Anonymizing your hacktop

A brief tour of unique identifiers accessible by software

Kenny McElroy
Security BSides PDX 2012

@

Unique Identifiers

- Who cares?
- What are we talking about?
- Where are they?
  - Laptops & Desktops
  - Peripherals
  - Smartphones
- Why change?
- How do we read/change them?

Who cares?

- Privacy advocates
- Anti-theft engineers
- Datacenter managers
- Equipment RMA departments
- Copy protection engineers
- European Parliament
- Even some end users

The Pentium III Processor. The chip with a serial number that tells the outside world exactly who you are.

©1999 www.jokewallpaper.com

What are we talking about?

Unique identifiers in this presentation are:

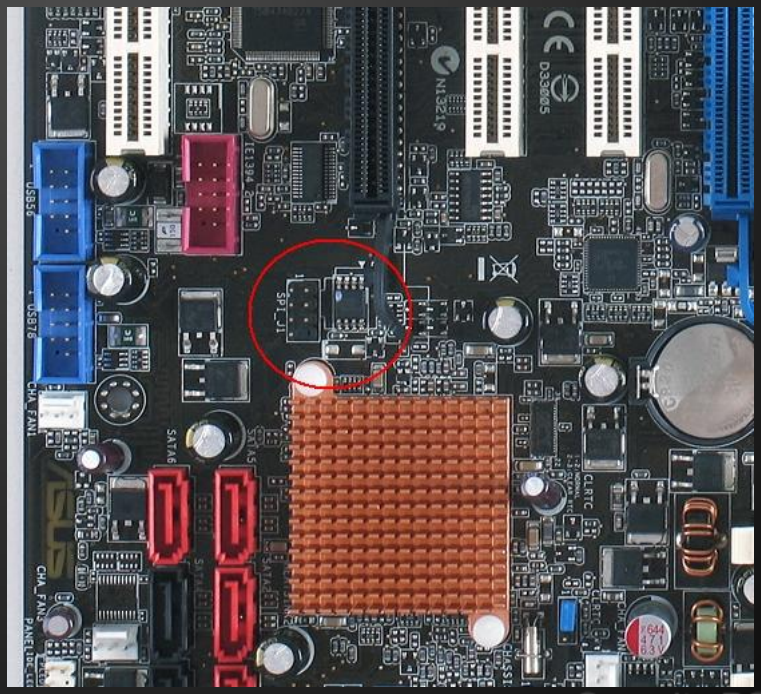
- Small (~32 bytes or less)
- Not digests or fingerprints
- Persistent
- Defined by manufacturer

Where are they? (Laptops/Desktops)

- Motherboard Serial
- PCIe Device Serial Number
- DIMM SPD serial number
- Hard Disk Drive serial
- Network hardware addresses

Motherboard Serial

- Rarely unique on consumer products
- Defined in System Management BIOS spec
- Frequently stored on SPI flash



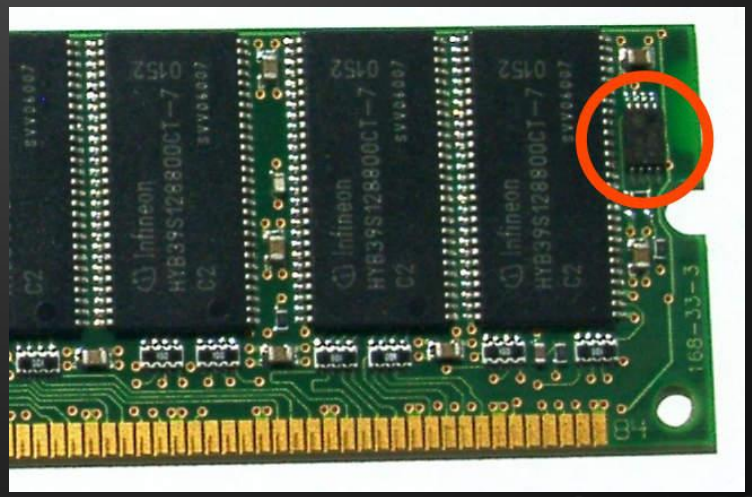
PCIe Device Serial Number

- Optional Enhanced Capability Header
- Not implemented in many PCIe devices
- 64-bit extended unique identifier
  - 24-bit company id assigned by IEEE
  - 40-bit extension identifier assigned by manufacturer
- Storage is implementation specific
  - Likely found on I²C/SPI EEPROM

