



HACKITO
ERGO SUM

THE HIDDEN DANGERS INSIDE THE PLATFORM



Who are we



BadUSB は序章にすぎない!?

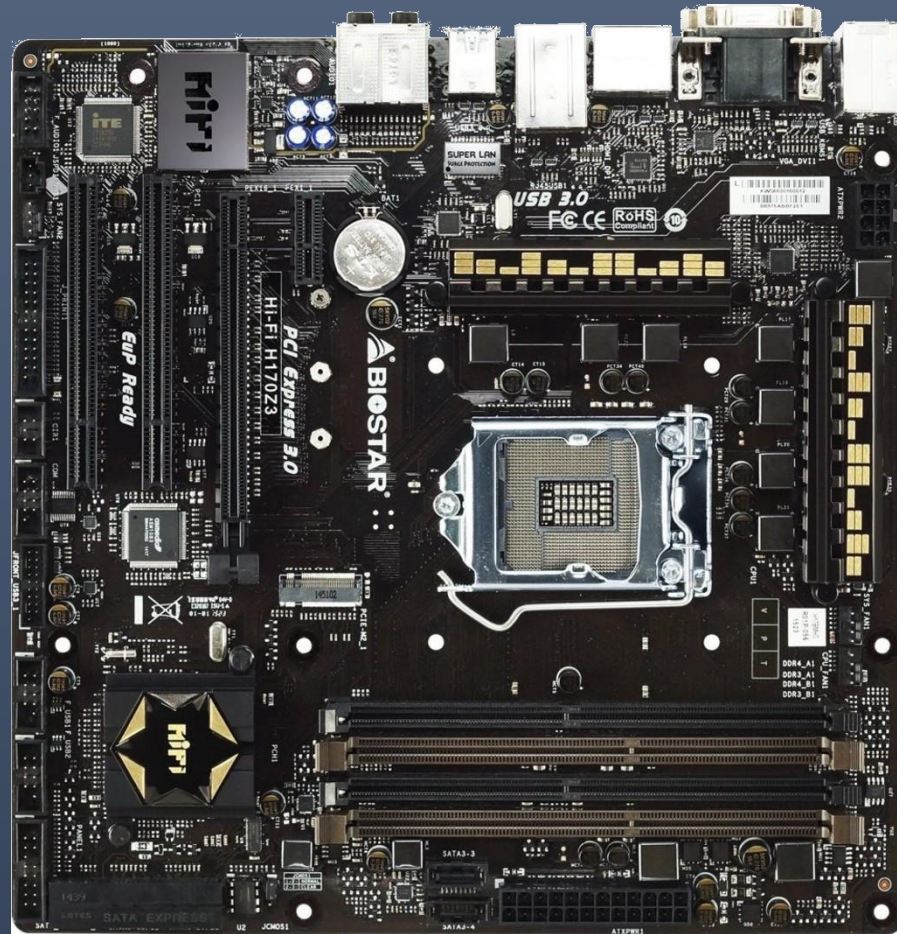
Classic platforms



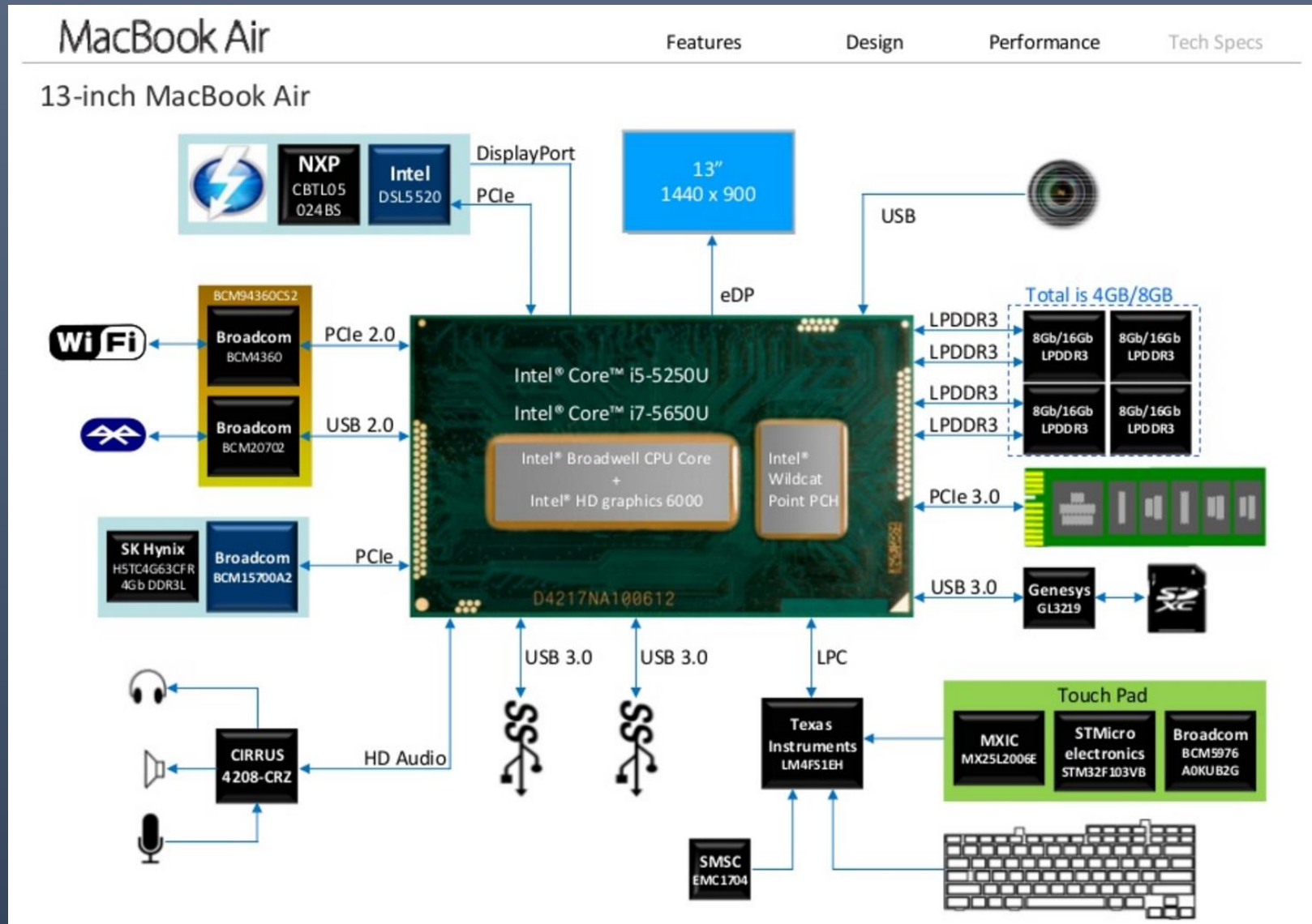


HACKITO
ERGO SUM

Classic platform



Modern platform



Modern platform

MacBook Air

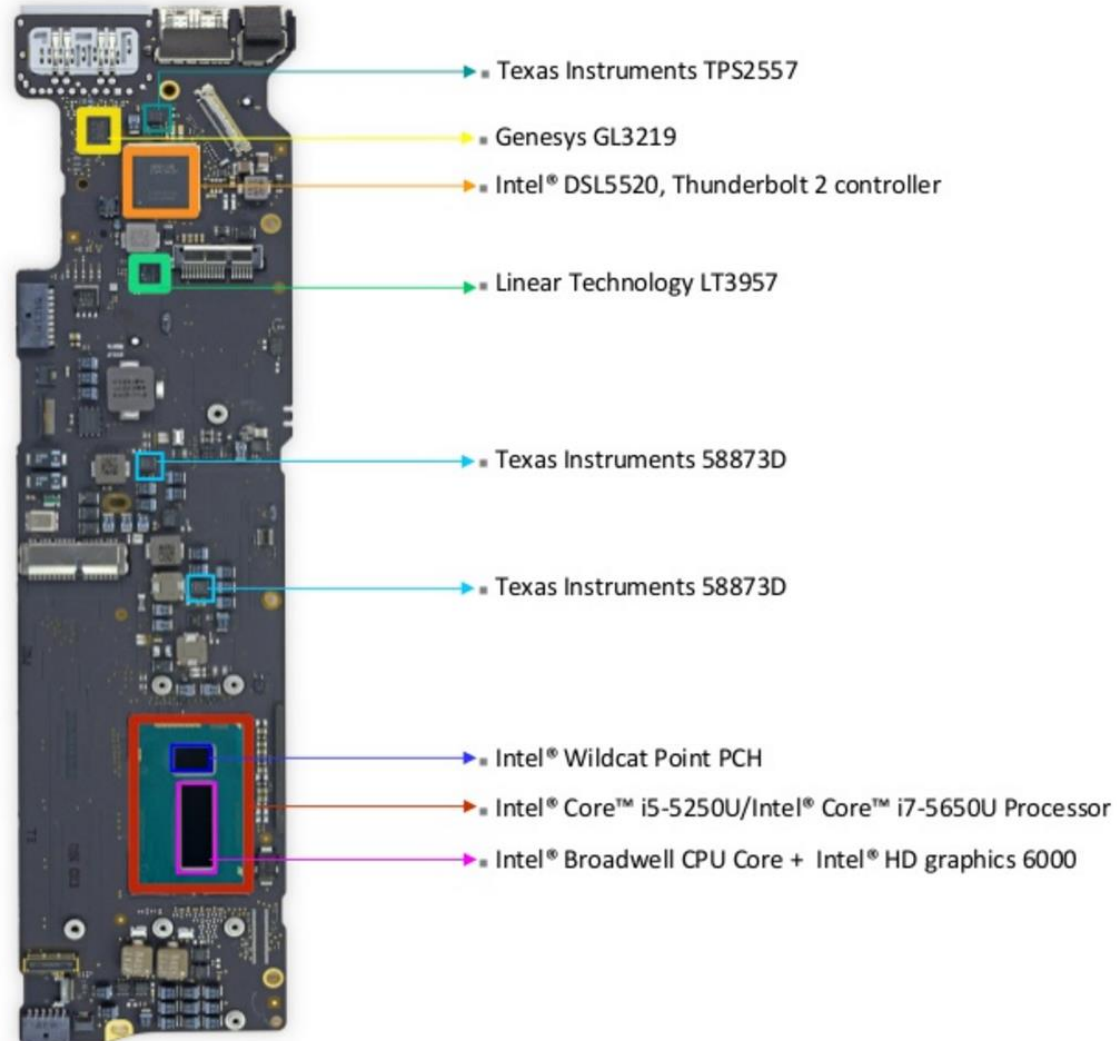
Features

Design

Performance

Tech Specs

13-inch MacBook Air



Modern platform

