DEF CON 23 LAS VEGAS

This talk will is not about LTE vulnerabilities

GENIUS
Why isn’t it working?
Download from Dreamstime.com
This watermarked comp image is for previewing purposes only.
ID 44501604
Ximagination | Dreamstime.com

DEF CON 23 LAS VEGAS

Scared Poopless – LTE and *your* laptop

Disclaimer:
During the slides you will be exposed to hacker stock photos from the internet.

Thank you!

Goldy
aSmig

DEMO

DEF CON 23 LAS VEGAS

What did I just see?

Who are we?

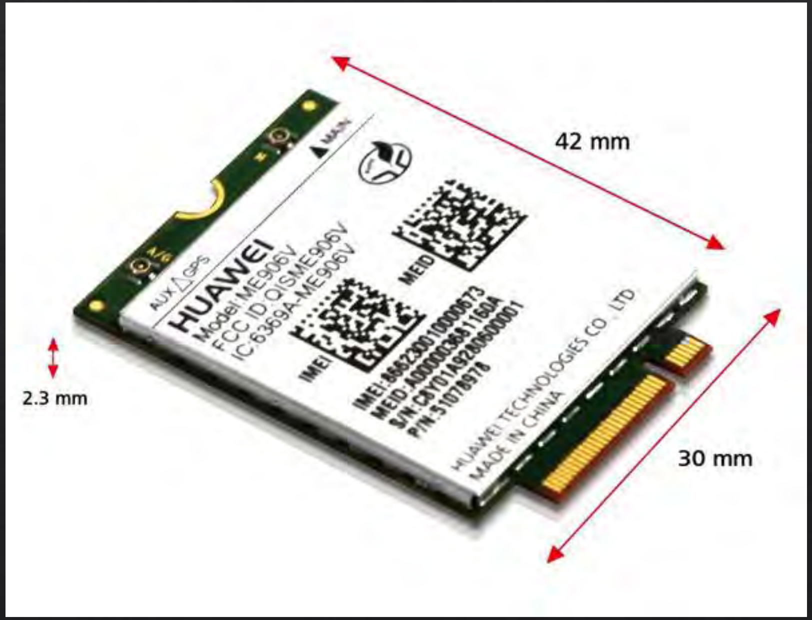
BadUSBは序章にすぎない!?
USBに潜む真の危険性を2人組のセキュリティ研究者が指摘する!!

Background

- Internal LTE/3G modems and who uses them?

I like to use my own keyboard
shutterstock
www.shutterstock.com · 24527389

- Internal LTE/3G modems and who uses them?
  - Business class devices

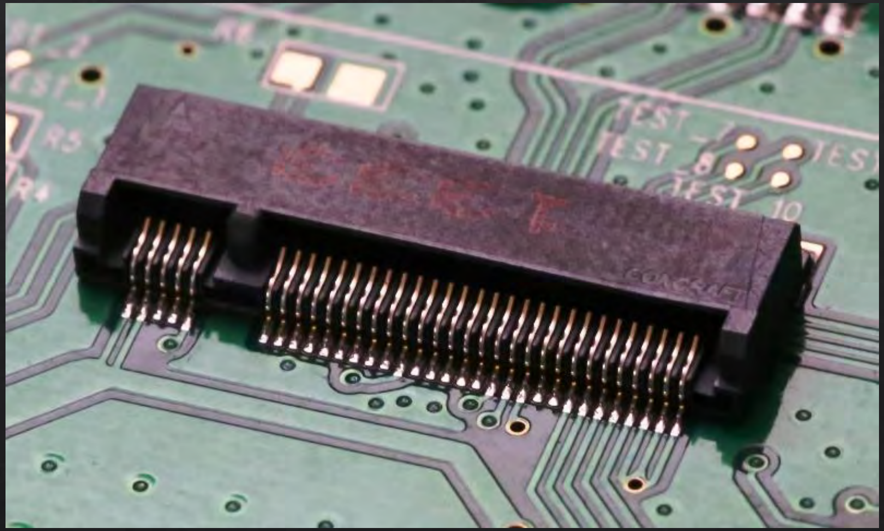


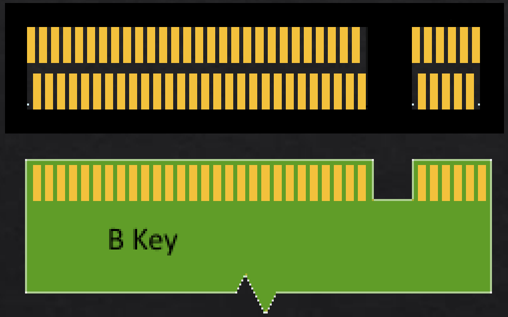
I think I have an idea!

- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in anyway?

Card against humanity 2015 world champion

- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in anyway?





- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in anyway?

PCIe ×2, SATA, USB 2.0 and 3.0, Audio, PCM, IUM, SSIC and I2C

I forgot mac's don't have a CD drive anymore

- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in anyway?
  - USB?!

- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in?
  - USB?!
- Why hack this device anyway?

Respect the gas/ski mask

Background

- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in?
  - USB?!
- Why hack this device anyway?
  - Module available worldwide
  - It’s plugged in [INSIDE] your laptop/tablet

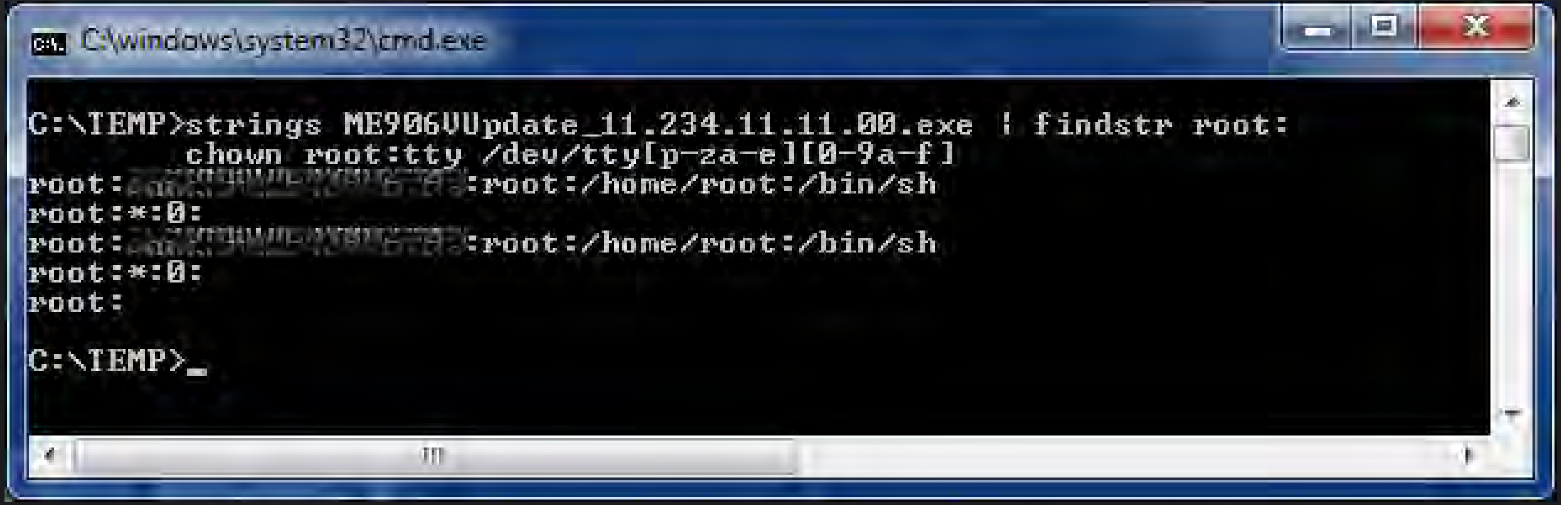
- Software
- Firmware
- Hardware

- Software
  - Windows utility for firmware updates
- Firmware
- Hardware

- Software
  - Windows utility for firmware updates
- Firmware
  - Packed in software utility
- Hardware

