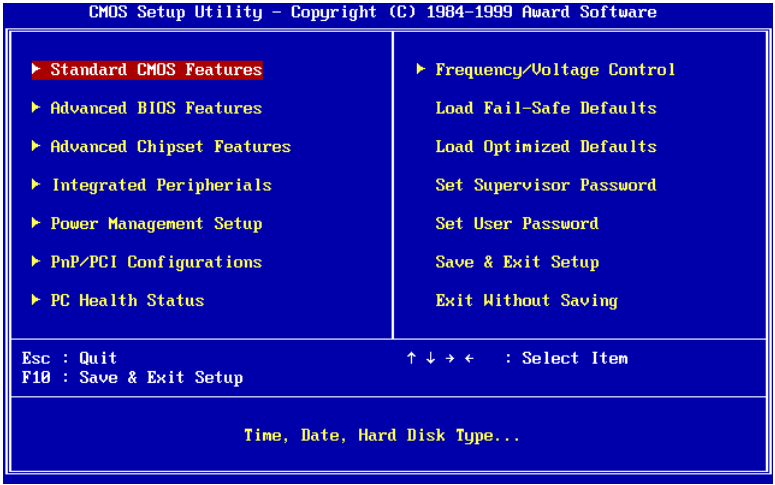
Who owns this notebook?

Where I come from?

- C and python developer
- hardware and embedded projects
- coreboot - open source bootloader
- OpenWrt - embedded Linux distribution
- freelancer

OpenWrt
Wireless Freedom

firmware


CMOS Setup Utility - Copyright (C) 1984-1999 Award Software
Standard CMOS Features
Advanced BIOS Features
Advanced Chipset Features
Integrated Peripherials
Power Management Setup
PnP/PCI Configurations
PC Health Status
Frequency/Voltage Control
Load Fail-Safe Defaults
Load Optimized Defaults
Set Supervisor Password
Set User Password
Save & Exit Setup
Exit Without Saving
Esc : Quit
F10 : Save & Exit Setup
↑ ↓ → ← : Select Item
Time, Date, Hard Disk Type...

firmware

firmware

- runs first

firmware

- runs first
- detects boot media

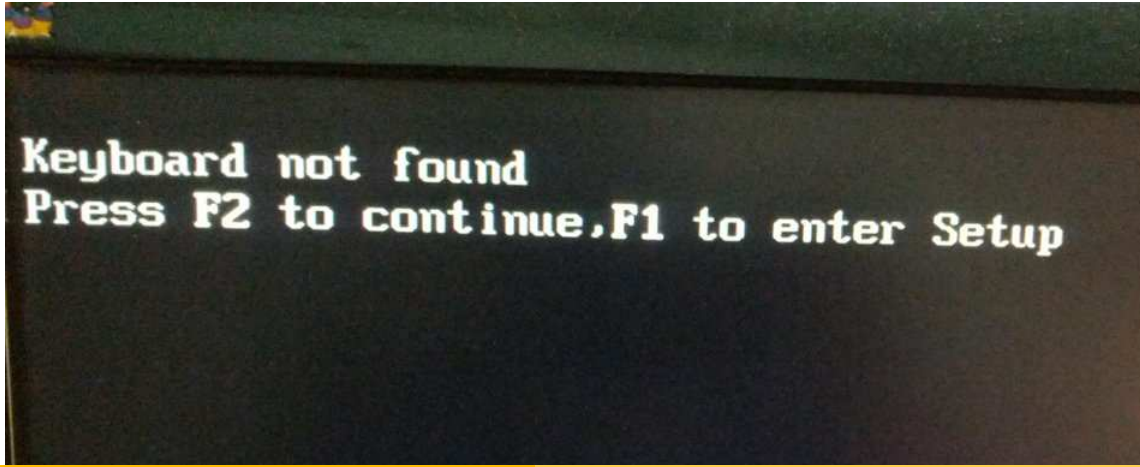
firmware

- runs first
- detects boot media
- boots the OS

firmware

- runs first
- detects boot media
- boots the OS
- best quality you can find

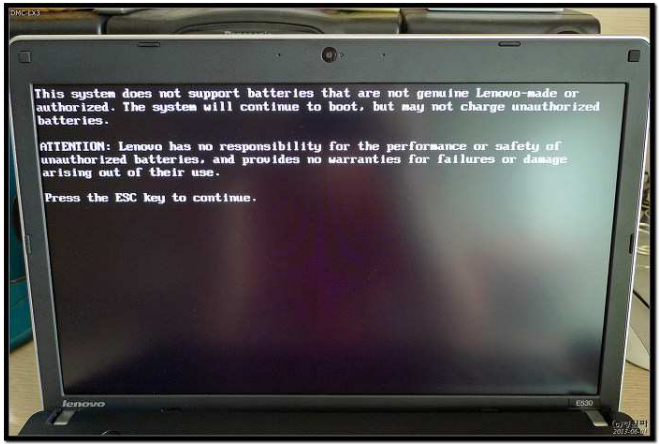
firmware



What means owning a notebook?

What means owning a notebook?

Replacing the battery?



Replacing the battery?

```
The system does not support batteries that are not genuine
Lenovo-made or authorized. The system will continue to boot,
but may not charge unauthorized batteries.

ATTENTION: Lenovo has no responsibility for the performance or
safety of unauthorized batteries, and provides no warranties
for failures or damage arising out of their use.

Press the ESC key to continue.
```

Replacing the wifi card?

Replacing the wifi card?

Unauthorized network card is plugged in.
Power off and remove the miniPCI network card.

What means owning a notebook?

- destroy it
- put stickers on it
- NO foreign wifi cards
- NO foreign batteries
- NO foreign power supply

Why this?

Why this?

- Security!!!

Why this?

- Security!!!
- secure their markets

Why is firmware security important?

Why is firmware security important?

- Heartbleed (Intel ME)

Why is firmware security important?

- Heartbleed (Intel ME)
- Rowhammer (RAM/DDR)

Why is firmware security important?

- Heartbleed (Intel ME)
- Rowhammer (RAM/DDR)
- buggy SMM (highest privileges)

Why is firmware security important?

- Browser has security leaks

Why is firmware security important?

- Browser has security leaks
- OS has leaks too

Why is firmware security important?

- Browser has security leaks
- OS has leaks too
- replace the firmware code

Why is firmware security important?

- Browser has security leaks
- OS has leaks too
- replace the firmware code
- They got all the power

Why is firmware security important?

- Browser has security leaks
- OS has leaks too
- replace the firmware code
- They got all the power
- Bonus point: outdated systems

Who updated the firmware this year?

What can coreboot fix for you?

- mitigate rowhammer (a little bit)
- very reduced SMM
- don't forbid using any hardware
- Open Source + reproducible

What can you do?

- Only money talks

- Make open hardware

Thank you

Alexander Couzens

<lynxis@fe80.eu>

390D CF78 8BF9 AA50 4F8F
F1E2 C29E 9DA6 A0DF 8604