HACKITO
ERGO SUM

THE HIDDEN DANGERS INSIDE THE PLATFORM

HACKITO ERGO SUM

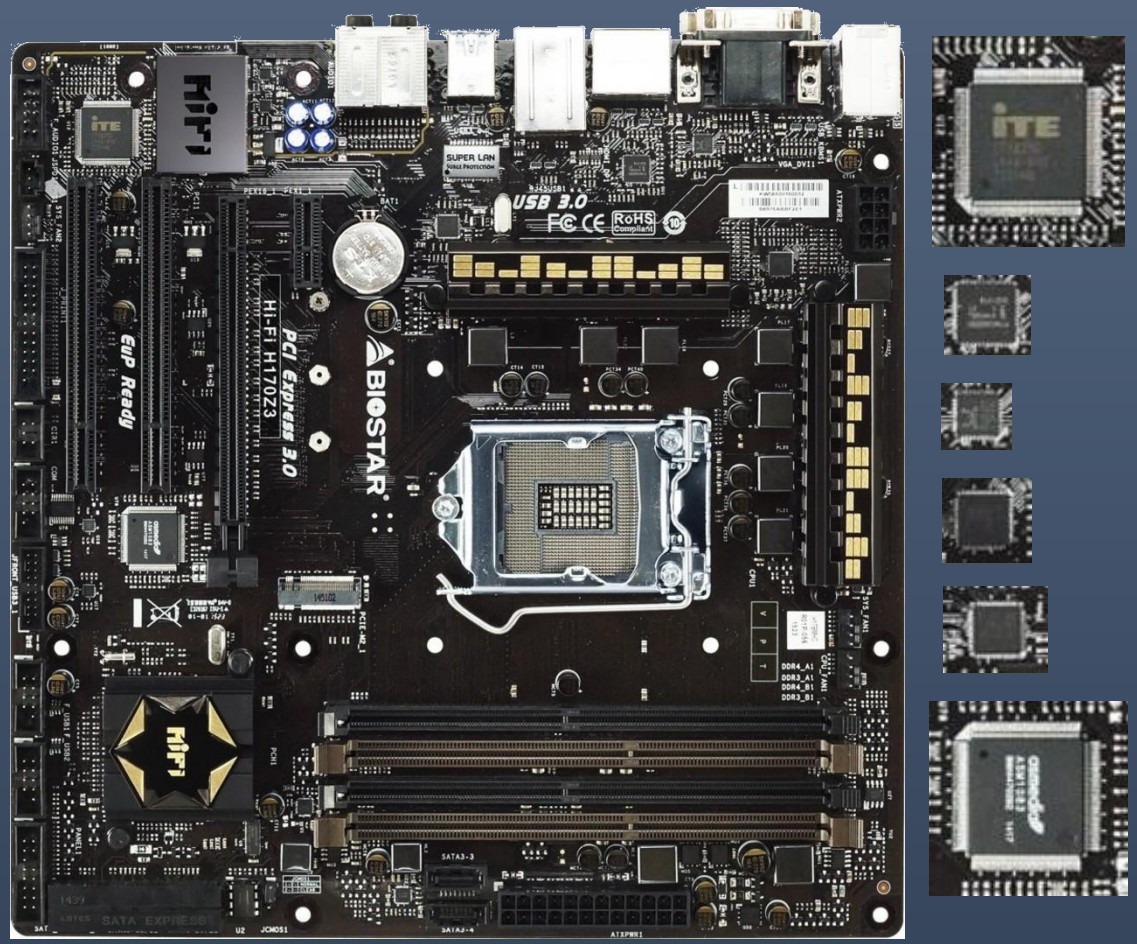
Who are we

HACKITO ERGO SUM

Classic platforms

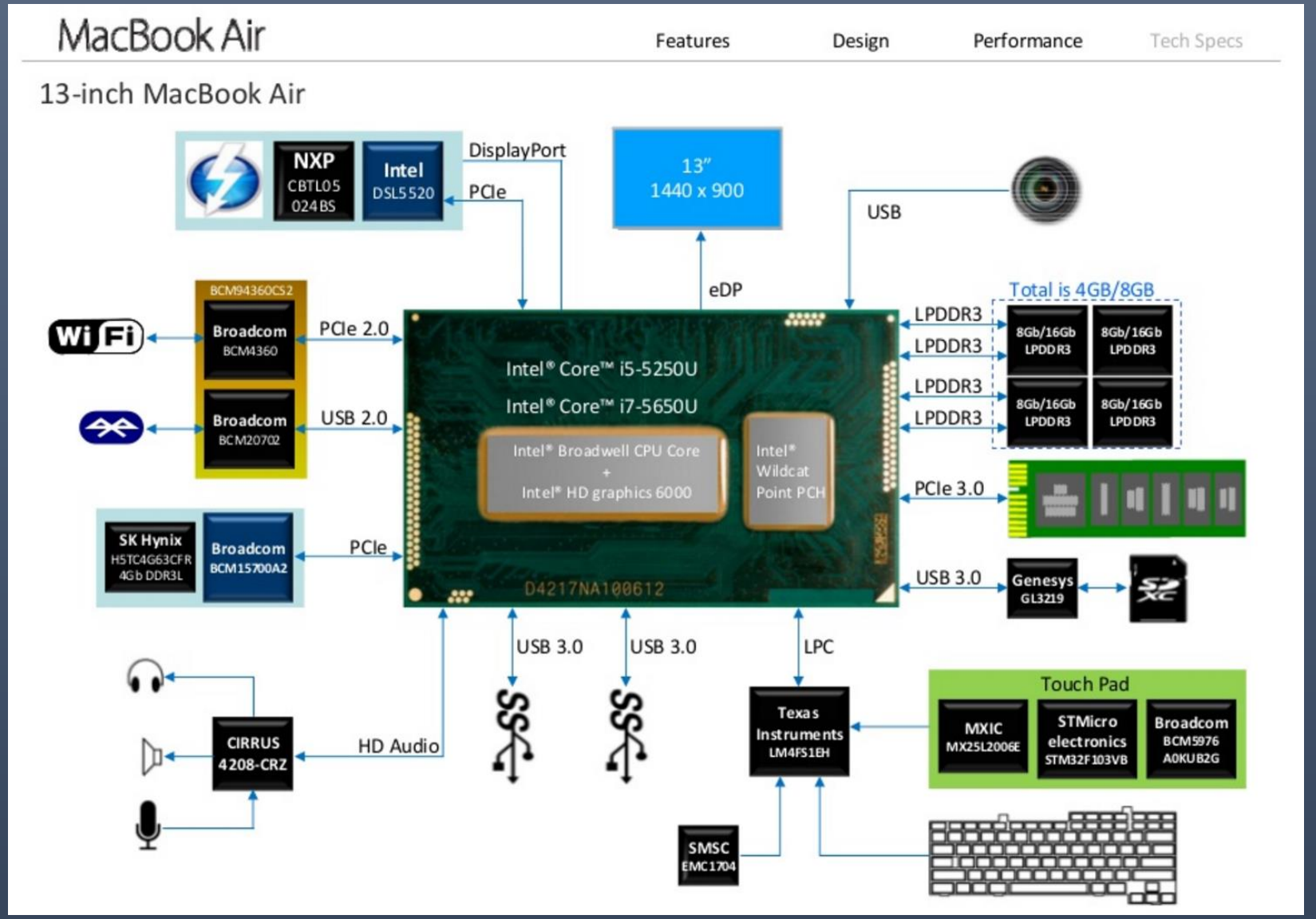
HACKITO ERGO SUM

Classic platform



HACKITO ERGO SUM

Modern platform



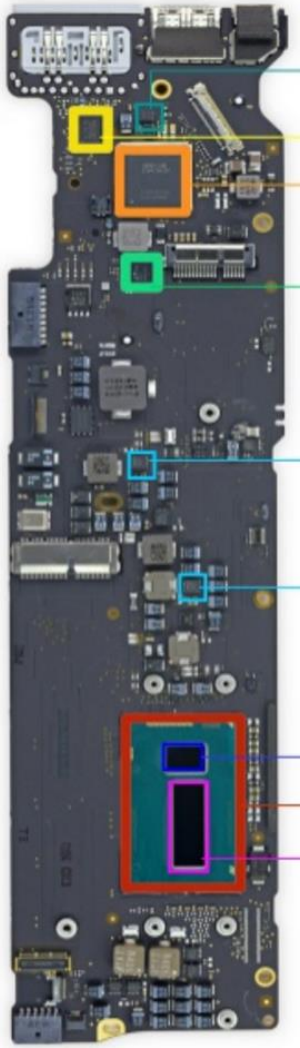
HACKITO ERGO SUM

Modern platform

MacBook Air

Features Design Performance Tech Specs

13-inch MacBook Air



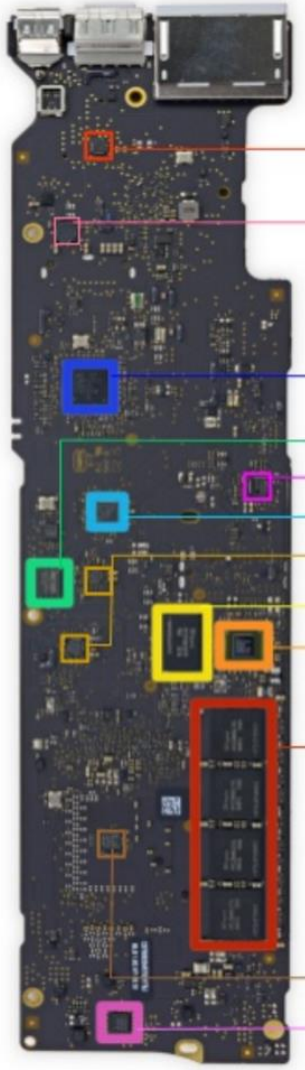
HACKITO ERGO SUM

Modern platform

MacBook Air

Features Design Performance Tech Specs

13-inch MacBook Air



- NXP CBTL05024BS
- Texas Instruments CD3211
- Texas Instruments Stellaris LM4FS1AH
- Macronix MX25L6473E serial multi I/O, 64 Mb flash memory
- Intersil ISL6259
- Texas Instruments TPS51980A
- Texas Instruments 51916
- SK Hynix H5TC4G63AFR ,4Gb DDR3L
- Broadcom BCM15700A2
- Four 8/16Gb LPDDR3-1600 chips.
  8Gb: SK Hynix H9CCNNN8JTALAR
- Total is up to 4GB/8GB density.
- SMSC EMC1704
- Intersil ISL95826AHRZ

HACKITO ERGO SUM

Modern platform

MacBook Air

Features Design Performance Tech Specs

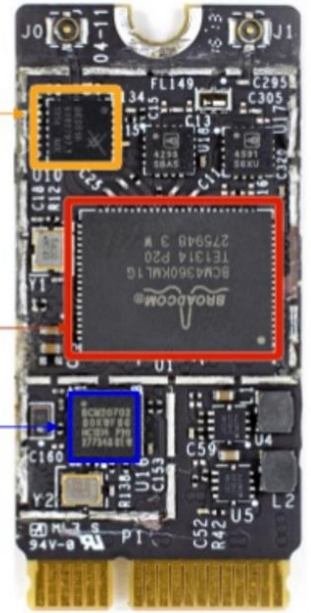
13-inch MacBook Air

PCIe-based SSD

- SAMSUNG S4LN053X01-8030 (ARM core) PCIe NAND Flash controller
- SAMSUNG K4E4E324ED- 4Gb LPDDR3
- SAMSUNG K9LDGY8S1D-XCK0 16GB NAND flash

Total is 128GB density.

