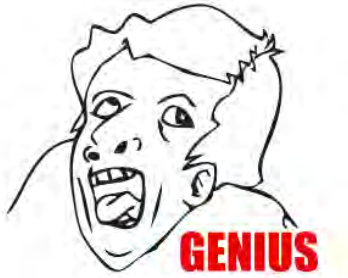
DEF CON 23 LAS VEGAS

This talk is not about LTE vulnerabilities

No cables





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.

DEF CON 23
LAS VEGAS

Thank you!

Goldy
aSmig
@octosavvi



DEF CON 23 LAS VEGAS

Intel Security would like to acknowledge and thank the Huawei PSIRT team for their responsiveness and cooperation on this issue.

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

http://huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-446601.htm



DEMO

DEF CON 23 LAS VEGAS

What did I just see?



DEF CON 23
LAS VEGAS



This is not a DELL problem

DEF CON 23 LAS VEGAS

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

NEVER FORGET

Adam Caudill
Brandon Wilson



DEF CON 23 LAS VEGAS

Who are we?

@jessemichael
@laplinker



DEF CON 23 LAS VEGAS

Background

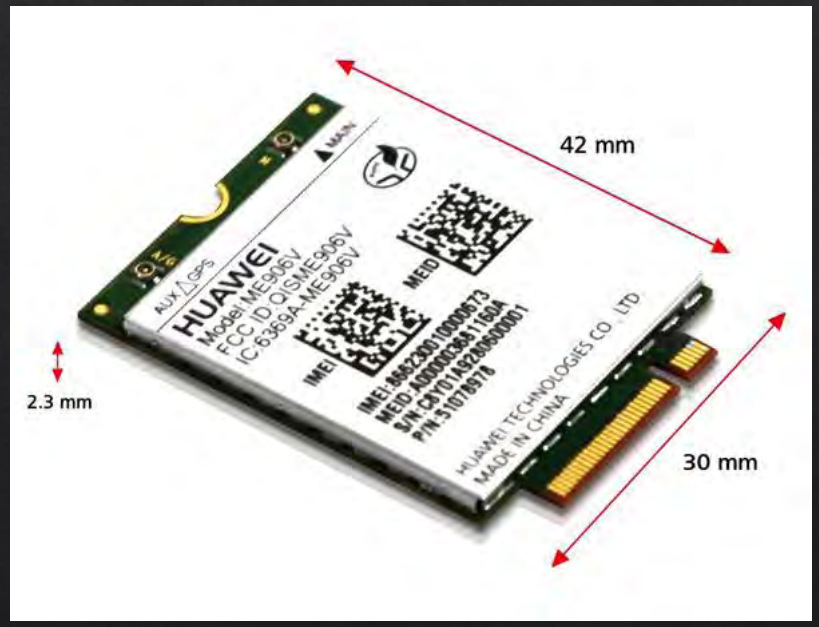
- Internal LTE/3G modems and who uses them?





