

Software

**WELCOME TO THE
OPEN SOURCE
FIRMWARE CONFERENCE**

Vincent Zimmer

Sr. Principal Engineer

INTEL SOFTWARE & SERVICES GROUP

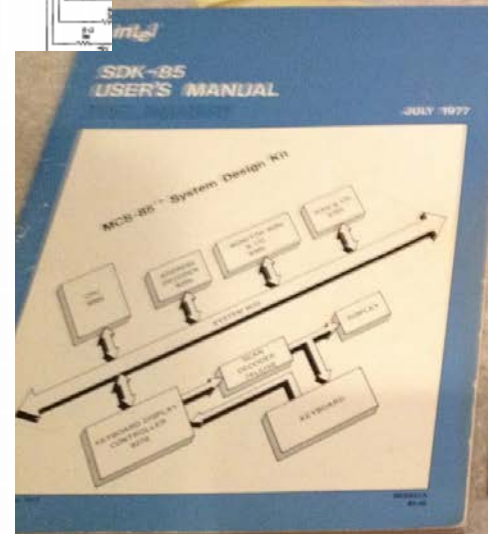
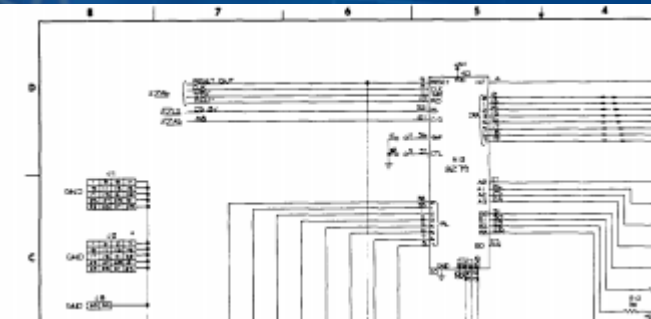