WiFi/BT Module



- Skyworks SE5516 dual-band 802.11 a/b/g/n/ac WLAN front-end module
- Broadcom BCM4360 802.11ac WiFi chip
- Broadcom BCM20702 BT4.0 chip

Attackers motivation

HACKITO
ERGO SUM

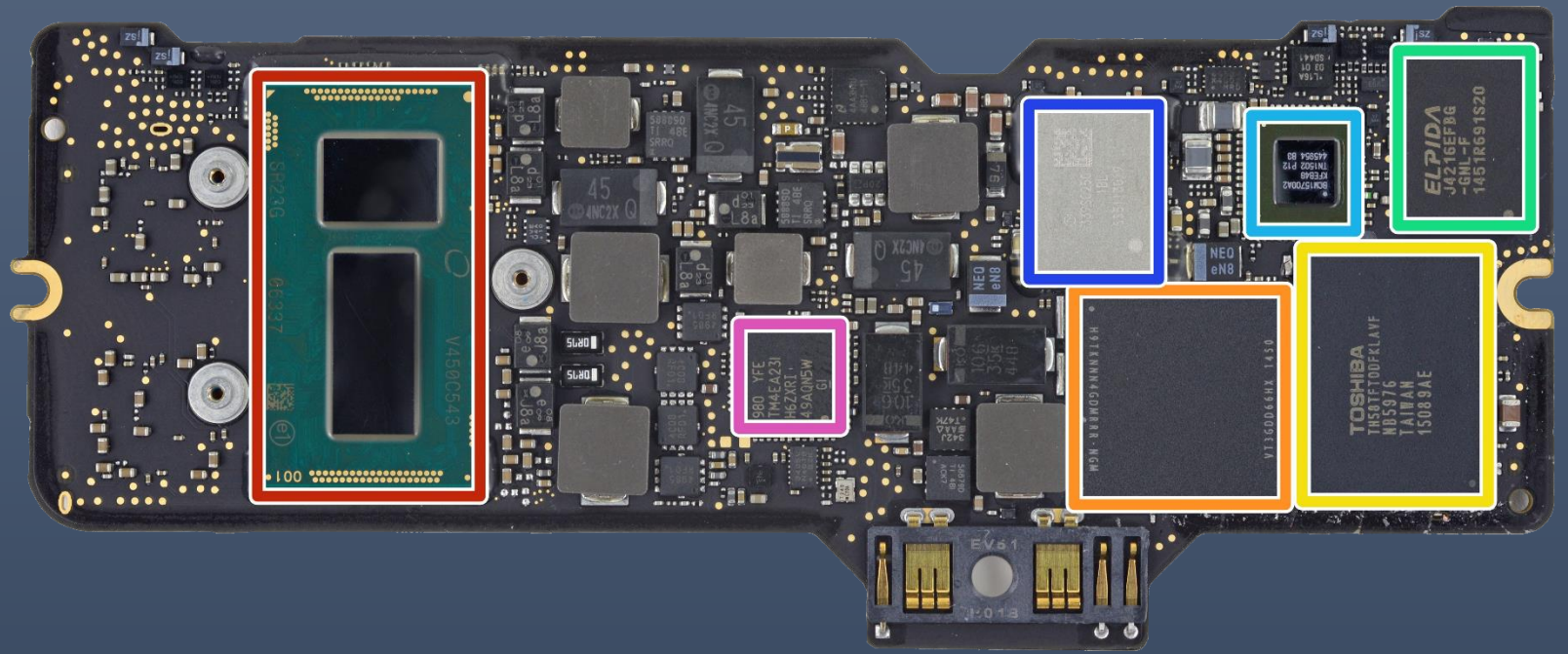
Attackers motivation

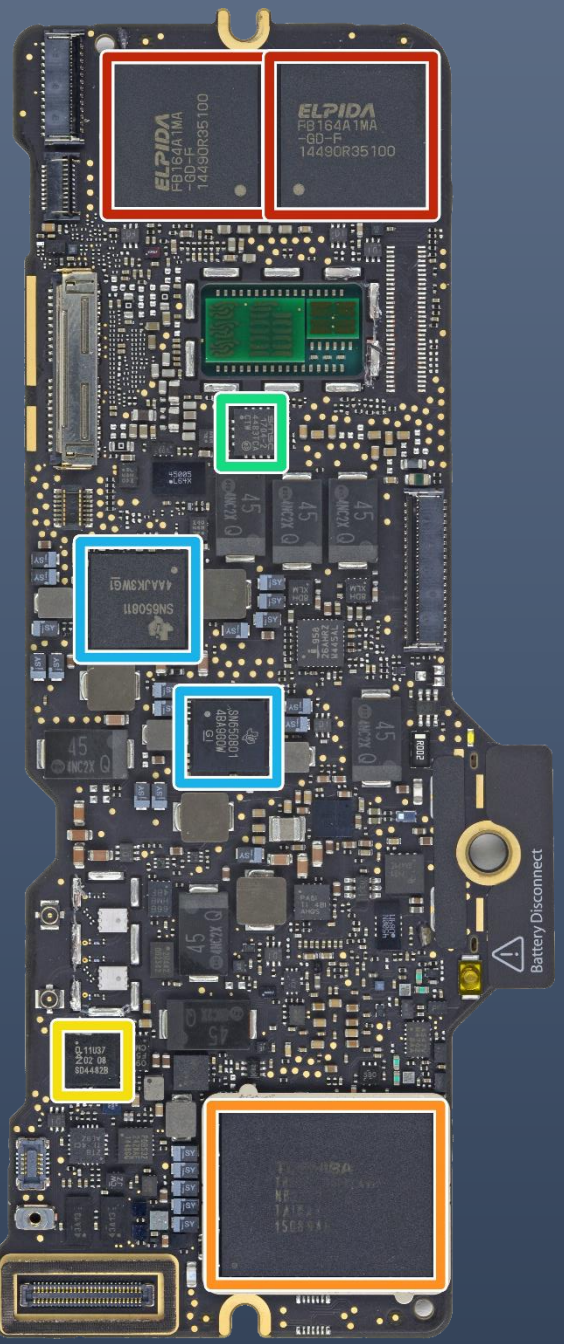
- Stealth
- Persistence
- Low level security bypass
- Data intercepts (USB)
- Side channel spying (sensors etc.)
- Privilege escalation
- VM escape

Attack surface review from the inside

HACKITO ERGO SUM

Modern platform



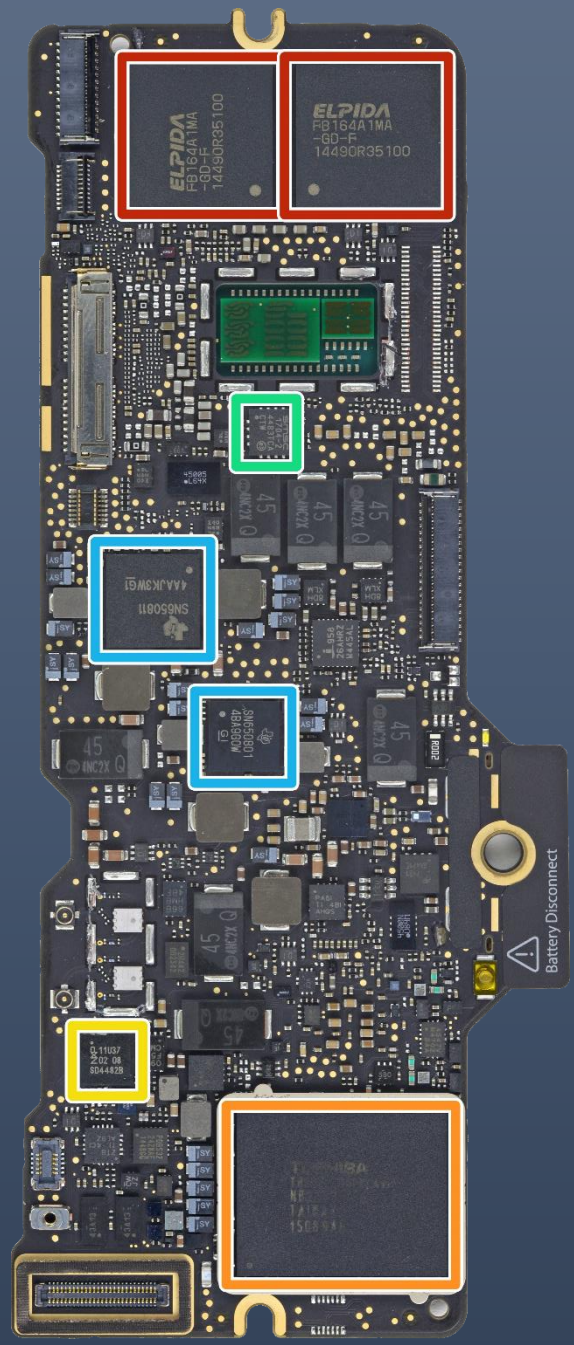


HACKITO ERGO SUM

Modern platform

- Hide a tiny amounts of data in SPD
- OLD attack – change SPD to indicated smaller RAM size and cause memory to wrap around