DEF CON 23 LAS VEGAS

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





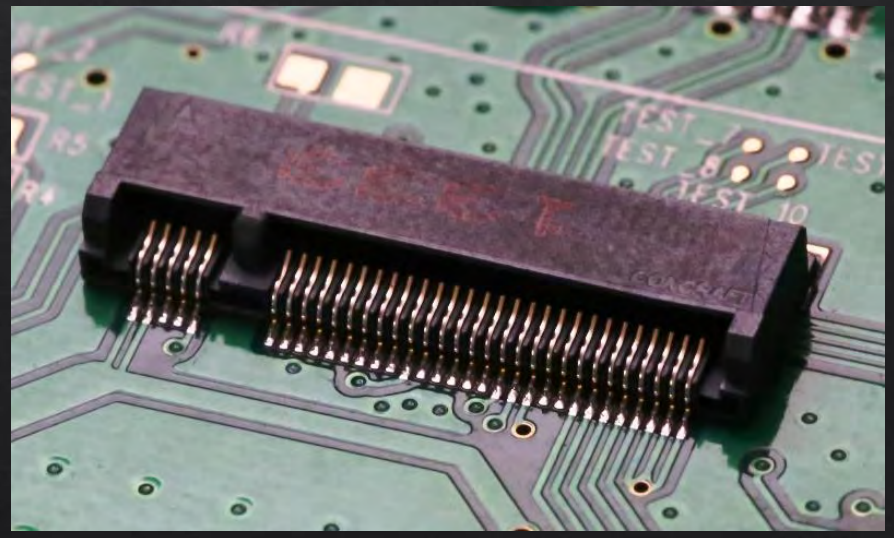
DEF CON 23 LAS VEGAS

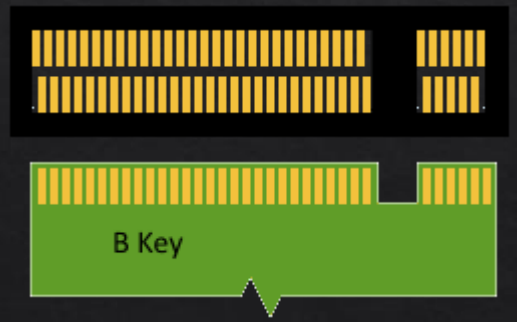
- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in anyway?



DEF CON 23 LAS VEGAS

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





DEF CON 23 LAS VEGAS

- 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





DEF CON 23 LAS VEGAS

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



DEF CON 23 LAS VEGAS

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



DEF CON 23

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



DEF CON 23 LAS VEGAS

- Software
- Firmware
- Hardware



DEF CON 23 LAS VEGAS

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



DEF CON 23 LAS VEGAS

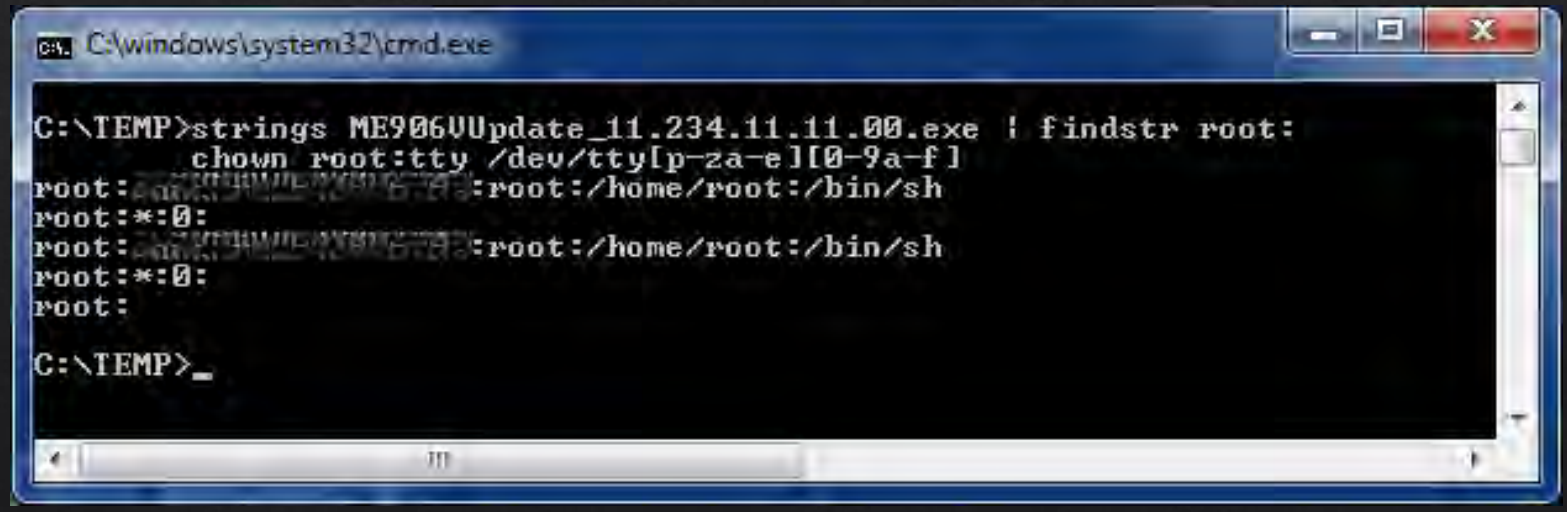
- Software
  - Windows utility for firmware updates
- Firmware
  - Packed in software utility
- Hardware