MacBook Air

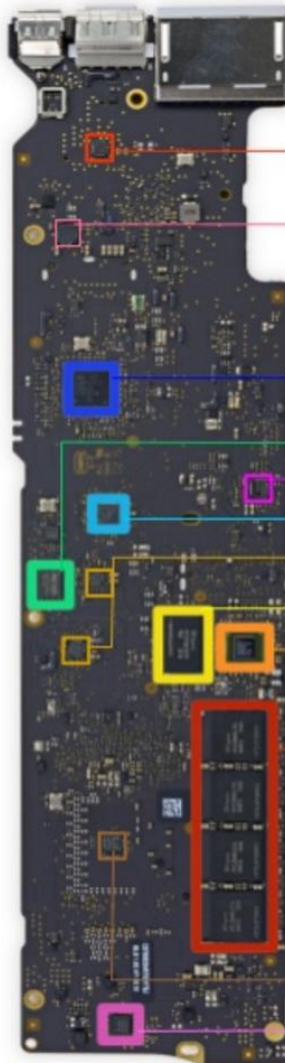
Features

Design

Performance

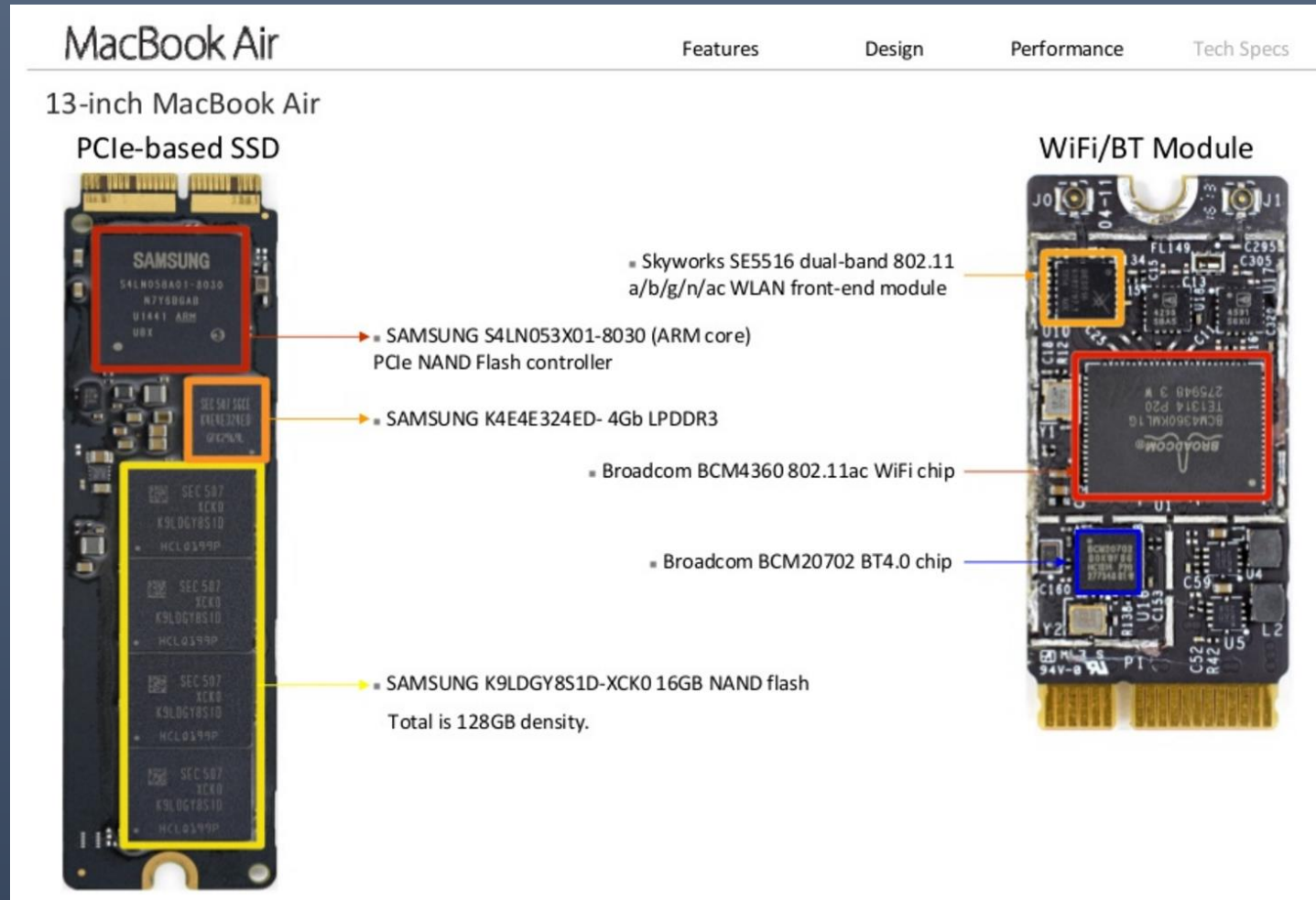
Tech Specs

13-inch MacBook Air



- NXP CBTLO5024BS
- 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

Modern platform



Attackers motivation



HACKITO
ERGO SUM

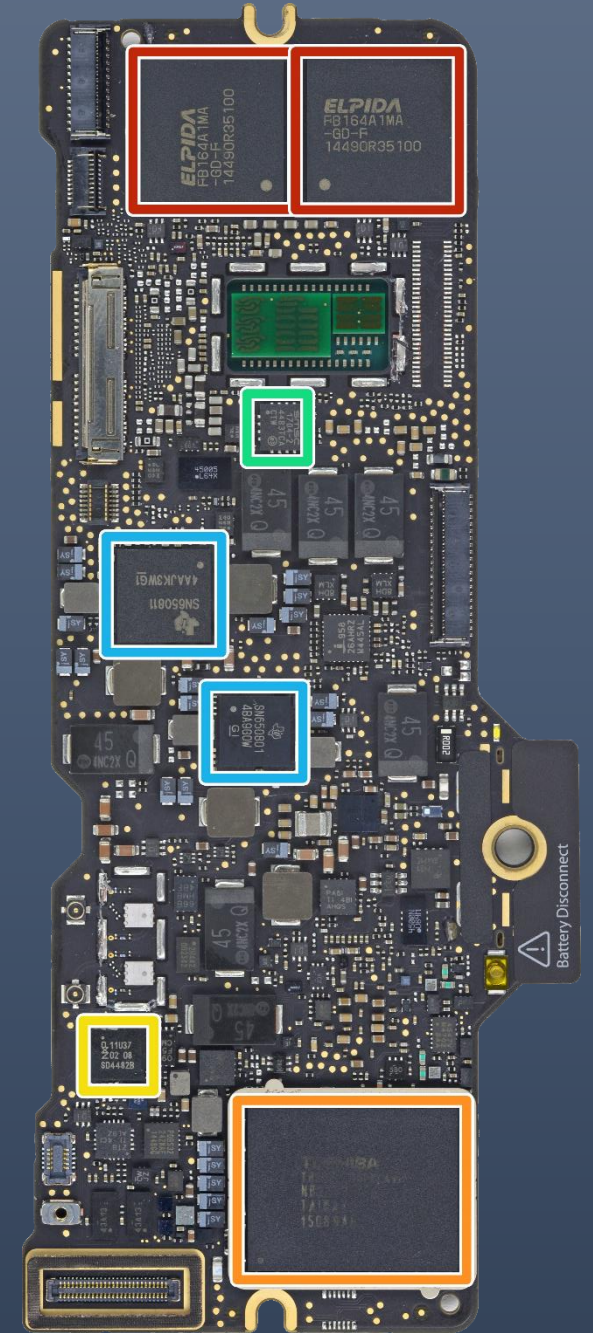
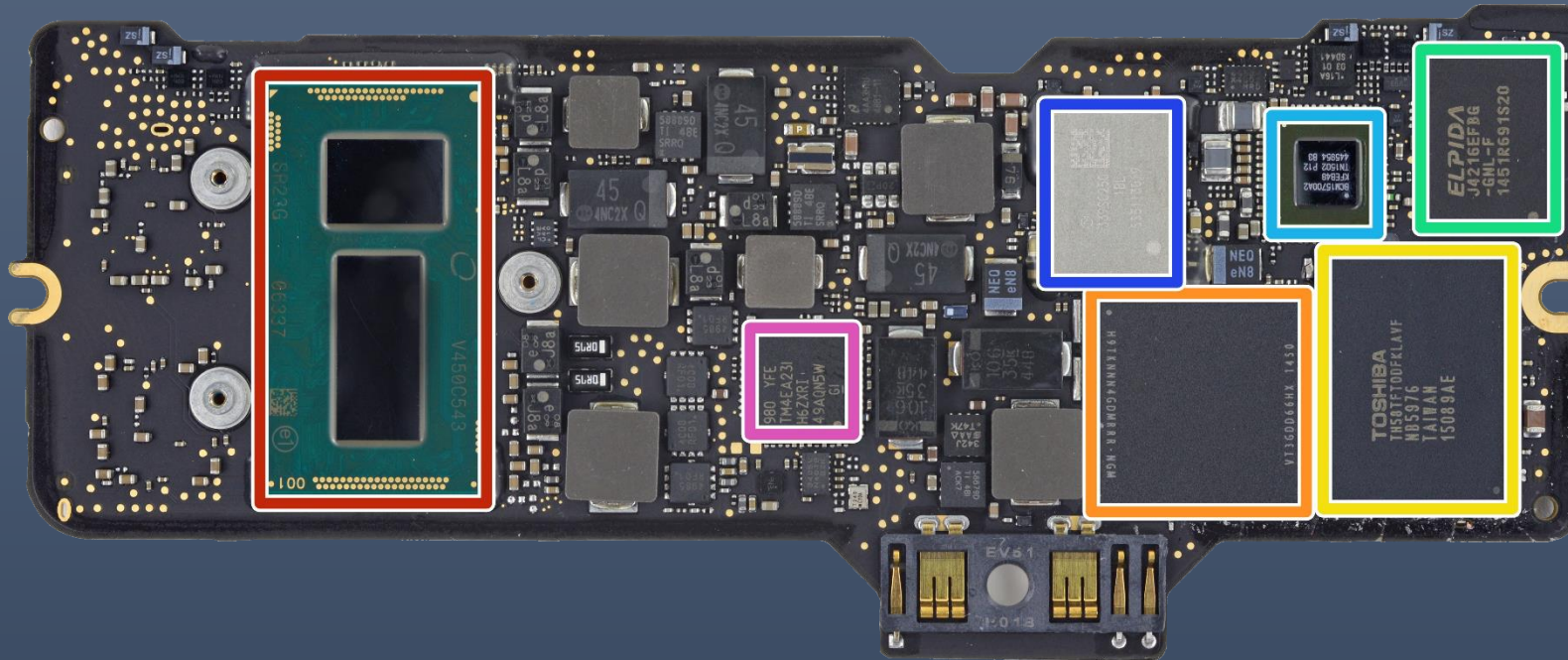
Attackers motivation