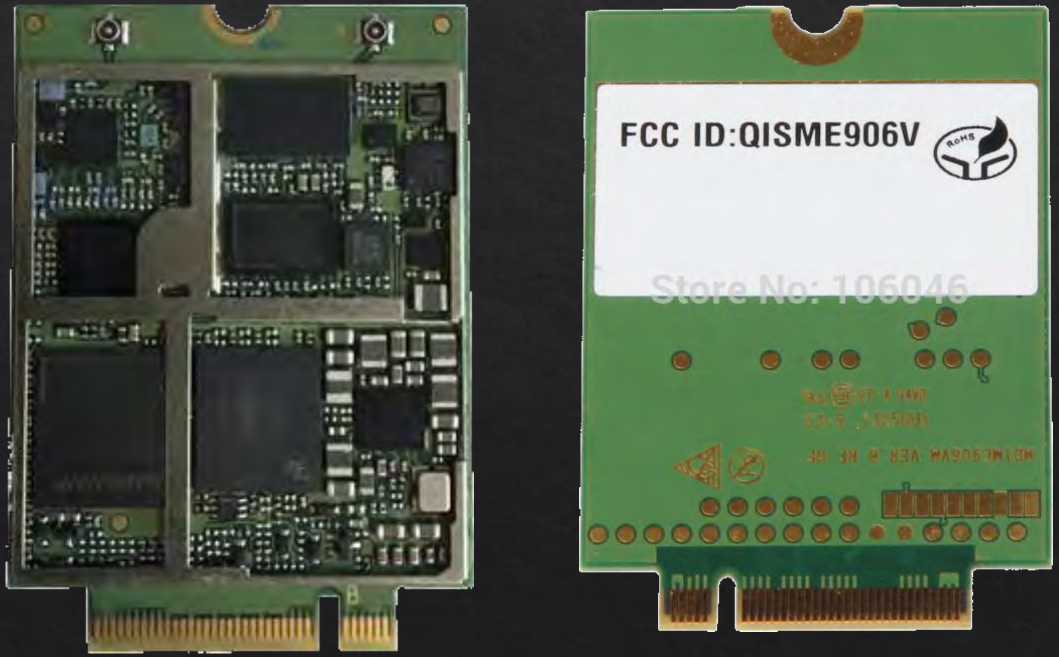
Low-cost anonymity

- Software
  - Windows utility for fi
- Firmware
  - Packed in software utility
- Hardware



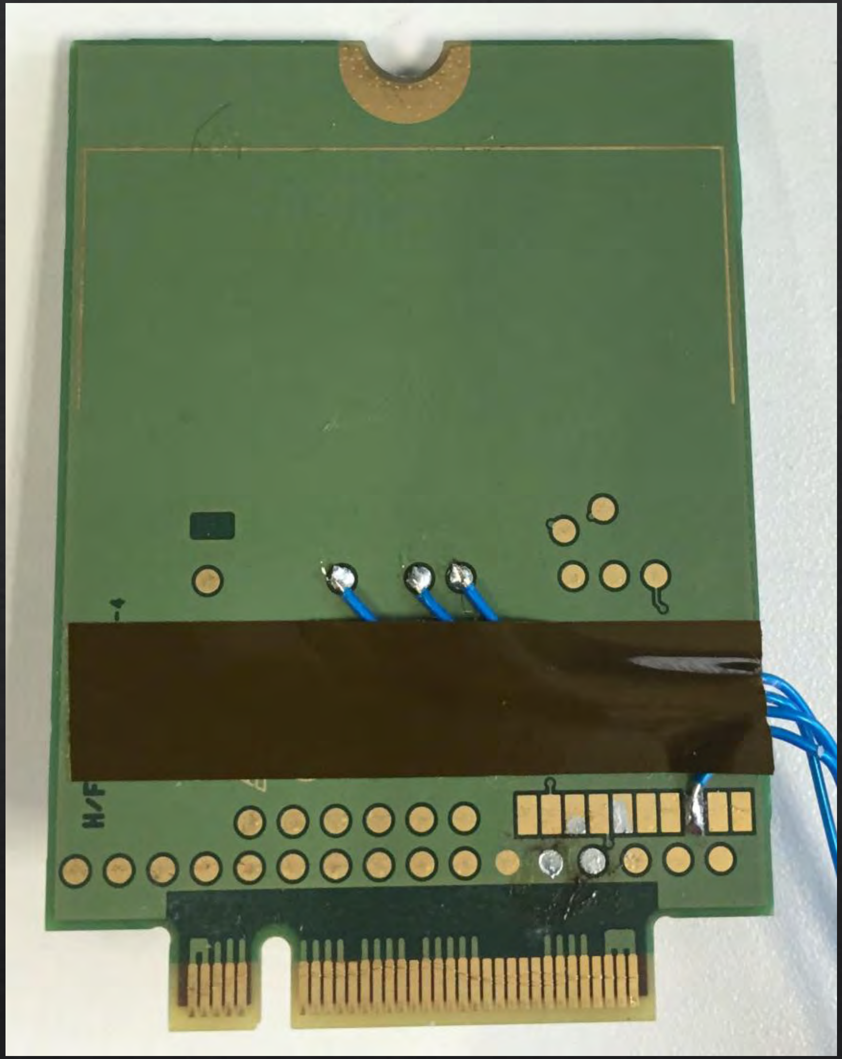
```
C:\TEMP>strings ME906VUpdate_11.234.11.11.00.exe | findstr root:
        chown root:tty /dev/tty[p-za-e][0-9a-f]
root:[redacted]:root:/home/root:/bin/sh
root:*:0:
root:[redacted]:root:/home/root:/bin/sh
root:*:0:
root:

C:\TEMP>_
```

