Breaking your computer by taking it apart and poking at it with wires

1. wat

Whatcha talkin' 'bout, Jeffrey?

Trust in your own technology

- How can you trust that the software you use follows your interests?
  - Obviously just use open source software and read all the code and then you know it's doing what you want, and that's all we need to do

Trust in your own technology

If you’re using x86

If you’re using x86

The Intel Management Engine

- Basically a separate computing system inside your processor that has full access to all your stuff
- “Ring -1”
- Even if you verify trustworthiness of your software, OS, firmware (with, say, coreboot), your CPU and UEFI are closed off from you

The Intel Management Engine

- Allows for remote administration, remote destruction, and a few other legitimate features
- But… what happens when bad people take it over?
  - And does Intel count as bad people?
- We also can't read its code
  - Compressed in the JEFF format – we don't know how it is compressed, so we can't just read the code as instructions
  - Some of the code is on the CPU die itself, so, have fun?

2. I don’t want that

Get rid of it

You can break things with wires

This is the boy

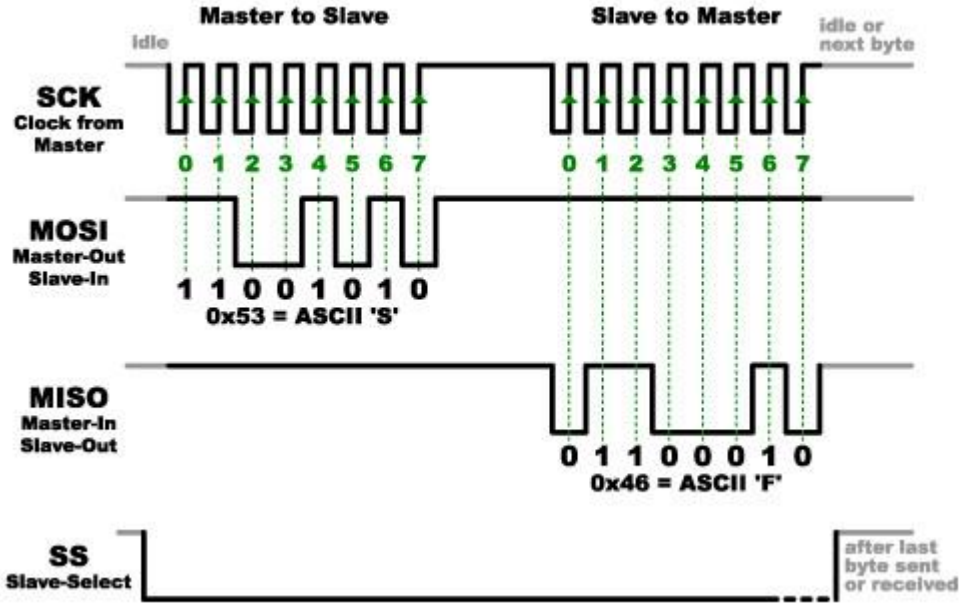
He contains the firmware

Do not anger him

SPI: Serial Peripheral Interface

- A master-slave, bussed synchronous serial communication interface
- Often used for LCD displays and SD cards
- All kinds of implementations, but all usually have at least four wires

SPI: Serial Peripheral Interface



SPI: Serial Peripheral Interface

- Your computer firmware is usually stored on a bit of memory that communicates over SPI
- For my laptop, the first 12KB are a descriptor, followed by ~5MB of the IME firmware, followed by ~3MB of rewritable memory, followed by ~96KB of bootblock
- You generally can't change this stuff while the computer is running, but if you are willing to poke things with wires…

External programmer

- If you poke things with wires, and pray, all your dreams can come true
- Lots of things can talk SPI – if you're patient, you can probably even use a computer with a parallel port to do it
- But I'm going to use a Pi Zero, since it has SPI already