- Elpida/Micron FB164A1MA-GD-F 8 GB LPDDR3 Mobile RAM
- Toshiba TH58TFT0DFKLAVF NB2953 128 GB MLC NAND Flash memory (+ 128 GB on the reverse side for a total of 256 GB)
- NXP 11U37 microcontroller; 128 kB flash, 10kB SRAM
- SMSC 1704-2 Temperature Sensor
- Texas Instruments SN6508 (probably power converter related to SN6501)



HACKITO ERGO SUM

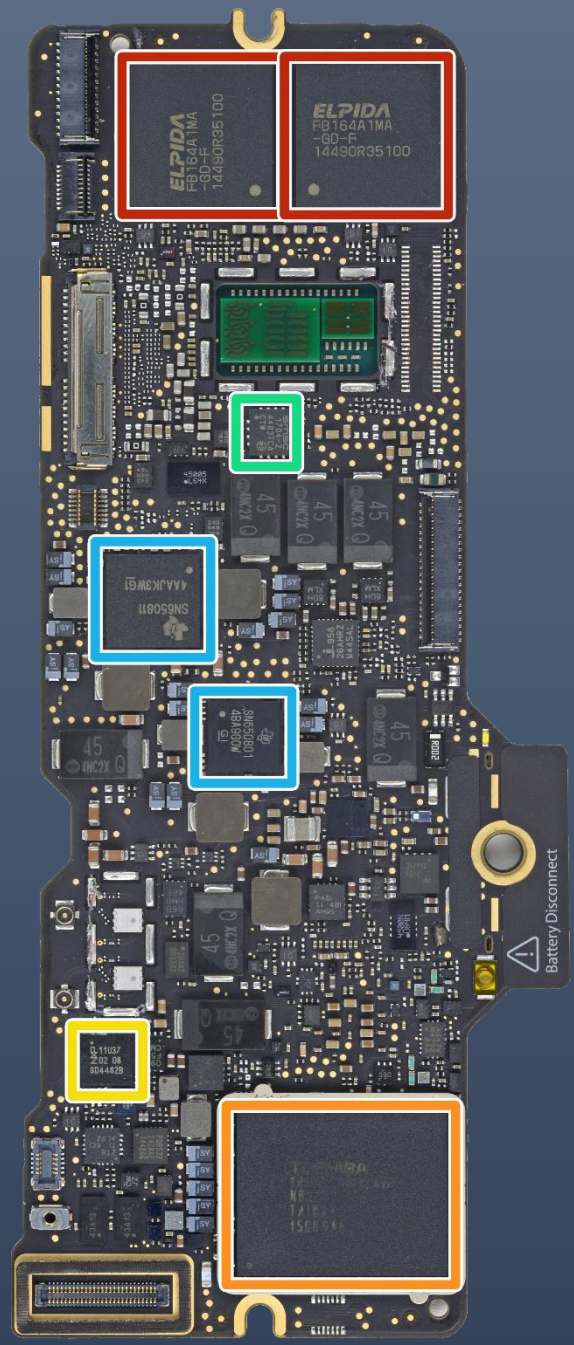
Modern platform

JEDEC Standard No. 84-B51
Page 72

6.6.18 Field Firmware Update

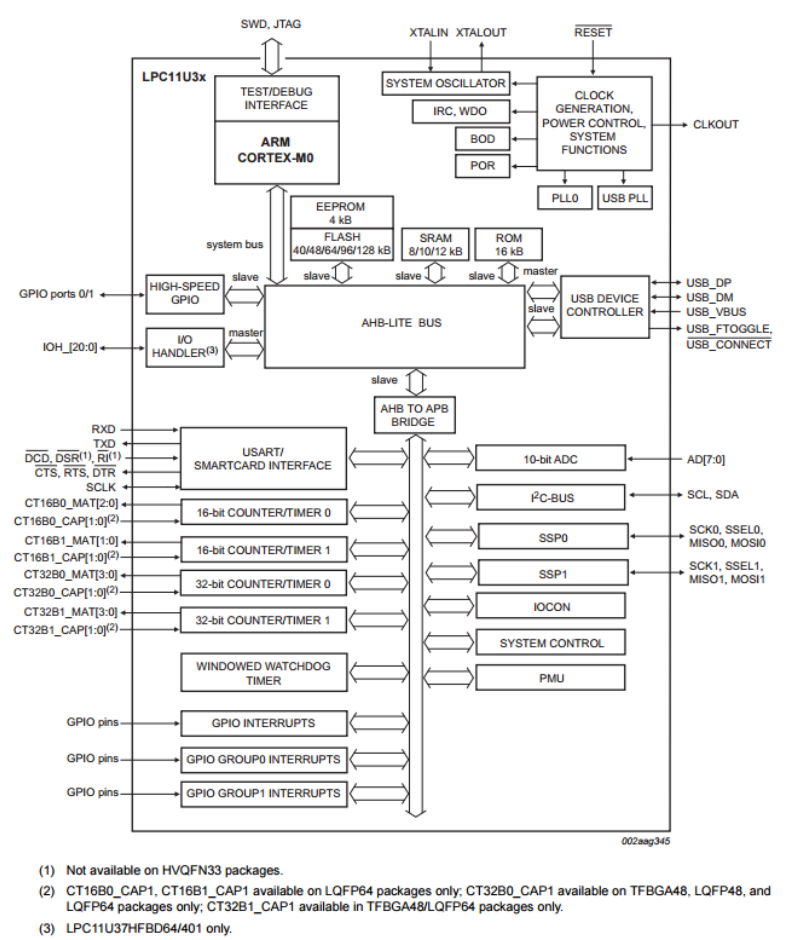
- JEDEC eMMC spec 5.1
  - Introduced FFU
  - FIELD FIRMWARE UPDATE

- Elpida/Micron FB164A1MA-GD-F 8 GB LPDDR3 Mobile RAM
- Toshiba TH58TFT0DFKLAVF NB2953 128 GB MLC NAND Flash memory (+ 128 GB on the reverse side for a total of 256 GB)
- NXP 11U37 microcontroller; 128 kB flash, 10kB SRAM
- SMSC 1704-2 Temperature Sensor
- Texas Instruments SN6508 (probably power converter related to SN6501)



HACKITO ERGO SUM

Modern platform

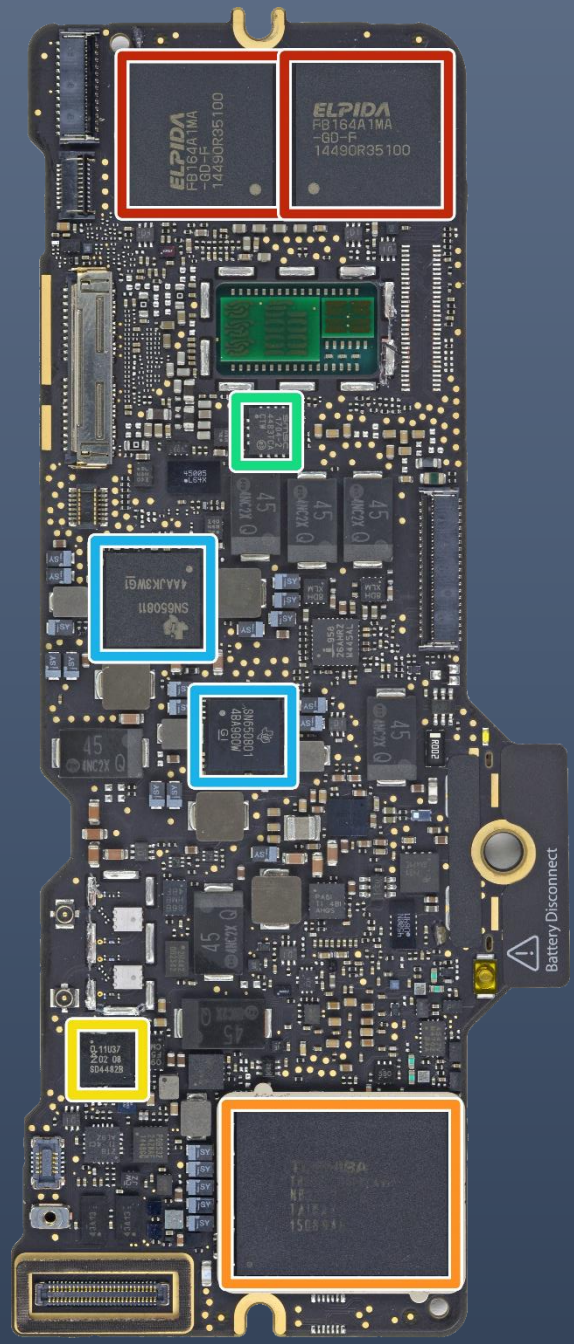


(1) Not available on HVQFN33 packages.

(2) CT16B0_CAP1, CT16B1_CAP1 available on LQFP64 packages only; CT32B0_CAP1 available on TFBGA48, LQFP48, and LQFP64 packages only; CT32B1_CAP1 available in TFBGA48/LQFP64 packages only.

(3) LPC11U37HFBD64/401 only.

