



LinuxBoot: Firmware is the new software

Trammell Hudson (Two Sigma Investments)

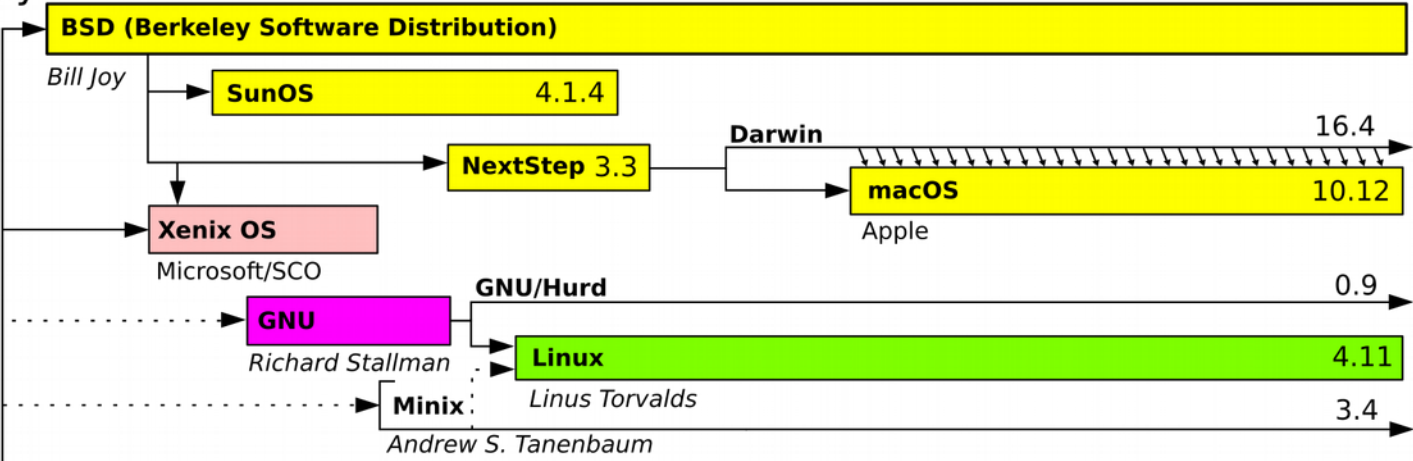
Ron Minnich (Google)

Andrea Barberio (Facebook)

Jean-Marie Verdun (Horizon Computing)

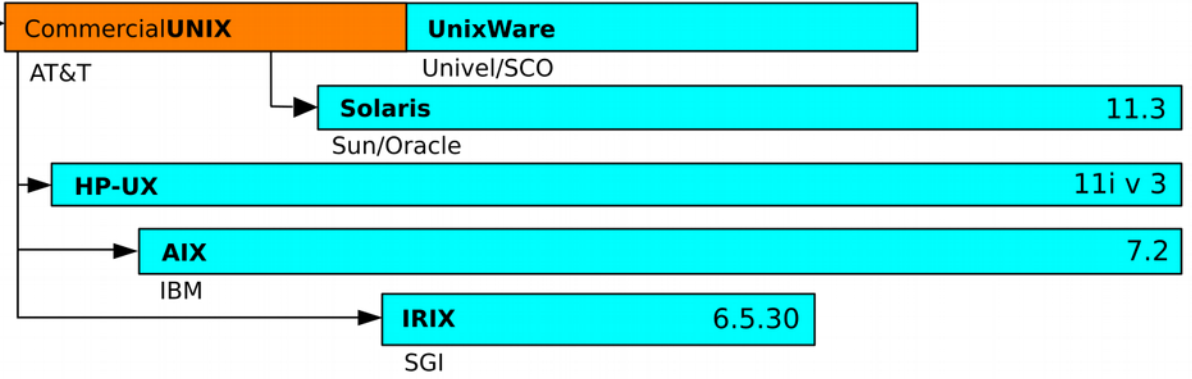
1970 1980 1990 2000 2010 Time

BSD family



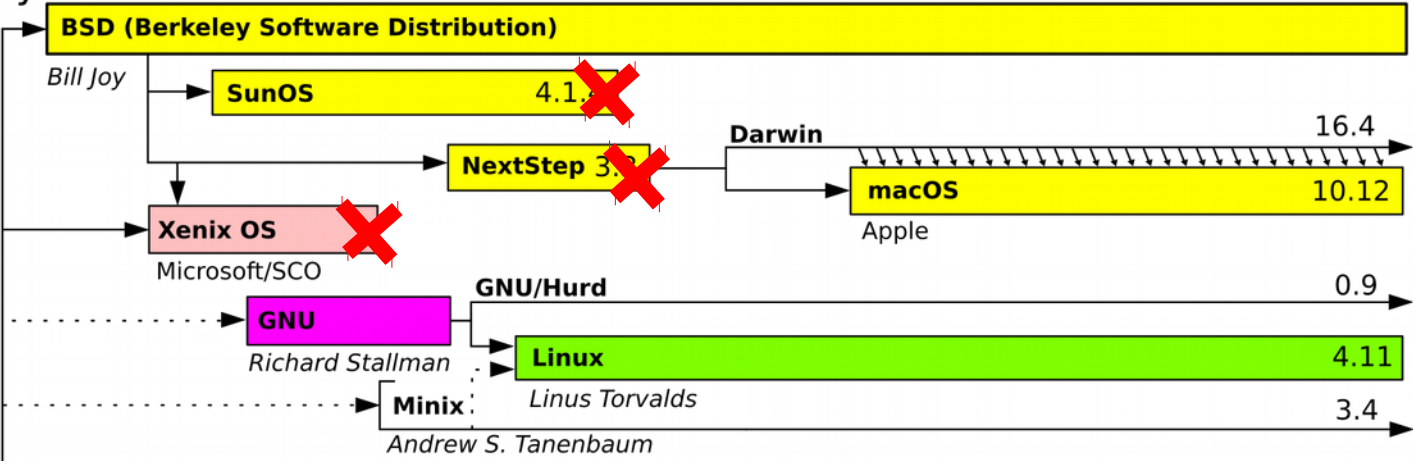
Research **UNIX** 10.5

Bell Labs: Ken Thompson, Dennis Ritchie, et al.



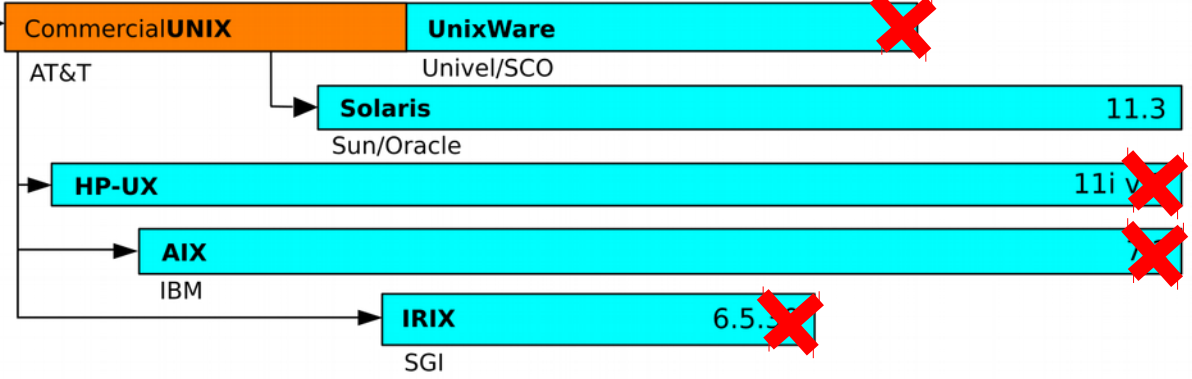
1970 1980 1990 2000 2010 Time

BSD family



Research UNIX 10.5

Bell Labs: Ken Thompson, Dennis Ritchie, et al.



System III & V family

1970 1980 1990 2000 2010 Time

BSD family



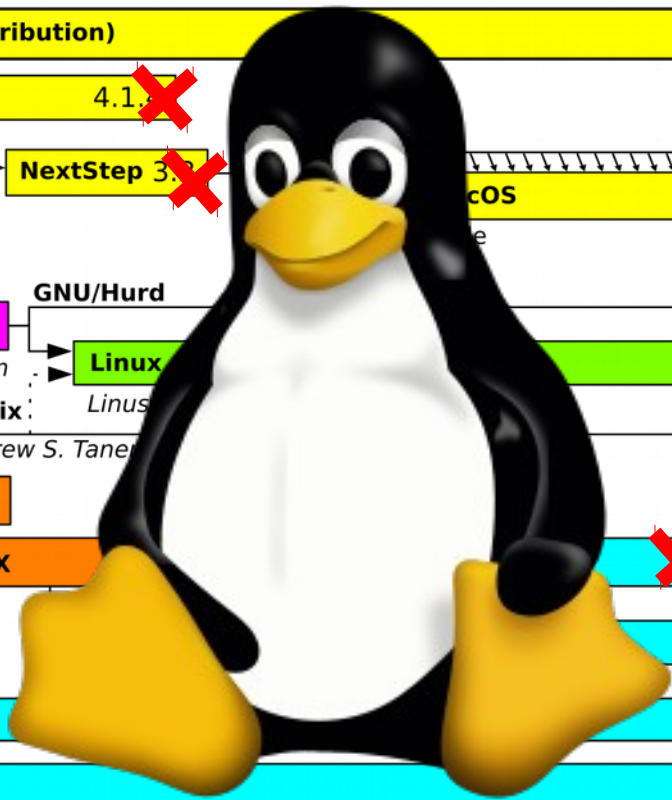
Bell Labs: Ken Thompson, Dennis Ritchie, et al.



System III & V family

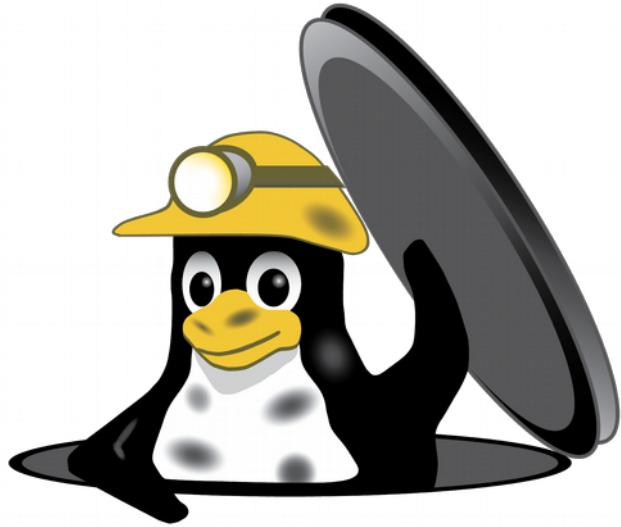


SGI

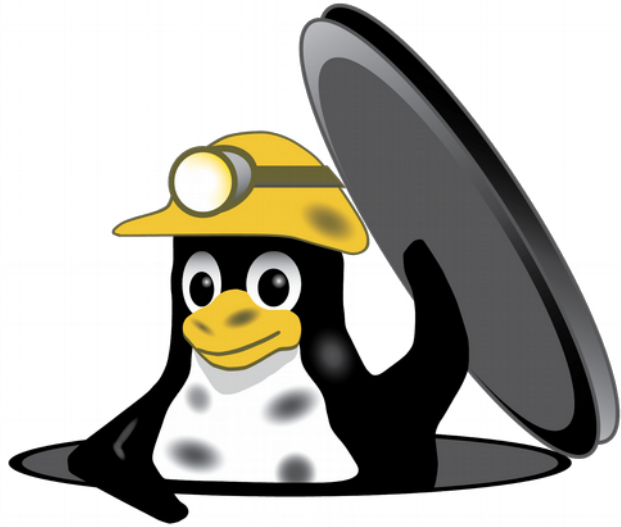


“Tux” by Larry Ewing





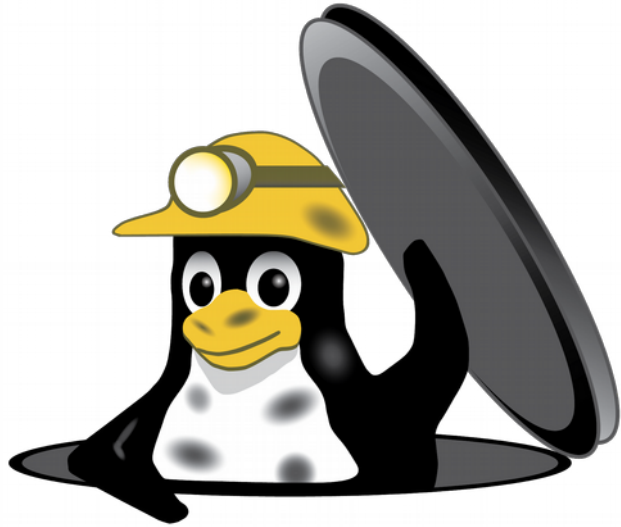
LinuxBIOS
(1999)



LinuxBIOS
(1999)



coreboot
(2008)

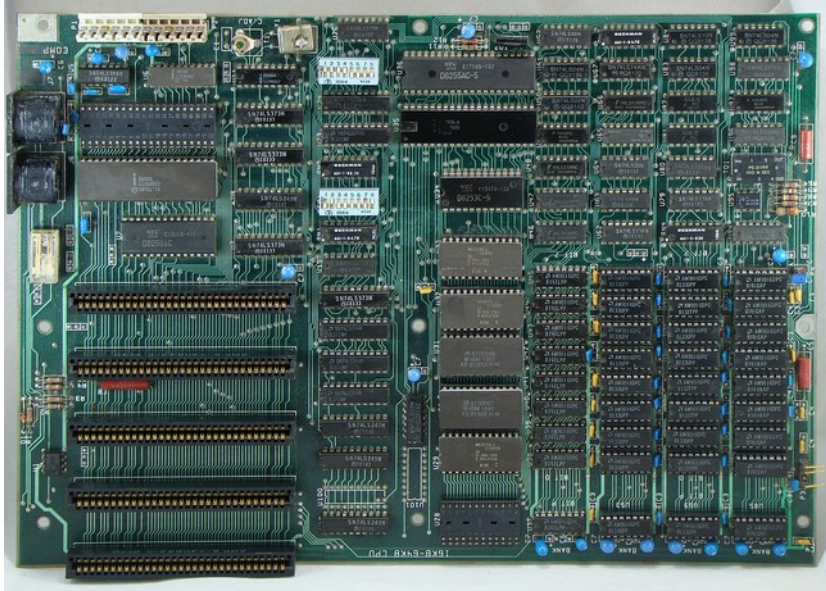


LinuxBIOS
(1999)

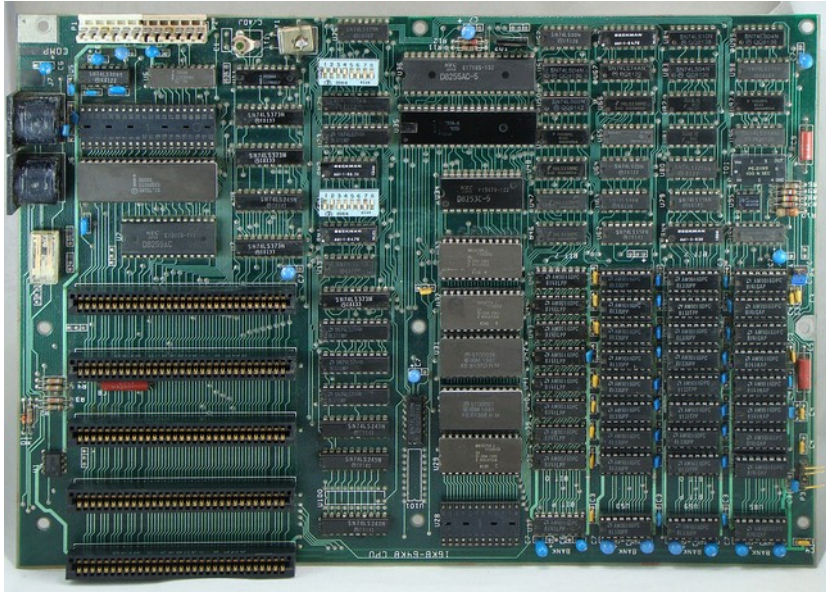


coreboot
(2008)





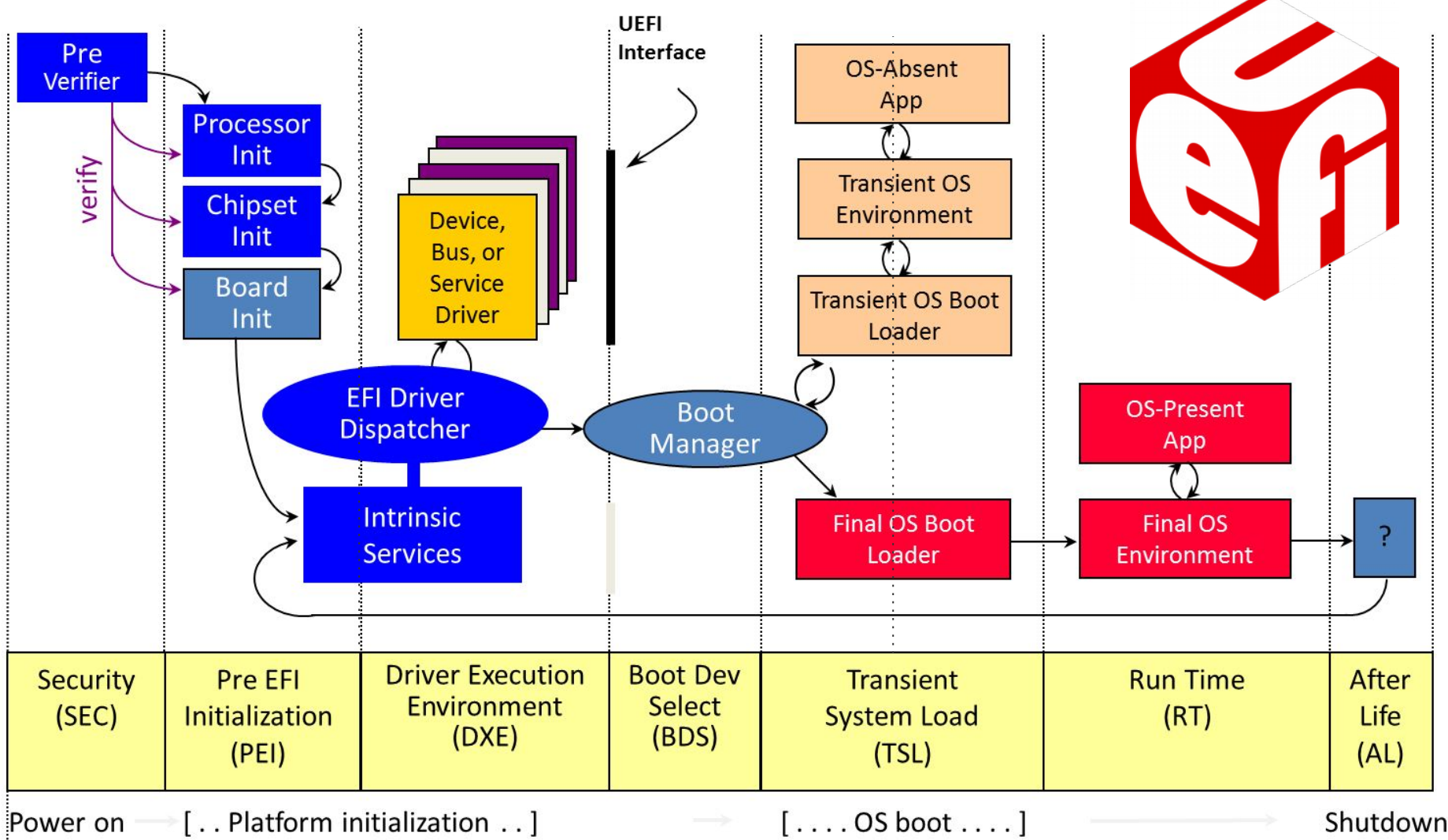
IBM BIOS
(1983)