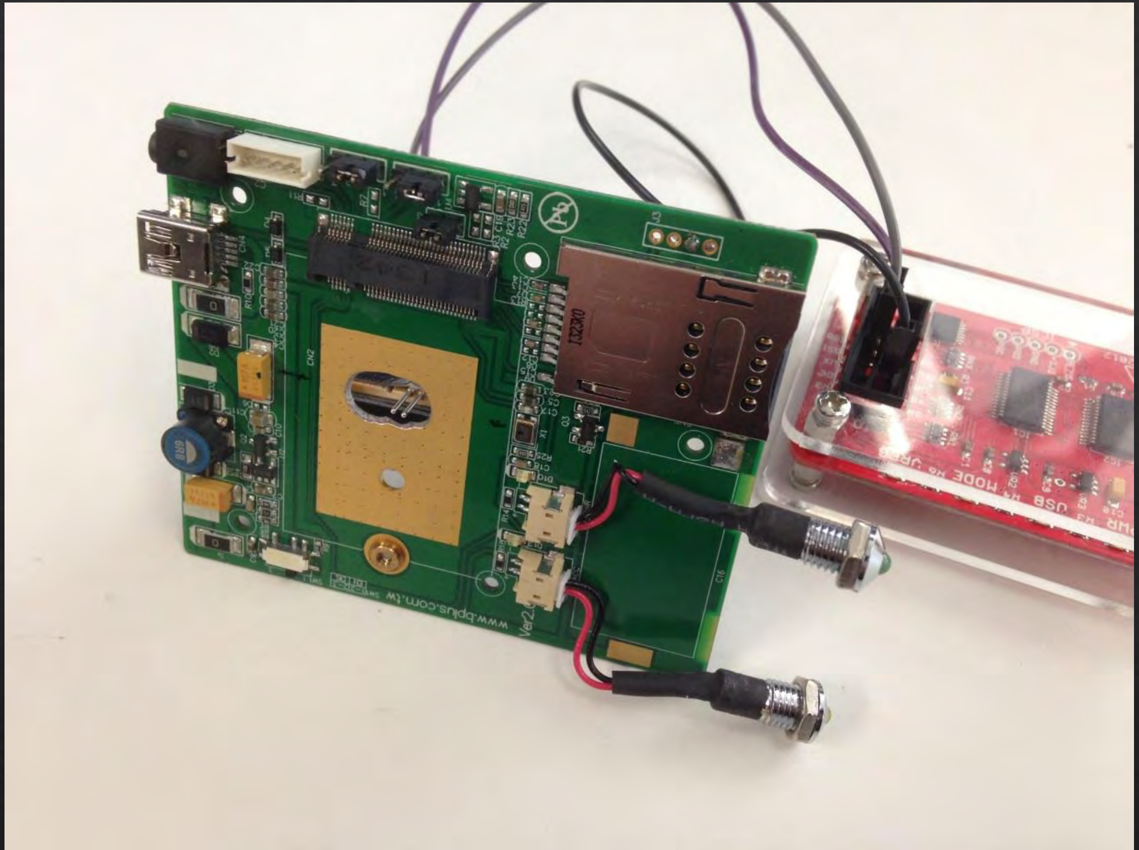
- Software
  - Windows utility for firmware updates
- Firmware
  - Strings is useful
- Hardware
  - Test pads?