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



Attack surface review from the inside

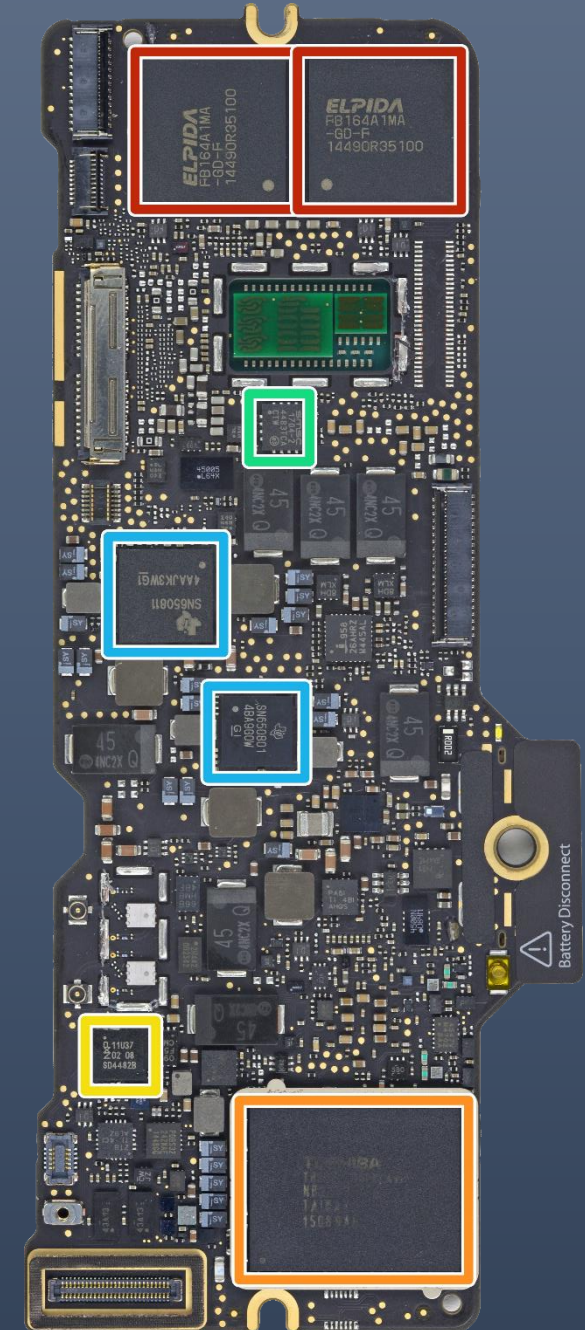
Modern platform



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)



