MUUGLines

The Manitoba UNIX User Group Newsletter

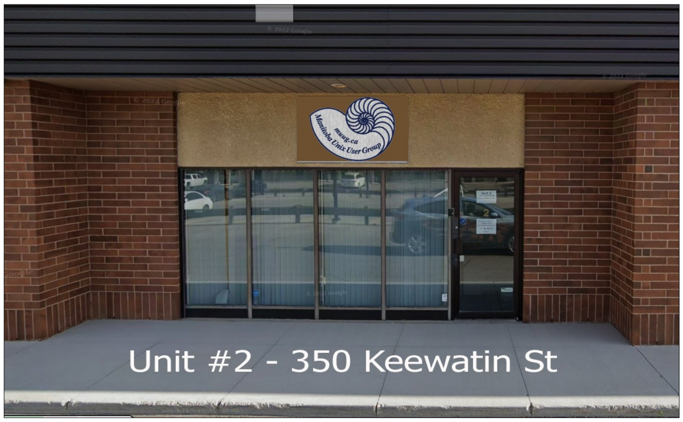
Volume 36 No. 5, Jan 2024

Editor: Tyhr Trubiak

Next Meeting: January 2nd, 2024 (In person and online video)

For the remainder of 2024 (and possibly longer), the meeting will be held **both physically in person**, and **online** via our Big Blue Button videoconferencing server.
We encourage all members to attend in person. If you cannot attend in person, you can watch and interact with the meeting online and partake of our professional-grade camera, microphone, and dedicated stream moderator.

If you show up in person you will be treated to more beverage choices than we've offered in over a decade: coffee, tea, and pop, as well as cookies. Parking is free, copious, safe, and within WiFi range! Although we encourage you to walk to few feet to a warmer welcoming room of like-minded individuals.



*There may be more or less snow than shown above…as the "M" in MUUG proudly stands for **Manitoba**.*

Please stay home if you are sick that day.

To attend via internet, check and refresh the following link after 7:00pm. There is no need to create an account in BBB, nor login. Just enter any name as your screen name and hit **join**.

`https://muug.ca/meet`

Presentation:

Working around LibreNMS dashboard limitations using Nagios, APIs, and ImageMagick

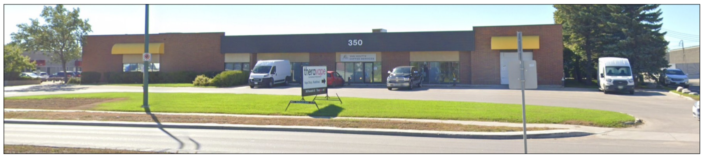
By: Chris Audet

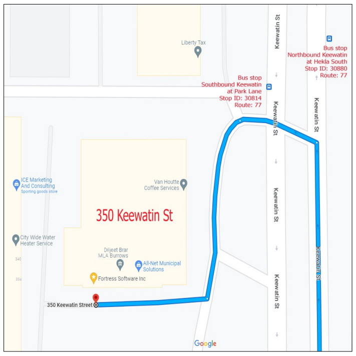
The latest meeting details are always at:
`https://muug.ca/meetings/`

Where to Find the Meeting

We are continuing to meet on the first Tuesday of every month.

Fortress Software Inc.
350 Keewatin St – Unit #2





Doors will open at 7:00pm. Meeting starts at 7:30pm.

If driving, enter the lot using the most north-eastern entrance (far right in the top picture) and drive around to the south west corner of the building (see route in map detail). You can use any of the free, ample, and safe parking spots that say “reserved” or “MUUG” in front of units #1 through #4 before entering into unit #2. Look for the sign over the door!

Bus stops #30814 and #30880 (route 77) are only 150 meters away. The last bus leaves for Polo Park at 10:15 pm and for Garden City at 10:31 pm. Logan Ave. bus routes #19, #26, and #27 are a 600 meter (8 minute) walk to the south.

Terrapin breaks SSH Integrity

A

A new attack called Terrapin, developed by researchers from the Ruhr University Bochum, breaks the SSH channel integrity when certain encryption models are used, such as: “**ChaCha20-Poly1305**” or “**CBC with Encrypt-then-MAC,**” both of which are cipher modes added to the SSH protocol (in 2013 and 2012, respectively). An estimated 77% of SSH servers exposed to the internet support at least one of the vulnerable modes.

Terrapin works by altering information transmitted in the SSH data stream during the handshake.

Terrapin lowers the security of the established connection by truncating negotiation messages without the client or server noticing it.

Note that this vulnerability can only be implemented when the attacker has an active “man-in-the-middle”, also known as MiTM, or sometimes referred to as “adversary-in-the middle”.

“The Terrapin attack exploits weaknesses in the SSH transport layer protocol in combination with newer cryptographic algorithms and encryption modes introduced by OpenSSH over 10 years ago,” say the researchers, adding that “these have been adopted by a wide range of SSH implementations, therefore affecting a majority of current implementations.”

One solution to Terrapin is to implement a strict key exchange on both the client and server, as the biggest mitigation factor is the MiTM requirement, making the threat less severe in many cases.

The team that created Terrapin have also released a vulnerability scanner on GitHub:

`https://github.com/RUB-NDS/Terrapin-Scanner`

The weaknesses and flaws associated with the attack are now identified as **CVE-2023-48795**, **CVE-2023-46445** and **CVE-2023-46446**.

