Sysadministrivia

Linux, Lagers, and Late Nights

S5E13: "Who Watches the Hypervisors?"

Posted 2020-08-16 23:59
Modified 2020-08-16 13:55
Comments 0

Navigation

Previous Episode	Next Episode
S5E12: "Bad Developer! No Biscuit!"	S5E14: "Self-Projection"

Log

Recorded (UTC)	Aired (UTC)	Editor
2020-08-06 02:32:33	2020-08-16 00:13:42	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`e4883db8f7c54282b1da028580e305ff00b5d7f02c42d9ce373b307a5f4a19d8`	click	click
OGG	`5d34ca0bfa719322442208bafe33f60ca2f6a595052fe1c4a64ec96c69f6672f`	click	click

Quicklisten:

We talk about the issues present in trying to keep security, privacy, and integrity for data-at-rest on hardware that you don't own.

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

Just the Tip

- Paden wants to remind you to actually check to make sure your backups are working.

Notes

Starts at **14m31s**.

I was drinking water. Paden was drinking 2% milk. Jthan was drinking Corona.

- How can you guarantee privacy and integrity of a volume on e.g. a VPS provider?
  - You can't! Not perfectly, anyways.
  - If a malicious party has access to the hardware or hypervisor level, there are many opportunities for tampering or even outright breaking your expectations of disk encryption.
  - Hardware:
    - A lot of the issues present here are considered Evil Maid attacks.
    - You need plaintext **somewhere** in the booting process. (This applies to any full-disk encryption including VPS/VMs. Or, technically, any disk encryption.)
  - Hypervisors:
    - Access to the above **and more** – direct virtual console access, they control the kernel for paravirt, etc.
    - Hosts can also affect character devices (direct input flow, etc.)
  - You **can** check for integrity/tampering a little more reliably than **preventing** data leaking; Arch has a package in the AUR that serves as a good starting point.
    - Remote audit logs to a device only you/your org controls can help a lot as well.

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 **54m40s**.

Jthan talks about remotely unlocking a LUKS FDE.

Errata

- Paden was talking about this comic.
- Jthan, in his pursuit of glorifying The Cloud™ instead of a VM lab, doesn't understand why 640+MB > 512MB.
  - He also doesn't understand that following processes verbatim teach nothing.
  - He also doesn't know how to read. This says **530 MB RAM** as the minimum, not 512 MB. (Plus the inherent overhead you'd have with ZoL.)
  - Also speaking of, the August release of the Arch installation ISO is 671MB, not 640-something.
- Jthan says to not FDE your router, but you absolutely can. There's nothing stopping you from remotely unlocking your full-box router (see the link in 15 Clams).

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Boh	TNKS	click	CC-BY-NC-SA 4.0
Outro	Navidub	The Dubbstyle	click	CC-BY-ND 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