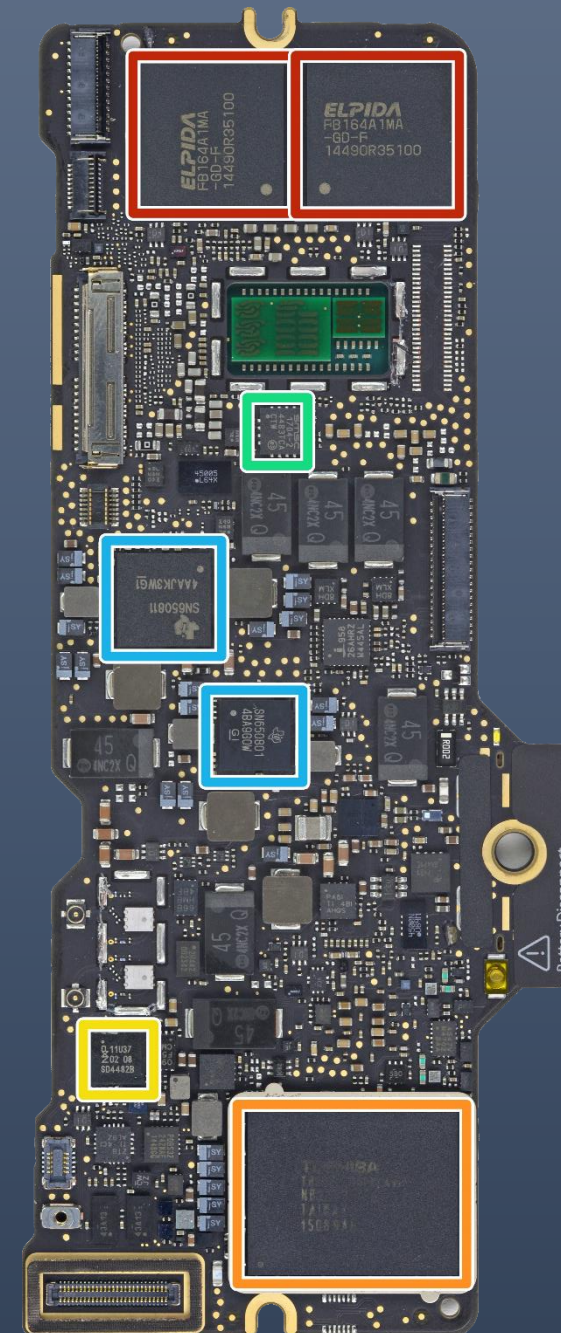
Modern platform

JEDEC Standard No. 84-B51
Page 72

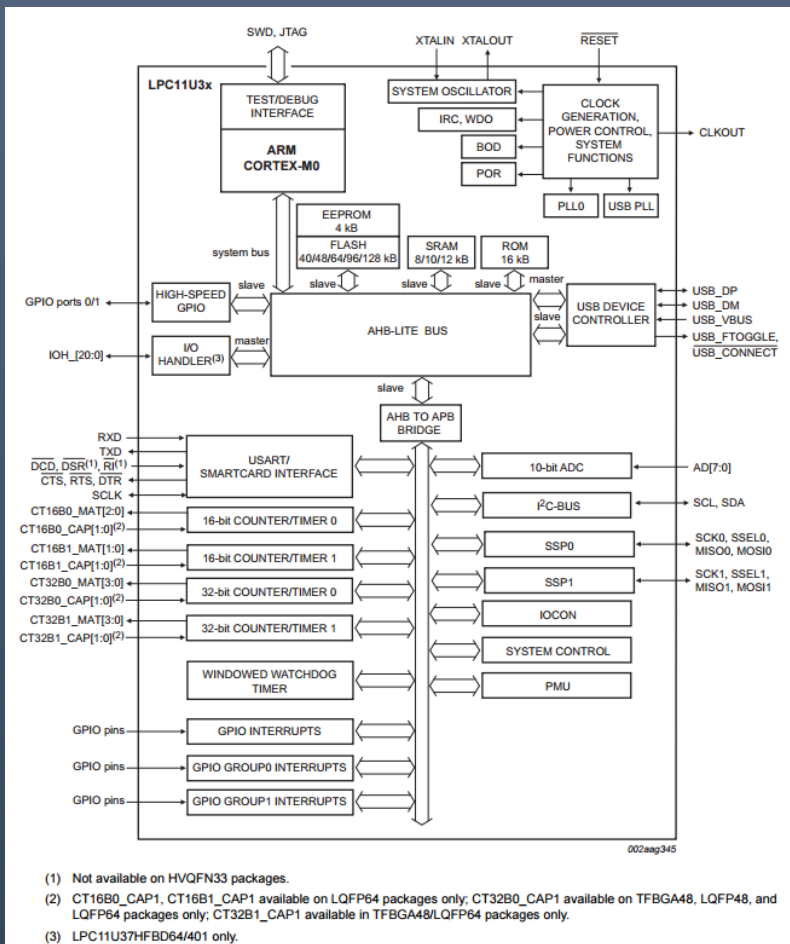
6.6.18 Field Firmware Update

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

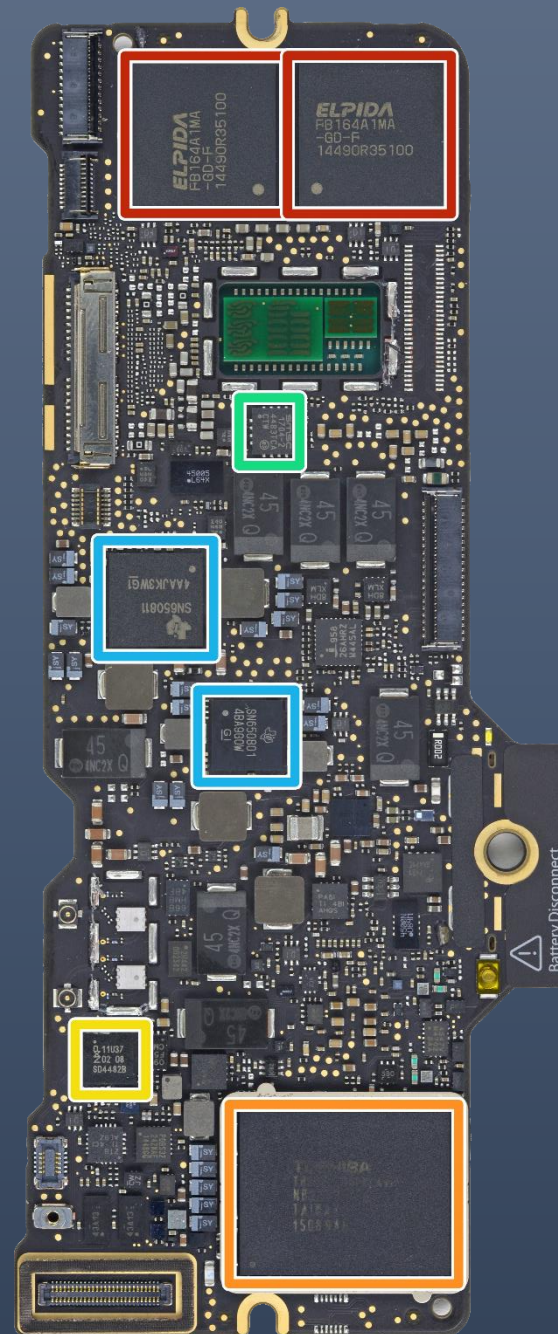
- Elpida/Micron FB164A1MA-GD-F 8 GB LPDDR3 Mobile RAM
- Toshiba TH58TFT0DFKLAVF NB2953 128 GB MLC NAND Flash memory (+ 128 GB on the reverse side for a total of 256 GB)
- NXP 11U37 microcontroller; 128 kB flash, 10kB SRAM
- SMSC 1704-2 Temperature Sensor
- Texas Instruments SN6508 (probably power converter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



Modern platform

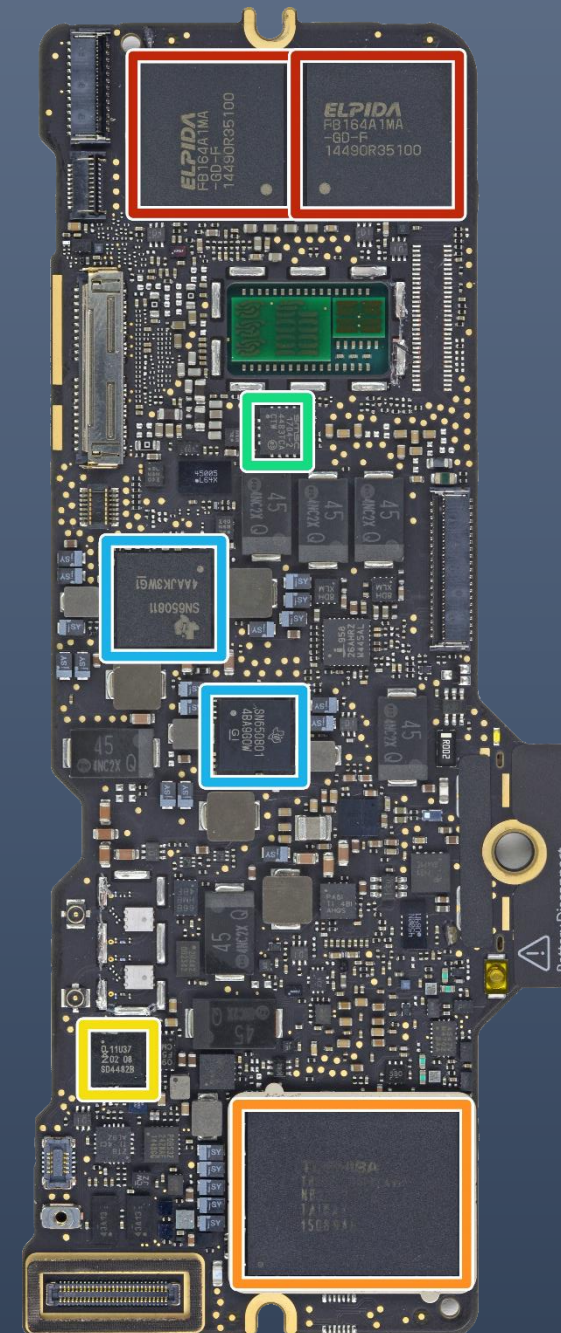


- Elpida/Micron FB164A1MA-GD-F 8 GB LPDDR3 Mobile RAM
- Toshiba TH58TFT0DFKLAVF NB2953 128 GB MLC NAND Flash memory (+ 128 GB on the reverse side for a total of 256 GB)
- NXP 11U37 microcontroller; 128 kB flash, 10kB SRAM
- SMSC 1704-2 Temperature Sensor
- Texas Instruments SN6508 (probably power converter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



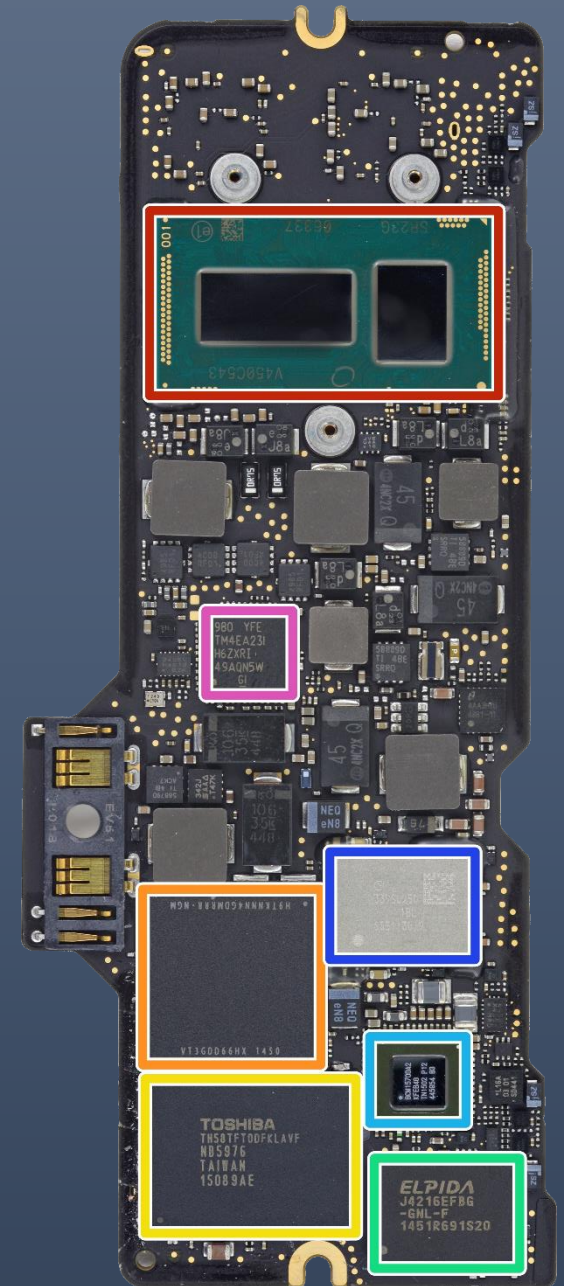
Modern platform

- 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 1779 temperature sensor
- Texas Instruments TPS5001 (probably power converter related to TPS5001)



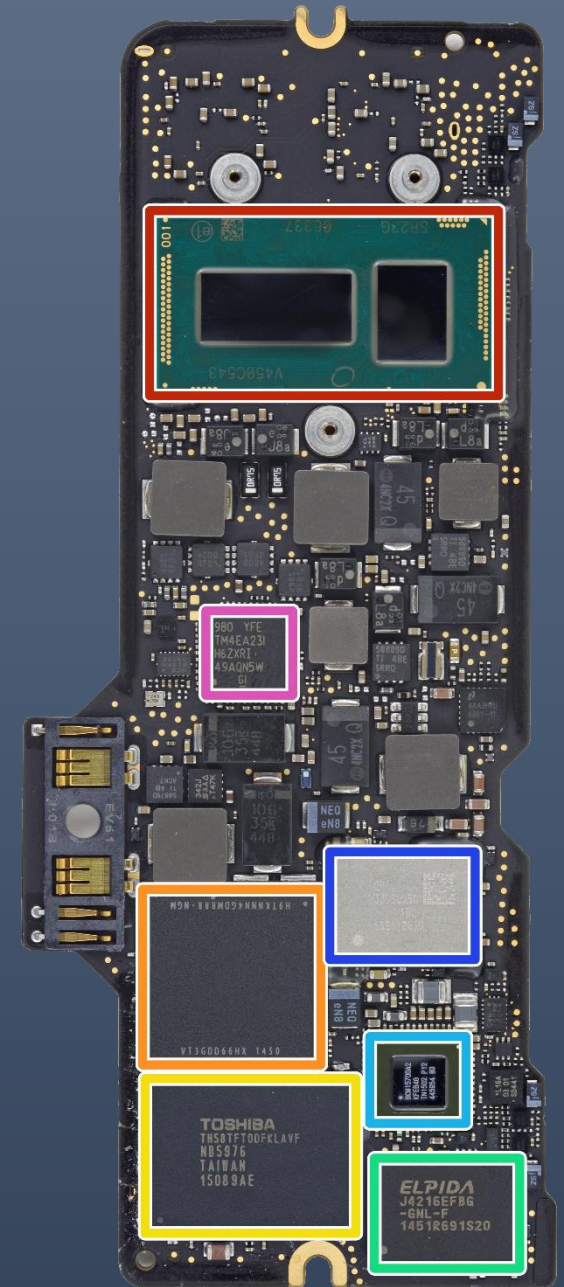
Modern platform

- 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)