@vincentzimmer

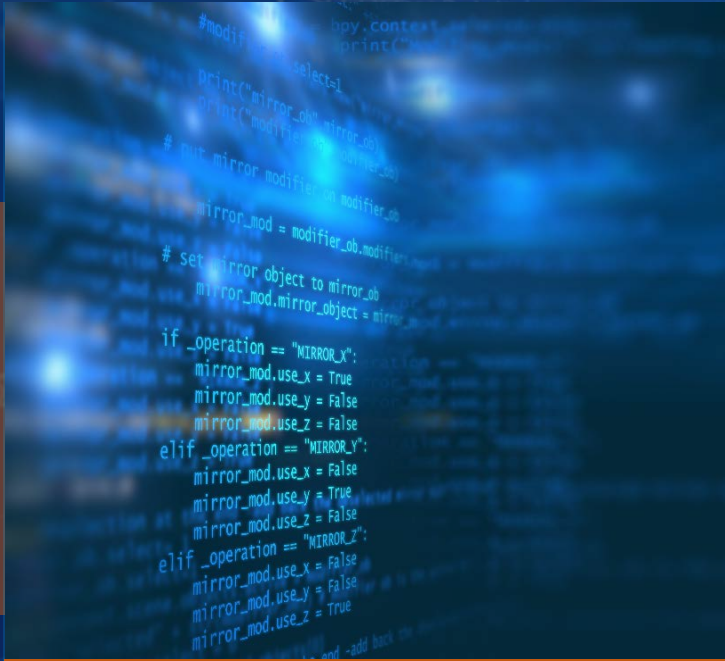
MY BEGINNING

ISIS-II 8080/8085 MACRO ASSEMBLER, X108 SDK85

```
LOC OBJ      SEQ      SOURCE STATEMENT
          933 ; DESCRIPTION: RGLOC RETURNS T
          934 ; INDICATED BY TH
          935 ;
          936 RGLOC:
02FC 2AFD20  937      LHLD  RGPTR ; GET R
02FF 2600   938      MVI   H,0 ; /IN H & L
0301 01ED03 939      LXI   B,RGTB ; GET REGISTER SAVE LOCATION TABLE ADDRESS
0304 09     940      DAD   B ; POINTER INDEXES TABLE
0305 6E     941      MOV   L,M ; GET LOW ORDER BYTE OF REGISTER SAVE LOC.
0306 2620   942      MVI   H,(RAMST SHR 8) ; GET HIGH ORDER BYTE OF
          943 ; /REGISTER SAVE LOCATION
0308 C9     944      RET
          945 ;
          946 ; *****
          947 ;
          948 ; FUNCTION: RGNAM - DISPLAY REGISTER NAME
          949 ; INPUTS: NONE
          950 ; OUTPUTS: NONE
          951 ; CALLS: OUTPT
          952 ; DESTROYS: A,B,C,D,E,H,L,P/P'S
          953 ; DESCRIPTION: RGNAM DISPLAYS, IN THE ADDRESS FIELD OF THE DISPLAY,
          954 ; THE REGISTER NAME CORRESPONDING TO THE CURRENT
          955 ; REGISTER POINTER VALUE.
          956 ;
          957 RGNAM:
0309 2AFD20  958      LHLD  RGPTR ; GET REGISTER POINTER
030C 2600   959      MVI   H,0
030E 29     960      DAD   H ; MULTIPLY POINTER VALUE BY 4
030F 29     961      DAD   H ;/(REGISTER NAME TABLE HAS 4 BYTE ENTRIES)
0310 01B903 962      LXI   B,NMTBL ; GET ADDRESS OF START OF REGISTER NAME TABLE
0313 09     963      DAD   B ; ARG - ADD TABLE ADDRESS TO POINTER - RESULT IS
          964 ; /ADDRESS OF APPROPRIATE REGISTER NAME IN H & L
0314 AF     965      XRA   A ; ARG - USE ADDRESS FIELD OF DISPLAY
0315 0600   966      MVI   B,NODOT ; ARG - NO DOT IN ADDRESS FIELD
0317 CDB702 967      CALL  OUTPT ; OUTPUT REGISTER NAME TO ADDRESS FIELD
031A C9     968      RET
          969 ;
          970 ; *****
          971 ;
          972 ; FUNCTION: RSTOR - RESTOR USER REGISTERS
          973 ; INPUTS: NONE
          974 ; OUTPUTS: NONE
          975 ; CALLS: NOTHING
          976 ; DESTROYS: A B C D E H L P/P'S
```