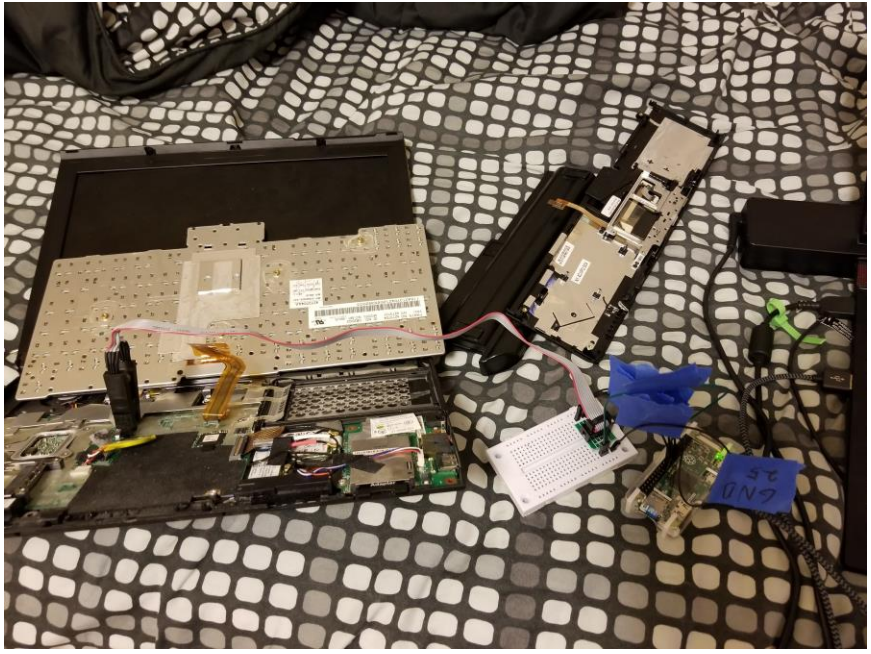
“

why would Kim Jong-un insult me by calling me "old," when I would NEVER call him "short and fat"? Oh well, I try so hard to be his friend - and maybe someday that will happen!

Read twice, write once

- It is not recommended to corrupt your firmware, and errors can happen during reading and writing, so first read the firmware TWICE
- Then diff them
- This is at least some reassurance that your read was correct
- I will use flashrom to read and write the firmware, following these pinouts: pi laptop

Setup



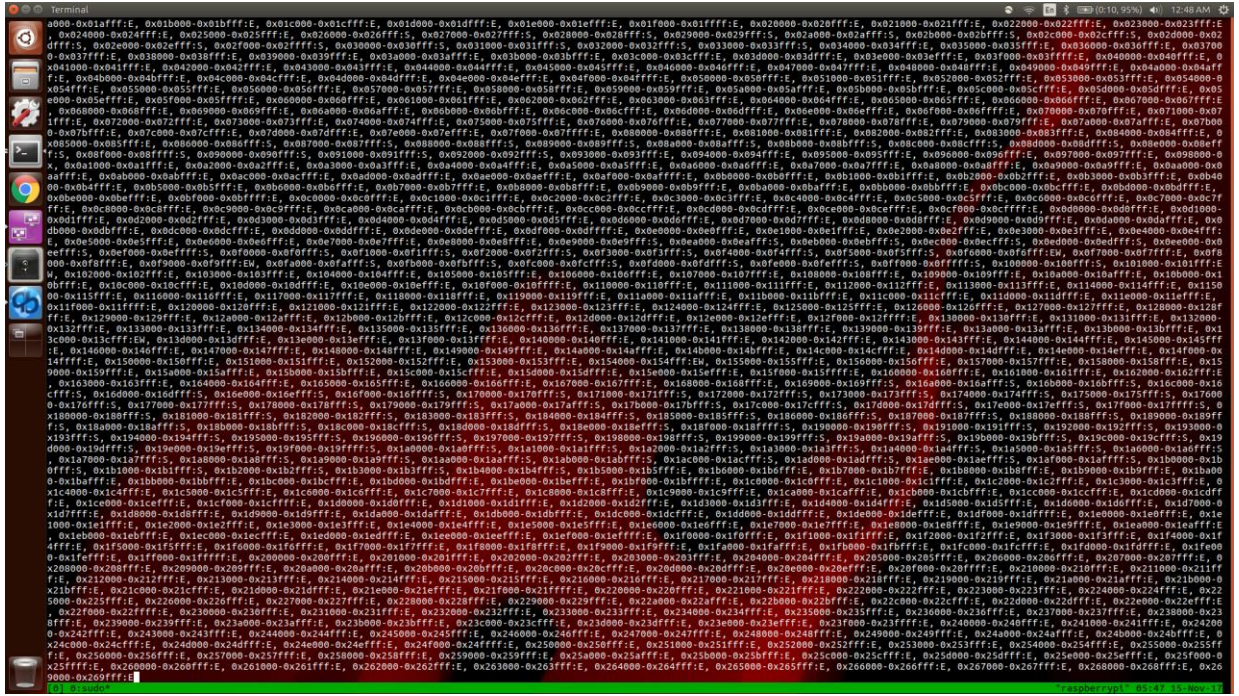
Reading at a fourth grade level

- I used the trick I did for my last lug talk, where I ssh into a pi0 over USB
- I started reading, and the pi0 switched interface names for no reason
- I hate Ubuntu
- Eventually I read it twice and the two reads matched…