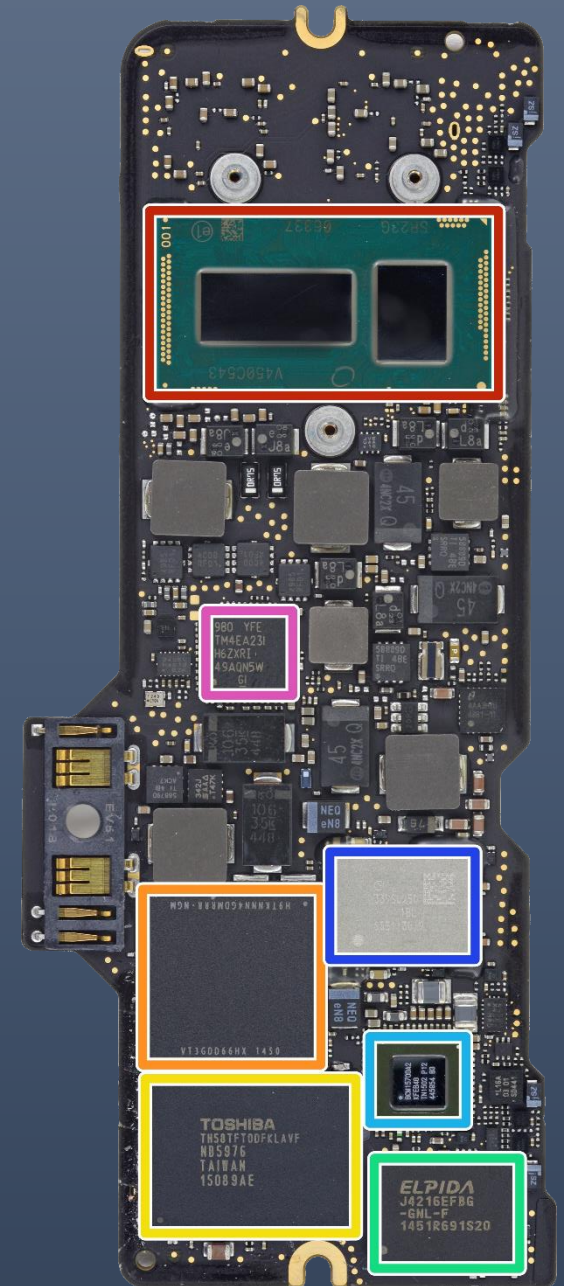
Modern platform

- 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)



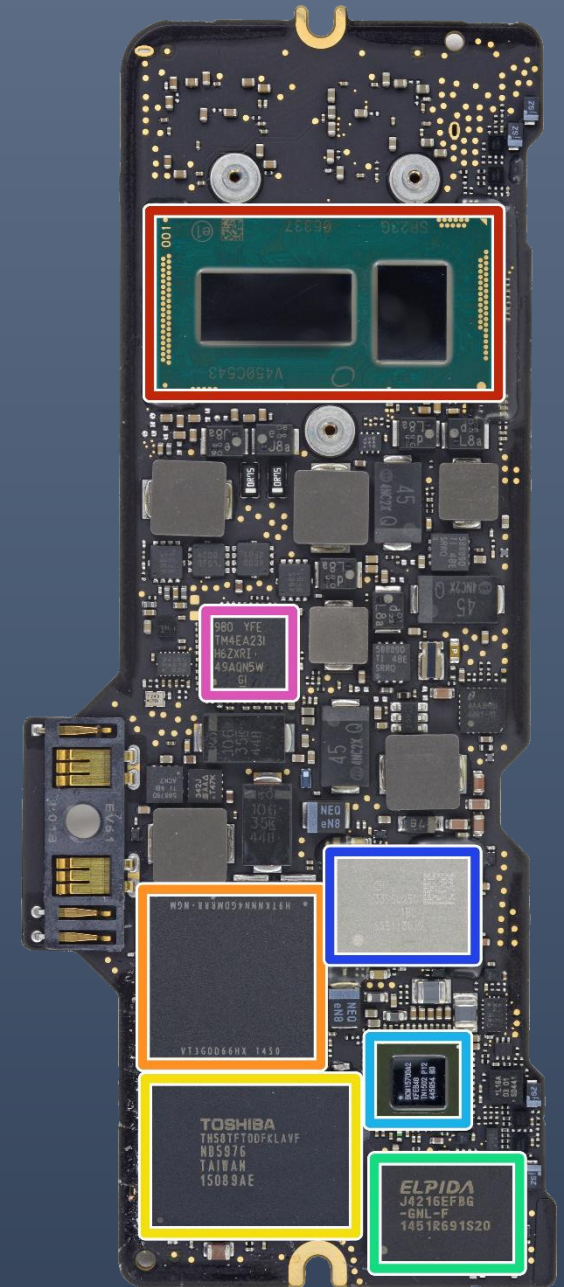
Modern platform

- 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 J4216FBG-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)



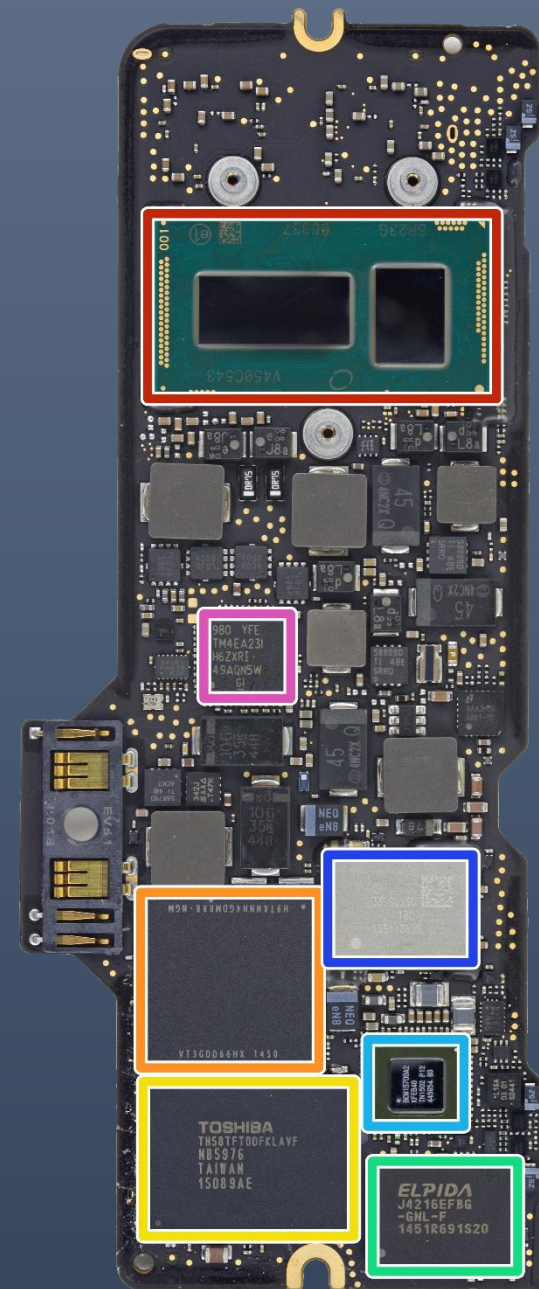
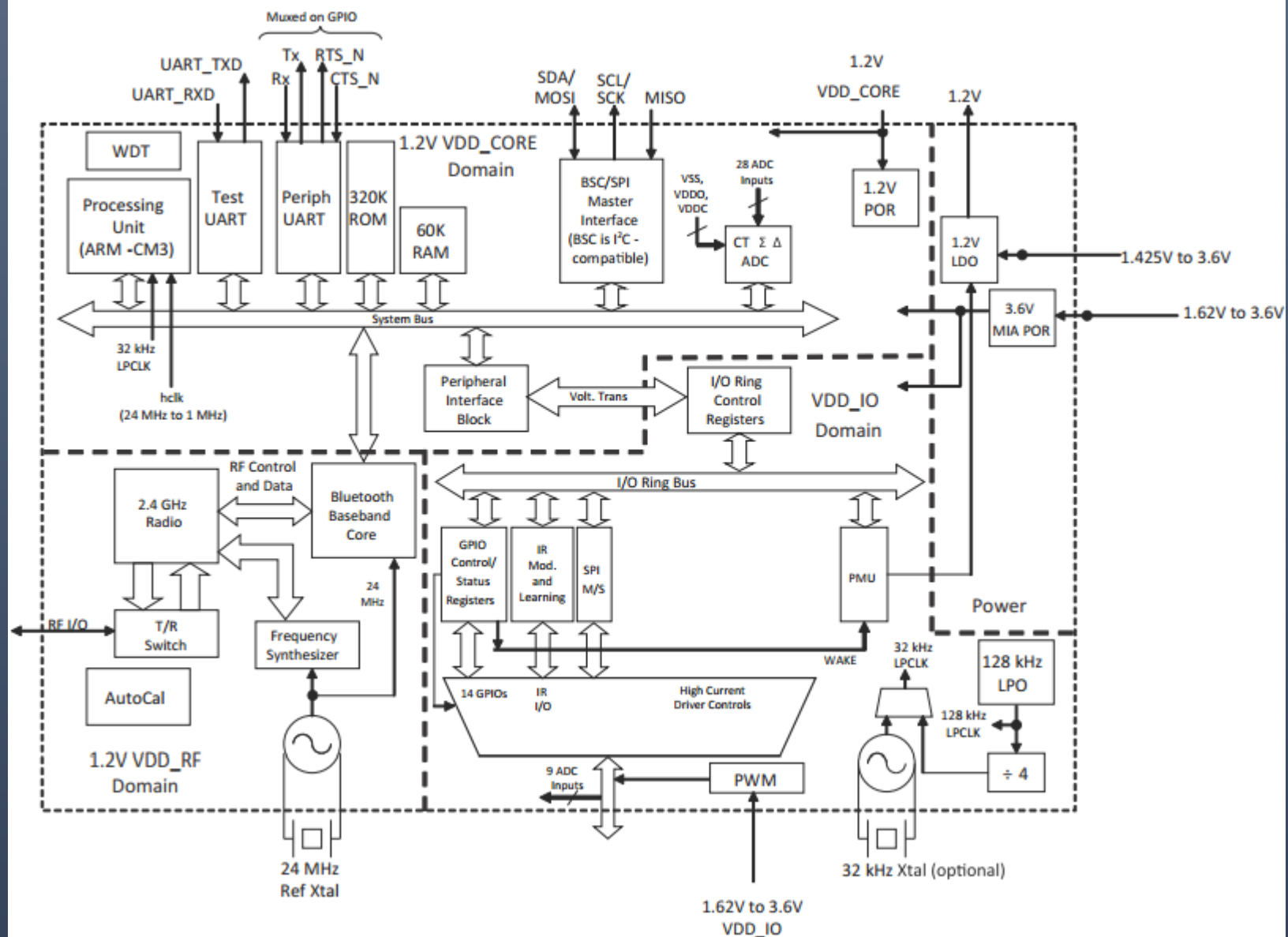
Modern platform