S.O.S



SIMPLICITY



OPENNESS



SECURITY

SIMPLICITY



THEN



**INTEL BUILDS BROAD AND
COMPLEX CODE BASE**

**CUSTOMERS ASSUME RISKS SIMPLIFYING
THE CODE**

OUR NEW FOCUS – SIMPLE AND SCALABLE SOLUTIONS

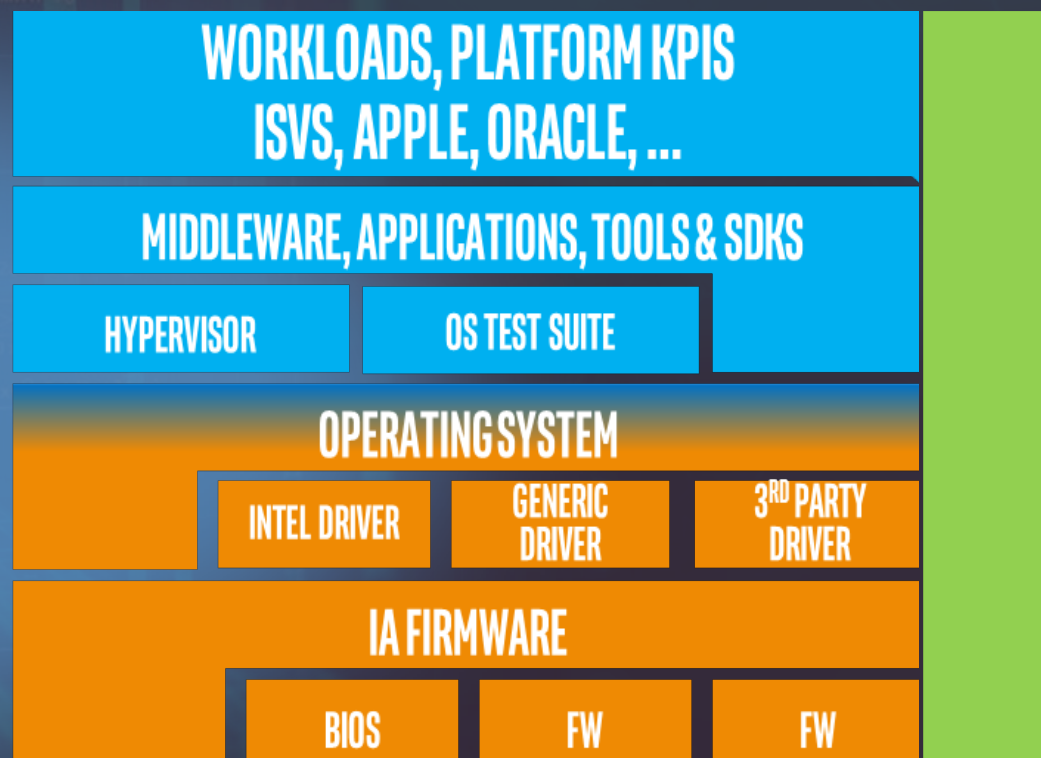
OPENNESS

PARTNERS DEMANDING OPEN SOURCE FURTHER DOWN THE ENTIRE STACK

CUSTOMER FOCUSED

SOLUTION ORIENTED

TECHNOLOGY ALIGNED



SECURITY

**DESIGN
+
DEVELOP**

EXTEND

**DISCOVER
+
MITIGATE**

EXTEND

**DISTRIBUTE
+
DEPLOY**

BROADENING OUR SECURITY MINDSET

WE'RE MAKING PROGRESS

**FSP2.0+
INTEL® SLIM
BOOTLOADER
MINI PLATFORM
ARCHITECTURE**

SIMPLICITY



OPENNESS



SECURITY

WE'RE MAKING PROGRESS

**FSP2.0+
INTEL® SLIM
BOOTLOADER
MIN PLATFORM
ARCHITECTURE**

SIMPLICITY

**OPEN SOURCE UEFI
PLATFORMS (CLIENT,
IOT, SERVER)
SOUND FIRMWARE,
MICROPYTHON**

OPENNESS



SECURITY

FSP – Firmware Support Package

UEFI – Unified Extensible Firmware Interface

WE'RE MAKING PROGRESS

**FSP2.0+
INTEL® SLIM
BOOTLOADER
MIN PLATFORM
ARCHITECTURE**

SIMPLICITY

**OPEN SOURCE UEFI
PLATFORMS (CLIENT,