DEF CON 23 LAS VEGAS

- Software
  - Windows utility for fi
- Firmware
  - Strings is useful
- Hardware





DEF CON 23 LAS VEGAS

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



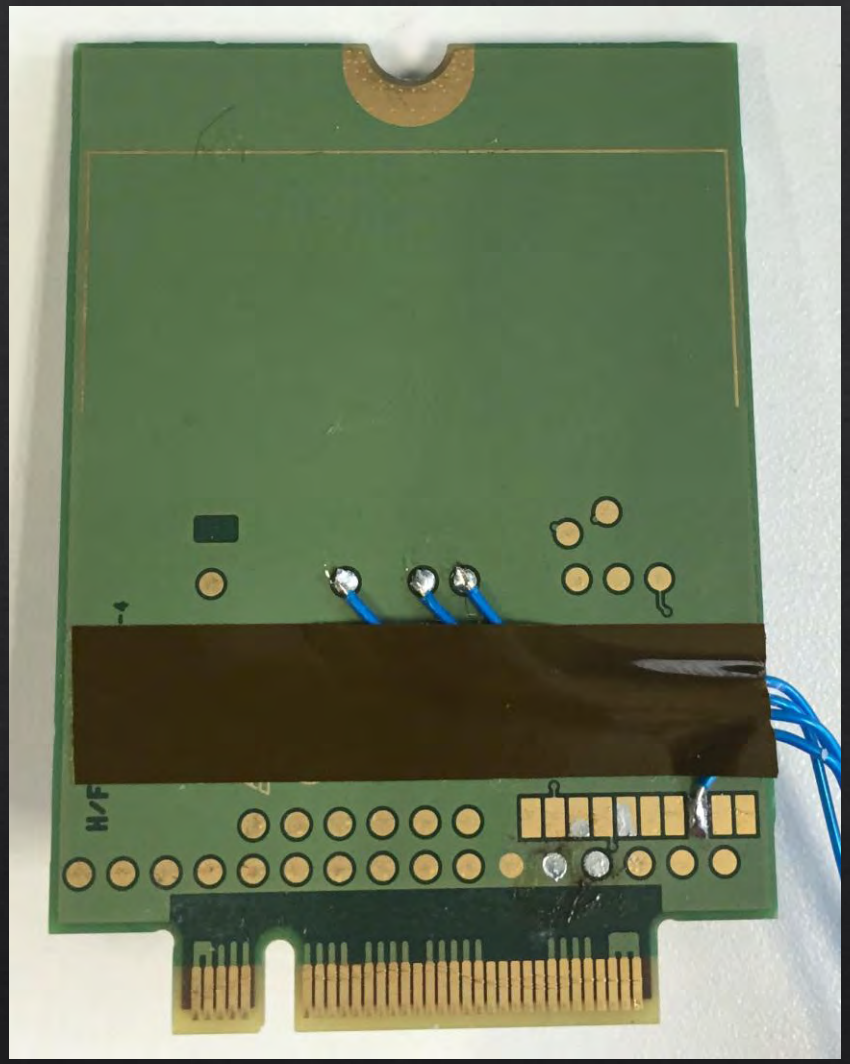


DEF CON 23 LAS VEGAS

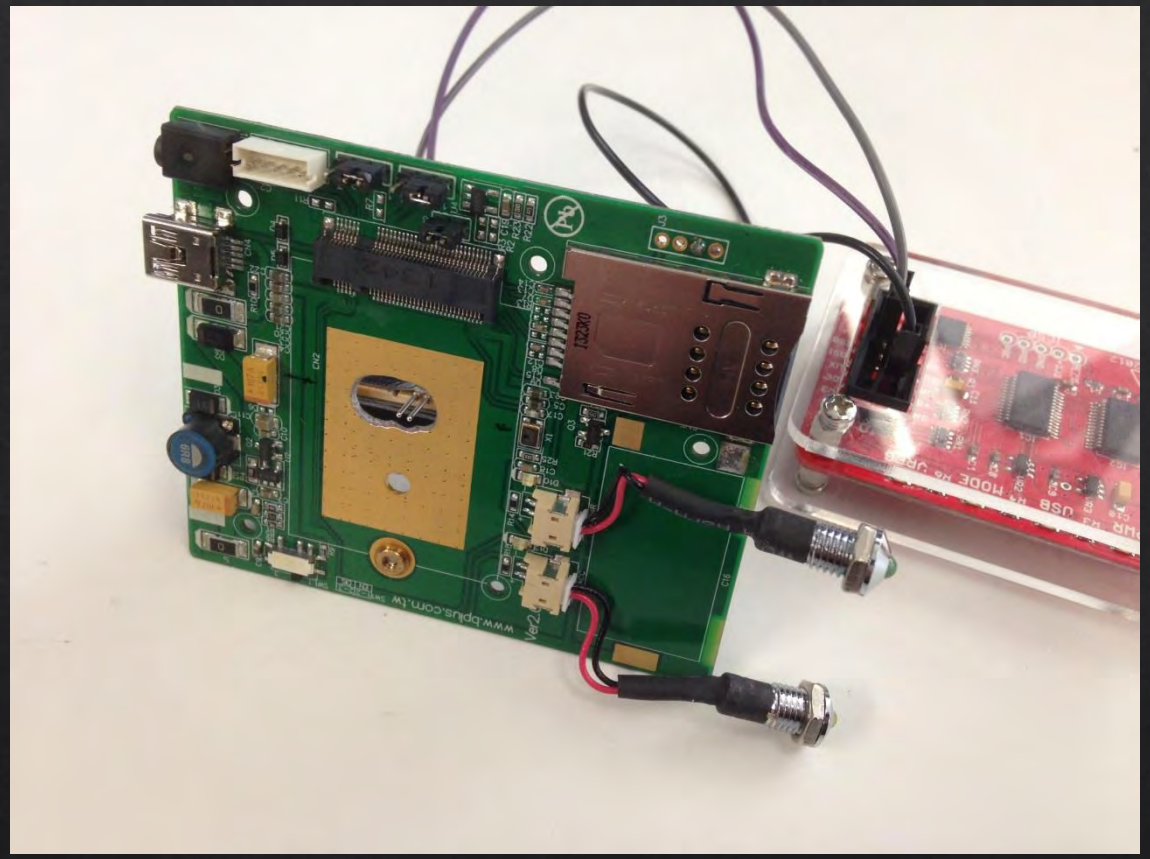
- Software
  - Windows utility for firmware updates
- Firmware
  - Strings is useful
- Hardware
  - Test pads?