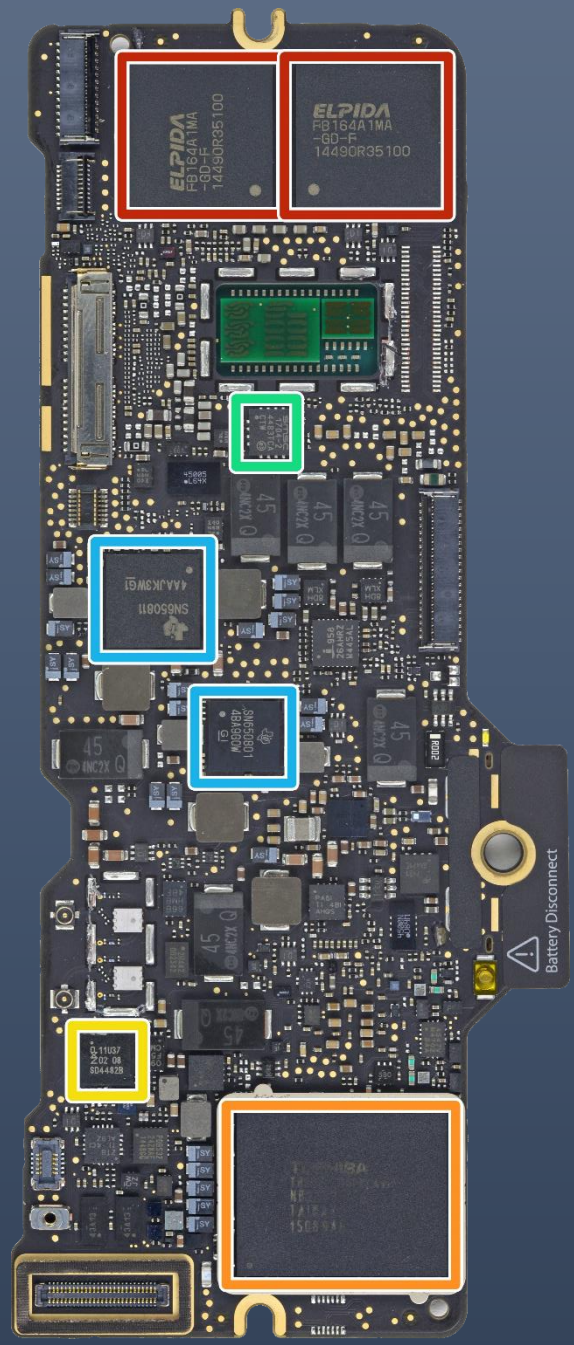
- Elpida/Micron FB164A1MA-GD-F 8 GB LPDDR3 Mobile RAM
- Toshiba TH58TFT0DFKLAVF NB2953 128 GB MLC NAND Flash memory (+ 128 GB on the reverse side for a total of 256 GB)
- NXP 11U37 microcontroller; 128 kB flash, 10kB SRAM
- SMSC 1704-2 Temperature Sensor
- Texas Instruments SN6508 (probably power converter related to SN6501)



HACKITO ERGO SUM

Modern platform

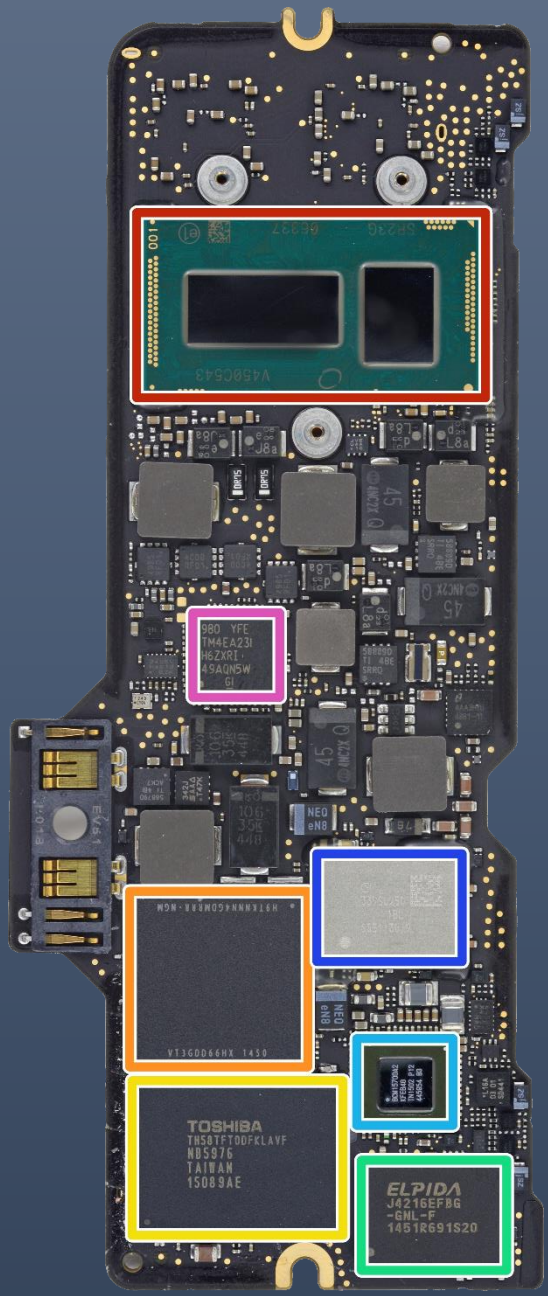
- Elpida/Micron FB164A1MA-GD-F 8 GB LPDDR3 Mobile RAM
- Toshiba TH58TFT0DFKLAVF NB2953 128 GB MLC NAND Flash memory (+ 128 GB on the reverse side for a total of 256 GB)
- NXP 11U37 microcontroller; 128 kB flash, 10kB SRAM
- SMSC 17[illegible]mperat[illegible]ensor
- Texas I[illegible]ument[illegible]508[illegible]obably power c[illegible]rter rel[illegible]6501)



HACKITO ERGO SUM

Modern platform

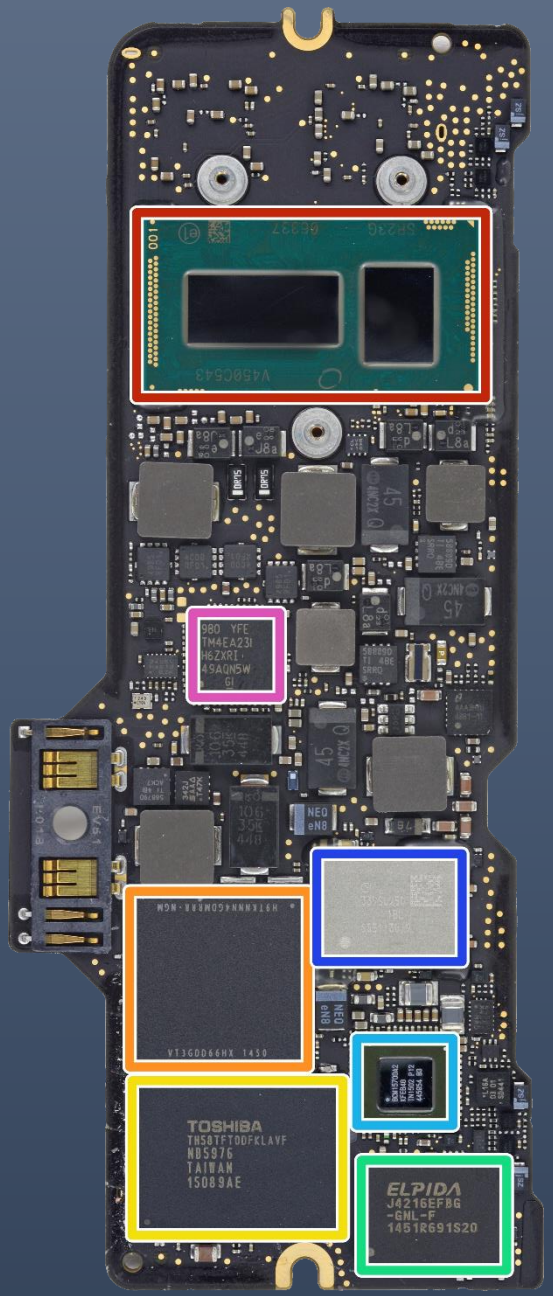
- Intel SR23G Core M-5Y31 CPU (Dual-Core, 1.1 GHz, Turbo Boost up to 2.4 GHz) with Intel HD Graphics 5300
- SK Hynix H9TKNNN4GDMRRR-NGM 4 Gb (512 MB) LPDDR2-SDRAM
- Toshiba TH58TFT0DFKLAVF 128 GB MLC NAND Flash
- Elpida/Micron J4216EFBG-GNL-F DDR3 SDRAM
- Broadcom BCM15700A2, appears to be a wireless networking chipset
- Murata 339S0250 (Likely an iteration of the 339S02541 Wi-Fi module found in the iPad Air 2)
- Texas Instruments/Stellaris LM4FS1EH SMC Controller (Replacement codename for TM4EA231)



HACKITO ERGO SUM

Modern platform

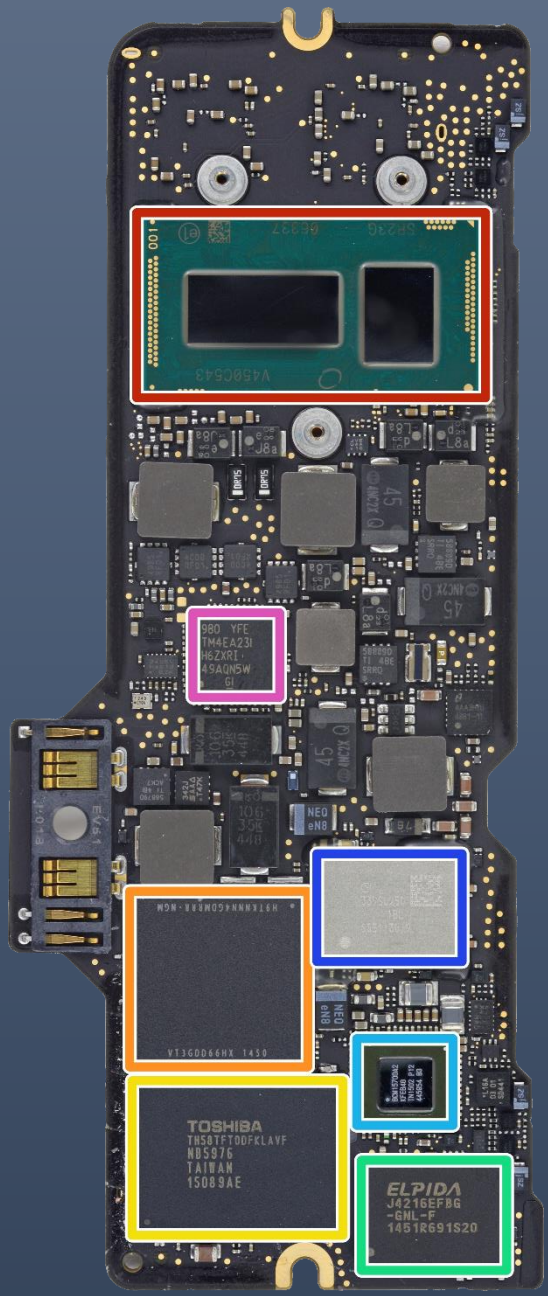
- Intel SR23G Core M-5Y31 CPU (Dual-Core, 1.1 GHz, Turbo Boost up to 2.4 GHz) with Intel HD Graphics 5300
- SK Hynix H9TKNNN4GDMRRR-NGM 4 Gb (512 MB) LPDDR2-SDRAM
- Toshiba TH58TFT0DFKLAVF 128 GB MLC NAND Flash
- Elpida/Micron J4216EFBG-GNL-F DDR3 SDRAM
- Broadcom BCM15700A2, appears to be a wireless networking chipset
- Murata 339S0250 (Likely an iteration of the 339S02541 Wi-Fi module found in the iPad Air 2)
- Texas Instruments/Stellaris LM4FS1EH SMC Controller (Replacement codename for TM4EA231)



