Sysadministrivia

Linux, Lagers, and Late Nights

S5E3: "Certifiably Insane"

Posted 2020-03-29 23:59
Modified 2020-03-29 18:33
Comments 0

Navigation

Previous Episode	Next Episode
S5E2: "I Am the Keymaster; Are You the Gatekeeper?"	S5E4: "You Had Better Watch Yourself"

Log

Recorded (UTC)	Aired (UTC)	Editor
2020-03-19 02:20:55	2020-03-29 21:08:41	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`ccee13c99f51adeb8aa62ea1fb390956799c1eab793b36db4c83e9ca858aba0c`	click	click
OGG	`7214b7212ed8d023578686cdf9cf7c8bf428847723e7422e7bcf5d711efdd000`	click	click

Quicklisten:

We talk about CRLs, OCSP, and OCSP stapling.

- Just the Tip
- Notes
- 15 Clams
- Errata
- Music

Just the Tip

- When working from home, it helps to follow your normal schedule/routine.
  - And make sure you wash your hands.

Notes

Starts at **21m52s**.

I was drinking a Jack and Coke. Paden was drinking water. Jthan was drinking Celestial Seasonings Peppermint.

- CRLs, OCSP, and OCSP stapling
  - Why?
    - Revocation of X.509 certificates.
      - A certificate should/will need to be revoked due to keys to certs may be compromised, organizational reasons, etc.
  - CRL (“Certificate Revocation List(s)”)
    - CRLs are essentially just a list of certificates that have been expired.
    - CRL is specified in RFC 3280 and RFC 5280.
  - OCSP
    - OCSP is certificate-specific; instead of requesting a list of revoked certificates, the client instead requests the status of a particular certificate.
    - OCSP is defined/clarified/revised in RFC 2560, RFC 4806, RFC 5019, and RFC 6960.
  - A key issue with both CRL and OCSP is client logic — what happens if the CRL or OCSP URL can’t be reached?
    - Either the client trusts the certificate anyways as valid, or
    - NONE of the certificates for that CA are trusted. This is more secure, but can cause a massive outage if a CA’s CRL/OCSP URL is inaccessible.
  - OCSP Stapling
    - Designed to overcome the availability requirement of CRL and OCSP.
    - A target server requests a signed timestamped validity status check from the CA for itself, and then “staples” that signed status to the certificate it serves.
    - You can find technical details in RFC 6066 § 8, RFC 6961, and the OCSP Stapling Required draft.
  - I haven’t written it yet, but at some point I’ll write an OCSP generator that interfaces with Vault and update this post (if I remember to). Vault already has an API endpoint for CRLs.
  - Firefox follows a specific revocation method. You can find a general overview of how browsers handle revocation here.

15 Clams

In this segment, Jthan shares with you a little slice of life. The title is a reference to this video. (2m16s in)

Starts at **38m24s**.

Jthan finally re-did his site. One of the blog posts he did was using Linode Object Storage with Borg.

But his **real** 15 Clams is about Folding@Home. He is folding for F@H in his work’s cluster for COVID-19.

I also mention SETI@Home.

Errata

- Paden is apparently having another baby in October…
  - Jthan didn’t know if his baby count was going “up or down”.
- We talk about toilet paper more than is interesting, probably. Sorry.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Nightmare	Javiis	click	CC-BY-NC-ND 4.0
Outro	Home	Cutside	click	CC-BY-NC-SA 4.0

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

Author r00t^2
Categories Season Five

Comments

There are currently no comments on this article.

Published with Textpattern CMS