Sysadministrivia

Linux, Lagers, and Late Nights

S0E8: "Something Old, Something New, Something Broken, Something Due"

Posted 2015-06-01 06:31
Modified 2017-05-09 13:05
Comments 0

Navigation

Previous Episode	Next Episode
S0E7: "The Isolation Chamber (pt. 1)"	S0E9: "Two Dicks and Two Virgins"

Log

Recorded (UTC)	Aired (UTC)	Editor
2015-05-22 03:01:15	2015-06-01 06:31:32	brent s.

Verification

Format	SHA256	GPG	Audio File
MP3	2f088727adce0dc83e42edbde42f3b07c7ddcc4a401e73535edd73f94838ffa4	click	click
OGG	265a19a2d4aa559555f131381633d091e0854556cbb3f70377015508250e03da	click	click

Quicklisten:

We talk about Logjam (and other security weaknesses), chat protocols/clients, filesystems, F/OSS licenses, and systemd.

- Notes
- Errata
- Music

Notes

- Jthan is drinking Miller Lite, whereas I am having a PBR.
  - I also mention Milwaukee's Best, or "the Beast" as my ex-frat cousin calls it. Bleugh.
- The Admin Admin Podcast is here. They mention us in Episode 020, around 52m37s in. Unfortunately they pronounce the name wrong, but I definitely blame myself for that- not many people know it's supposed to be a portmanteau! (And it definitely looks like "Sysadmin is trivia". We mostly rant about trivial bullshit at the end of the day anyways.)
  - They have a much higher Windows focus than we do, so you multi-platform admins/Microsoft shop admins might want to give them a shot!
- Logjam's site can be found here. There will be a banner at the top saying if your browser is vulnerable or not (most still are).
  - It is CVE-2015-4000.
  - Super handy is the guide for closing the hole they provide here. You can test your webserver right on that page (I closed the hole already for sysadministrivia.com, so feel free to test with our site against your own). It includes directives for securing Apache's httpd (via mod_ssl), Nginx (pronounced "Engine-X", what I use to host our site), Microsoft IIS, Lighttpd (pronounced "Lighty"), Apache's Tomcat (Apache's Java application server), Postfix (SMTP/MTA server), Sendmail (SMTP/MTA server), Dovecot (POP/IMAP/LDA/MDA server], HAproxy (high-availability TCP load-balancer/failover proxy), and OpenSSH (ubiquitous SSH daemon).
  - The venerable Bruce Schneier, the Chuck Norris of digital security, has written a blog post about it
  - Despite no response to my tweet to @OpenVPN, it would seem that it is not vulnerable
  - ...but Java 6 is. Sorry, Java 6 devs; Java 6 only supports <1024 DH keysize.
- You can find the SSH hardening guide here. Our mirror is here.
- There is a version of PuTTY that has a trojan. **The current safe version is 0.64**. The SHA256 of putty-0.64-installer.exe is 3ddf21ed30a4f8264b9df0742fa62eaf0892eb0e7e803ac6cbdcb5b7cc3b542a. Be wary, Windows users.
  - As a reminder, we offer SHA256 sums and GPG signatures of all our episodes.
- We like irssi for IRC. We also mention bitchX and weechat (but don't like them as much).
  - And I use Pidgin a lot.
    - Sometimes it chokes on certain XMPP commands (like registering for presence on ejabberd)... for those, I use Psi.
  - We also mention bitlbee
  - MS Comic Chat, lel.
  - We <3 XMPP (also check out the org-side, Jabber).
    - You can view various XEPs (RFC's for XMPP, basically) here.
  - We also mention eJabberd (and love it) and Openfire (and don't). There are lots though.

    - And we mention Xabber.

- The Phoronix article for the 4.0.x + ext4 + mdraid0 corruption bug is here.
    - The cause has since been found…
    - And the fix mainlined into the stable kernel tree.
    - For some grisly details, this might provide some accurate information.

