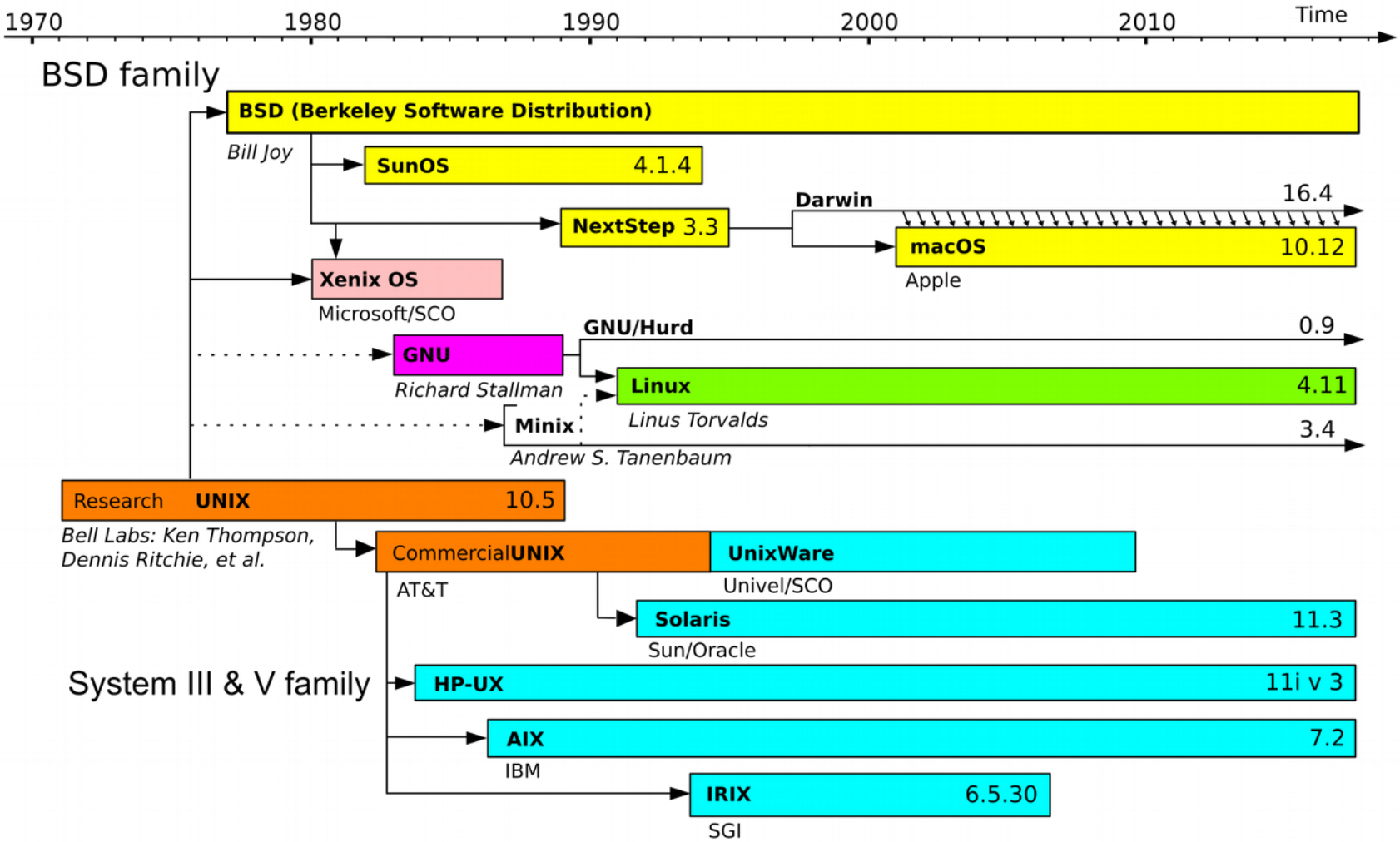
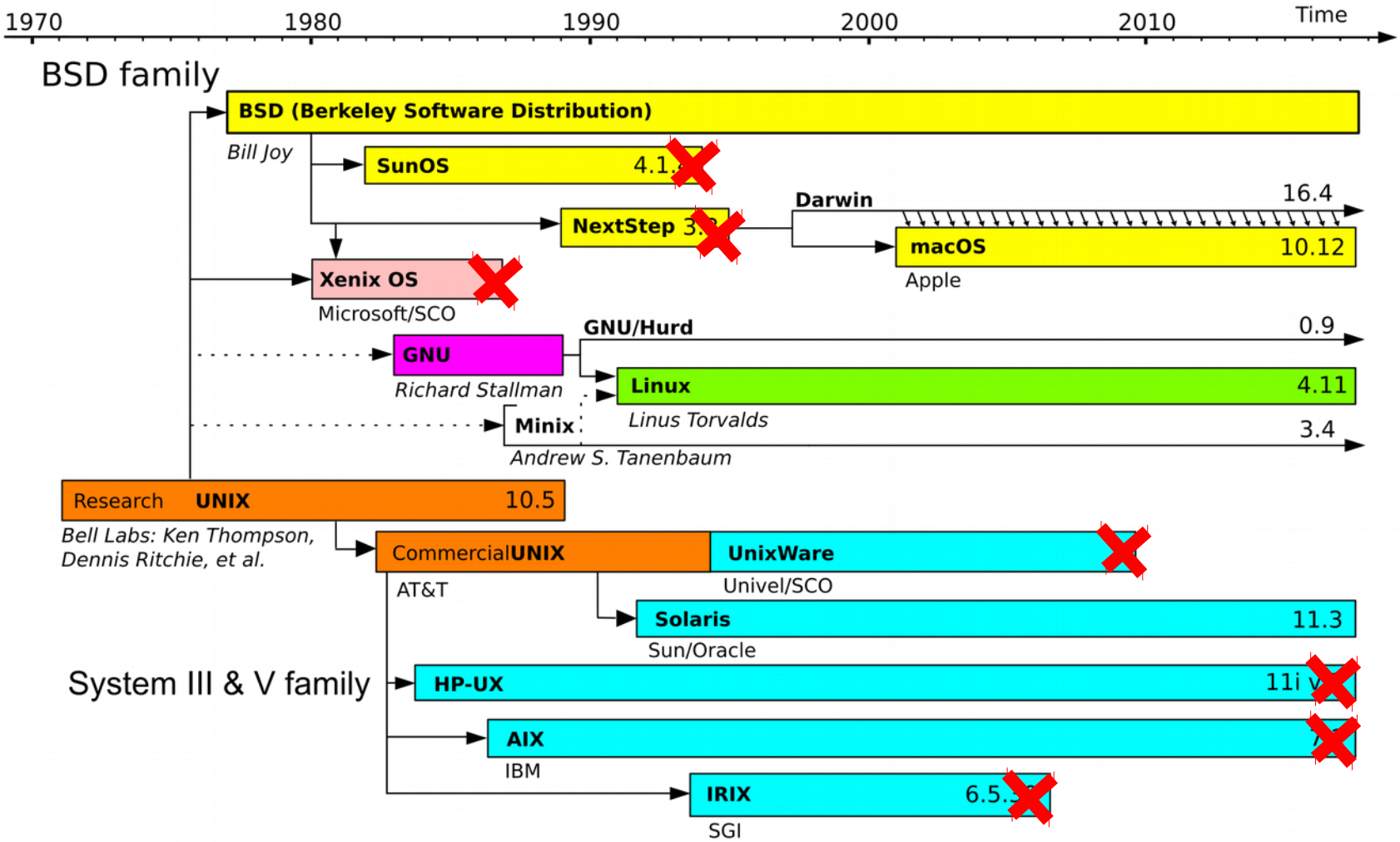
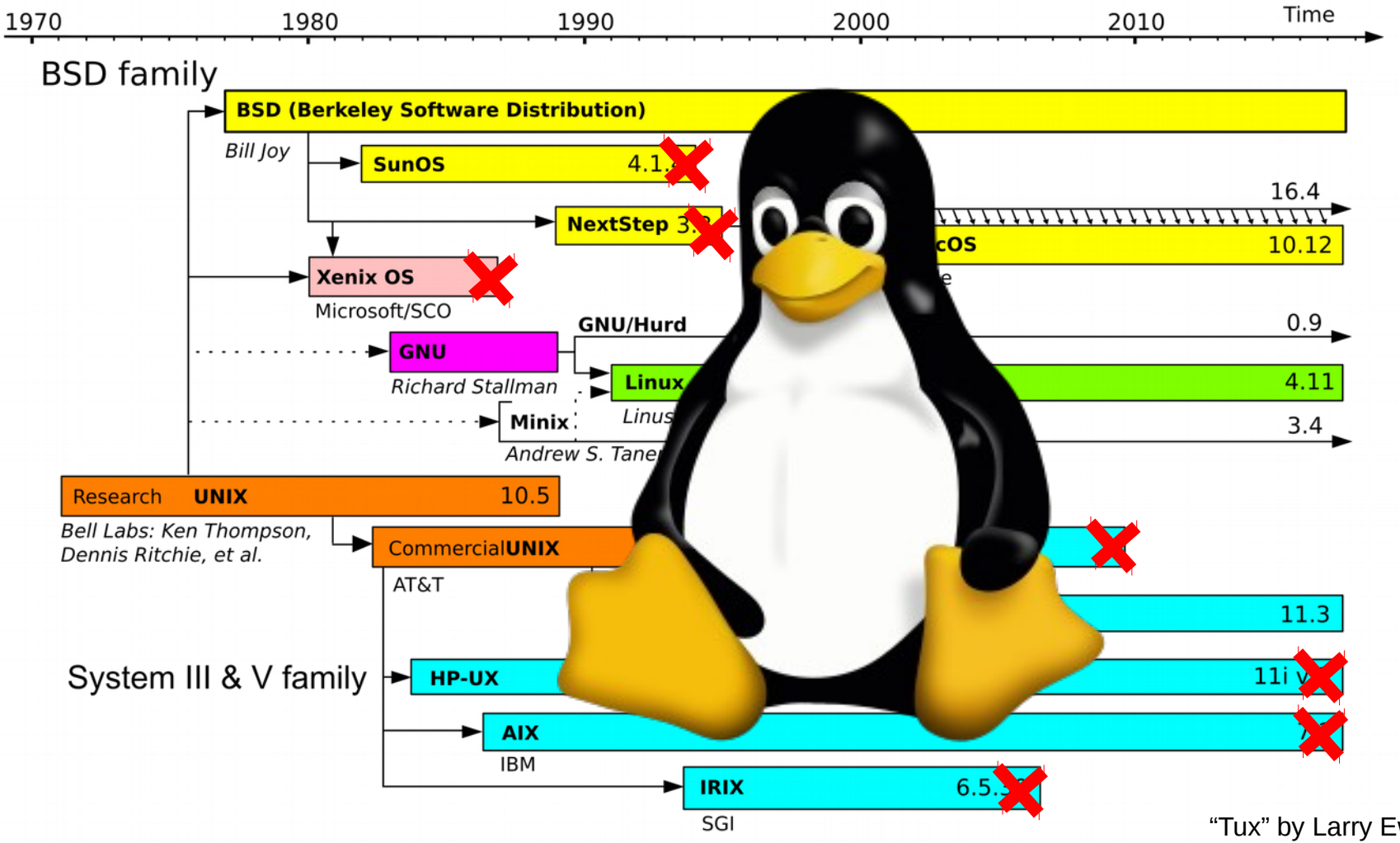
LinuxBoot: Firmware is the new software

Trammell Hudson (Two Sigma Investments)
Ron Minnich (Google)
Andrea Barberio (Facebook)
Jean-Marie Verdun (Horizon Computing)

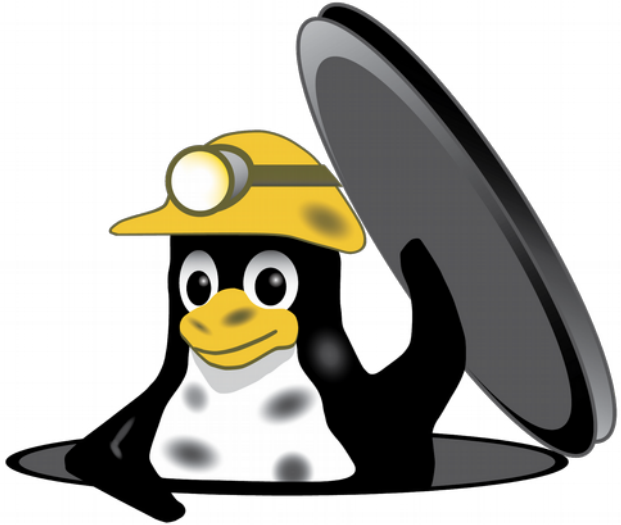

1970
1980
1990
2000
2010
Time
BSD family
BSD (Berkeley Software Distribution)
Bill Joy
SunOS 4.1.4
NextStep 3.3
Darwin
16.4
macOS 10.12
Apple
Xenix OS
Microsoft/SCO
GNU/Hurd
0.9
GNU
Richard Stallman
Linux 4.11
Linus Torvalds
Minix
3.4
Andrew S. Tanenbaum
Research UNIX 10.5
Bell Labs: Ken Thompson,
Dennis Ritchie, et al.
CommercialUNIX
UnixWare
AT&T
Univel/SCO
Solaris 11.3
Sun/Oracle
System III & V family
HP-UX 11i v 3
AIX 7.2
IBM
IRIX 6.5.30
SGI


1970
1980
1990
2000
2010
Time
BSD family
BSD (Berkeley Software Distribution)
Bill Joy
SunOS
4.1.
NextStep 3.
Darwin
16.4
macOS
10.12
Apple
Xenix OS
Microsoft/SCO
GNU
Richard Stallman
GNU/Hurd
0.9
Linux
4.11
Linus Torvalds
Minix
3.4
Andrew S. Tanenbaum
Research UNIX
10.5
Bell Labs: Ken Thompson,
Dennis Ritchie, et al.
CommercialUNIX
AT&T
UnixWare
Univel/SCO
Solaris
11.3
Sun/Oracle
System III & V family
HP-UX
11i v
AIX
IBM
IRIX
6.5.
SGI

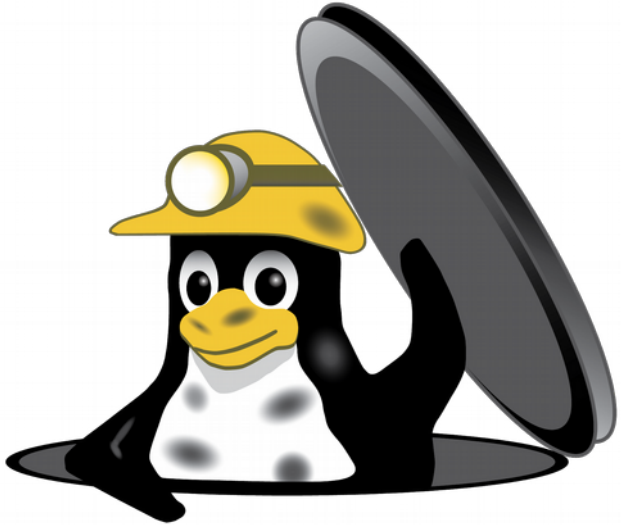


“Tux” by Larry Ewing

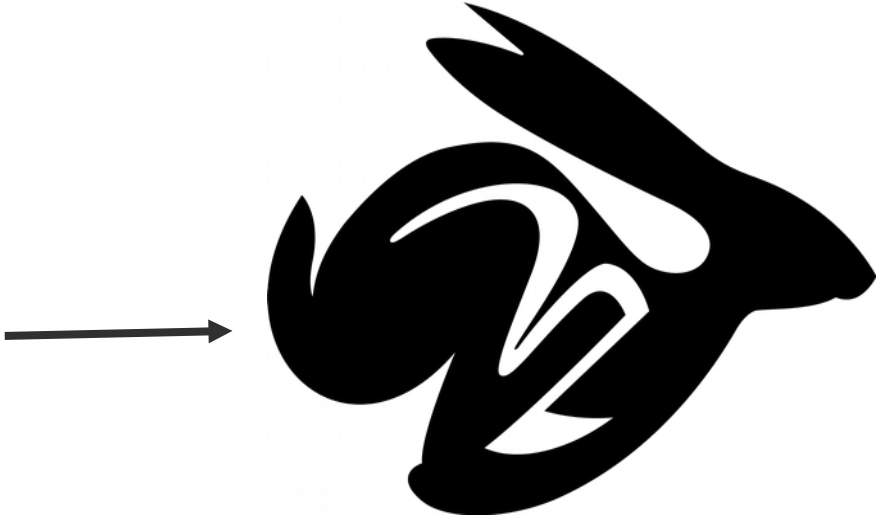

High Resolution
Ocean Mo



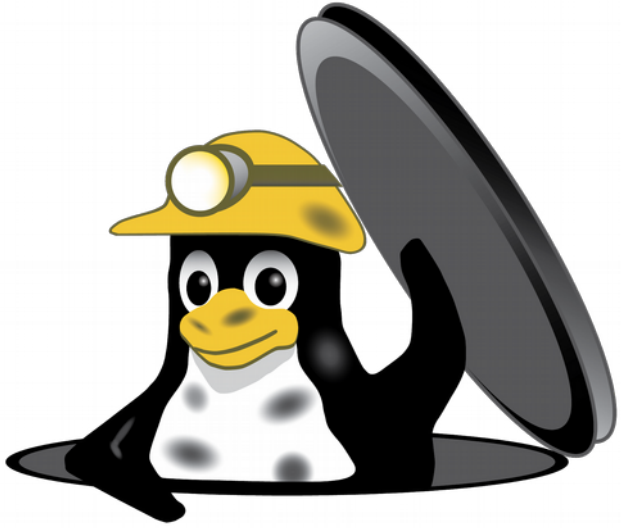
LinuxBIOS
(1999)



LinuxBIOS
(1999)

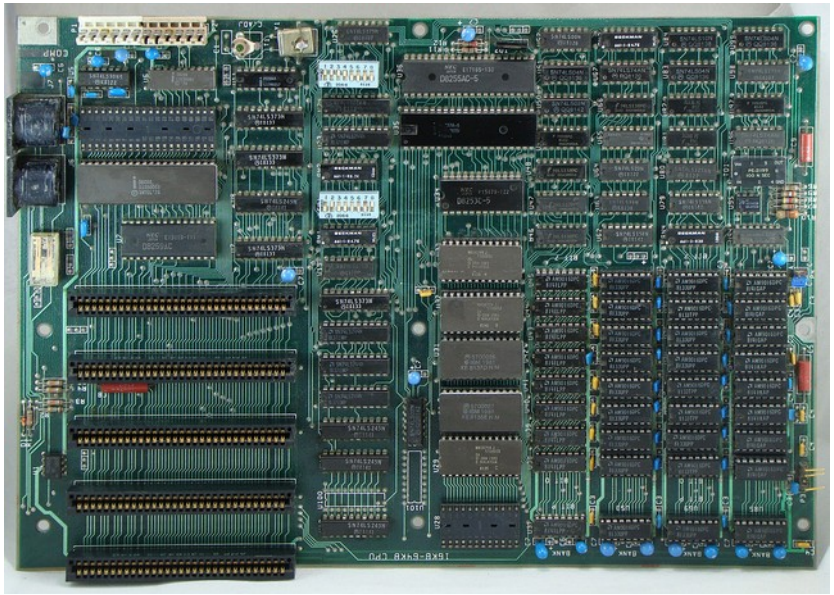


coreboot
(2008)

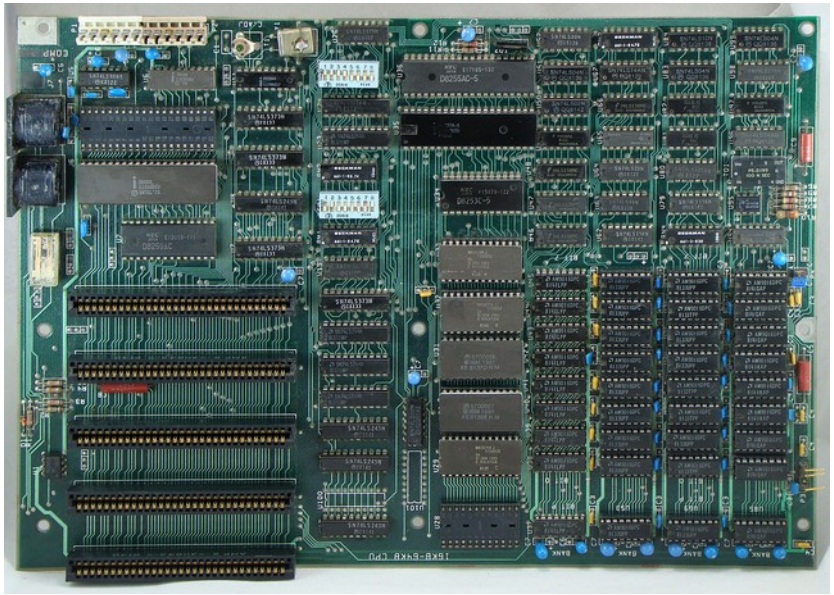


LinuxBIOS
(1999)

coreboot
(2008)

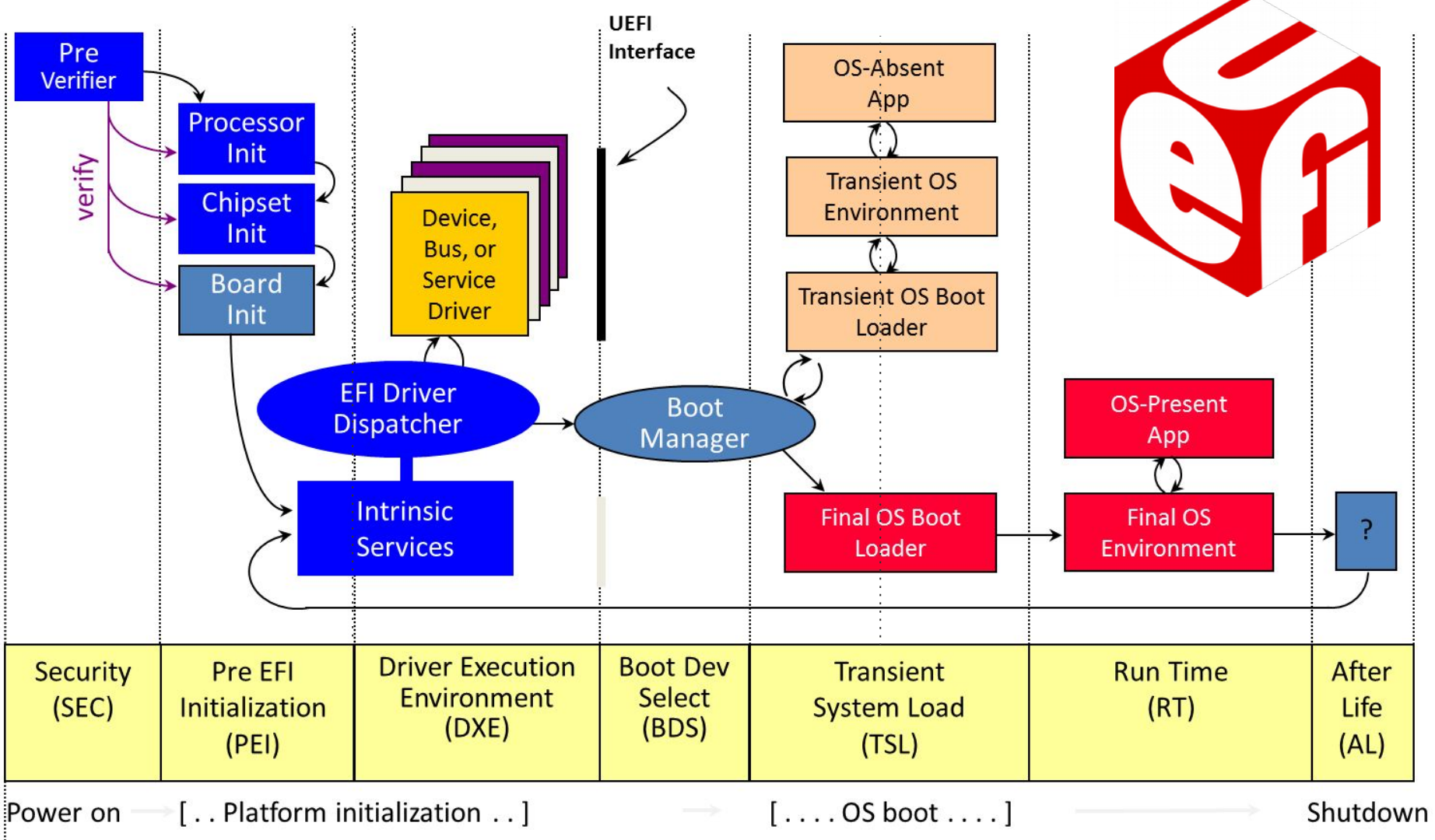


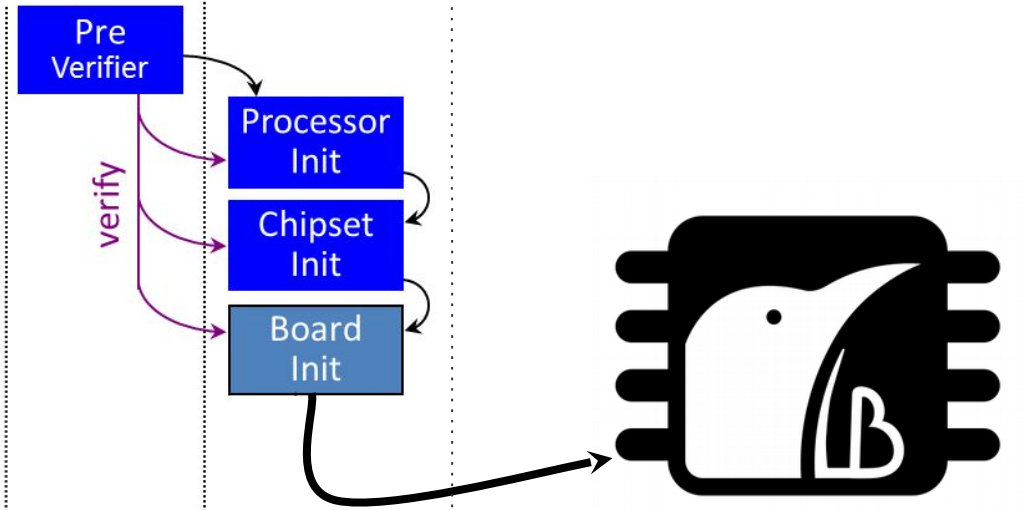
IBM BIOS
(1983)



IBM BIOS
(1983)

Unified Extensible
Firmware Interface
(1995)

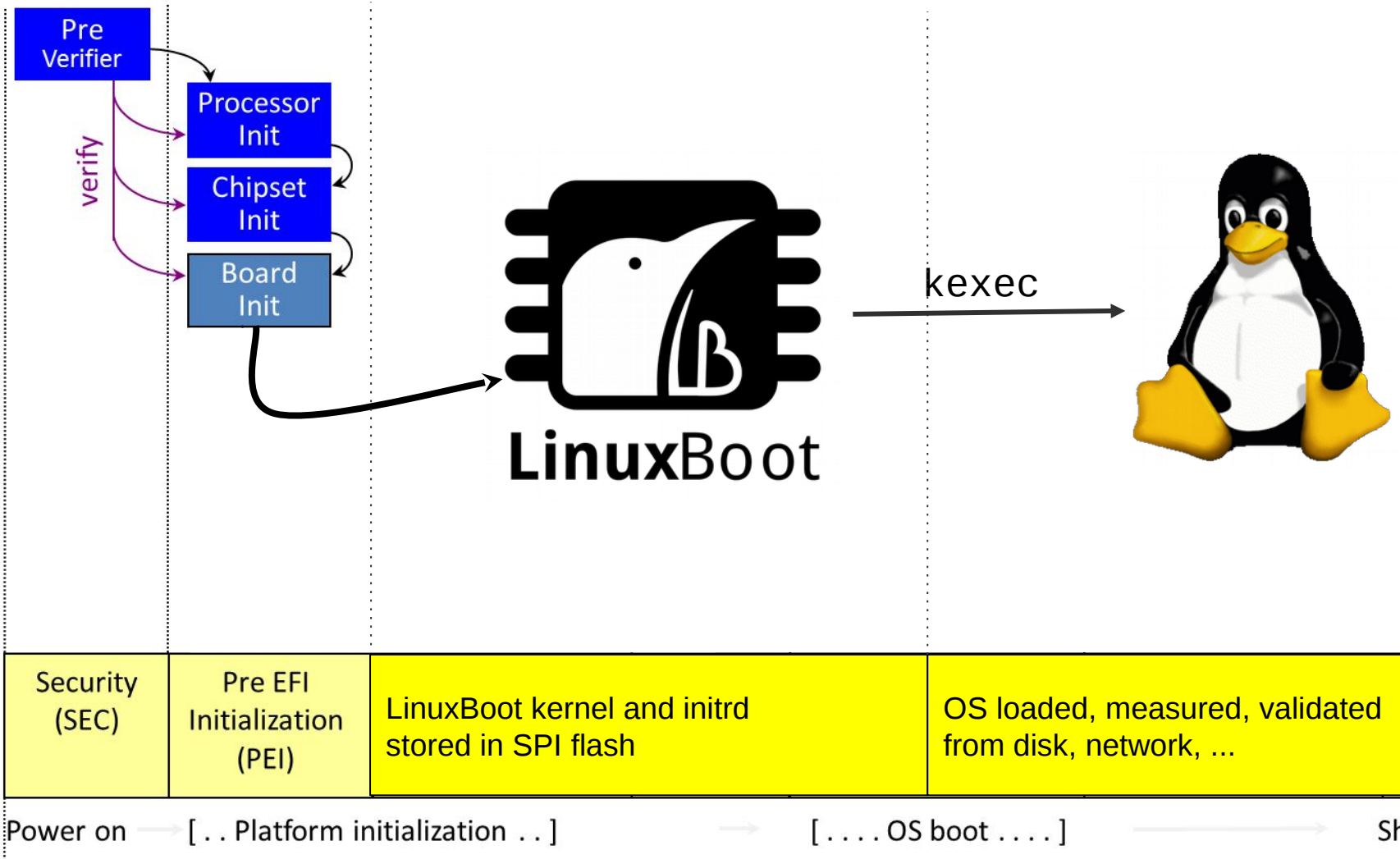

Pre Verifier
verify
Processor Init
Chipset Init
Board Init
Device, Bus, or Service Driver
UEFI Interface
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
EFI Driver Dispatcher
Boot Manager
Intrinsic Services
Final OS Boot Loader
OS-Present App
Final OS Environment
?
Security (SEC)
Pre EFI Initialization (PEI)
Driver Execution Environment (DXE)
Boot Dev Select (BDS)
Transient System Load (TSL)
Run Time (RT)
After Life (AL)
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown

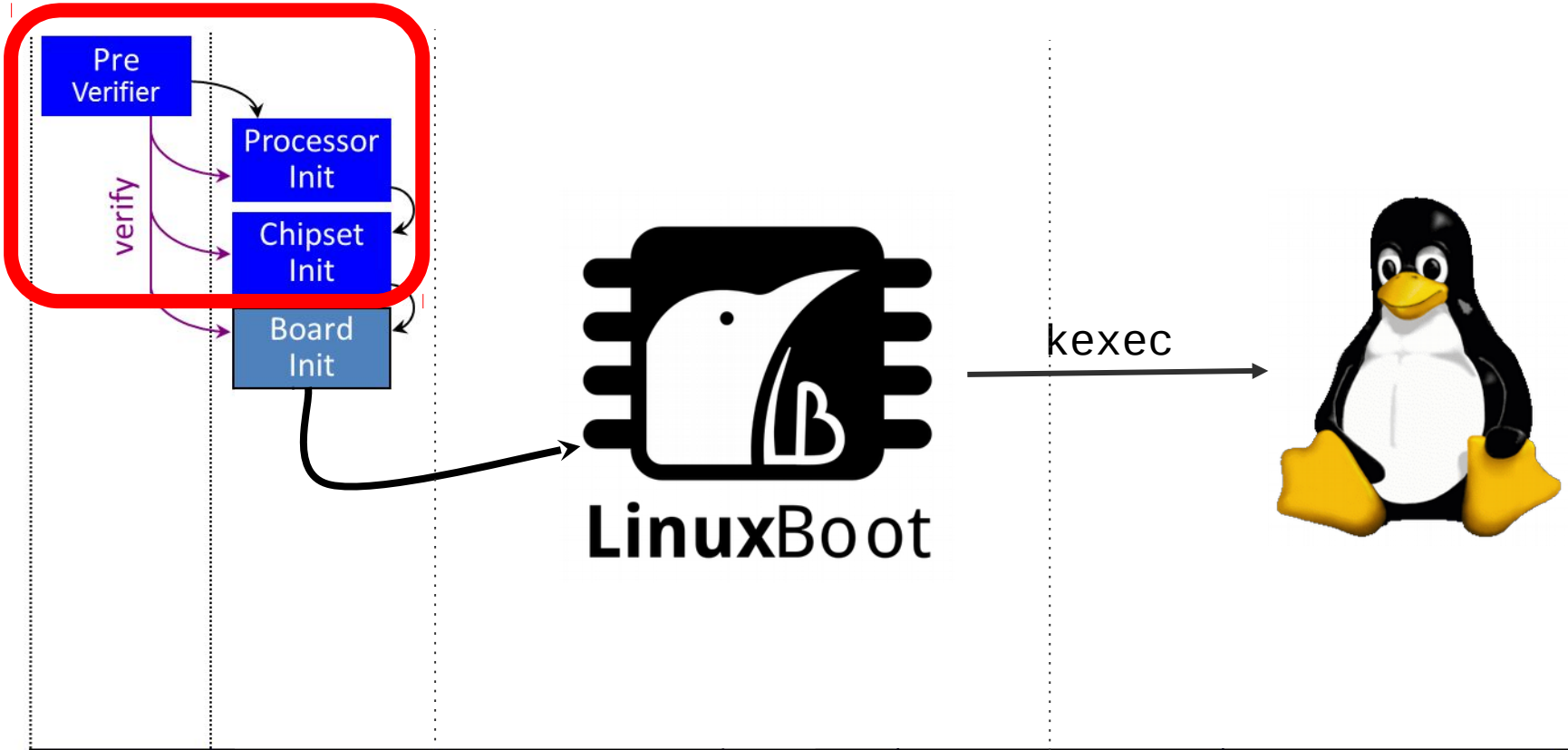


LinuxBoot

Security (SEC)	Pre EFI Initialization (PEI)	LinuxBoot kernel and initrd stored in SPI flash	OS loaded, measured, validated from disk, network, ...