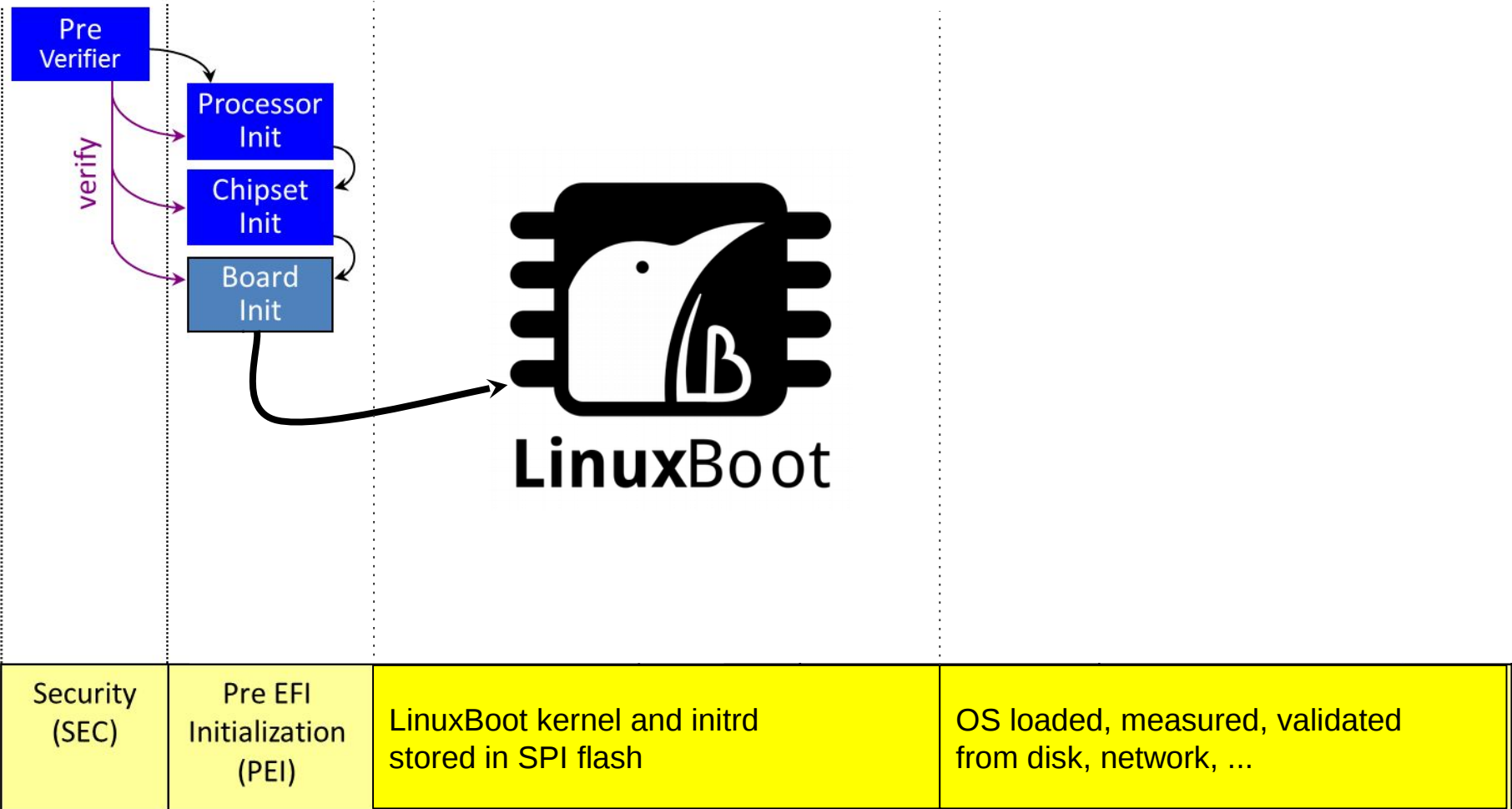


IBM BIOS
(1983)

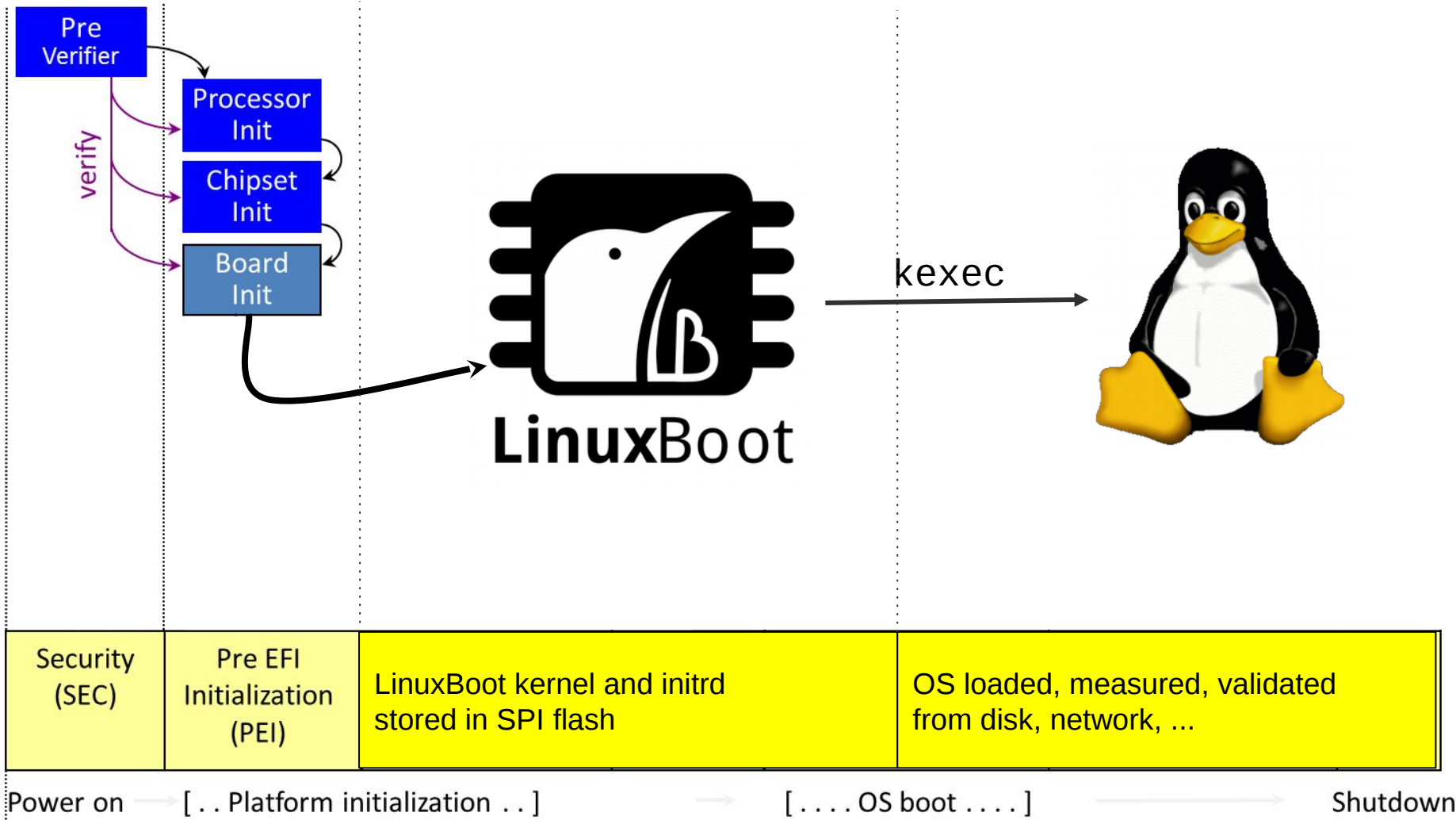


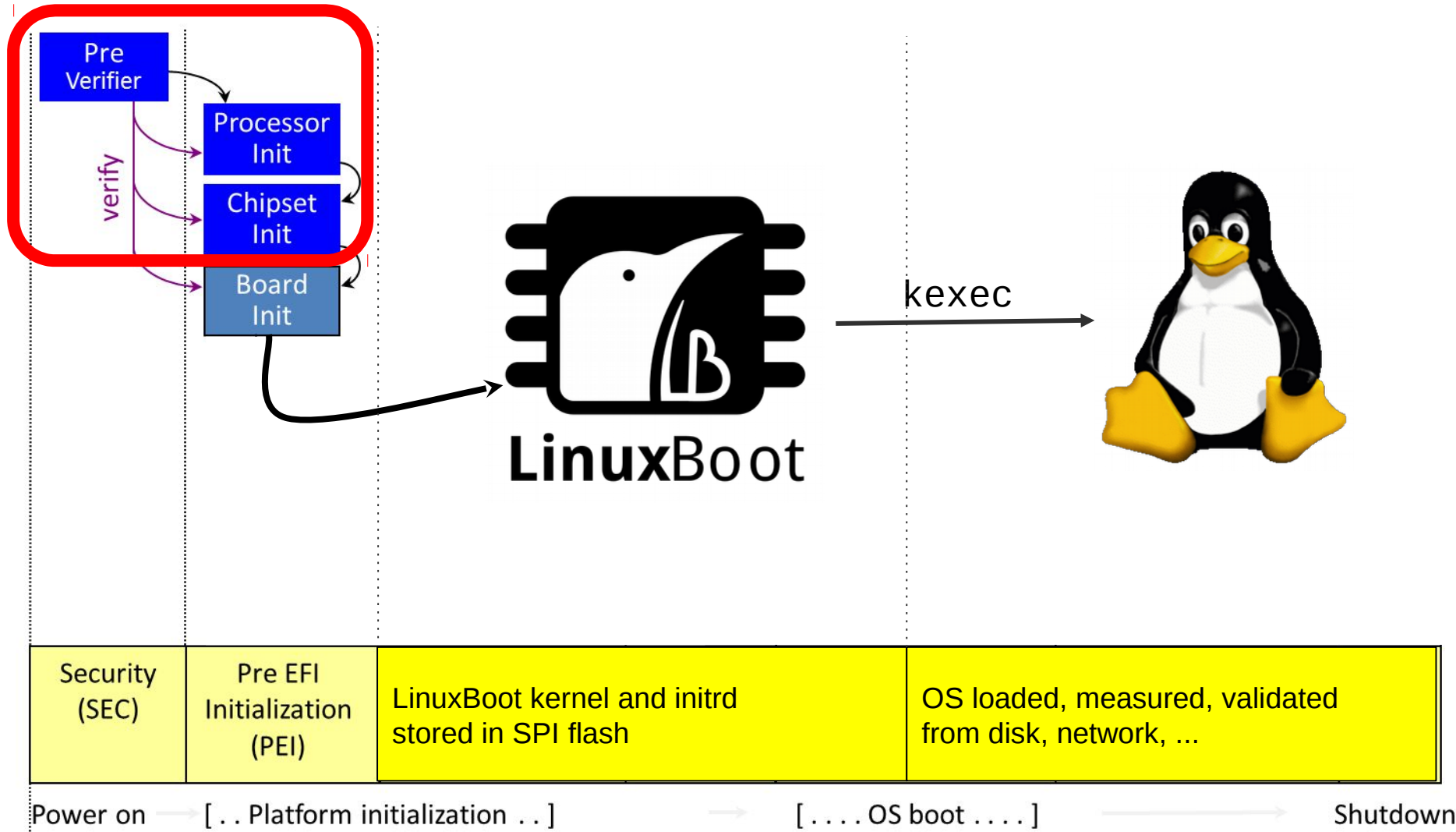
Unified Extensible
Firmware Interface
(1995)





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







RESOURCE &
DESIGN CENTER



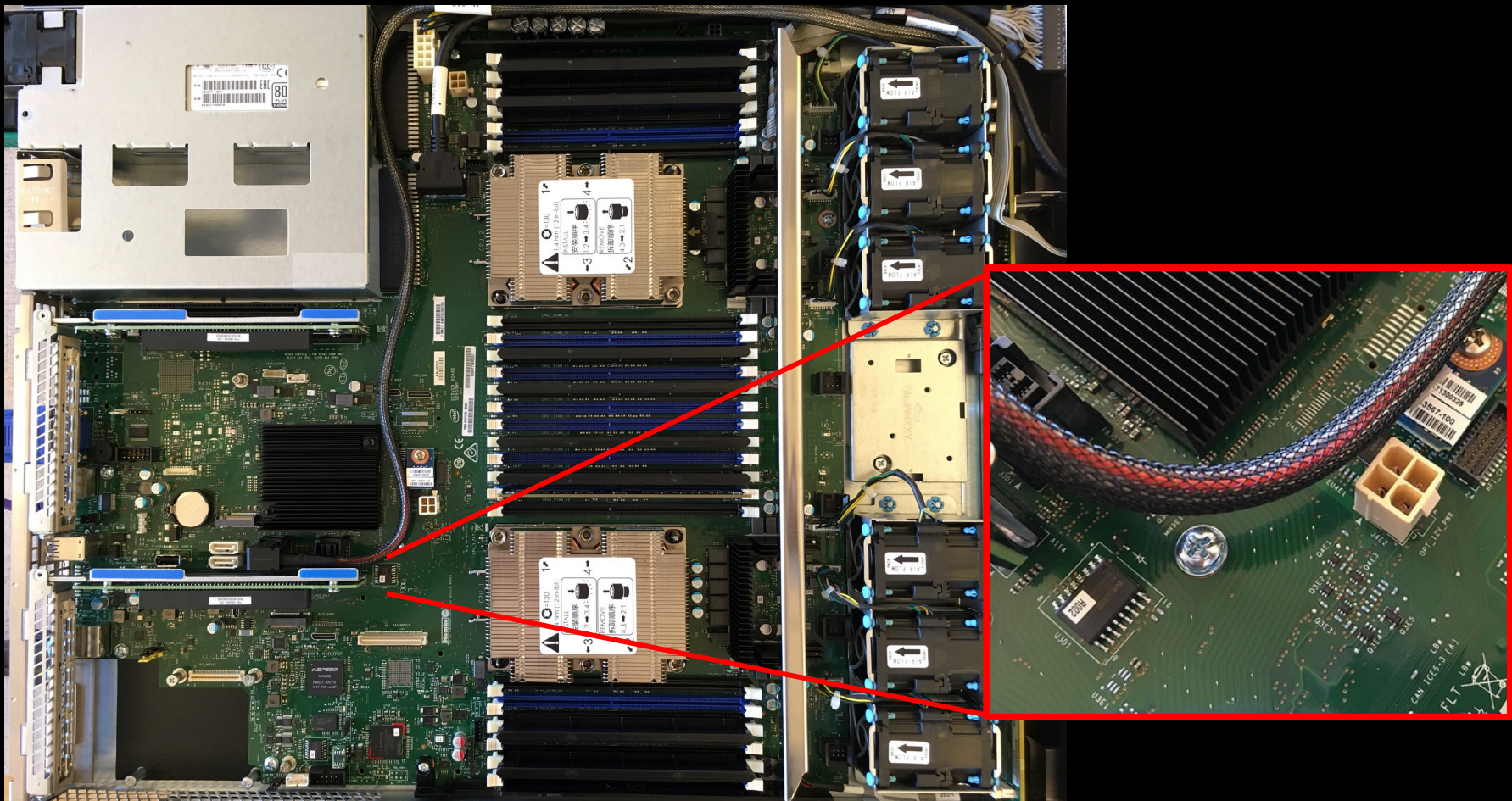
Intel® Firmware Support Package

AN EASY-TO-INTEGRATE AND SCALABLE FIRMWARE SOLUTION FOR DEVELOPERS

Intel® Firmware Support Package (Intel® FSP) provides key programming information for initializing Intel® silicon and can be easily integrated into a boot loader of the developer's choice. It is easy to adopt, scalable to design, and economical to build. Components include:

- › **CPU, memory controller, and Intel® chipset initialization functions as a binary pack** preserves existing features and frameworks, and fits into existing boot loaders
- › **Integration guide:** Describes the APIs available to communicate with Intel FSP and to integrate it with a boot-loader solution

Vincent Zimmer from Intel
Presenting after the break!



Intel S2600WF



Open Systems Firmware



Boot Loaders Support



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.

```
root@kali:~# cd /root/.ssh/
root@kali:~/.ssh# ls
authorized_keys  id_rsa.pub  id_rsa
root@kali:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCA...
root@kali:~/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCA...
root@kali:~/.ssh# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA...
-----END RSA PRIVATE KEY-----
root@kali:~/.ssh#
```



