

# MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 26 No. 10, June 2014

Editor: K. McGregor/W. Zacharias

## Next Meeting: June 10th, 2014

### RTFM and presentation:

This month, Trevor Cordes will be demonstrating how to screen scrape web pages and programatically control Firefox with Perl. We'll tackle the scraping of even complicated, anti-scrape websites that require JavaScript logins. Now no site is unscrapable!

Adam Thompson will be covering the netcat nc(1) utility for the RTFM section this time.

## Where to Find the Meeting

1L12 Lockhart Hall, University of Winnipeg

University of Winnipeg Lockhart Hall (marked "L" on the map), on the south-east corner of Spence and Ellice. Parking is available on the surrounding streets. Meetings are normally in room 1L08, but occasionally are relocated to nearby rooms. If there is a change, it should be conveyed via a sign on the door to 1L08.



## Goodbye TrueCrypt

The anonymous developers responsible for building and maintaining the free whole-disk encryption suite TrueCrypt apparently threw in the towel this week, shuttering the TrueCrypt site and warning users that the product is no longer secure now that Microsoft has ended support for Windows XP.

Sometime around May 14, truecrypt.org began forwarding visitors to the program's home page on sourceforge.net. That page includes instructions for helping Windows users transition drives protected by TrueCrypt over to BitLocker, the proprietary disk encryption program that ships with some Windows versions (Ultimate/Enterprise) since Vista. The page also includes this ominous warning:

“WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues”

“This page exists only to help migrate existing data encrypted by TrueCrypt.”

“The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.”

Doubters soon questioned whether the redirect was a hoax or the result of the TrueCrypt site being hacked. But a cursory review of the site's historic hosting, WHOIS and DNS records shows no substantive changes recently.

What's more, the last version of TrueCrypt uploaded to the site on May 27 shows that the key used to sign the executable installer file is the same one that was used to sign the program back in January 2014. Taken together,

these two facts suggest that the message is legitimate, and that TrueCrypt is officially being retired.

## Popularity Contest

How popular are the various web servers? Nginx just tied Apache (at 39.2%) for sites in the top 10,000, and is now ahead of Apache for the top 1,000 (38.8% to 33.7%)!

<http://tinyurl.com/72rl5jy>

## You Can Be a Kernel Hacker

Kernel programming is often seen as a black magic. In Arthur C Clarke's sense, it probably is. The Linux kernel is quite different from its user space: many abstractions are waived, and you have to take extra care, as a bug in your code affects the whole system. There is no easy way to do floating-point maths, the stack is fixed and small, and the code you write is always asynchronous so you need to think about the concurrency. Despite all of this though, the Linux kernel is just a very large and complex C program that is open for everyone to read, learn and improve, and you too can be a part of it.

Check out the tutorial at Linux Voice:

<http://www.linuxvoice.com/be-a-kernel-hacker/>

## Updates for Windows XP

A simple registry change is all that's needed to continue to get security updates for Windows XP until 2019. The change makes Windows XP appear to be Windows Embedded POSReady 2009 to Windows Update, which will be eligible for these updates until April 9, 2019.

A Microsoft spokesperson said "We recently became aware of a hack that purportedly aims to provide security updates to Windows XP customers. The security updates that could be installed are intended for Windows Embedded and Windows Server 2003 customers and do not fully protect Windows XP customers. Windows XP customers also run a significant risk of functionality issues with their machines if they install these updates, as they are not tested against Windows XP. The best way for Windows XP customers to protect their systems is to upgrade to a more modern operating system, like" FreeBSD or Linux.

<http://tinyurl.com/kurchqu>

## Raspberry Pi Compute Module

Raspberry Pi Director of Hardware James Adams announced:

"The compute module contains the guts of a Raspberry Pi (the BCM2835 processor and 512Mbyte of RAM) as well as a 4Gbyte eMMC Flash device (which is the equivalent of the SD card in the Pi). This is all integrated on to a small 67.6x30mm board which fits into a standard DDR2 SODIMM connector (the same type of connector as used for laptop memory [*physically, not electrically – Ed.*]). The Flash memory is connected directly to the processor on the board, but the remaining processor interfaces are available to the user via the connector pins. You get the full flexibility of the BCM2835 SoC (which means that many more GPIOs and interfaces are available as compared to the Raspberry Pi), and designing the module into a custom system should be relatively straightforward as we've put all the tricky bits onto the module itself.

So what you are seeing here is a Raspberry Pi shrunk down to fit on a SODIMM with onboard memory, whose connectors you can customise for your own needs.

The Compute Module is primarily designed for those who are going to create their own PCB."