- For the differences between EXT2-EXT3-EXT4, check out this.
    - FAT, NTFS…
    - HFS and HFS+…
    - FFS (also called UFS).
    - JFFS and JFFS2…
    - Reiser and Reiser4
        - Seriously, though. Hans Reiser's eyes pierce your very soul. Also, one creepy motherfucker.
    - And XFS is still super popular…
    - Jthan has a hard-on for ZFS. FreeBSD supports it, but not as well as Solaris (and variants such as illumos)
        - But again. FreeBSD's implementation isn't as good as Solaris', and Solaris still sucks. Slow piece of shit.
    - We talk about Btrfs (Wikipedia article here)…
        - And the Arch Wiki article on it)
    - But you may want to just read this list of different types of filesystems
    - Or perhaps just the more technological comparison.
    - I also mention TRIM. If you use SSD in GNU/Linux, this is required reading.

- Open Source Initiative (OSI) and Free Software Foundation (FSF)
    - FSF has much more strict guidelines than OSI's requirements, which (of course) RMS criticizes heavily and often.
    - We mention the BSD2 and BSD3. Which (of course) RMS criticizes. Again. But supposedly the BSD3 is compatible with the GPL (and considered "Free" according to FSF).
    - Notable software that uses the Apache license besides httpd is serf, spamassassin, subversion
    - GPL v2.0, GPL v3.0
    - MIT license
    - CC 0-1.0, the "Creative Commons Public Domain" license
    - MPL 2.0
    - CDDL
    - The OSI has a list of licenses, and the FSF does as well.

- The episode I reference in which we interview Lyz (Krumbach) Joseph is S0E4.
    - The Debian fork we mention that's trying to strip out systemd is Devuan. Hell, there's a whole wiki for the haters.
        - But seriously. This is just coldplug/hotplug/devfs vs. udev all over again, forever and ever. Over and over. Looking back, these people seem like batshit silly, curmudgeonly luddites, don't they? Because hindsight is 20/20, and we realized that hey, once everybody got over it and udev stabilized, it was actually pretty dang useful. Same goes (potentially) for systemd. systemd haters seem just like those udev haters from yore to me, and yet udev was one of the most powerful and useful mechanisms to hit the GNU/Linux world, in **every** arena- embedded, server, desktop, every implementation of GNU/Linux.
            - But if you want to prove a point, go ahead and do an install and strip out udev, switch to devfs/coldplug/hotplug. I'll wait. Let me know how fast you get frustrated.
    - The PCWorld article Jthan references is here.
    - And this comment thread (for a totally irrelevant topic, it should be noted, because the anti-systemd trolls are loud).
    - And the bug I mention? It's a half-bug, of sorts.
        - Like I said, I have a **batshit crazy** partitioning/mounting scheme. i take the fall for this, partially.
    - Unix broke "The Unix Philosophy" ALL the DANG TIME. Enough to inspire multiple people to even write a book about it.
    - When captives/hostages fall in love with their captors, it's called Stockholm syndrome.
    - Upstart is all but dead for the same reasons that non-systemd forks will die- lack of momentum and lack of developer base.
    - If this segment left a bad taste in your mouth, I sincerely encourage you to read this. It admits when myths are true, when they're false, and to what extent.

Errata

- Logjam does indeed open up the possibility of MitM attacks
- MSN Messenger/Windows Live Messenger fully shut down last year, and is superseded by Skype (since Microsoft's acquisition of it).
    - Jthan, you ignorant slut, iChat **is** a client. Not a protocol. It was replaced by Messages, which supports the *protocols* of iMessage and FaceTime.
    - And now I'm the ignorant slut, it's **Open** Whisper Systems. Their mobile app is called **TextSecure Private Messenger** (on Android) and Signal – Private Messenger (on iOS).
    - WiKID is, indeed, a 2FA system.
        - Not to be confused with Wicked.
    - Xabber does, indeed, support OTR.
- I think the default openBSD filesystem is now UFS2…
    - UFS2. Not FFS+. Whoops.
- The CDDL is **definitely** not the "proper public domain license". It seems that's the MIT.
- I goofed; I implied the PCWorld systemd article's title didn't seem subjective. I meant it didn't seem **objective**.
    - I was right with my gut instinct, his name is Lennart Poettering.
    - General consensus is that RMS did, indeed, coin the word POSIX.
    - Per the above-referenced systemd myths link (0pointer.de/blog/projects/the-biggest-myths), systemd is **not** backed by other freedesktop.org developers- they're just HOSTED there.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Hyperfun	Kevin MacLeod	click	CC-BY 3.0

Outro	Vivacity	Kevin MacLeod	click	CC-BY 3.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories (Pilot Season)

Comments

There are currently no comments on this article.