Security

Flexibility

Resiliency

Security

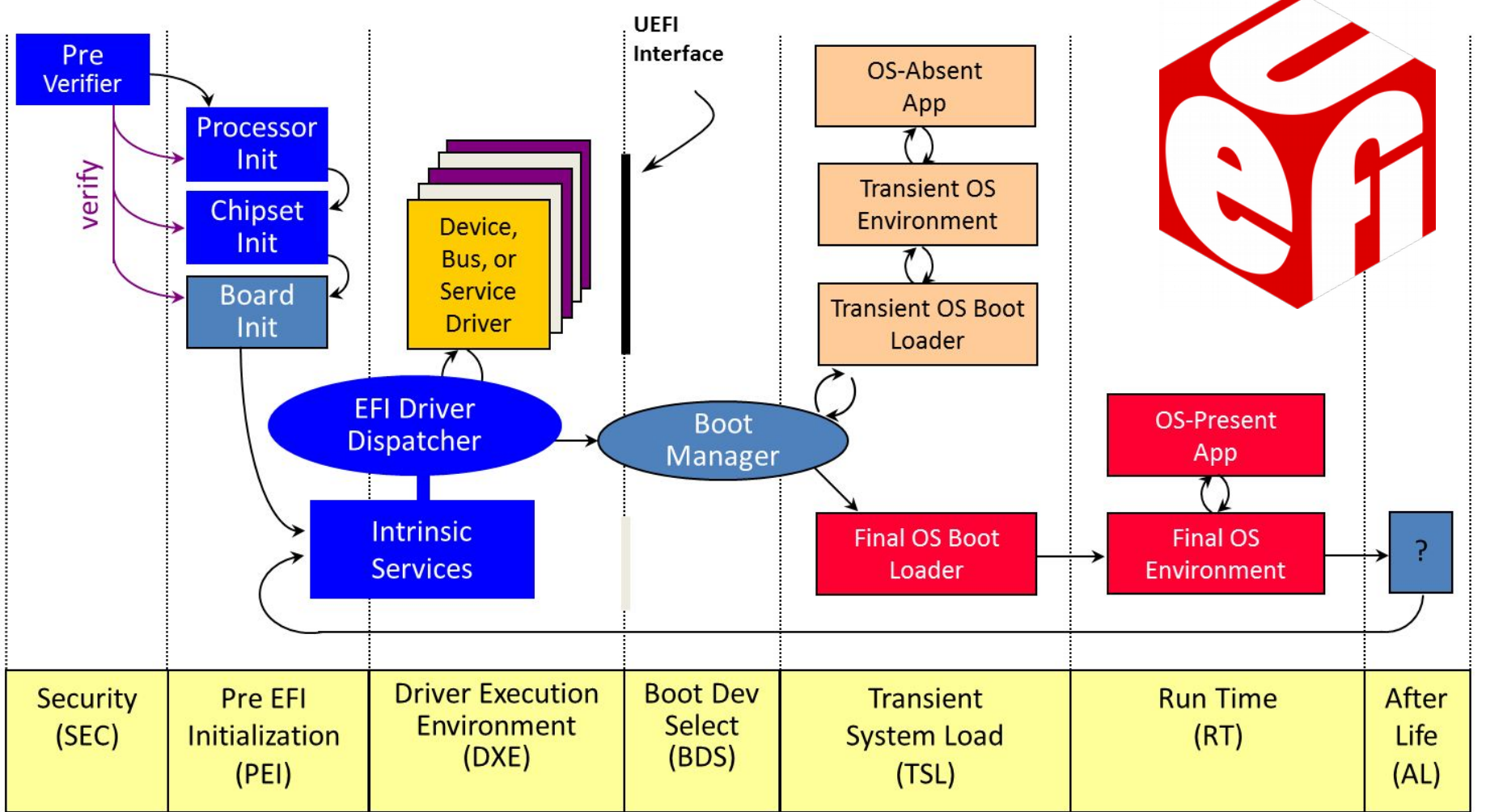
Flexibility

Resiliency

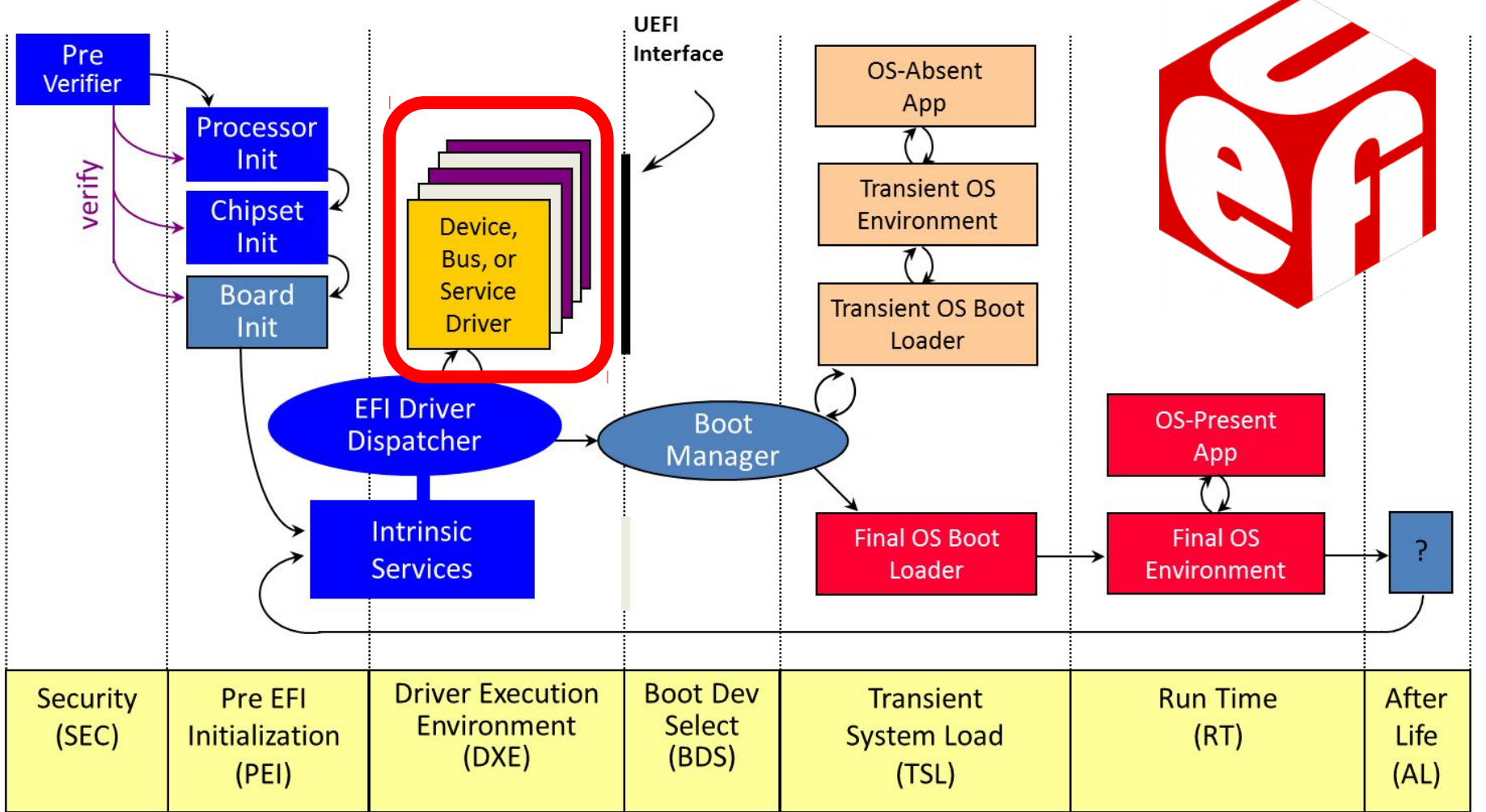
Minimize attack surface

Reduce

~~Minimize~~ attack surface



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



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

DxeCore	SlotDataUpdateDxeLightningRidgeEXRP	CpuIoDxe	ItkLogoProcess	TcgDxe	PiSmmCore	WheaElog
FastVideoDxe	SsidSvidDataUpdateDxeLightningRidgeEXRP	CpuIo2Dxe	SmIFlashSigned	TcgSmm	SmmCommunicationBuffer	UncoreErrorLog
PcdDxe	StaticSkuDataDxeSawtoothPass	HiiDatabase	SINIT	BmcAcpiSwChild	PiSmmCpuDxeSmm	PcieErrorLog
RegAccessDxe	SetupConfigUpdateDxeSawtoothPass	DataHubDxe	TxtDxe	PlatformPreVariableDxe	CpuIo2Smm	PvModule
RegAccessSMM	OpromUpdateDxeSawtoothPass	FrameworkHiiAlias	FixedPlatformDxe	DFSDxe	BIOSGuard	KtiErrorRuntime
ReportStatusCodeRouterRuntimeDxe	SmbiosDataUpdateDxeSawtoothPass	Legacy8259	HistiHvProviderDxe	BmcElog	Ps2KeyboardDxe	KtiErrorLogPost
StatusCodeHandlerRuntimeDxe	Usb0cUpdateDxeSawtoothPass	CpuArchDxe	SnpDxe	PlatformErrorGeneration	Ps2MouseDxe	WheaPlatformBoot
ReportStatusCodeRouterSmm	IioCfjUpdateDxeSawtoothPass	PlatformCpuPolicy	DnpDxe	GenericElog	S3SaveStateDxe	WheaErrorLog
StatusCodeHandlerSmm	SlotDataUpdateDxeSawtoothPass	CpuPmpDxe	MnpDxe	SmbMmcElog	AcpiS3SaveDxe	LastBootErrorLog
DataHubStatusCodeHandlerDxe	SsidSvidDataUpdateDxeSawtoothPass	SMBIOSFilter	VlanConfigDxe	SmmGenericElog	BootGraphicsResourceTableDxe	McBankErrorInjection
StatusCodeRuntimeDxe	FpkConfigUpdateDxeSawtoothPass	Metronome	ArpDxe	IpMRedirFlow	BootScriptExecutorDxe	CpuCsAccess
SectionExtractionDxe	StaticSkuDataDxeNeonCityFPGA	WatchdogTimer	Dhcp4Dxe	OsMdt	SmmLockBox	CpuCsAccessSMM
GenericIpmi	SetupConfigUpdateDxeNeonCityFPGA	PcRtc	Ip4Dxe	BmcVariableDriver	PiSmmCommunicationSmm	CrystalRidge
SmmGenericIpmi	OpromUpdateDxeNeonCityFPGA	RuntimeDxe	Mftfp4Dxe	OmMefwPatch	AcpiSmmPlatform	CrystalRidgeSMM
UbaConfigDatabaseDxe	SmbiosDataUpdateDxeNeonCityFPGA	PciHostBridge	Udp4Dxe	SoIStatus	PciHotPlug	JedecNVDimm
UbaInitDxe	Usb0cUpdateDxeNeonCityFPGA	PpmInitialize	Tcp4Dxe	FrBDriver	PlatformBmc	JedecNVDimmSMM
StaticSkuDataDxeNeonCityEPRP	IioCfjUpdateDxeNeonCityFPGA	IioSmm	UefiPxeBcDxe	GenericFru	BreakpointCallbackDxe	SerialOverLan
SetupConfigUpdateDxeNeonCityEPRP	SlotDataUpdateDxeNeonCityFPGA	LpcPlatform	IScsiDxe	AtaBusDxe	UefiOptimizedBootDxe	AlertStandardFormatDxe
OpromUpdateDxeNeonCityEPRP	StaticSkuDataDxeBlueMountainPass	PciTVPcB374	IpxDxe	AtaAtapiPassThruDxe	RtkUsbUhdOptimizeLoad	ActiveManagement
SmbiosDataUpdateDxeNeonCityEPRP	SetupConfigUpdateDxeBlueMountainPass	ReserveMem	TcpDxe	IntelRaIdAtaAtapiPassThru	UbaSetupUpdateDxe	MeFwDowngrade
Usb0cUpdateDxeNeonCityEPRP	OpromUpdateDxeBlueMountainPass	FwBkocService	Udp6Dxe	IntelRaIdBiosThunk	GenerationSetup	BiosExtensionsLoader
SlotDataUpdateDxeNeonCityEPRP	SmbiosDataUpdateDxeBlueMountainPass	FwBkocServiceSmm	Dhcp6Dxe	IncompatiblePciDeviceSupport	HeciInitDxe	AmtWrapperDxe
Usb0cUpdateDxeNeonCityEPRP	Usb0cUpdateDxeBlueMountainPass	GraphicInterruptHookDxe	Mftfp6Dxe	IsaBusDxe	HeciIoInitDxe	AmtTable
IioCfjUpdateDxeNeonCityEPRP	IioCfjUpdateDxeBlueMountainPass	LegacyBiosReverseThunk	Httpp6Dxe	IsaSerialDxe	MePolicyInitDxe	AmtPetAlert
StaticSkuDataDxeOpalCitySTHI	SlotDataUpdateDxeBlueMountainPass	TcgLegacy	HttppBootDxe	IsaFloppyDxe	Platform	AmtPetAlert
SetupConfigUpdateDxeOpalCitySTHI	PchUsb2EyeDiagramDxeBlueMountainPass	TcgLegacyInstallInitia	HttptUtilitiesDxe	LegacyBiosDxe	SmbiosMisc	AmtInt16_csm
OpromUpdateDxeOpalCitySTHI	SsidSvidDataUpdateDxeBlueMountainPass	SmmFailTolerantWriteDxe	DnsDxe	IBMCVidDxe	SmbiosIFWI	MeSmbios
SmbiosDataUpdateDxeOpalCitySTHI	PchHsioCTLEDxeBlueMountainPass	VariableSmm	AcpiTableDxe	SycfgSyncDxe	ReaBmcCommands	Mebx
Usb0cUpdateDxeOpalCitySTHI	SystemBoardDxe	SmiVariableInt15	BlockIoDxe	PciPlatform	ReaInit	MebxSetupBrowser
IioCfjUpdateDxeOpalCitySTHI	PlatformType	SmiVariableInstallInt15Dxe	SnpInp16	LegacyBiosPlatform	BmcSmbiosDxe	IcPlatform
SlotDataUpdateDxeOpalCitySTHI	IioAspmWA	MonotonicCounterRuntimeDxe	BiosVideoDxe	MEPOLICY	SmbiosItkUpdateDxe	IcOverClocking
SsidSvidDataUpdateDxeOpalCitySTHI	UuidDxe	BdsDxe	CopPlatformDxe	FpgaDxe	FpgaDxe	SpsAcpiHooks
StaticSkuDataDxeWolfPass	SpdRawData	SecurityStubDxe	CopSplitterDxe	FpgaSmm	BmcAcpiDxe	SpsDxe
SetupConfigUpdateDxeWolfPass	SyncSetupVariableToPcd	JpegDecoderDxe	GraphicsConsoleDxe	BmcAcpiDxe	AcpiVTD	Heci3Smm
OpromUpdateDxeWolfPass	PlatformStatusCodeHandlerDxe	OemBadgingDxe	TerminalDxe	AcpiVTD	GetCpuInfo	SpsSmm
SmbiosDataUpdateDxeWolfPass	PlatformStatusCodeHandlerSmm	CapsuleRuntimeDxe	VgaClassDxe	SystemStidSvidProgramDxe	HpWltSmm	Heci3Smm
Usb0cUpdateDxeWolfPass	SysconfigSysInfoHide	RandomPoweronRacks	DataHubStdErrDxe	RStesSATAEFI	PlatformCpuBoard	SocketSetup
IioCfjUpdateDxeWolfPass	PlatformVariableInitDxe	AcemErrorReport	DiskIoDxe	RStesSATAEFI	SvsSmmSupport	FpgaSocketSetup
SlotDataUpdateDxeWolfPass	CommonErrorGeneration	Mft10emActivation	DevicePathDxe	VMDVROC2	SvsSmmHandler	OpnPlatCfg
PchUsb2EyeDiagramDxeWolfPass	ErrorManagerSetup	TpmPlatformDxe	LegacyRegion2	VMDVROC1	CpuHotAdd	OPARPlatConfigSkt0
SsidSvidDataUpdateDxeWolfPass	PostErrorToSoc	CpPcbiosId	EbcDxe	HfIpcieGen3	KtiRas	OPARPlatConfigSkt1
FpkConfigUpdateDxeWolfPass	PlatformPassword	SetupBmcCfg	NullMemoryTestDxe	IBMCVidGop	CpuRas	OPARPlatConfig_IFP45b_H79275
DMIMarginUpdateDxeWolfPass	ShellPasswordDxe	ITK59	PchInitDxe	ASTVBIOS	IoRas	OPARPlatConfig_IFT45b_H79267_H79272
SwitchledWA	PowerOnPassword	EarlyBootTimeOut	PchSmbusDxe	AspedVideo	HpIOXAccess	LsiVtdSupport.inf
StaticSkuDataDxeBuchananPass	VariableSmmRuntimeDxe	BootOrderPolicyDxe	PchSmbusSmm	PartitionDxe	RasInit	LegacyFV/CSM_v74
SetupConfigUpdateDxeBuchananPass	SmiVariable	SmmNm1Button	LegacyInterrupt	PciBmsDxe	PolicySampleDriver	UsbRt
OpromUpdateDxeBuchananPass	NmiButton	NmiButton	SecurityInIESS	MemorySubClass	ImcErrorHandler	Uhd
SmbiosDataUpdateDxeBuchananPass	IpmiBootOrder	Smbios00bMdr1	SetupSmIDispatcher	SetupBrowser	ProcessorErrorHandler	KbcEmulSMM
Usb0cUpdateDxeBuchananPass	StartupMarketFileBootOrder	Smbios00bMdr2	PchInitSmm	FpkSetup	PcieErrorHandler	KbcEmulDxe
StaticBootOrder	StaticBootOrder	MemoryVariableDob	SmmControl	PlatformDevSUpdate	PartialMirrorHandler	UsbInt13
SlotDataUpdateDxeBuchananPass	NetworkBootApp	OemPostScreenDisplayDxe	SataController	DisplayEngine	EnhancedMcAErrorLog	AmLegacyBiosHook
RiserPcieBifurcationDxeBuchananPass	FrontPanelLockout	SoIStatusPlatform	PchSpiRuntime	SmbiosDxe	WheaErrorLogListener	LegacySreDir
PchUsb2EyeDiagramDxeBuchananPass	SataSgnio	ConsoleBdsUpdate	PchSpiSmm	SmbiosMeasurementDxe	PpV1ErrorLogListener	LegacyBridgeDxe
SsidSvidDataUpdateDxeBuchananPass	SmbiosPcTable	DualVideo	PchSerialGpio	EnglishDxe	WheaErrorInj2	ChlSpecific
FpkConfigUpdateDxeBuchananPass	SecureBootErrorHandlerDxe	PayloadBoot	SmartTimer	PlatformDrvOverrideDxe	RASMiscDriver	RASDxe
BdsUpdateHookBuchananPass	SecureBootProvisionDxe	UefiNetworkStackProtocolDxe	PchResetRuntime	NvmExpressDxe	McBankErrorInjection	UefiOptRomDispatchPolicy
StaticSkuDataDxeLightningRidgeEXRP	SecureBootSetup	UefiOpromSetup	WdtDxe	ESRTIISataEffi	QuiesceSupport	Y2KRollover
SetupConfigUpdateDxeLightningRidgeEXRP	SecureBootCtrlDxe	Enter	PlatformReset	Scsibus	IsPlatformSupportWhea	MEForceUpdateDxe
OpromUpdateDxeLightningRidgeEXRP	BiosGuardServices	BootManagerSetup	PowerButtonHandler	ScsiDisk	WheaErrorInj	SmiGraphicsOutput
SmbiosDataUpdateDxeLightningRidgeEXRP	MeSmmPlatformThunk	BootMantSetup	TcgMor	AcpiPlatform		
Usb0cUpdateDxeLightningRidgeEXRP	S3NvramSave	DriverHealthDxe	Tcg2Dxe	SmmAccess		
IioCfjUpdateDxeLightningRidgeEXRP	PlatformEarlyDxe	FDPUpdate	Tcg2Smm	PiSmmIpl		

DxeCore	SlotDataUpdateDxeLightningRidgeEXRP	CpuIoDxe	ItkLogoProcess	TcgDxe	PiSmmCore	WheaElog
FastVideoDxe	SsidSvidDataUpdateDxeLightningRidgeEXRP	CpuIo2Dxe	SmIFlashSigned	TcgSmm	SmmCommunicationBuffer	UncoreErrorLog
PcdDxe	StaticSkuDataDxeSawtoothPass	Hi11Database	SINIT	BmcAcpiSwChild	PiSmmCpuDxeSmm	PcieErrorLog
RegAccessDxe	SetupConfigUpdateDxeSawtoothPass	DataHubDxe	TxtDxe	PlatformPreVariableDxe	CpuIo2Smm	PvModule
RegAccessSMM	OpromUpdateDxeSawtoothPass	FrameworkHi11Alias	HeaderPlatformDxe	DFSDxe	BIOSGuard	KtiErrorRuntime
ReportStatusCodeRouterRuntimeDxe	SmbiosDataUpdateDxeSawtoothPass	Legacy8259	HsithVProviderDxe	BmcElog	Ps2KeyboardDxe	KtiErrorLogPost
StatusCodeHandlerRuntimeDxe	Usb0cUpdateDxeSawtoothPass	CpuArchDxe	PlatformErrorGeneration	PlatformErrorGeneration	Ps2MouseDxe	WheaPlatformBoot
ReportStatusCodeRouterSmm	IioCfUpdateDxeSawtoothPass	PlatformCpuPolicy	GenericElog	GenericElog	S3SaveStateDxe	WheaErrorLog
StatusCodeHandlerSmm	SlotDataUpdateDxeSawtoothPass	CpuMpDxe	SmbMoeDxe	AcpiS3SaveDxe	AcpiS3SaveDxe	LastBootErrorLog
DataHubStatusCodeHandlerDxe	SsidSvidDataUpdateDxeSawtoothPass	SMBIOSFilter	SmmGenericElog	BootGraphicsResourceTableDxe	BootGraphicsResourceTableDxe	McBankErrorInjection
StatusCodeRuntimeDxe	FpkConfigUpdateSawtoothPass	Metronome	IpmlRedirFlw	BootScriptExecutorDxe	SmmLockBox	CpuCsAccess
SectionExtractionDxe		WatchdogTimer	OsWdt	SmmLockBox	PiSmmCommunicationSmm	CpuCsAccessSMM
GenericIpmi		PcRtc	BmcVariableDriver	PiSmmCommunicationSmm	AcpiSmmPlatform	CrystalRidge
SmmGenericIpmi		RuntimeDxe	OmMeFwPatch	AcpiSmmPlatform	PciHotPlug	CrystalRidgeSMM
UbaConfigDatabaseDxe		PciHostBridge	SolStatus	PciHotPlug	PlatformBmc	JedecNvDimm
UbaInitDxe		PpmInitialize	FrBdDriver	PlatformBmc	BreakpointCallbackDxe	JedecNvDimmSMM
StaticSkuDataDxeNeonCityEPRP	IioCfUpdateDxeNeonCityFPGA	IioSmm	GenericFru	BreakpointCallbackDxe	UefiOptimizedBootDxe	SerialOverLan
SetupConfigUpdateDxeNeonCityEPRP	SlotDataUpdateDxeNeonCityFPGA	LpcPlatform	AtaBusDxe	UefiOptimizedBootDxe	RtkUsbUhdOptimizeLoad	AlertStandardFormatDxe
OpromUpdateDxeNeonCityEPRP	StaticSkuDataDxeBlueMountainPass	PilotVpC8374	AtaAtapiPassThruDxe	RtkUsbUhdOptimizeLoad	UbaSetupUpdateDxe	ActiveManagement
SmbiosDataUpdateDxeNeonCityEPRP	SetupConfigUpdateDxeBlueMountainPass	ReserveMem	IntelRaIdAtaAtapiPassThru	UbaSetupUpdateDxe	GenerationSetup	MeFwDowngrade
OpromUpdateDxeNeonCityEPRP	OpromUpdateDxeBlueMountainPass	FwBkLockService	IntelRaIdBiosThunk	GenerationSetup	HeciInitDxe	BiosExtensionsLoader
IioCfUpdateDxeNeonCityEPRP	SmbiosDataUpdateDxeBlueMountainPass	FwBkLockServiceSmm	IncompatiblePciDeviceSupport	HeciInitDxe	MePolicyInitDxe	AmtWrapperDxe
Usb0cUpdateDxeBlueMountainPass	LegacyInterruptHookDxe	LegacyInterruptHookDxe	IsaBusDxe	MePolicyInitDxe	Platform	AsfTable
SlotDataUpdateDxeBlueMountainPass	LegacyBiosReverseThunk	LegacyBiosReverseThunk	IsaSerialDxe	Platform	IsaFirmwareDxe	AmtPetAlert
IioCfUpdateDxeBlueMountainPass	TcgLegacy	TcgLegacy	IsaFirmwareDxe	Platform	LegacyBiosDxe	AmtInt16_csm
SsidSvidDataUpdateDxeOpalCitySTHI	SlotDataUpdateDxeBlueMountainPass	VariableSmm	IsaFirmwareDxe	SmbiosMisc	IBMCVideo	AmtInt16_csm
SetupConfigUpdateDxeOpalCitySTHI	SsidSvidDataUpdateDxeBlueMountainPass	SystemBoardDxe	IntelTolerantWriteDxe	SmbiosIFWI	SysCfgSyncDxe	MeSmbios
OpromUpdateDxeOpalCitySTHI	PchHsioCTLEDxeBlueMountainPass	SystemBoardDxe	VariableSmm	ReaBmcCommands	AcpiTableDxe	Mebx
SmbiosDataUpdateDxeOpalCitySTHI	SystemBoardDxe	SmiVariableInt15	AcpiTableDxe	ReaInit	BlockIoDxe	MebxSetupBrowser
Usb0cUpdateDxeOpalCitySTHI	PlatformType	SmiVariableInstallInt15Dxe	PciPlatform	ReaInit	BiosIoDxe	IcePlatform
IioCfUpdateDxeOpalCitySTHI	IioAspmWA	MonotonicCounterRuntimeDxe	LegacyBiosPlatform	BmcSmbiosDxe	MEPolicy	IcoOverClocking
SlotDataUpdateDxeOpalCitySTHI	UuidDxe	BsdDxe	NPVMDriver	SmbiosItkUpdateDxe	FpgaDxe	SpsAcpiHooks
SsidSvidDataUpdateDxeOpalCitySTHI	SpdRawData	SecurityStubDxe	NVMDMMHii	FpgaSmm	BmcAcpiDxe	SpsDxe
StaticSkuDataDxeWolfPass	SyncSetupVariableToPcd	JpegDecoderDxe	SATAAHCI	BmcAcpiDxe	AcpiVTD	HeciSmm
SetupConfigUpdateDxeWolfPass	PlatformStatusCodeHandlerDxe	OemBadgingDxe	RSTeSATALegacy	AcpiVTD	GetCpuInfo	Heci35smm
OpromUpdateDxeWolfPass	PlatformStatusCodeHandlerSmm	CapsuleRuntimeDxe	RSTeSATALegacy	SystemSsidSvidProgramDxe	HpWptSmm	IioInit
SmbiosDataUpdateDxeWolfPass	SysconfigSysInFOHide	RandomPoweronRacks	RSTeSATAEFI	HpWptSmm	PlatformCpuBoard	RosetTesting
Usb0cUpdateDxeWolfPass	PlatformVariableInitDxe	AcemReport	RSTeSATAEFI	PlatformCpuBoard	SvsSmmSupport	SocketSetup
IioCfUpdateDxeWolfPass	CommonErrorGeneration	Mft0emActivation	DevicePathDxe	SvsSmmSupport	SvsSmmHandler	FngaSocketSetup
SlotDataUpdateDxeWolfPass	ErrorManagerSetup	TpmPlatformDxe	VMDVR0C2	SvsSmmHandler	CpuHotAdd	OpnPlatCfg
PchUsb2EyeDiagramDxeWolfPass	PostErrorToSol	CpPcbiosId	VMDVR0C1	CpuHotAdd	KtiRas	OPARPlatConfigSkt0
SsidSvidDataUpdateDxeWolfPass	PlatformPassword	SetupBmcCfg	HfPcieGen3	KtiRas	CpuRas	OPARPlatConfigSkt1
FpkConfigUpdateDxeWolfPass	ShellPasswordDxe	ITK59	IBMCVideoGop	OPARPlatConfig_IFP45b_H79275	IOAs	OPARPlatConfig_IFT45b_H79267_H79272
DMIMarginUpdateDxeWolfPass	PowerOnPassword	EarlyBootTimeOut	PartitionDxe	OPARPlatConfig_IFT45b_H79267_H79272	HpIOXAccess	LsiVtdSupport.inf
SwitchedWA	VariableSmmRuntimeDxe	BootOrderPolicyDxe	PciBusDxe	LsiVtdSupport.inf	RasInit	LegacyFV/CSM_v74
StaticSkuDataDxeBuchananPass	SmiVariable	SmmNm1Button	MemorySubClass	RasInit	PolicySampleDriver	UsbRt
SetupConfigUpdateDxeBuchananPass	NmiButton	Smbios00bMdr1	SetupBrowser	IncErrorHandler	IncErrorHandler	Uhd
OpromUpdateDxeBuchananPass	MemoryMdr2	Smbios00bMdr2	FpkSetup	ProcessorErrorHandler	ProcessorErrorHandler	KbcEmulSMM
SmbiosDataUpdateDxeBuchananPass	PlatformDevSUpdate	MemoryMdringDob	PlatformDevSUpdate	PcieErrorHandler	PcieErrorHandler	KbcEmulDxe
Usb0cUpdateDxeBuchananPass	DisplayEngine	OemPostScreenDisplayDxe	DisplayEngine	PartialMirrorHandler	PartialMirrorHandler	UsbInt13
IioCfUpdateDxeBuchananPass	SmbiosDxe	SolStatusPlatform	SmbiosDxe	EnhancedMcAErrorLog	EnhancedMcAErrorLog	AmLegacyBiosHook
SlotDataUpdateDxeBuchananPass	SmbiosMeasurementDxe	ConsoleBdsUpdate	SmbiosMeasurementDxe	WheaErrorLogListener	WheaErrorLogListener	LegacySredir
RiserPcieBifurcationDxeBuchananPass	EnglishDxe	DualVideo	PlatformOverrideDxe	PpV1ErrorLogListener	PpV1ErrorLogListener	LegacyBridgeDxe
PchUsb2EyeDiagramDxeBuchananPass	PlayloadBoot	SecureBootErrorHandlerDxe	NvmExpressDxe	WheaErrorInj2	WheaErrorInj2	ChlSpecific
SsidSvidDataUpdateDxeBuchananPass	UefiNetworkStackProtocolDxe	SecureBootProvisionDxe	ESRTIISataEffi	RASMiscDriver	RASMiscDriver	RASDxe
FpkConfigUpdateDxeBuchananPass	UefiPromSetup	SecureBootSetup	ScsiBus	McBankErrorInjection	McBankErrorInjection	UefiOptRomDispatchPolicy
BdsUpdateHookBuchananPass	Enter	SecureBootCtrlDxe	ScsiDisk	QuiesceSupport	QuiesceSupport	Y2KRollover
StaticSkuDataDxeLightningRidgeEXRP	BootManagerSetup	SecureBootCtrlDxe	AcpiPlatform	IsPlatformSupportWhea	IsPlatformSupportWhea	MEForceUpdateDxe
SetupConfigUpdateDxeLightningRidgeEXRP	BootManagerSetup	BiosGuardServices	SmmAccess	WheaSupport	WheaSupport	SmiGraphicsOutput
OpromUpdateDxeLightningRidgeEXRP	BootManagerSetup	SmbiosDataUpdateDxeLightningRidgeEXRP	PiSmmInpl	WheaErrorInj	WheaErrorInj	
SmbiosDataUpdateDxeLightningRidgeEXRP	DriverHealthDxe	MeSmmPlatformThunk	S5SmmInpl			
Usb0cUpdateDxeLightningRidgeEXRP	FDPUpdate	S3NvramSave	PiSmmInpl			
IioCfUpdateDxeLightningRidgeEXRP		PlatformEarlyDxe				