HACKITO ERGO SUM

Modern platform

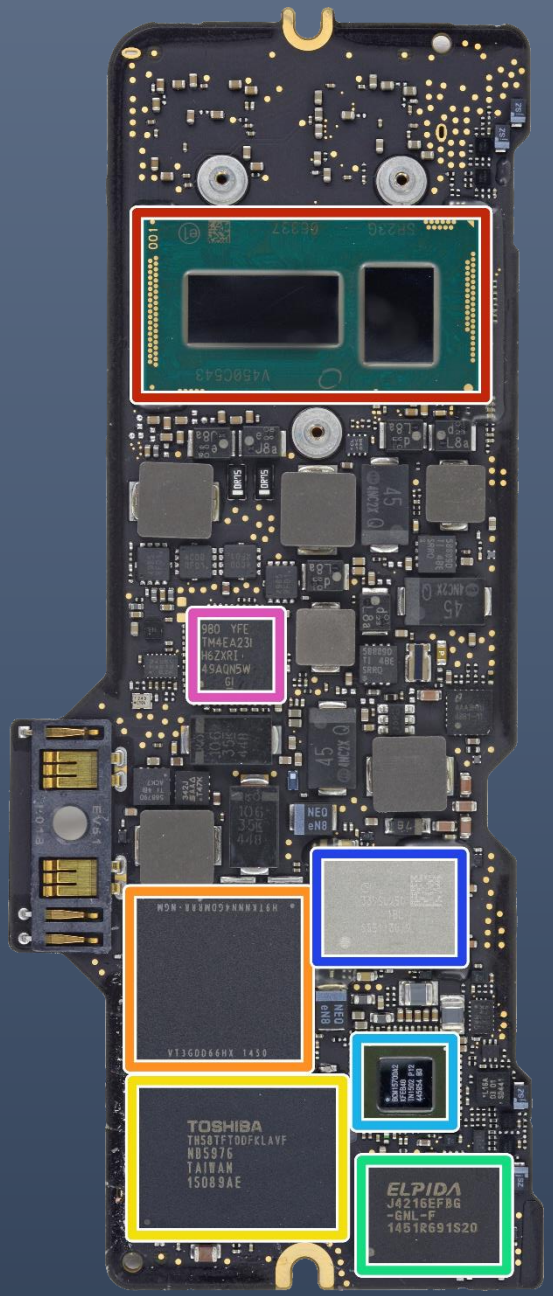
- Intel SR23G Core M-5Y31 CPU (Dual-Core, 1.1 GHz, Turbo Boost up to 2.4 GHz) with Intel HD Graphics 5300
- SK Hynix H9TKNNN4GDMRRR-NGM 4 Gb (512 MB) LPDDR2-SDRAM
- Toshiba TH58TFT0DFKLAVF 128 GB MLC NAND Flash
- Elpida/Micron J4216EFBG-GNL-F DDR3 SDRAM
- Broadcom BCM15700A2, appears to be a wireless networking chipset
- Murata 339S0250 (Likely an iteration of the 339S02541 Wi-Fi module found in the iPad Air 2)
- Texas Instruments/Stellaris LM4FS1EH SMC Controller (Replacement codename for TM4EA231)



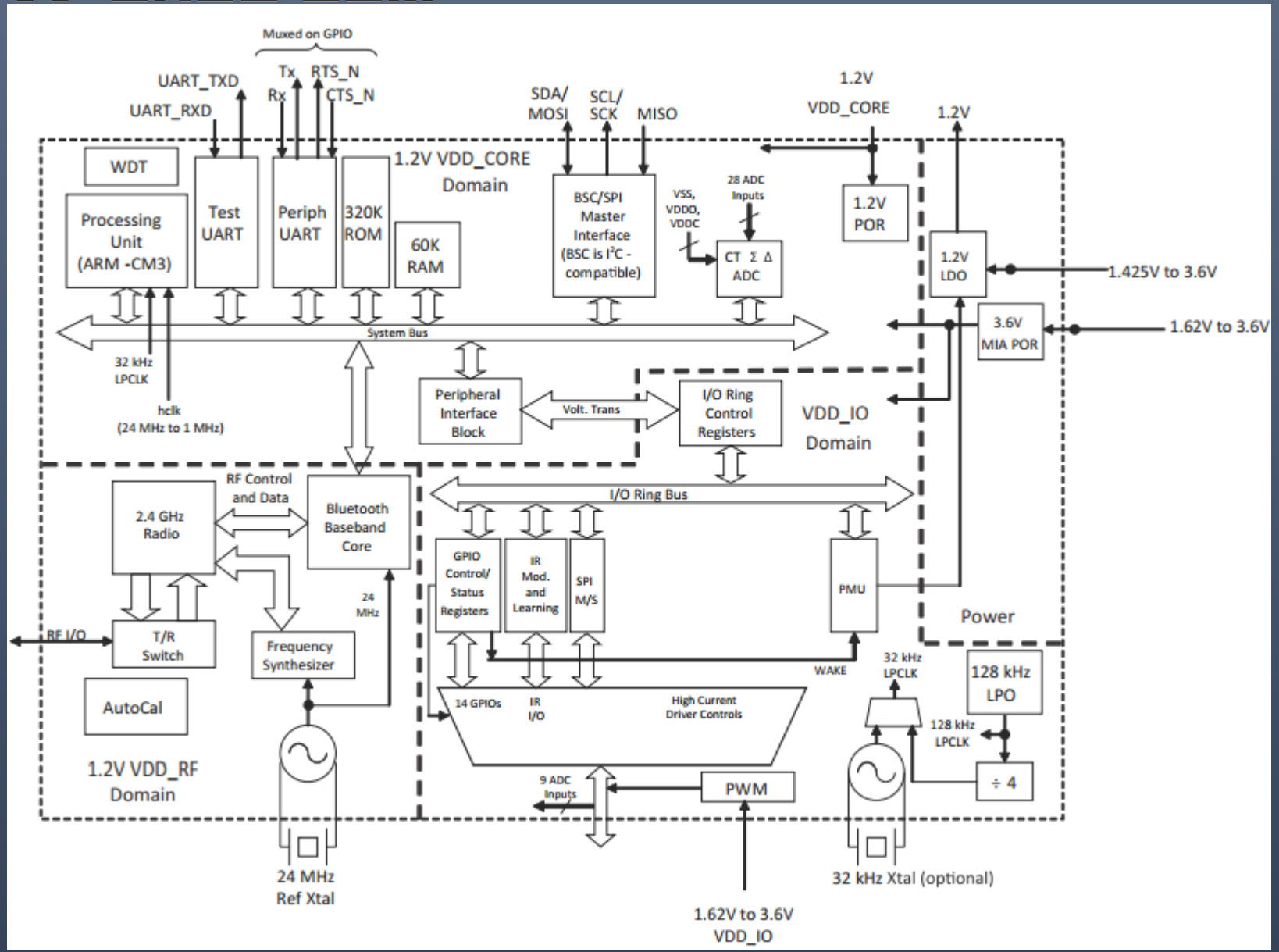
HACKITO ERGO SUM

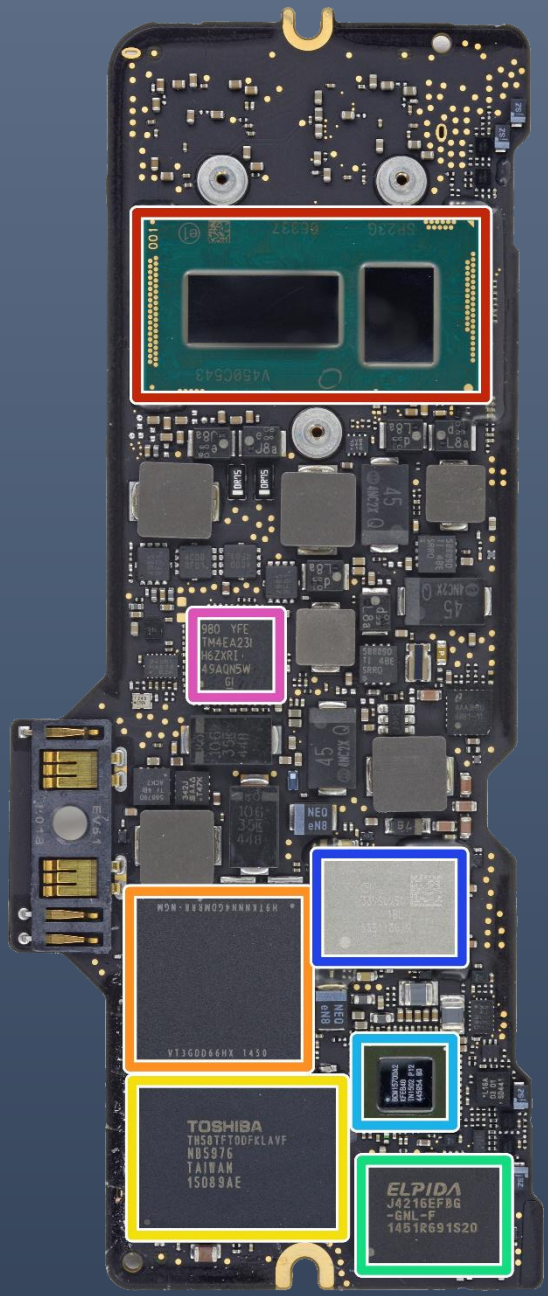
Modern platform

- Intel SR23G Core M-5Y31 CPU (Dual-Core, 1.1 GHz, Turbo Boost up to 2.4 GHz) with Intel HD Graphics 5300
- SK Hynix H9TKNNN4GDMRRR-NGM 4 Gb (512 MB) LPDDR2-SDRAM
- Toshiba TH58TFT0DFKLAVF 128 GB MLC NAND Flash
- Elpida/Micron J4216EFBG-GNL-F DDR3 SDRAM
- Broadcom BCM15700A2, appears to be a wireless networking chipset
- Murata 339S0250 (Likely an iteration of the 339S02541 Wi-Fi module found in the iPad Air 2)
- Texas Instruments/Stellaris LM4FS1EH SMC Controller (Replacement codename for TM4EA231)



