Open System Firmware

John Looney
PE Host Provisioning
Facebook Dublin

What is Provisioning ?

- Turn it on
- Update Firmware
- Install Software
- Check it’s good

What can go wrong ?

- Hardware can have faults
- Software can have bugs
- People keep changing things
- Firmware is terrible

I love my job

Unified Extensible Firmware Interface

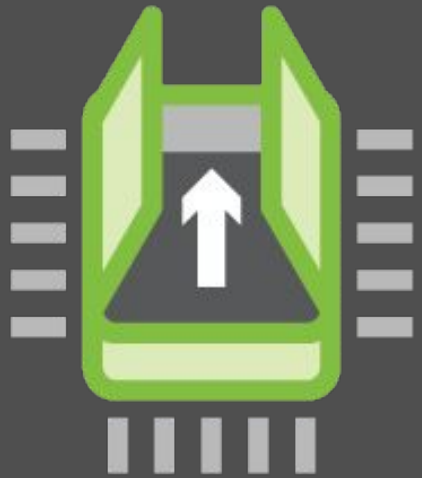
- Initialises all x86 hardware
- Software, written by hardware engineers
- As old as Windows ‘98
- Over 5000 pages of a specification
- Hacked on by multitudes ever since
- It doesn't work for everyone

https://commons.wikimedia.org/wiki/File:Uefi_logo.svg

Expand on“it doesn't work for everyone”..

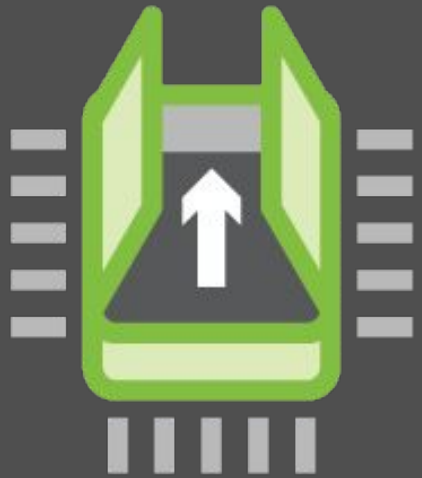
- Machines take 5 months to netboot
- Maybe network cards don’t init
- Maybe it doesn’t work with IPv6
- Maybe we can get a fix in 4 months
- 17 million lines of code. To run tftp.

2F



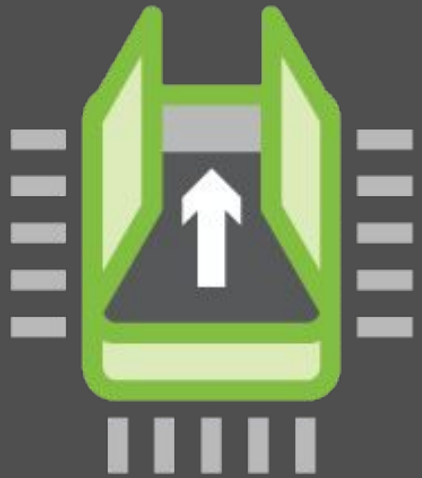
Open System Firmware

- Designed and built by software people
- Minimal hardware initialisation code
- Jump into Linux + u-root
- Linux finds an operating system to boot



Challenges

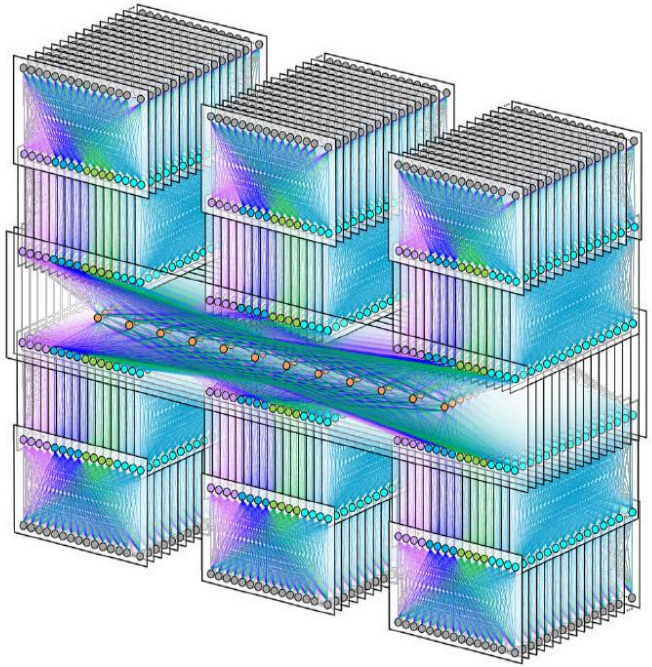
- We depend on silicon vendors
- Hardware initialisation is voodoo
- 16MB vs. 32MB flash: save €0.10