Kill it with fire

- Next up was using me_cleaner to edit the firmware dump
- This was straightforward, it was just a python script
- Finally, I again used flashrom to write back the modified file – you don't have to write twice, and it will automatically verify the write was successful by reading and checking

Kill it with fire



3. How’d it go

Did you break it like you promised?

Black screen forever

Questions?

Oh wait it started doing the thing

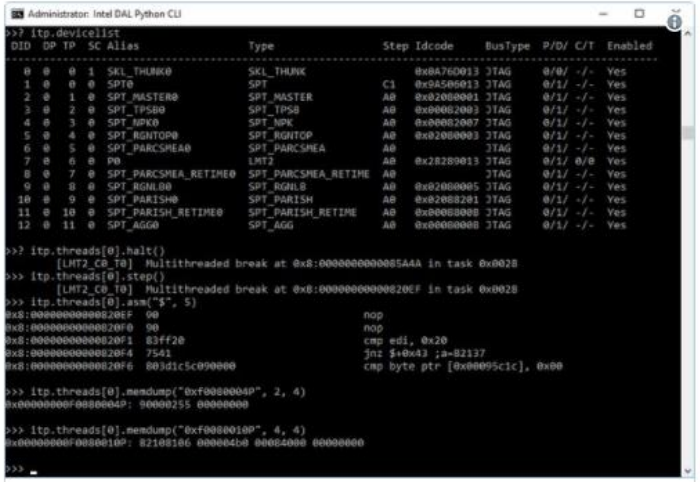
4. Recent developments

I feel like someone mentioned this thing in the lug chat before…

MINIX

- Made by Prof. Abstract Syntax Tree
- Microkernel
- Influenced early Linux
- Post 2015, all intel chips run MINIX in the IME

JTAG



Maxim Goryachy
@h0t_max

Game over! We (I and @_markel___) have obtained fully functional JTAG for Intel CSME via USB DCI. #intelme #jtag #inteldci

9:33 AM - Nov 8, 2017

109 1,974 2,482

JTAG

- Meant for testing boards – grants a serial debug port
- Also commonly used for firmware programming on chips
- Commonly grants power to do things like execute instructions and read/write registers and RAM
- So basically, “ring -2”

Questions?


Ash
@ashcammm
guys literally only want one thing
and it's
disgusting
2017-10-22, 1:56 AM
150 Retweets 516 Likes
Article Talk
Read
Free software
From Wikipedia, the free encyclopedia
For other uses, see Free software (disambiguation).
Not to be confused with Freeware.
For a broader coverage related to this topic, see Free software movement.
Free Software also shares similarities with Open-Source Software and is now part of the broader term Free and
Free software or libre software[1][2] is computer software distributed under terms that allow users to run the softwa
purpose as well as to study, change, and distribute it and any adapted versions.[3][4][5][6][7] Free software is a matter
not price: users —individually or in cooperation with computer programmers— are free to do what they want with the
a free software (including profiting from them) regardless of how much is paid to obtain the program.[8][2] Computer
are deemed free insofar as they give users (not just the developer) ultimate control over the first, thereby allowing th
control what their computers are programmed to do.[5][9]
The right to study and modify a computer program entails that source code —the preferred format for making chang
made available to users of that program. While this is often called 'access to source code' or 'public availability', the
Software Foundation recommends against thinking in those terms,[10] because it might give the impression that use
obligation (as opposed to a right) to give non-users a copy of the program.
Although the term free software had been used loosely in the past,[11] Richard Stallman is credited with tying it to th
under discussion and starting the Free Software movement in 1983, when he launched the GNU Project: a collabor
create a freedom-respecting operating system, and revive the spirit of cooperation once prevalent among hackers
early days of computing.[12][13]