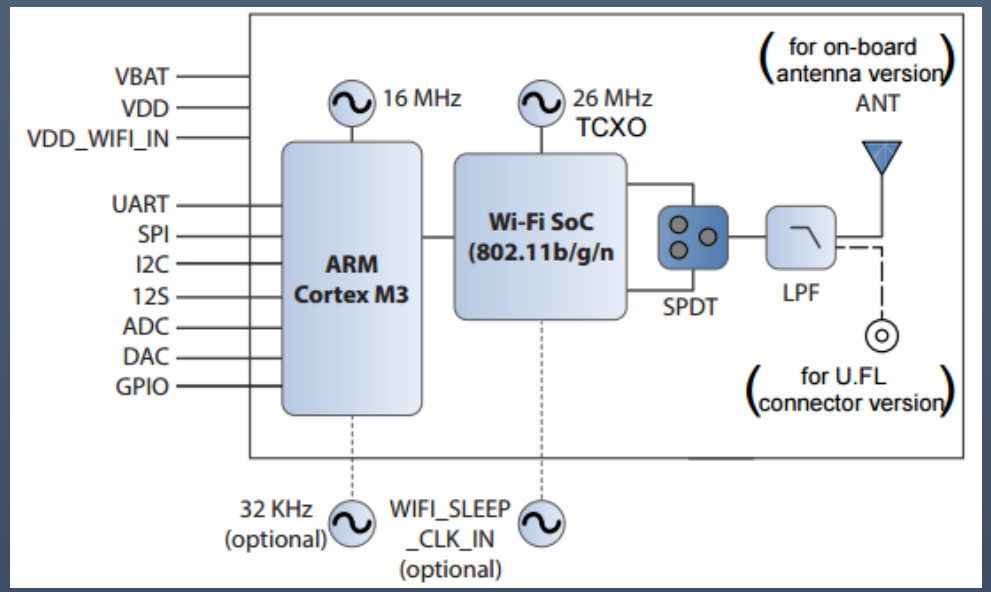
HACKITO ERGO SUM



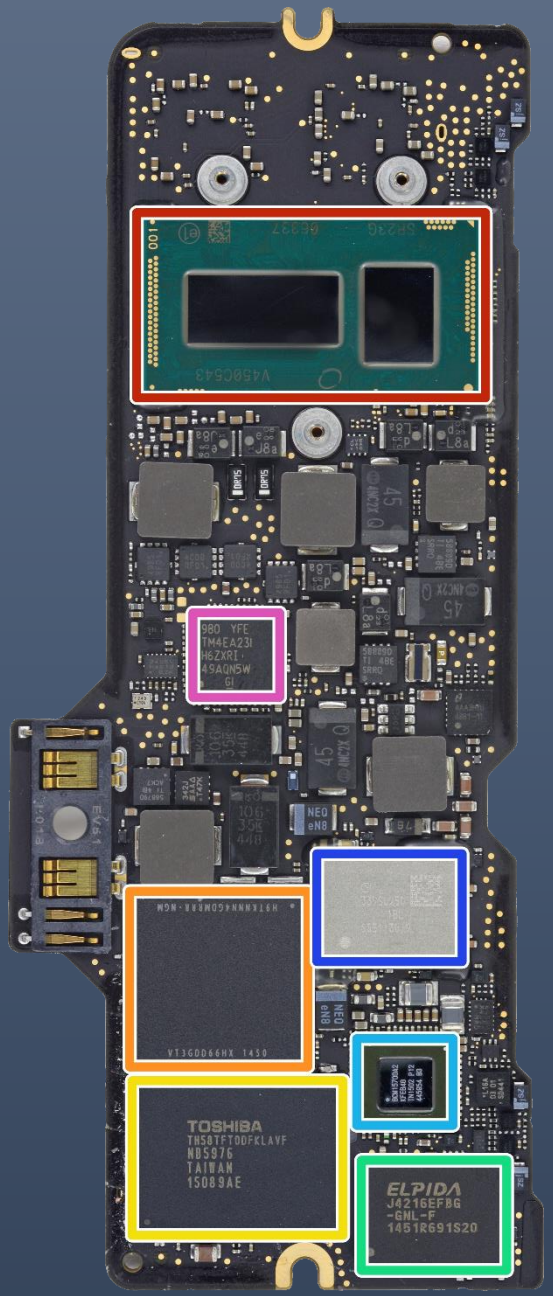


HACKITO ERGO SUM

Modern platform

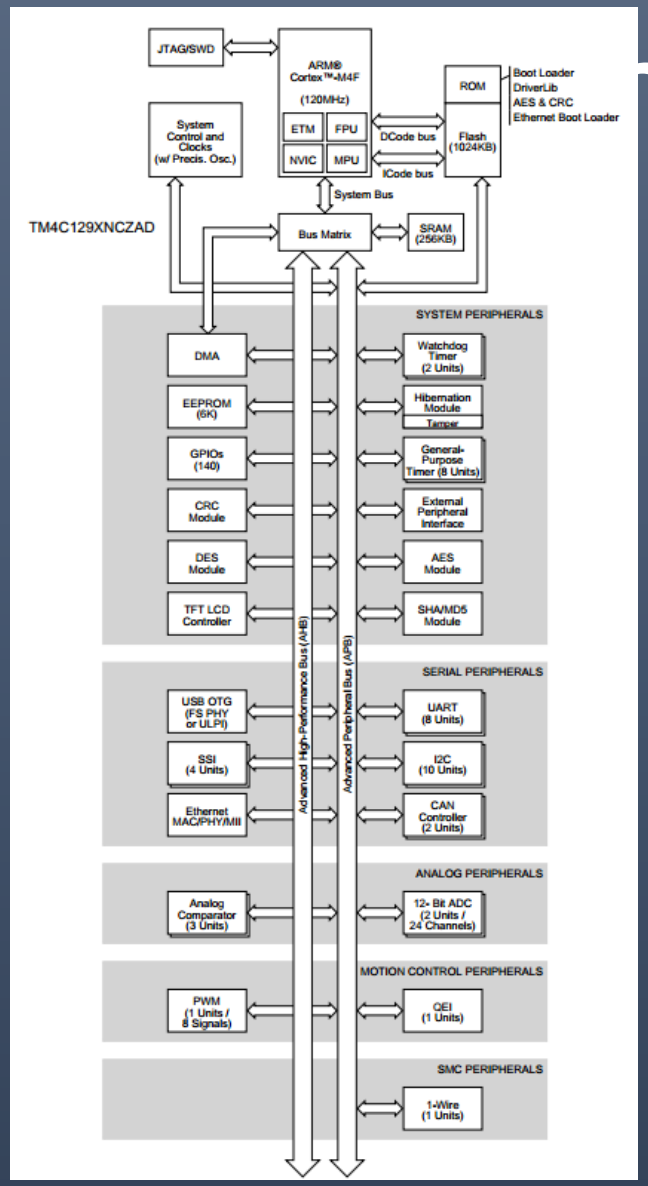


- Intel SR23G Core M-5Y31 CPU (Dual-Core, 1.1 GHz, Turbo Boost up to 2.4 GHz) with Intel HD Graphics 5300
- SK Hynix H9TKNNN4GDMRRR-NGM 4 Gb (512 MB) LPDDR2-SDRAM
- Toshiba TH58TFT0DFKLAVF 128 GB MLC NAND Flash
- Elpida/Micron J4216EFBG-GNL-F DDR3 SDRAM
- Broadcom BCM15700A2, appears to be a wireless networking chipset
- Murata 339S0250 (Likely an iteration of the 339S02541 Wi-Fi module found in the iPad Air 2)
- Texas Instruments/Stellaris LM4FS1EH SMC Controller (Replacement codename for TM4EA231)

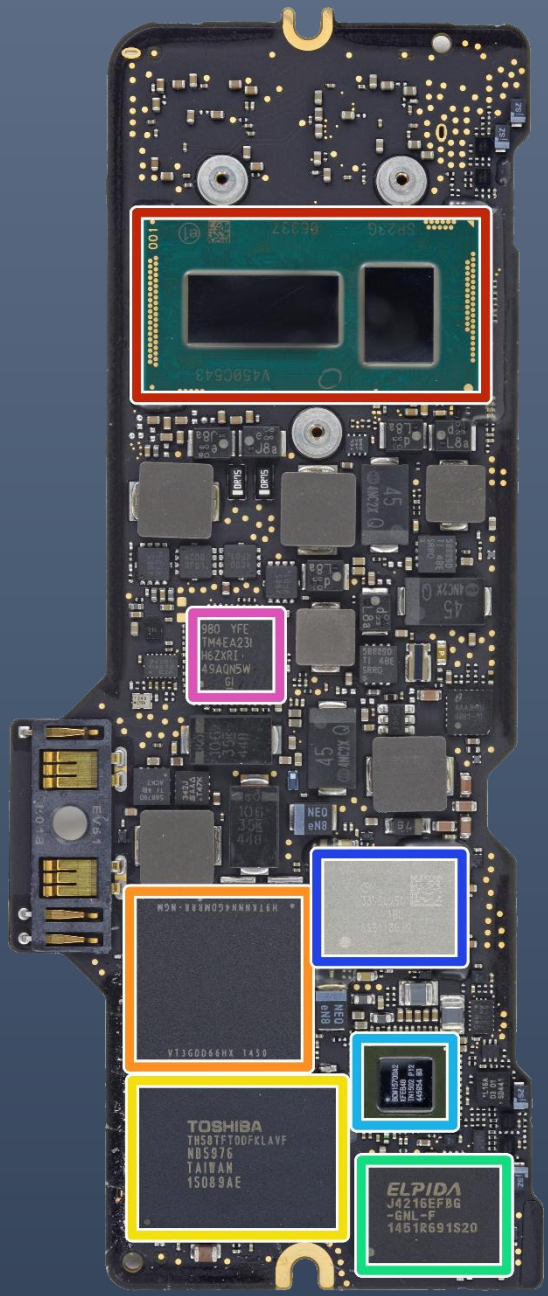


HACKITO ERGO SUM

h platform



- Intel SR23G Core M-5Y31 CPU (Dual-Core, 1.1 GHz, Turbo Boost up to 2.4 GHz) with Intel HD Graphics 5300
- SK Hynix H9TKNNN4GDMRRR-NGM 4 Gb (512 MB) LPDDR2-SDRAM
- Toshiba TH58TFT0DFKLAVF 128 GB MLC NAND Flash
- Elpida/Micron J4216EFBG-GNL-F DDR3 SDRAM
- Broadcom BCM15700A2, appears to be a wireless networking chipset
- Murata 339S0250 (Likely an iteration of the 339S02541 Wi-Fi module found in the iPad Air 2)
- Texas Instruments/Stellaris LM4FS1EH SMC Controller (Replacement codename for TM4EA231)