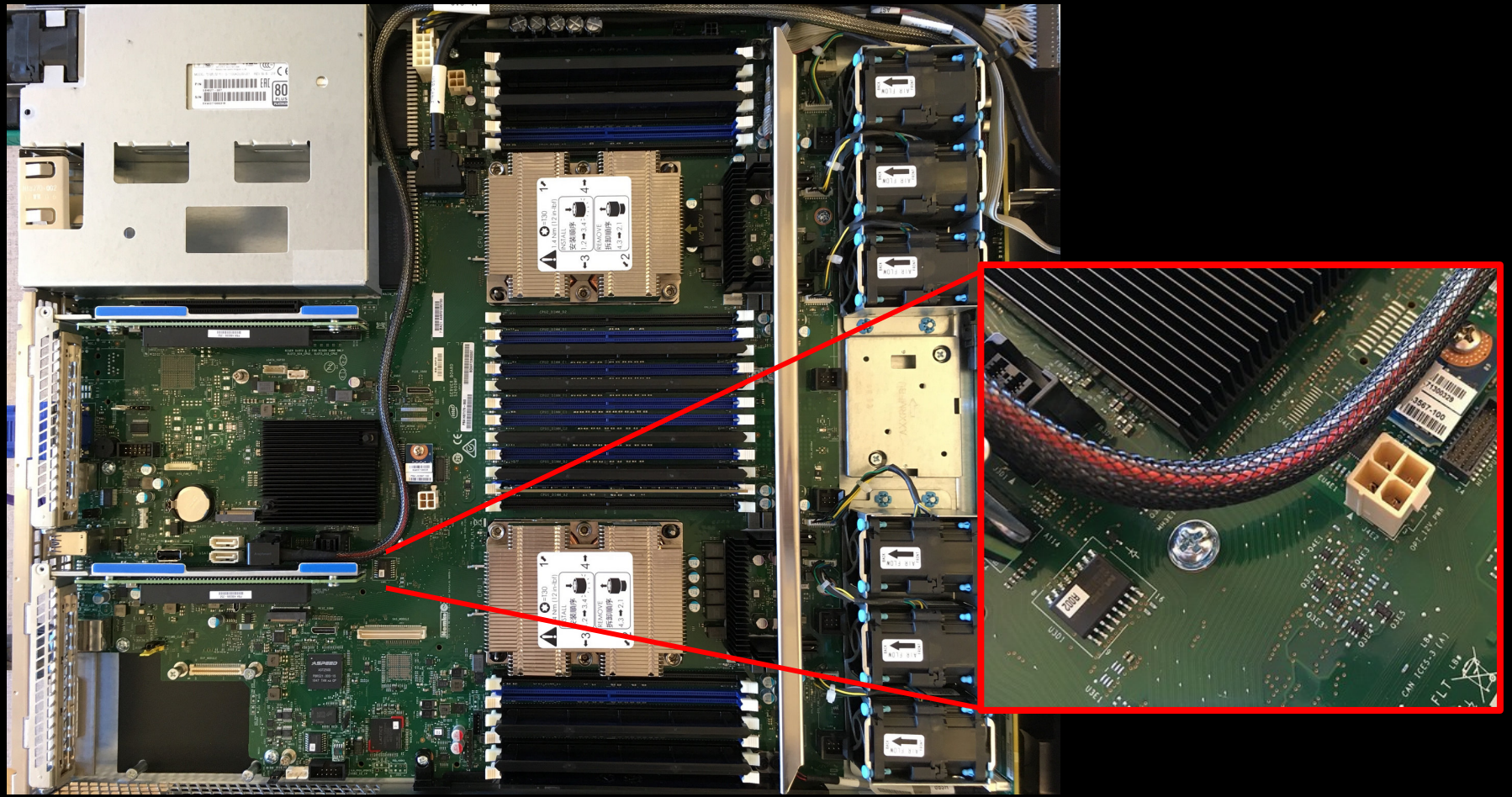
Power on → [. . Platform initialization . .] → [. . . . OS boot . . . .] → Shutdown


Pre Verifier
verify
Processor Init
Chipset Init
Board Init
LinuxBoot
kexec
Security (SEC)
Pre EFI Initialization (PEI)
LinuxBoot kernel and initrd stored in SPI flash
OS loaded, measured, validated from disk, network, ...
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown


Pre Verifier
Processor Init
Chipset Init
Board Init
verify
LinuxBoot
kexec
Security (SEC)
Pre EFI Initialization (PEI)
LinuxBoot kernel and initrd stored in SPI flash
OS loaded, measured, validated from disk, network, ...
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown

Vincent Zimmer from Intel
Presenting after the break!

https://www.intel.com/content/www/us/en/intelligent-systems/intel-firmware-support-package/intel-fsp-overview.html



Intel S2600WF


LinuxBoot.org
LinuxBoot


Open Systems Firmware
Boot Loaders Support
LinuxBoot
Platform Code
UEFI
Silicon Interface Support
Root of Trust /Hardware Security
OPEN. FOR BUSINESS.
OCP
SUMMIT

System Startup Gets a Boost with New LinuxBoot Project

By Mike Dolan | January 25, 2018

Enables Server Setup and Boot with a Linux Kernel

The Linux Foundation is pleased to welcome LinuxBoot to our family of open source projects and to support the growth of the project community. LinuxBoot looks to improve system boot performance and reliability by replacing some firmware functionality with a Linux kernel and runtime.

Firmware has always had a simple purpose: to boot the OS. Achieving that has become much more difficult due to increasing complexity of both hardware and deployment. Firmware often must set up many components in the system, interface with more varieties of boot media, including high-speed storage and networking interfaces, and support advanced protocols and security features

Security
Flexibility
Resiliency

Security

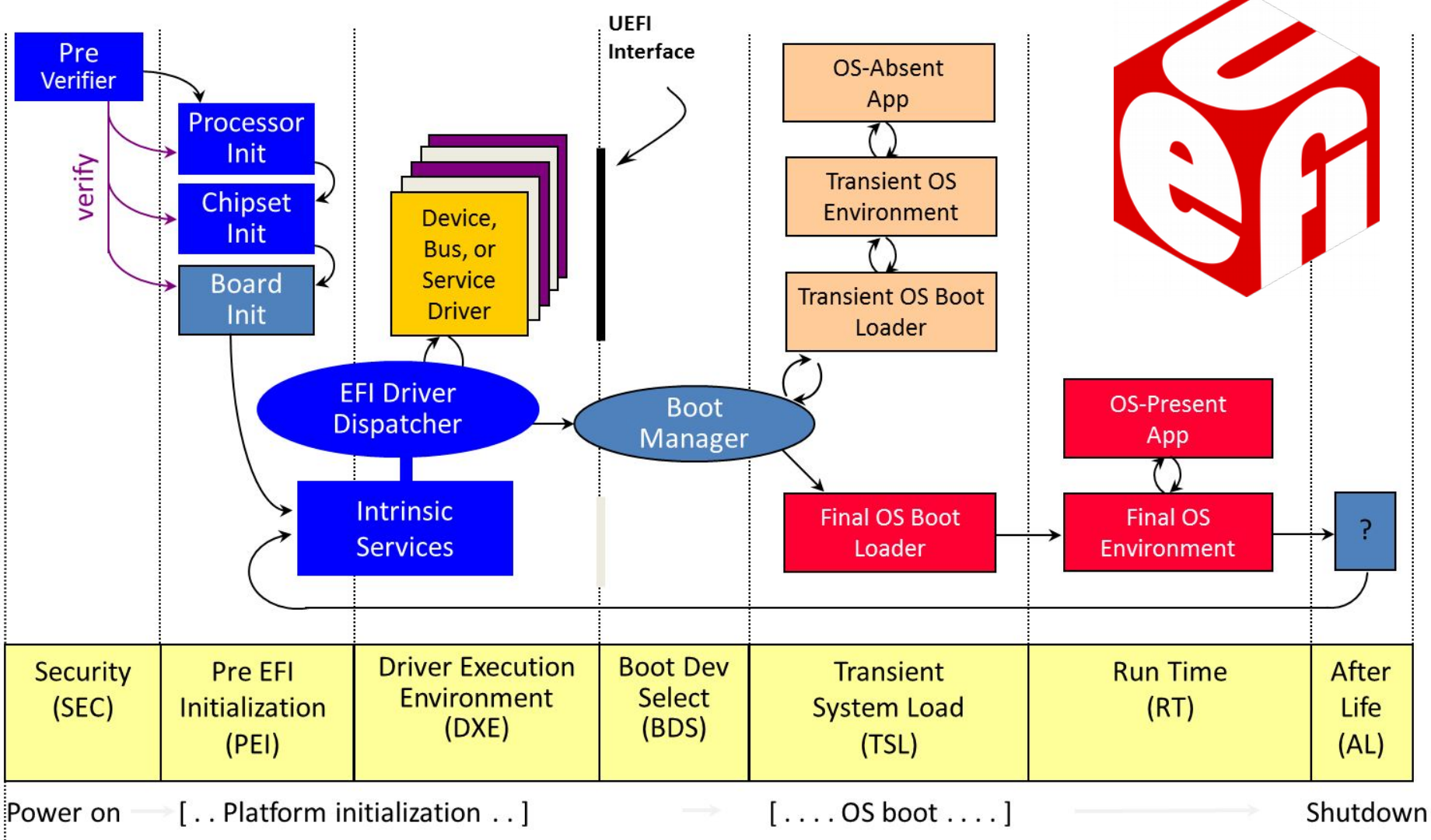
Flexibility

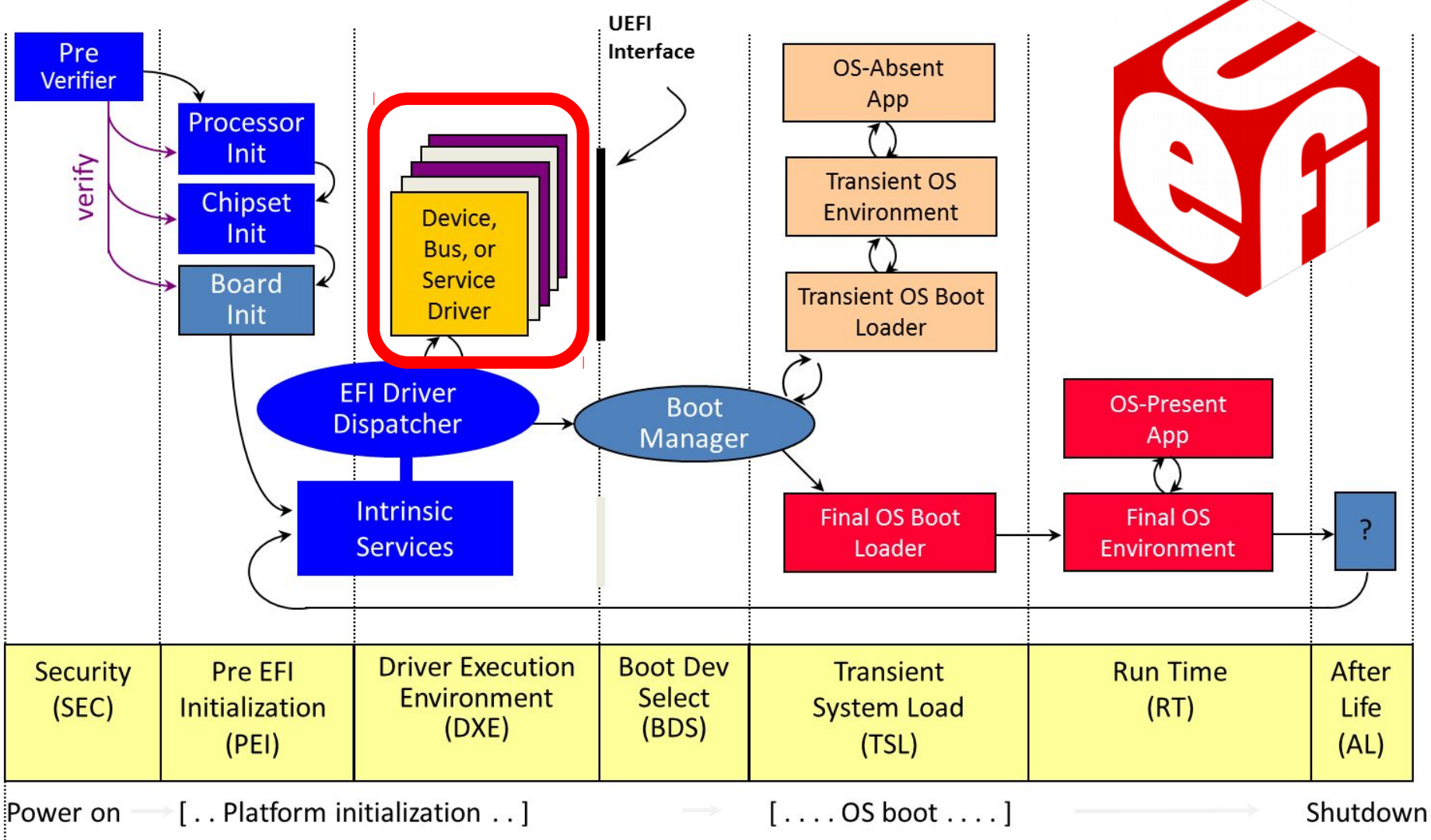
Resiliency

Minimize attack surface

Reduce

~~Minimize~~ attack surface


Pre Verifier
verify
Processor Init
Chipset Init
Board Init
Device, Bus, or Service Driver
UEFI Interface
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
EFI Driver Dispatcher
Boot Manager
OS-Present App
Intrinsic Services
Final OS Boot Loader
Final OS Environment
?
Security (SEC)
Pre EFI Initialization (PEI)
Driver Execution Environment (DXE)
Boot Dev Select (BDS)
Transient System Load (TSL)
Run Time (RT)
After Life (AL)
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown


Pre Verifier
verify
Processor Init
Chipset Init
Board Init
UEFI Interface
Device, Bus, or Service Driver
EFI Driver Dispatcher
Intrinsic Services
Boot Manager
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
Final OS Boot Loader
OS-Present App
Final OS Environment
?
Security (SEC)
Pre EFI Initialization (PEI)
Driver Execution Environment (DXE)
Boot Dev Select (BDS)
Transient System Load (TSL)
Run Time (RT)
After Life (AL)
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown

DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DatahubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDxe
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDxe
UbaInitDxe
StaticSkuDataDxeNeonCityEPRP
SetupConfigUpdateDxeNeonCityEPRP
OpromUpdateDxeNeonCityEPRP
SmbiosDataUpdateDxeNeonCityEPRP
UsbOcUpdateDxeNeonCityEPRP
IioCfgUpdateDxeNeonCityEPRP
SlotDataUpdateDxeNeonCityEPRP
SsidSvidDataUpdateDxeNeonCityEPRP
StaticSkuDataDxeOpalCitySTHI
SetupConfigUpdateDxeOpalCitySTHI
OpromUpdateDxeOpalCitySTHI
SmbiosDataUpdateDxeOpalCitySTHI
UsbOcUpdateDxeOpalCitySTHI
IioCfgUpdateDxeOpalCitySTHI
SlotDataUpdateDxeOpalCitySTHI
SsidSvidDataUpdateDxeOpalCitySTHI
StaticSkuDataDxeWolfPass
SetupConfigUpdateDxeWolfPass
OpromUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
UsbOcUpdateDxeWolfPass
IioCfgUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateWolfPass
DMIMarginUpdateDxeWolfPass
SwitchLedWA
StaticSkuDataDxeBuchananPass
SetupConfigUpdateDxeBuchananPass
OpromUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
UsbOcUpdateDxeBuchananPass
IioCfgUpdateDxeBuchananPass
SlotDataUpdateDxeBuchananPass
RiserPCIeBifurcationDxeBuchananPass
PchUsb2EyeDiagramDxeBuchananPass
SsidSvidDataUpdateDxeBuchananPass
FpkConfigUpdateBuchananPass
BdsUpdateHookBuchananPass
StaticSkuDataDxeLightningRidgeEXRP
SetupConfigUpdateDxeLightningRidgeEXRP
OpromUpdateDxeLightningRidgeEXRP
SmbiosDataUpdateDxeLightningRidgeEXRP
UsbOcUpdateDxeLightningRidgeEXRP
IioCfgUpdateDxeLightningRidgeEXRP
SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
UsbOcUpdateDxeSawtoothPass
IioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass
StaticSkuDataDxeNeonCityFPGA
SetupConfigUpdateDxeNeonCityFPGA
OpromUpdateDxeNeonCityFPGA
SmbiosDataUpdateDxeNeonCityFPGA
UsbOcUpdateDxeNeonCityFPGA
IioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass
OpromUpdateDxeBlueMountainPass
SmbiosDataUpdateDxeBlueMountainPass
UsbOcUpdateDxeBlueMountainPass
IioCfgUpdateDxeBlueMountainPass
SlotDataUpdateDxeBlueMountainPass
PchUsb2EyeDiagramDxeBlueMountainPass
SsidSvidDataUpdateDxeBlueMountainPass
PchHsioCTLEDxeBlueMountainPass
SystemBoardDxe
PlatformType
IioAspmWA
UuidDxe
SpdRawData
SyncSetupVariableToPcd
PlatformStatusCodeHandlerDxe
PlatformStatusCodeHandlerSmm
SysconfigSysinfoHide
PlatformVariableInitDxe
CommonErrorGeneration
ErrorManagerSetup
PostErrorToSel
PlatformPassword
ShellPasswordDxe
PowerOnPassword
VariableSmmRuntimeDxe
SmiVariable
BootManagerMenuApp
IpmiBootOrder
StartupMarkerFileBootOrder
StaticBootOrder
NetworkBootApp
FrontPanelLockout
SataSgpio
SmbiosPcTable
SecureBootErrorHandlerDxe
SecureBootProvisionDxe
SecureBootSetup
SecureBootCtrlDxe
BiosGuardServices
MeSmmProtocolThunk
S3NvramSave
PlatformEarlyDxe
CpuIoDxe
CpuIo2Dxe
HiiDatabase
DataHubDxe
FrameworkHiiAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotIVPc8374
ReserveMem
FwBlockService
FwBlockServiceSmm
LegacyInterruptHookDxe
LegacyBiosReverseThunk
TcgLegacy
TcgLegacyInstallInt1A
SmmFaultTolerantWriteDxe
VariableSmm
SmiVariableInt15
SmiVariableInstallInt15Dxe
MonotonicCounterRuntimeDxe
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcmErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupBmcCfg
ITK50
EarlyBootTimeOut
BootOrderPolicyDxe
SmmNmiButton
NmiButton
SmbiosOobMdr1
SmbiosOobMdr2
MemoryMappingOob
OemPostScreenDisplayDxe
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootMaintSetup
DriverHealthDxe
FdUpdate
ItkLogoProcess
SmiFlashSigned
SINIT
TxtDxe
HstiPlatformDxe
HstiIhvProviderDxe
SnpDxe
DpcDxe
MnpDxe
VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
AcpiTableDxe
BlockIoDxe
BiosSnp16
BiosVideoDxe
ConPlatformDxe
ConSplitterDxe
GraphicsConsoleDxe
TerminalDxe
VgaClassDxe
DataHubStdErrDxe
DiskIoDxe
DevicePathDxe
LegacyRegion2
EbcDxe
NullMemoryTestDxe
PchInitDxe
PchSmbusDxe
PchSmbusSmm
LegacyInterrupt
SecurityInEISS
PchSmiDispatcher
PchInitSmm
SmmControl
SataController
PchSpiRuntime
PchSpiSmm
PchSerialGpio
SmartTimer
PchResetRuntime
WdtDxe
PlatformReset
PowerButtonHandler
TcgMor
Tcg2Dxe
Tcg2Smm
TcgDxe
TcgSmm
BmcAcpiSwChild
PlatformPreVariableDxe
DFSDxe
BmcElog
PlatformErrorGeneration
GenericElog
SmBmcElog
SmGenericElog
IpmiRedirFru
OsWdt
BmcVariableDriver
OemMeFwPatch
SolStatus
FrbDriver
GenericFru
AtaBusDxe
AtaAtapiPassThruDxe
IntelRaidAtaAtapiPassThru
IntelRaidBiosThunk
IncompatiblePciDeviceSupport
IsaBusDxe
IsaSerialDxe
IsaFloppyDxe
LegacyBiosDxe
iBMCVideo
SysCfgSyncDxe
PciPlatform
LegacyBiosPlatform
MEPolicy
NVMDIMMDriver
NVMDIMMHii
SATAAHCI
RSTeSATALegacy
RSTesSATALegacy
RSTeSATAEFI
RSTesSATAEFI
VMDVROC2
VMDVROC1
HfiPcieGen3
iBMCVideoGop
ASTVBIOS
AspeedVideo
PartitionDxe
PciBusDxe
MemorySubClass
SetupBrowser
FpkSetup
PlatformDevsUpdate
DisplayEngine
SmbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatDriOverrideDxe
NvmExpressDxe
ESRTIISataEfi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl
PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
S3SaveStateDxe
AcpiS3SaveDxe
BootGraphicsResourceTableDxe
BootScriptExecutorDxe
SmmLockBox
PiSmmCommunicationSmm
AcpiSmmPlatform
PciHotPlug
PlatformBmc
BreakpointCallbackDxe
UefiOptimizedBootDxe
RtkUsbUndiOptimizeLoad
UbaSetupUpdateDxe
GenerationSetup
HeciInitDxe
MePolicyInitDxe
IePolicyInitDxe
Platform
SmbiosMisc
SmbiosIFWI
RsaBmcCommands
RsaInit
BmcSmbiosDxe
SmbiosItkUpdateDxe
FpgaDxe
FpgaSmm
BmcAcpiDxe
AcpiVTD
GetCpuInfo
SystemSsidSvidProgramDxe
HwpLvtSmm
PlatformCpuBoard
SvSmmSupport
SvSmmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcaErrorLog
WheaErrorLogListener
PprVlsErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiescSupport
IsPlatformSupportWhea
WheaSupport
WheaErrorInj
WheaElog
UncoreErrorLog
PcieErrorLog
PvMode
KtiErrLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog
LastBootErrorLog
McBankErrorInjection
CpuCsrAccess
CpuCsrAccessSMM
CrystalRidge
CrystalRidgeSMM
JedecNvDimm
JedecNvDimmSMM
SerialOverLan
AlertStandardFormatDxe
ActiveManagement
MeFwDowngrade
BiosExtensionLoader
AmtWrapperDxe
AsfTable
AmtPetAlert
AmtInt16
AmtInt16_csm
MeSmbios
Mebx
MebxSetupBrowser
IccPlatform
IccOverClocking
SpsAcpiHooks
SpsDxe
HeciSmm
SpsSmm
Heci3Smm
IioInit
ResetTesting
SocketSetup
FpgaSocketSetup
OpaPlatCfg
OPAPlatConfigSkt0
OPAPlatConfigSkt1
OPAPlatConfig_IFP45b_H79275
OPAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySredir
LegacyBridgeDxe
CblSpecific
RASDXE
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput

DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DatahubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDx
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDx
UbaInitDxe
StaticSkuDataDxeNeonCityEPRP
SetupConfigUpdateDxeNeonCityEPRP
OpromUpdateDxeNeonCityEPRP
SmbiosDataUpdateDxeNeonCityEPRP
UsbOcUpdateDxeNeonCityEPRP
IioCfgUpdateDxeNeonCityEPRP
SlotDataUpdateDxeNeonCityEPRP
SsidSvidDataUpdateDxeNeonCityEPRP
StaticSkuDataDxeOpalCitySTHI
SetupConfigUpdateDxeOpalCitySTHI
OpromUpdateDxeOpalCitySTHI
SmbiosDataUpdateDxeOpalCitySTHI
UsbOcUpdateDxeOpalCitySTHI
IioCfgUpdateDxeOpalCitySTHI
SlotDataUpdateDxeOpalCitySTHI
SsidSvidDataUpdateDxeOpalCitySTHI
StaticSkuDataDxeWolfPass
SetupConfigUpdateDxeWolfPass
OpromUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
UsbOcUpdateDxeWolfPass
IioCfgUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateWolfPass
DMIMarginUpdateDxeWolfPass
SwitchLedWA
StaticSkuDataDxeBuchananPass
SetupConfigUpdateDxeBuchananPass
OpromUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
UsbOcUpdateDxeBuchananPass
IioCfgUpdateDxeBuchananPass
SlotDataUpdateDxeBuchananPass
RiserPCIeBifurcationDxeBuchananPass
PchUsb2EyeDiagramDxeBuchananPass
SsidSvidDataUpdateDxeBuchananPass
FpkConfigUpdateBuchananPass
BdsUpdateHookBuchananPass
StaticSkuDataDxeLightningRidgeEXRP
SetupConfigUpdateDxeLightningRidgeEXRP
OpromUpdateDxeLightningRidgeEXRP
SmbiosDataUpdateDxeLightningRidgeEXRP
UsbOcUpdateDxeLightningRidgeEXRP
IioCfgUpdateDxeLightningRidgeEXRP
SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
UsbOcUpdateDxeSawtoothPass
IioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass
UefiOpromSetup
IioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass
OpromUpdateDxeBlueMountainPass
SmbiosDataUpdateDxeBlueMountainPass
UsbOcUpdateDxeBlueMountainPass
IioCfgUpdateDxeBlueMountainPass
SlotDataUpdateDxeBlueMountainPass
PchUsb2EyeDiagramDxeBlueMountainPass
SsidSvidDataUpdateDxeBlueMountainPass
PchHsioCTLEDxeBlueMountainPass
SystemBoardDxe
PlatformType
IioAspmWA
UuidDxe
SpdRawData
SyncSetupVariableToPcd
PlatformStatusCodeHandlerDxe
PlatformStatusCodeHandlerSmm
SysconfigSysinfoHide
PlatformVariableInitDxe
CommonErrorGeneration
ErrorManagerSetup
PostErrorToSel
PlatformPassword
ShellPasswordDxe
PowerOnPassword
VariableSmmRuntimeDxe
SmiVariable
BootManagerMenuApp
IpmiBootOrder
StartupMarkerFileBootOrder
StaticBootOrder
NetworkBootApp
FrontPanelLockout
SataSgpio
SmbiosPcTable
SecureBootErrorHandlerDxe
SecureBootProvisionDxe
SecureBootSetup
SecureBootCtrlDxe
BiosGuardServices
MeSmmProtocolThunk
S3NvramSave
PlatformEarlyDxe
CpuIoDxe
CpuIo2Dxe
HiiDatabase
DataHubDxe
FrameworkHiiAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotIVPc8374
ReserveMem
FwBlockService
FwBlockServiceSmm
LegacyInterruptHookDxe
LegacyBiosReverseThunk
TcgLegacy
TcgLegacyInstallInt1A
SmmFaultTolerantWriteDxe
VariableSmm
SmiVariableInt15
SmiVariableInstallInt15Dxe
MonotonicCounterRuntimeDxe
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcmErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupBmcCfg
ITK50
EarlyBootTimeOut
BootOrderPolicyDxe
SmmNmiButton
NmiButton
SmbiosOobMdr1
SmbiosOobMdr2
MemoryMappingOob
OemPostScreenDisplayDxe
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootMaintSetup
DriverHealthDxe
FdUpdate
ItkLogoProcess
SmiFlashSigned
SINIT
TxtDxe
HstiPlatformDxe
HstiIhvProviderDxe
SnpDxe
DpcDxe
MnpDxe
VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
AcpiTableDxe
BlockIoDxe
BiosSnp16
BiosVideoDxe
ConPlatformDxe
ConSplitterDxe
GraphicsConsoleDxe
TerminalDxe
VgaClassDxe
DataHubStdErrDxe
DiskIoDxe
DevicePathDxe
LegacyRegion2
EbcDxe
NullMemoryTestDxe
PchInitDxe
PchSmbusDxe
PchSmbusSmm
LegacyInterrupt
SecurityInEISS
PchSmiDispatcher
PchInitSmm
SmmControl
SataController
PchSpiRuntime
PchSpiSmm
PchSerialGpio
SmartTimer
PchResetRuntime
WdtDxe
PlatformReset
PowerButtonHandler
TcgMor
Tcg2Dxe
Tcg2Smm
TcgDxe
TcgSmm
BmcAcpiSwChild
PlatformPreVariableDxe
DFSDxe
BmcElog
PlatformErrorGeneration
GenericElog
SmBmcElog
SmGenericElog
IpmiRedirFru
OsWdt
BmcVariableDriver
OemMeFwPatch
SolStatus
FrbDriver
GenericFru
AtaBusDxe
AtaAtapiPassThruDxe
IntelRaidAtaAtapiPassThru
IntelRaidBiosThunk
IncompatiblePciDeviceSupport
IsaBusDxe
IsaSerialDxe
IsaFloppyDxe
LegacyBiosDxe
iBMCVideo
SysCfgSyncDxe
PciPlatform
LegacyBiosPlatform
MEPolicy
NVMDIMMDriver
NVMDIMMHii
SATAAHCI
RSTeSATALegacy
RSTesSATALegacy
RSTeSATAEFI
RSTesSATAEFI
VMDVROC2
VMDVROC1
HfiPcieGen3
iBMCVideoGop
ASTVBIOS
AspeedVideo
PartitionDxe
PciBusDxe
MemorySubClass
SetupBrowser
FpkSetup
PlatformDevsUpdate
DisplayEngine
SmbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatDriOverrideDxe
NvmExpressDxe
ESRTIISataEfi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl
PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
S3SaveStateDxe
AcpiS3SaveDxe
BootGraphicsResourceTableDxe
BootScriptExecutorDxe
SmmLockBox
PiSmmCommunicationSmm
AcpiSmmPlatform
PciHotPlug
PlatformBmc
BreakpointCallbackDxe
UefiOptimizedBootDxe
RtkUsbUndiOptimizeLoad
UbaSetupUpdateDxe
GenerationSetup
HeciInitDxe
MePolicyInitDxe
IePolicyInitDxe
Platform
SmbiosMisc
SmbiosIFWI
RsaBmcCommands
RsaInit
BmcSmbiosDxe
SmbiosItkUpdateDxe
FpgaDxe
FpgaSmm
BmcAcpiDxe
AcpiVTD
GetCpuInfo
SystemSsidSvidProgramDxe
HwpLvtSmm
PlatformCpuBoard
SvSmmSupport
SvSmmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcaErrorLog
WheaErrorLogListener
PprVlsErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiesceSupport
IsPlatformSupportWhea
WheaSupport
WheaErrorInj
WheaElog
UncoreErrorLog
PcieErrorLog
PvMode
KtiErrLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog
LastBootErrorLog
McBankErrorInjection
CpuCsrAccess
CpuCsrAccessSMM
CrystalRidge
CrystalRidgeSMM
JedecNvDimm
JedecNvDimmSMM
SerialOverLan
AlertStandardFormatDxe
ActiveManagement
MeFwDowngrade
BiosExtensionLoader
AmtWrapperDxe
AsfTable
AmtPetAlert
AmtInt16
AmtInt16_csm
MeSmbios
Mebx
MebxSetupBrowser
IccPlatform
IccOverClocking
SpsAcpiHooks
SpsDxe
HeciSmm
SpsSmm
Heci3Smm
IioInit
ResetTesting
SocketSetup
FpgaSocketSetup
OpaPlatCfg
OPAPlatConfigSkt0
OPAPlatConfigSkt1
OPAPlatConfig_IFP45b_H79275
OPAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySredir
LegacyBridgeDxe
CblSpecific
RASDXE
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput

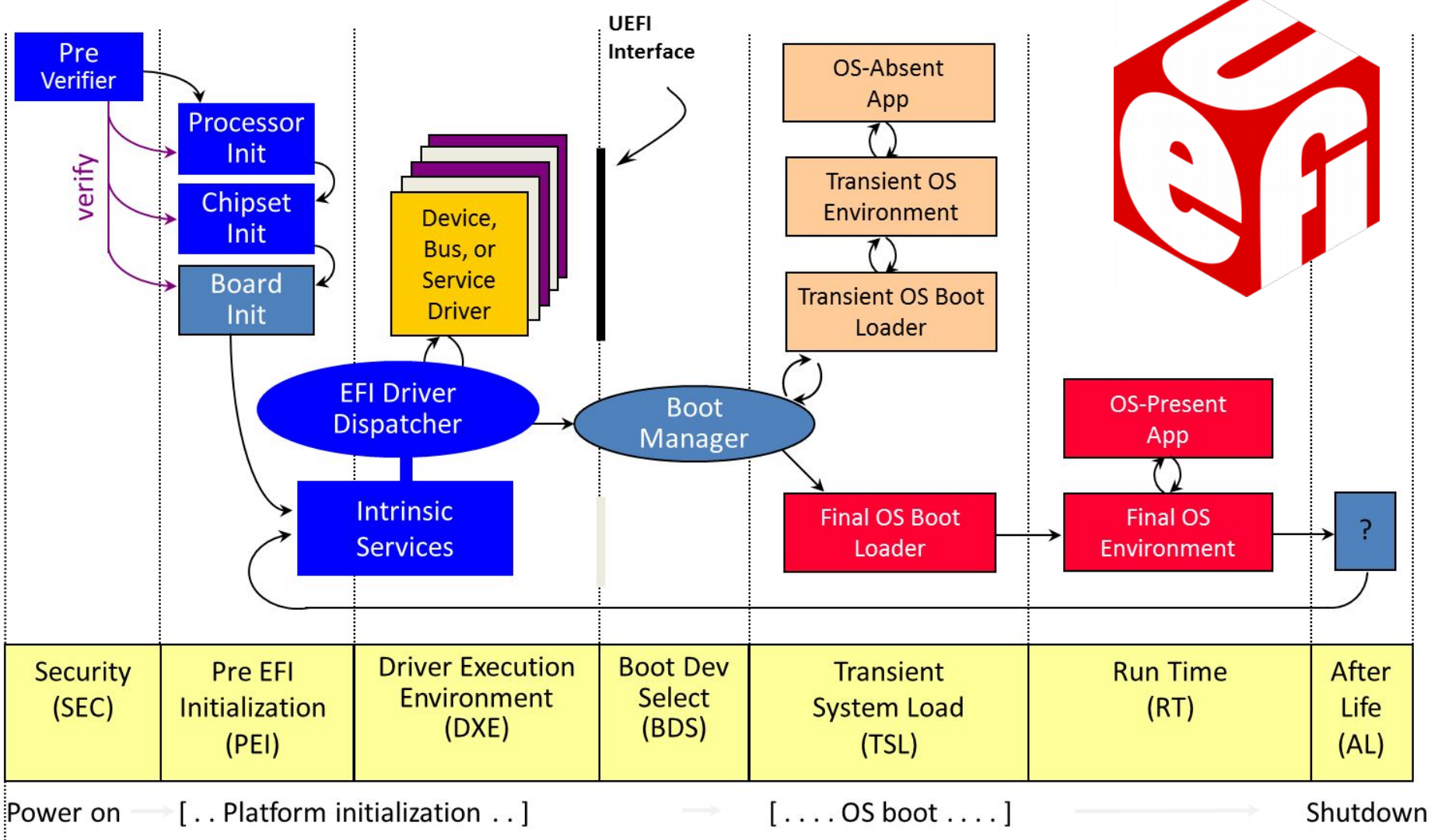
DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DatahubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDx
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDx
UbaInitDxe
StaticSkuDataDxeNeonCityEPRP
SetupConfigUpdateDxeNeonCityEPRP
OpromUpdateDxeNeonCityEPRP
SmbiosDataUpdateDxeNeonCityEPRP
UsbOcUpdateDxeNeonCityEPRP
IioCfgUpdateDxeNeonCityEPRP
SlotDataUpdateDxeNeonCityEPRP
SsidSvidDataUpdateDxeNeonCityEPRP
StaticSkuDataDxeOpalCitySTHI
SetupConfigUpdateDxeOpalCitySTHI
OpromUpdateDxeOpalCitySTHI
SmbiosDataUpdateDxeOpalCitySTHI
UsbOcUpdateDxeOpalCitySTHI
IioCfgUpdateDxeOpalCitySTHI
SlotDataUpdateDxeOpalCitySTHI
SsidSvidDataUpdateDxeOpalCitySTHI
StaticSkuDataDxeWolfPass
SetupConfigUpdateDxeWolfPass
OpromUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
UsbOcUpdateDxeWolfPass
IioCfgUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateWolfPass
DMIMarginUpdateDxeWolfPass
SwitchLedWA
StaticSkuDataDxeBuchananPass
SetupConfigUpdateDxeBuchananPass
OpromUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
UsbOcUpdateDxeBuchananPass
IioCfgUpdateDxeBuchananPass
SlotDataUpdateDxeBuchananPass
RiserPCIeBifurcationDxeBuchananPass
PchUsb2EyeDiagramDxeBuchananPass
SsidSvidDataUpdateDxeBuchananPass
FpkConfigUpdateBuchananPass
BdsUpdateHookBuchananPass
StaticSkuDataDxeLightningRidgeEXRP
SetupConfigUpdateDxeLightningRidgeEXRP
OpromUpdateDxeLightningRidgeEXRP
SmbiosDataUpdateDxeLightningRidgeEXRP
UsbOcUpdateDxeLightningRidgeEXRP
IioCfgUpdateDxeLightningRidgeEXRP
SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
UsbOcUpdateDxeSawtoothPass
IioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass
UefiOpromSetup
IioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass
OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess
IioAspmWA
UuidDxe
SpdRawData
SyncSetupVariableToPcd
PlatformStatusCodeHandlerDxe
PlatformStatusCodeHandlerSmm
SysconfigSysinfoHide
PlatformVariableInitDxe
CommonErrorGeneration
ErrorManagerSetup
PostErrorToSel
PlatformPassword
ShellPasswordDxe
PowerOnPassword
VariableSmmRuntimeDxe
SmiVariable
BootManagerMenuApp
IpmiBootOrder
StartupMarkerFileBootOrder
StaticBootOrder
NetworkBootApp
FrontPanelLockout
SataSgpio
SmbiosPcTable
SecureBootErrorHandlerDxe
SecureBootProvisionDxe
SecureBootSetup
SecureBootCtrlDxe
BiosGuardServices
MeSmmProtocolThunk
S3NvramSave
PlatformEarlyDxe
CpuIoDxe
CpuIo2Dxe
HiiDatabase
DataHubDxe
FrameworkHiiAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotIVPc8374
ReserveMem
kService
kServiceSmm
yInterruptHookDxe
yBiosReverseThunk
gacy
gacyInstallInt1A
ultTolerantWriteDxe
bleSmm
riableInt15
riableInstallInt15Dxe
MonotonicCounterRuntimeDxe
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcmErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupBmcCfg
ITK50
EarlyBootTimeOut
BootOrderPolicyDxe
SmmNmiButton
NmiButton
SmbiosOobMdr1
SmbiosOobMdr2
MemoryMappingOob
OemPostScreenDisplayDxe
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootMaintSetup
DriverHealthDxe
FdUpdate
ItkLogoProcess
SmiFlashSigned
SINIT
TxtDxe
HstiPlatformDxe
HstiIhvProviderDxe
SnpDxe
DpcDxe
MnpDxe
VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
AcpiTableDxe
BlockIoDxe
BiosSnp16
BiosVideoDxe
ConPlatformDxe
ConSplitterDxe
GraphicsConsoleDxe
TerminalDxe
VgaClassDxe
DataHubStdErrDxe
DiskIoDxe
DevicePathDxe
LegacyRegion2
EbcDxe
NullMemoryTestDxe
PchInitDxe
PchSmbusDxe
PchSmbusSmm
LegacyInterrupt
SecurityInEISS
PchSmiDispatcher
PchInitSmm
SmmControl
SataController
PchSpiRuntime
PchSpiSmm
PchSerialGpio
SmartTimer
PchResetRuntime
WdtDxe
PlatformReset
PowerButtonHandler
TcgMor
Tcg2Dxe
Tcg2Smm
TcgDxe
TcgSmm
BmcAcpiSwChild
PlatformPreVariableDxe
DFSDxe
BmcElog
PlatformErrorGeneration
GenericElog
SmBmcElog
SmGenericElog
IpmiRedirFru
OsWdt
BmcVariableDriver
OemMeFwPatch
SolStatus
FrbDriver
GenericFru
AtaBusDxe
AtaAtapiPassThruDxe
IntelRaidAtaAtapiPassThru
IntelRaidBiosThunk
IncompatiblePciDeviceSupport
IsaBusDxe
IsaSerialDxe
IsaFloppyDxe
LegacyBiosDxe
iBMCVideo
SysCfgSyncDxe
PciPlatform
LegacyBiosPlatform
MEPolicy
NVMDIMMDriver
NVMDIMMHii
SATAAHCI
RSTeSATALegacy
RSTesSATALegacy
RSTeSATAEFI
RSTesSATAEFI
VMDVROC2
VMDVROC1
HfiPcieGen3
iBMCVideoGop
ASTVBIOS
AspeedVideo
PartitionDxe
PciBusDxe
MemorySubClass
SetupBrowser
FpkSetup
PlatformDevsUpdate
DisplayEngine
SmbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatDriOverrideDxe
NvmExpressDxe
ESRTIISataEfi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl
PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
S3SaveStateDxe
AcpiS3SaveDxe
BootGraphicsResourceTableDxe
BootScriptExecutorDxe
SmmLockBox
PiSmmCommunicationSmm
AcpiSmmPlatform
PciHotPlug
PlatformBmc
BreakpointCallbackDxe
UefiOptimizedBootDxe
RtkUsbUndiOptimizeLoad
UbaSetupUpdateDxe
GenerationSetup
HeciInitDxe
MePolicyInitDxe
IePolicyInitDxe
Platform
SmbiosMisc
SmbiosIFWI
RsaBmcCommands
RsaInit
BmcSmbiosDxe
SmbiosItkUpdateDxe
FpgaDxe
FpgaSmm
BmcAcpiDxe
AcpiVTD
GetCpuInfo
SystemSsidSvidProgramDxe
HwpLvtSmm
PlatformCpuBoard
SvSmmSupport
SvSmmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcaErrorLog
WheaErrorLogListener
PprVlsErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiesceSupport
IsPlatformSupportWhea
WheaSupport
WheaErrorInj
WheaElog
UncoreErrorLog
PcieErrorLog
PvMode
KtiErrLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog
LastBootErrorLog
McBankErrorInjection
CpuCsrAccess
CpuCsrAccessSMM
CrystalRidge
CrystalRidgeSMM
JedecNvDimm
JedecNvDimmSMM
SerialOverLan
AlertStandardFormatDxe
ActiveManagement
MeFwDowngrade
BiosExtensionLoader
AmtWrapperDxe
AsfTable
AmtPetAlert
AmtInt16
AmtInt16_csm
MeSmbios
Mebx
MebxSetupBrowser
IccPlatform
IccOverClocking
SpsAcpiHooks
SpsDxe
HeciSmm
SpsSmm
Heci3Smm
IioInit
ResetTesting
SocketSetup
FpgaSocketSetup
OpaPlatCfg
OPAPlatConfigSkt0
OPAPlatConfigSkt1
OPAPlatConfig_IFP45b_H79275
OPAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySredir
LegacyBridgeDxe
CblSpecific
RASDXE
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput

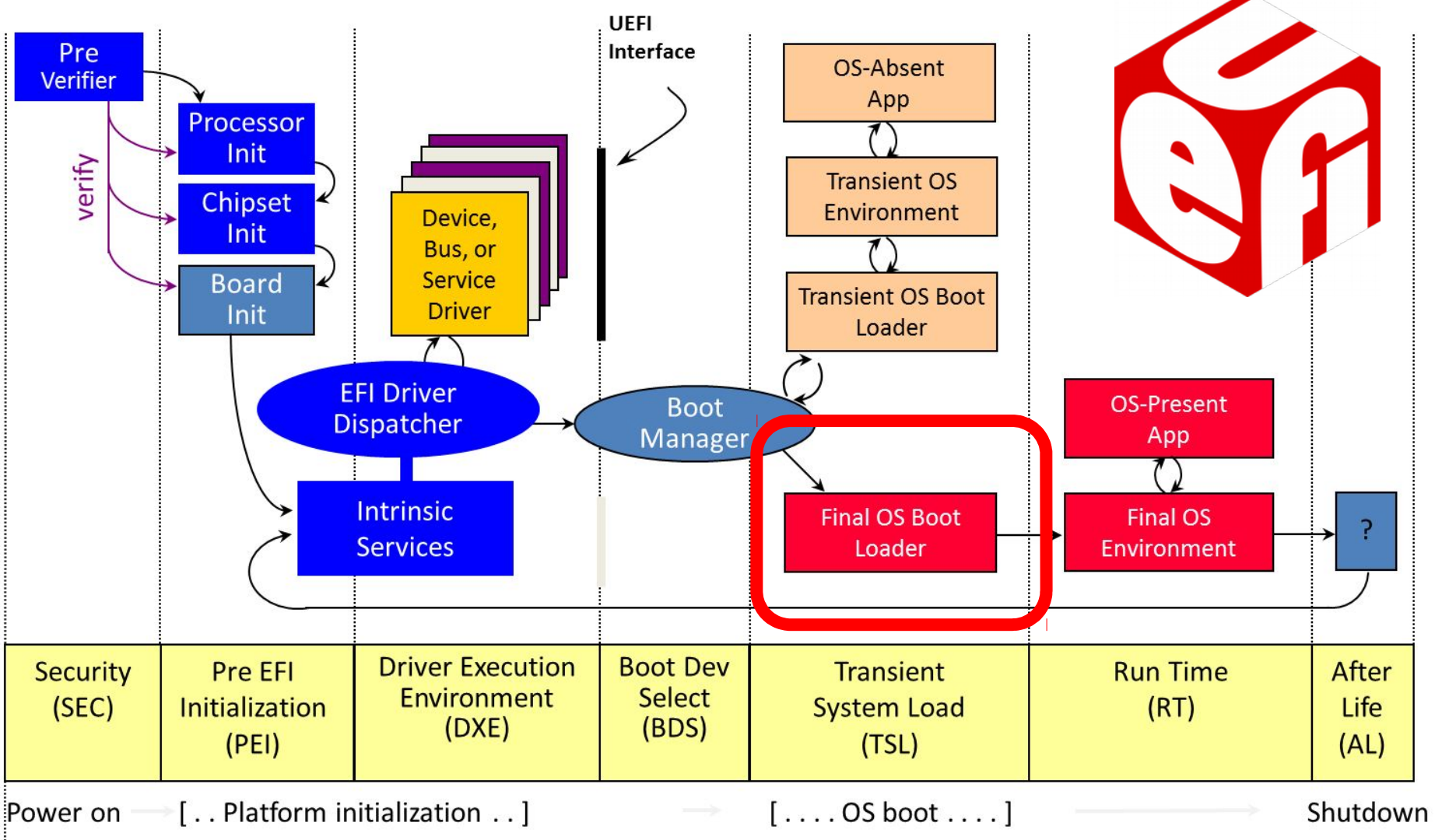
DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DatahubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDx
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDx
UbaInitDxe
StaticSkuDataDxeNeonCityEPRP
SetupConfigUpdateDxeNeonCityEPRP
OpromUpdateDxeNeonCityEPRP
SmbiosDataUpdateDxeNeonCityEPRP
UsbOcUpdateDxeNeonCityEPRP
IioCfgUpdateDxeNeonCityEPRP
SlotDataUpdateDxeNeonCityEPRP
SsidSvidDataUpdateDxeNeonCityEPRP
StaticSkuDataDxeOpalCitySTHI
SetupConfigUpdateDxeOpalCitySTHI
OpromUpdateDxeOpalCitySTHI
SmbiosDataUpdateDxeOpalCitySTHI
UsbOcUpdateDxeOpalCitySTHI
IioCfgUpdateDxeOpalCitySTHI
SlotDataUpdateDxeOpalCitySTHI
SsidSvidDataUpdateDxeOpalCitySTHI
StaticSkuDataDxeWolfPass
SetupConfigUpdateDxeWolfPass
OpromUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
UsbOcUpdateDxeWolfPass
IioCfgUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateWolfPass
DMIMarginUpdateDxeW
SwitchLedWA
StaticSkuDataDxeBuc
SetupConfigUpdateDxeBuchananPass
OpromUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
UsbOcUpdateDxeBuchananPass
IioCfgUpdateDxeBuchananPass
SlotDataUpdateDxeBuchananPass
RiserPCIeBifurcationDxeBuchananPass
PchUsb2EyeDiagramDxeBuchananPass
SsidSvidDataUpdateDxeBuchananPass
FpkConfigUpdateBuchananPass
BdsUpdateHookBuchananPass
StaticSkuDataDxeLightningRidgeEXRP
SetupConfigUpdateDxeLightningRidgeEXRP
OpromUpdateDxeLightningRidgeEXRP
SmbiosDataUpdateDxeLightningRidgeEXRP
UsbOcUpdateDxeLightningRidgeEXRP
IioCfgUpdateDxeLightningRidgeEXRP
SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
UsbOcUpdateDxeSawtoothPass
IioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass
UefiOpromSetup
IioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass
OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess
IioAspmWA
UuidDxe
SpdRawData
SyncSetupVariableToPcd
PlatformStatusCodeHandlerDxe
PlatformStatusCodeHandlerSmm
SysconfigSysinfoHide
PlatformVariableInitDxe
CommonErrorGeneration
ErrorManagerSetup
PostErrorToSel
MsftOemActivation
BootManagerMenuApp
IpmiBootOrder
StartupMarkerFileBootOrder
StaticBootOrder
NetworkBootApp
FrontPanelLockout
SataSgpio
SmbiosPcTable
SecureBootErrorHandlerDxe
SecureBootProvisionDxe
SecureBootSetup
SecureBootCtrlDxe
BiosGuardServices
MeSmmProtocolThunk
S3NvramSave
PlatformEarlyDxe
CpuIoDxe
CpuIo2Dxe
HiiDatabase
DataHubDxe
FrameworkHiiAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotIVPc8374
ReserveMem
kService
kServiceSmm
yInterruptHookDxe
yBiosReverseThunk
gacy
gacyInstallInt1A
ultTolerantWriteDxe
bleSmm
riableInt15
riableInstallInt15Dxe
MonotonicCounterRuntimeDxe
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcmErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupBmcCfg
BootTimeOut
rderPolicyDxe
SmiVariable
SmmAmiButton
NmiButton
SmbiosOobMdr1
SmbiosOobMdr2
MemoryMappingOob
OemPostScreenDisplayDxe
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootMaintSetup
DriverHealthDxe
FdUpdate
ItkLogoProcess
SmiFlashSigned
SINIT
TxtDxe
HstiPlatformDxe
HstiIhvProviderDxe
SnpDxe
DpcDxe
MnpDxe
VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
AcpiTableDxe
BlockIoDxe
BiosSnp16
BiosVideoDxe
ConPlatformDxe
ConSplitterDxe
GraphicsConsoleDxe
TerminalDxe
VgaClassDxe
DataHubStdErrDxe
DiskIoDxe
DevicePathDxe
LegacyRegion2
EbcDxe
NullMemoryTestDxe
PchInitDxe
PchSmbusDxe
PchSmbusSmm
LegacyInterrupt
SecurityInEISS
PchSmiDispatcher
PchInitSmm
SmmControl
SataController
PchSpiRuntime
PchSpiSmm
PchSerialGpio
SmartTimer
PchResetRuntime
WdtDxe
PlatformReset
PowerButtonHandler
TcgMor
Tcg2Dxe
Tcg2Smm
TcgDxe
TcgSmm
BmcAcpiSwChild
PlatformPreVariableDxe
DFSDxe
BmcElog
PlatformErrorGeneration
GenericElog
SmBmcElog
SmGenericElog
IpmiRedirFru
OsWdt
BmcVariableDriver
OemMeFwPatch
SolStatus
FrbDriver
GenericFru
AtaBusDxe
AtaAtapiPassThruDxe
IntelRaidAtaAtapiPassThru
IntelRaidBiosThunk
IncompatiblePciDeviceSupport
IsaBusDxe
IsaSerialDxe
IsaFloppyDxe
LegacyBiosDxe
iBMCVideo
SysCfgSyncDxe
PciPlatform
LegacyBiosPlatform
MEPolicy
NVMDIMMDriver
NVMDIMMHii
SATAAHCI
RSTeSATALegacy
RSTesSATALegacy
RSTeSATAEFI
RSTesSATAEFI
VMDVROC2
VMDVROC1
HfiPcieGen3
iBMCVideoGop
ASTVBIOS
AspeedVideo
PartitionDxe
PciBusDxe
MemorySubClass
SetupBrowser
FpkSetup
PlatformDevsUpdate
DisplayEngine
SmbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatDriOverrideDxe
NvmExpressDxe
ESRTIISataEfi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl
PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
S3SaveStateDxe
AcpiS3SaveDxe
BootGraphicsResourceTableDxe
BootScriptExecutorDxe
SmmLockBox
PiSmmCommunicationSmm
AcpiSmmPlatform
PciHotPlug
PlatformBmc
BreakpointCallbackDxe
UefiOptimizedBootDxe
RtkUsbUndiOptimizeLoad
UbaSetupUpdateDxe
GenerationSetup
HeciInitDxe
MePolicyInitDxe
IePolicyInitDxe
Platform
SmbiosMisc
SmbiosIFWI
RsaBmcCommands
RsaInit
BmcSmbiosDxe
SmbiosItkUpdateDxe
FpgaDxe
FpgaSmm
BmcAcpiDxe
AcpiVTD
GetCpuInfo
SystemSsidSvidProgramDxe
HwpLvtSmm
PlatformCpuBoard
SvSmmSupport
SvSmmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcaErrorLog
WheaErrorLogListener
PprVlsErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiescSupport
IsPlatformSupportWhea
WheaSupport
WheaErrorInj
WheaElog
UncoreErrorLog
PcieErrorLog
PvMode
KtiErrLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog
LastBootErrorLog
McBankErrorInjection
CpuCsrAccess
CpuCsrAccessSMM
CrystalRidge
CrystalRidgeSMM
JedecNvDimm
JedecNvDimmSMM
SerialOverLan
AlertStandardFormatDxe
ActiveManagement
MeFwDowngrade
BiosExtensionLoader
AmtWrapperDxe
AsfTable
AmtPetAlert
AmtInt16
AmtInt16_csm
MeSmbios
Mebx
MebxSetupBrowser
IccPlatform
IccOverClocking
SpsAcpiHooks
SpsDxe
HeciSmm
SpsSmm
Heci3Smm
IioInit
ResetTesting
SocketSetup
FpgaSocketSetup
OpaPlatCfg
OPAPlatConfigSkt0
OPAPlatConfigSkt1
OPAPlatConfig_IFP45b_H79275
OPAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySredir
LegacyBridgeDxe
CblSpecific
RASDXE
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput

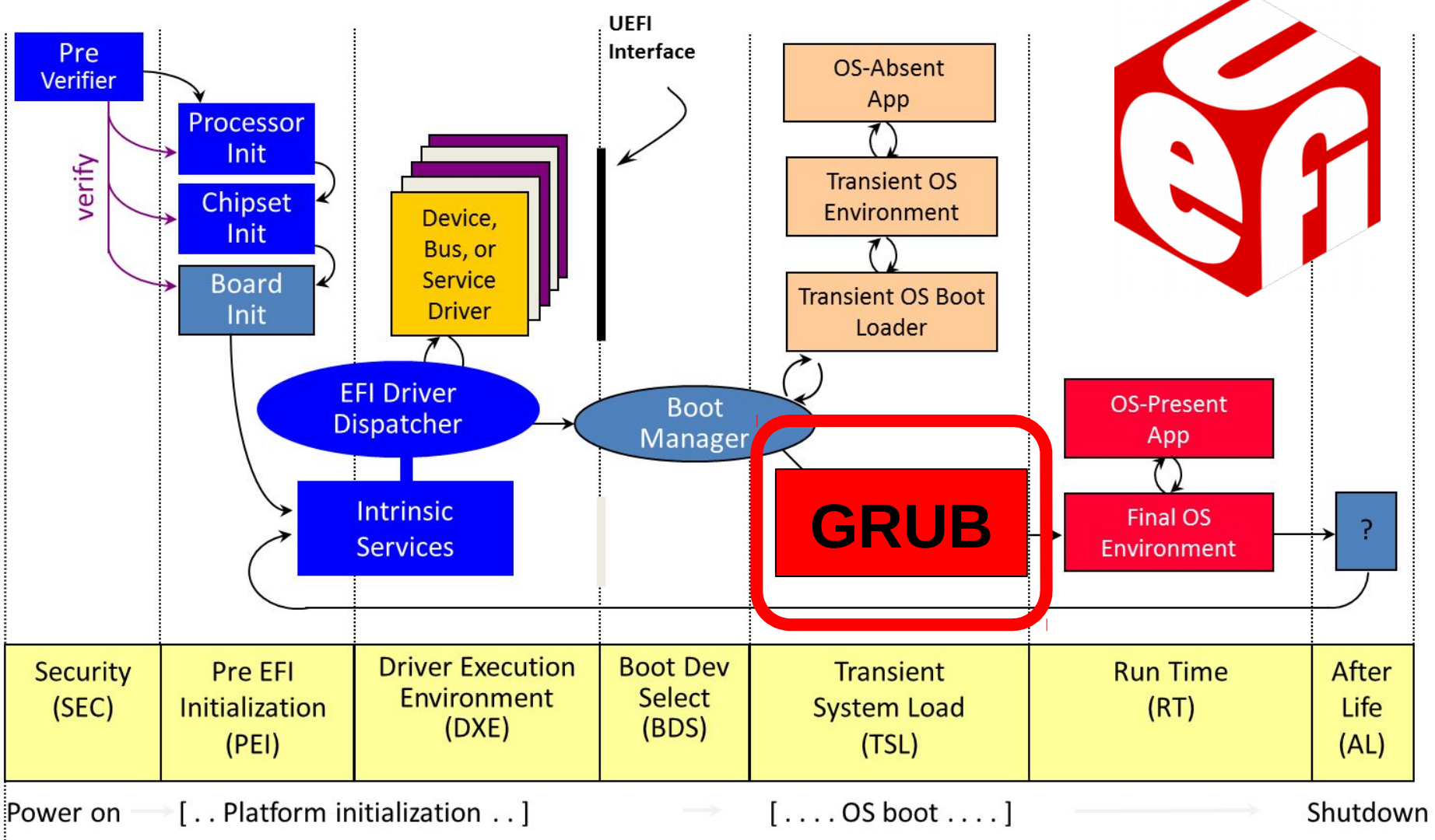

VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
UefiOpromSetup
OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess
MsftOemActivation
DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DatahubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDx
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDx
UbaInitDxe
StaticSkuDataDxeNeonCityEPRP
SetupConfigUpdateDxeNeonCityEPRP
OpromUpdateDxeNeonCityEPRP
SmbiosDataUpdateDxeNeonCityEPRP
UsbOcUpdateDxeNeonCityEPRP
IioCfgUpdateDxeNeonCityEPRP
SlotDataUpdateDxeNeonCityEPRP
SsidSvidDataUpdateDxeNeonCityEPRP
StaticSkuDataDxeOpalCitySTHI
SetupConfigUpdateDxeOpalCitySTHI
OpromUpdateDxeOpalCitySTHI
SmbiosDataUpdateDxeOpalCitySTHI
UsbOcUpdateDxeOpalCitySTHI
IioCfgUpdateDxeOpalCitySTHI
SlotDataUpdateDxeOpalCitySTHI
SsidSvidDataUpdateDxeOpalCitySTHI
StaticSkuDataDxeWolfPass
SetupConfigUpdateDxeWolfPass
OpromUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
UsbOcUpdateDxeWolfPass
IioCfgUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateWolf
DMIMarginUpdateDxeW
SwitchLedWA
StaticSkuDataDxeBuc
SetupConfigUpdateDx
OpromUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
UsbOcUpdateDxeBuchananPass
IioCfgUpdateDxeBuchananPass
SlotDataUpdateDxeBuchananPass
RiserPCIeBifurcationDxeBuchananPass
PchUsb2EyeDiagramDxeBuchananPass
SsidSvidDataUpdateDxeBuchananPass
FpkConfigUpdateBuchananPass
BdsUpdateHookBuchananPass
StaticSkuDataDxeLightningRidgeEXRP
SetupConfigUpdateDxeLightningRidgeEXRP
OpromUpdateDxeLightningRidgeEXRP
SmbiosDataUpdateDxeLightningRidgeEXRP
UsbOcUpdateDxeLightningRidgeEXRP
IioCfgUpdateDxeLightningRidgeEXRP
SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
UsbOcUpdateDxeSawtoothPass
IioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass
IioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass
IioAspmWA
UuidDxe
SpdRawData
SyncSetupVariableToPcd
PlatformStatusCodeHandlerDxe
PlatformStatusCodeHandlerSmm
SysconfigSysinfoHide
PlatformVariableInitDxe
CommonErrorGeneration
ErrorManagerSetup
PostErrorToSel
BootManagerMenuApp
IpmiBootOrder
StartupMarkerFileBootOrder
StaticBootOrder
NetworkBootApp
FrontPanelLockout
SataSgpio
SmbiosPcTable
SecureBootErrorHandlerDxe
SecureBootProvisionDxe
SecureBootSetup
SecureBootCtrlDxe
BiosGuardServices
MeSmmProtocolThunk
S3NvramSave
PlatformEarlyDxe
CpuIoDxe
CpuIo2Dxe
HiiDatabase
DataHubDxe
FrameworkHiiAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotIVPc8374
ckService
ckServiceSmm
yInterruptHookD
yBiosReverseThu
gacy
gacyInstallInt1
ultTolerantWrit
bleSmm
riableInt15
riableInstallIn
MonotonicCounterRunt
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcmErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupBmcCfg
BootTimeOut
rderPolicyDxe
SmmNmiButton
NmiButton
SmbiosOobMdr1
SmbiosOobMdr2
MemoryMappingOob
OemPostScreenDisplay
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootMaintSetup
DriverHealthDxe
FdUpdate
ItkLogoProcess
Smm
AcpiSwChild
tformPreVariableDxe
Dxe
Elog
tformErrorGeneration
nericElog
mcElog
enericElog
iRedirFru
dt
VariableDriver
MeFwPatch
Status
Driver
nericFru
BusDxe
AtapiPassThruDxe
elRaidAtaAtapiPassThru
elRaidBiosThunk
compatiblePciDeviceSupport
BusDxe
SerialDxe
FloppyDxe
gacyBiosDxe
MCVideo
cfgSyncDxe
Platform
gacyBiosPlatform
Policy
DIMMDriver
DIMMHii
AHCI
eSATALegacy
esSATALegacy
eSATAEFI
esSATAEFI
VROC2
VROC1
PcieGen3
MCVideoGop
VBIOS
eedVideo
titionDxe
BusDxe
morySubClass
upBrowser
Setup
tformDevsUpdate
splayEngine
mbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatDriOverrideDxe
NvmExpressDxe
ESRTIISataEfi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl
TcgDxe
PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
S3SaveStateDxe
AcpiS3SaveDxe
BootGraphicsResourceTableDxe
BootScriptExecutorDxe
SmmLockBox
PiSmmCommunicationSmm
AcpiSmmPlatform
PciHotPlug
PlatformBmc
BreakpointCallbackDxe
UefiOptimizedBootDxe
RtkUsbUndiOptimizeLoad
UbaSetupUpdateDxe
GenerationSetup
HeciInitDxe
MePolicyInitDxe
IePolicyInitDxe
Platform
SmbiosMisc
SmbiosIFWI
RsaBmcCommands
RsaInit
BmcSmbiosDxe
SmbiosItkUpdateDxe
FpgaDxe
FpgaSmm
BmcAcpiDxe
AcpiVTD
GetCpuInfo
SystemSsidSvidProgramDxe
HwpLvtSmm
PlatformCpuBoard
SvSmmSupport
SvSmmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcaErrorLog
WheaErrorLogListener
PprVlsErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiesceSupport
IsPlatformSupportWhea
WheaSupport
WheaErrorInj
WheaElog
UncoreErrorLog
PcieErrorLog
PvMode
KtiErrLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog
LastBootErrorLog
McBankErrorInjection
CpuCsrAccess
CpuCsrAccessSMM
CrystalRidge
CrystalRidgeSMM
JedecNvDimm
JedecNvDimmSMM
SerialOverLan
AlertStandardFormatDxe
ActiveManagement
MeFwDowngrade
BiosExtensionLoader
AmtWrapperDxe
AsfTable
AmtPetAlert
AmtInt16
AmtInt16_csm
MeSmbios
Mebx
MebxSetupBrowser
IccPlatform
IccOverClocking
SpsAcpiHooks
SpsDxe
HeciSmm
SpsSmm
Heci3Smm
IioInit
ResetTesting
SocketSetup
FpgaSocketSetup
OpaPlatCfg
OPAPlatConfigSkt0
OPAPlatConfigSkt1
OPAPlatConfig_IFP45b_H79275
OPAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySredir
LegacyBridgeDxe
CblSpecific
RASDXE
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput
PchSpiSmm
PchSerialGpio
SmartTimer
PchResetRuntime
WdtDxe
PlatformReset
PowerButtonHandler
TcgMor
Tcg2Dxe
Tcg2Smm


UefiOpromSetup
OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess
MsftOemActivation
VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
IsaBusDxe
IsaFloppyDxe
IsaSerialDxe
LegacyRegion2
LegacyBiosPlatform
Legacy8259
LegacyInterrupt
LegacyInterruptHookDxe
LegacyBiosDxe


UefiOpromSetup
OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess
MsftOemActivation
VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
IsaBusDxe
IsaFloppyDxe
IsaSerialDxe
LegacyRegion2
LegacyBiosPlatform
Legacy8259
LegacyInterrupt
LegacyInterruptHookDxe
LegacyBiosDxe
Y2KRollover


Pre Verifier
verify
Processor Init
Chipset Init
Board Init
Device, Bus, or Service Driver
UEFI Interface
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
EFI Driver Dispatcher
Boot Manager
OS-Present App
Intrinsic Services
Final OS Boot Loader
Final OS Environment
?
Security (SEC)
Pre EFI Initialization (PEI)
Driver Execution Environment (DXE)
Boot Dev Select (BDS)
Transient System Load (TSL)
Run Time (RT)
After Life (AL)
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown


Pre Verifier
verify
Processor Init
Chipset Init
Board Init
Device, Bus, or Service Driver
UEFI Interface
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
EFI Driver Dispatcher
Boot Manager
Intrinsic Services
Final OS Boot Loader
OS-Present App
Final OS Environment
?
Security (SEC)
Pre EFI Initialization (PEI)
Driver Execution Environment (DXE)
Boot Dev Select (BDS)
Transient System Load (TSL)
Run Time (RT)
After Life (AL)
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown


Pre Verifier
verify
Processor Init
Chipset Init
Board Init
Device, Bus, or Service Driver
UEFI Interface
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
EFI Driver Dispatcher
Boot Manager
Intrinsic Services
GRUB
OS-Present App
Final OS Environment
?
Security (SEC)
Pre EFI Initialization (PEI)
Driver Execution Environment (DXE)
Boot Dev Select (BDS)
Transient System Load (TSL)
Run Time (RT)
After Life (AL)
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown


GNU GRUB version 2.02~beta2-29
*Debian GNU/Linux
Advanced options for Debian GNU/Linux
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.

SLOC	Directory	SLOC-by-Language (Sorted)
69604	lib	ansic=63197,asm=6268,sh=139
30594	gnulib	ansic=30102,sh=492
23599	fs	ansic=23599
15250	kern	ansic=13791,asm=1459
15027	loader	ansic=15027
14598	commands	ansic=14531,asm=67
11856	video	ansic=11856
11237	disk	ansic=11237
8518	osdep	ansic=8518
7528	net	ansic=7528
6788	normal	ansic=6788
5911	term	ansic=5911
5246	bus	ansic=5246
4436	gfxmenu	ansic=4436
3498	tests	ansic=2978,asm=520
2659	boot	asm=2540,ansic=119
2579	efiemu	ansic=2466,asm=113
2384	script	ansic=1723,lex=393,yacc=268
1784	io	ansic=1784
1480	partmap	ansic=1480
1262	font	ansic=1262
1128	mmap	ansic=994,asm=134
559	gdb	ansic=396,asm=163
419	gettext	ansic=419
340	top_dir	sh=234,awk=75,ansic=31
112	parttool	ansic=112
79	hook	ansic=79

generated using David A. Wheeler's 'SLOCCount'

SLOC	Directory	SLOC-by-Language (Sorted)
69604	lib	ansic=63197,asm=6268,sh=139
30594	gnulib	ansic=30102,sh=492
23599	fs	ansic=23599
15250	kern	ansic=13791,asm=1459
15027	loader	ansic=15027
14598	commands	ansic=14531,asm=67
11856	video	ansic=11856
11237	disk	ansic=11237
8518	osdep	ansic=8518
7528	net	ansic=7528
6788	normal	ansic=6788
5911	term	ansic=5911
5246	bus	ansic=5246
4436	gfxmenu	ansic=4436
3498	tests	ansic=2978,asm=520
2659	boot	asm=2540,ansic=119
2579	efiemu	ansic=2466,asm=113
2384	script	ansic=1723,lex=393,yacc=268
1784	io	ansic=1784
1480	partmap	ansic=1480
1262	font	ansic=1262
1128	mmap	ansic=994,asm=134
559	gdb	ansic=396,asm=163
419	gettext	ansic=419
340	top_dir	sh=234,awk=75,ansic=31
112	parttool	ansic=112
79	hook	ansic=79

generated using David A. Wheeler's 'SLOCCount'

SLOC	Directory	SLOC-by-Language (Sorted)
69604	lib	ansic=63197,asm=6268,sh=139
30594	gnulib	ansic=30102,sh=492
23599	fs	ansic=23599
15250	kern	ansic=13791,asm=1459
15027	loader	ansic=15027
14598	commands	ansic=14531,asm=67
11856	video	ansic=11856
11237	disk	ansic=11237
8518	osdep	ansic=8518
7528	net	ansic=7528
6788	normal	ansic=6788
5911	term	ansic=5911
5246	bus	ansic=5246
4436	gfxmenu	ansic=4436
3498	tests	ansic=2978,asm=520
2659	boot	asm=2540,ansic=119
2579	efiemu	ansic=2466,asm=113
2384	script	ansic=1723,lex=393,yacc=268
1784	io	ansic=1784
1480	partmap	ansic=1480
1262	font	ansic=1262
1128	mmap	ansic=994,asm=134
559	gdb	ansic=396,asm=163
419	gettext	ansic=419
340	top_dir	sh=234,awk=75,ansic=31
112	parttool	ansic=112
79	hook	ansic=79

generated using David A. Wheeler's 'SLOCCount'

SLOC	Directory	SLOC-by-Language (Sorted)
69604	lib	ansic=63197,asm=6268,sh=139
30594	gnulib	ansic=30102,sh=492
23599	fs	ansic=23599
15250	kern	ansic=13791,asm=1459
15027	loader	ansic=15027
14598	commands	ansic=14531,asm=67
11856	video	ansic=11856
11237	disk	ansic=11237
8518	osdep	ansic=8518
7528	net	ansic=7528
6788	normal	ansic=6788
5911	term	ansic=5911
5246	bus	ansic=5246
4436	gfxmenu	ansic=4436
3498	tests	ansic=2978,asm=520
2659	boot	asm=2540,ansic=119
2579	efiemu	ansic=2466,asm=113
2384	script	ansic=1723,lex=393,yacc=268
1784	io	ansic=1784
1480	partmap	ansic=1480
1262	font	ansic=1262
1128	mmap	ansic=994,asm=134
559	gdb	ansic=396,asm=163
419	gettext	ansic=419
340	top_dir	sh=234,awk=75,ansic=31
112	parttool	ansic=112
79	hook	ansic=79

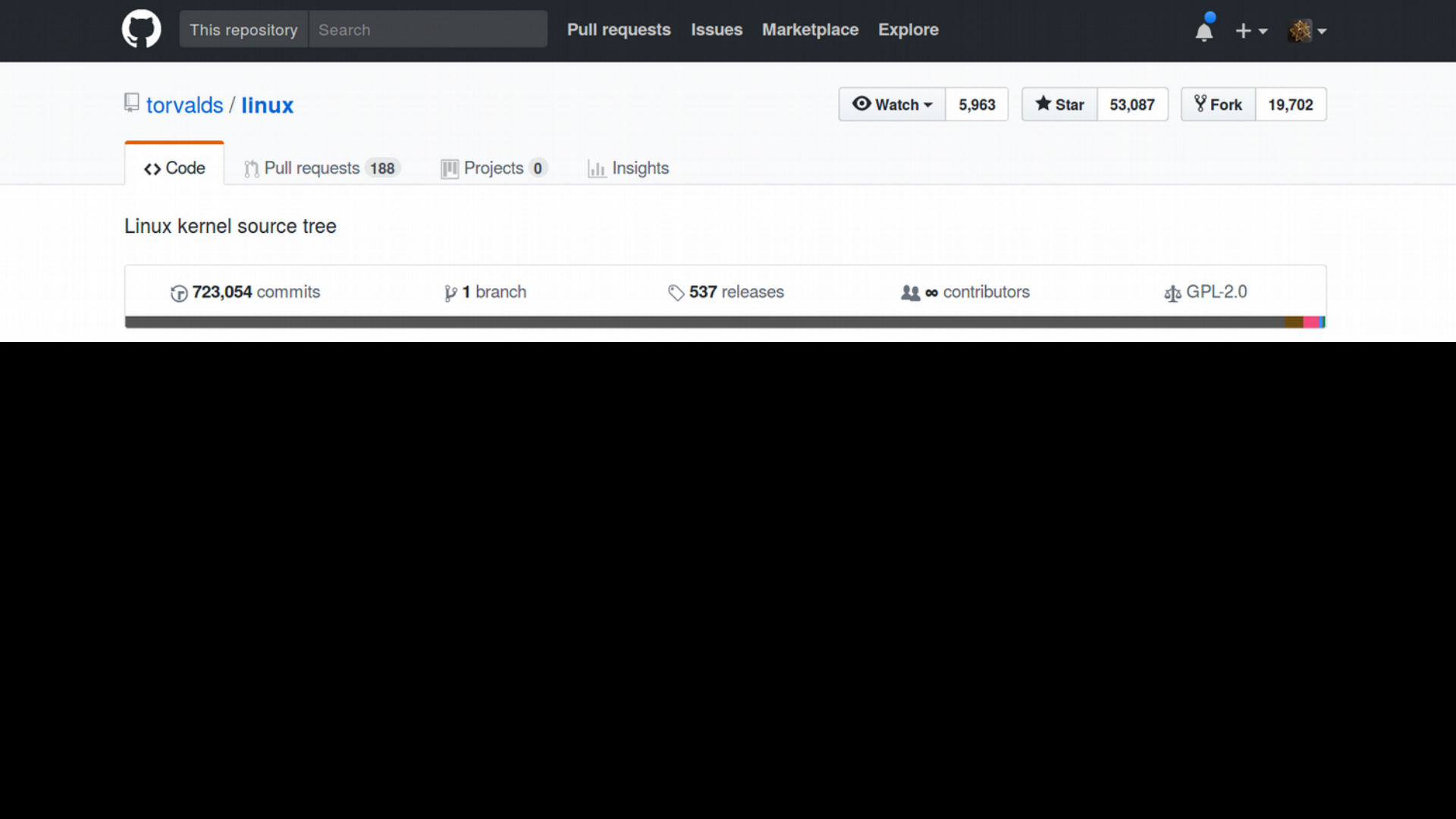
generated using David A. Wheeler's 'SLOCCount'

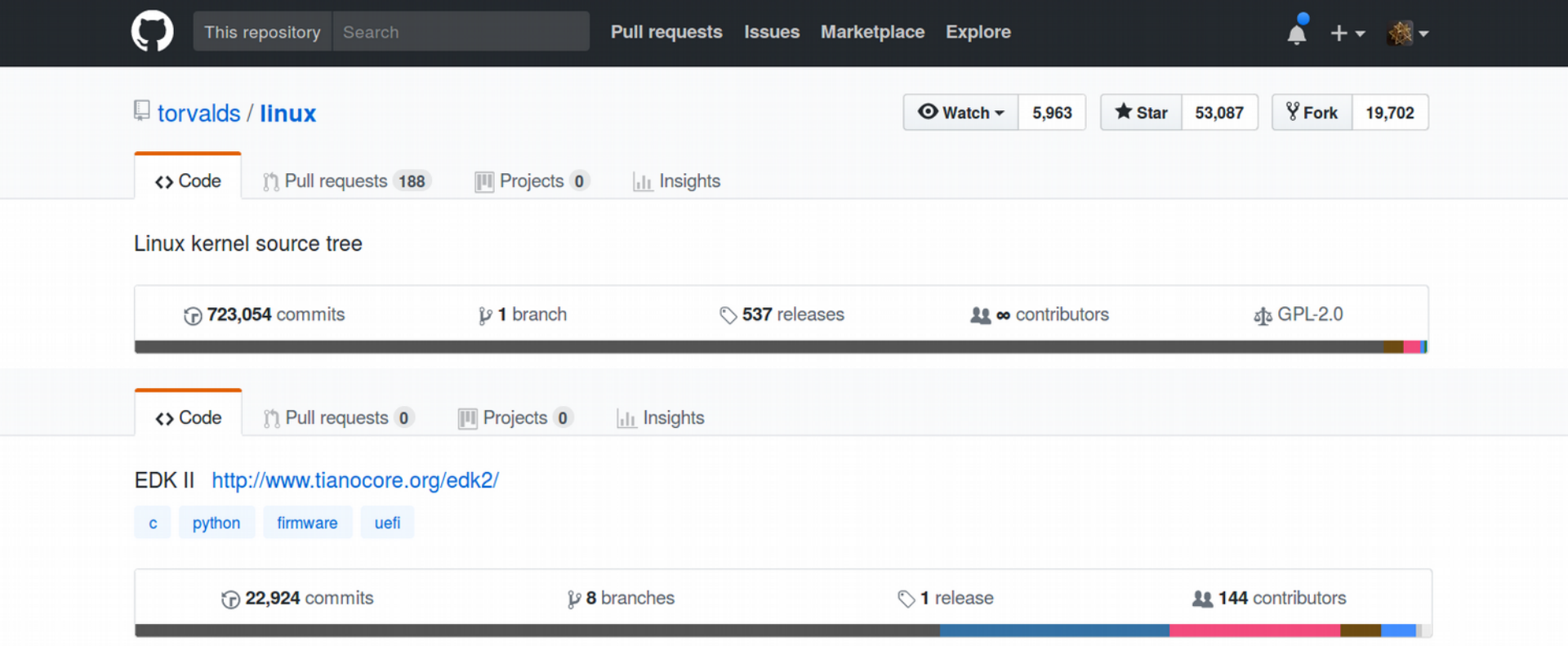
SLOC	Directory	SLOC-by-Language (Sorted)
69604	lib	ansic=63197,asm=6268,sh=139
30594	gnulib	ansic=30102,sh=492
23599	fs	ansic=23599
15250	kern	ansic=13791,asm=1459
15027	loader	ansic=15027
14598	commands	ansic=14531,asm=67
11856	video	ansic=11856
11237	disk	ansic=11237
8518	osdep	ansic=8518
7528	net	ansic=7528
6788	normal	ansic=6788
5911	term	ansic=5911
5246	bus	ansic=5246
4436	gfxmenu	ansic=4436
3498	tests	ansic=2978,asm=520
2659	boot	asm=2540,ansic=119
2579	efiemu	ansic=2466,asm=113
2384	script	ansic=1723,lex=393,yacc=268
1784	io	ansic=1784
1480	partmap	ansic=1480
1262	font	ansic=1262
1128	mmap	ansic=994,asm=134
559	gdb	ansic=396,asm=163
419	gettext	ansic=419
340	top_dir	sh=234,awk=75,ansic=31
112	parttool	ansic=112
79	hook	ansic=79

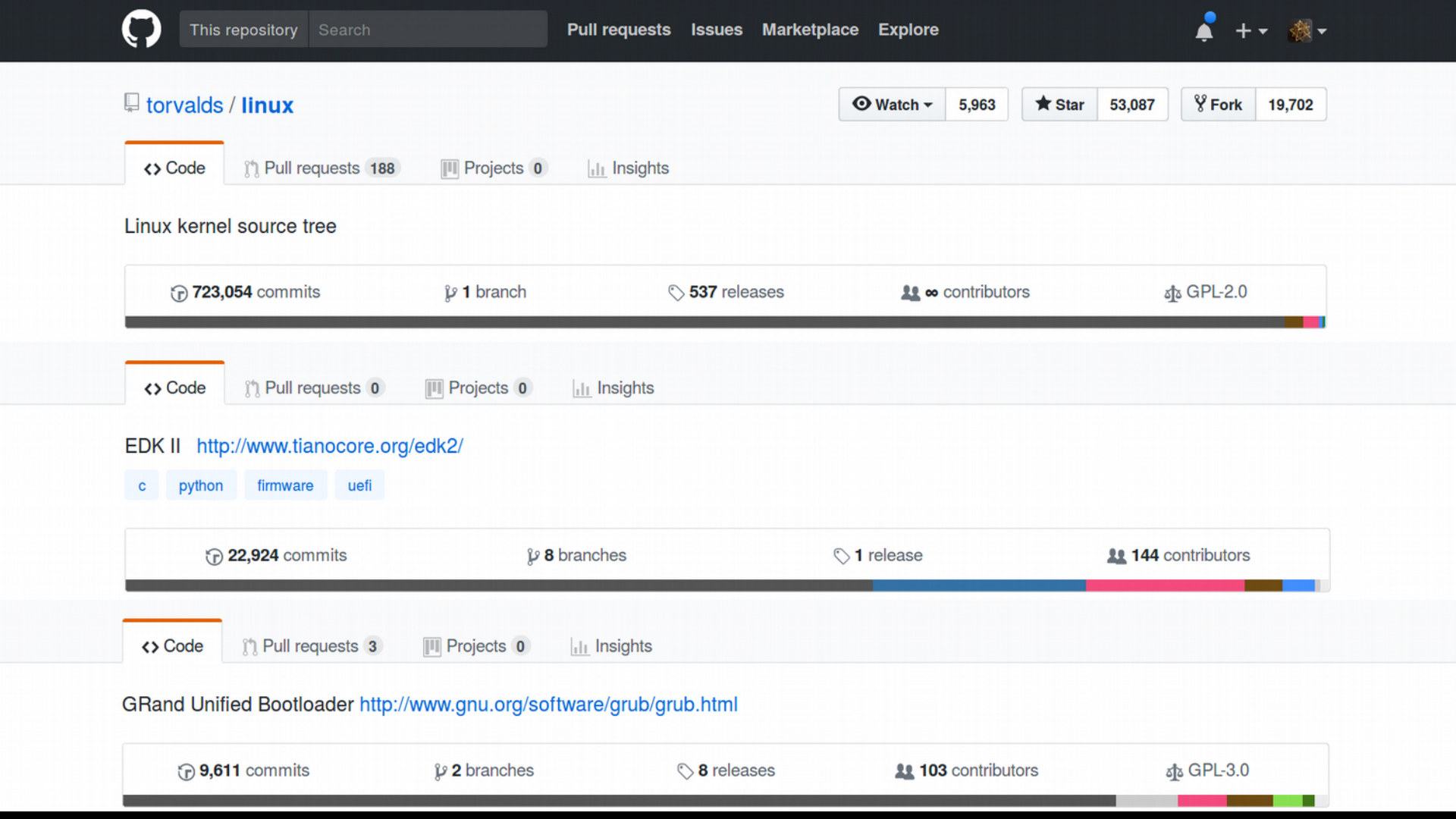
./grub/grub-core SLOC count:

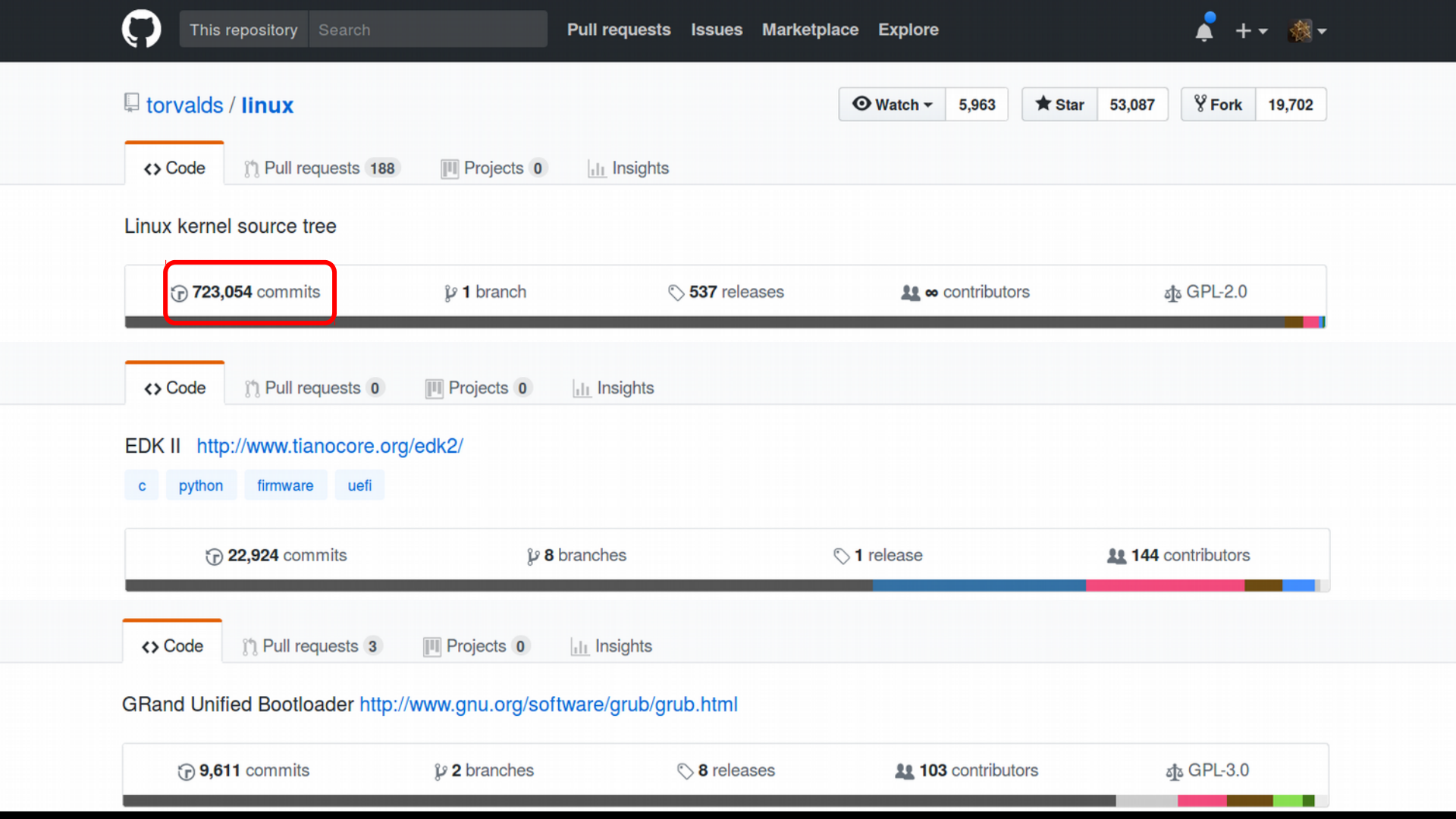
ansic:	235,636	(94.82%)
asm:	11,264	(4.53%)
sh:	865	(0.35%)
lex:	393	(0.16%)
yacc:	268	(0.11%)
awk:	75	(0.03%)
Total:	248,501	lines of code

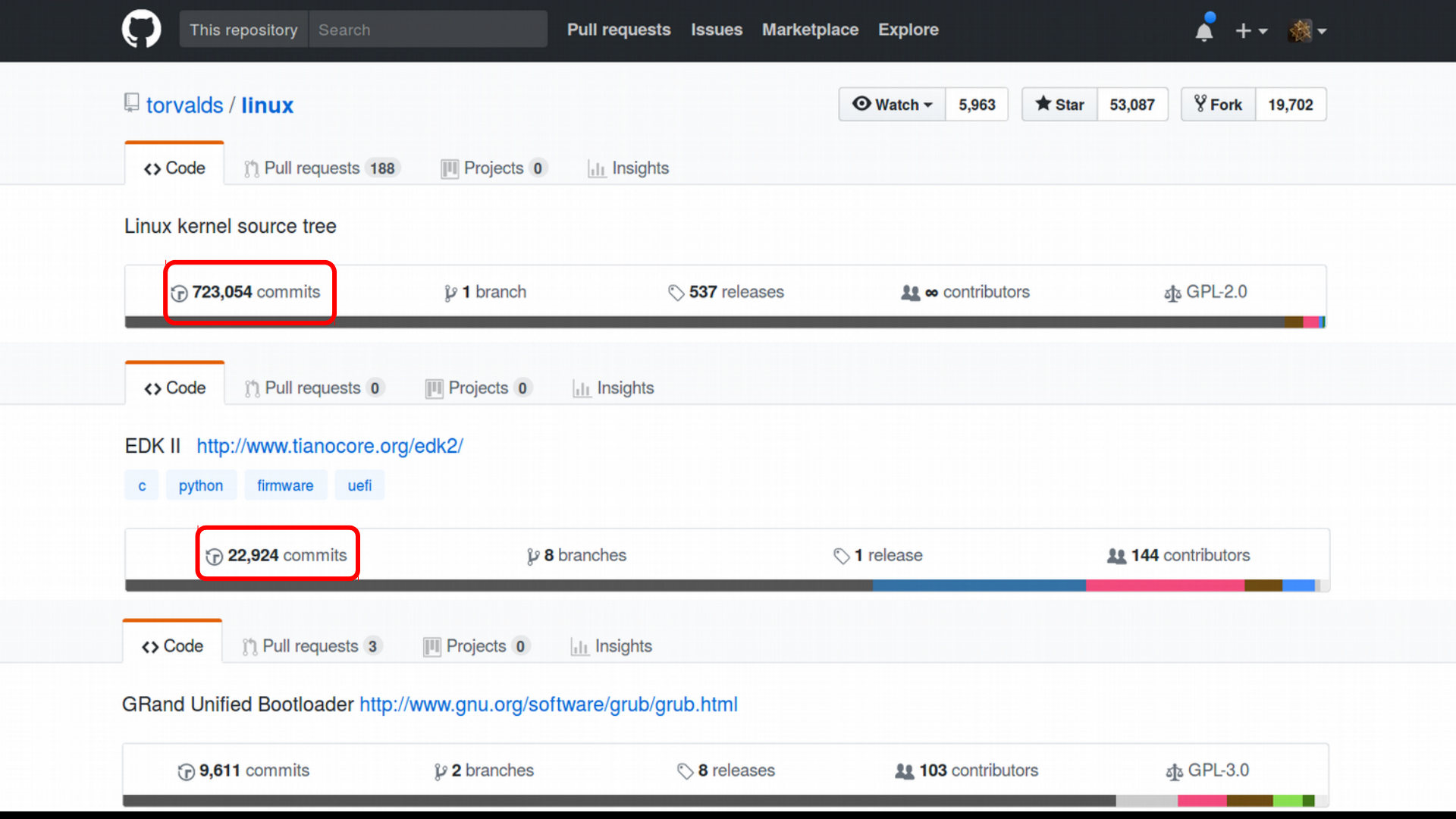
generated using David A. Wheeler's 'SLOCCount'