<http://tinyurl.com/q4qyp46>

## Laser Internet to the Moon

A joint project involving NASA and MIT researchers had demonstrated technology last year that could supply a lunar colony with broadband via lasers ("faster Internet access than many U.S. homes get") and has already demonstrated its worth in communications with spacecraft.

From ComputerWorld's article: "The Lunar Laser Communication Demonstration (LLCD) kicked off last September with the launch of NASA's LADEE (Lunar Atmosphere and Dust Environment Explorer), a research satellite [formerly] orbiting the moon. NASA built a laser communications module into LADEE for use in the high-speed wireless experiment. LLCD has already proved itself, transmitting data from LADEE to Earth at 622 Mbps (bits per second) and in the other direction at 19.44 Mbps, according to MIT. It beat the fastest-ever radio communication to the moon by a factor of 4,800."

Communicating at such distances means overcoming various challenges; one of the biggest is the variability

in Earth's atmosphere. The LLCD didn't try to power through the atmosphere at only one spot, therefore, but used four separate beams in the New Mexico desert, each aimed "through a different column of air, where the light-bending effects of the atmosphere are slightly different. That increased the chance that at least one of the beams would reach the receiver on the LADEE.

Test results [were] promising, according to MIT, with the 384,633-kilometer optical link providing error-free performance in both darkness and bright sunlight, through partly transparent thin clouds, and through atmospheric turbulence that affected signal power." At the CLEO: 2014 conference in June, researchers will provide a comprehensive explanation of how it worked.

<http://m.slashdot.org/story/202495>

## OpenSSL Beyond Repair

OpenBSD founder Theo de Raadt has created a fork of OpenSSL, the widely used open source cryptographic software library that contained the notorious Heartbleed security vulnerability.

OpenSSL has suffered from a lack of funding and code contributions despite being used in websites and products by many of the world's biggest and richest corporations.

The decision to fork OpenSSL is bound to be controversial given that OpenSSL powers hundreds of thousands of Web servers. When asked why he wanted to start over instead of helping to make OpenSSL better, de Raadt said the existing code is too much of a mess.

"Our group removed half of the OpenSSL source tree in a week. It was discarded leftovers," de Raadt told Ars in an e-mail. "The Open Source model depends [on] people being able to read the code. It depends on clarity. That is not a clear code base, because their community does not appear to care about clarity. Obviously, when such cruft builds up, there is a cultural gap. I did not make this decision... in our larger development group, it made itself."

The LibreSSL code base is on [OpenBSD.org](http://OpenBSD.org), and the project is supported financially by the OpenBSD Foundation and OpenBSD Project. LibreSSL has a bare bones website that is intentionally unappealing.

"This page scientifically designed to annoy web hipsters," the site says. "Donate now to stop the Comic

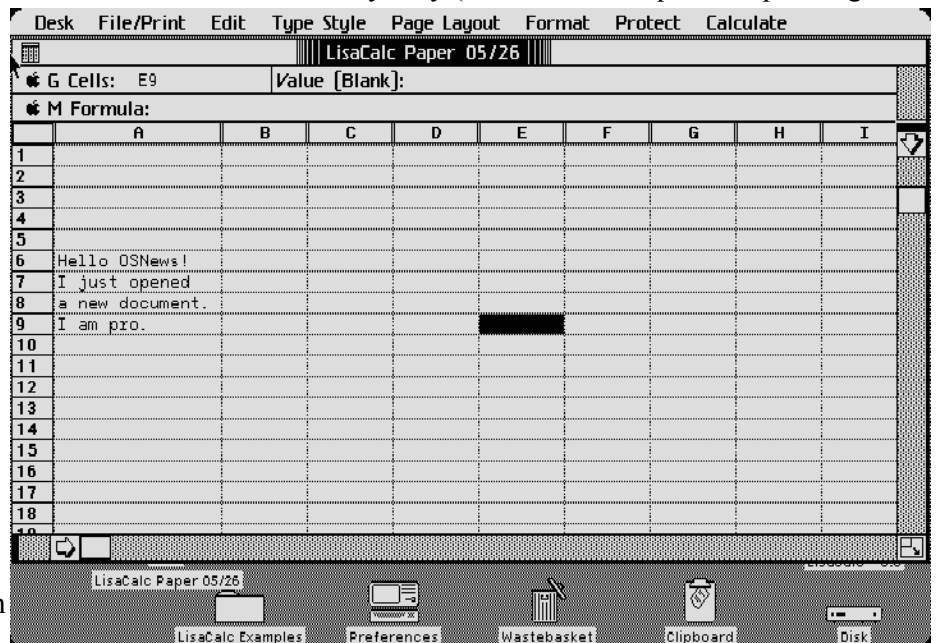
Sans and Blink Tags." In explaining the decision to fork, the site links to a YouTube video of a cover of the Twisted Sister song "We're not gonna take it."

