MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 30 No. 3, November 2017 Editor: Tyhr Trubiak

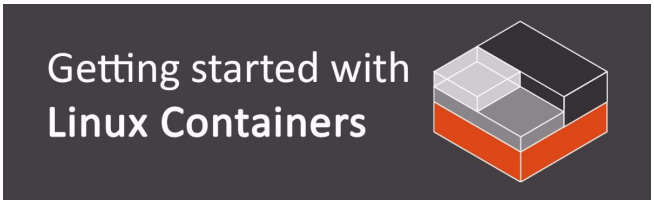
Next Meeting: November 14, 2017

7:30pm

RTFM: MacPorts

Adam Thompson will present and demonstrate **MacPorts**, one of the systems used for compiling, installing and upgrading command-line, X11 or Aqua based open-source software on the Mac operating system.

Presentation: Linux containers (intro)



Kevin McGregor will be presenting an introduction to LXD containers in linux. LXD is a next-generation system container manager, which offers a user experience similar to virtual machines but using Linux containers instead. Kevin McGregor will be presenting an introduction to basic Linux containers using LXD on Ubuntu.

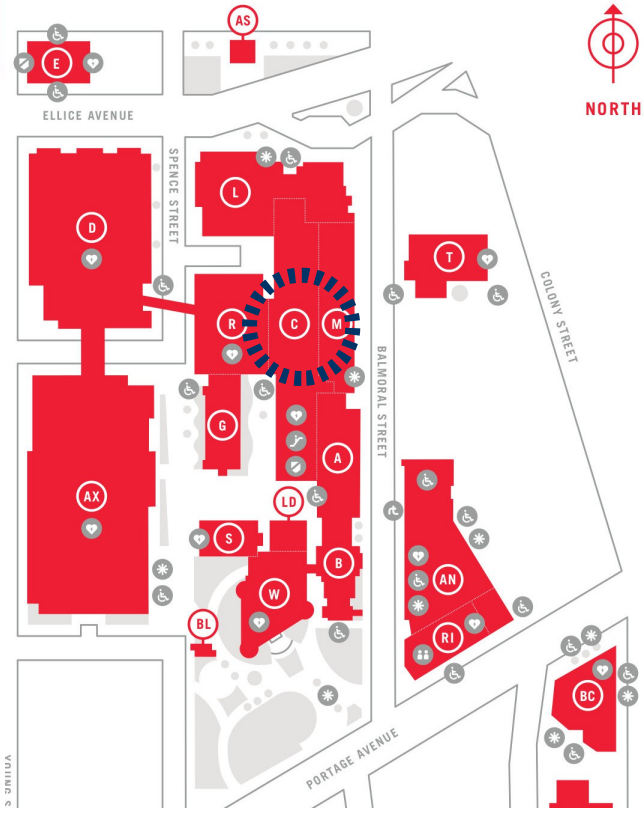
Door Prizes

We will be giving away a couple of e-books & the usual assortment of magazines and miscellanea. Come to the meeting for your chance to win!

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

This Month's Meeting
1C16A Centennial Hall



This month's meeting is in Centennial Hall. Look for a sign on the door. There are elevators and escalators scattered around the buildings. A convenient one might be the elevator located right at the Ellice Ave entrance. Doors are usually open by 7:00 pm with the meeting starting at 7:30 pm. Parking is available on the surrounding streets. Please see http://www.uwinnipeg.ca/maps for further information about parking and access to the campus.

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

2017-2018 MUUG Board Elections

Adam Thompson, Nomination Committee Chair

Every November, the group holds its Annual General Meeting. The main goals of the meeting are to elect the new board, and to pass any special resolutions, if required. The Board may consist of up to nine (9) people.

The following 8 members are allowing their names to stand for re-election:

Trevor Cordes

Owner - Tecnopolis Enterprises

Trevor Cordes (B.Sc. CompSci) has owned and operated Tecnopolis Enterprises, a computer VAR, programming and consultancy company, since 1999. Linux and FOSS have been the keystone of Tecnopolis since inception, embodied in their flagship do-everything appliances for small business. Trevor was President of the Atari ST User's Group for four years, between 1995-1999. He prefers Fedora and Perl.