- 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 J4216FBG-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)

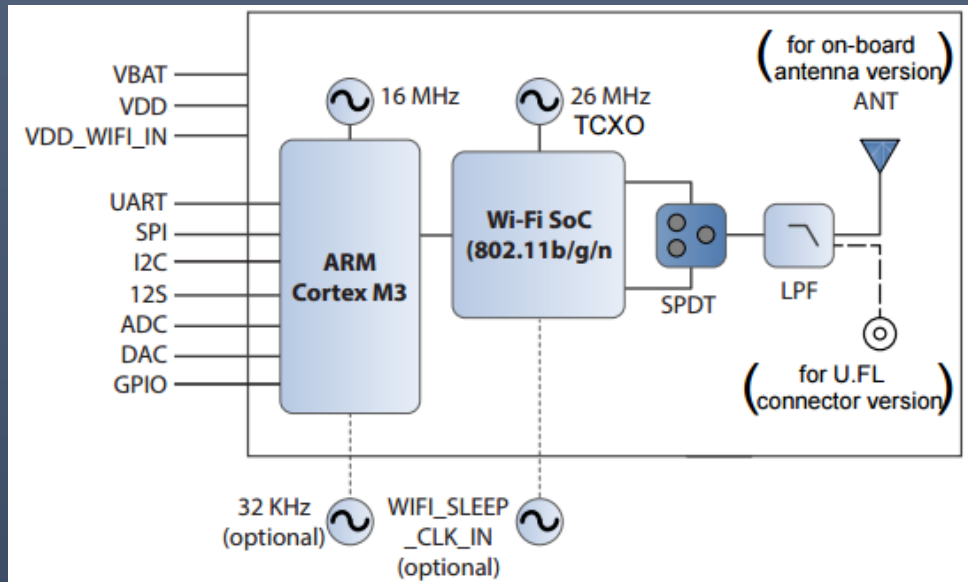




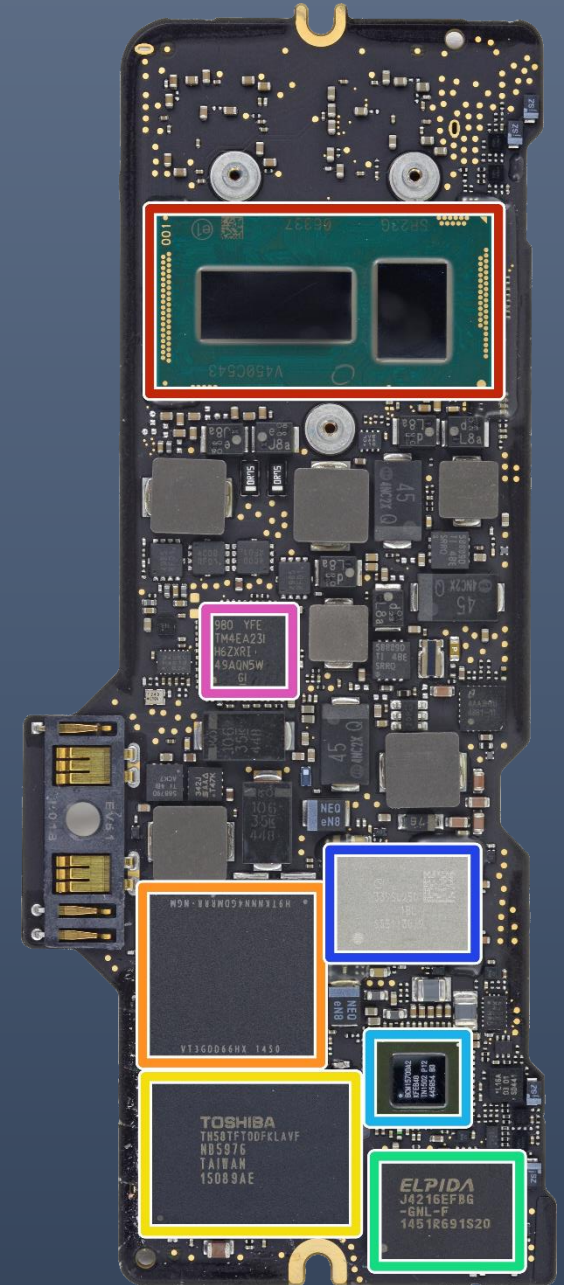
HACKITO ERGO SUM



Modern platform

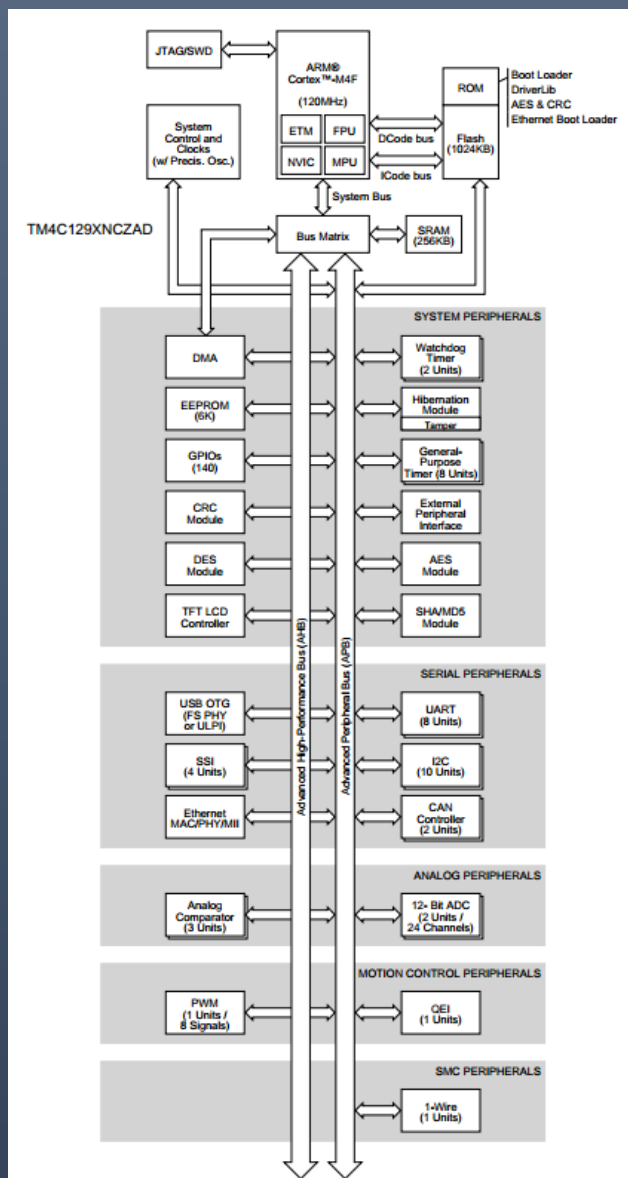


- Intel SR23G Core M-5Y31 CPU (Dual-Core, 1.1 GHz, Turbo Boost up to 2.4 GHz) with Intel HD Graphics 5300
- SK Hynix H9TKNNN4GDMRRR-NGM 4 Gb (512 MB) LPDDR2-SDRAM
- Toshiba TH58TFT0DFKLAVF 128 GB MLC NAND Flash
- Elpida/Micron J4216EFBG-GNL-F DDR3 SDRAM
- Broadcom BCM15700A2, appears to be a wireless 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)