UefiOpromSetup

DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DataHubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDxe
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDxe
UbaInitDxe
StaticSkuDataDxeNeonCityEPPR
SetupConfigUpdateDxeNeonCityEPPR
OprumUpdateDxeNeonCityEPPR
SmbiosDataUpdateDxeNeonCityEPPR
UbsocUpdateDxeNeonCityEPPR
TioCfgUpdateDxeNeonCityEPPR
SlotDataUpdateDxeNeonCityEPPR
SsidSvidDataUpdateDxeNeonCityEPPR
StaticSkuDataDxeOpalCitySTH
SetupConfigUpdateDxeOpalCitySTH
OprumUpdateDxeOpalCitySTH
SmbiosDataUpdateDxeOpalCitySTH
UbsocUpdateDxeOpalCitySTH
TioCfgUpdateDxeOpalCitySTH
SlotDataUpdateDxeOpalCitySTH
SsidSvidDataUpdateDxeOpalCitySTH
StaticSkuDataDxeWolfPass
SetupConfigUpdateDxeWolfPass
OprumUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
UbsocUpdateDxeWolfPass
TioCfgUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateDxeWolfPass
DMIMarginUpdateDxeWolfPass
SwitchLedWA
StaticSkuDataDxeBuchananPass
SetupConfigUpdateDxeBuchananPass
OprumUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
UbsocUpdateDxeBuchananPass
TioCfgUpdateDxeBuchananPass
SlotDataUpdateDxeBuchananPass
RiserPCIeBifurcationDxeBuchananPass
PchUsb2EyeDiagramDxeBuchananPass
SsidSvidDataUpdateDxeBuchananPass
FpkConfigUpdateDxeBuchananPass
BdsUpdateHookBuchananPass
StaticSkuDataDxeLightningRidgeEXRP
SetupConfigUpdateDxeLightningRidgeEXRP
OprumUpdateDxeLightningRidgeEXRP
SmbiosDataUpdateDxeLightningRidgeEXRP
UbsocUpdateDxeLightningRidgeEXRP
TioCfgUpdateDxeLightningRidgeEXRP

SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OprumUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
UbsocUpdateDxeSawtoothPass
TioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass
TioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass
ReserveMem
CkService
CkServiceSmm
InterruptHookDxe
VbiosReverseThunk
Gacy
GacyInstallInt1A
IoTolerantWriteDxe
IoSmm
FirmwareInt15
FirmwareInstallInt15Dxe
MonotonicCounterRuntimeDxe
BdsDxe
SpdRawData
SyncSetupVariableToPcd
PlatformStatusCodeHandlerDxe
PlatformStatusCodeHandlerSmm
SysconfigSysInfoHide
PlatformVariableInitDxe
CommonErrorGeneration
ErrorManagerSetup
PostErrorToSoc
PlatformPassword
ShellPasswordDxe
PowerOnPassword
VariableSmmRuntimeDxe
SmiVariable
NmiButton
Smbios00bMdr1
Smbios00bMdr2
MemoryMappingDob
OemPostScreenDisplayDxe
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootMmSetup
DriverHealthDxe
FirmwareUpdate

CpuIoDxe
CpuIo2Dxe
Hi11Database
DataHubDxe
FrameworkHiiAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuPnpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IoSmm
LpcPlatform
PilotVPC8374
ReservedMem
CkService
CkServiceSmm
InterruptHookDxe
VbiosReverseThunk
Gacy
GacyInstallInt1A
IoTolerantWriteDxe
IoSmm
FirmwareInt15
FirmwareInstallInt15Dxe
MonotonicCounterRuntimeDxe
BdsDxe
SpdRawData
SyncSetupVariableToPcd
PlatformStatusCodeHandlerDxe
PlatformStatusCodeHandlerSmm
SysconfigSysInfoHide
PlatformVariableInitDxe
CommonErrorGeneration
ErrorManagerSetup
PostErrorToSoc
PlatformPassword
ShellPasswordDxe
PowerOnPassword
VariableSmmRuntimeDxe
SmiVariable
NmiButton
Smbios00bMdr1
Smbios00bMdr2
MemoryMappingDob
OemPostScreenDisplayDxe
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootMmSetup
DriverHealthDxe
FirmwareUpdate

ItkLogoProcess
SmiFlashSigned
SINIT
TxtDxe
Hs12PlatformDxe
Legacy8259
SnpDxe
DnpDxe
MnpDxe
VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mftfp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TdpDxe
Udp6Dxe
Dhcp6Dxe
Mftfp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
AcpiTableDxe
BlockIoDxe
NvMmSnp16
BiosVideoDxe
ConPlatformDxe
ConSplitterDxe
GraphicsConsoleDxe
TerminalDxe
VgaClassDxe
DataHubStdErrDxe
DiskIoDxe
DevicePathDxe
LegacyRegion2
VMDVROC2
EbcDxe
NullMemoryTestDxe
PchInitDxe
PchSmbusDxe
PchSmbusSmm
LegacyInterrupt
SecurityInIESS
SetupBrowser
FpkSetup
PlatformDevSUpdate
DisplayEngine
SmbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatformOverrideDxe
NvmExpressDxe
ESRTIISataFfi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PisMmIpl

PisMmCore
SmmCommunicationBuffer
PisMmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
S3SaveStateDxe
AcpiS3SaveDxe
BootGraphicsResourceTableDxe
BootScriptExecutorDxe
SmmLockBox
PisMmCommunicationSmm
AcpiSmmPlatform
PciHotPlug
PlatformBmc
BreakpointCallbackDxe
UefiOptimizedBootDxe
RtkUbsbndOptimizeLoad
UbaSetupUpdateDxe
GenerationSetup
HeciInitDxe
MePolicyInitDxe
IoPolicyInitDxe
Platform
SmbiosMisc
SmbiosIFWI
ReaBmcCommands
ReaInit
BmcSmbiosDxe
SmbiosItkUpdateDxe
FpgaDxe
FpgaSmm
BmcAcpiDxe
AcpiVTD
GetCpuInfo
SystemSsidSvidProgramDxe
HwPvtSmm
PlatformCpuBoard
SvSmmSupport
SvSmmHandler
CpuHotAdd
KtiRas
CpuRas
IoRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcErrorHandler
WheaErrorLogListener
PpV1ErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiesceSupport
IsPlatformSupportWhea
WheaSupport
WheaErrorInj

WheaElog
UncoreErrorLog
PcieErrorLog
PvMode
KtiErrorLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog
LastBootErrorLog
McBankErrorInjection
CpuCsAccess
CpuCsAccessSMM
CrystalRidge
CrystalRidgeSMM
JedecNvdImm
JedecNvdImmSMM
SerialOverLan
AlertStandardFormatDxe
ActiveManagement
MeFwDowngrade
NvMmExtensionLoader
AmtWrapperDxe
AsfTable
AmtPetAlert
AmtInt16
AmtInt16_csm
MeSmbios
Mebx
MebxSetupBrowser
IcePlatform
IceOverClocking
SpsAcpiHooks
SpsDxe
SpsSmm
Heci35mm
SpsSmm
Heci35mm
IoInit
ResetTesting
SocketSetup
FpgaSocketSetup
OpaPlatCfg
OPAPlatConfigSkt0
OPAPlatConfigSkt1
OPAPlatConfig_IPF45b_H79275
OPAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySreDir
LegacyBridgeDxe
ChlSpecific
RASDxe
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput

UefiOpromSetup

OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess

DxeCore	SlotDataUpdateDxeLightningRidgeEXRP	CpuIoDxe	ItkLogoProcess	TcgDxe	PiSmmCore	WheaElog
FastVideoDxe	SsidSvidDataUpdateDxeLightningRidgeEXRP	CpuIo2Dxe	SmIFlashSigned	TcgSmm	SmmCommunicationBuffer	UncoreErrorLog
PcdDxe	StaticSkuDataDxeSawtoothPass	HiiDatabase	SINIT	BmcAcpiSwChild	PiSmmCpuDxeSmm	PcieErrorLog
RegAccessDxe	SetupConfigUpdateDxeSawtoothPass	DataHubDxe	TxtDxe	PlatformPreVariableDxe	CpuIo2Smm	PvMode
RegAccessSMM	OpromUpdateDxeSawtoothPass	FrameworkHiiAlias	HeaderPlatformDxe	DFSDxe	BIOSGuard	KtiErrorLogRuntime
ReportStatusCodeRouterRuntimeDxe	SmbiosDataUpdateDxeSawtoothPass	Legacy8259	HeaderIthvProviderDxe	BmcElog	Ps2KeyboardDxe	KtiErrorLogPost
StatusCodeHandlerRuntimeDxe	Usb0cUpdateDxeSawtoothPass	CpuArchDxe	SndDxe	PlatformErrorGeneration	Ps2MouseDxe	WheaPlatformBoot
ReportStatusCodeRouterSmm	IioCfgUpdateDxeSawtoothPass	PlatformCpuPolicy	DnpDxe	GenericElog	S3SaveStateDxe	WheaErrorLog
StatusCodeHandlerSmm	SlotDataUpdateDxeSawtoothPass	CpuPmpDxe	MnpDxe	SmbMmcElog	AcpiS3SaveDxe	LastBootErrorLog
DataHubStatusCodeHandlerDxe	SsidSvidDataUpdateDxeSawtoothPass	SMBIOSFilter	VlanConfigDxe	SmmGenericElog	BootGraphicsResourceTableDxe	McBankErrorInjection
StatusCodeRuntimeDxe	FpkConfigUpdateSawtoothPass	Metronome	ArpDxe	IpmiRedirFlw	BootScriptExecutorDxe	CpuCsrAccess
SectionExtractionDxe		WatchdogTimer	Dhcp4Dxe	OsWdt	SmmLockBox	CpuCsrAccessSMM
GenericIpmi		PcRtc	Ip4Dxe	BmcVariableDriver	PiSmmCommunicationSmm	CrystalRidge
SmmGenericIpmi		RuntimeDxe	Mftfp4Dxe	OemMefwPatch	AcpiSmmPlatform	CrystalRidgeSMM
UbaConfigDatabaseDxe		PciHostBridge	Udp4Dxe	SoLStatus	PciHotPlug	JedecNvDimm
UbaInitDxe		PpmInitialize	Tcp4Dxe	FrBdDriver	PlatformBmc	JedecNvDimmSMM
StaticSkuDataDxeNeonCityEPRP	IioCfgUpdateDxeNeonCityFPGA	IioSmm	UefiPxeBcDxe	GenericFru	BreakpointCallbackDxe	SerialOverLan
SetupConfigUpdateDxeNeonCityEPRP	SlotDataUpdateDxeNeonCityFPGA	LpcPlatform	IScSI0Dxe	AtaBusDxe	UefiOptimizedBootDxe	AlertStandardFormatDxe
OpromUpdateDxeNeonCityEPRP	StaticSkuDataDxeBlueMountainPass	PilotVPC8374	Ip6Dxe	AtaAtapiPassThruDxe	RtkUsbUhdOptimizeLoad	ActiveManagement
SmbiosDataUpdateDxeNeonCityEPRP	SetupConfigUpdateDxeBlueMountainPass	ReservedMem	TcpDxe	IntelRaIdAtaAtapiPassThru	UbaSetupUpdateDxe	MeFwDowngrade
Usb0cUpdateDxeNeonCityEPRP		CsService	Udp6Dxe	IntelRaIdBiosThunk	GenerationSetup	NonExtraneousLoader
IioCfgUpdateDxeNeonCityEPRP		CsServiceSmm	Dhcp6Dxe	IncompatiblePciDeviceSupport	HeciInitDxe	AmtWrapperDxe
SlotDataUpdateDxeNeonCityEPRP		InterruptHookDxe	Mftfp6Dxe	IsaBusDxe	MePolicyInitDxe	AsiTable
SsidSvidDataUpdateDxeNeonCityEPRP		VBiosReverseThunk	HttpDxe	IsaSerialDxe	IoPolicyInitDxe	AmtPetAlert
StaticSkuDataDxeOpalCitySTH1		Gacy	HttpBootDxe	IsaLoppyDxe	Platform	AmtInt16
SetupConfigUpdateDxeOpalCitySTH1		GacyInstallInt1A	HttpUtilitiesDxe	LegacyBiosDxe	SmbiosMisc	AmtInt16_csm
OpromUpdateDxeOpalCitySTH1		tolerantWriteDxe	DnsDxe	IBMCVideo	SmbiosIFWI	MeSmbios
SmbiosDataUpdateDxeOpalCitySTH1		IoSmm	AcpiTableDxe	SysCfgSyncDxe	ReaBmcCommands	Mebx
Usb0cUpdateDxeOpalCitySTH1		VariableInt15	BlockIoDxe	PciPlatform	ReaInit	MebxSetupBrowser
StaticSkuDataDxeOpalCitySTH1		VariableInstallInt15Dxe	BlockSnp16	LegacyBiosPlatform	BmcSmbiosDxe	IcePlatform
SlotDataUpdateDxeOpalCitySTH1		MonotonicCounterRuntimeDxe	BiosVideoDxe	MEPolicy	SmbiosItkUpdateDxe	IcOverClocking
SsidSvidDataUpdateDxeOpalCitySTH1		BdsDxe	ConPlatformDxe	NVMMIOmDriver	FpgaDxe	SpsAcpiHooks
StaticSkuDataDxeWolfPass		SecurityStubDxe	ConSplitterDxe	NVMMIOmHii	FpgaSmm	SpsDxe
SetupConfigUpdateDxeWolfPass		JpegDecoderDxe	GraphicsConsoleDxe	SATAAHCI	BmcAcpiDxe	HeciSmm
OpromUpdateDxeWolfPass		OemBadgingDxe	TerminalDxe	RSTeSATALegacy	AcpiVTD	SpsSmm
SmbiosDataUpdateDxeWolfPass		CapsuleRuntimeDxe	VgaClassDxe	RSTesSATALegacy	GetCpuInfo	Heci35smm
Usb0cUpdateDxeWolfPass		RandomPoweronRacks	DataHubStdErrDxe	RSTeSATAEFI	SystemStdSvidProgramDxe	IoInit
IioCfgUpdateDxeWolfPass		AcromReport	DiskIoDxe	RSTesSATAEFI	HwPvtSmm	RasetTesting
SlotDataUpdateDxeWolfPass		MsfOemActivation	DevicePathDxe	VMDVROC2	PlatformCpuBoard	SocketSetup
PchUsb2EyeDiagramDxeWolfPass		TpmPlatformDxe	LegacyRegion2	VMDVROC1	SvsSmmSupport	FpgaSocketSetup
SsidSvidDataUpdateDxeWolfPass		CpCebiosId	EbcDxe	NullMemoryTestDxe	SvsSmmHandler	OpaPlatCfg
FpkConfigUpdateDxeWolfPass		PlatformBmcCfg	NullMemoryTestDxe	PchInitDxe	CpuHotAdd	OPAPlatConfigSkt0
DMIMarginUpdateDxeWolfPass		BootTimeOut	PchSmbusDxe	PchSmbusSmm	KtiRas	OPAPlatConfigSkt1
SwitchLedWA		OrderPolicyDxe	PchSmbusSmm	AspedVideo	CpuRas	OPAPlatConfig_IFP45b_H79275
StaticSkuDataDxeBuc		SmmButton	PartitionDxe	PartitionDxe	IoRas	OPAPlatConfig_IFT45b_H79267_H79272
SetupConfigUpdateDxeBuchananPass		NmiButton	LegacyInterrupt	PciBusDxe	HpIOXAccess	LsiVtdSupport.inf
OpromUpdateDxeBuchananPass		Smbios00bMdr1	SecurityIntEISS	MemorySubClass	RasInit	LegacyFV/CSM_v74
SmbiosDataUpdateDxeBuchananPass		Smbios00bMdr2	SetupBrowser	SetupBrowser	PolicySampleDriver	UsbRt
Usb0cUpdateDxeBuchananPass		MemoryMappingDob	FpkSetup	FpkSetup	IncErrorHandler	Uhd
StaticBootOrder		OemPostScreenDisplayDxe	PlatformDevSUpdate	PlatformDevSUpdate	ProcessorErrorHandler	KbcEmulSMM
StartupMarkerFileBootOrder		SoLStatusPlatform	DisplayEngine	DisplayEngine	PcieErrorHandler	KbcEmulDxe
StaticBootOrder		ConsoleBdsUpdate	SmbiosDxe	SmbiosDxe	PartialMirrorHandler	UsbInt13
NetworkBootApp		DualVideo	SmbiosMeasurementDxe	SmbiosMeasurementDxe	EnhancedMcErrorHandler	AmiLegacyBiosHook
RiserPCIEBifurcationDxeBuchananPass		SecureBootErrorHandlerDxe	EnglishDxe	EnglishDxe	WheaErrorLogListener	LegacySredir
FrontPanelLockout		SecureBootProvisionDxe	PlatformOverrideDxe	PlatformOverrideDxe	PpV1ErrorLogListener	LegacyBridgeDxe
SataSgpio		SecureBootSetup	UefiNetworkStackProtocolDxe	UefiNetworkStackProtocolDxe	WheaErrorInj2	ChlSpecific
PchUsb2EyeDiagramDxeBuchananPass		SecureBootCtrlDxe	UefiPromSetup	UefiPromSetup	RASMiscDriver	RASDxe
SsidSvidDataUpdateDxeBuchananPass		SecureBootSetup	Enter	Enter	McBankErrorInjection	UefiOptNonRomDispatchPolicy
FpkConfigUpdateDxeBuchananPass		BiosGuardServices	BootManagerSetup	BootManagerSetup	QuiesceSupport	Y2KRollover
BdsUpdateHookBuchananPass		MeSmmPlatformThunk	BootManagerSetup	BootManagerSetup	IsPlatformSupportWhea	MEForceUpdateDxe
StaticSkuDataDxeLightningRidgeEXRP		S3NvramSave	DriverHealthDxe	DriverHealthDxe	WheaSupport	SmiGraphicsOutput
SetupConfigUpdateDxeLightningRidgeEXRP		PlatformEarlyDxe	FdUpdate	FdUpdate	WheaErrorInj	