HACKITO ERGO SUM

Modern platform

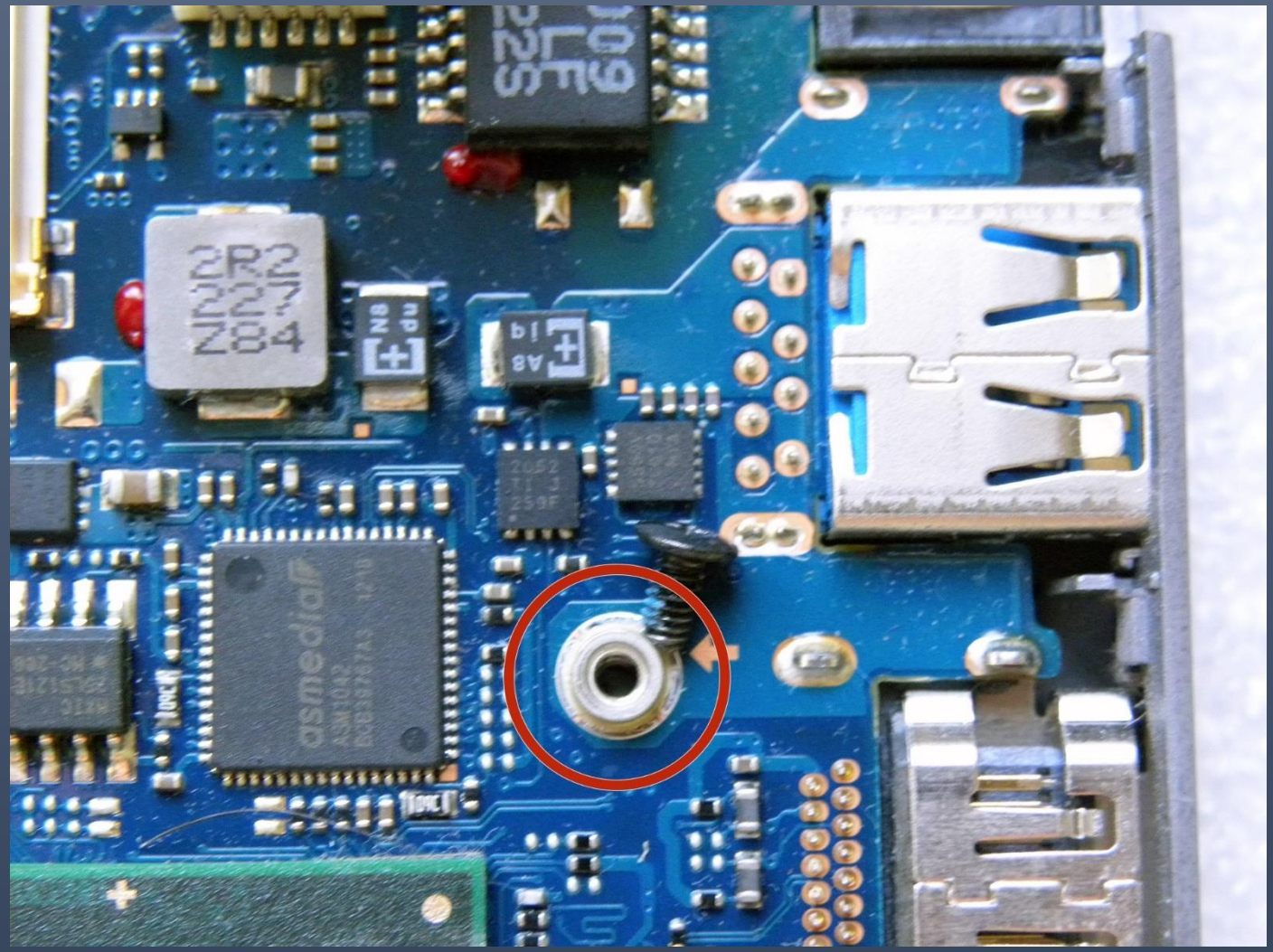
The curious case of “pluggable”

- USB 3.0 SATA dock for external HDD
- Controller used is made by asmedia
- Release a firmware update tool and patch back in 2013

- http://plugable.com/2013/03/05/usb3-sata-u3-firmware-update

HACKITO ERGO SUM

Modern platform

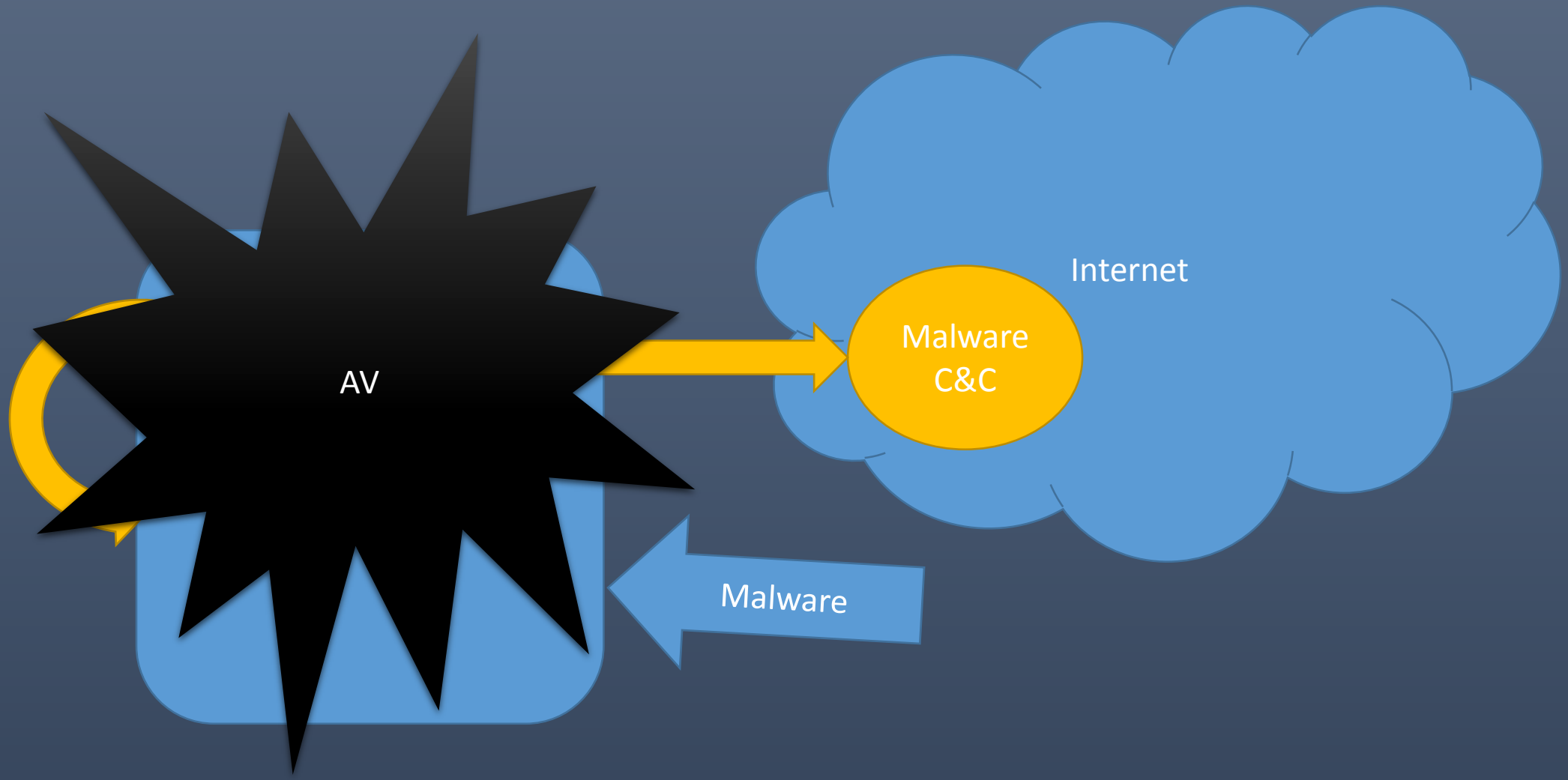


Example

- Malware gets installed on a platform via phishing etc.
  - It detects a vulnerable platform component.
    - Then uses that component for persistence on the device.

