Sysadministrivia

Linux, Lagers, and Late Nights

S3E7: "Dude, Where's My Cert?"

Posted 2018-06-04 03:59
Modified 2018-06-04 02:55
Comments 0

Navigation

Previous Episode	Next Episode
S3E6: "The Hubris of Man"	S3E8: "When You Have to Swing Both Ways"

Log

Recorded (UTC)	Aired (UTC)	Editor
2018-05-23 02:33:16	2018-06-02 17:02:43	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`031e1b5799790a0fe56ece277c78df5ec4aad5ad349b6e9f2f7e40d7cec67e73`	click	click
OGG	`d83e73c2fe0c9138d0cd0afd7ff70f19272711cbd56a0309fcd4f27b4e21be0d`	click	click

Quicklisten:

In this episode, we talk about the shortcomings of ZFS on Linux and briefly introduce you to the world of running your own private PKI.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- Rowhammer is back and “better” than ever via Throwhammer.
  - We talked about Rowhammer back in S1E14.
- Either all OS devs need to step their reading comprehension game up or Intel can’t write proper documentation.
  - Related CVE: CVE-2018-8897.
  - We talk about patching in the context of security in S2E18 and further in-depth in S2E19.
- From the “we already knew this” department, working from home boosts productivity.
  - Seriously, we’ve known this for a while.
- The Secure Data Act seeks to eliminate government-mandated backdoors…
  - **And** the 4th District ruled that warrantless/suspicionless searches of electronic devices at the border are unconstitutional!
- The US Senate voted to overturn the recent FCC changes with regards to Net Neutrality.
- The Signal desktop application had an RCE.
  - Can we stop pretending Javascript is a viable language for applications now?
- There have been suspicious covert surveillance devices all around DC, MD, and VA (though this shouldn’t surprise anyone).

Notes

Starts at **29m47s**.

I was drinking Jefferson’s Reserve bourbon. Paden was drinking Stella. Jthan was drinking FATE Brewing Company’s Laimas Watermelon Kölsch Style Ale (mixed with vodka for “maximum enjoyment”).

- ZFS on Linux
  - ZFS sucks for multi-platform infrastructure.

- Running your own PKI **(45m17s)**
  - You can’t use your own PKI for e.g. a website unless you manually import and trust the CA certificate you generate into the browser’s trust store.
  - “Trusted” CAs usually bundle with pre-configured trust in various browsers, though.
  - Juniper has a better explanation of the process with some pretty good diagrams when it comes to client certificate management.
  - There are several engines supporting SSL/TLS; most commonly these are OpenSSL, GnuTLS, and LibreSSL.
  - There are several handy ways of interacting with these backend engines.
    - OpenSSL has a commandline utility

    - There’s easy-rsa (which is essentially just a wrapper around the OpenSSL CLI)
    - PyOpenSSL is **extremely** handy for programmatically managing a PKI.
    - The GUI (which is cross-platform) I was trying to remember is XCA.
- There’s a couple tutorials for using the OpenSSL CLI. Here’s one. Here’s another.
- While the use-case may be limited, setting up your own PKI gives you a deeper understanding into what goes on “under-the-hood”.
- Also worth checking out is the ACME protocol.
    - And of course, Let’s Encrypt is entirely open source (boulder is the server-side ACME component).

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(57m23s)**

Havoc was wrought when it was discovered that plaintext passwords were leaking from a teen monitoring app.

Errata

- The echo didn’t show up on the recording — but Jthan and I narrowed it down. It was Paden, and it only exhibited over Mumble. Thank goodness it didn’t show up in the recording!

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Glitterhater	Computer Music All-stars	click	CC-BY 4.0
Outro	Humming for you	Ema Grace	click	CC-BY 4.0

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

Author r00t^2
Categories Season Three

Comments

There are currently no comments on this article.
