 CPU?

Hector Martin, who ported Linux to the PS4, is trying to port Linux to Apple's new M1 CPU. By now almost everyone has heard that Apple is changing their Macs from Intel CPUs to their own in-house-designed silicon.

Hector is crowdfunding to support his porting goal and he promises to not only get the kernel working, but to fully support the custom Apple hardware, including the "most complicated component" the "custom Apple GPU".

https://apple.slashdot.org/story/20/12/01/234232/hector-martin-promises-to-bring-linux-to-the-m1-chip

But maybe not so fast, says Linus Torvalds:

> *I've been waiting for an ARM laptop that can run Linux for a long time. The new Air would be almost perfect, except for the OS. And I don't have the time to tinker with it, or the inclination to fight companies that don't want to help.*
>
> *[...]*
>
> *The main problem with the M1 for me is the GPU and other devices around it, because that's likely what would hold me off using it because it wouldn't have any Linux support unless Apple opens up.*

So Hector might try pulling it off, but Linus doesn't seem keen to help at the outset, and the whole world knows Apple will make life difficult trying to figure out how to program their proprietary hardware. Hmm, where have we heard that before?

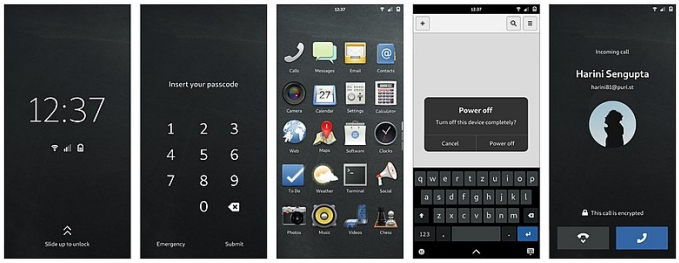
https://hardware.slashdot.org/story/20/11/24/2225209/linus-torvalds-would-like-to-use-an-m1-mac-for-linux-but

Free And Private Smartphone

Yes! says Purism! After a $2.2M crowdfund, this company (dedicated to privacy and freedom in the extreme) is now shipping their new Librem 5 smartphone.

Like all Purism products (they have long sold laptops), the Librem 5 is designed to eliminate as much of the non-free hardware and software as is humanly possible. Openness and transparency is their stated goal. They have received plaudits from the FSF.

For the privacy-conscious this new phone should be a boon. Everyone knows iOS and Android try to



track nearly everything you do and allow governments to access your data. Disabling said tracking is made extremely difficult, and in some cases, impossible.

Librem 5 will have none of these problems. It runs Purism's PureOS, which is not at all based on Google's Android. In fact, it's the same OS used on Purism's Laptops and mini PCs.

The phone will have a user-removable cellular modem, WiFi card and battery. There are external hardware kill switches to the modem, WiFi, BT, GPS, accelerometer and all other sensors.

Purism developed many necessary software components to enable the usability of PureOS on a phone form-factor, including: libhandy, phosh, squeekboard, and the uniquely named phoc. (Can't wait to see the bugzilla reports for that one.)

As an added bonus, the phone can attach to a dock to become a full-fledged desktop computer with a full-sized monitor and other HIDs.

Purism and the Librem 5 are not without detractors. There is some disagreement over how far along FSF's (possibly impossible) scale of "perfectly-free" Purism's products are. However, the difficulty in producing "exceedingly-free" hardware products and OSs these days should lead one to commend the current effort, and to cheer on further progress.

One slight downside: the *Librem 5 USA* costs $1999 USD, proving that you can buy *free*, but not for *free*!

https://puri.sm/posts/librem-5-mass-production-phone-has-begun-shipping/

https://shop.puri.sm/shop/librem-5-usa/

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

Creative Commons License

A big thanks to Les.net for providing MUUG with free hosting and all that bandwidth! Les.net (1996) Inc. is a local provider of VoIP, Internet and Data Centre services. Contact **sales@les.net** by email, or +1 (204) 944-0009 by phone.