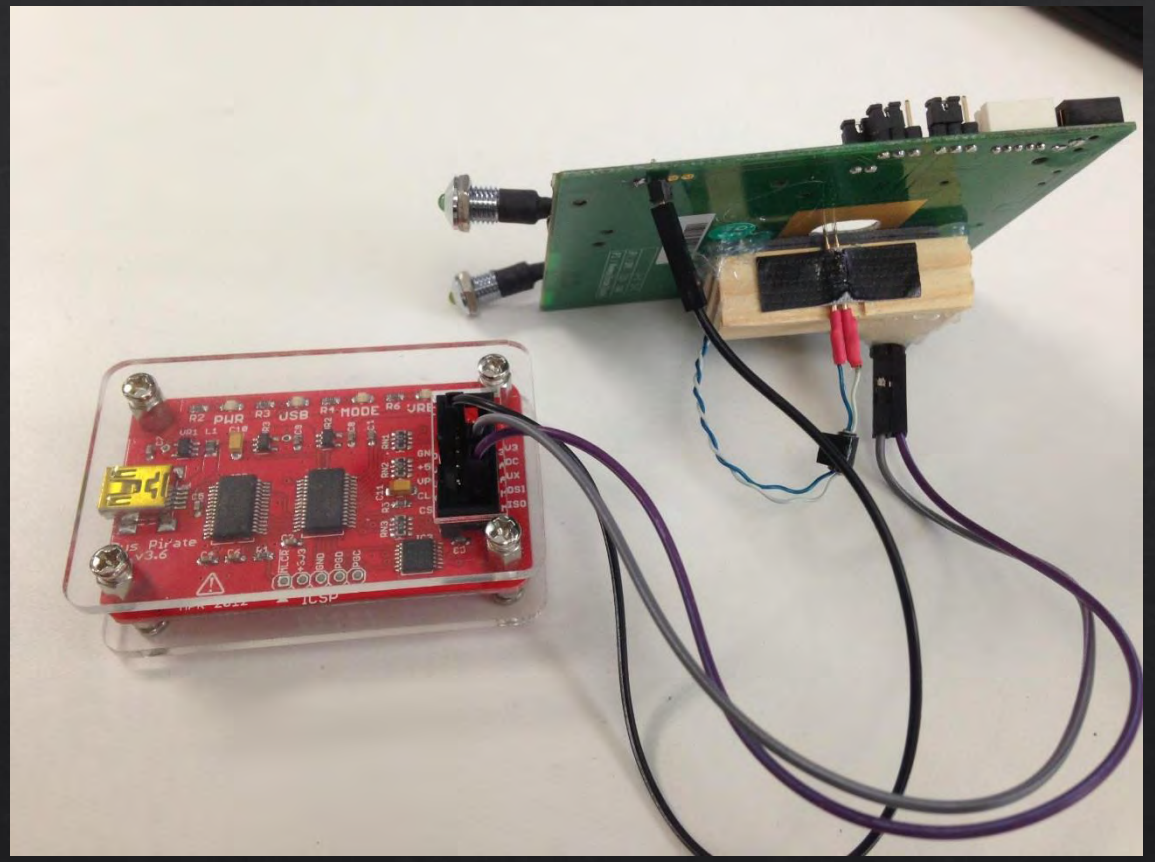


DEF CON 23
LAS VEGAS



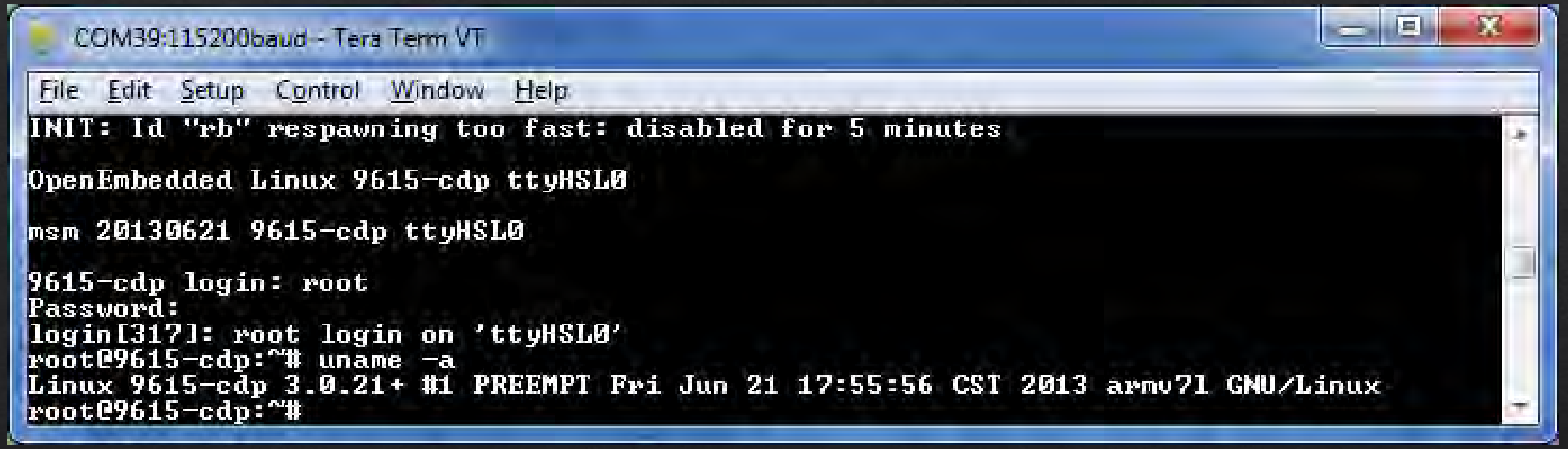
DEF CON 23
LAS VEGAS





DEF CON 23 LAS VEGAS

Got root shell!



DEF CON 23 LAS VEGAS

Happy shell dance



DEF CON 23 LAS VEGAS

Obligatory success meme



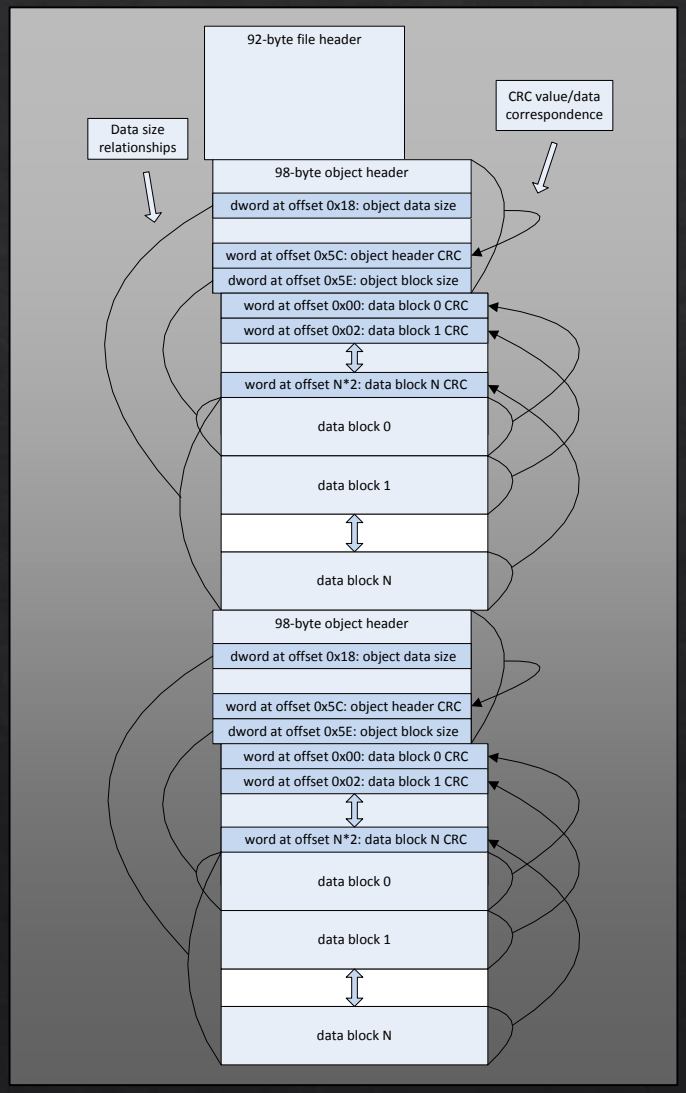
DEF CON 23 LAS VEGAS

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



DEF CON 23 LAS VEGAS

Firmware structure





DEF CON 23 LAS VEGAS

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
- Total op code change = 6 (not including NOP padding)



DEF CON 23 LAS VEGAS

Summary

- We had a cool demo!
- There is such a thing as an insider threat, literally.
- Secure your firmware updates.

DEF CON 23 LAS VEGAS

Questions?