IOT, SERVER)
SOUND FIRMWARE,
MICROPYTHON**

OPENNESS

**CHIPSEC
CAPSULE UPDATE**

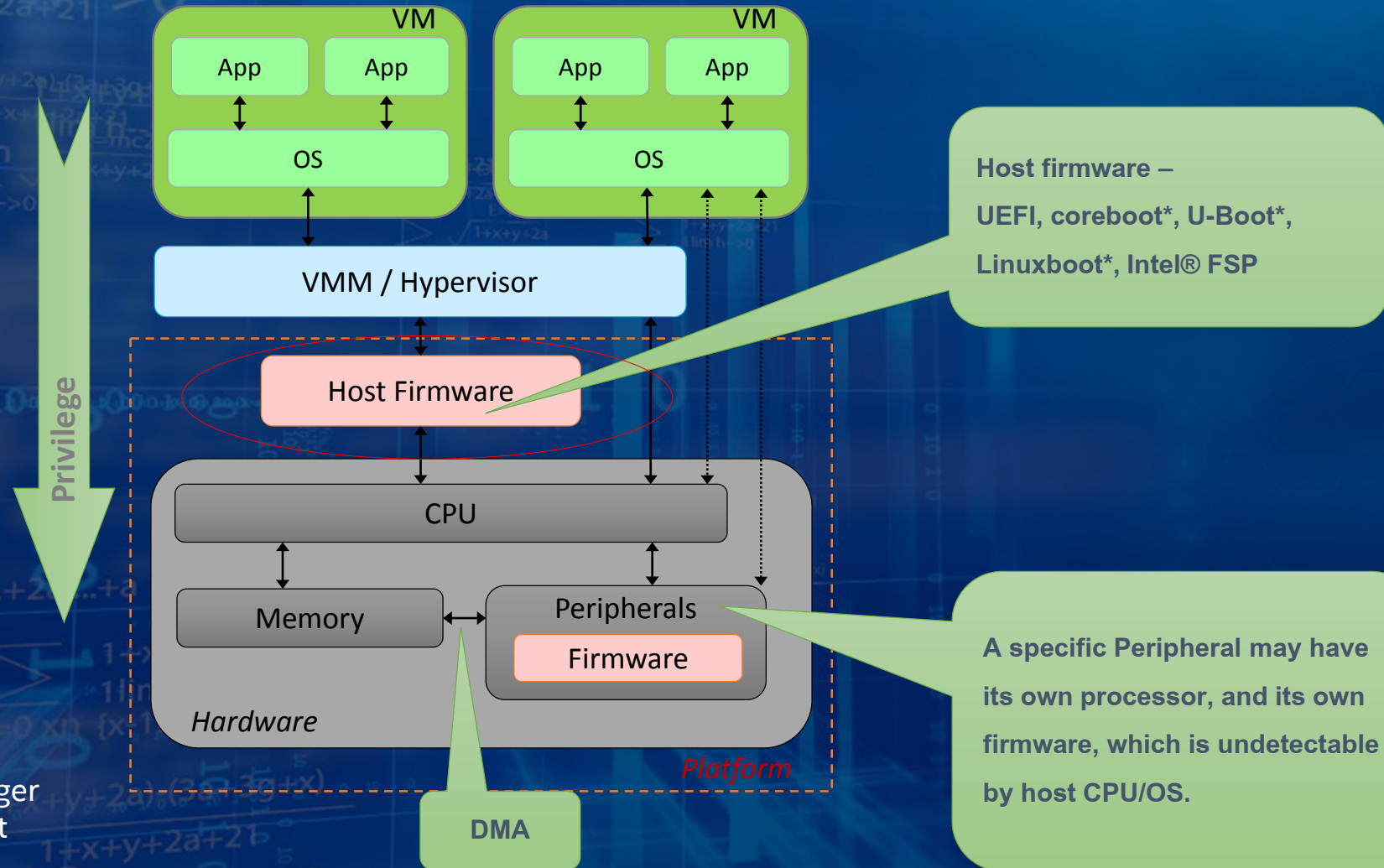
SECURITY



Firmware options

From https://en.wikipedia.org/wiki/Chinese_restaurant

WHERE IS FIRMWARE?



VM – Virtual Machine
OS – Operating System
VMM – Virtual Machine Manager
CPU – Central Processing Unit
DMA – Direct Memory Access

Do others believe this?

The Future of Firmware

We have been witnessing an interesting phenomenon since the beginning of this century: open source projects are gaining momentum, led by companies such as Google and Facebook. Many legacy and proprietary software solutions are either disappearing or losing steam very quickly; open source solutions are becoming a primary interest of technologists at an amazing speed.

Even though this century is still young, we are riding on a fascinating wave that will make the 21st century a distinctly different century than any other. The phrase “open source” clearly connotes sharing and collaboration, in contrast to the waning business philosophy of