`https://arstechnica.com/security/2023/12/hackers-can-break-ssh-channel-integrity-using-novel-data-corruption-attack/`

`https://www.bleepingcomputer.com/news/security/terrapin-attacks-can-downgrade-security-of-openssh-connections/`

OpenSSH 9.6 released!

As of December 19, 2023, OpenSSH 9.6 has been released. It includes some minor improvements and a fix for the Terrapin attack described above.

MongoDB Corporate Hacked

MongoDB, primarily known for it’s No-SQL database, has confirmed a malicious “hack” of its corporate systems.

MongoDB states among the stolen data, it is believed that that customer account metadata and contact information were compromised.

In a notice to customers, MongoDB Chief Information Security Officer Lena Smart said the company was not aware of any exposure to the data that customers store in its flagship MongoDB Atlas product.

`https://www.securityweek.com/mongodb-confirms-hack-says-customer-data-stolen/`

Window’s Blue Screen of Death is coming to Linux!

The “Blue Screen of Death”, from now on denoted as BSOD, *(not to be confused with BSD)*, was originally supposed to be a diagnostic tool/information screen to help administrators on Windows systems. It was somewhat similar to the intent to the Macintosh’s “Sad Mac” or the Amiga’s “Guru Meditation”, except that there seemed to be a period of time when the BSOD was...a little too commonly displayed.

The BSOD’s error codes were notoriously too vague to be of useful to the average computer enthusiast...but that does not mean the intention was a bad idea.

Although currently listed as “experimental” and “subject to change”, Version 255 of the Linux systemd project honors that intent by adding a “systemd-bsod” component that generates a full-screen display of some error messages when a Linux system crashes.

Error messages will only be shown if the error is of the “LOG_EMERG” log level.

Additionally, Phoronix reports that the Linux version will also generate a **QR code** to make it easier to look up information on your phone *(which is also a feature currently in Windows).*

The odds are fairly good that whatever Linux version you are using, if it uses systemd, you will eventually see this feature enabled.

Systemd management is in the majority of the well-known Linux distributions, such as Debian, Fedora, Arch, Ubuntu, CentOS, and Red Hat Enterprise Linux.

Version 255 of systemd also has a lot more useful and significant features added...it’s just that the BSOD makes for a catchier headline.

Expect more additions related to TPM support, disk encryption, and the ability to use hibernation with btrfs file systems.
Support for System V service scripts has been dropped, with complete removal in a future release, and systemctl will now automatically soft-reboot if a new root file system is found under “/run/nextroot/” when a reboot action is done.

https://arstechnica.com/gadgets/2023/12/linux-distros-are-about-to-get-a-killer-windows-feature-the-blue-screen-of-death/

Project Sputnik (Origin Story of Ubuntu on Dell Laptops)

Linus Torvalds loves the Dell XPS-13 -- love it. As Torvalds recently said, “Normally, I wouldn’t name names, but I’m making an exception for the XPS 13 just because I liked it so much that I also ended up buying one for my daughter when she went off to college.”

So, how did Dell end up building top-of-the-line Ubuntu Linux laptops, a project internally known as “Project Sputnik”.

Dell has supported Linux desktops and laptops since the middle 2000’s, although it was primarily Red Hat Enterprise Linux powering workstations.

They brainstormed how how they could appeal to the developer market, which they felt was trending more towards laptops.

When Dell started an in-house innovation fund, Barton George, Dell Technologies’ Developer Community manager, pitched it and was granted $40,000 to pursue the idea.

Barton George felt is was enough to get going, and he put together an official team. He stated, "But none of us were full-time on this. We got approval from their managers to work on this officially, but it was sort of in our spare time. At times, the project staff was two people and a dog."

When George pitched Google and Amazon, while they did not feel it was a good fit for the masses, George felt "It was enough to prove there was a business case for a developer-focused Ubuntu Linux laptop."

When George announced on his personal blog what Dell was planning, his traffic went from 60 views a day to 15,000.

Not quite the numbers Instagram influencers get, but still quite significant, and without any NSFW tags...

So, Dell got together with Canonical, Ubuntu Linux's parent company, to make sure all the drivers were in place for a top-notch Ubuntu Linux developer desktop experience. "We announced a beta program for the machine with a 10% off offer. We thought, well, we'll probably get 300 people. Instead, we got 6,000. This is where senior management said OK, you've got something real. We went from slides to launch in nine months. That's pretty fast for building a system."

As for the name, 'Project Sputnik' is a nod to Mark Shuttleworth, Ubuntu founder and Canonical CEO. A decade before the project itself, Shuttleworth had spent eight days orbiting the Earth in a Soviet Soyuz spacecraft. George and the crew decided "Soyuz" didn't have an inspiring ring to it, so the company went with "Sputnik" instead.

https://www.zdnet.com/article/how-ubuntu-linux-snuck-into-high-end-dell-laptops-and-why-its-called-project-sputnik/

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

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.

Thank You Michael W. Lucas

MUUG would like to thank Michael W. Lucas for donating one of his e-books every month as a door prize. You can view and purchase his highly recommended tech books here:

https://www.tiltedwindmillpress.com/product-category/tech/

Creative Commons License