<http://tinyurl.com/l8sj8lp>

## Apple Lisa

Thom Holwerda at OSNews writes: "I'm more or less assuming all of us are familiar with the Apple Lisa, Apple's and Steve Jobs' first attempt at turning Xerox PARC's work into a marketable product. It was a flop, but many of its ideas carried over onto the Macintosh, and in fact, Macintosh development took place on the Lisa.

Due to the fact few Lisas were sold, it's hard to get your hands on a working model, meaning most of us will never get the opportunity to actually use one. Luckily, there's a very advanced Lisa emulator available, written by Ray Arachelian. It's open source (GPL) and available for Windows, Linux, and Mac OS X. Setting it up is remarkably easy (there are non-hqx Lisa operating



system files too), but do note that technically, you need to own a Lisa yourself in order to use the ROMs. But, of course you do.

The Lisa user interface takes a bit of time to get used to, as its terminology is a bit alien, and some things feel quite a bit arbitrary from our modern, harmonised perspective. For instance, it took me a while to figure out how to open a new file in the Lisa office applications; it turns out that you need to double-click a special kind of icon ('stationary'), which the Lisa calls 'tear off stationary', which creates what to me looks like a copy of said stationary icon. This icon is the actual new file; double-click it to open it.

I'm having quite some fun poking around the Lisa, and the emulator has been holding up perfectly - no crashes, and it's remarkably easy to use. I would definitely advise giving this a go if you have some spare time."

<http://tinyurl.com/kv9hob2>

## BSDCan 2014 Videos Online

The fine folks at BSDNow (<http://www.bsdnow.tv>) have made the videos of the presentations at this May's BSDCan available.

BSDCan, a BSD conference held in Ottawa, Canada, is a technical conference for people working on and with 4.BSD-based operating systems and related projects. The organizers have found a fantastic formula that appeals to a wide range of people from extreme novices to advanced developers.

<http://tinyurl.com/ozpw4ml>

## Chrome Extensions Blocked

As Google announced late last year, the company is making things difficult for Chrome Extensions installed outside of the Chrome Web Store. Any Chrome extension installed directly from a website or as part of a program install will be remotely disabled.

Google is looking to crack down on malicious extensions, which have increasingly become the preferred attack vector against Chrome users. While installing a program, it's easy for developers to include an unwanted Chrome extension that injects ads into web pages or hijacks search queries.

Google is trying to put a stop to malicious extensions without hurting legitimate local extension use cases. Local installs can still be performed by enabling "Developer mode" from the extensions screen, and installs via Enterprise policy are still supported. Websites or programs that want to include a Chrome extension can use the inline installation feature, which pops up a box from the Chrome Web Store asking users if they want to install the extension. Now Google just needs to do a better job of policing its extension store and, in theory, malicious extensions should be reduced.

Strangely, this change is only happening on Windows. Users on other operating systems will still be able to install local extensions without having to click the developer checkbox. Apparently program installs for those OSes can be trusted.

## Linux Sucks

Watch the video of the 5<sup>th</sup> (or so) annual talk on the subject by Bryan Lunduke at the 2014 LinuxFest Northwest and see if you agree!

<https://www.youtube.com/watch?v=5pOxlazS3zs>

## China Looks to Linux (Again)

China may look at the open source Linux as a replacement for Windows, following an official ban on Microsoft's Windows 8 for government procured computers.

Chinese Government news agency Xinhua published an article claiming Chinese vendors are using a ban on Windows 8 to push Linux-based OS variants.

According to the reports, Chinese developers may receive "preferential policy" treatment and official support for developing Linux-based operating systems.

The Linux distributions and other locally developed programs often "are created in accordance with Chinese people's habits" and as such "beat foreign rivals", the official news agency recorded.

An earlier effort by Chinese developers to create a Linux-based operating system floundered. The Red Flag distribution closed down this year after the Chinese Academy of Sciences withdrew funding for the project, citing general mismanagement and an inability to complete specific projects.

China's software industry counts several successes however, including Tencent's popular messaging program QQ and the Baidu search engine, both used by millions of people.

Ironically enough, Microsoft's heightened security stance may be one reason the Chinese government slammed the door shut on Windows 8.

Ni Guangnan, an academic with the Chinese Academy of Sciences, was quoted in the Chinese news reports criticising the built-in malware and security defences in Windows 8. Windows Defender and SmartScreen for Internet Explorer put users at risk of being monitored and endangering national security, he claimed, especially if run on government computers.