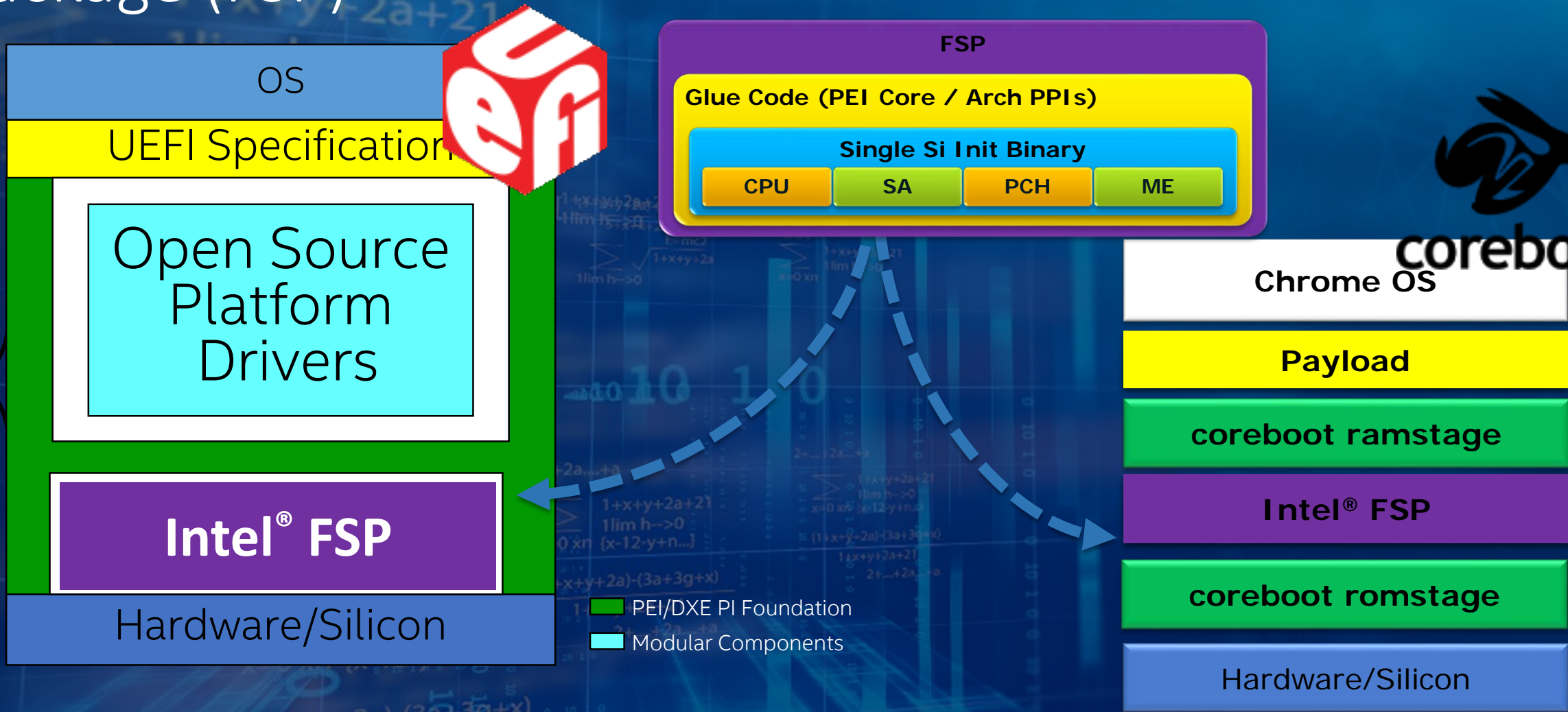
From <https://www.apress.com/us/book/9781484200711>

What are we doing

- Open development environment
 - Open source core
 - Min Core
 - Open source platform code
 - Min Platform, Advanced Feature Packages
 - IP protected initialization in well-defined binary blob
 - Open up all of the build tools
 - Standards
 - De jure but move to 'code first', De facto

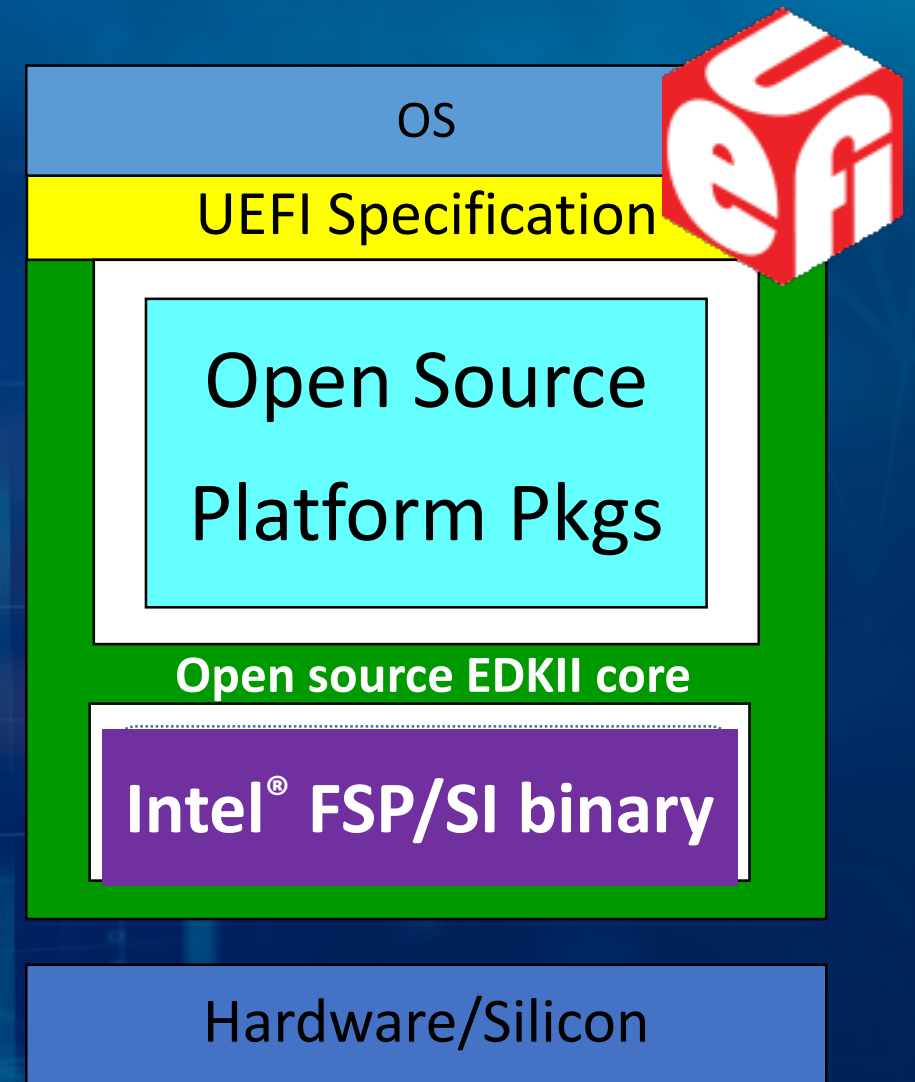
UEFI and coreboot with the Intel Firmware Support Package (FSP)