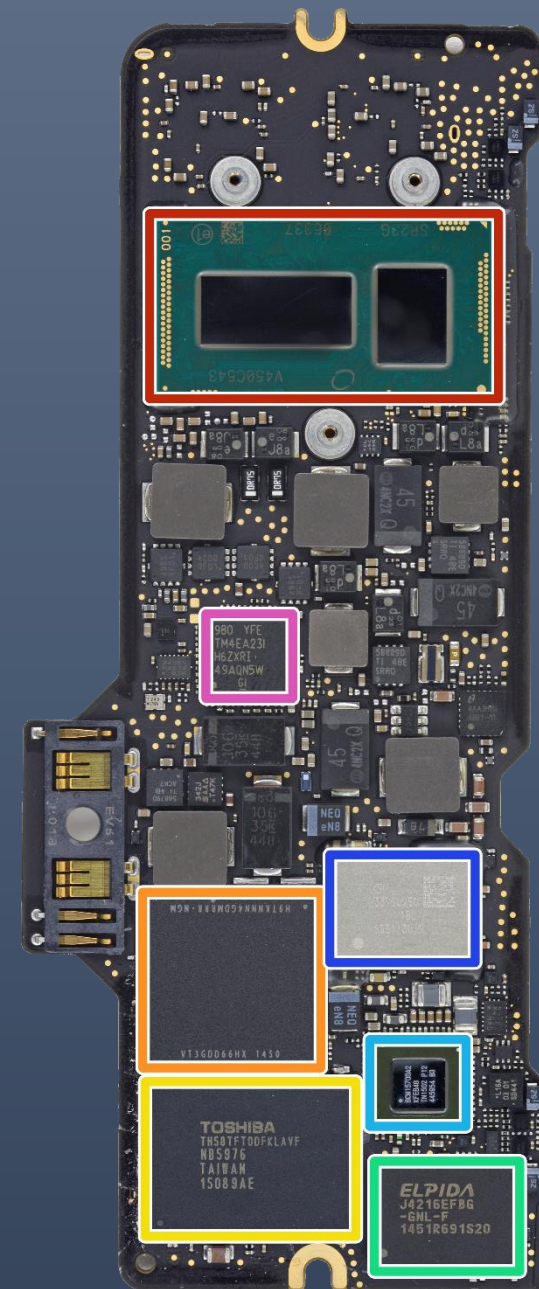


HACKITO ERGO SUM



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 J4216FBG-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 LM4F51EH SMC Controller (Replacement codename for TM4EA231)



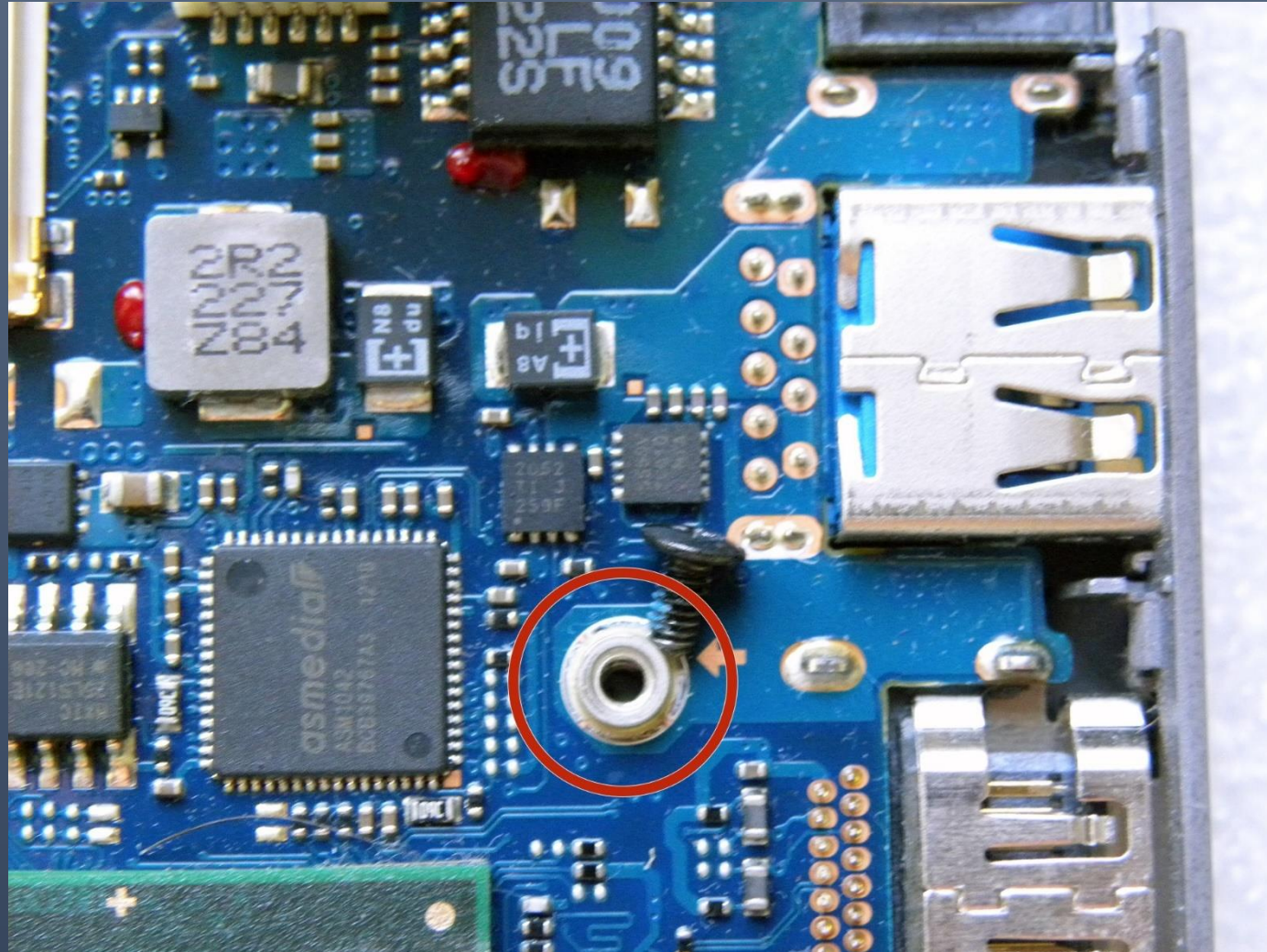
Modern platform

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://pluggable.com/2013/03/05/usb3-sata-u3-firmware-update>



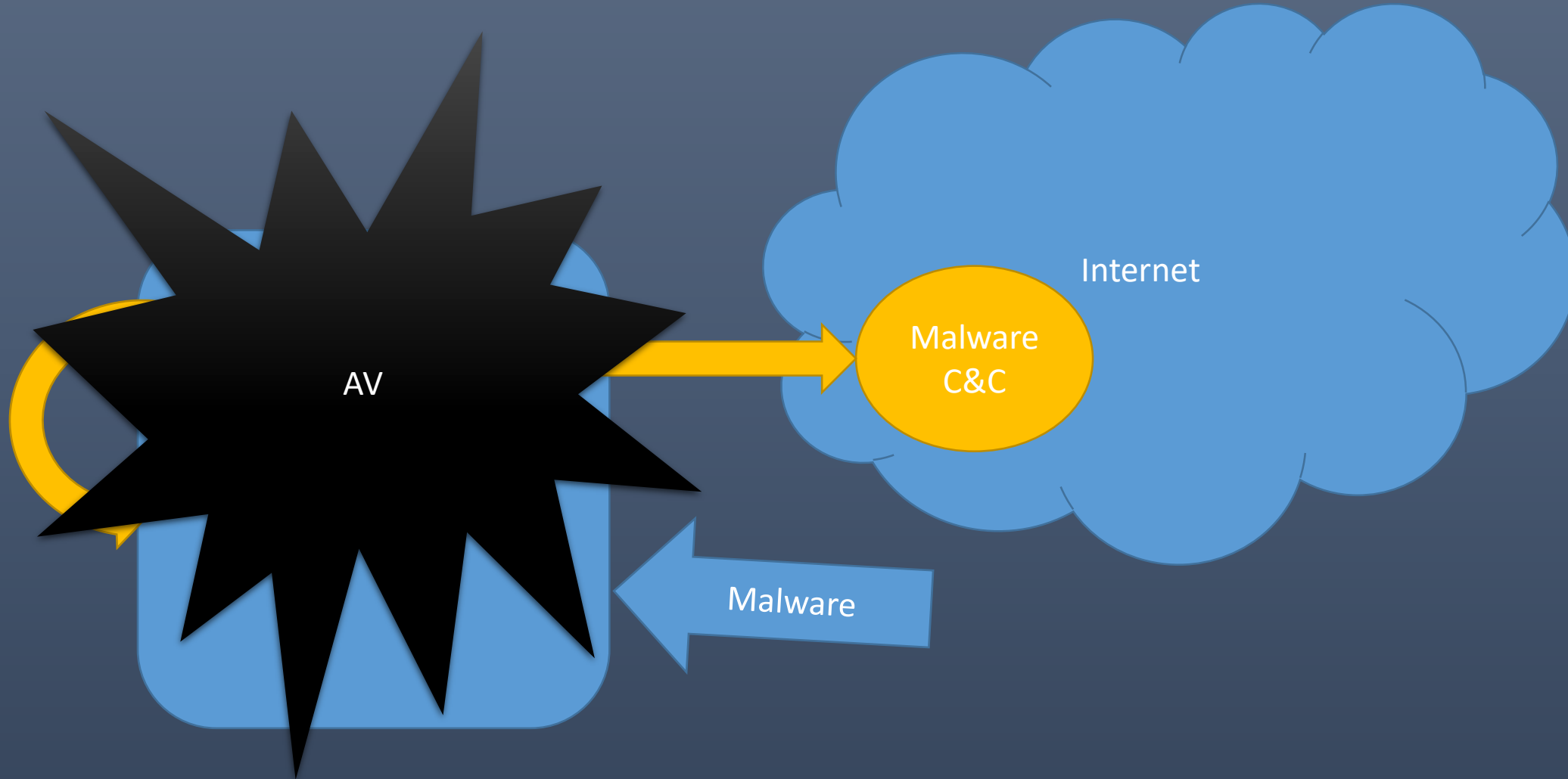
Modern platform



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.

