1 heartbleed: Why and How to use the LibreSSL program

Heartbleed is a serious omission in the `openssl` program that left a buffer overflow exploitable, exposing passwords and encryption keys and so on from 2014 to 2017.

Because it is open source, everyone assumed that someone else had checked it ... but no-one had.

Eric Raymond in his book "The Cathedral and the Bazaar" enthusiastically proposed that 'Open Source' is superior because 'given enough eyeballs, all bugs are shallow' ... Oh, well, so much for that!

The LibreSSL people forked it and cleaned up the code massively, and you can download and compile and link and run it instead of `openssl`. Few distros have binary packages for it, instructions may be found at `libressl.org` or `libressl.org/releases.html` and `penzin.net/libressl.html`.

2 serendipity: Get the Huawei E8372 LTE Wingle to work

This device appeared at our 'Linux Learners Lounge' recently. I stuck it into a Samsung notebook on which we had just installed Mint 18.3 ... and waited ... but could not detect evidence that it was working.

Why not? Because I'm so old fashioned – I have not dealt with these creatures since the Optus E160/E1762 USB dongle. In those days they were detected after being plugged in to the USB port; devices created; their mode switched; configured as a serial modem, run by the point-to-point daemon; and the `ppp0` interface created to manage connections. Nothing at all like that happened with this one. Complete silence, from my point of view. No `mobile-broadband` entry in the network manager, either.

I was quite stuck for inspiration.

Trusting Knoppix to deal with most hardware, I booted Knoppix 8.1 on a Lenovo laptop, and stuck in the dongle. It was seen by `dmesg`. But the really weird thing was that the interface `eth0` was created, even though this laptop has no ethernet NIC.

Did this come from the dongle? An IP address was handed out, too, at 192.168.1.100, and `ping` saw `linuxlsga.net`, and browsing worked! `/sbin/route -n` showed `eth0` as the only way out. So which program was handling the connection? `ps ax` returned `dhclient`. All so odd to me.

OK. Try one more computer ... Devuan 2.0 on a Macbook with `eth0` and `wlan0` NICs.

Boot; insert; `eth1` created. But this time I had `wicd` in control, not `network-manager`. And there, amongst the other wireless-access points, was one I had not seen before at home, but that had been present at the Lounge, named like TWD4GABC. I clicked `connect` and it said: `This needs a WPA2 encryption key`.

`RTFM`. Onto another computer, download the manual, which explained that a `wingle` is a `dongle` with the added ability to be connected by wifi. It suggested pulling off the cover of the dongle, which revealed ... the SSID (like TWD4GABC) and the WPA2 key (like 98543322).

So I typed in the key, clicked `connect`, and it associated, authenticated, got an IP address (192.168.1.100), this time creating the interface `wlan0` instead. And now `ps ax` showed that `wpa_supplicant` was running the session. Aha! It all worked perfectly! And at last I understood that the old method of treating it like a dial-up modem has now been replaced by the new method of treating it as a wireless access point. Both have their logic, but a 'wingle' ain't a 'dongle'. Old habits die hard, but I am now one happy chappy again!

3 /etc/hosts: Reduce the Overhead of fetching Trackers

Instead of installing an add-on to each browser, make use of the Linux system searching for the IP address of a website, first in its `/etc/hosts` file, and then out on the web in a domain name server. If it is found locally as `IP=0.0.0.0` then nothing is further fetched, speeding up sites that access myriad trackers. You can download a list of over 14,000 popular trackers in the file `winhelp2002.mvps.org/hosts.zip`, unzip it and tack the resulting HOSTS file on the end of your `/etc/hosts` file. For example, to stop the site `csh.actiondesk.com` being accessed during your html loading, add the line `0.0.0.0 csh.actiondesk.com` to the end of `/etc/hosts`. Go to `linux-magazine.com/Online/Blogs/Productivity-Sauce/` and do a search for the folder `Block Ads and Malware Sites with a Unified Host File`. Works for all browsers.