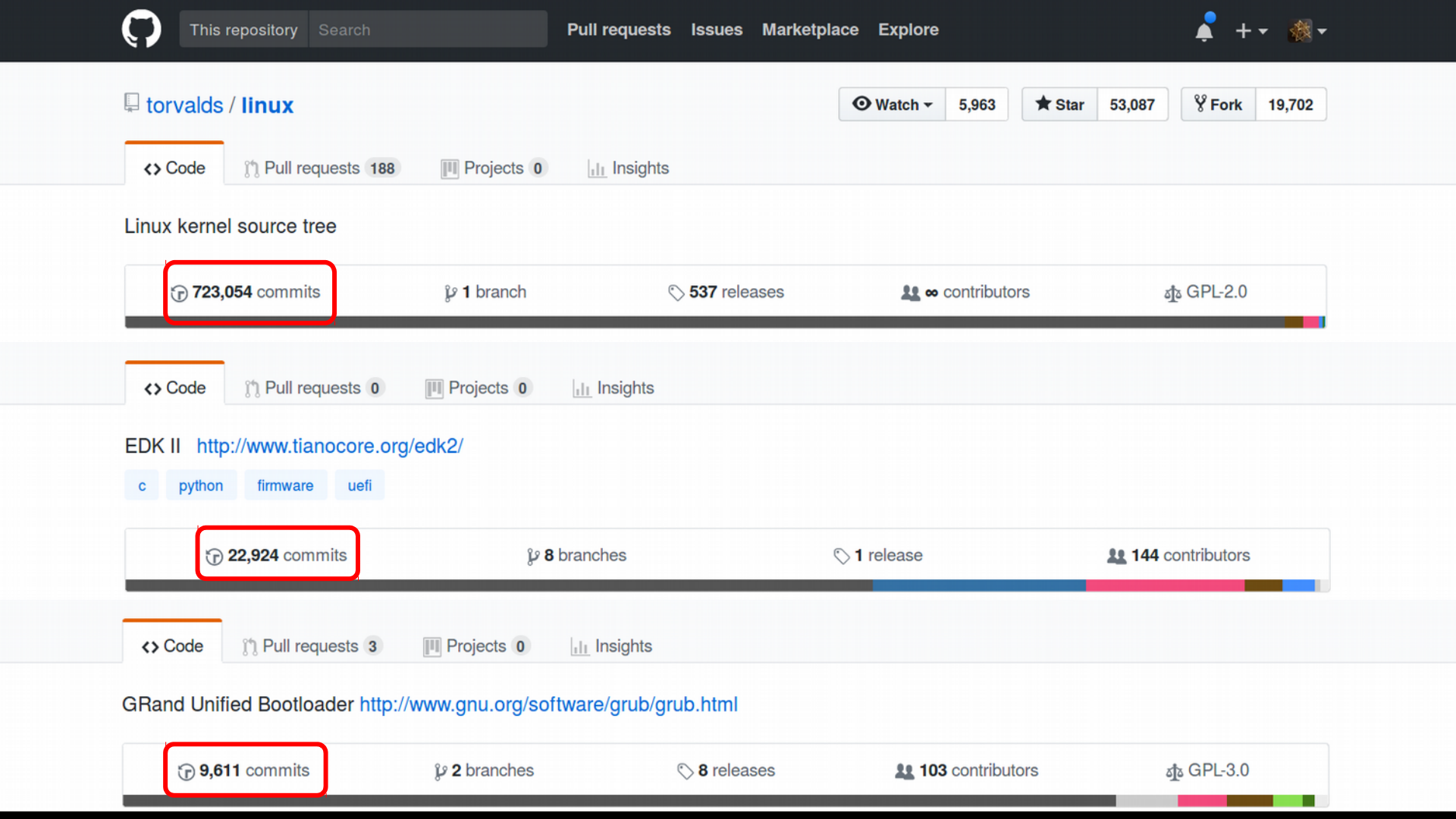

This repository
Search
Pull requests
Issues
Marketplace
Explore
torvalds / linux
Watch 5,963
Star 53,087
Fork 19,702
Code
Pull requests 188
Projects 0
Insights
Linux kernel source tree
723,054 commits
1 branch
537 releases
∞ contributors
GPL-2.0


This repository
Search
Pull requests
Issues
Marketplace
Explore
torvalds / linux
Watch 5,963
Star 53,087
Fork 19,702
Code
Pull requests 188
Projects 0
Insights
Linux kernel source tree
723,054 commits
1 branch
537 releases
∞ contributors
GPL-2.0
Code
Pull requests 0
Projects 0
Insights
EDK II http://www.tianocore.org/edk2/
c
python
firmware
uefi
22,924 commits
8 branches
1 release
144 contributors


This repository
Search
Pull requests
Issues
Marketplace
Explore
torvalds / linux
Watch 5,963
Star 53,087
Fork 19,702
Code
Pull requests 188
Projects 0
Insights
Linux kernel source tree
723,054 commits
1 branch
537 releases
∞ contributors
GPL-2.0
Code
Pull requests 0
Projects 0
Insights
EDK II http://www.tianocore.org/edk2/
c
python
firmware
uefi
22,924 commits
8 branches
1 release
144 contributors
Code
Pull requests 3
Projects 0
Insights
GRand Unified Bootloader http://www.gnu.org/software/grub/grub.html
9,611 commits
2 branches
8 releases
103 contributors
GPL-3.0


This repository
Search
Pull requests
Issues
Marketplace
Explore
torvalds / linux
Watch 5,963
Star 53,087
Fork 19,702
Code
Pull requests 188
Projects 0
Insights
Linux kernel source tree
723,054 commits
1 branch
537 releases
∞ contributors
GPL-2.0
Code
Pull requests 0
Projects 0
Insights
EDK II http://www.tianocore.org/edk2/
c
python
firmware
uefi
22,924 commits
8 branches
1 release
144 contributors
Code
Pull requests 3
Projects 0
Insights
GRand Unified Bootloader http://www.gnu.org/software/grub/grub.html
9,611 commits
2 branches
8 releases
103 contributors
GPL-3.0


This repository
Search
Pull requests
Issues
Marketplace
Explore
torvalds / linux
Watch 5,963
Star 53,087
Fork 19,702
Code
Pull requests 188
Projects 0
Insights
Linux kernel source tree
723,054 commits
1 branch
537 releases
∞ contributors
GPL-2.0
Code
Pull requests 0
Projects 0
Insights
EDK II http://www.tianocore.org/edk2/
c
python
firmware
uefi
22,924 commits
8 branches
1 release
144 contributors
Code
Pull requests 3
Projects 0
Insights
GRand Unified Bootloader http://www.gnu.org/software/grub/grub.html
9,611 commits
2 branches
8 releases
103 contributors
GPL-3.0


This repository
Search
Pull requests
Issues
Marketplace
Explore
torvalds / linux
Watch 5,963
Star 53,087
Fork 19,702
Code
Pull requests 188
Projects 0
Insights
Linux kernel source tree
723,054 commits
1 branch
537 releases
∞ contributors
GPL-2.0
Code
Pull requests 0
Projects 0
Insights
EDK II http://www.tianocore.org/edk2/
c
python
firmware
uefi
22,924 commits
8 branches
1 release
144 contributors
Code
Pull requests 3
Projects 0
Insights
GRand Unified Bootloader http://www.gnu.org/software/grub/grub.html
9,611 commits
2 branches
8 releases
103 contributors
GPL-3.0

Trust No One

Trust ~~No One~~

Fewer Parties

[redacted] used shady 'rootkit' tactic to quietly reinstall unwanted software

Even when users reinstalled a clean version of Windows on some devices, the software would still reappear.

By Zack Whittaker for Zero Day | August 12, 2015 -- 15:21 GMT (08:21 PDT) | Topic: Security

(Image: Sarah Tew/CBS Interactive)

NEWS

Hacking Team's malware uses a UEFI rootkit to survive operating system reinstalls

The feature allows the company's software to persist even if the hard disk drive if replaced.

By Lucian Constantin | Follow

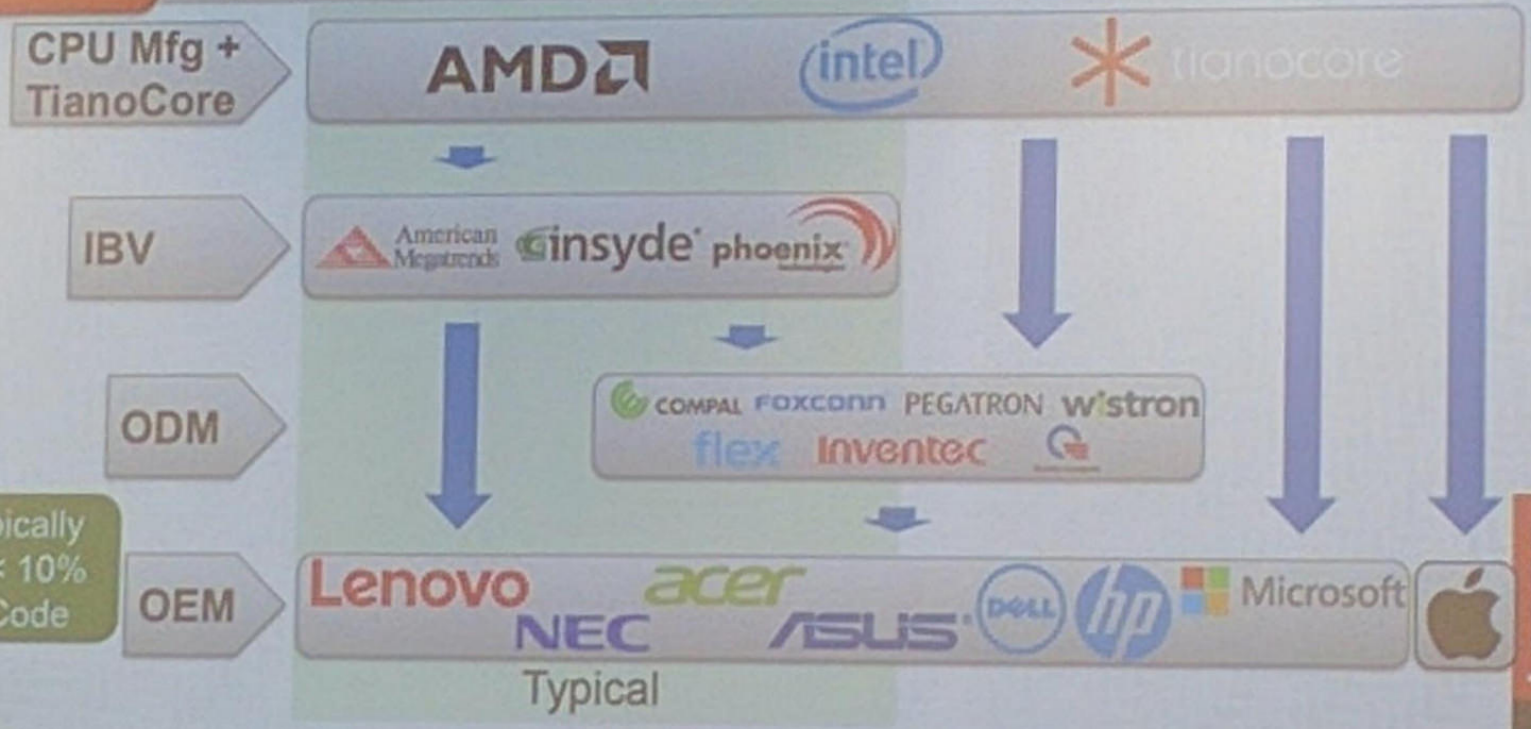
Romania Correspondent, IDG News Service

Jul 14, 2015 6:56 AM PT

BIOS Software Supply Chain Breakdown

Definition: IBV

- Independent BIOS Vendors are 3rd-party UEFI developers that sell value-added UEFI, toolkits, and custom development services



Trust…. but verify

Trust…. ~~but~~ verify

only what you can

osresearch / **heads**

Watch 45 Star 512 Fork 54

Code Issues 73 Pull requests 11 Projects 0 Wiki Insights

Branch: **master**

Commits on May 7, 2018

Merge branch 'usb-scan-gui' of https://github.com/kylerankin/heads
osresearch committed 9 days ago — Verified — 9c95b4e

Merge branch 'word_wrap_whiptail' of https://github.com/kylerankin/heads ...
osresearch committed 9 days ago — 62

Merge branch 'flashrom' of https://github.com/flammit/heads
osresearch committed 9 days ago — 44

This commit was signed with a **verified signature**.

osresearch
Trammell Hudson

GPG key ID: B65BFE540DEF86C0
Learn about signing commits

Commits on May 5, 2018

Add back flashrom support for KGPE-D16 ...
flammit committed 11 days ago — Verified — bb0e13c

reproducible-builds.org

Provide a verifiable path from source code to binary.

What is it about?

Reproducible builds are a set of software development practices that create a **verifiable path from** human readable **source code to** the **binary** code used by computers. (Full definition)

Why does it matter?

Most aspects of software verification are done on source code, as that is what humans can reasonably understand. But most of the

reproducible-builds.org

Provide a verifiable path from source code to binary.

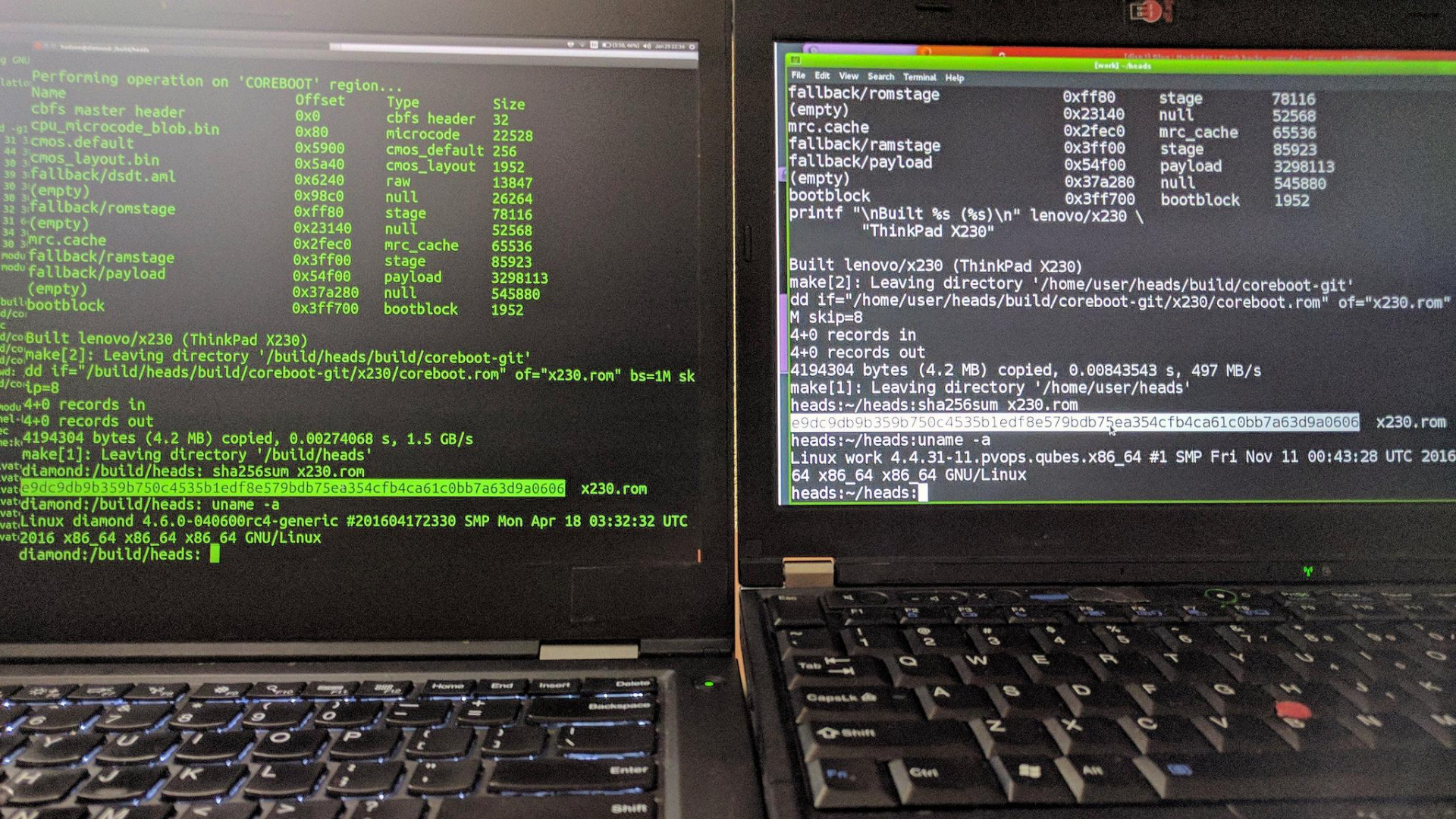
With *reproducible builds*, multiple parties can **independently** ensure they **all get *exactly* the same result**.

What is it about?

Reproducible builds are a set of software development practices that create a **verifiable path from** human readable **source code to** the **binary** code used by computers. (Full definition)

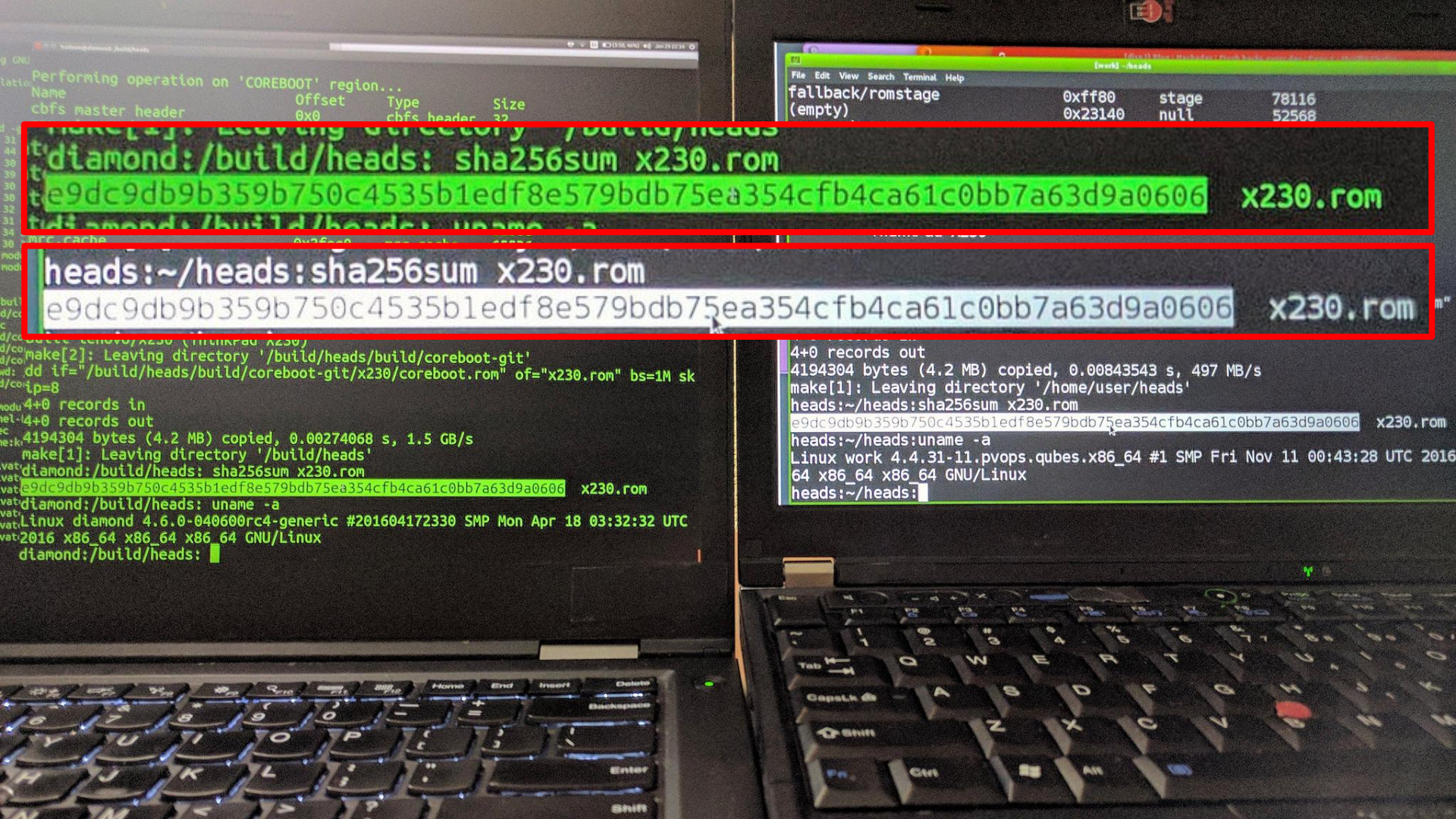
Why does it matter?

Most aspects of software verification are done on source code, as that is what humans can reasonably understand. But most of the



```
Performing operation on 'COREBOOT' region...
    Name                    Offset     Type           Size
    cbfs master header      0x0        cbfs header    32
    cpu_microcode_blob.bin  0x80       microcode      22528
    cmos.default            0x5900     cmos_default   256
    cmos_layout.bin         0x5a40     cmos_layout    1952
    fallback/dsdt.aml       0x6240     raw            13847
    (empty)                 0x98c0     null           26264
    fallback/romstage       0xff80     stage          78116
    (empty)                 0x23140    null           52568
    mrc.cache               0x2fec0    mrc_cache      65536
    fallback/ramstage       0x3ff00    stage          85923
    fallback/payload        0x54f00    payload        3298113
    (empty)                 0x37a280   null           545880
    bootblock               0x3ff700   bootblock      1952

Built lenovo/x230 (ThinkPad X230)
make[2]: Leaving directory '/build/heads/build/coreboot-git'
dd if="/build/heads/build/coreboot-git/x230/coreboot.rom" of="x230.rom" bs=1M sk
ip=8
4+0 records in
4+0 records out
4194304 bytes (4.2 MB) copied, 0.00274068 s, 1.5 GB/s
make[1]: Leaving directory '/build/heads'
diamond:/build/heads: sha256sum x230.rom
e9dc9db9b359b750c4535b1edf8e579bdb75ea354cfb4ca61c0bb7a63d9a0606  x230.rom
diamond:/build/heads: uname -a
Linux diamond 4.6.0-040600rc4-generic #201604172330 SMP Mon Apr 18 03:32:32 UTC
2016 x86_64 x86_64 x86_64 GNU/Linux
diamond:/build/heads:
```

```
[work] ~/heads
File  Edit  View  Search  Terminal  Help
fallback/romstage       0xff80     stage          78116
(empty)                 0x23140    null           52568
mrc.cache               0x2fec0    mrc_cache      65536
fallback/ramstage       0x3ff00    stage          85923
fallback/payload        0x54f00    payload        3298113
(empty)                 0x37a280   null           545880
bootblock               0x3ff700   bootblock      1952
printf "\nBuilt %s (%s)\n" lenovo/x230 \
       "ThinkPad X230"

Built lenovo/x230 (ThinkPad X230)
make[2]: Leaving directory '/home/user/heads/build/coreboot-git'
dd if="/home/user/heads/build/coreboot-git/x230/coreboot.rom" of="x230.rom"
M skip=8
4+0 records in
4+0 records out
4194304 bytes (4.2 MB) copied, 0.00843543 s, 497 MB/s
make[1]: Leaving directory '/home/user/heads'
heads:~/heads:sha256sum x230.rom
e9dc9db9b359b750c4535b1edf8e579bdb75ea354cfb4ca61c0bb7a63d9a0606  x230.rom
heads:~/heads:uname -a
Linux work 4.4.31-11.pvops.qubes.x86_64 #1 SMP Fri Nov 11 00:43:28 UTC 2016
64 x86_64 x86_64 GNU/Linux
heads:~/heads:
```


diamond:/build/heads: sha256sum x230.rom
e9dc9db9b359b750c4535b1edf8e579bdb75ea354cfb4ca61c0bb7a63d9a0606 x230.rom
heads:~/heads:sha256sum x230.rom
e9dc9db9b359b750c4535b1edf8e579bdb75ea354cfb4ca61c0bb7a63d9a0606 x230.rom
Performing operation on 'COREBOOT' region...
Name Offset Type Size
cbfs master header 0x0 cbfs header 32
make[2]: Leaving directory '/build/heads/build/coreboot-git'
dd if="/build/heads/build/coreboot-git/x230/coreboot.rom" of="x230.rom" bs=1M sk
ip=8
4+0 records in
4+0 records out
4194304 bytes (4.2 MB) copied, 0.00274068 s, 1.5 GB/s
make[1]: Leaving directory '/build/heads'
diamond:/build/heads: sha256sum x230.rom
e9dc9db9b359b750c4535b1edf8e579bdb75ea354cfb4ca61c0bb7a63d9a0606 x230.rom
diamond:/build/heads: uname -a
Linux diamond 4.6.0-040600rc4-generic #201604172330 SMP Mon Apr 18 03:32:32 UTC
2016 x86_64 x86_64 x86_64 GNU/Linux
diamond:/build/heads:
File Edit View Search Terminal Help
fallback/romstage 0xff80 stage 78116
(empty) 0x23140 null 52568
4+0 records out
4194304 bytes (4.2 MB) copied, 0.00843543 s, 497 MB/s
make[1]: Leaving directory '/home/user/heads'
heads:~/heads:sha256sum x230.rom
e9dc9db9b359b750c4535b1edf8e579bdb75ea354cfb4ca61c0bb7a63d9a0606 x230.rom
heads:~/heads:uname -a
Linux work 4.4.31-11.pvops.qubes.x86_64 #1 SMP Fri Nov 11 00:43:28 UTC 2016
64 x86_64 x86_64 GNU/Linux
heads:~/heads:

