OpenSSL CONFERENCE

Self-Encrypting Disks in Linux

Fast, Expensive and Mostly Harmless

Milan Brož, mbroz@openssl.org

Milan Brož

mbroz@openssl.org

This talk is about Linux open-source disk encryption that uses the OpenSSL library.

Cryptsetup is (and will be) developed independently of the OpenSSL Corporation.

- *Cryptsetup and Linux Unified Key Setup (LUKS).*
- *Support Self-Encrypting disks (SEDs).*
- *Trusted Computing Group (TCG) Opal2.*
- *And who cares if it is done right...*

Scope

- Introducing Opal SED support to LUKS2.
- SED usability and security testing.
- Everything mentioned here is open-source.
- For technical details and used software see our papers at ArXiv:
  - **Linux disk encryption and self-encrypting drives**
    A case study on Opal2 drives security
    https://arxiv.org/abs/2607.11563
  - **XTS mode revisited: high hopes for key scopes?**
    https://arxiv.org/abs/2502.18631

Self-Encrypting Disks (SEDs)

OpenSSL CONFERENCE

- Sector-base encryption **in hardware.**
- Locking Ranges (LRs) ~ partitions.
- Trusted Computing Group (TCG) standards.
  - **Opal2 – media encryption**
  - Pyrite – authentication only.
- Only small subset of drives support Opal SED.
- Some open-source tools supports Opal, none supports all features.

Our research testbed and testsuite

OpenSSL CONFERENCE

- Collection of Opal (and Pyrite) devices.
- NVMe and SATA SSDs
  - ~ 40 Opal drives (and ~ 10 Pyrite)
  - we bricked some ☺
- Rotational disks are rare.
- Using Low-level commands.
- Linux Kernel API.
- Testsuite (using opal-toolset).

Findings #1 - TCG

- TCG standards are overengineered.
- Vendors implement bare minimum of features.
  - No connection encryption / no TLS in HW – thanks ☺
  - No password length extensions (limited to 32 characters).
  - Single User Mode extension issues.
- No usable acceptance tests.
- No reference implementation.
- Implementations are often “too creative”.

