

Security Leftovers

By *Roy Schestowitz*

Created *13/08/2015 - 8:56pm*

Submitted by Roy Schestowitz on Thursday 13th of August 2015 08:56:09 PM Filed under [Security](#) [1]

- [Linux Concerns: Convenience vs. Security](#) [2]

Once upon a recent time, Linux was more secure than it is today. Only the root user could mount external device, and in many distributions new users were automatically assigned a few groups that limited the hardware they could access. Distributions followed the principle of least privilege (aka least access), under which users, applications, and devices receive only the access to the system that they absolutely require.

- [Security updates for Thursday](#) [3]

- [One Definition Of Lock-in: Running ?2003? So Many Years Later](#) [4]

Why do they do it? Run ?2003? in 2015! It?s not cost, because Debian GNU/Linux would cost \$0. It?s lock-in whether by habit or by application. Lots of folks have invested heavily in applications that still work so they are willing to risk everything, perhaps by adding other layers of security. Why?

- [Imploding Barrels and Other Highlights From Hackfest DefCon](#) [5]

Visiting Las Vegas can feel a bit like being a metal sphere in a pinball machine?you?re tossed from bright lights to blaring shows and back again until you eventually (hopefully) emerge out

a hole at your home airport. When you visit Vegas with a swarm of hackers and security researchers, the dizziness gets amped up tenfold and can be laced with a dose of dark mischief.

- [Cisco networking gear can be hijacked, warns company](#) [6]

An attacker can swap out the device's firmware with altered, malicious software.

- [Video Shows a Terrifying Drug Infusion Pump Hack in Action](#) [7]

It's one thing to talk about security vulnerabilities in a product, but another to provide a proof-of-concept demonstration showing the device being hacked.

That's what occurred last month when BlackBerry Chief Security Officer David Kleidermacher and security professional Graham Murphy showed how easy it is for hackers to take control of a hospital drug infusion pump by overwriting the device's firmware with malicious software.

- [August 15 security fixes for Adobe Flash](#) [8]

...Adobe released updated Flash player plugins which address many new vulnerabilities (as usual).

[Security](#)

Source URL: <http://www.tuxmachines.org/node/78984>

Links:

- [1] <http://www.tuxmachines.org/taxonomy/term/59>
- [2] <http://www.datamation.com/feature/linux-concerns-convenience-vs.-security.html>
- [3] <http://lwn.net/Articles/654409/rss>
- [4] <http://mropogson.com/2015/08/13/one-definition-of-lock-in-running-2003-so-many-years-later/>
- [5] <http://www.wired.com/2015/08/highlights-from-defcon-2015/>
- [6] <http://www.zdnet.com/article/cisco-networking-gear-can-be-hijacked-warns-company/>
- [7] <http://www.wired.com/2015/08/video-shows-terrifying-drug-infusion-pump-hack-action/>
- [8] <http://www.alpinelinux.org/posts/Alpine-3.2.3-released.html>