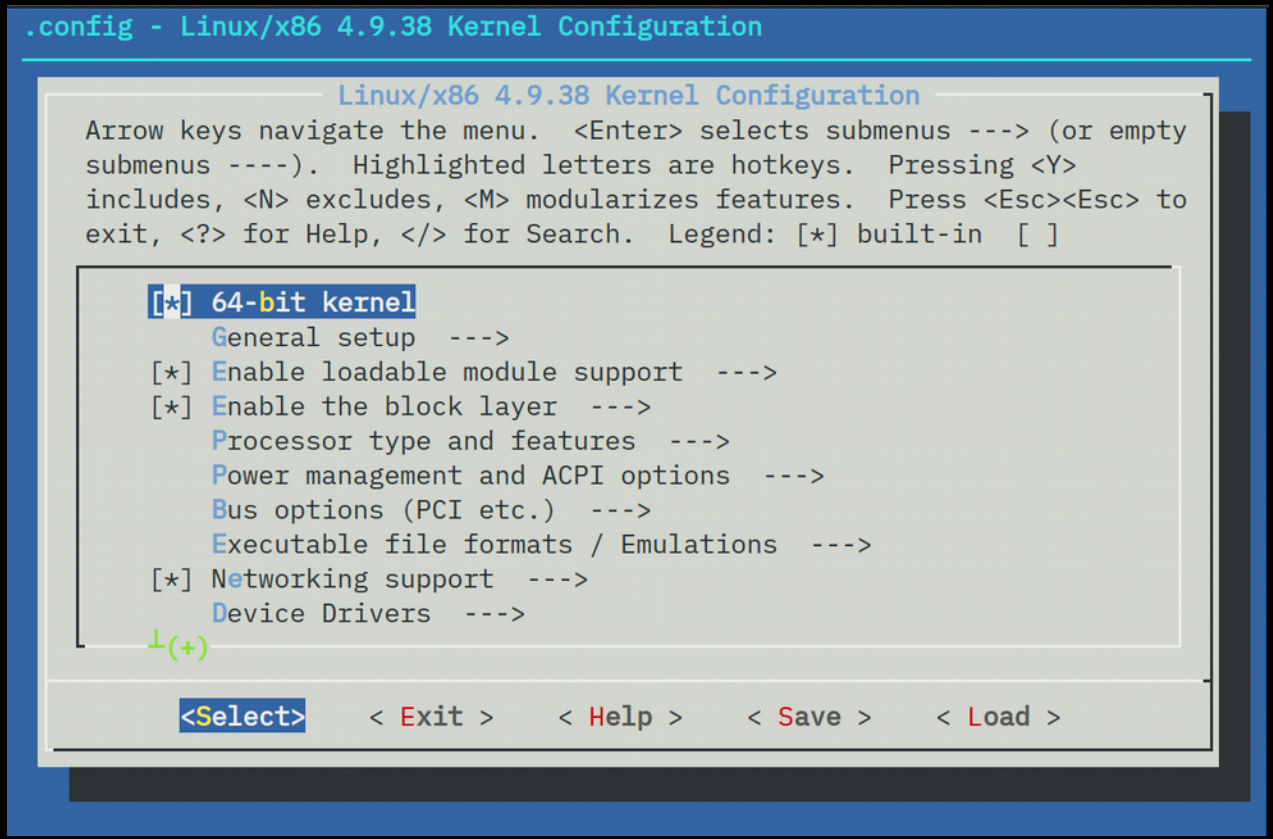
Security

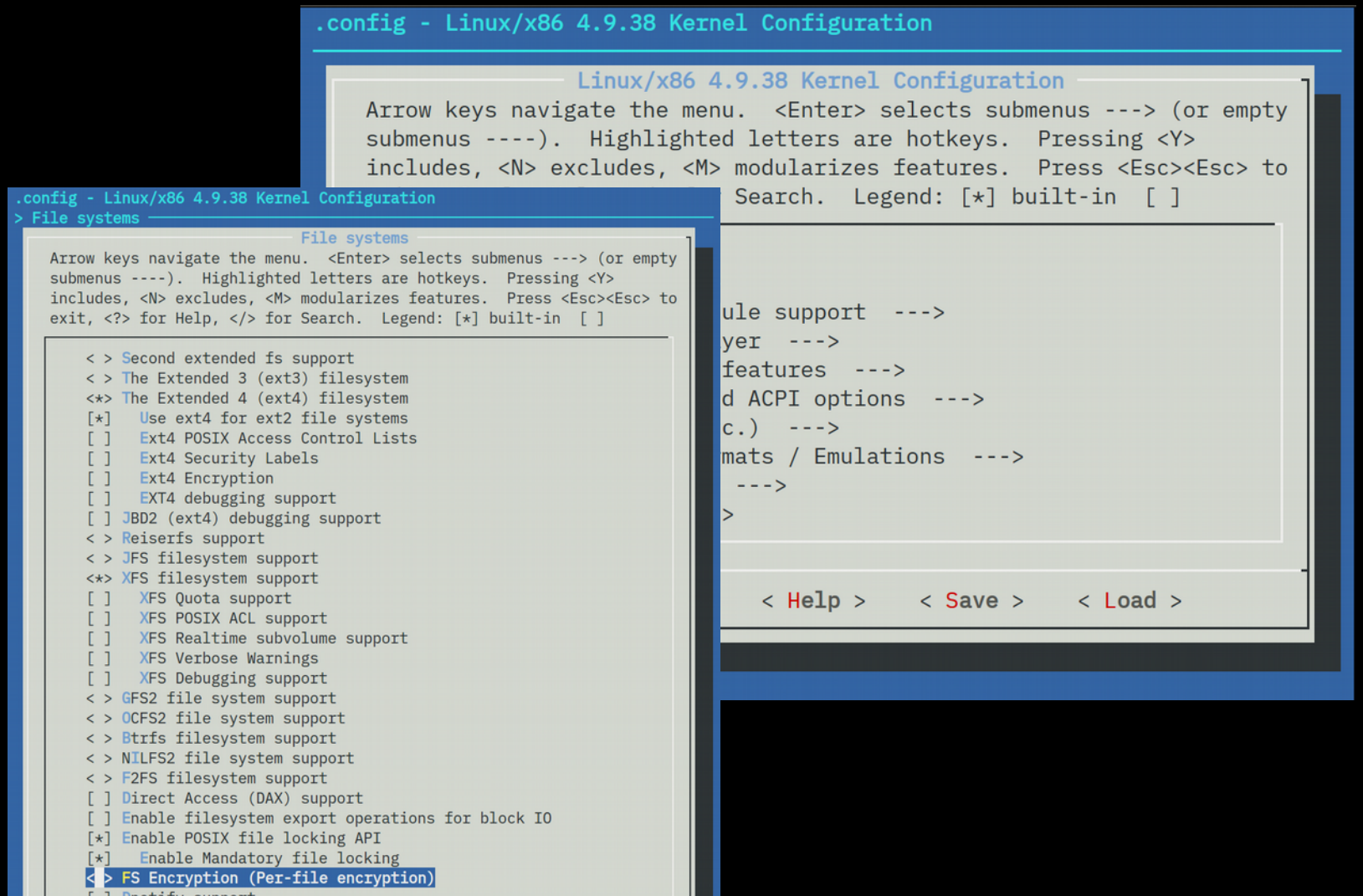
Flexibility

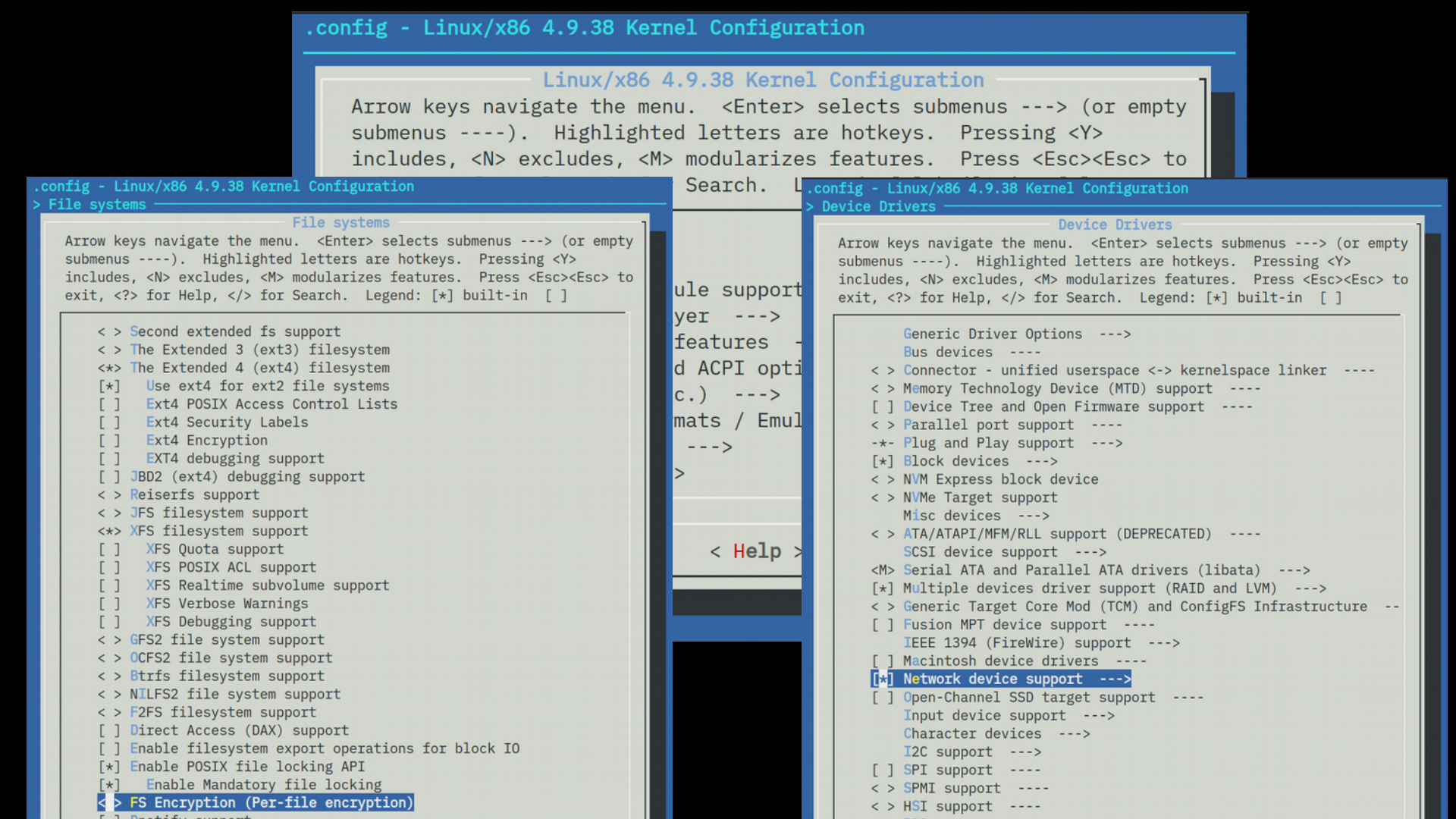
Resiliency

“LinuxBoot converts your Linux developers into firmware engineers”

```
#!/bin/sh
# This is the very first script invoked by the Linux kernel and is
# running out of the ram disk.  There are no fileysstems mounted.
# It is important to have a way to invoke a recovery shell in case
# the boot scripts are messed up, but also important to modify the
# PCRs if this happens to prevent the TPM disk keys from being revealed.

# First thing it is vital to mount the /dev and other system directories
mkdir /proc /sys /dev /tmp /boot /media 2>&- 1>&-
mount /dev
mount /proc
mount /sys

# Setup the pty psudeo filesystem
mkdir /dev/pts
mount /dev/pts

if [ ! -r /dev/ptmx ]; then
        ln -s /dev/pts/ptmx /dev/ptmx
fi

# bring up the ethernet
```


.config - Linux/x86 4.9.38 Kernel Configuration
Linux/x86 4.9.38 Kernel Configuration
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ]
[*] 64-bit kernel
General setup --->
[*] Enable loadable module support --->
[*] Enable the block layer --->
Processor type and features --->
Power management and ACPI options --->
Bus options (PCI etc.) --->
Executable file formats / Emulations --->
[*] Networking support --->
Device Drivers --->
(+)
<Select>
< Exit >
< Help >
< Save >
< Load >


.config - Linux/x86 4.9.38 Kernel Configuration
Linux/x86 4.9.38 Kernel Configuration
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty
submenus ----). Highlighted letters are hotkeys. Pressing <Y>
includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to
Search. Legend: [*] built-in [ ]
ule support --->
yer --->
features --->
d ACPI options --->
c.) --->
mats / Emulations --->
--->
>
< Help > < Save > < Load >
.config - Linux/x86 4.9.38 Kernel Configuration
> File systems
File systems
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty
submenus ----). Highlighted letters are hotkeys. Pressing <Y>
includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to
exit, <?> for Help, </> for Search. Legend: [*] built-in [ ]
< > Second extended fs support
< > The Extended 3 (ext3) filesystem
<*> The Extended 4 (ext4) filesystem
[*] Use ext4 for ext2 file systems
[ ] Ext4 POSIX Access Control Lists
[ ] Ext4 Security Labels
[ ] Ext4 Encryption
[ ] EXT4 debugging support
[ ] JBD2 (ext4) debugging support
< > Reiserfs support
< > JFS filesystem support
<*> XFS filesystem support
[ ] XFS Quota support
[ ] XFS POSIX ACL support
[ ] XFS Realtime subvolume support
[ ] XFS Verbose Warnings
[ ] XFS Debugging support
< > GFS2 file system support
< > OCFS2 file system support
< > Btrfs filesystem support
< > NILFS2 file system support
< > F2FS filesystem support
[ ] Direct Access (DAX) support
[ ] Enable filesystem export operations for block IO
[*] Enable POSIX file locking API
[*] Enable Mandatory file locking
< > FS Encryption (Per-file encryption)

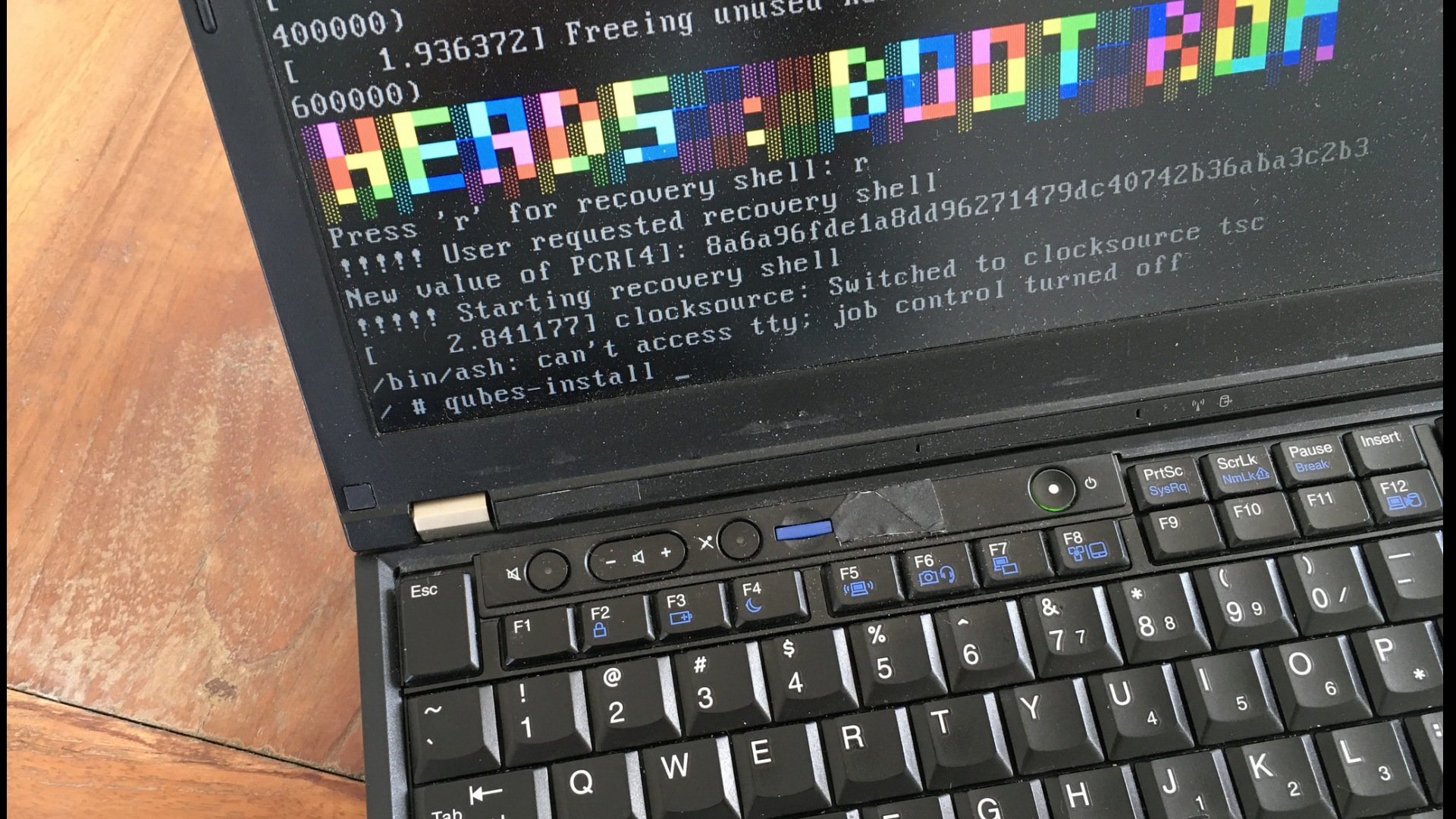

.config - Linux/x86 4.9.38 Kernel Configuration
Linux/x86 4.9.38 Kernel Configuration
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to
.config - Linux/x86 4.9.38 Kernel Configuration
> File systems
File systems
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ]
< > Second extended fs support
< > The Extended 3 (ext3) filesystem
<*> The Extended 4 (ext4) filesystem
[*] Use ext4 for ext2 file systems
[ ] Ext4 POSIX Access Control Lists
[ ] Ext4 Security Labels
[ ] Ext4 Encryption
[ ] EXT4 debugging support
[ ] JBD2 (ext4) debugging support
< > Reiserfs support
< > JFS filesystem support
<*> XFS filesystem support
[ ] XFS Quota support
[ ] XFS POSIX ACL support
[ ] XFS Realtime subvolume support
[ ] XFS Verbose Warnings
[ ] XFS Debugging support
< > GFS2 file system support
< > OCFS2 file system support
< > Btrfs filesystem support
< > NILFS2 file system support
< > F2FS filesystem support
[ ] Direct Access (DAX) support
[ ] Enable filesystem export operations for block IO
[*] Enable POSIX file locking API
[*] Enable Mandatory file locking
< > FS Encryption (Per-file encryption)
.config - Linux/x86 4.9.38 Kernel Configuration
> Device Drivers
Device Drivers
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ]
Generic Driver Options --->
Bus devices ----
< > Connector - unified userspace <-> kernelspace linker ----
< > Memory Technology Device (MTD) support ----
[ ] Device Tree and Open Firmware support ----
< > Parallel port support ----
-*- Plug and Play support --->
[*] Block devices --->
< > NVM Express block device
< > NVMe Target support
Misc devices --->
< > ATA/ATAPI/MFM/RLL support (DEPRECATED) ----
SCSI device support --->
<M> Serial ATA and Parallel ATA drivers (libata) --->
[*] Multiple devices driver support (RAID and LVM) --->
< > Generic Target Core Mod (TCM) and ConfigFS Infrastructure --
[ ] Fusion MPT device support ----
IEEE 1394 (FireWire) support --->
[ ] Macintosh device drivers ----
[*] Network device support --->
[ ] Open-Channel SSD target support ----
Input device support --->
Character devices --->
I2C support --->
[ ] SPI support ----
< > SPMI support ----
< > HSI support ----


adversary: nation state (NSA!!!!!!1)
them:
$$$$$$$$
power of the law
power of the beyond the law
rational & amoral
you:
all the encryption
all the Tor
become famous enough you can't be secretly murdered?
steph
@corcra
your threat model is not my threat model but your threat model is okay
7:52 AM - 1 Jun 2015
13 Retweets 46 Likes

Boot strapping slightly more secure systems

Trammell Hudson @qrs

A6C7 4E34 1054 A169 CE52
BE5F B65B FE54 0DEF 86C0


400000)
[1.936372] Freeing unused
600000)
HEADS: BOOTING
Press 'r' for recovery shell: r
!!!!! User requested recovery shell
New value of PCR[4]: 8a6a96fde1a8dd96271479dc40742b36aba3c2b3
!!!!! Starting recovery shell
[2.841177] clocksource: Switched to clocksource tsc
/bin/ash: can't access tty; job control turned off
/ # qubes-install -


Embedded Linux
Conference
Europe
Replace Your Exploit-Ridden Firmware with Linux
Ronald Minnich, Google
THE LINUX FOUNDATION
Embedde
Conferen
urope

Results

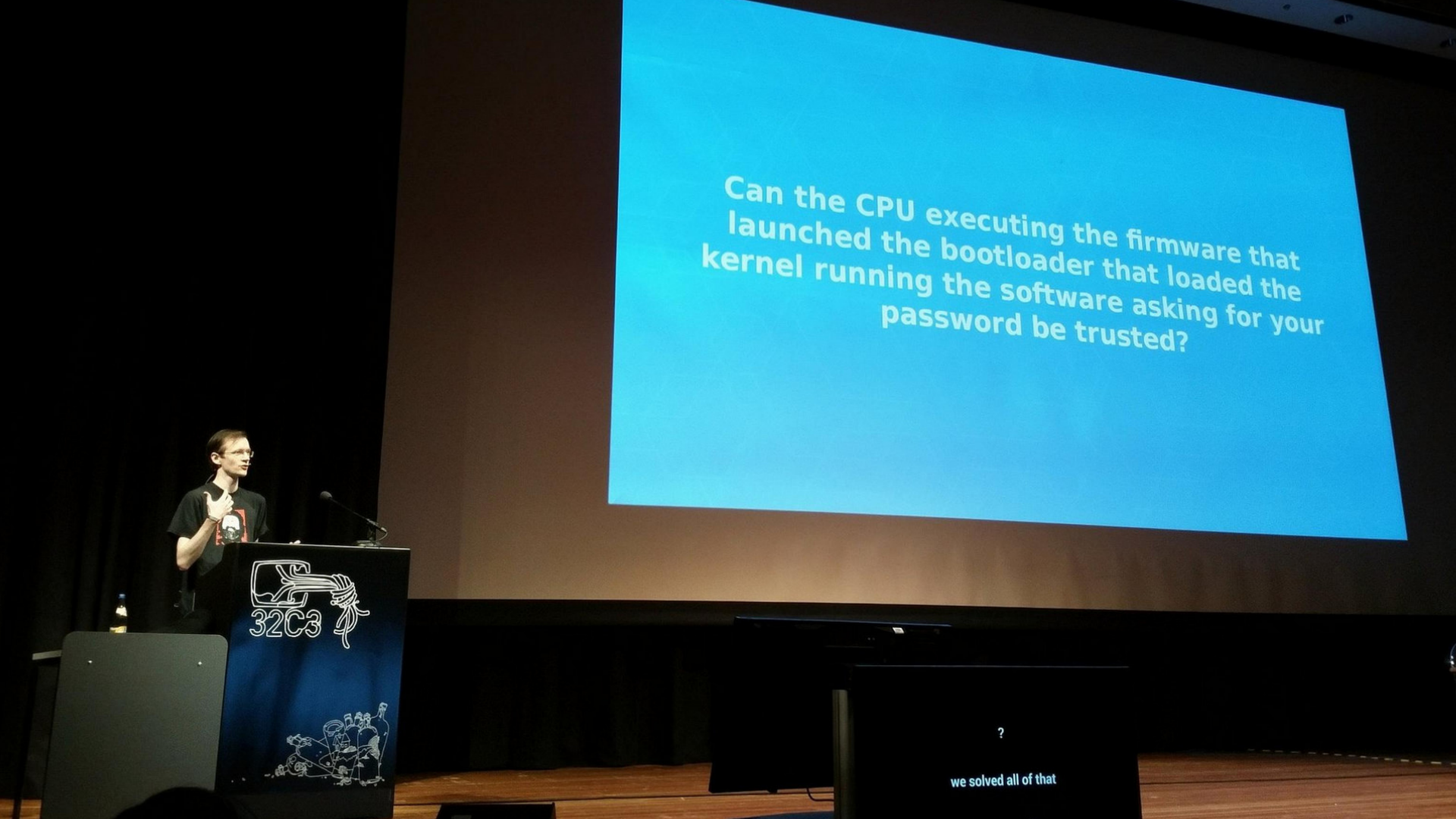
- OCP boot time: 8 minutes -> 20 seconds
  - I.e. 24x speedup
  - This is to a shell prompt in Linux
- OCP -> DHCP -> wget -> kexec: 25 seconds
- All userland written in Go
- Linux performance and reliability in firmware
- Eliminate *all* UEFI/ME post-boot activity

Results

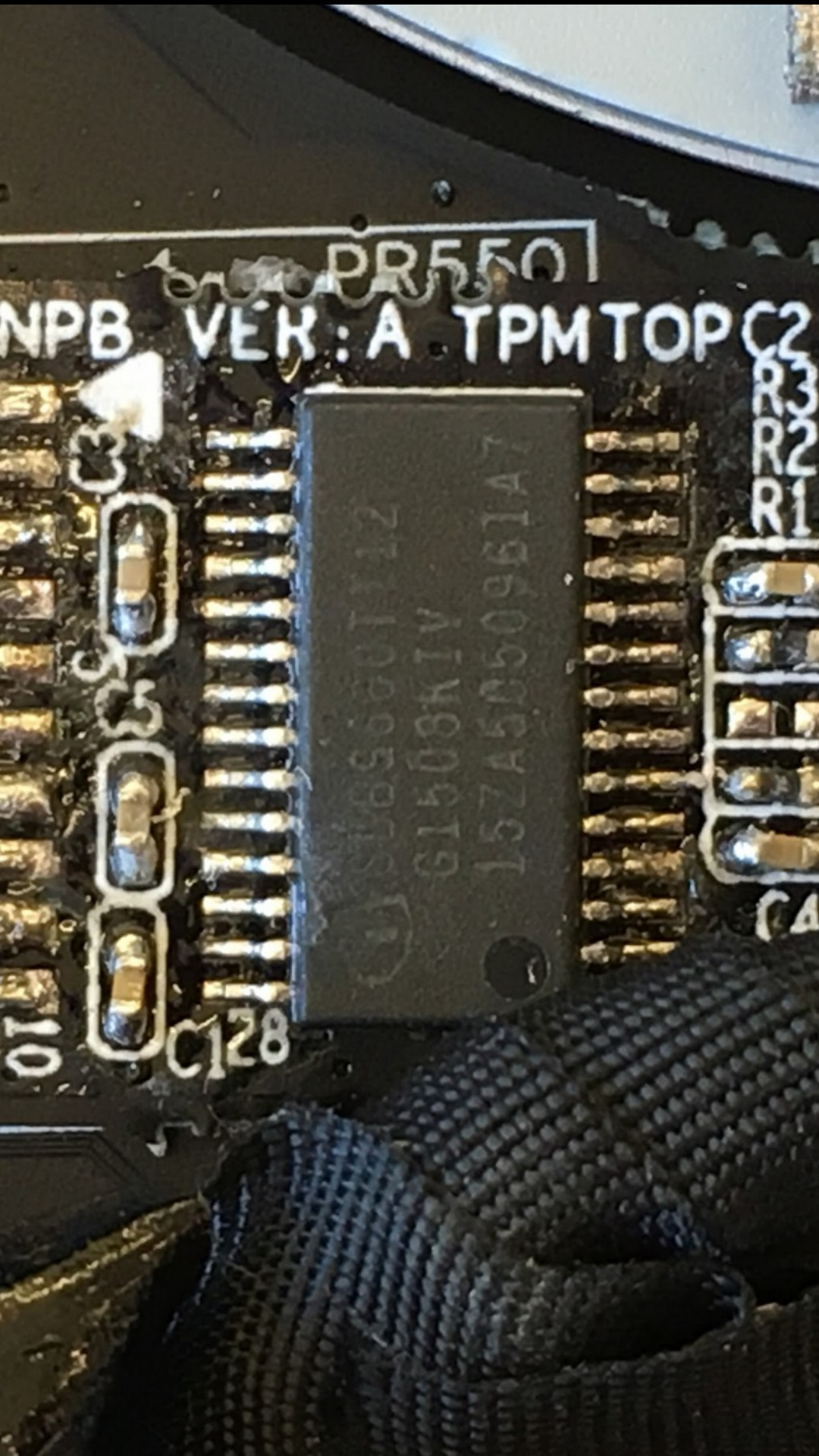
- OCP boot time: 8 minutes -> 20 seconds
  - I.e. 24x speedup
  - This is to a shell prompt in Linux
- OCP -> DHCP -> wget -> kexec: 25 seconds
- All userland written in Go
- Linux performance and reliability in firmware
- Eliminate *all* UEFI/ME post-boot activity

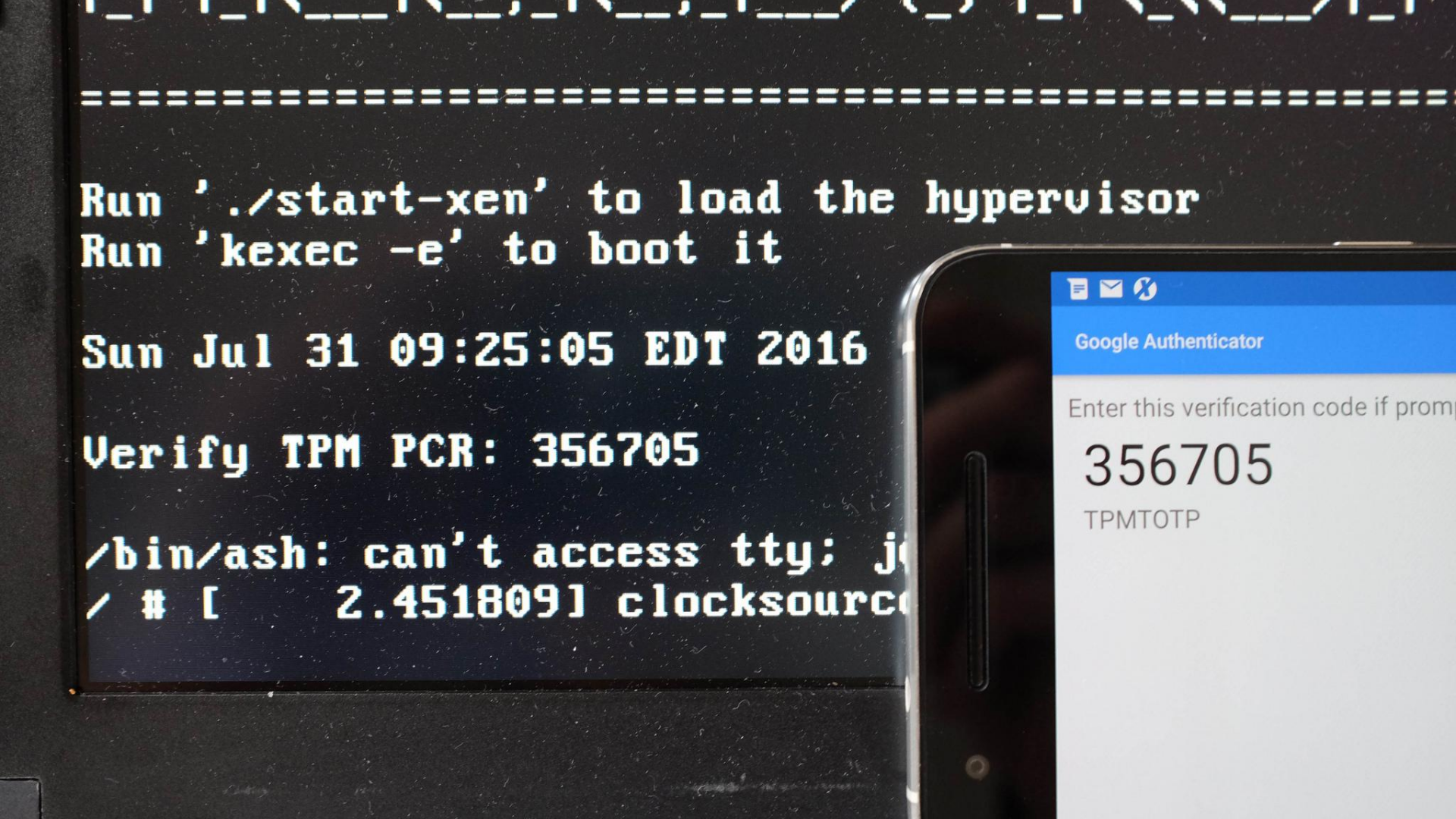

facebook
intel
Server: Yosemite
coreboot
LinuxBoot
coreboot built from mostly upstream sources
Intel FSP from Github
Linux + initramfs on boot ROM
Highest transparency, security, and customization
Power on to shell in a few seconds
Serial console is the main bottleneck
Can integrate with vboot, trusted boot, measured boot, remote attestation, etc.

Security
Flexibility
Resiliency

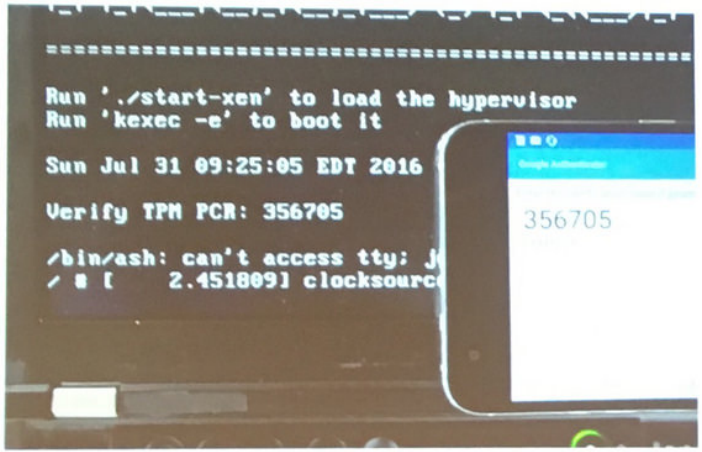

Can the CPU executing the firmware that launched the bootloader that loaded the kernel running the software asking for your password be trusted?
32C3
?
we solved all of that

Measure Everything (Static root of trust)


PR550
NPB VER:A TPMTOP
C2
R3
R2
R1
C128


Run './start-xen' to load the hypervisor
Run 'kexec -e' to boot it
Sun Jul 31 09:25:05 EDT 2016
Verify TPM PCR: 356705
/bin/ash: can't access tty; j
/ # [2.451809] clocksourc
Google Authenticator
Enter this verification code if prom
356705
TPMTOTP

Trusted Boot



doi>10.1145/2991079.2991104

Bootstrapping and Maintaining Trust in the Cloud *

Nabil Schear
MIT Lincoln Laboratory
nabil@ll.mit.edu

Patrick T. Cable II
Threat Stack, Inc.
pat@threatstack.com

Thomas M. Moyer
MIT Lincoln Laboratory
tmoyer@ll.mit.edu

Bryan Richard
MIT Lincoln Laboratory
bryan.richard@ll.mit.edu

Robert Rudd
MIT Lincoln Laboratory
robert.rudd@ll.mit.edu

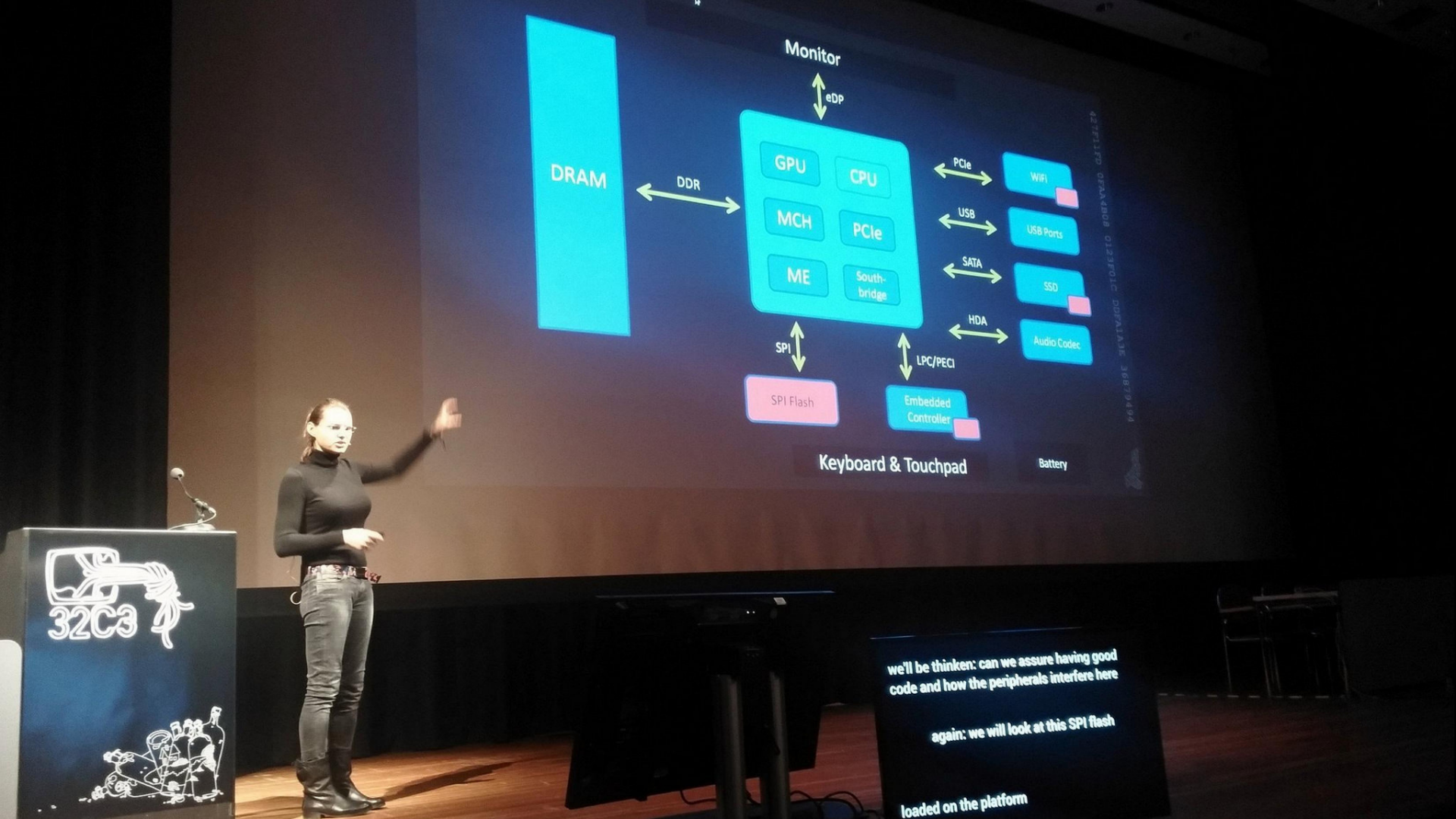
ABSTRACT

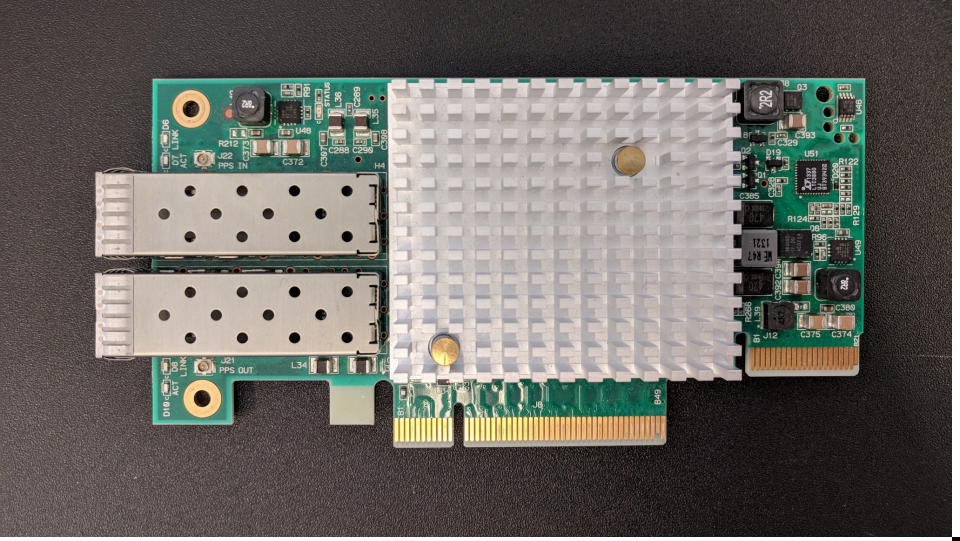
Today's infrastructure as a service (IaaS) cloud environments rely upon full trust in the provider to secure applications and data. Cloud providers do not offer the ability to create hardware-rooted cryptographic identities for IaaS cloud resources or sufficient information to verify the integrity of systems. Trusted computing protocols and hardware like the TPM have long promised a solution to this problem. However, these technologies have not seen broad adoption because of their complexity of implementation, low performance, and lack of compatibility with virtualized environments. In this paper we introduce `keylime`, a scalable trusted cloud key management system. `keylime` provides an end-to-end solution for both bootstrapping hardware rooted cryptographic identities for IaaS nodes and for

