MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 33 No. 7, March 2021 Editor: Alberto Abrao

Next Meeting: March 9th, 2021 (Online Jitsi Video Meeting)

Feature Presentation: MeshCentral

Following up on our recent Open Source Solutions for Remote Work series, Alberto Abrao will show how to install and use MeshCentral, a simple and efficient open-source solution for management and control of computers, phones and tablets.

A web portal provides the tools for managing and controlling all paired devices. The server runs on Windows, Linux, or OpenBSD. These can be hosted on cloud platforms such as Azure and Amazon EC2, or a cheap VPS instance by virtue of its light footprint. It is also suitable for self-hosting, either Internet-facing or restricted to your Local Area Network (LAN). The Agent to be installed on client devices is compatible with Windows, Linux, *BSD, MacOS, and Android.

Where to Find the Meeting:

`jitsi.merlin.mb.ca/muug.2021.03`

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.

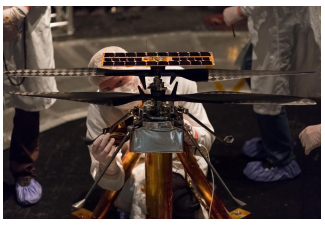
The latest meeting details are always at:
`https://muug.ca/meetings/`

The year of Linux has finally arrived... and it is out of this world

Many Linux users look forward to seeing our system of choice dominating the Desktop world.

Others argue that it already did, by striking the word Desktop, as most computing devices are already running one of its many flavours. If that fails, getting all smug about supercomputers does the trick.

As of February 18, 2021, we can, at once, dial up the smugness and not worry about these earthly quibbles, as the year of Linux has dawned upon Mars.



Ingenuity, the helicopter that travelled to Mars, attached to Perseverance's belly, is now on the Red Planet. It is the first helicopter to arrive on another planet, which is a feat in itself, but its mission is not over yet: it must keep itself warm during Martian nights, which can go down to -90 degrees Celsius: that alone makes Canada's worst winter feel like the warmest Caribbean summer. It also has to keep itself charged, using its solar panel.

Then, after a few other tests, it will attempt to fly autonomously and, hopefully, land successfully after that. If that goes well, up to four more test flights are scheduled.

The tiny marvel is running F´ (F Prime), a "Flight-Proven, Multi-Platform, Open-Source Flight Software Framework", developed at NASA's JPL (Jet Propulsion Laboratory) for cubesats and instruments, and later open-sourced. It also uses many off-the-shelf "commercial grade" hardware components that were tested and verified to withstand the harsh conditions of the Red Planet.

Hopefully, the scrappy, space-grade flying bot will succeed in its mission, bringing not only valuable intelligence but bragging rights galore to both space aficionados and open-source enthusiasts.

Come back down to earth: the state of computer security, sunlight or not

The last couple of years saw a huge increase in IT security incidents, the most recent one being the SolarWinds snafu.

Now, if we must come back down to earth, we shall leave our smugness on Mars: yes, SolarWinds Orion is proprietary, and their dismissive attitude toward openness did come back to haunt them, but our brave new open-source world is not immune to these threats.

In the 90s, Open Source was tied to amateurism: "*a bunch of folks in their basements duct-taping code and hardware together so it would pass for the real thing*". It did not take long for this assumption to be proven wrong, but the myth persisted in many circles. SolarWinds' past comments about Open Source are a cheap, yet nutritious source of *schadenfreude*.

A little bit of history is in order. What follows may be surprising to many, being that "open" is often tied to "free" (as in beer). Going back the decades, however, "open" is often a rallying cry to defeat the jaws of vendor lock-in, not because one isn't willing to spend money, but to keep vendors honest and make sure they are not using backhanded tactics to force others to do their will, be it clients or competitors.

This was a concern long before names such as Linux, BSD-derived OSs (not BSD itself), etc., were a thing: the Open Software Foundation (OSF) was created in 1988 as an attempt to prevent AT&T and Sun from trying to hold other vendors hostage by doing just that.

While they were working to keep each other honest, uncle Bill was chipping at their lunch. Later on, court documents presented during Microsoft's antitrust trials showed that all that gluttony was, at least in part, brought by the infamous *Embrace, Extend, and Extinguish* (EEE) strategy.