UefiOpromSetup

OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess

MsftOemActivation

DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DataHubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDxe
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDxe
UbaInitDxe

SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
UsbOciUpdateDxeSawtoothPass
IioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass

CpuIoDxe
CpuIo2Dxe
HiIoDatabase
DataHubDxe
FrameworkHiIoAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpdxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotVPC8374
ReservedMem

TtkLogoProcess
TcgDxe
ISmm
AcpiSwChild
IstfomPreVariableDxe
SDxe
ELog
IstfomErrorGeneration
MetricELog
FmcELog
IreneELog
RedirFlu
Icdt
VariableDriver
IMEFWPatch
Status
IDriver
MetricFlu
Icdt
VariableDriver
IMEFWPatch
Status
IDriver
MetricFlu
Icdt

PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
P2KeyboardDxe
P2MouseDxe
S3SaveStateDxe
AcpiS3SaveDxe
BootGraphicsResourceTableDxe
BootScriptExecutorDxe
SmmLockBox
PiSmmCommunicationSmm
AcpiSmmPlatform
PciHotPlug
PlatformBmc
BreakpointCallbackDxe
UefiOptimizedBootDxe
RtkUsbUmdOptimizeLoad
UbaSetupUpdateDxe
GenerationSetup
HeciInitDxe
MePolicyInitDxe
IoPolicyInitDxe
Platform
SmbiosMisc
SmbiosIFWI
ResBmcCommands
ReaInit
BmcSmbiosDxe
SmbiosItkUpdateDxe
Policy
FpgaDxe
FpgaSmm
BmcAcpiDxe
AcpiVTD
GetCpuInfo
SystemSsidSvidProgramDxe
HwptLstSmm
PlatformCpuBoard
SvSmmSupport
SvSmmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcErrorHandler
WheaErrorLogListener
PpV1ErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiesceSupport
ISPlatformSupportWhea
WheaSupport
WheaErrorInj

WheaElog
UncoreErrorLog
PcieErrorLog
PvMode
KtiErrorLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog
LastBootErrorLog
McBankErrorInjection
CpuCsrAccess
CpuCsrAccessSMM
CrystalRidge
CrystalRidgeSMM
JedecNvDimm
JedecNvDimmSMM
SerialOverLan
AlertStandardFormatDxe
ActiveManagement
MeFWDowngrade
MeFWExtensionLoader
AmtWrapperDxe
AsiTable
AmtPetAlert
AmtInt16
AmtInt16_csm
MeSmbios
Mebx
MebxSetupBrowser
IcePlatform
IceOverClocking
SpsAcpiHooks
SpsDxe
HeciSmm
SpsSmm
Heci35smm
IioInit
ResetTesting
SocketSetup
FpgaSocketSetup
OpaPlatCfg
OPAPlatConfigSkt0
OPAPlatConfigSkt1
OPAPlatConfig_IFP45b_H79275
OPAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhdcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySreDir
LegacyBridgeDxe
ChlSpecific
RASDxe
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput

UefiOpromSetup

IioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass

OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess

MsftOemActivation

IioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass

ReserveMem
CkService
CkServiceSmm
InterruptHookD
VbiosReverseThu
gacy
gacyInstallInt1
IltolerantWrit
IoSmm
IableInt15
IableInstallIn
MonotonicCounterRunt
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcemErrorReport
MsfOemActivation
TpmPlatformDxe
CpPcbiosId
SetupBmcCfg

VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mftftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mftftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe

BootTimeOut
OrderPolicyDxe
SmmInitButton
NmiButton
Smbios00bMdr1
Smbios00bMdr2
MemoryMappingDob
OemPostScreenDisplay
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootManagerSetup
DriverHealthDxe
FdUpdate

CompatiblePciDeviceSupport
BusDxe
SerialDxe
IFlopDxe
gacyBiosDxe
ICVidee
IcfsgSyncDxe
Platform
FacyBiosPlatform
Policy
IDIMMDriver
IDIMMhii
FAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
SvSmmSupport
SvSmmHandler
CpuHotAdd
VBIOS
eedVideo
ctitionDxe
BusDxe
norySubClass
upBrowser
ISetup
IstfomDevSUpdate
IstfomEngine
IioSdx
SmbiosMeasurementDxe
EnglishDxe
PldtDrvOverrideDxe
NvmExpressDxe
ESRTIISataEffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

Platform
FacyBiosPlatform
Policy
IDIMMDriver
IDIMMhii
FAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
SvSmmSupport
SvSmmHandler
CpuHotAdd
VBIOS
eedVideo
ctitionDxe
BusDxe
norySubClass
upBrowser
ISetup
IstfomDevSUpdate
IstfomEngine
IioSdx
SmbiosMeasurementDxe
EnglishDxe
PldtDrvOverrideDxe
NvmExpressDxe
ESRTIISataEffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

Platform
FacyBiosPlatform
Policy
IDIMMDriver
IDIMMhii
FAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
SvSmmSupport
SvSmmHandler
CpuHotAdd
VBIOS
eedVideo
ctitionDxe
BusDxe
norySubClass
upBrowser
ISetup
IstfomDevSUpdate
IstfomEngine
IioSdx
SmbiosMeasurementDxe
EnglishDxe
PldtDrvOverrideDxe
NvmExpressDxe
ESRTIISataEffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

Platform
FacyBiosPlatform
Policy
IDIMMDriver
IDIMMhii
FAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
SvSmmSupport
SvSmmHandler
CpuHotAdd
VBIOS
eedVideo
ctitionDxe
BusDxe
norySubClass
upBrowser
ISetup
IstfomDevSUpdate
IstfomEngine
IioSdx
SmbiosMeasurementDxe
EnglishDxe
PldtDrvOverrideDxe
NvmExpressDxe
ESRTIISataEffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

Platform
FacyBiosPlatform
Policy
IDIMMDriver
IDIMMhii
FAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
SvSmmSupport
SvSmmHandler
CpuHotAdd
VBIOS
eedVideo
ctitionDxe
BusDxe
norySubClass
upBrowser
ISetup
IstfomDevSUpdate
IstfomEngine
IioSdx
SmbiosMeasurementDxe
EnglishDxe
PldtDrvOverrideDxe
NvmExpressDxe
ESRTIISataEffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

Platform
FacyBiosPlatform
Policy
IDIMMDriver
IDIMMhii
FAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
SvSmmSupport
SvSmmHandler
CpuHotAdd
VBIOS
eedVideo
ctitionDxe
BusDxe
norySubClass
upBrowser
ISetup
IstfomDevSUpdate
IstfomEngine
IioSdx
SmbiosMeasurementDxe
EnglishDxe
PldtDrvOverrideDxe
NvmExpressDxe
ESRTIISataEffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DataHubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDxe
GenericIpmi
SmmGenericIpmi
UbaConfigDatabaseDxe
UbaInitDxe
StaticSkuDataDxeNeonCityEPRP
SetupConfigUpdateDxeNeonCityEPRP
OpromUpdateDxeNeonCityEPRP
SmbiosDataUpdateDxeNeonCityEPRP
Ubs0cUpdateDxeNeonCityEPRP
TioCfgUpdateDxeNeonCityEPRP
SlotDataUpdateDxeNeonCityEPRP
SsidSvidDataUpdateDxeOpalCitySTHI
SetupConfigUpdateDxeOpalCitySTHI
OpromUpdateDxeOpalCitySTHI
SmbiosDataUpdateDxeOpalCitySTHI
Ubs0cUpdateDxeOpalCitySTHI
TioCfgUpdateDxeOpalCitySTHI
SlotDataUpdateDxeOpalCitySTHI
SsidSvidDataUpdateDxeOpalCitySTHI
StaticSkuDataDxeWolfPass
SetupConfigUpdateDxeWolfPass
OpromUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
Ubs0cUpdateDxeWolfPass
TioCfgUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateDxeWolfPass
DMIMarginUpdateDxeWolfPass
SwitchedWA
StaticSkuDataDxeBuchananPass
SetupConfigUpdateDxeBuchananPass
OpromUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
Ubs0cUpdateDxeBuchananPass
StaticBootOrder
StartupMarkerFileBootOrder
StaticBootOrder
NetworkBootApp
RiserPCIeBifurcationDxeBuchananPass
FrontPanelLockout
SataSgpio
PchUsb2EyeDiagramDxeBuchananPass
SsidSvidDataUpdateDxeBuchananPass
FpkConfigUpdateDxeBuchananPass
BdsUpdateHookBuchananPass
StaticSkuDataDxeLightningRidgeEXRP
SetupConfigUpdateDxeLightningRidgeEXRP
OpromUpdateDxeLightningRidgeEXRP
SmbiosDataUpdateDxeLightningRidgeEXRP
Ubs0cUpdateDxeLightningRidgeEXRP
TioCfgUpdateDxeLightningRidgeEXRP

UefiOpromSetup

OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess

MsftOemActivation

SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
Ubs0cUpdateDxeSawtoothPass
TioCfgUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass
TioCfgUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass
ReserveMem
CkService
CkServiceSmm
InterruptHookDxe
VbiosReverseThrottle
GacyInstallInt15
TolerantWriteSmm
VariableInt15
VariableInstallIn
MonotonicCounterRunt
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcpiErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupSmcCfg
BootTimeout
OrderPolicyDxe
SmmInitButton
NmiButton
Smbios00bMdr1
Smbios00bMdr2
MemoryMappingDob
OemPostScreenDisplay
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootManagerSetup
MeSmmPlatformThunk
S3NvramSave
PlatformEarlyDxe

CpuIoDxe
CpuIo2Dxe
HiDatabase
DataHubDxe
FrameworkHiiAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotVPC8374
ReserveMem
CkService
CkServiceSmm
InterruptHookDxe
VbiosReverseThrottle
GacyInstallInt15
TolerantWriteSmm
VariableInt15
VariableInstallIn
MonotonicCounterRunt
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcpiErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupSmcCfg
BootTimeout
OrderPolicyDxe
SmmInitButton
NmiButton
Smbios00bMdr1
Smbios00bMdr2
MemoryMappingDob
OemPostScreenDisplay
SolStatusPlatform
ConsoleBdsUpdate
DualVideo
PayloadBoot
UefiNetworkStackProtocolDxe
UefiOpromSetup
Enter
BootManagerSetup
BootManagerSetup
MeSmmPlatformThunk
S3NvramSave
PlatformEarlyDxe

VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mtftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mtftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe
PchSpiSmm
PchSerialGpio
SmartTimer
PchResetRuntime
WdtDxe
PlatformReset
PowerButtonHandler
TcgMor
Tcg2Dxe
Tcg2Smm

TtkLogoProcess
TcgDxe
Smm
AcpiSwChild
IstfomPreVariableDxe
Sdxe
Elog
IstfomErrorGeneration
MericElog
MmcDxe
MericElog
IRedirFru
Idt
VariableDrive
IMEFWPatch
Status
IDriver
MericFru
IBusDxe
IAtapIPassThru
IraidAtaAtapi
IraidBiosThru
CompatiblePciDxe
IBusDxe
SerialDxe
IFloppyDxe
IacyBiosDxe
ICVideDxe
IcfSyncDxe
Platform
IacyBiosPlatform
Policy
IDMMDriver
IDMMHii
IAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
IVROC1
PciGen3
ICVideoGop
VBIOs
CpuRas
eedVideo
ctitionDxe
BusDxe
IorySubClass
UpBrowser
Setup
IstfomDevSUpdate
IstfomEngine
IbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatformOverrideDxe
NvmExpressDxe
ESRTIISataffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
WheaElog
UncoreErrorLog
PcieErrorLog
PvModule
KtiErrorRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorInj
IsaBusDxe
IsaFloppyDxe
IsaSerialDxe
LegacyRegion2
LegacyBiosPlatform
Legacy8259
LegacyInterrupt
LegacyInterruptHookDxe
LegacyBiosDxe
SvsMmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcaErrorLog
WheaErrorLogListener
Ppv1ErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInjection
QuiesceSupport
IsPlatformSupportWhea
WheaSupport
WheaErrorInj

IsaBusDxe
IsaFloppyDxe
IsaSerialDxe
LegacyRegion2
LegacyBiosPlatform
Legacy8259
LegacyInterrupt
LegacyInterruptHookDxe
LegacyBiosDxe

WheaElog
UncoreErrorLog
PcieErrorLog
PvModule
KtiErrorRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorInj
OpalPlatform
OpalPlatformConfigSkt0
OpalPlatformConfigSkt1
OpalPlatformConfig_IFP45b_H79275
OpalPlatformConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRt
Uhdcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySredir
LegacyBridgeDxe
ChlSpecific
RASDxe
UefiOptionRomDispatchPolicy
Y2KRollover
MEForceUpdateDxe
SmiGraphicsOutput

DxeCore
FastVideoDxe
PcdDxe
RegAccessDxe
RegAccessSMM
ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm
StatusCodeHandlerSmm
DatahubStatusCodeHandlerDxe
StatusCodeRuntimeDxe
SectionExtractionDxe
GenericIpml
SmmGenericIpml
UbaConfigDatabaseDxe
UbaInitDxe

UefiOpromSetup

SlotDataUpdateDxeLightningRidgeEXRP
SsidSvidDataUpdateDxeLightningRidgeEXRP
StaticSkuDataDxeSawtoothPass
SetupConfigUpdateDxeSawtoothPass
OpromUpdateDxeSawtoothPass
SmbiosDataUpdateDxeSawtoothPass
Usb0cUpdateDxeSawtoothPass
IioCfUpdateDxeSawtoothPass
SlotDataUpdateDxeSawtoothPass
SsidSvidDataUpdateDxeSawtoothPass
FpkConfigUpdateSawtoothPass

IioCfUpdateDxeNeonCityFPGA
SlotDataUpdateDxeNeonCityFPGA
StaticSkuDataDxeBlueMountainPass
SetupConfigUpdateDxeBlueMountainPass

OemBadgingDxe
JpegDecoderDxe
ItkLogoProcess

MsftOemActivation

IioApmPWA
UuidDxe
SpdRawData
SetupConfigUpdateDxeWolfPass
OpromUpdateDxeWolfPass
SmbiosDataUpdateDxeWolfPass
Usb0cUpdateDxeWolfPass
IioCfUpdateDxeWolfPass
SlotDataUpdateDxeWolfPass
PchUsb2EyeDiagramDxeWolfPass
SsidSvidDataUpdateDxeWolfPass
FpkConfigUpdateDxeWolfPass
DMIMarginUpdateDxe
SwitchedWA
StaticSkuDataDxeBuc
SetupConfigUpdateDxeBuchananPass
OpromUpdateDxeBuchananPass
SmbiosDataUpdateDxeBuchananPass
Usb0cUpdateDxeBuchananPass
StaticBootOrder
StartupMarkerFileBootOrder
StaticBootOrder
NetworkBootApp
RiserPCIeBifurcationDxeBuchananPass
FrontPanelLockout
SataSgnio
SmbiosPcTable
SecureBootErrorHandlerDxe
BdsUpdateHookBuchananPass
SecureBootSetup
SecureBootCtrlDxe
BiosGuardServices
SmbiosDataUpdateDxeLightningRidgeEXRP
S3NvramSave
PlatformEarlyDxe

CpuIoDxe
CpuIo2Dxe
HiiteDatabase
DataHubDxe
FrameworkHiIAlias
Legacy8259
CpuArchDxe
PlatformCpuPolicy
CpuMpDxe
SMBIOSFilter
Metronome
WatchdogTimer
PcRtc
RuntimeDxe
PciHostBridge
PpmInitialize
IioSmm
LpcPlatform
PilotVPC8374
ReserveMem
CkService
CkServiceSmm
InterruptHookD
VBiosReverseThu
gacy
gacyInstallIntl
ItoTolerantWrit
bloSmm
riableInt15
riableInstallIn
MonotonicCounterRunt
BdsDxe
SecurityStubDxe
JpegDecoderDxe
OemBadgingDxe
CapsuleRuntimeDxe
RandomPoweronRacks
AcpiErrorReport
MsftOemActivation
TpmPlatformDxe
CpPcBiosId
SetupSmcCf

VlanConfigDxe
ArpDxe
Dhcp4Dxe
Ip4Dxe
Mftftp4Dxe
Udp4Dxe
Tcp4Dxe
UefiPxeBcDxe
IScsiDxe
Ip6Dxe
TcpDxe
Udp6Dxe
Dhcp6Dxe
Mftftp6Dxe
HttpDxe
HttpBootDxe
HttpUtilitiesDxe
DnsDxe

PchSpiSmm
PchSerialGpio
SmartTimer
PchResetRuntime
WdtDxe
PlatformReset
PowerButtonHandler
TcgMor
Tcg2Dxe
Tcg2Smm

ItkLogoProcess

TcgDxe
Smm
AcpiSwChild
IstformPreVariableDxe
SDxe
IEllog
IstformErrorGeneration
IericEllog
ImcDxe
IericEllog
IiRedirFru
Idt
VariableDrive
IMeFwPatch
IStatus
IDriver
IericFru
IBusDxe
IAtapIPassThru
Irel RAIDAtaAtapi
Irel RAIDBiosThur
compatiblePciD
IBusDxe
ISerialDxe
IFloppyDxe
IacyBiosDxe
ICVide
IcfsyncDxe
IPlatform
IacyBiosPlatfo
IPolicy
IDIMMDriver
IDIMMHii
IAHCI
esSATALegacy
esSATALegacy
esSATAEFI
esSATAEFI
IVROC2
IVROC1
ICpioGen3
ICVideogop
VBIOs
IeedVideo
IctitionDxe
IBusDxe
IorySubClass
IupBrowser
ISetup
IstformDevSUpdate
IplayEngine
IbiosDxe
SmbiosMeasurementDxe
EnglishDxe
PlatformOverrideDxe
NvmExpressDxe
ESRTIISataEffi
ScsiBus
ScsiDisk
AcpiPlatform
SmmAccess
PiSmmIpl