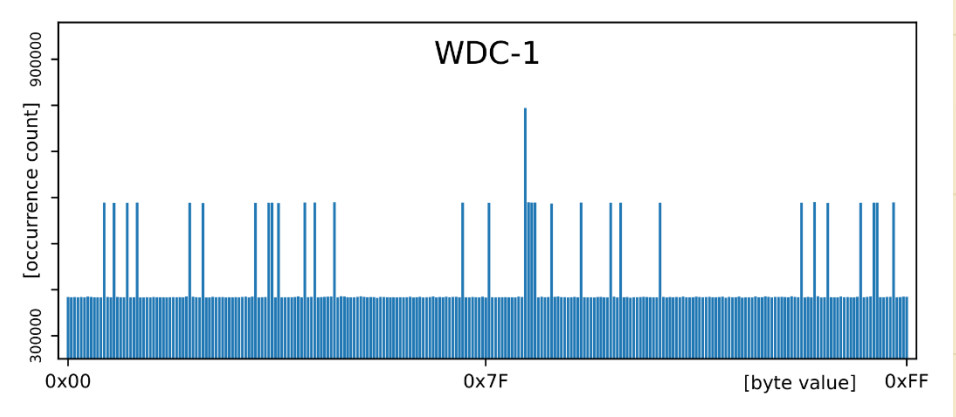
Findings #2 - cryptography

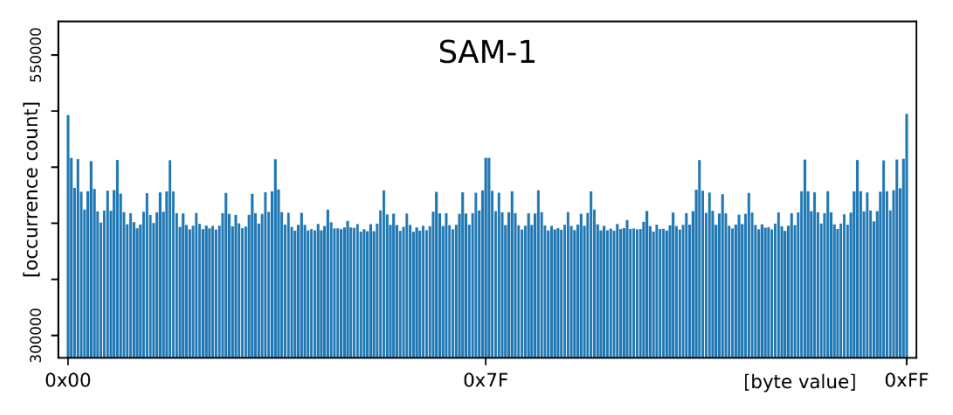
OpenSSL CONFERENCE

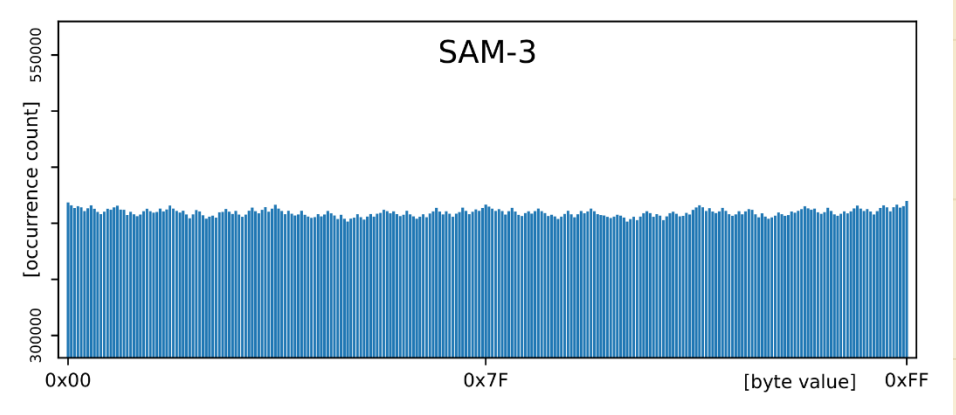
- We focused only what we need for LUKS2 integration.
- Black-box approach – run only test through API.
- No reverse engineering.
- Some examples (for details see paper)
  - Random Number Generators, Encryption modes, PSID (physical presence code to reset)
- Nothing super-serious, but it is 2026, right?
- And yes, we reported findings.
  Except one, there is either **no answer** or **no longer supported** answer.

RNG analysis

- We have access only to exported random() function.
- This is probably not used internally for media keys.
- Some returns fixed sequence (!)
- Byte histogram of some drives failing RNG tests.







Encryption modes

- Should be AES-XTS (except very old drives).
- How to check if implemented correctly?
  - For older drives - ciphertext patterns.
    Changing encryption key keep patterns in decrypted ciphertext.
  - New drives cannot be tested this way (it wipes data after key change).
    We would need to analyze flash chips.
- 5 drives form our testbed show patterns - implements AES-XTS incorrectly.

PSID – physical presence ID

- A (randomly generated) code to reset drive to manufacturing state.
- The only way to reset drive if you forget passwords.
- Usually 32-character code printed on label. (How to access this in a sealed notebook?)
- Nobody handles this as private information.
- Try image search for “NVMe PSID” ☺
- Not a big deal, except if attacker get access to device (remotely) and wipes your data…

Opal Single User Mode

OpenSSL CONFERENCE

- Opal Admin user can unlock all locking ranges.
  Note: This is intentional design decision.
- That bypasses our LUKS keyslots key derivation protections.
- TCG define Single User Mode (SUM) extension to avoid that.
  - Only few drives support it.
    20 of 38 in out testbed (see paper).
- A lot of bugs in firmware
  - We try to detect them and inform user to disable SUM in that case.

Cryptsetup LUKS2 SED support

OpenSSL CONFERENCE

- Request and code originally coming from community.
- Reworked it and supported Opal2 since version 2.7.
- Many Linux distros integrated it already in installers.
- **Single User Mode (SUM) is ready for 2.9 (November 2026).**
  - Should be used automagically if drive supports it.
  - Upgrade (not losing data) from non-SUM not implemented.
- We try to detect SUM issues, sometimes it requires PSID reset by user.

What's wrong here? Developers

- We want to test new hardware, but it is very expensive. (Thanks, AI.)
- Could vendors have some program for providing samples?
  (Some have, thanks to WDC!)
- Note: there is no emulator for Opal hardware.
  Brave students please contact me, nice master thesis ☺
- We will never support new TCG inventions like "Key per I/O".
  Seems hardware vendors do not implement it anyway.

What's wrong here? Academics

- Publish or perish (not improve and share).
- Often a missing connection between engineering and research.
- Such boring topic like storage encryption is not interesting for anyone. Right?
- Except it is used **everywhere.**
- PQC buzzword is nice, but we need new symmetric storage encryption modes.
- AES-XTS is becoming problematic.
- Happy to see some research (like double-decker mode).
- And we have students to working on it.

What's wrong here? Standards & certification

- We want our open-source code to be compliant with standards.
- Just it often does not make sense.
- Efforts from standardization bodies to retrospectively apply new requirements.
- Note: life-span of encrypted storage is decades, it is used for backups.
  These must remain accessible.
- Could standards use more keep-it-simple principle?
  Why we need features nobody implements in real-world hardware?

Conclusion

“Do not give up.”

Thanks for your attention!