UEFI/PI Scope - Green "H" w/ EDKII
Open Source "Core"



Internal mode of evolution

- **FSP / Binary FV's** - Evolution of the Intel[®] Firmware Support Package (FSP) from 1.0 to 1.1(simplified boot flow), to 2.0 – Intel.com/fsp
- **Open Source platform code** – Simplified, product quality, open source capable platform package. Built on industry standards and EDK II technology for ease of porting. Upstream platform code. – tianocore.org
- **EDKII** – existing upstream/open source core
- **MinTree** – minimum open source core and platform code to boot shrinkwrap OS

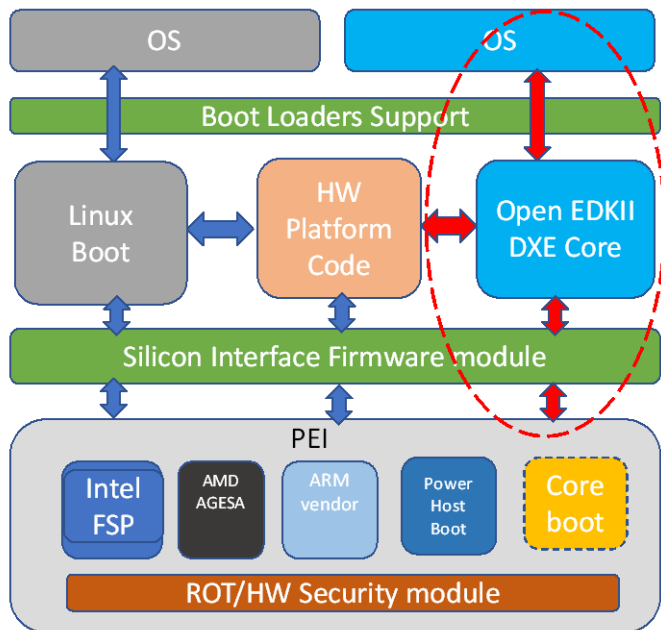


Status on open source host firmware

- Active work stream in Open Compute Conference (OCP) for Open Source http://www.opencompute.org/wiki/Open_System_Firmware
- Intel FSP 2.0 binaries for all client Atom and Core CPU's
- <https://github.com/intelfsp> and other opaque binaries at <https://github.com/tianocore/edk2-non-osi/>
- Open source EDKII platform code for IOT, client and server at <https://github.com/tianocore/edk2-platforms>
- UEFI EDKII core at <https://github.com/tianocore/edk2>
- Open source platforms for Atom, Core and Microserver at <https://github.com/coreboot/coreboot>

EXAMPLES

Open EDK II workstream prog



**<https://github.com/tianocore/edk2-platforms/tree/devel-MinPlatform/Platform>

Open EDK II

- Make comp
- Support mu
- Standardize modules
- Support new interfaces' t
- Simply Setu
- Optimize th
- Serviceabilit
- **Delivered
- Mt.Olympus
- Working on setup option
- IPMI interfa

Let's together accelerate OSF development

phoronix

ARTICLES & REVIEWS

NEWS ARCHIVE

FORUMS

PREMIUM

CATEGORIES

AZULLC
QUANTUM ACCESS

World's Smallest
Windows® PC!