HACKITO ERGO SUM

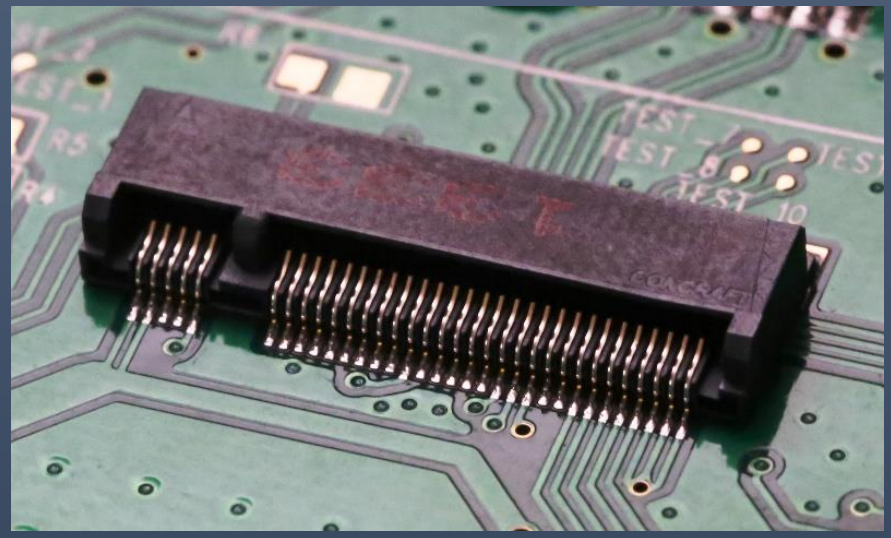
DEMO



HACKITO
ERGO SUM

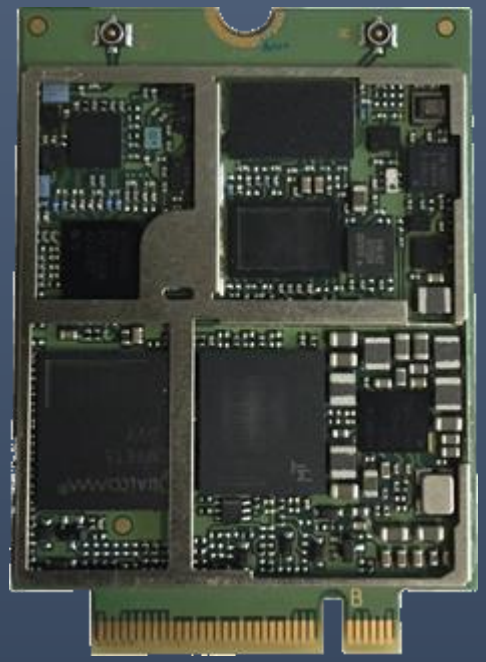
HACKITO ERGO SUM

- Internal Huawei LTE modem
  - Connected via USB interface in M.2 socket

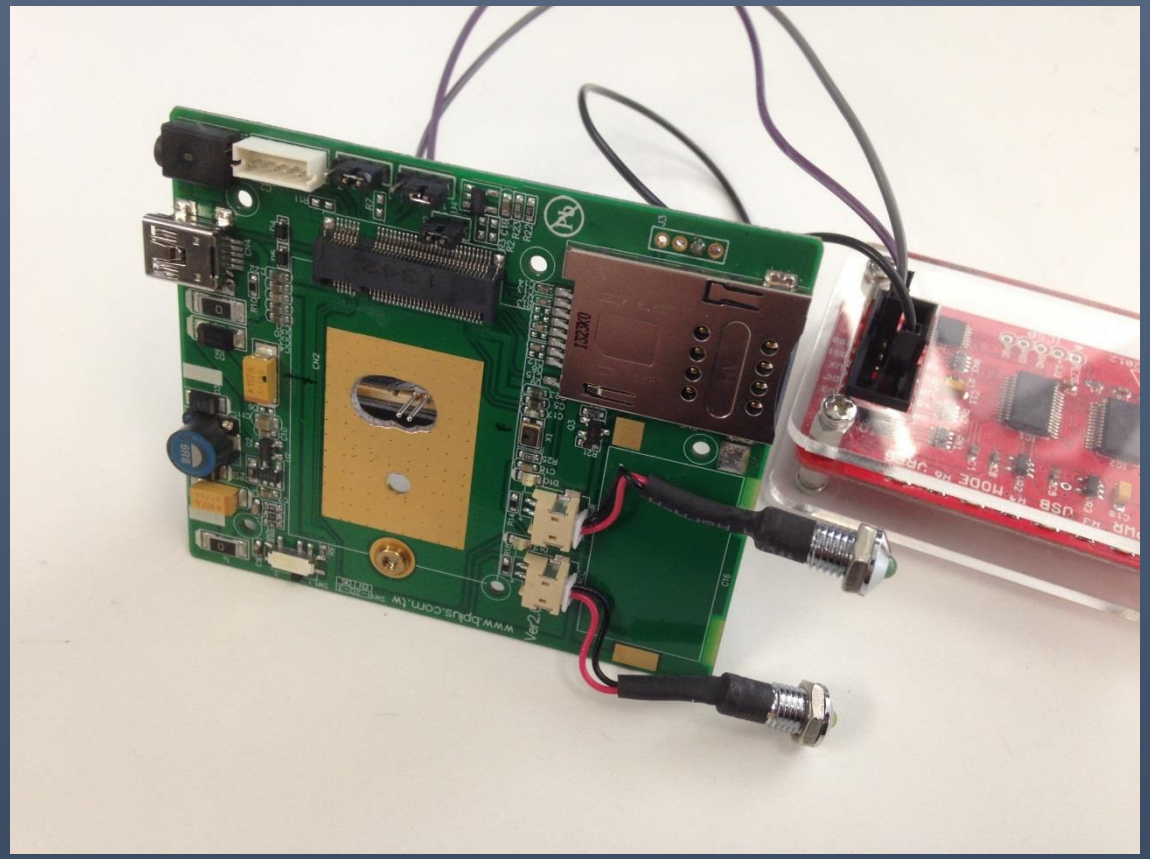


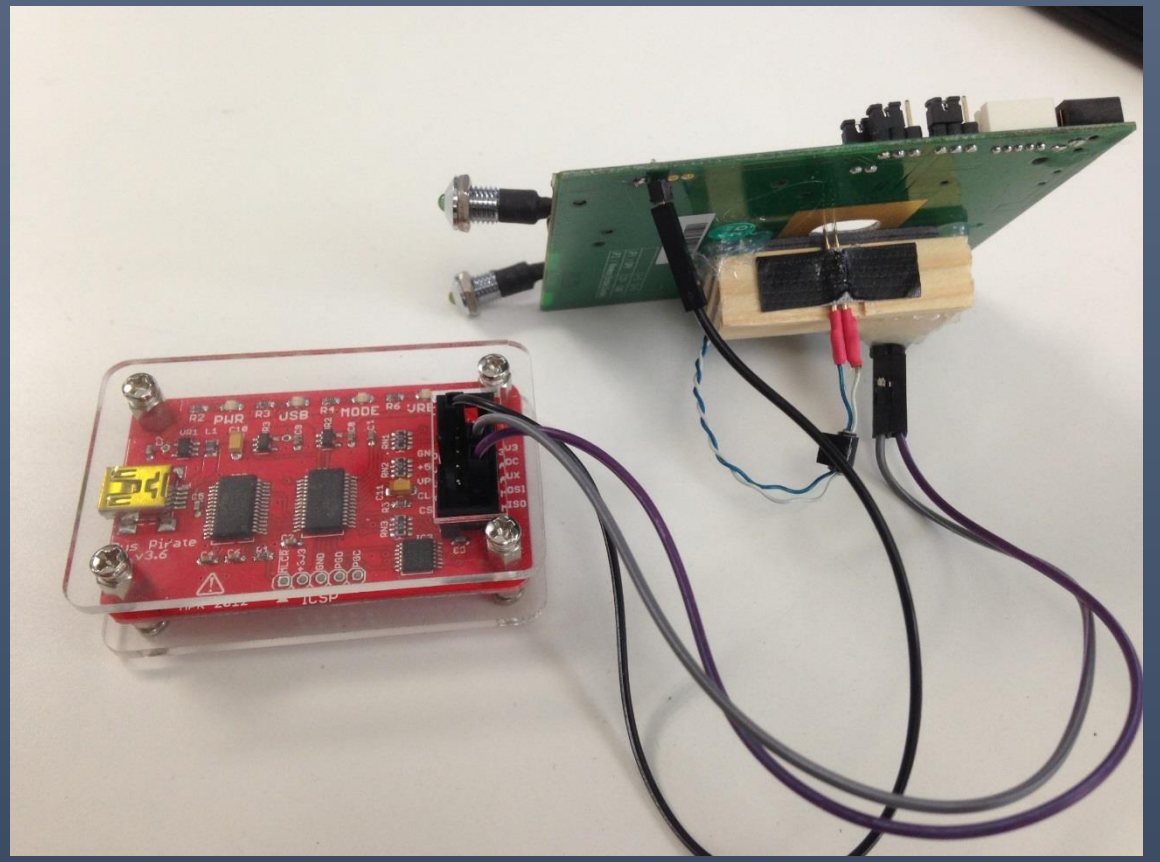
HACKITO ERGO SUM

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



HACKITO
ERGO SUM





HACKITO ERGO SUM

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

HACKITO ERGO SUM

- All of the affected products:
  - Huawei
    - ME906V/J/E
  - HP
    - HP EliteBook 725 G2,HP EliteBook 745 G1,HP EliteBook 755 G2,HP EliteBook 820 G1,HP EliteBook 820 G2,HP EliteBook 840 G1,HP EliteBook 840 G2,HP EliteBook 850 G1,HP EliteBook 850 G2,HP EliteBook 1040 G1,HP EliteBook 1040 G2,HP EliteBook Folio 9470m,HP EliteBook Revolve 810 G2,HP EliteBook Revolve 810 G3,HP ElitePad 1000 G2,HP Elite x2 1011 G2,HP ProBook 430 G1,HP ProBook 430 G2,HP ProBook 440 G0,HP ProBook 440 G1,HP ProBook 440 G2,HP ProBook 450 G0,HP ProBook 450 G1,HP ProBook 450 G2,HP ProBook 640 G1,HP ProBook 645 G1,HP ProBook 650 G1,HP ProBook 655 G1,HP Pro x2 612 G1,HP Spectre x2 13-SMB Pro,HP ZBook 14,HP ZBook 14 G2,HP ZBook 15,HP ZBook 15 G2,HP ZBook 15u HP ZBook 17,HP Zbook 17 G2,mt41 Thin Client

Questions?