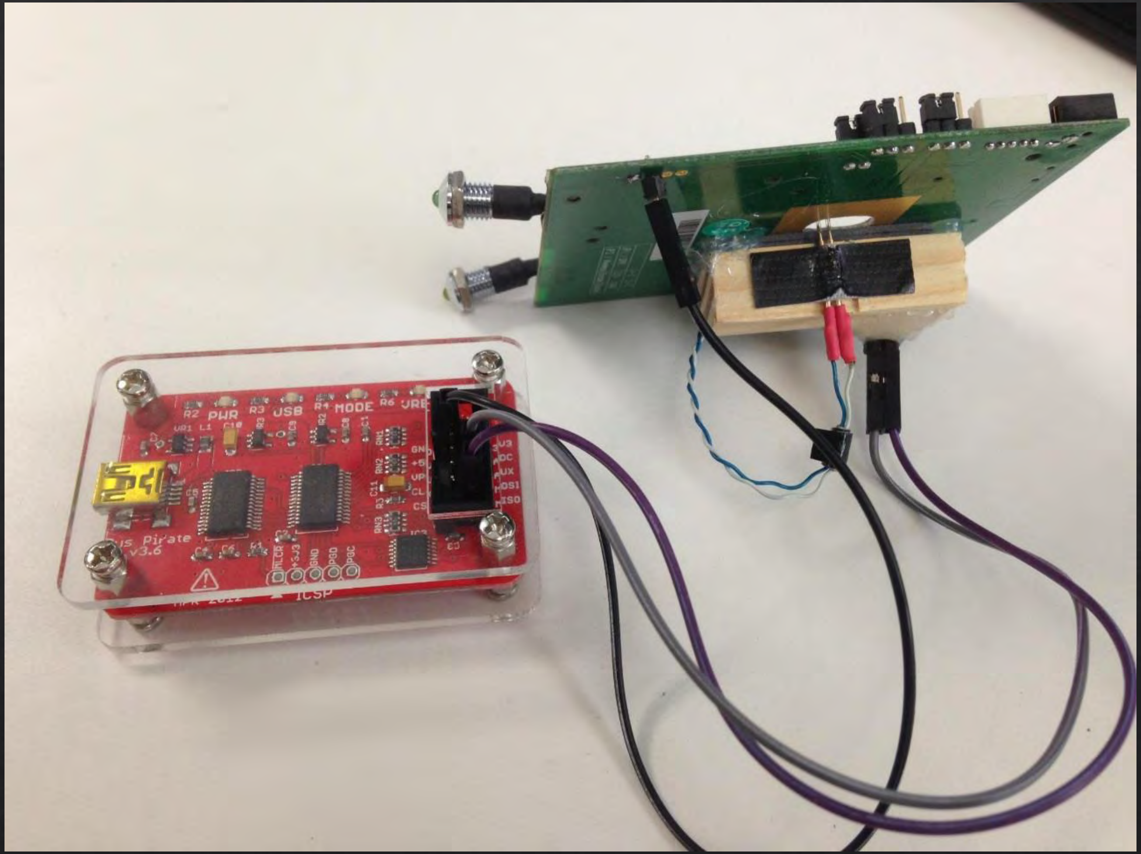


- Software
  - Windows utility for firmware updates
- Firmware
  - Strings reveals too much
- Hardware
  - Test pads?