Thus, even before Free/Libre and Open Source Software (FLOSS) went mainstream, and security was not (yet) a pressing matter, the threat of vendor lock in was seen as dangerous even by big companies.

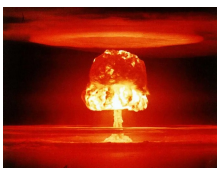
That also proves that our friendly "basement dweller neckbeards", spearheading the FLOSS efforts in the 80s, 90s and beyond, were right: sunlight is the best disinfectant, both for code and for nefarious business practices.

Disinfecting the latter is *complicated*. The former, though, looks easy enough, at least for Open Source Software: the bits of code are out there, anyone can take a look at it. Of course others are reviewing it, *right*?

Yeah, right. Heartbleed (2014) threw a big wrench on that assumption. A lot was said about the OpenSSL project having scant resources, being maintained by volunteers, only one of them full-time, all the while being a critical part of the Internet's fabric. This realization spawned the Core Infrastructure Initiative from the Linux Foundation, whose goal is "to fund open source projects that are in the critical path for core computing functions." It also marked the beginning of Google's Project Zero.

The idea that a ragtag crew of volunteers would make something bulletproof out of rainbows and unicorns took a huge blow. Even the brightest of us is only human after all.

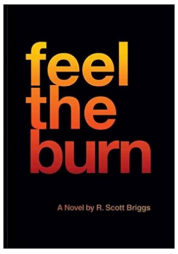
Since then, vulnerabilities are an everyday thing. The sunlight theory gave way to the *cult of the security update, they who must be installed.* That brings much *joy* to all Windows system administrators and technical support staff



everywhere: *Today is Patch Tuesday, did you bring lunch? What about dinner?*

Fast forward to the SolarWinds Orion debacle from a few months ago, when the rogue bits were slipstreamed on the company's build system and eventually found their way into an update package. Which was released through official channels, then promptly installed by most sysadmins – save a few *irresponsible* ones. These, in hindsight, ended up being the smart ones, just like those who postponed upgrading their CentOS servers from version 7 to 8 are smiling now. *Not lazy, efficient.*

Breaking news: a corporation, just like our ragtag crew of volunteers, is also comprised of humans after all… with closed source software though, there was no canary. All from a vendor who touts the virtues of not being vulnerable to… well, to the exact same thing that happened to them. Ouch.



Security vulnerabilities are an everyday thing at this point. Most just update and go on, others may want to check the CVE (Common Vulnerabilities and Exposure) entry to see if it is relevant to their environment, test the patch to ensure it will not interfere with a critical application etc. The sun shines upon us, imperfect as we are, and we're still here. Same for vulnerabilities.

Accepting the inevitability of our imperfection, however, does not answer the question about what to do when flawed beings are *perfectly* deliberate about their desire to watch the world burn.

To answer this question, Google, a former darling of the Open Source World, has proposed a framework for the discussion around vulnerabilities in open source that can roughly be summarized as "*audit it all – on our platform… obviously (tm)*", the new standard operating procedure for all companies vying to be the feudal lord of our 21st Century Digital Feudalism.

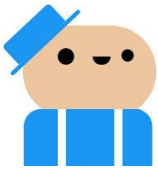
Just like that, all feathers were ruffled on that chaotic little planet of ours. Long since demoted from darling status, Google's announcement saw trucks of salt go crazy around the world, enabling all to have a grain handy if they so desired.

That was not enough: critics were quick to point out how ironic it was that the company responsible for Chromium, a project notoriously hard to build from source, had the gall to propose this big initiative for all others to follow, on their terms, their platform, their rules. Their fiefdom.

Incidentally, the same is said about Android, another project from… listen, *there are no patterns here whatsoever, let us carry on, shall we?*

Google was founded around the time Microsoft was being investigated for its monopolistic practices. It seems they are now trying to avoid the late bloomer moniker by pulling similar shenanigans, and many argue that an investigation is on its way.