Gilbert Detillieux

Systems Analyst - University of Manitoba

Gilbert Detillieux has been working with UNIX as a programmer, system administrator, and trainer since 1980. He worked as a computer consultant specializing in UNIX, from 1983 to 1989, and is currently working as a Systems Analyst for the University of Manitoba's Department of Computer Science, where's he's worked since 1989, installing, supporting and upgrading the department's network and UNIX server infrastructure. He was co-founder and past president of the Technical UNIX User Group (now MUUG), and has been an active member of the MUUG board ever since.

Kevin McGregor

Systems Administrator - City of Winnipeg

Kevin McGregor provides server, platform and infrastructure support in the City of Winnipeg's Information Systems Department. After having briefly used UTS on an Amdahl mainframe in university in the mid-80s, he dabbled in Coherent and then converted to Linux and OpenBSD. He has been a member of MUUG since the early 90s, edited the group's newsletter for a number of years, presented various topics at MUUG meetings and has served on the board for the majority of his membership.

Katherine Scrupa

LAN Administrator II - Steinbach Credit Union

Katherine has been a member of MUUG since 2006, during which she has been using Linux at home. Her educational pursuits in Computer Science led her to a Network Technology CCNA (Hons.) program at Red River College in 2010, with an emphasis on networking and system administration. Katherine's current work comprises of root cause analysis, configuration management, automation, and containers.

Adam Thompson

Senior Systems Administrator -
Avant Systems Group

Adam first unknowingly used UNIX in 1988, while playing NetHack on the QNX BBS in Ottawa, which gave him a huge advantage the first time he encountered vi(1)! He first ran into UNIX professionally in 1990, and started using Linux in 1991. Adam is the author of several termcap(5) and terminfo(5) entries, deployed the first cross-platform, public, networked instantmessaging system in Manitoba, and installed the first UnixWare system in Manitoba. He has developed several UNIX/Linux courses, and has also taught RDBMS administration. Adam has been a member of MUUG since 1995, and a board member for over a decade. Adam currently attempts to make multiple versions of Linux, Windows, Solaris and BSD all play together nicely, in between working on customer installations of Atlassian software and making virtualization environments do his bidding.

Tyhr Trubiak

Systems Administrator - Thorkelson Consulting

Tyhr Trubiak has been a member of MUUG since 2013. He manages a mix of Red Hat/CentOS and OpenSUSE servers within VMWare, as well as

some Windows and Cisco devices. His first exposure to UNIX was when he received his B.Sc. CompSci at the University of Manitoba, which he found similar to his first love - the Commodore Amiga. He hasn't found a desktop distro he's liked enough to remain loyal to since, but is currently testing Elementary OS on his laptop. He has enjoyed 2D node-based digital compositing in the past (Blackmagic Fusion, formerly known as Eyeon Fusion), acting and anything Jeep related.

Brad Vokey

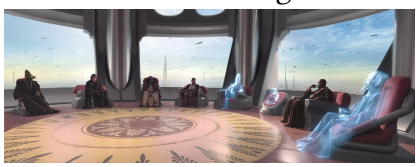
Owner - Fortress Software

Brad is the owner of Fortress Software Inc. And the creator of the Matchmaker Fundraiser (aka "Matchomatics" - a fundraiser that provides compatibility lists for millions of students across Canada and the US). Brad started the company in 1985 using Apple][computers and 6502 machine language. Then switched to 68000 machine language on Atari ST computers in 1986 and then to C on Atari TT030 computers soon after. The original C program and Atari TT030 computers are still very much alive and in use to this day! In 2004, Brad started using Linux on Tecnopolis servers, and joined MUUG in 2006. He previously served on the board of the Atari ST Users Group (STUG) and became a board member of MUUG in 2011. He has been keeping our finances in order as your MUUG treasurer since 2013.

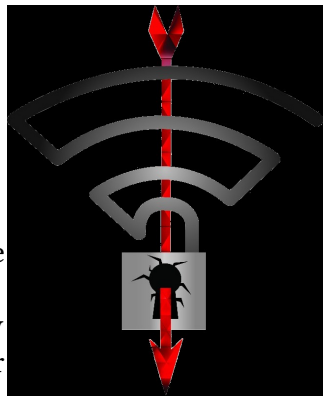
Wyatt Zacharias

Unix/Linux and Network Administrator - Manitoba Blue Cross

Wyatt Zacharias is a system administrator at Manitoba Blue Cross. He manages a mix of RedHat Linux and HP-UX servers, as well as Cisco routing and switching gear and enterprise firewall appliances. Wyatt has been president of MUUG for the previous three years, and served as vice-president the year before that. Wyatt graduated from Red-River college in 2014, and is a RedHat certified engineer.



