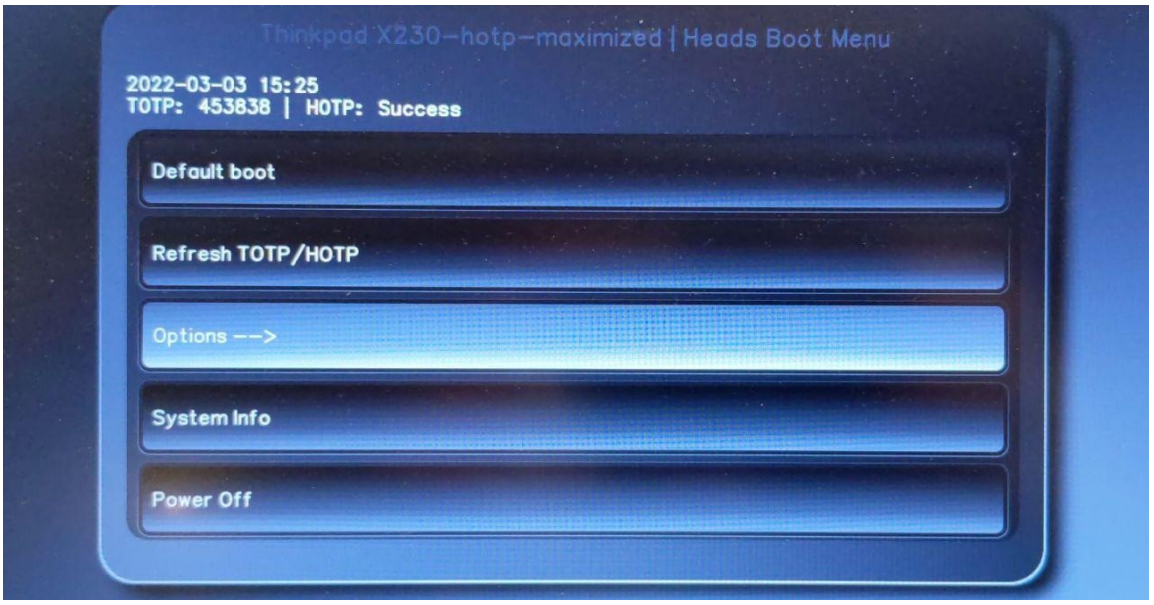
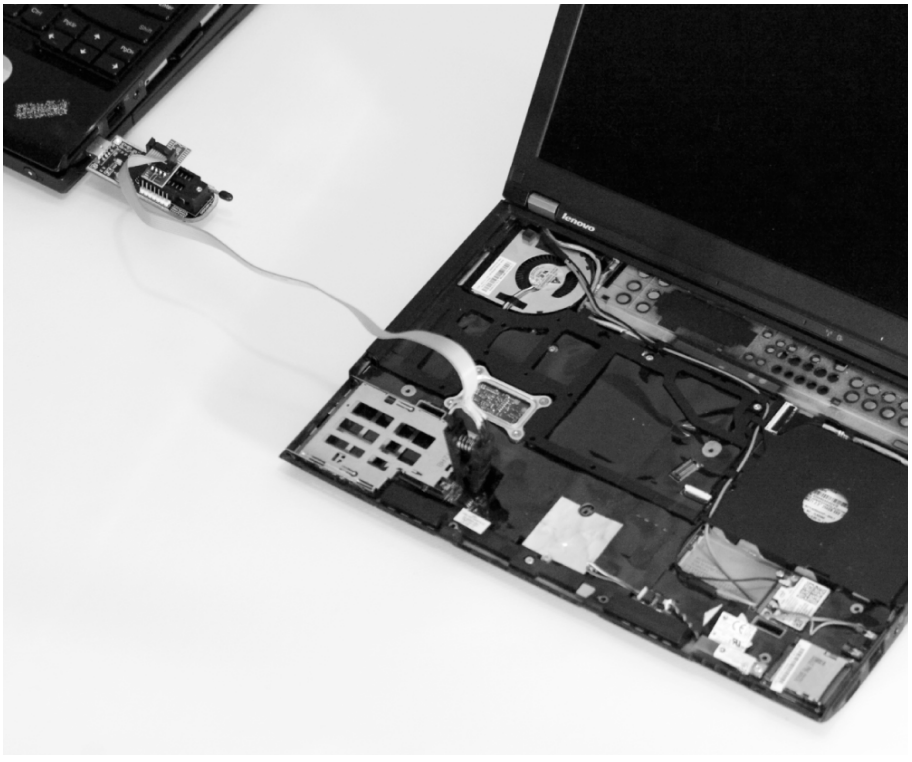
About

3-3 minutes



Overview

Heads is an open source custom firmware and OS configuration for laptops and servers that aims to provide slightly better physical security and protection for data on the system. Unlike Tails, which aims to be a stateless OS that leaves no trace on the computer of its presence, Heads is intended for the case where you need to store data and state on the computer.



Heads is not just another Linux distribution – it combines physical hardening of specific hardware platforms

and flash security features with custom coreboot firmware and a Linux boot loader in ROM. This moves the root of trust into the write-protected region of the SPI flash and prevents further software modifications to the bootup code (and on platforms that support it, Bootguard can protect against many hardware attacks as well). Controlling the first instruction the CPU executes allows Heads to measure every step of the boot firmware and configuration into the TPM, which makes it possible to attest to the user or a remote system that the machine has not been tampered with. While modern Intel CPUs require binary blobs to boot, these non-Free components are included in the measurements and are at least guaranteed to be unchanging. Once the system is in a known good state, the TPM is used as a hardware key storage to decrypt the drive.

Additionally, the hypervisor, kernel and initrd images are signed by keys controlled by the user. While all of these firmware and software changes don't secure the system against every possible attack vector, they address several classes of attacks against the boot process and physical hardware that have been neglected in traditional installations, hopefully raising the difficulty beyond what most attackers are willing to spend.

Further reading

Conferences

- 2016 - 33C3 - Trammel Hudson - Heads Presentation
- 2017 - 34C3 - Trammel Hudson - LinuxBoot Presentation
- 2019 - Platform Security Summit - Thierry Laurion - Accessible Security: An OEM approach to transferring device and secrets ownership
- 2020 - FOSDEM - Thierry Laurion - Heads OEM device initial/trasfer of ownership
- 2020 - SOCALINUXEXPO - Kyle Rankin - Tamper Evident Firmware with User-controlled keys
- 2023 - FOSDEM - Thierry Laurion - Heads status update

Articles

- 2023 - BLOG - Michael Atfield - Trusted Boot (Anti-Evil-Mail, Heads and Pureboot

Learn more about Heads

- Heads threat model - goes into more detail about what classes of threats Heads attempts to counter.
- Frequently Asked Questions
- Requirements for Heads