PiSmmCore
SmmCommunicationBuffer
PiSmmCpuDxeSmm
CpuIo2Smm
BIOSGuard
Ps2KeyboardDxe
Ps2MouseDxe
PS2TrackPointDxe

IsaBusDxe
IsaFloppyDxe
IsaSerialDxe
LegacyRegion2
LegacyBiosPlatform
Legacy8259
LegacyInterrupt
LegacyInterruptHookDxe
LegacyBiosDxe

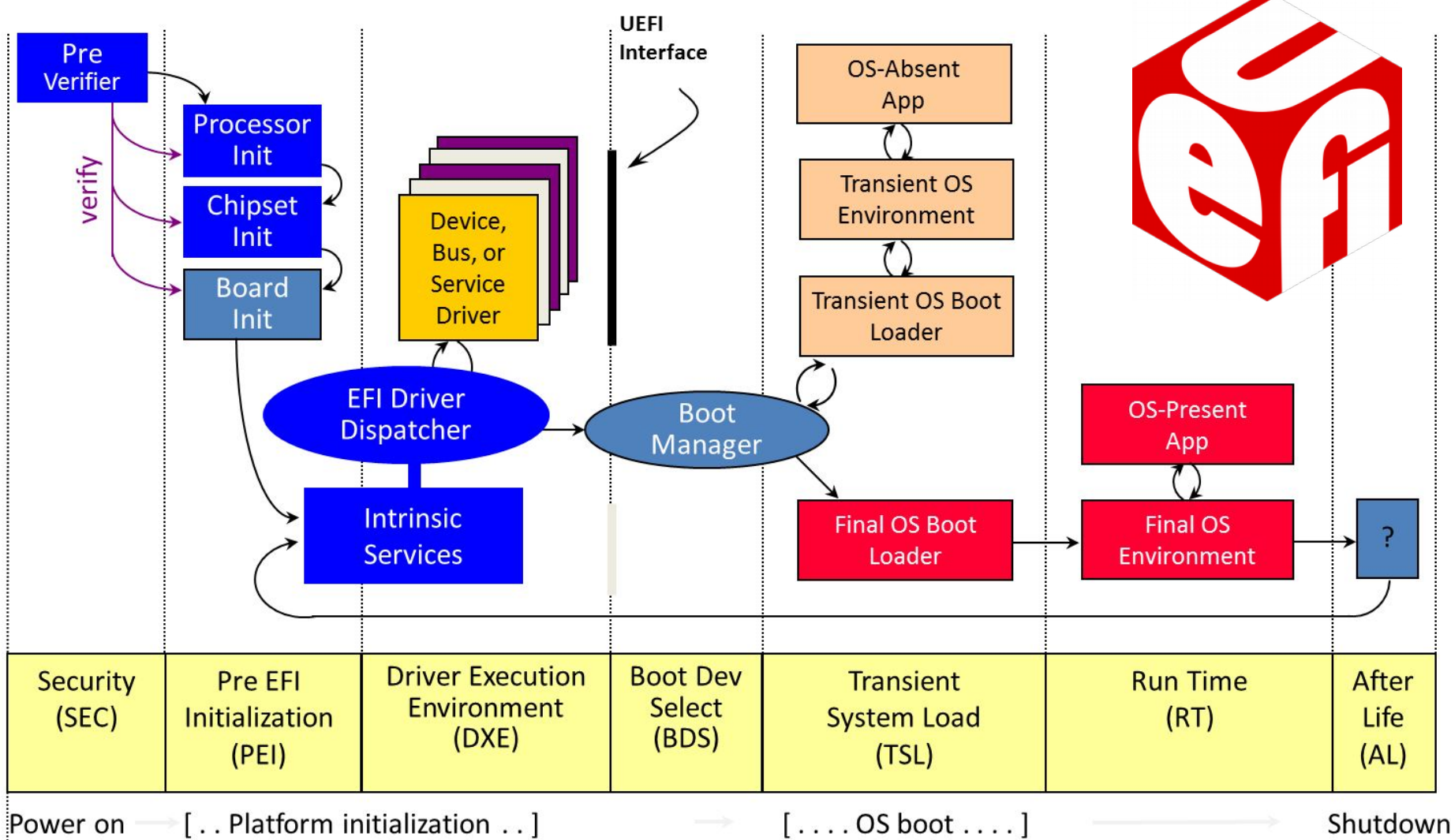
SvsSmmHandler
CpuHotAdd
KtiRas
CpuRas
IioRas
HpIOXAccess
RasInit
PolicySampleDriver
ImcErrorHandler
ProcessorErrorHandler
PcieErrorHandler
PartialMirrorHandler
EnhancedMcErrorHandlerLog
WheaErrorLogListener
PprV1ErrorLogListener
WheaErrorInj2
RASMiscDriver
McBankErrorInj
QuiesceSupport
IstPlatformSupportamba
WheaSupport
WheaErrorInj

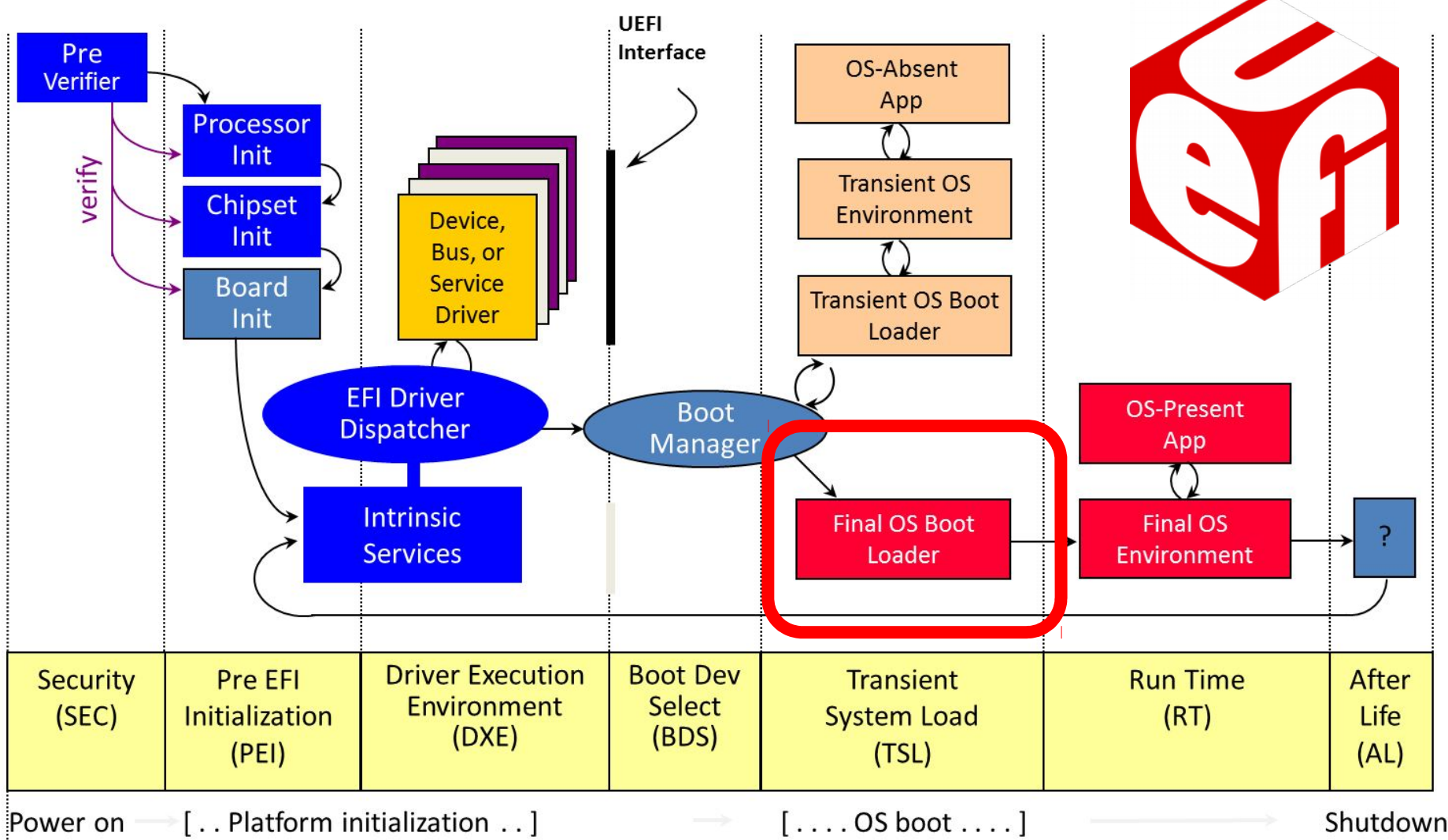
WheaElog
UncoreErrorLog
PcieErrorLog
PvModule
KtiErrorLogRuntime
KtiErrorLogPost
WheaPlatformBoot
WheaErrorLog

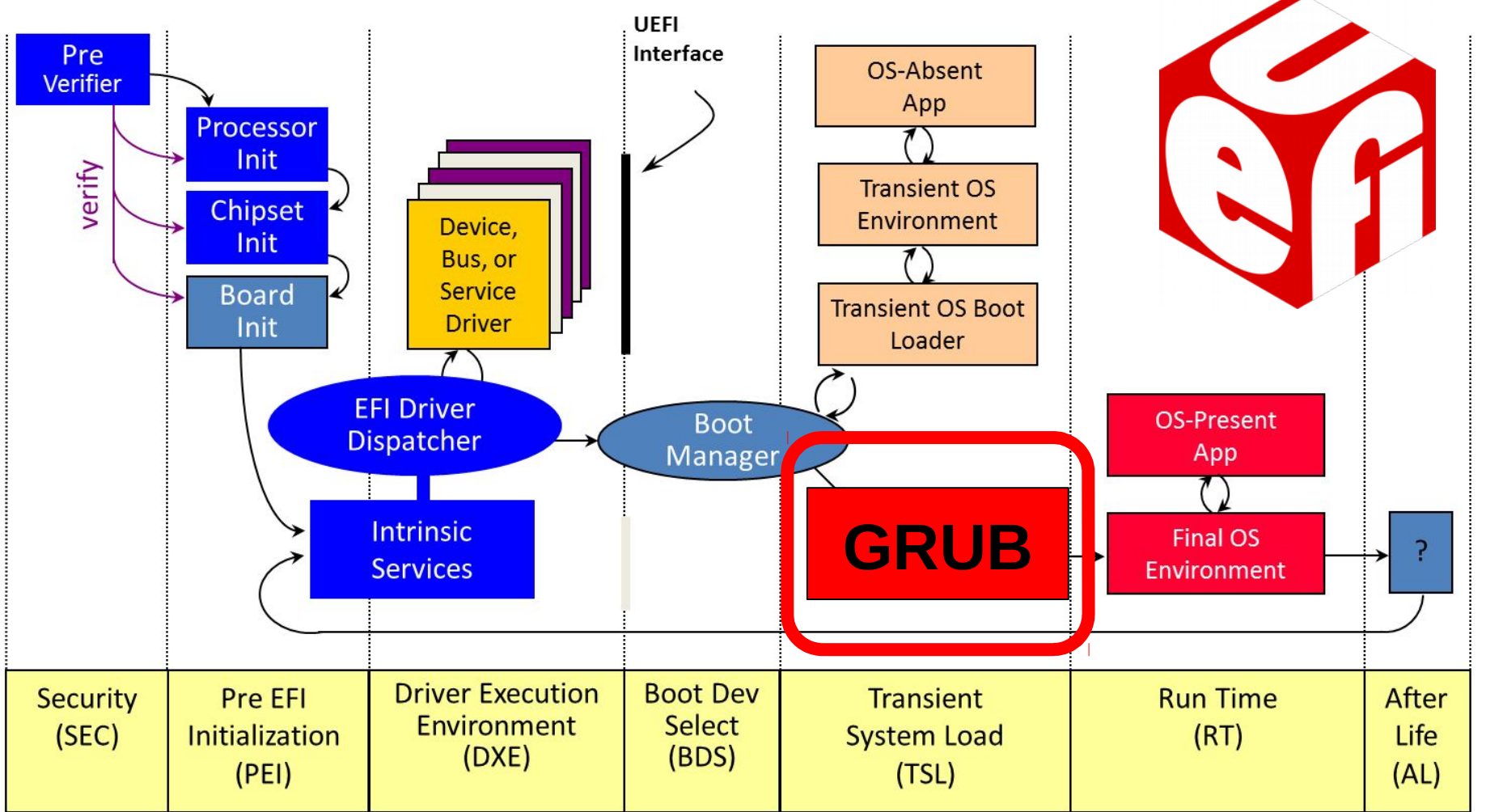
Opaplatic
OpAPlatConfigSkt0
OpAPlatConfigSkt1
OpAPlatConfig_IFP45b_H79275
OpAPlatConfig_IFT45b_H79267_H79272
LsiVtdSupport.inf
LegacyFV/CSM_v74
UsbRT
Uhdcd
KbcEmulSMM
KbcEmulDxe
UsbInt13
AmiLegacyBiosHook
LegacySredir
LegacyBridgDxe

Y2KRoller

McBankErrorInj
SmiGraphicsOutput







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

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

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

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

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:

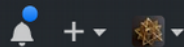
ansic:	235,636	(94.82%)
asm:	11,264	(4.53%)
sh:	865	(0.35%)
lex:	393	(0.16%)
yacc:	268	(0.11%)
awk:	75	(0.03%)

Total: 248,501 lines of code



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](#)



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



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

GRandom Unified Bootloader <http://www.gnu.org/software/grub/grub.html>

9,611 commits

2 branches

8 releases

103 contributors

GPL-3.0



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

GRandom Unified Bootloader <http://www.gnu.org/software/grub/grub.html>

9,611 commits

2 branches

8 releases

103 contributors

GPL-3.0



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

GRandom Unified Bootloader <http://www.gnu.org/software/grub/grub.html>

9,611 commits

2 branches

8 releases

103 contributors

GPL-3.0



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

GRandom 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

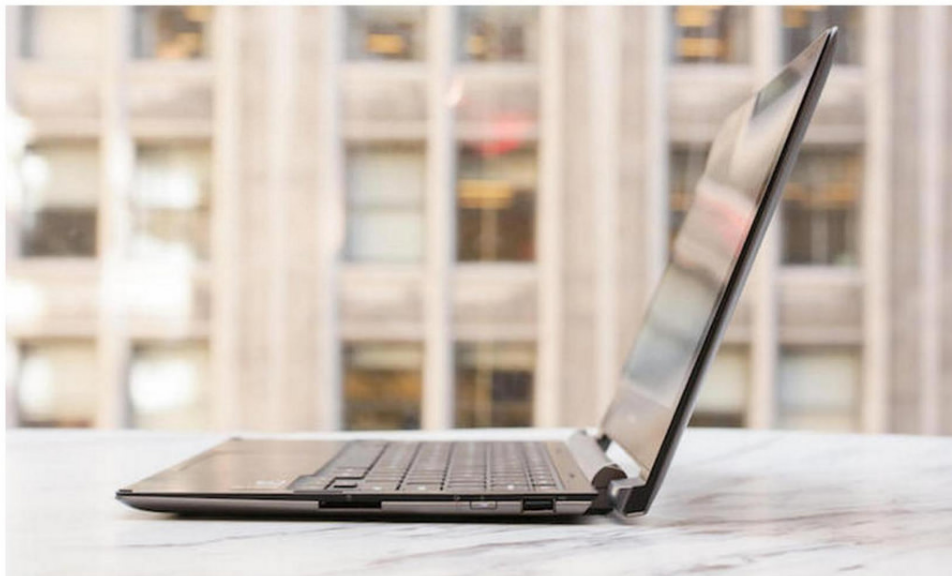
Trust ~~No One~~
Fewer Parties

██████████ 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

REVIEWS

HOW-TO

VIDEO

BUSINESS

LAPTOPS

TABLETS

PHONES

HARDWARE

SECURITY

SOFTWARE

GADGETS



Privacy

Encryption

Antivirus

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 is 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

CPU Mfg +
TianoCore

AMD

intel



tianocore

IBV

American Megatrends

insyde

phoenix

ODM

COMPAL

FOXCONN

PEGATRON

wistron

flex

Inventec

ASUS

OEM's typically
generate < 10%
of BIOS Code

OEM

Lenovo

NEC

acer

ASUS

DELL

hp

Microsoft

Apple

Typical

Lenovo

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.

[Documentation](#)

[Talks & Resources](#)

[Tools](#)

[Contribute](#)

[Events](#)

[Blog](#)

[Who is involved?](#)

[News](#)

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

```
g GNU
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

Build 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 skip=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
workl -heads
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: █
```



```
Performing operation on 'COREBOOT' region...
Name      Offset      Type      Size
cbfs master header 0x0        cbfs header 32
make[2]: 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:
```

```
heads:~/heads:sha256sum x230.rom
e9dc9db9b359b750c4535b1edf8e579bdb75ea354cfb4ca61c0bb7a63d9a0606 x230.rom
```

```
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”



Open Systems Firmware
Ron Minnich/SWE/Google
Gundra Devender Goud/Director/Microsoft

OPEN. FOR BUSINESS.

 OCP SUMMIT

Stage 4 08:00 AM, 2014

10/26/14

The slide features a white background with a green and purple geometric logo in the top left. The text is centered. A green banner at the bottom contains the slogan "OPEN. FOR BUSINESS." and the OCP Summit logo on the right. The bottom left corner shows a small text string "Stage 4 08:00 AM, 2014" and the bottom right corner shows "10/26/14".

```
#!/bin/sh
# This is the very first script invoked by the Linux kernel and is
# running out of the ram disk. There are no filesystems 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
```

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 []

.config - Linux/x86 4.9.38 Kernel Configuration

> File systems

File systems

Arrow keys navigate the menu. <Enter> selects submenu ---> (or empty submenu ----). 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)
```

```
ule support --->
yer --->
features --->
d ACPI options --->
c.) --->
mats / Emulations --->
--->
>
```

< 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. L

.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 <-> kernel-space linker ----
< > Memory Technology Device (MTD) support ----
[ ] Device Tree and Open Firmware support ----
< > Parallel port support ----
-* Plug and Play support --->
[*] Block devices --->
< > NVMe 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 ----
```

ule support
yer --->
features
d ACPI opti
c.) --->
mats / Emul
--->

< Help >

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



NSA SECURITY ESP 1



Boot strapping slightly more secure systems

Trammell Hudson @grs

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



33c3
EM ROF SKROW