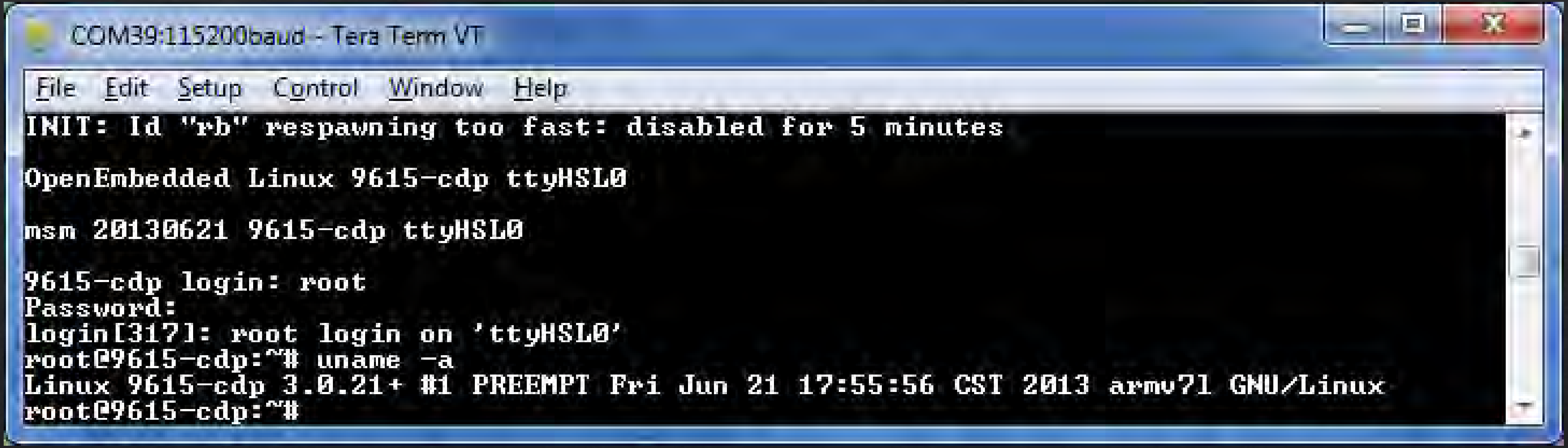
© Can Stock Photo - csp6595179




www.bplus.com.tw
Ver2
USB
MODE
PWR


PWR
USB
MODE
Bus Pirate v3.6
ICSP

Got root shell!



COM39:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
INIT: Id "rb" respawning too fast: disabled for 5 minutes