Available at
amazon
BUY NOW



We Rely On Your Support: This site is primarily supported by advertisements. Ads are what have allowed this site to be maintained for the past 14 years. We do our best to ensure only clean, relevant ads are shown, when any nasty ads are detected, we work to remove them ASAP. If you would like to view the site without ads while still supporting our work, please consider our [ad-free Phoronix Premium](#). You can also consider a [tip via PayPal](#).

Intel Has Also Relicensed Their FSP Binaries: A Big Win To Coreboot, LinuxBoot

Written by [Michael Larabel](#) in [Intel](#) on 24 August 2018 at 05:25 AM EDT. 17 Comments



There's some good news beyond [Intel's CPU microcode re-licensing](#) to clear up the confusion among users and developers this week: Intel is also re-licensing their FSP binaries to this same shorter and much more concise license.

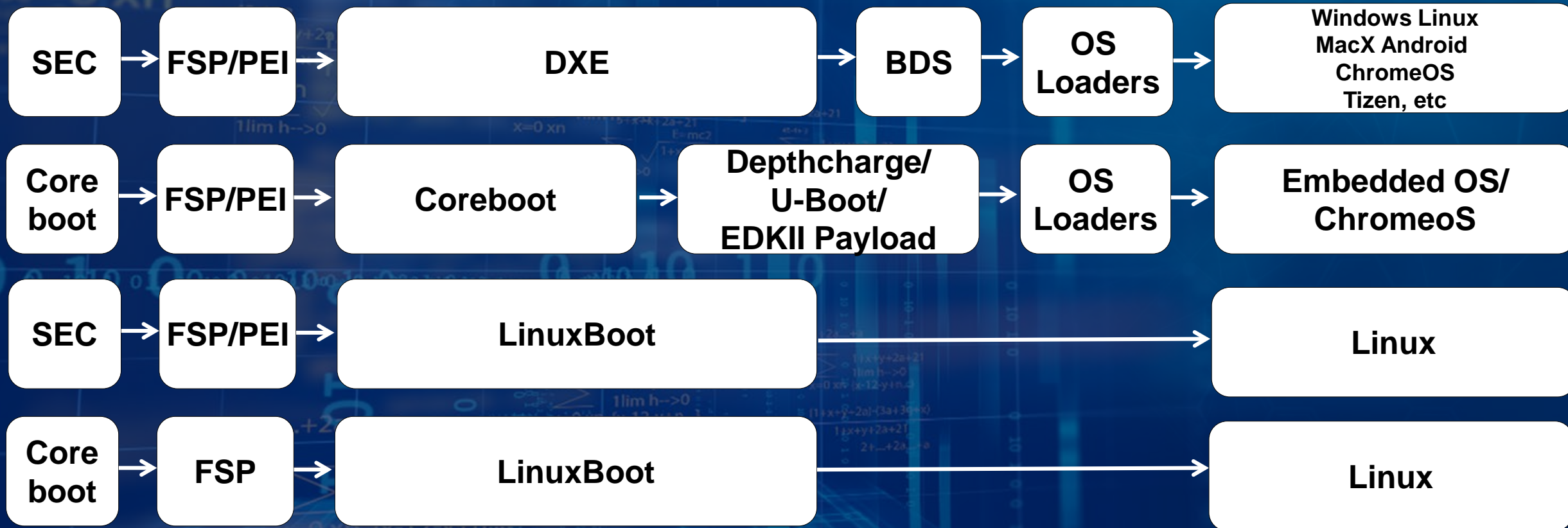
The FSP "Firmware Support Package" binaries used by the likes of Coreboot, [LinuxBoot](#), and Facebook's Open Compute Project is under this same license now as the CPU microcode files. The FSP bits have been closed-source for several generations but are used by Coreboot and friends for allowing their "BIOS" to be as open as possible otherwise. The Intel Firmware Support Package is basically the firmware that initializes the processor, memory controller, chipset, and other certain bits that unfortunately don't have open-source initialization code available.