1. INTRODUCTION

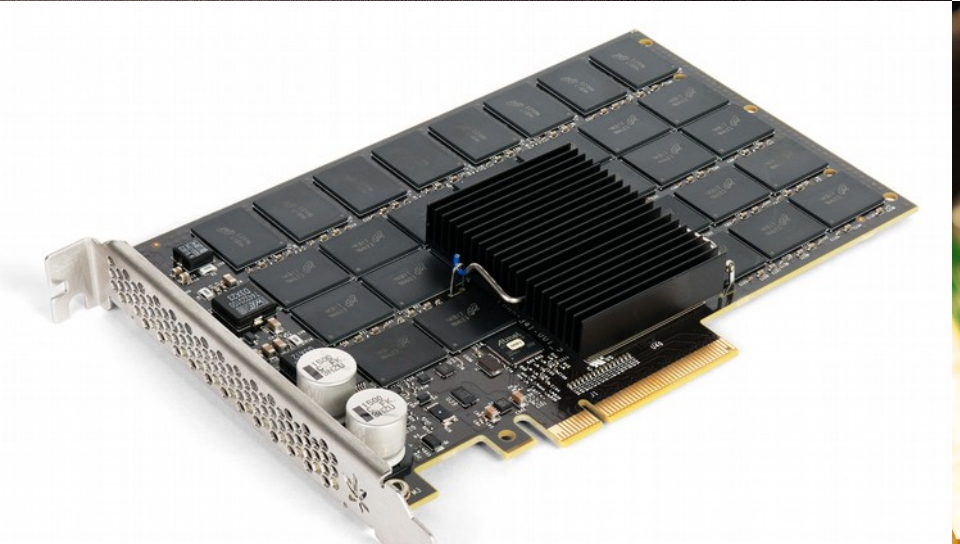
The proliferation and popularity of infrastructure-as-a-service (IaaS) cloud computing services such as Amazon Web Services and Google Compute Engine means more cloud tenants are hosting sensitive, private, and business critical data and applications in the cloud. Unfortunately, IaaS cloud service providers do not currently furnish the building blocks necessary to establish a trusted environment for hosting these sensitive resources. Tenants have limited ability to verify the underlying platform when they deploy to the cloud and to ensure that the platform remains in a good state for the duration of their computation. Additionally, current practices restrict tenants' ability to establish unique, unforgeable identities for individual nodes that are tied to a hardware root of trust. Often, identity is based solely on a

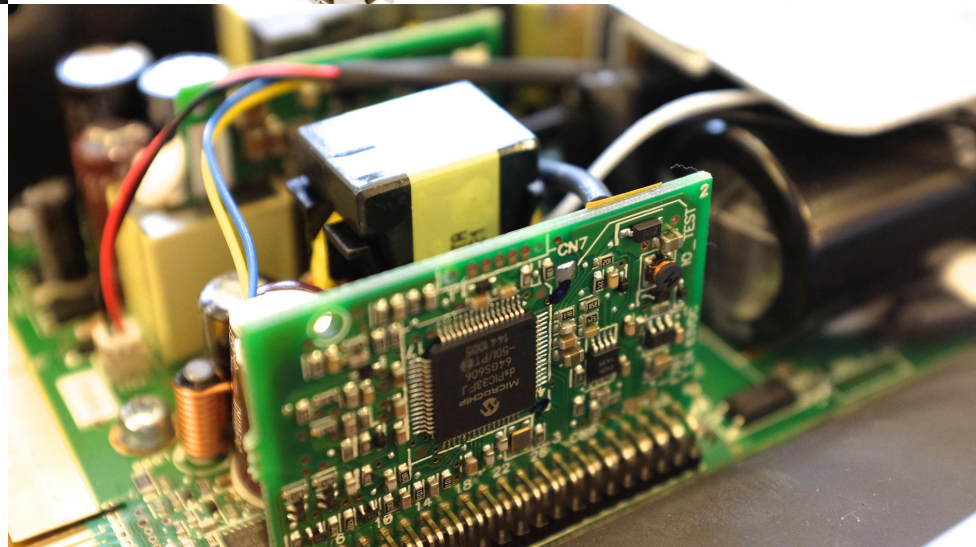
Measure “Everything”?


Monitor
eDP
DRAM
DDR
GPU
CPU
MCH
PCIe
ME
South-bridge
PCIe
WiFi
USB
USB Ports
SATA
SSD
HDA
Audio Codec
SPI
LPC/PECI
SPI Flash
Embedded Controller
Keyboard & Touchpad
Battery
32C3
we'll be thinken: can we assure having good code and how the peripherals interfere here
again: we will look at this SPI flash
loaded on the platform

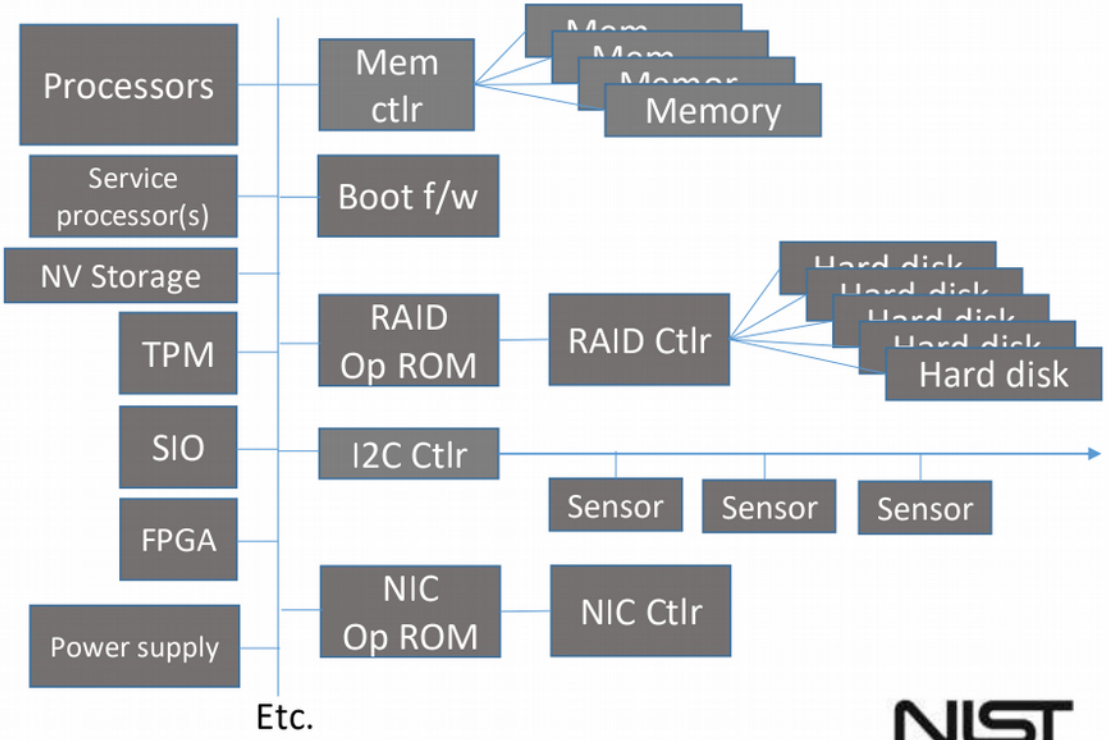



NVIDIA TESLA





NIST Special Publication 800-193
Platform Firmware Resiliency Guidelines



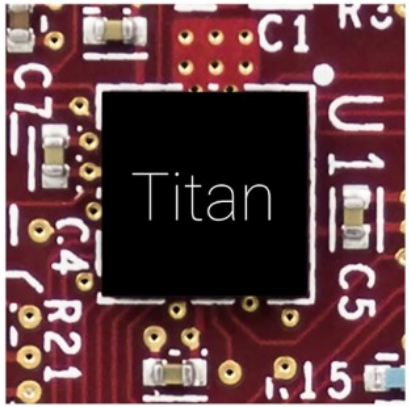
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

https://doi.org/10.6028/NIST.SP.800-193

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Preventing Persistence

Custom security modules



Titan

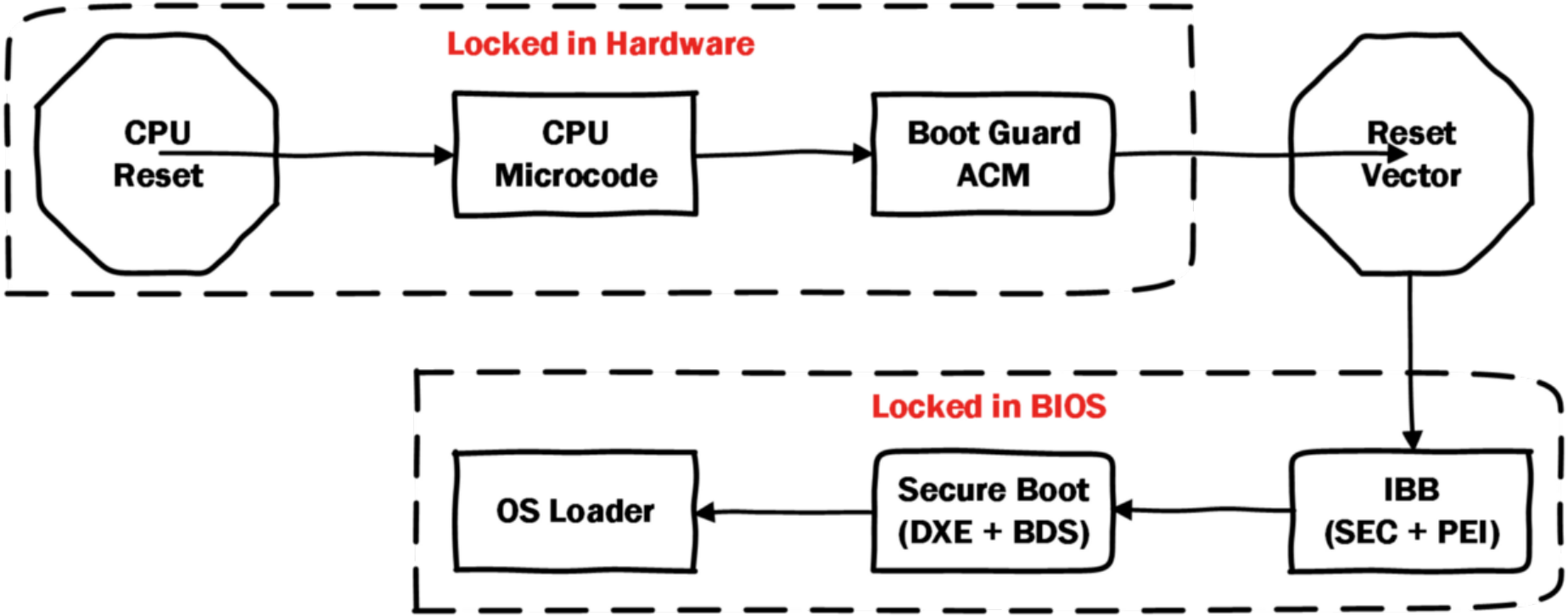
Purpose-built chip to establish hardware root of trust for Google Cloud servers

Google's purpose-built server

Jon McCune from Google
Presenting tomorrow!

https://cloudplatform.googleblog.com/2017/08/Titan-in-depth-security-in-plaintext.html

Intel BootGuard on commodity hardware

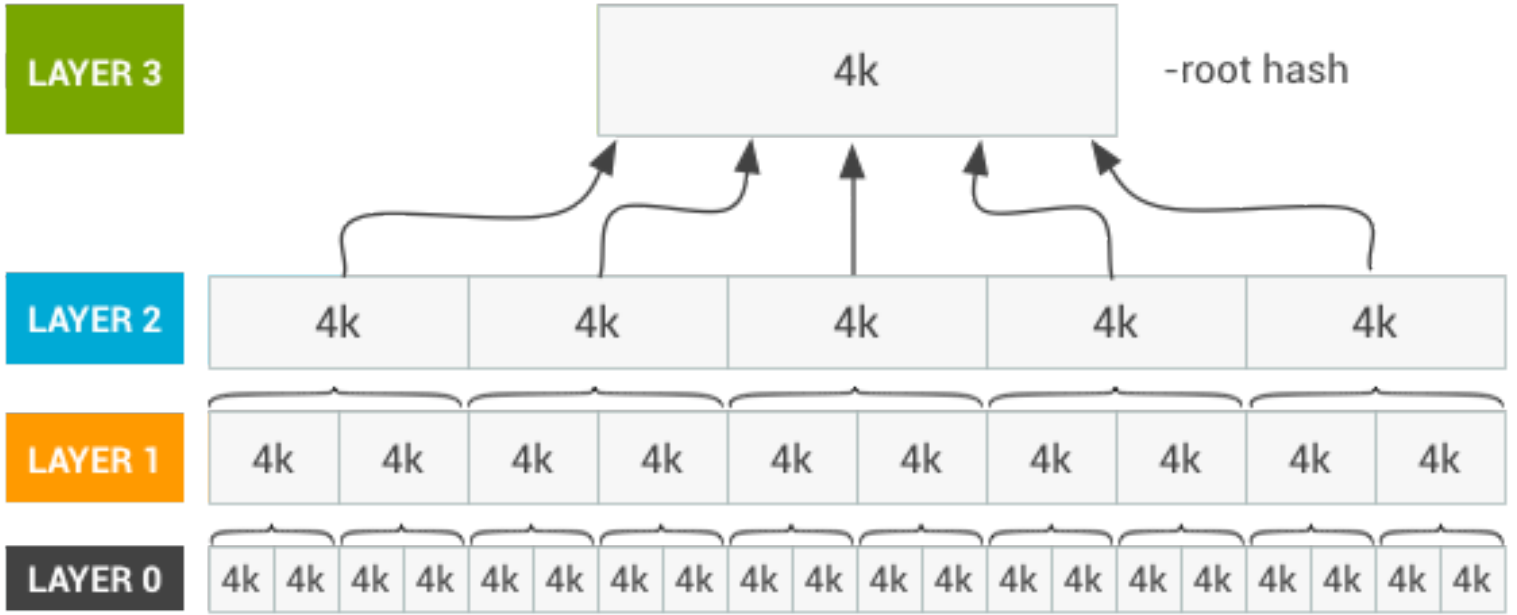


https://medium.com/@matrosov/bypass-intel-boot-guard-cc05edfca3a9


Yubico

```
#!/bin/sh
# Verify the next stages, extract the TPM root filesystem key
# and invoke the new hypervisor and dom0 kernel.

XEN=/boot/xen-4.6.3.gz
INITRD=/boot/initramfs-4.4.14-11.pvops.qubes.x86_64.img
KERNEL=/boot/vmlinuz-4.4.14-11.pvops.qubes.x86_64

gpgv "${XEN}.asc" "${XEN}" || die "Xen signature failed"
gpgv "${INITRD}.asc" "${INITRD}" || die "Initrd signature failed"
gpgv "${KERNEL}.asc" "${KERNEL}" || die "Kernel signature failed"

unseal-key /initrd/secret.key || die "root unseal failed"

kexec -l \
        --module "${KERNEL} root=LABEL=root rd.luks.keyfile=/secret.key" \
        --module "${INITRD}" \
        --command-line "no-real-mode console=vga" \
        "${XEN}" \
|| die "Unable to load kernel/hypervisor/initrd"

kexec -e || die "Unable to kexec"
```

dm-verity for signed, read-only filesystems



https://source.android.com/security/verifiedboot/

QUBES OS

A REASONABLY SECURE OPERATING SYSTEM

"If you're serious about security, Qubes OS is the best OS available today. It's what I use, and free."

— Edward Snowden, *whistleblower and privacy advocate*

Brendan Kerrigan on AEM
Presenting tomorrow!

System Management Mode


Do Hypervisors Dream
of Electric Sheep?
Vulnerability used in this section is VU#976132 a.k.a. S3 Resume Boot Script Vulnerability independently discovered by ATR of Intel Security, Rafal Wojtczuk of Bromium and LegbaCore
It's also used in Thunderstrike 2 by LegbaCore & Trammell Hudson


Put SMM handlers in Linux, not coreboot
Ron Minnich, Google
European coreboot Conference

Management Engine

Ring -3 OS: ME (Management Engine)

- Full Network manageability
- Regular Network manageability
- Manageability
- Small business technology
- Level III manageability
- IntelR Anti-Theft (AT)
- IntelR Capability Licensing Service (CLS)
- IntelR Power Sharing Technology (MPC)
- ICC Over Clocking
- Protected Audio Video Path (PAVP)
- IPV6
- KVM Remote Control (KVM)
- Outbreak Containment Heuristic (OCH)
- Virtual LAN (VLAN)
- TLS
- Wireless LAN (WLAN)

The Register®
Biting the hand that feeds IT

Security

https://www.theregister.co.uk/2017/05/01/intel_amt_me_vulnerability/

Red alert! Intel patches remote execution hole that's been hidden in chips since 2010

Vuln reported in March, now fix is coming...

By Chris Williams, US editor 1 May 2017 at 20:27

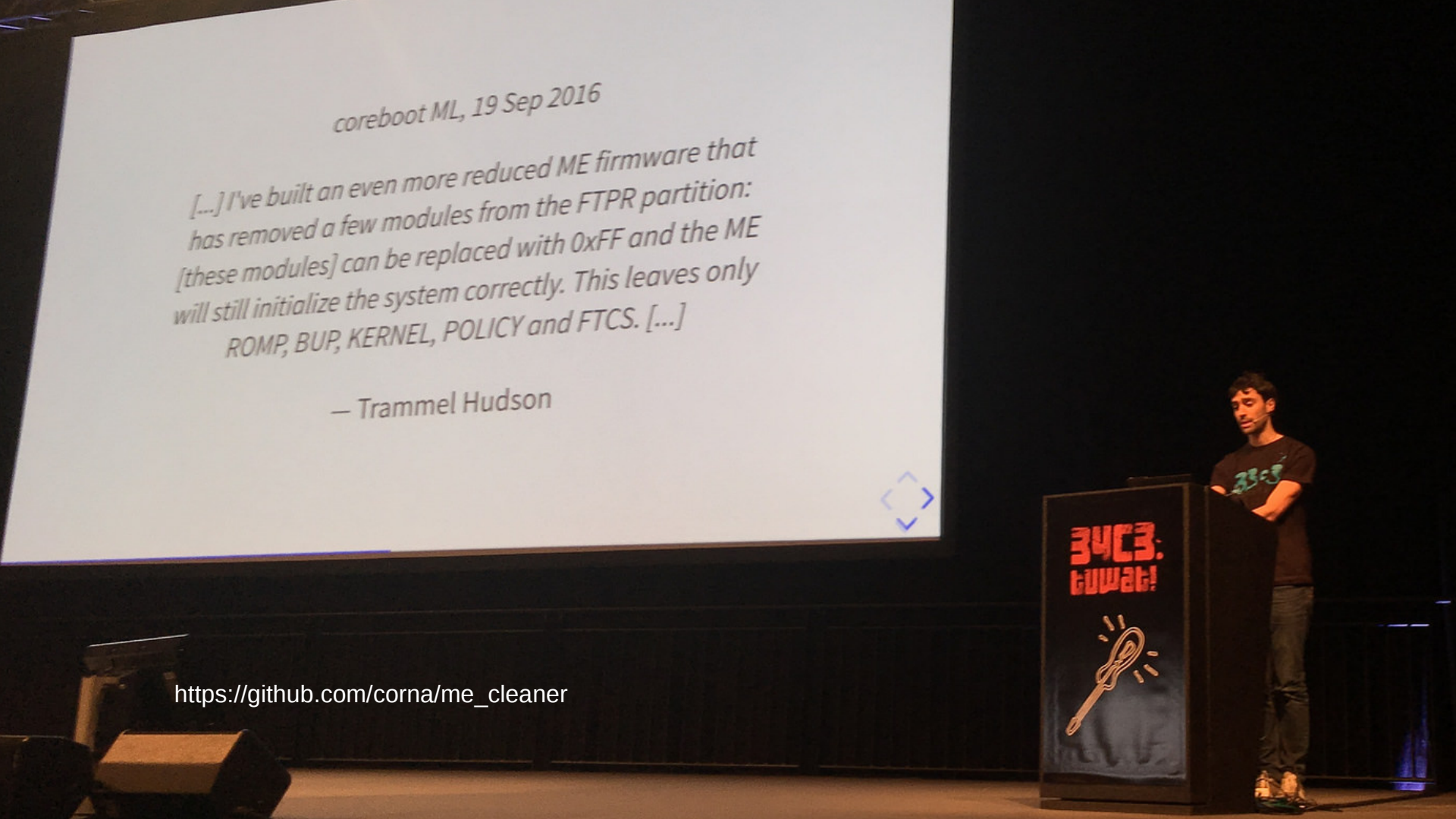
86 SHARE ▼

coreboot ML, 19 Sep 2016

[...] I've built an even more reduced ME firmware that has removed a few modules from the FTPR partition: [these modules] can be replaced with 0xFF and the ME will still initialize the system correctly. This leaves only ROMP, BUP, KERNEL, POLICY and FTCS. [...]

