But can it run coreboot?

Checking your AMD platform for Platform Secure Boot

whoami

- Michał Kopeć
- Firmware Engineer working primarily with coreboot and EDK2
- Have been at 3mdeb for 3 years now
- Free and open source software enthusiast

Agenda

- What do we need to be able to run coreboot?
- What is Platform Secure Boot?
- How do I check if I have it?
- Demo
- Future plans
- Discussion

Can x run coreboot?

Abridged checklist

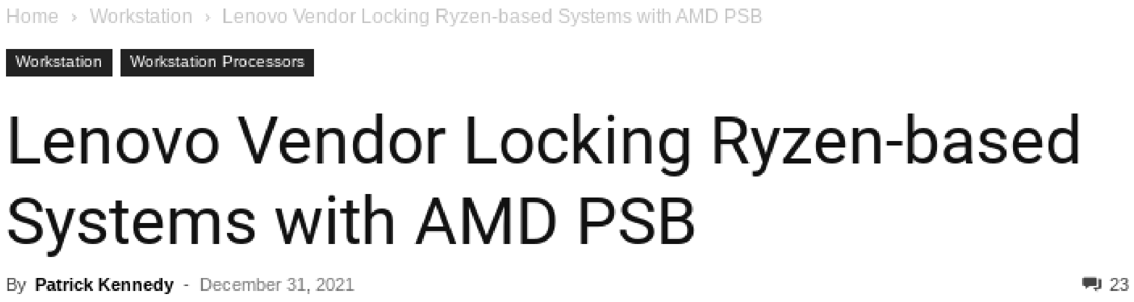
1. Is there existing code for the silicon in question?
   - check coreboot/src/soc directory
2. Does x have any hardware RoT fused to vendor’s keys?
   - On x86: Intel Boot Guard, AMD Platform Secure Boot
   - Can also be external to the silicon platform, e.g. BMC

Step 1 can be checked fairly easily, and because Google has many vendors for chromebooks and chromeboxes, mobile/laptop SoCs are often supported ahead of release

Step 2 is more tricky :)

What is AMD Platform Secure Boot?

- AMD’s version of Intel Boot Guard
- In summary, AMD ASP is fused to only accept BIOS images signed by board vendor’s private key
  - Fuses are on the CPU package itself, whereas on Intel they’re in the PCH
  - This means that on socketed desktop platforms, bypassing PSB is as simple as replacing the CPU
  - Also means that once fused, a CPU will only be usable inside boards from that specific vendor, or even only in that device model
  - Kills used CPU market, so it’s seldom used in enthusiast / DIY boards



Home › Workstation › Lenovo Vendor Locking Ryzen-based Systems with AMD PSB

Workstation Workstation Processors

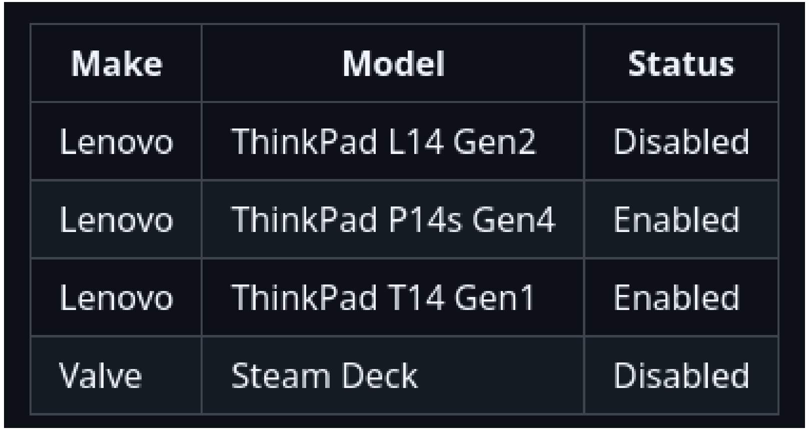
Lenovo Vendor Locking Ryzen-based Systems with AMD PSB

By Patrick Kennedy - December 31, 2021 23

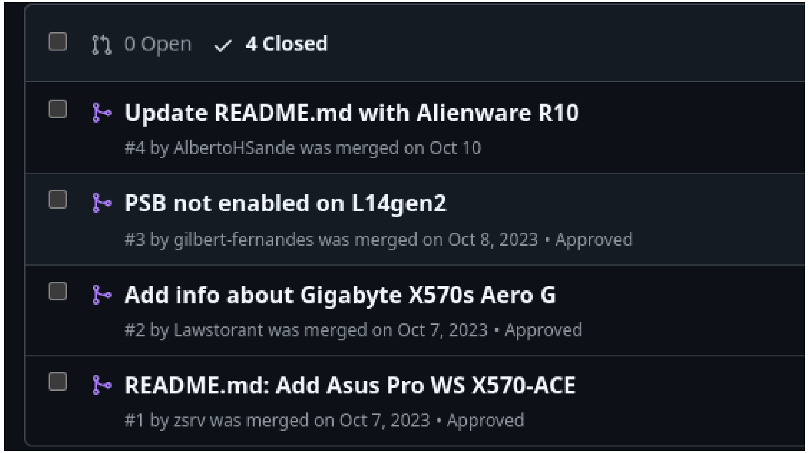
Source: ServeTheHome

How do I check if I have it?

- For Intel, we have Felix Singer’s bootguard-status project: https://github.com/felixsinger/bootguard-status
- For AMD, there wasn’t a comparable tool, so I wrote psb_status
  - Very small bash script (32 LoC)
  - Based on coreboot’s implementation of PSB
  - Checks for FUSE_PLATFORM_SECURE_BOOT_EN bit in PSB_STATUS_OFFSET register
  - I also compile a list of user reports, so feel free to contribute :)



Make	Model	Status
Lenovo	ThinkPad L14 Gen2	Disabled
Lenovo	ThinkPad P14s Gen4	Enabled
Lenovo	ThinkPad T14 Gen1	Enabled
Valve	Steam Deck	Disabled



□ 0 Open ✓ 4 Closed

□ **Update README.md with Alienware R10**
#4 by AlbertoHSande was merged on Oct 10

□ **PSB not enabled on L14gen2**
#3 by gilbert-fernandes was merged on Oct 8, 2023 • Approved

□ **Add info about Gigabyte X570s Aero G**
#2 by Lawstorant was merged on Oct 7, 2023 • Approved

□ **README.md: Add Asus Pro WS X570-ACE**
#1 by zsrv was merged on Oct 7, 2023 • Approved

Demo

Future plans

- Make checking more reliable
    - One user reported discrepancy between psb_status and fwupd HSI
    - Check more status bits
- Make it easier to submit results
- Remove dependency on external tools (iotools)
- Offline analysis of BIOS binaries

Discussion