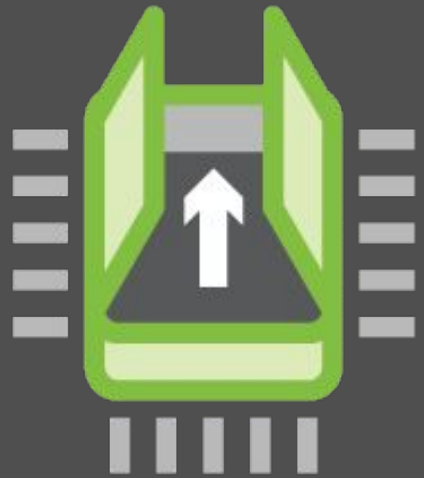


Today

- Minipacks ships with OSFW
- Boot in 7 seconds, not 4 minutes
- Debug issues in 20 seconds, not 3 weeks
- Fix in 30 minutes, not 4 months
- Anyone who knows Go can extend it

Minipack!

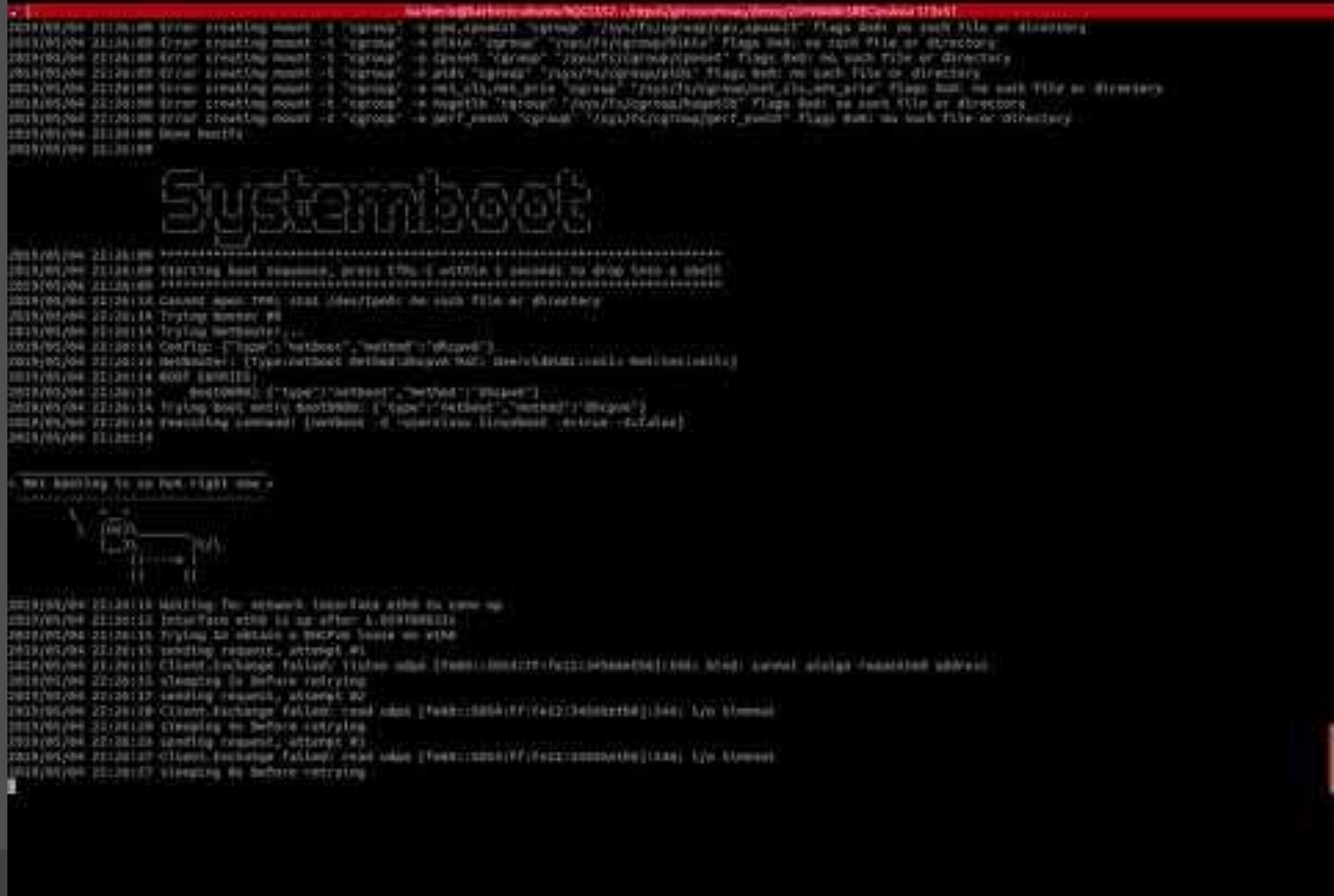




Tomorrow

- Netboot via https or bittorrent
- Broken-hardware checker in firmware
- Firmware Transparency
- Plan9

Demo Time!



Thanks!