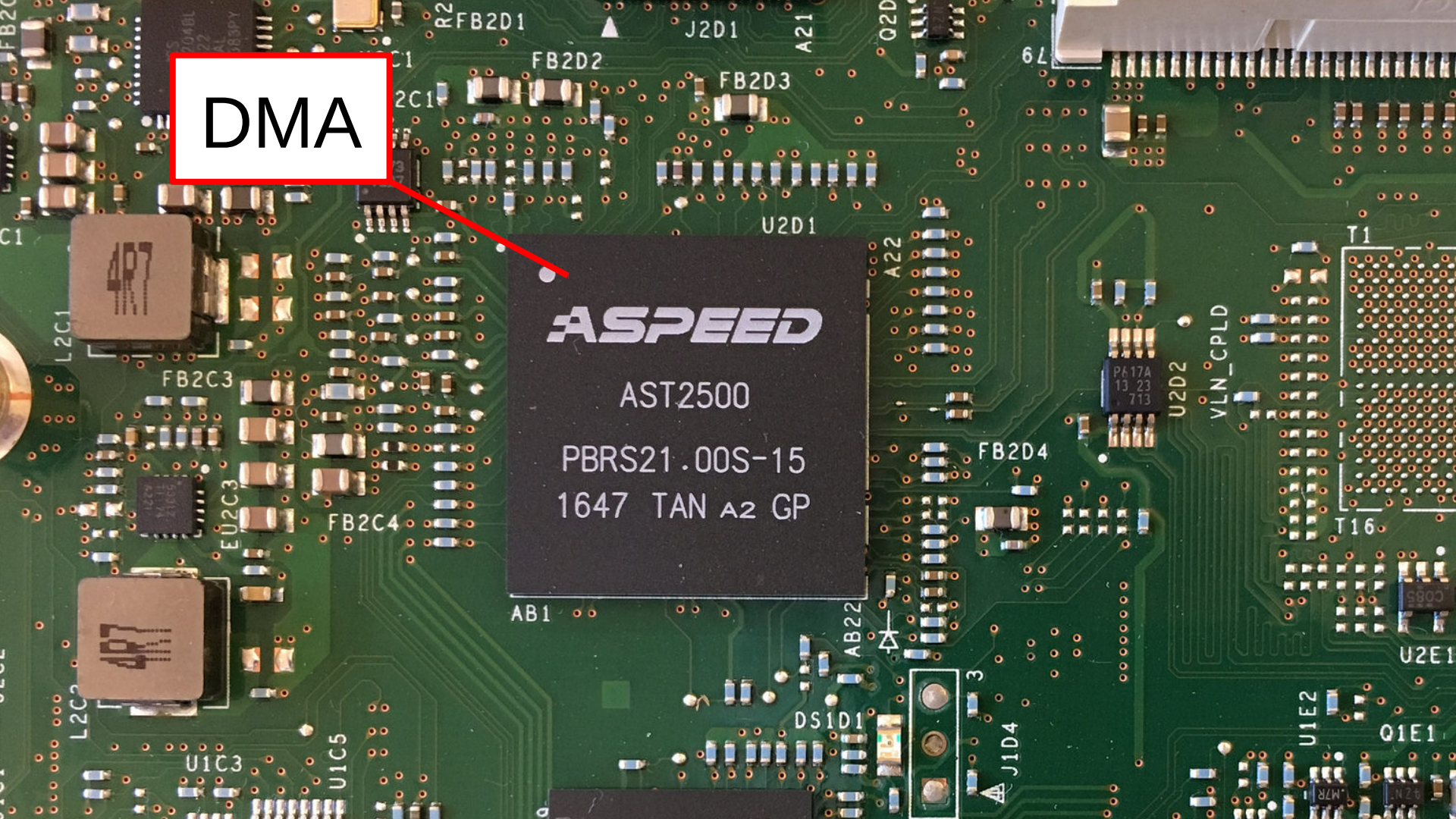
— Trammel Hudson

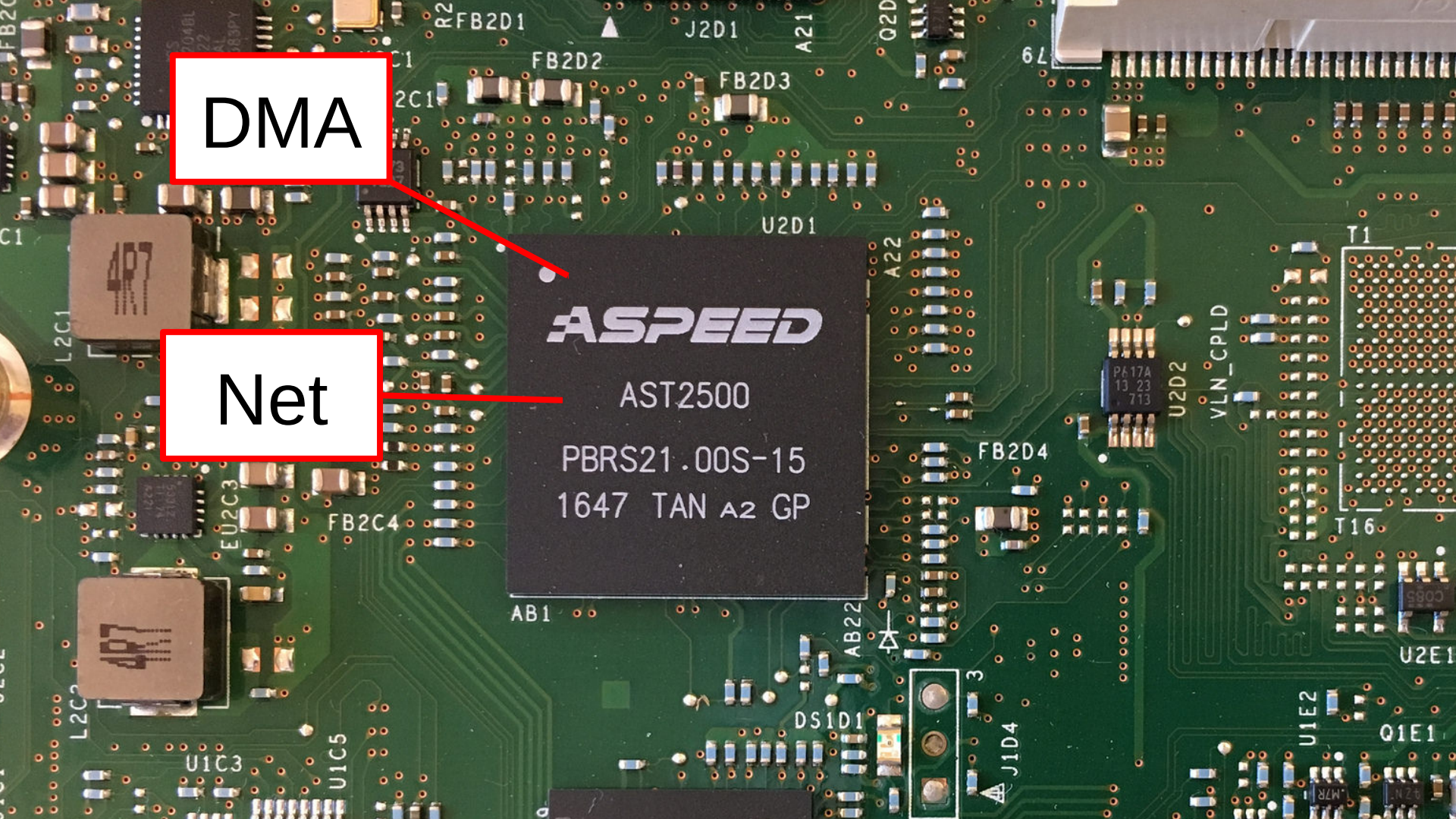
https://github.com/corna/me_cleaner

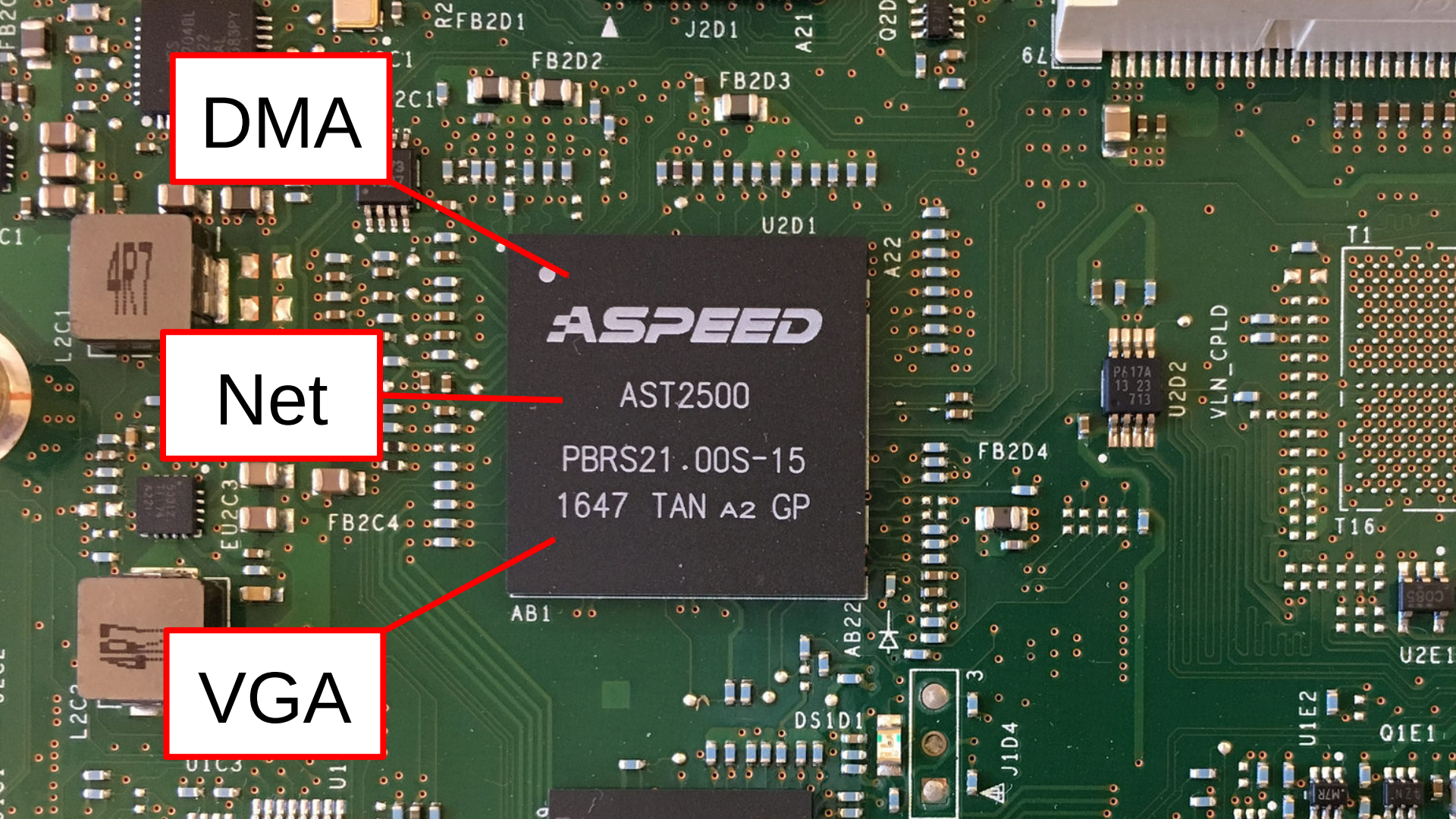


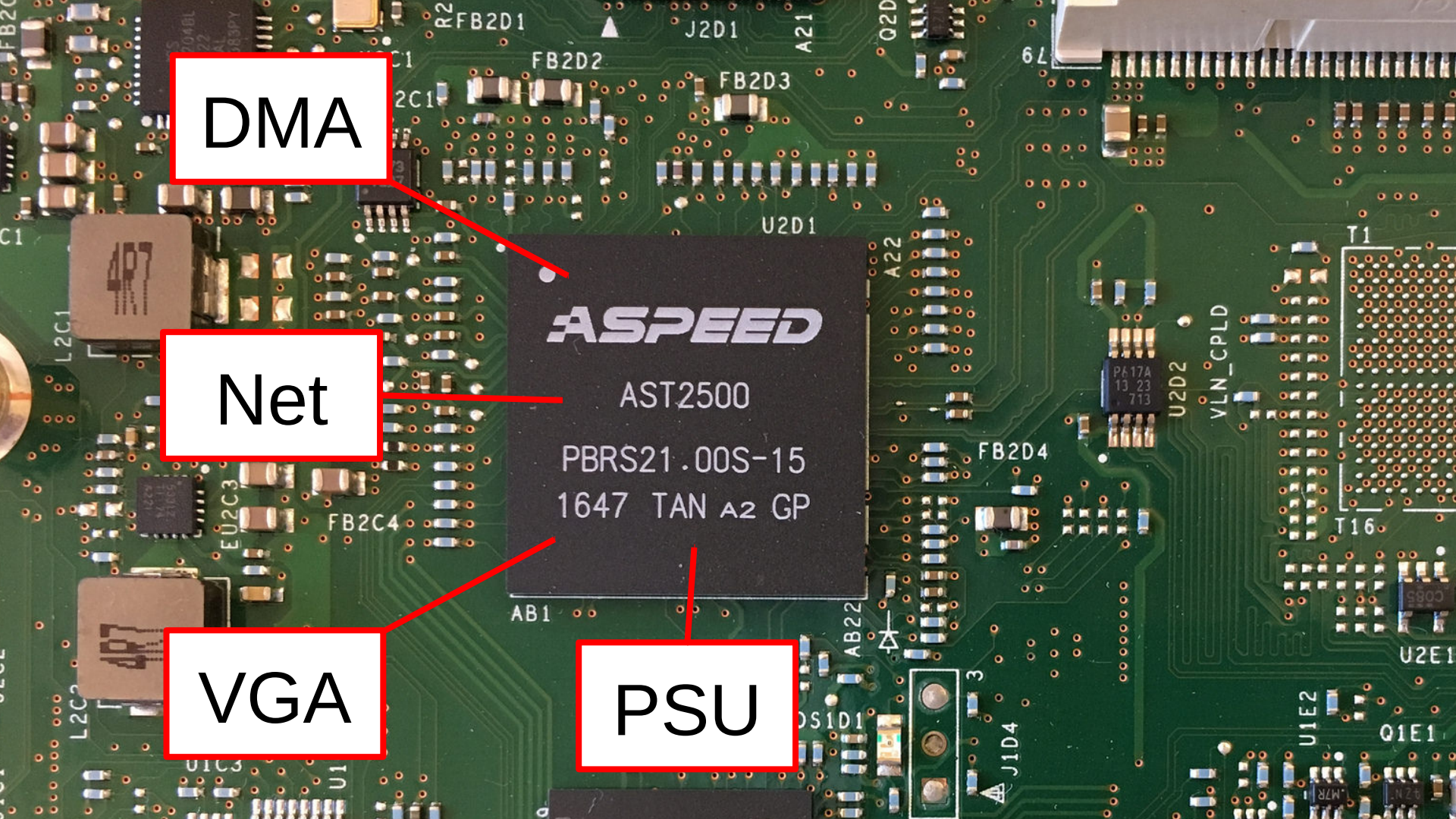
Board Management Controller

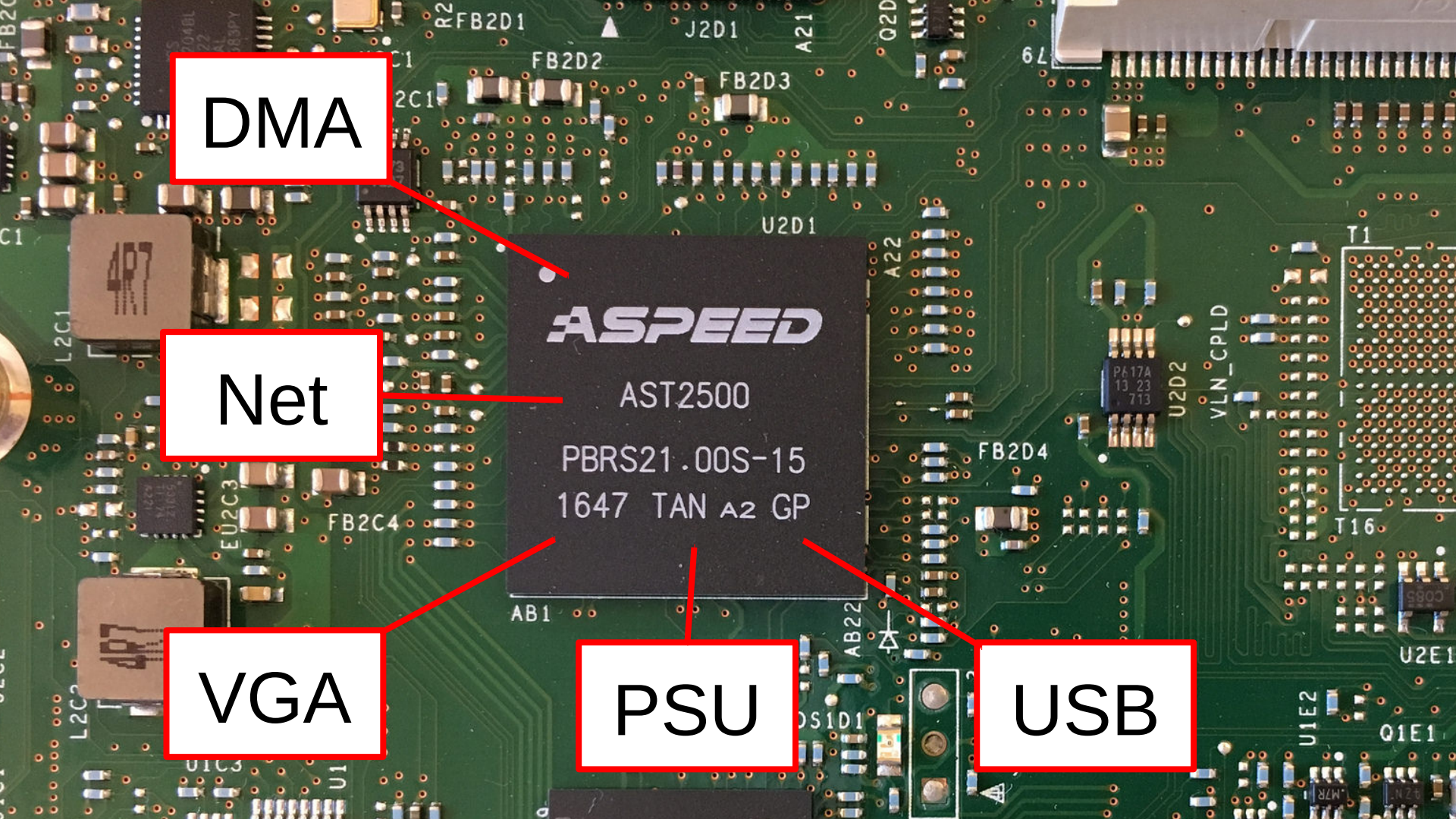

ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP
FB2D1
FB2D2
FB2D3
FB2D4
FB2C2
FB2C3
FB2C4
U2C1
Y2C1
U2D1
J2D1
A21
A22
AB1
AB22
U2D2
VLN_CPLD
T1
T16
U2E1
Q1E1
U1E2
DS1D1
J1D4
U1C3
U1C5
L2C1
L2C2
U2C3

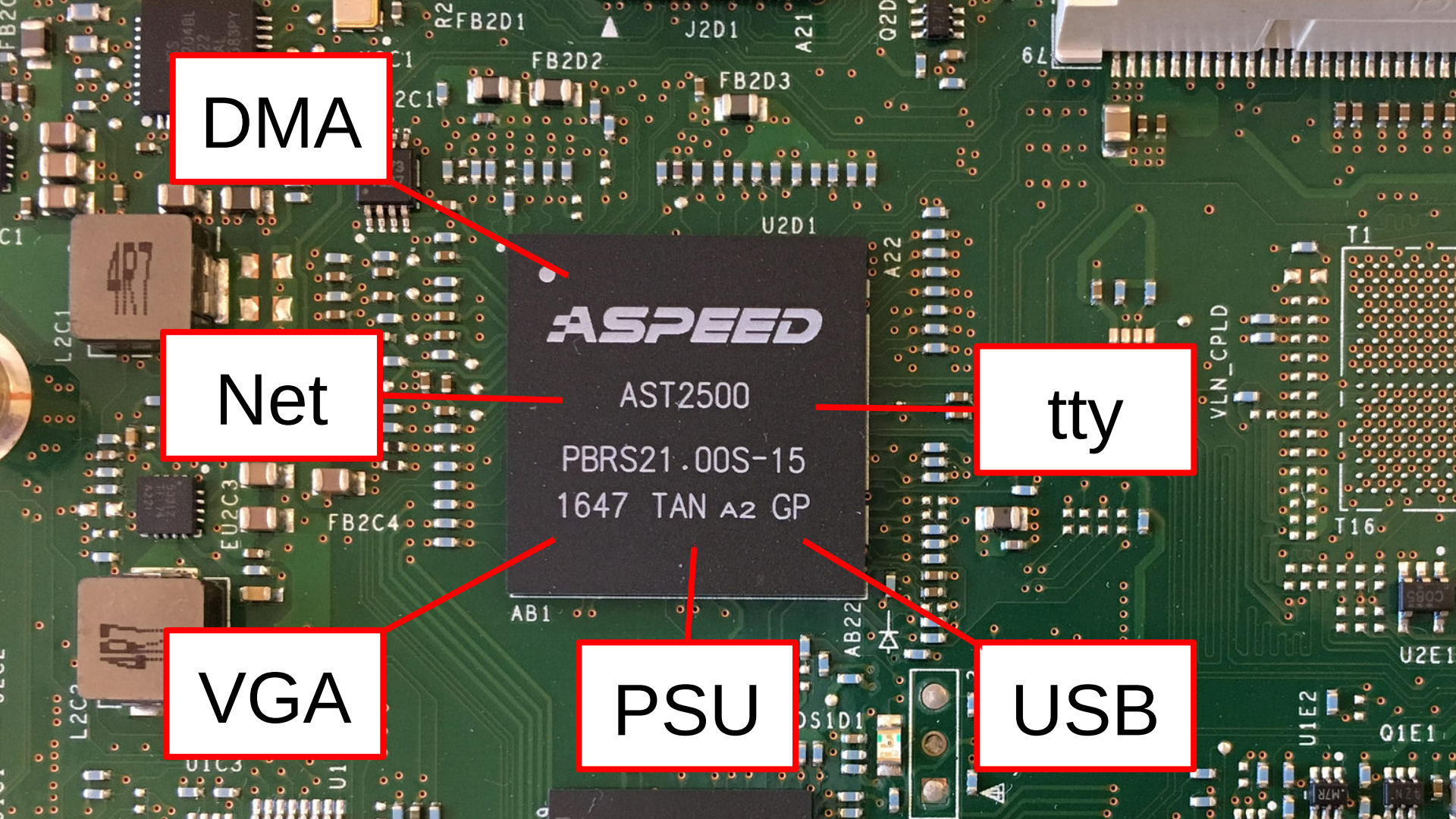

DMA
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP
U2D1
FB2D1
FB2D2
FB2D3
FB2D4
FB2C3
FB2C4
J2D1
A21
A22
AB1
AB22
T1
T16
U2D2
VLN_CPLD
U2E1
Q1E1
U1E2
DS1D1
J1D4
U1C3
U1C5
L2C1
L2C2
U2C3

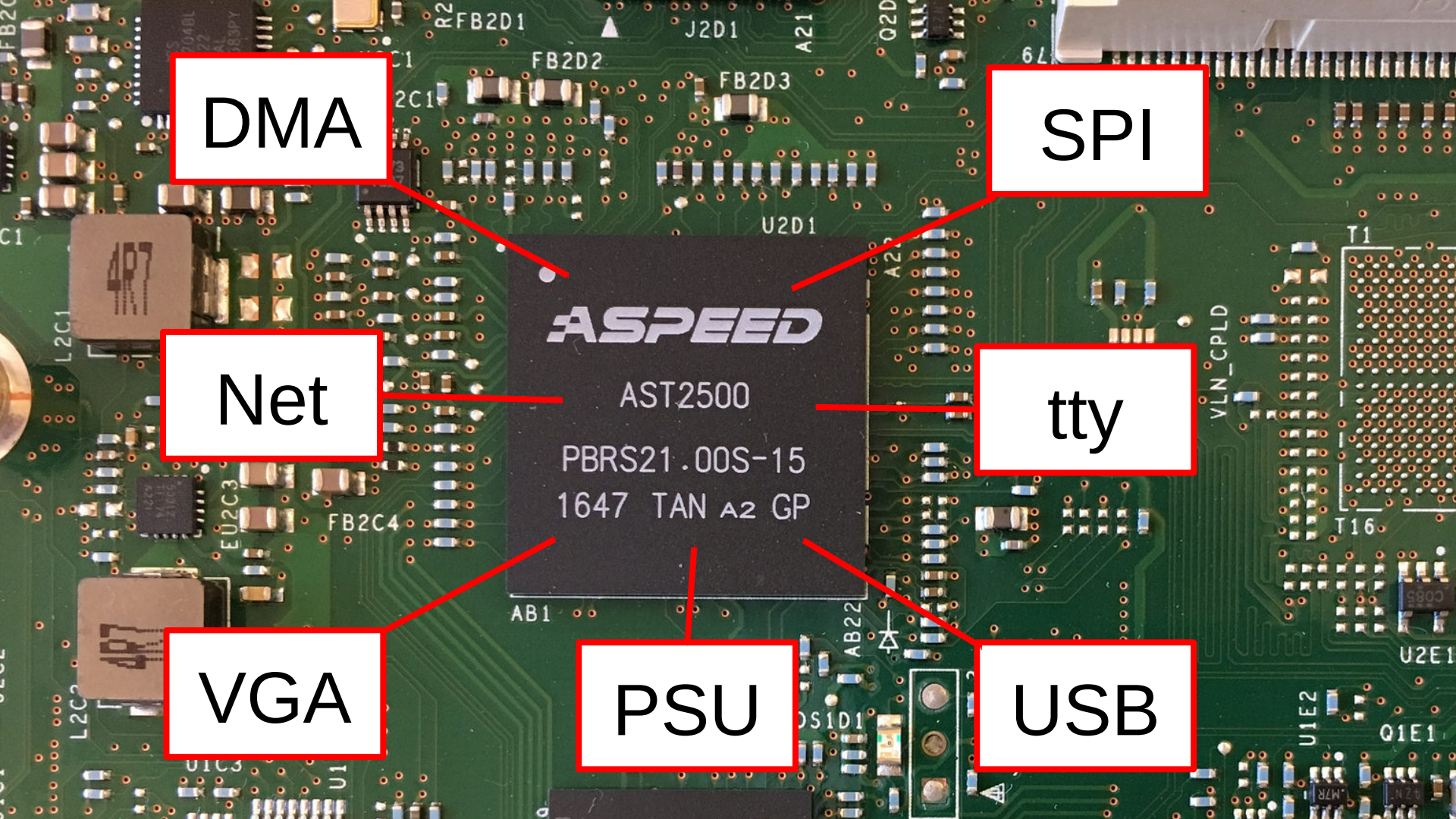

DMA
Net
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP
U2D1
FB2D1
FB2D2
FB2D3
FB2D4
FB2C4
J2D1
U2D2
VLN_CPLD
T1
T16
U2E1
Q1E1
U1E2
DS1D1
J1D4
U1C3
U1C5
AB1
AB22
A22
A21

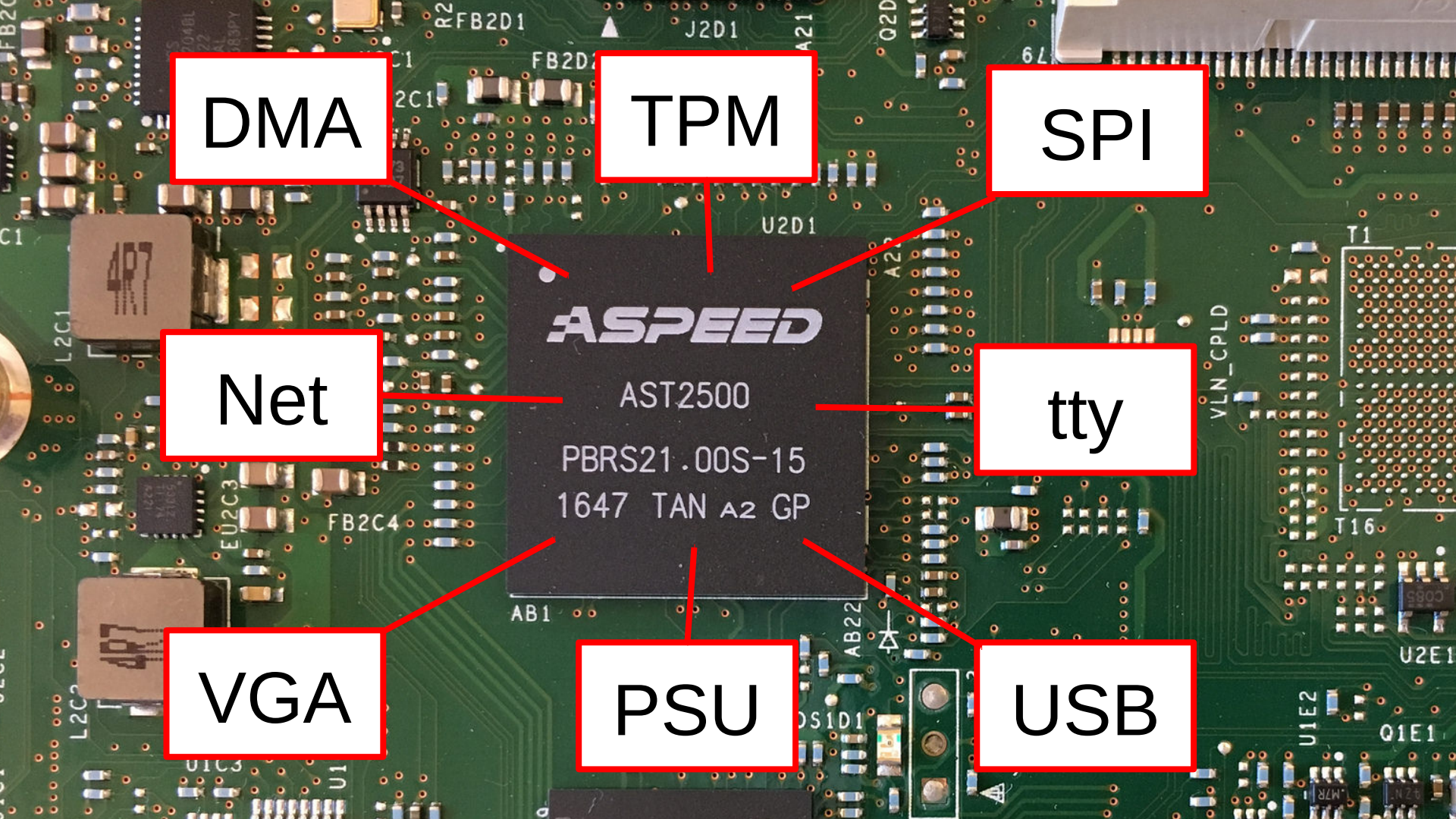

DMA
Net
VGA
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP
U2D1
FB2D1
FB2D2
FB2D3
FB2D4
FB2C4
J2D1
U2D2
VLN_CPLD
T1
T16
U2E1
Q1E1
U1E2
DS1D1
J1D4
AB1
AB22
A22
A21
U1C3
L2C1
L2C2
U2C3

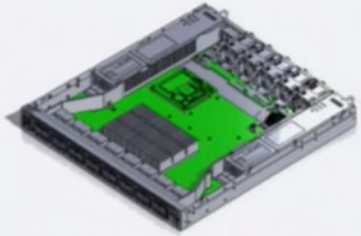

DMA
Net
VGA
PSU
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP
U2D1
FB2D1
FB2D2
FB2D3
FB2D4
J2D1
FB2C4
U2D2
VLN_CPLD
U2E1
Q1E1
J1D4
T1
T16
AB1
AB22
A21
A22

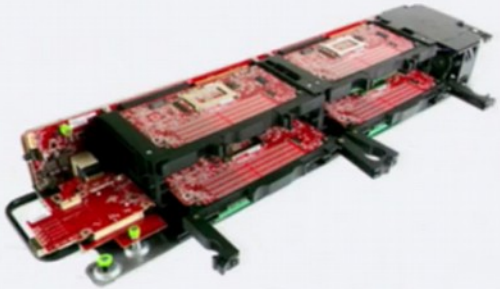

DMA
Net
VGA
PSU
USB
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP

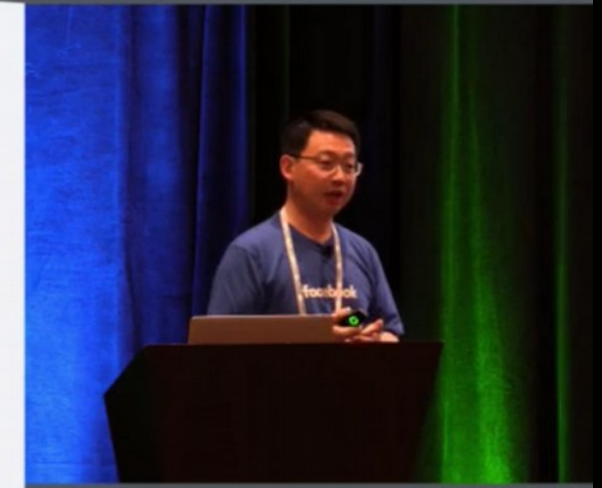

DMA
Net
VGA
PSU
tty
USB
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP


DMA
SPI
Net
tty
VGA
PSU
USB
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP


DMA
TPM
SPI
Net
tty
VGA
PSU
USB
ASPEED
AST2500
PBRS21.00S-15
1647 TAN A2 GP







Embedded Linux Conference

OpenIoTSummit

OpenBMC - A Customized Linux Distribution Running on BMC (Tian Fang @ Facebook)

Quanta
P/N:DAF20TB18C0 Rev:
P/N: 20F20BU0150
ARTFBF2009701059S2A00LS
05000236
MAC1
1009.15

Getting started with LinuxBoot

Secure | https://github.com/linuxboot/linuxboot

linuxboot / linuxboot

Watch 29 | Star 154 | Fork 9

Code | Issues 8 | Pull requests 0 | Projects 0 | Insights

The LinuxBoot project is working to enable Linux to replace your firmware on all platforms.

firmware uefi bios linux-kernel security

564 commits | **2** branches | **0** releases | **10** contributors | GPL-2.0

Secure | https://github.com/osresearch/heads

osresearch / heads

Watch 45 | Star 516 | Fork 54

Code | Issues 73 | Pull requests 10 | Projects 0 | Wiki | Insights

A minimal Linux that runs as a coreboot or LinuxBoot ROM payload to provide a secure, flexible boot environment for laptops and servers. http://osresearch.net/

coreboot bootrom xen firmware linux tpm verifiedboot rom

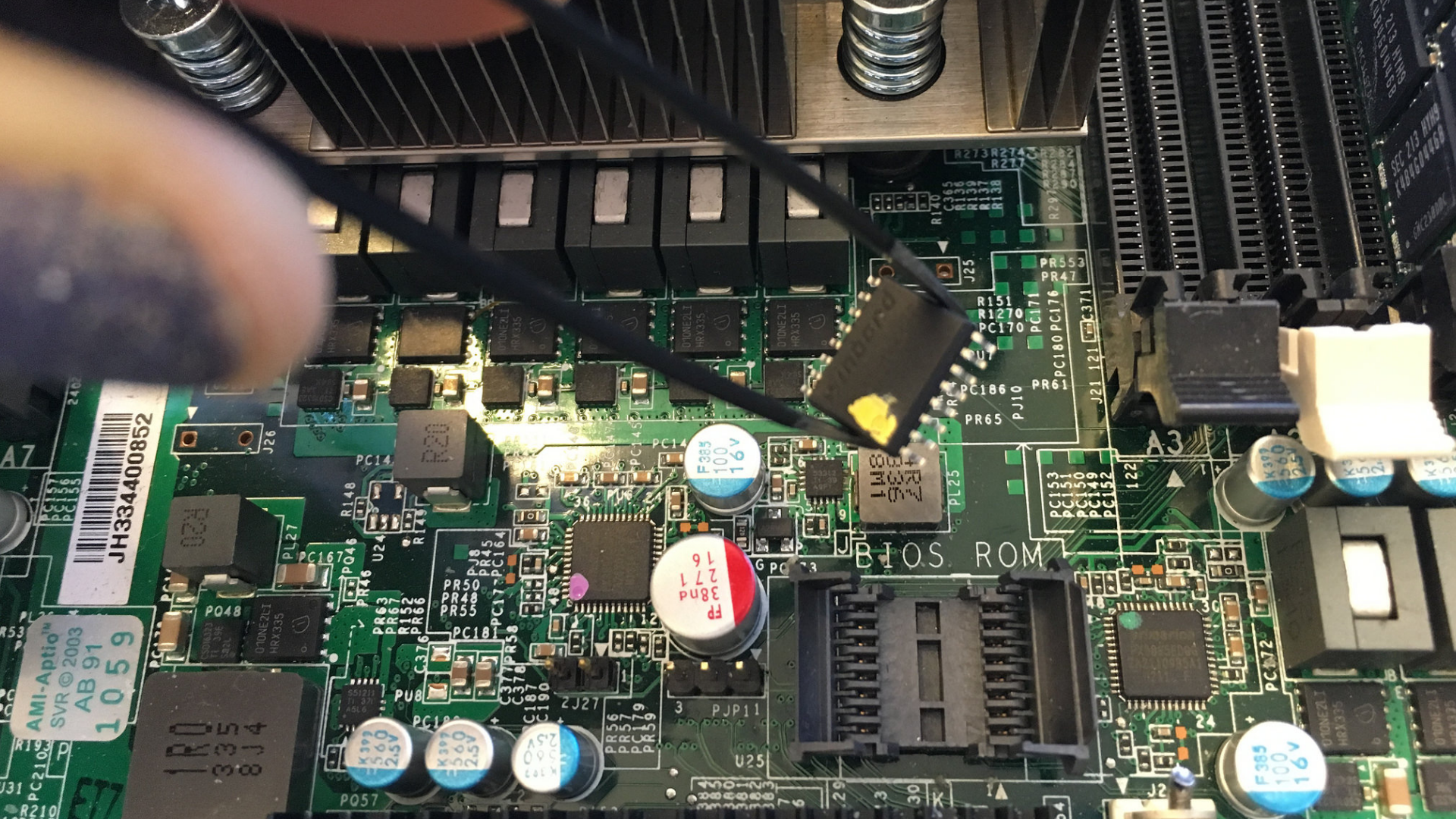
716 commits | **3** branches | **6** releases | **13** contributors | GPL-2.0

U_SPI_BIOS1

U_SPI_BIOS2

R9994

BIOS
1.0.4


JH334400852
AMI-Aptio™
SVR © 2003
AB 91
1059
BIOS ROM

Secure
Flexible
Resilient

Open
Reproducible
Measured


LinuxBoot.org