Amusingly, less than 48 hours after *that*, three big security issues had to be tackled by the all-knowing-G on its ~~Internet Explorer 6~~, sorry, Chrome browser: a way for malware to bypass firewalls, a zero-day tied to its ~~ActiveX~~, ugh, JavaScript engine, and a widely-used extension called The Great Suspender that had to be… well, suspended.



The Great Suspender was sold in June of 2020 by its original developer to an unnamed person/entity, who vowed to keep it open source. By November, many started inquiring, on the project's GitHub page, why the version numbers between it and the Chrome Store were out of sync.

These questions were raised before the debacle, proving that, insofar as Open Source is not the definitive answer to all problems of the cosmos, sunlight does seem to keep people honest – or, failing that, provides the "dead canary" we need to ring the alarm. That may be all we, as imperfect human beings, can realistically ask for.

As for Google, it seems that AI, lasers and automated support bots that ban your account for unspeakable things – thus not able to provide you with a reason for its obliteration – are not really doing that great, or are they? Well, they sure know what ads we want to see… yes, for all products we want… that we bought the week before.

Without futuristic tech that most mortals shall not ever understand – or even use, when AI and lasers nuke your account – good old sunlight is working just fine, imperfect as it is. Both history and developers past and present are witness to the importance of keeping control of your destiny – and code. Any drawbacks pale to the antics of yet another massive corporation unable to cooperate without eventually *EEE*'ing its partners.

Speaking of history, a quick trip down memory lane: our MUUG (also known as TUUG) newsletter archives

As much as humanity loves to tout its progress, **Monsieur Ex** (a mysterious Frenchman who is *absolutely, totally not around here anymore, honest!*) would probably state that "plus ça change, plus c'est la même chose". The seemingly eternal struggle between freedom and control is well documented in our past newsletters.

In our May 1991 newsletter, Eric Carsted wrote on the President's Corner:

"I am guilty.

Of what? you may ask. Well, ever since the formation of the OSF (Open Software Foundation) and their announcement of OSF/1, I have completely ignored any announcements regarding features and specifications.

Basically, I have been preaching Open Systems but had a closed mind.

I have felt that the OSF was formed for two specific reasons, greed and greed. I felt that IBM's motive was to cause fragmentation and confusion in the Unix market, to give OS/2 time to catch up and to try to take over in the Unix arena. I did not take into account the increase that AT&T was going to charge for its licence, or the advantage SUN would have by working on the development of the kernel (six to twelve months). At the time of its formation, OSF/1 was based on ADC, a crippled OS controlled by Big Blue Brother. I have a thing about IBM, especially since the Micro Channel bus and OS2 (another move motivated by greed). If IBM is involved, I am very suspicious. When the OSF announced it would use the Mach kernel, I was pleased and relieved but was still resentful of the confusion that the split in the market was causing. Many announcements have been made in the intervening time but if the title of the story had 'OSF' in it, I skipped on right by. Until now."*

That all sounds… unsettlingly familiar. The more things change, the more they stay the same, indeed.

A commercial advantage for Open Source solutions may be brewing

It is notorious that Google yanks support and kill things willy-nilly – even the security initiative outlined above was greeted by jokes like "how long will it last until Google kills it?" – but it now seems that Microsoft, who has backwards compatibility as one of its main competitive advantages, wants to jump into the fray as well.

The perpetual nemesis of many software freedom's connoisseurs is both reducing the support window for its LTSC versions of Windows and making it clear that anything that is not cloud-related will not only be more expensive, but you are also on your own for support.

If the plethora of FLOSS projects that rely on selling support for revenue are able to exploit this growing trend, they are poised to make their finances go all the way to the moon… if they can resist the urge to follow the trend themselves, of course.

It does seem to be working great for Nextcloud, and we hope others follow.

Summer is coming, but the bugs are already here

After the long-standing **sudo** vulnerability was discovered in late January – and mentioned on our last month's newsletter – we never, ever skip a beat around here! – we have another one, just in time for this month's edition.

