Participants – Ben, George, Esha, Yu

Signal shielding

Bug

Cross-inductions

Flip (1-0) a piece of memory by hammering certain row then the change in temperature would alter it.

Time side channels – going through hardware

Meltdown

Specter

Anti-hammering – hardware prevents guessing a password very fast ‘hammering’.

Apple phone – has the best encryption, thumb print is isolated in hardware in some extent. Pushed more on the logic on secureness with face recognition.

iPhone 5 – NAND mirroring. 4-6 digit pins to decrypt.

Keep on guessing on the iPhone would wipe the memory.

NAND mirroring makes the reset for the counter to stop the wiping of memory.

When guessing, 90% of pins are 10% of the possible values.

Tubular pick lock

Ben

19/20 years old

The 1st Xbox has unique capability. Stream.

Bought Xbox, modified hardware, put linux and not use their subscription service.

Special software with a nice menu. Pirated files.

eyeOpener – first hardware modified, a computer with modem.

If you put a hard drive you can put your own OS. 40-pin ribbon cable.

Years later – worked for Xbox. Told them in the job interview of the Xbox problem. Got hired.

Germany – Chaos Computer Club

Improv Lab - <http://www.improvlabs.com/>

Radiance energy management

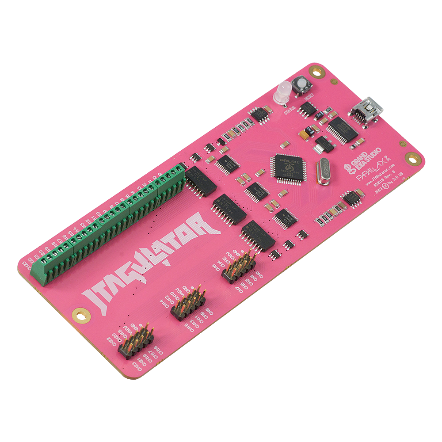
**Tools**

Jtagulator 32115 Parallax Inc – if you don’t know the pins. This will run for 26 hours to check for all possible combination to label what is the clock, input, output and modify.

Or Arduino with jtagulator

Raise the clock, whats the bit? Lower the clock, whats the bit?

The data in-pin would put random data and looks at the data out-pin, suppose to happen.



USB Fuzzer

Mag strip

**Notes**

Open ocd – talks to the debugger

Gdp is the debugger

gdb-multiarch obviously supports a range of other architectures besides ARM, so if that is something that would be useful for you then it might make sense to use that.

Concatenates the files, dongle and openocd

Tricky – once you get openocd to work.

Have to open a new terminal. 4444

Opens up a listening that’s why you need a new terminal

Voting machine is running on Windows CE (Platform Builder)

Jtag pin out – search online for diagram

Adafruit

cpu

Cpld and fpga are just logic gates but faster than cpu.

Cpld

Fpga – always need to push program

**Linux - terminal**

sudo apt update

sudo apt install openocd gdb-multiarch

sudo apt --fix-broken install

set arch armw5te

gdb\_port