```
[ 400000)
[ 1.936372] Freeing unused m
600000)
HEARTS
```

```
Press 'r' for recovery shell: r
!!!! User requested recovery shell
New value of PCR[4]: 8aba96fde1a8dd96271479dc40742b36aba3c2b3
!!!! Starting recovery shell
[ 2.841177] clocksource: Switched to clocksource tsc
/bin/ash: can't access tty; job control turned off
# qubes-install -
```



Replace Your Exploit-Ridden Firmware with Linux

Ronald Minnich, *Google*

 Embedded
Conference
Europe



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



 THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
EUROPE

 Embedded Linux
Conference Europe

Results

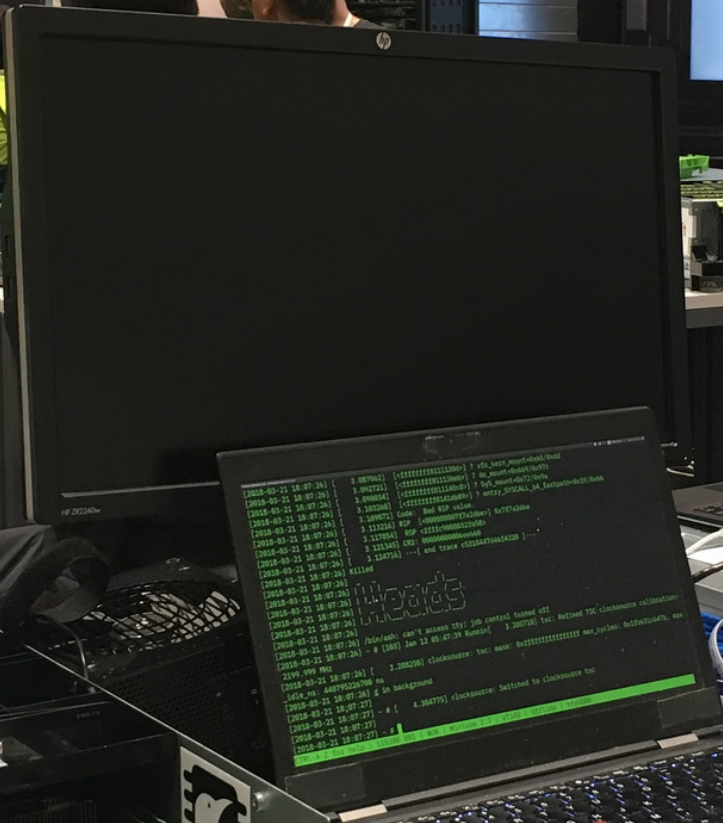
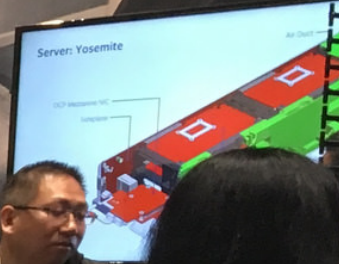
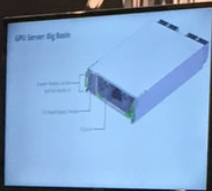
- OCP boot time: 8 minutes -> 20 seconds
 - I.e. 24x speedup
 - This is to a shell prompt in Linux
- OCP -> DHCP -> wget -> kexec: 25 seconds
- All userland written in Go
- Linux performance and reliability in firmware
- Eliminate *all* UEFI/ME post-boot activity





facebook



OPEN OPTIMIZED INFRASTRUCTURE BUILDING




LinuxBoot
provided image
minimize FW
and boot flow
security

 + 
coreboot + LinuxBoot

- coreboot built from mostly upstream sources
- Intel FSP from GitHub
- Linux + invariants on base ROM
- Highest transparency, security, and customization.
- Power on to shell in a few seconds
- Serial console is the main bottleneck.
- Can integrate with sbt, 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)

NPB VER: A TPM TOP C2

PR5F01

856968T12
G1508KIV
15ZA5050961A7

10 C128

R1 R2 R3

CA

=====
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; job
/ # [2.451809] clocksource



Google Authenticator

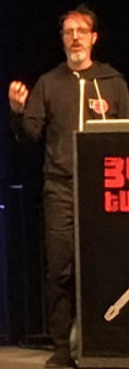
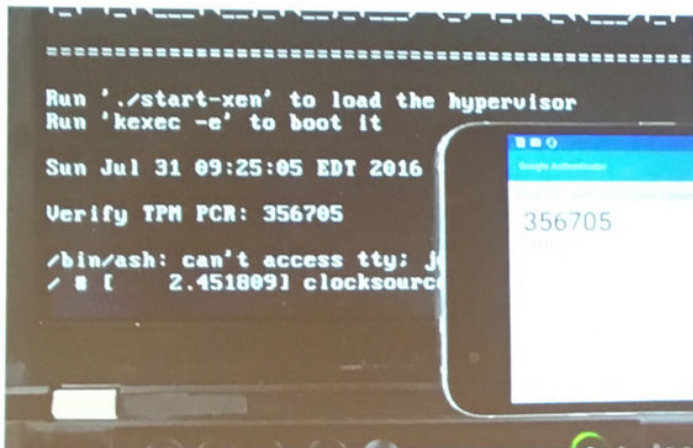
Enter this verification code if prom

356705

TPMTOTP



Trusted Boot



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

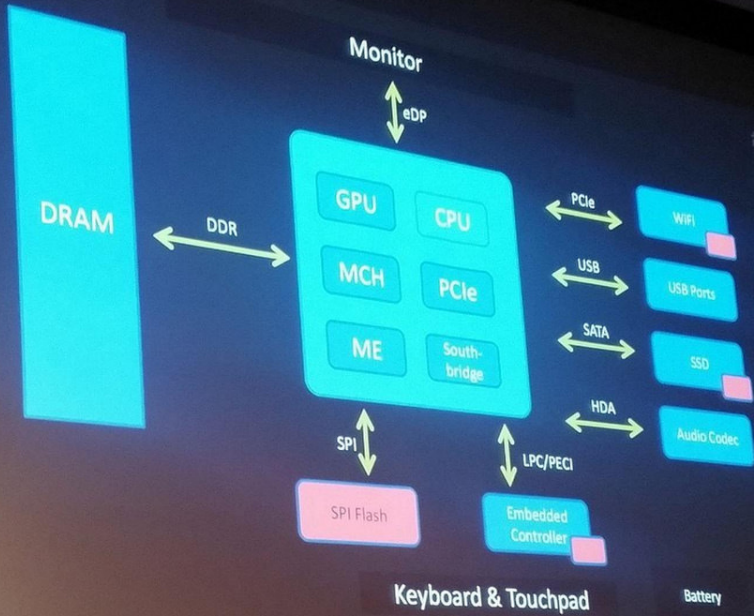
ABSTRACT

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

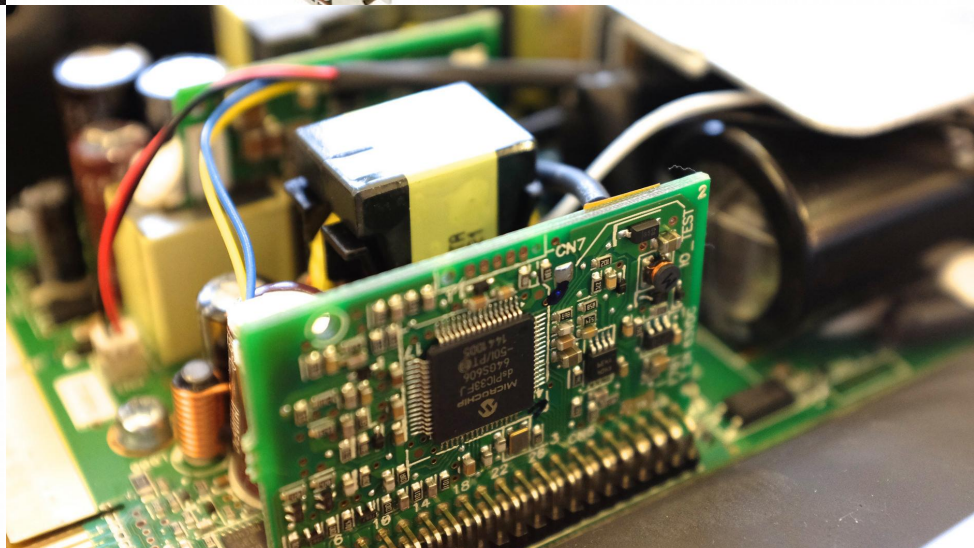
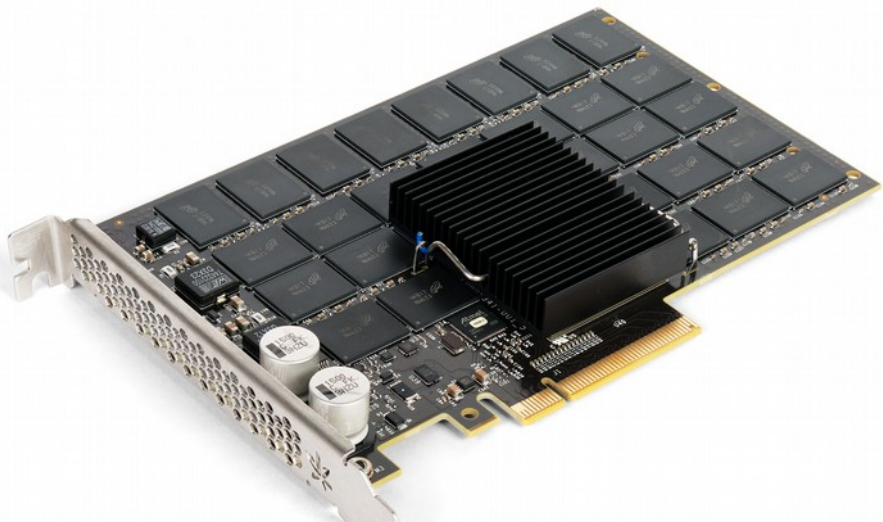
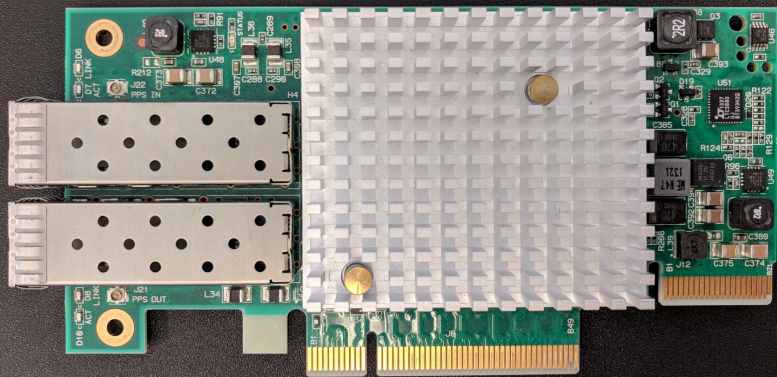
The proliferation and popularity of infrastructure-as-a-service (IaaS) cloud computing services such as Amazon Web Services and Google Compute Engine means more cloud tenants are hosting sensitive, private, and business critical data and applications in the cloud. Unfortunately, IaaS cloud service providers 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 software based cryptographic solution or unverifiable trust

Measure “Everything”?



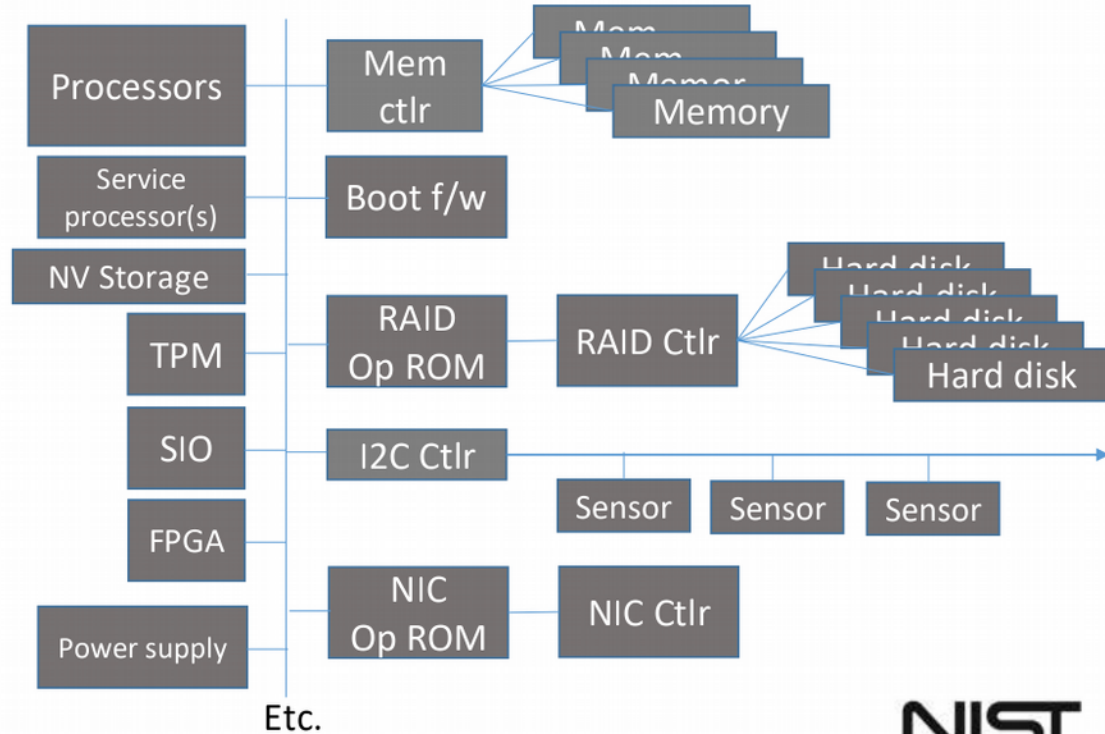
we'll be thinking: can we assure having good code and how the peripherals interfere here

again: we will look at this SPI flash loaded on the platform



NIST Special Publication 800-193

Platform Firmware Resiliency Guidelines



Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Preventing Persistence

Custom security modules



Titan

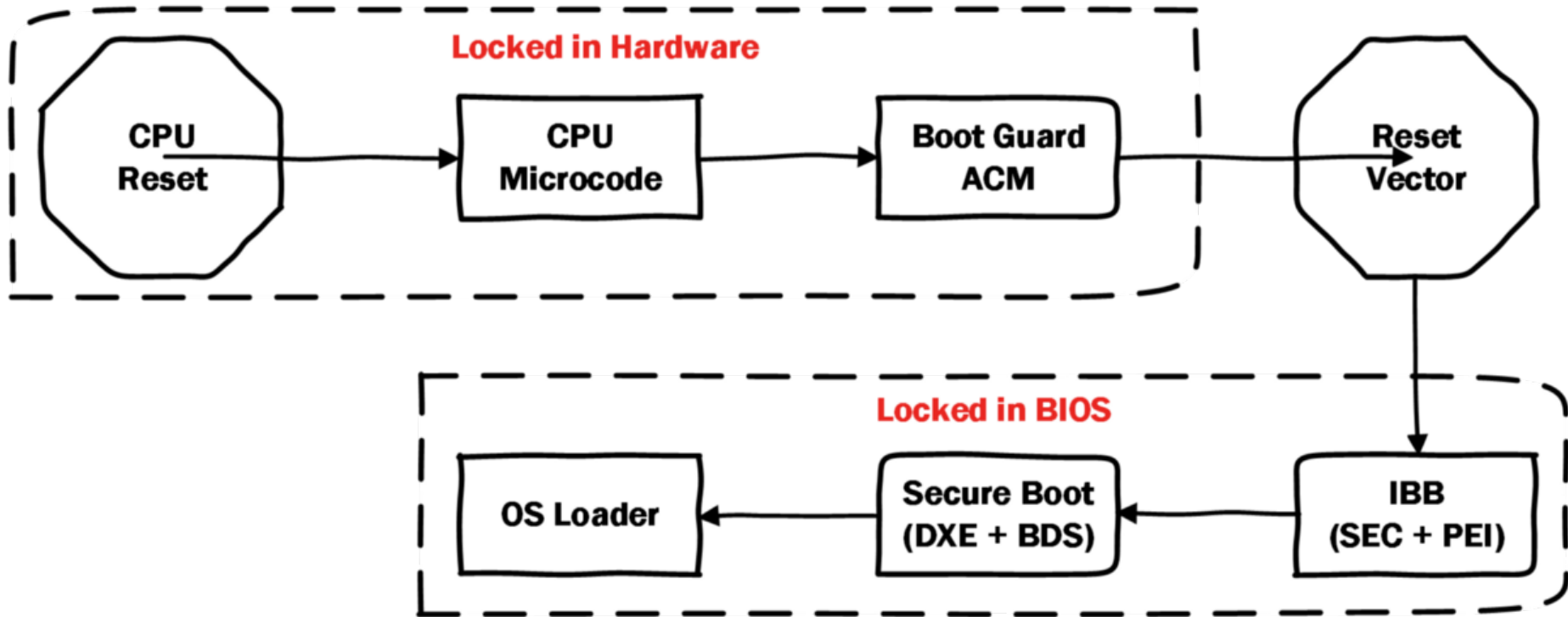
Purpose-built chip to establish hardware root of trust for Google Cloud servers

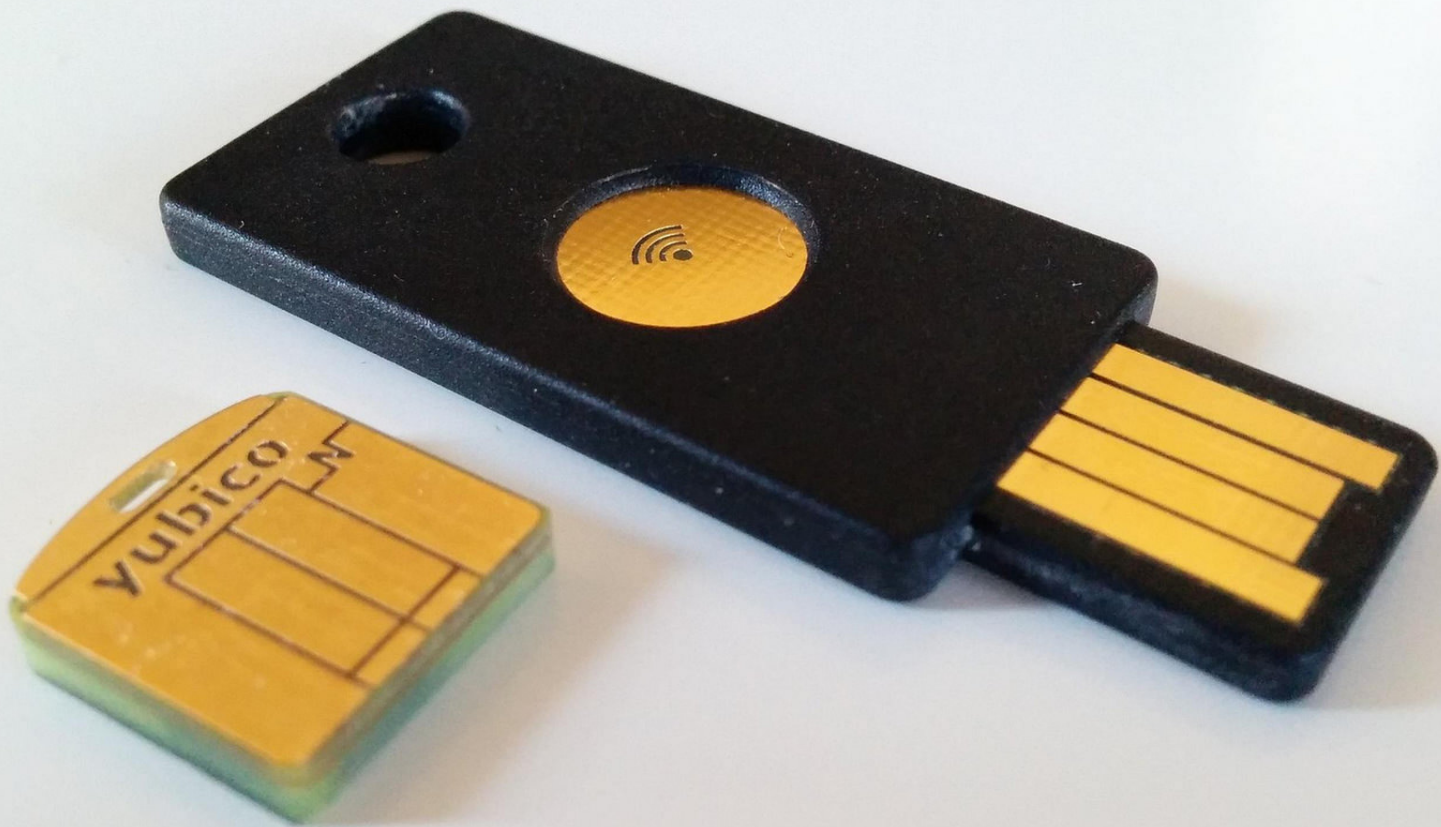


Google's purpose-built server

**Jon McCune from Google
Presenting tomorrow!**

Intel BootGuard on commodity hardware





```
#!/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}" \
```

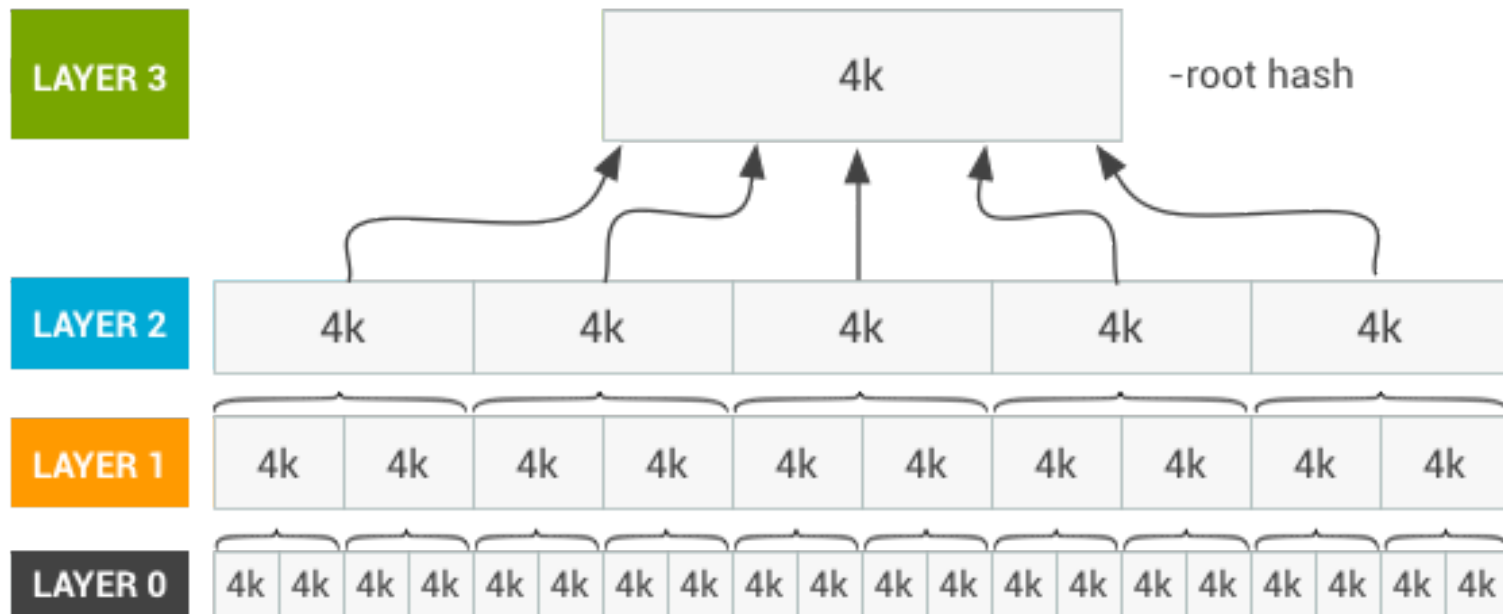
```
  --command-line "no-real-mode console=vga" \
```