OpenEmbedded Linux 9615-cdp ttyHSL0

msm 20130621 9615-cdp ttyHSL0

9615-cdp login: root
Password:
login[317]: root login on 'ttyHSL0'
root@9615-cdp:~# uname -a
Linux 9615-cdp 3.0.21+ #1 PREEMPT Fri Jun 21 17:55:56 CST 2013 armv7l GNU/Linux
root@9615-cdp:~#
```

Happy shell dance

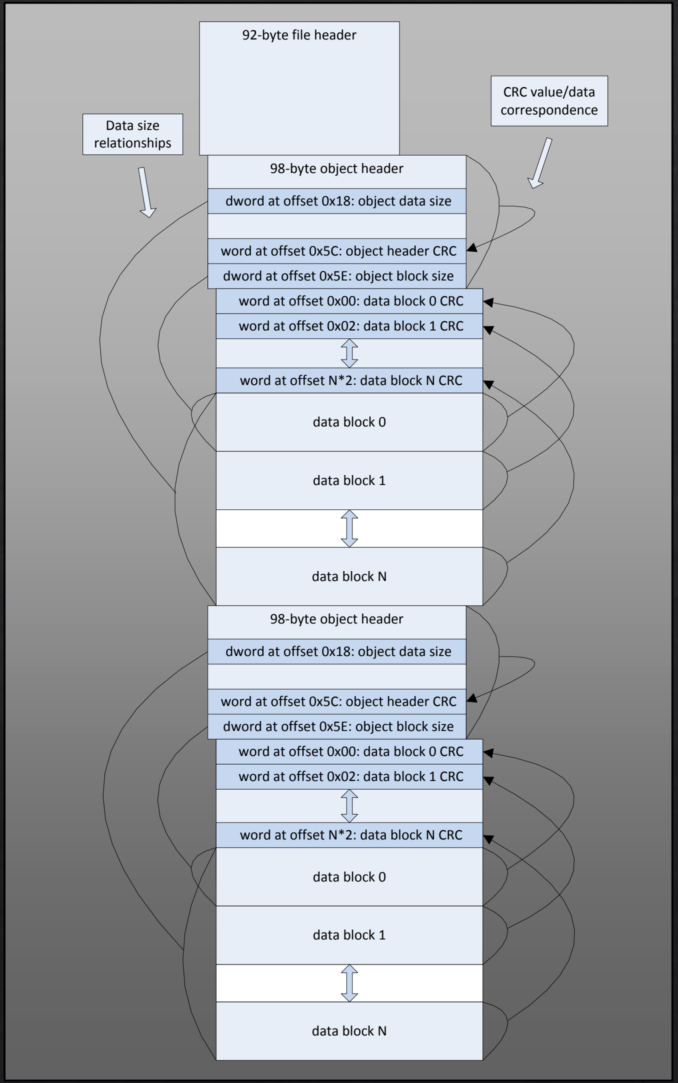
Obligatory success meme

- We have root shell on a linux run, independent device inside the physical platform.

© Can Stock Photo - csp1645735

- CVE-2015-5367: Insecure Linux Image in Firmware
- CVE-2015-5368: Insecure Firmware Update Authentication

Firmware structure

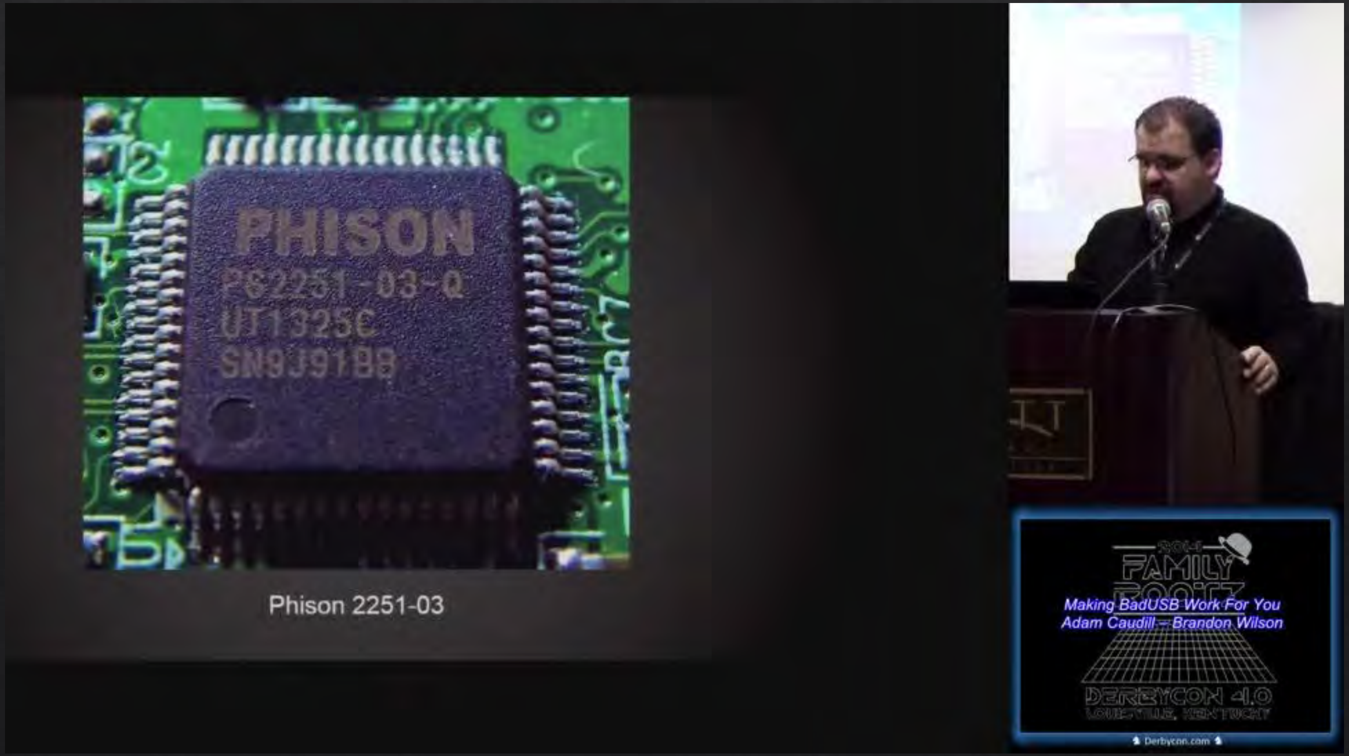

92-byte file header
Data size relationships
CRC value/data correspondence
98-byte object header
dword at offset 0x18: object data size
word at offset 0x5C: object header CRC
dword at offset 0x5E: object block size
word at offset 0x00: data block 0 CRC
word at offset 0x02: data block 1 CRC
word at offset N*2: data block N CRC
data block 0
data block 1
data block N
98-byte object header
dword at offset 0x18: object data size
word at offset 0x5C: object header CRC
dword at offset 0x5E: object block size
word at offset 0x00: data block 0 CRC
word at offset 0x02: data block 1 CRC
word at offset N*2: data block N CRC
data block 0
data block 1
data block N

Updater patch

- Updater checks CRC
- Updater calculates the correct CRC and compares to the one in the firmware image
- Modify updater code to save correct CRC in image instead of comparing it

Remember kids!
This is why you should do secure firmware updates

NEVER FORGET



Phison 2251-03

What next?

Questions?