DEMO

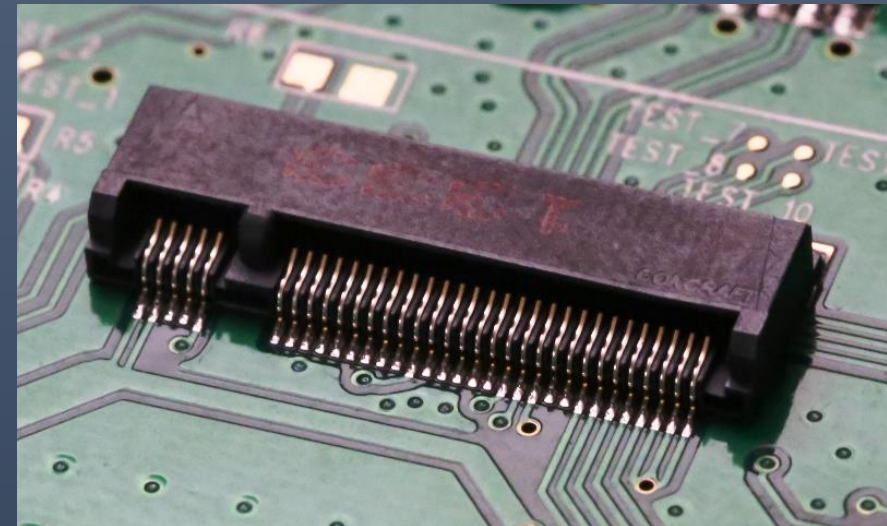




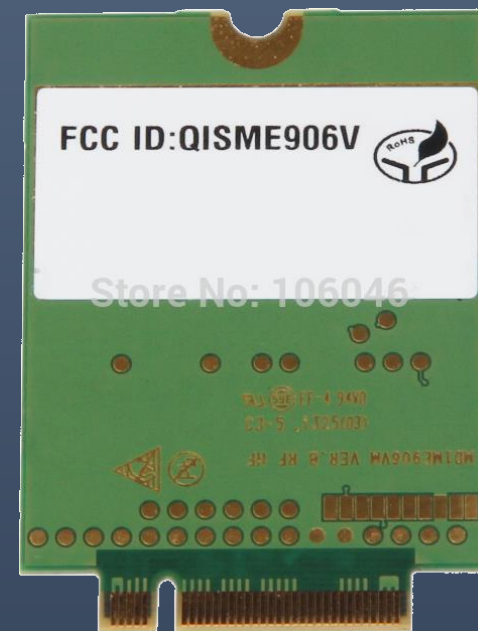
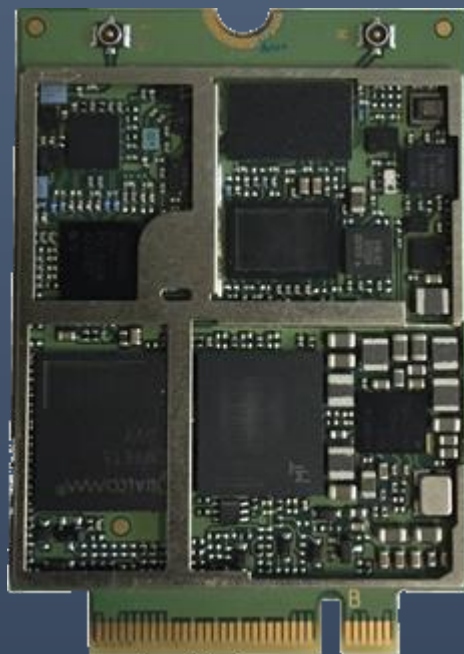
HACKITO ERGO SUM



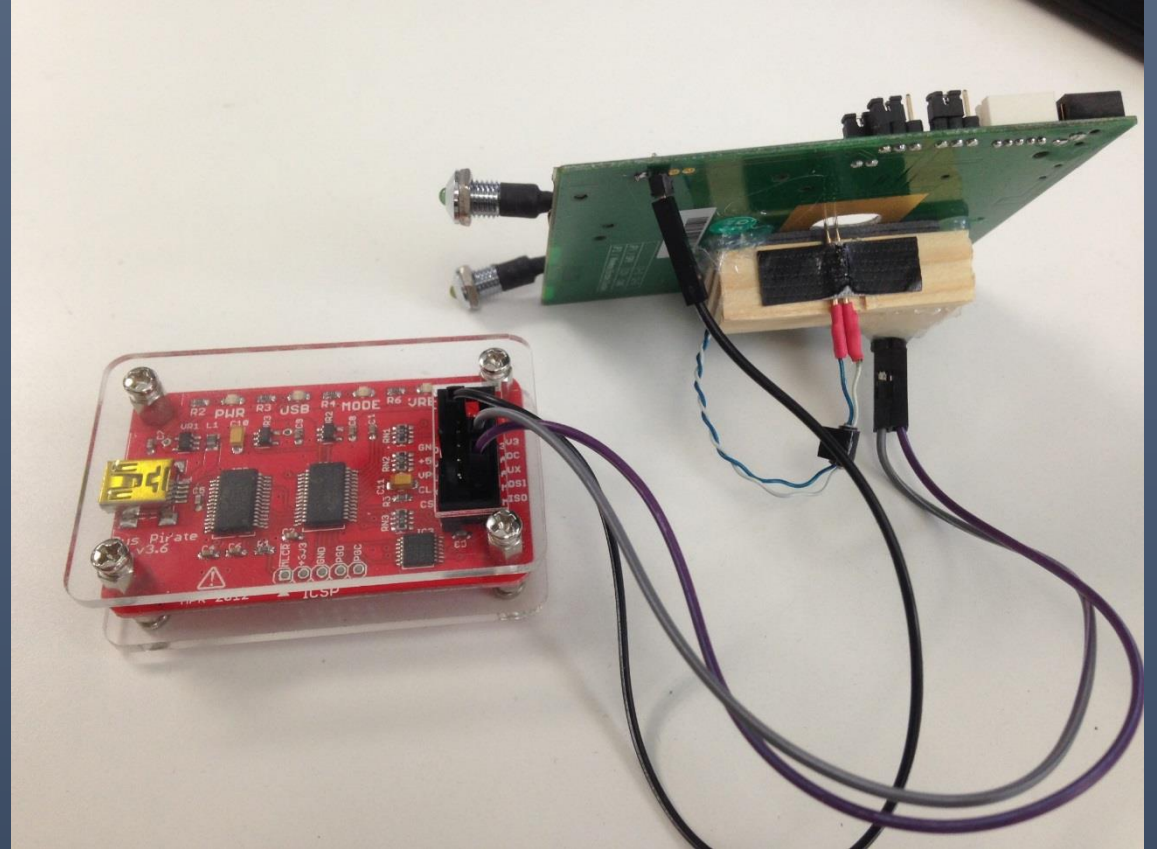
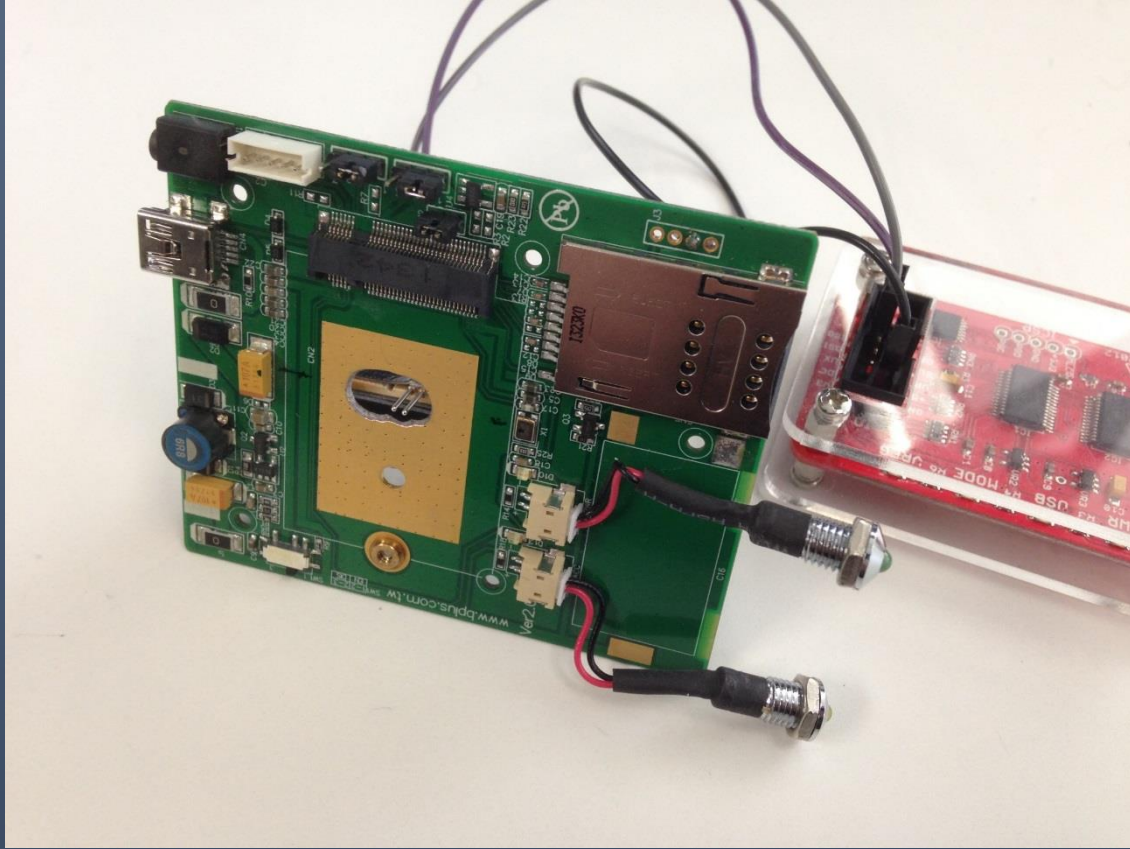
- Internal Huawei LTE modem
 - Connected via USB interface in M.2 socket



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



HACKITO ERGO SUM



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





- 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



Thanks for your research and for giving the DefCon talk. I was there in the audience.

Huawei is refusing to provide the ME906 firmware update directly to end users. Instead, they refer to the OEM partner (Sony, etc.), who in turn knows nothing about this. It's a classic case of finger pointing.

Do you have any insight and/or suggestions on how an end user of one of these LTE modules can acquire the patch? In my case, it's the Sony variant.

Thanks in advance for your assistance. Please excuse the anonymous disposable email, but I'm sure you know it's the only way to remain secure.

Regards,
A (Disgruntled) Huawei Modem Owner



Questions?