[Phoronix article](#)

Challenges

- Free up tools
 - Many SI tools are still closed
- Free up SI code
 - Intel FSP considered 'soft' lock down. Can go 2 paths – hard lock-down/boot-rom or liberate code and fully open source
- Documentation delay
 - Open source has to await public documents like EDS
- Debug of binaries
- Rest of the platform
 - Non host firmware

Tying it all up



Path to openness

Open Source core
+ Open Source Platform code
+ Intel FSP binary

Open source core
+ closed source
Silicon Code (MRC)

Open Source core + Open
Source Platform code
+ Intel FSP SDK (source + binary)

All
closed



All
Open
Source

ENGAGEMENT/FEEDBACK

S.

SIMPLICITY: KEEP IT SIMPLE & SCALABLE (KISS)

O.

OPENNESS: DESIGN FOR AN OPEN WORLD

S.

SECURITY: BROADEN OUR APPROACH

Call to action

- Provide feedback on this direction
- Get involved in the various open source firmware and standards activities

More information

- <http://www.uefi.org/>
- <http://www.tianocore.org>
- <https://github.com/tianocore/edk2>
- <https://github.com/tianocore/edk2-platforms>
- <https://github.com/tianocore/tianocore.github.io/wiki/EDK-II-white-papers>
- <https://github.com/IntelFsp/FSP>
- <http://www.intel.com/fsp>
- <http://firmware.intel.com>
- <http://www.coreboot.org>
- <http://opencompute.org/>
- <http://opencompute.org/projects/open-system-firmware/>
- <https://www.apress.com/us/book/9781484200711>
- <https://www.degruyter.com/view/product/484468>
- <https://www.degruyter.com/view/product/484477>
- <https://www.youtube.com/watch?v=Dh6N7Pj1CL>
- https://cansecwest.com/slides/2015/UEFI%20open%20platforms_Vincent.pptx
- <https://github.com/rrbranco/BlackHat2017/blob/master/BlackHat2017-BlackBIOS-v0.13-Published.pdf>
- https://github.com/tianocore/edk2-platforms/blob/develop/MinPlatform/Platform/Intel/MinPlatformPkg/Docs/A_Tour_Beyond_BIOS_Open_Source_IA_Firmware_Platform_Design_Guide_in_EFI_Developer_Kit_II%20-%20V2.pdf
- https://firmware.intel.com/sites/default/files/A_Tour_Beyond_BIOS_Creating_the_Intel_Firmware_Support_Package_with_the_EFI_Developer_Kit_II_%28FSP2.0%29.pdf
- https://firmware.intel.com/sites/default/files/A_Tour_Beyond_BIOS_Using_the_Intel_Firmware_Support_Package_with_the_EFI_Developer_Kit_II_%28FSP2.0%29.pdf
- <https://software.intel.com/en-us/blogs/2018/09/10/designing-firmware-for-an-open-world>
- https://www.phoronix.com/scan.php?page=news_item&px=Intel-Better-FSP-License

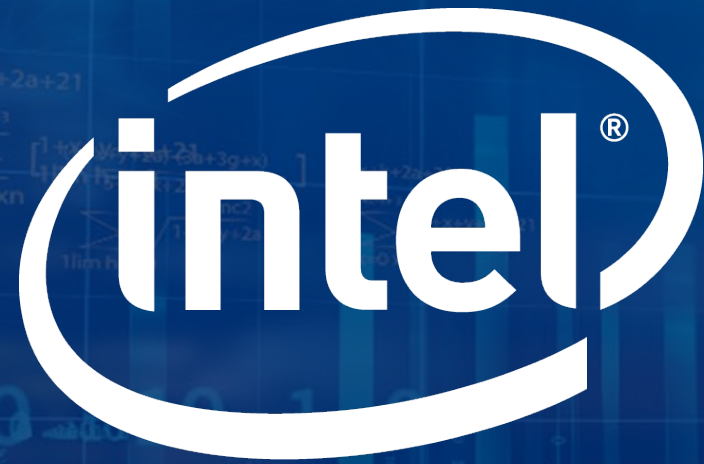
Legal Notice

No computer system can be absolutely secure.

Intel, the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others

© Intel Corporation.



Software