Xterm, part of that old, crusty, yet resilient windowing system known to some as "*Mumm-Ra*", realized that having CVEs mentioning your precious little name is all the rage now, and it makes them feel younger! *I still have what it takes! Look. At. Me.*

The issue, detailed on `CVE-2021-27135`, stems from a crafty UTF-8 character sequence that, when displayed through an Xterm session, may cause a segmentation fault, potentially allowing remote code execution, and all the other *bad stuff that may potentially happen.*

As usual, update, update, update. *Oh, darn it…*

`https://access.redhat.com/security/cve/cve-2021-27135`

The cosmos: party on the web like it is 1993 with Gemini – or the MUUG website, your choice

MUUG, being the *extraordinaire*, inclusive and eclectic group that we all know and love, has people of all ages and walks of life.

Not exclusive to MUUG is a divide between generations, where old folks start reminiscing about the good old days, while younger ones facepalm about how delusional they are, because the future is now, and it has lasers.

Yet lasers, just like those pesky GUIs that prioritize form over function and are idolized by all these damn youngsters, often spoil the bunch. The shiny is there, but the content was burned by it.

Those of us who were around when our most glorious MUUG website's aesthetics were *avant-garde* appreciate how, no matter how much those pesky little buggers insist that it looks "old fashioned" by now, all the information is right there, easily accessible, without distractions.

The old way makes it easy for all the *experienced* folks to just sit down and communicate their wisdom, without the need for a team of graphic designers, who demand their fancy meals and distract them from their mission.

Or, for the not-so-experienced ones who grew up willing to grok man pages instead of playing soccer, the old way is a reminder on how rewarding it was to dig for information, when mostly everything on the web was precise, honest, written by people who were doing so out of passion and desire to share. The days before copy-pasta "click on me, I am an ad!"–infested websites became the norm, and we spend a lot of time trying to find a place where a modicum of effort is spent – not wasted – on making sure the content has at least some context, instead of being a hodgepodge of keywords put together mainly for Search Engine Optimization (SEO) purposes.

If the web of yore sounds interesting to you, you may want to check `https://gemini.circumlunar.space/`

If it doesn't, well, get off my lawn.

GNOME turns 40, finally grows up

GNOME has released the beta for its version 40. Like Firefox 10-ish years ago, many were scratching their heads, wondering if they are going insane, or just missed the time warp.

Settle down, everyone: they did pull the "drop the dot, every update is now a major version number!" move from 10 years ago, but it is like the rebellious kid who eventually finds their individuality, yet still wants one last chance to play the contrarian, just to remind themselves of who they *really* are.

Gnome 40 – tested on Fedora 34 pre-release – is a mature, coherent desktop environment. It keeps all of its newfangled desktop metaphors that are now around 10 years old, but its flow is now mature, with visual cues that *finally* make sense, making for a surprisingly pleasant desktop experience.

Far from the early days of GNOME 3, the latest point releases of the old version are good enough for daily use. They suffer from a lack of continuity in its design: animations: things move around too much, darken the screen too much, move when they shouldn't, stay put when they oughtn't; and all the things that the environment suggest you would be able to do, but can't – such as nest icons on the "App" launcher screen to form groups, for example.

GNOME 40 delivers all of that. No more insane shade variations, or not delivering on things suggested by the feel of the environment they defied the whole community to implement. Not in a revolutionary way – GNOME 3 is already 10 years old – but by finally making good on their promise of a different, yet coherent and enjoyable environment, by working on the coherent part. Coupled with the many performance improvements, the new version is certainly a big – and welcome – step forward.

If you are set in your ways, there's always good old XFCE

The venerable, slow moving XFCE is always there if you really, really don't like GNOME and its "new-ish" way of doing things.

Long stuck on version 4.12 (February 2015), rumours that the project was dead were all over the Internet.

They were wrong: version 4.14 was released in August 2019. It was a big update, tackling the move from GTK 2 to GTK 3. There were many visual updates as well, adding to the polish of the environment while keeping its lightweight footprint. Yet, a promise of further enhancements for its user interface was postponed.

Version 4.16, released on December 2020, delivers on that, and makes it clear that the project, albeit focused on things very much different from GNOME, is far from dead.

How's Your Jitsi experience?

MUUG still 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.

We've made it mandatory you enter a screen name in order to join the meeting.

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.