KRACK Attack!



Serious flaw in WPA2 protocol lets attackers intercept passwords and much more.
Researchers have discovered a key flaw in the WPA2 WiFi encryption protocol that could allow hackers to intercept your credit card numbers, passwords, photos and other sensitive information. The flaws, dubbed "Key Reinstallation Attacks," or "Krack Attacks," are in the WiFi standard and not specific products. That means that just about every router, smartphone and PC out there could be impacted, though attacks against Linux and Android 6.0 or greater devices may be "particularly devastating," according to KU Leuven University's Mathy Vanhoef and Frank Piessens, who found the flaw.

Here's how it works. Attackers find a vulnerable WPA2 network, then make a carbon copy of it and impersonate the MAC address, then change the WiFi channel. This new, fake network acts as a "man in the middle," so when a device attempts to connect to the original network, it can be forced to bypass it and connect to the rogue one. Normally, WPA2 encryption requires a unique key to encrypt each block of plain text. However, the hack described in the Krack Attack paper forces certain implementations of WPA2 to reuse the same key combination multiple times.
The problem is made worse by Android and Linux, which, thanks to a bug in the WPA2 standard, don't force the client to demand a unique encryption key each time. Rather, they allow a key to be cleared and replaced by an "all-zero encryption key," foiling a key part of the handshake process. In some cases, a script can also force a connection to bypass HTTPS, exposing usernames, passwords and other critical data.

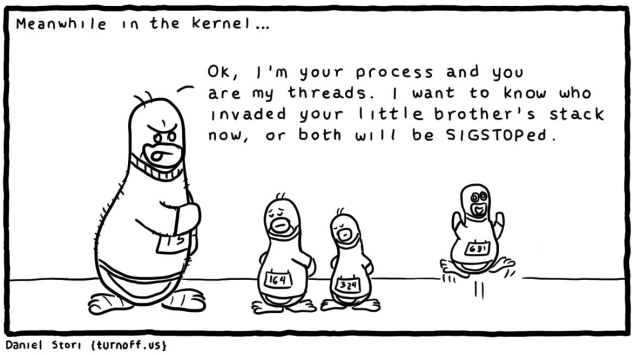
The system takes advantage of a flaw in the "handshake" method to direct users to the malicious network. Neither WiFi passwords nor secret keys can be obtained, the researchers say, as the hack works by forging the entire network. As such, it can't be used to attack routers, but

hackers can still eavesdrop on traffic, making it particularly dangerous for corporations.
After earlier, more limited hacks, the WPA2 protocol has been suspect for a while, so many security folks were already bracing themselves for something bad. If you still doubt the seriousness of it, Alex Hudson, for one, is actually advising Android users to "turn off WiFi on these devices until fixes are applied." He adds that "you can think of this a little bit like your firewall being defeated."

As such, you can protect yourself to a great extent by sticking with sites that have solid, proven HTTPS security. And of course, the attack won't work unless the attacker is nearby and can physically access your network.

The problem should be relatively easy to fix. A firmware change can force routers to require a dedicated certificate for each handshake, instead of relying on the one already generated. And, as the security researchers who discovered it say, "implementations can be patched in a backwards-compatible manner."

That means if you patch your Android device and not your router, you can still communicate and be safe, and vice-versa. Nevertheless, they also advise to patch all your devices as soon as security updates are available.



Creative Commons License

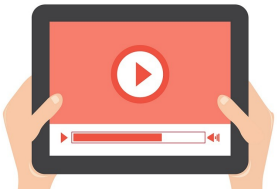
MUUG has gone social!

Twitter:
twitter.com/manitobaunix

Facebook:
facebook.com/ManitobaUnix

MeetUp:
meetup.com/Manitoba-UNIX-User-Group

Watch MUUG Online



Missed a meeting, or want to follow along with a demo at home? Video recordings of the Daemon-Dash 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

User Group Discounts

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/