Memory module serial number

DDR3 DIMM SPD:

- 16-bit manufacturer ID
- 8-bit manufacture location
- 16-bit year/week of manufacture
- 32-bit serial number
- I²C* EEPROM



*SMBus

Hard Disk Drive serial number

ATA/ATAPI:

- 20 ASCII characters serial number
- 40 character model number

SCSI:

- 8-byte Drive Serial Number
- 16-byte Product Identification

Network hardware addresses

MAC-48 / EUI-48 48-bit address:

- Ethernet - 802.3*
- WiFi - 802.11*
- WiMax - 802.16*
- most IEEE 802 networks

EUI-64 64-bit address:

- FireWire
- IPv6
- ZigBee

Where are they? (Peripherals)

- Display EDID
- Software protection dongles
- RFID

Display EDID

Extended Display Identification Data v1.3:

- 16-bit manufacturer ID
- 16-bit product ID
- 16-bit year/week of manufacture
- 32-bit serial number

Software protection dongles

- Tough to change, by design
- Easy to read

Where are they? (Smartphones)

- International Mobile Subscriber Identity
  - Country Code, Carrier Code, Subscriber Number
- GSM (T-Mobile, AT&T)
  - International Mobile Equipment Identity (handset)
  - Integrated Circuit Card IDentifier (SIM)
- CDMA (Sprint, Verizon, Cricket)
  - Mobile Equipment IDentifier
- Apple
  - Unique Device IDentifier

Why change?

- Well, you probably shouldn't
- Popular belief says you can't
- It will probably break stuff anyway
- What good will it do you?

How do we read them?

Linux:

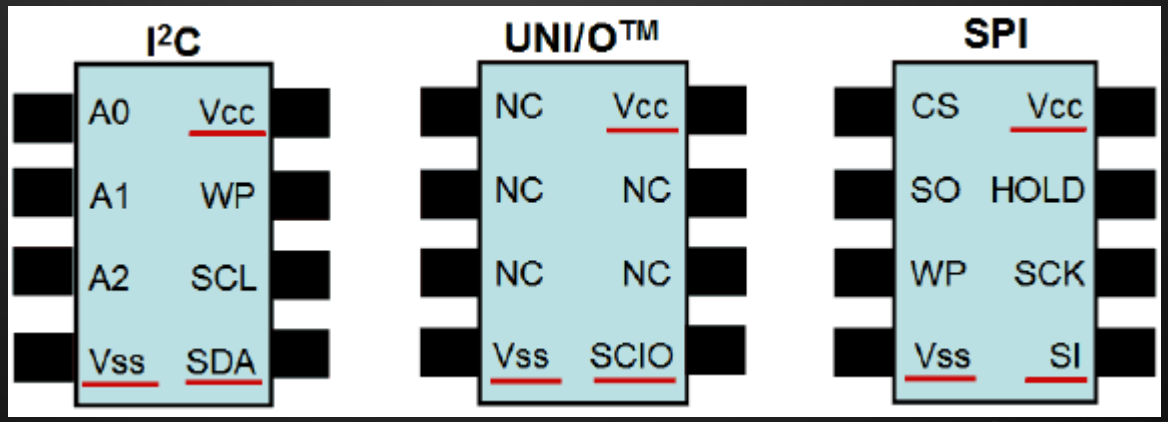
- lshw
- dmidecode
- hwinfo
- lspci -v
- lsusb -v

Windows:

- Device Manager
- EVEREST
- AIDA64

How do we change them?

- Software
- BusPirate
- GoodFET
- Arduino
- Just about any devkit



Questions?

I would love to hear about your success stories ...or failures. kenny@romhat.net

Who wants to have a workshop?

Thanks!