```
  "${XEN}" \
```

```
|| die "Unable to load kernel/hypervisor/initrd"
```

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

dm-verity for signed, read-only filesystems



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?

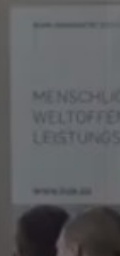
Vulnerability used in this section is [VU#976132](#) a.k.a. [S3 Resume Boot Script Vulnerability](#) independently discovered by [ATR](#) of Intel Security, Rafal Wojtczuk of [Bromium](#) and [LegbaCore](#)

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)



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



34C3:
tuxat!



Board
Management
Controller

ASPEED

AST2500

PBR521.00S-15

1647 TAN A2 GP



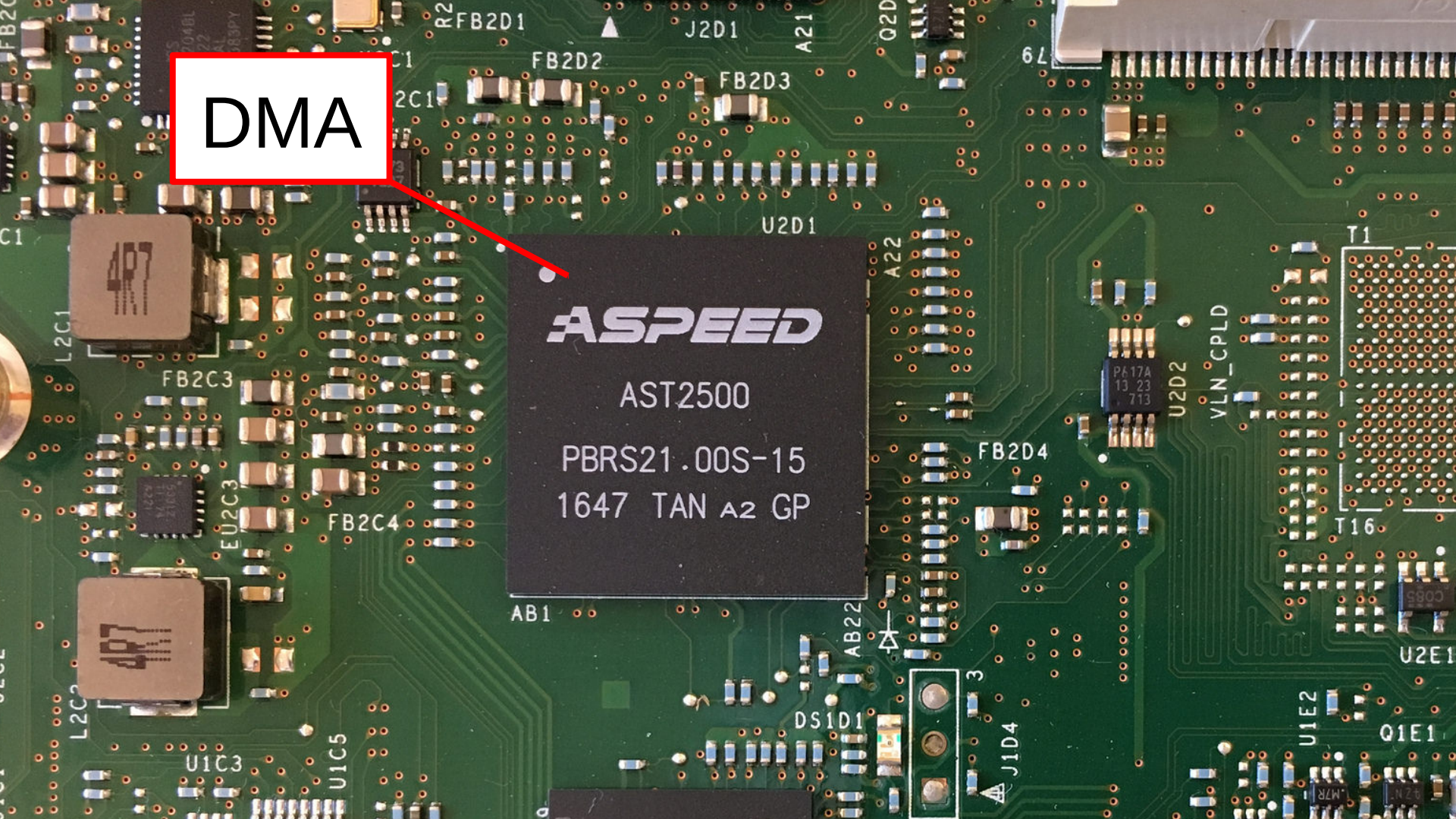
DMA

ASPEED

AST2500

PBR521.00S-15

1647 TAN A2 GP



DMA

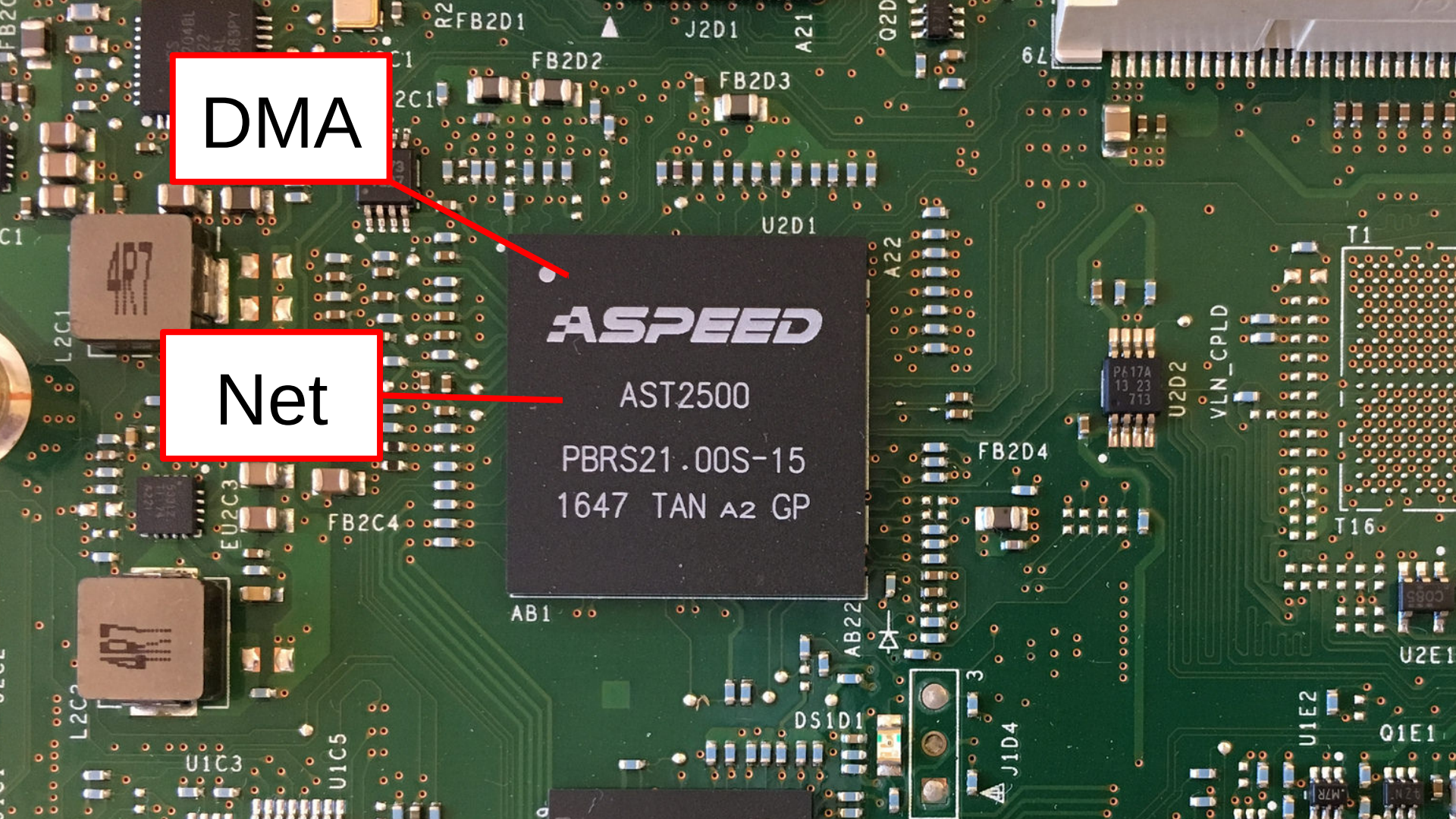
Net

ASPEED

AST2500

PBR521.00S-15

1647 TAN A2 GP



DMA

Net

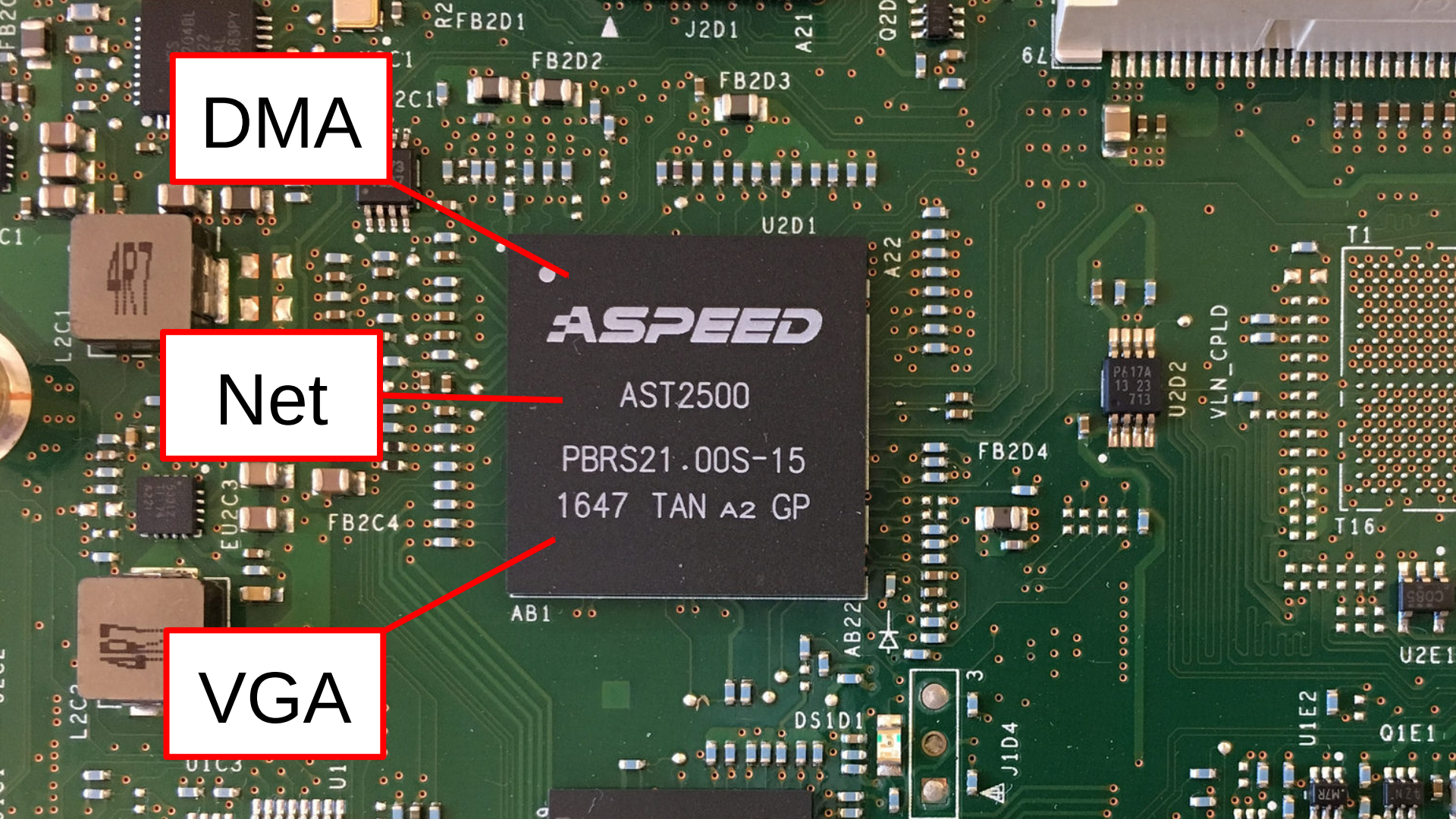
VGA

ASPEED

AST2500

PBR521.00S-15

1647 TAN A2 GP



DMA

Net

VGA

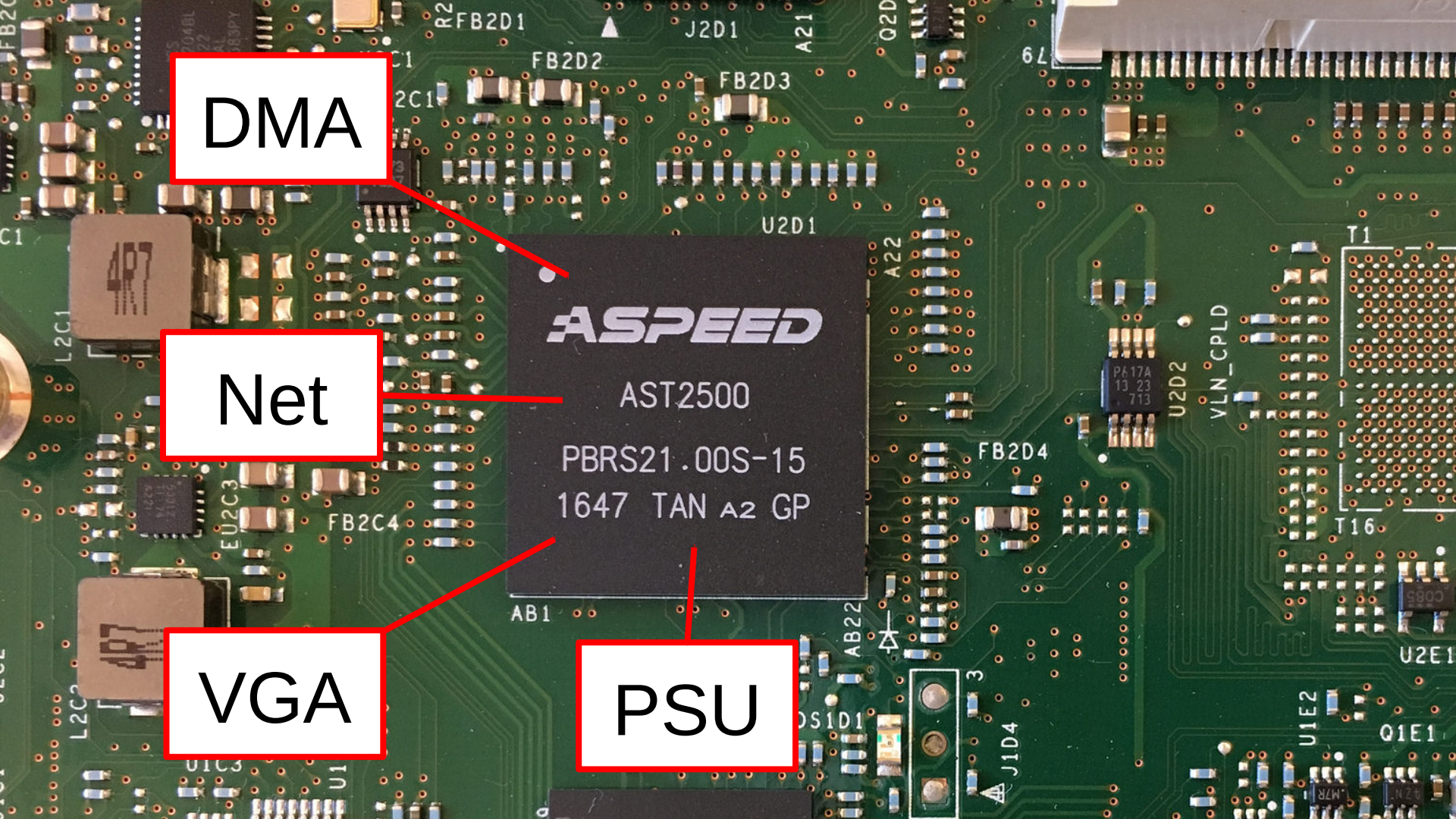
PSU

ASPEED

AST2500

PBR521.00S-15

1647 TAN A2 GP



DMA

Net

VGA

PSU

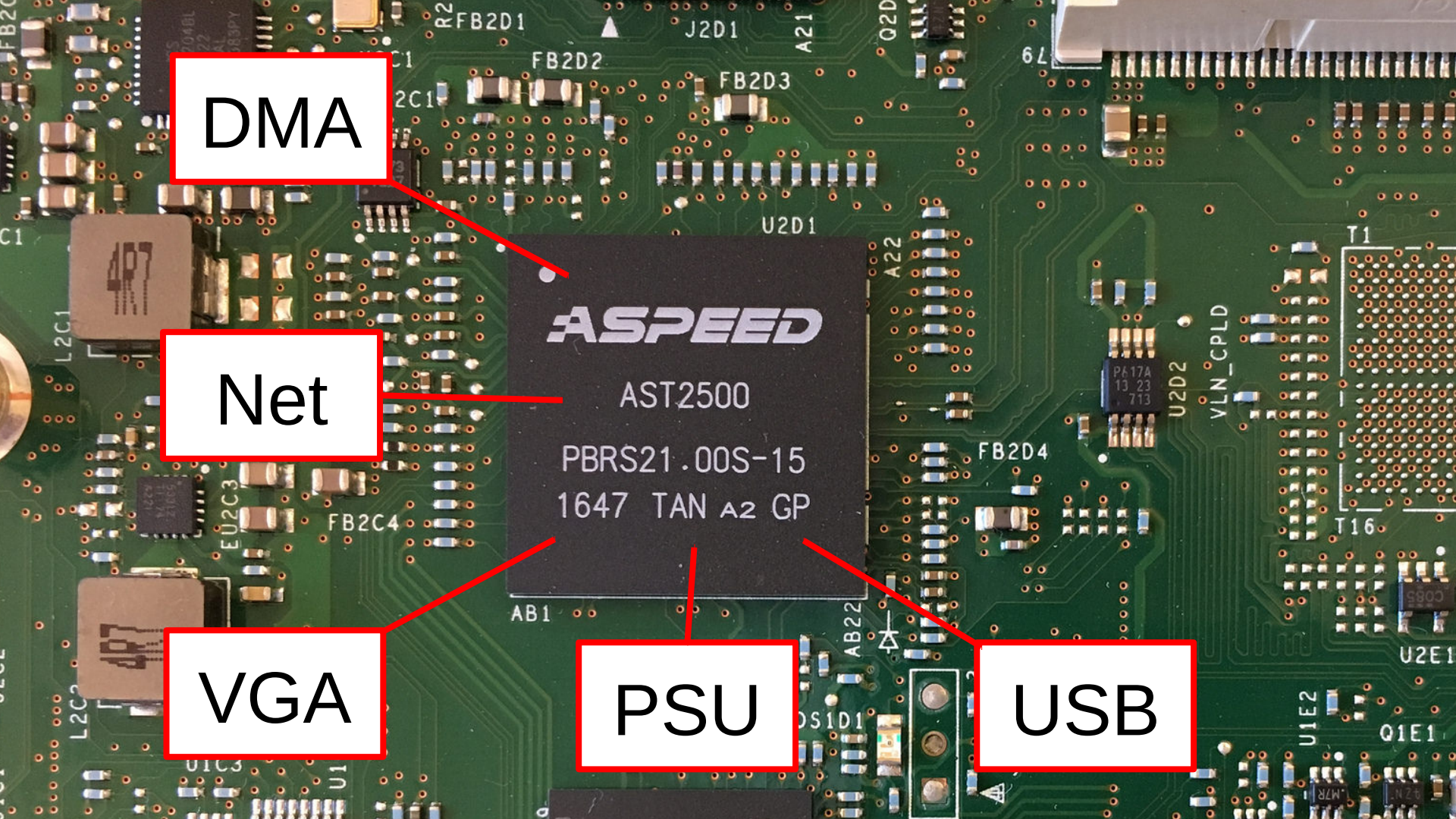
USB

ASPEED

AST2500

PBRS21.00S-15

1647 TAN A2 GP



DMA

Net

VGA

ASPEED

AST2500

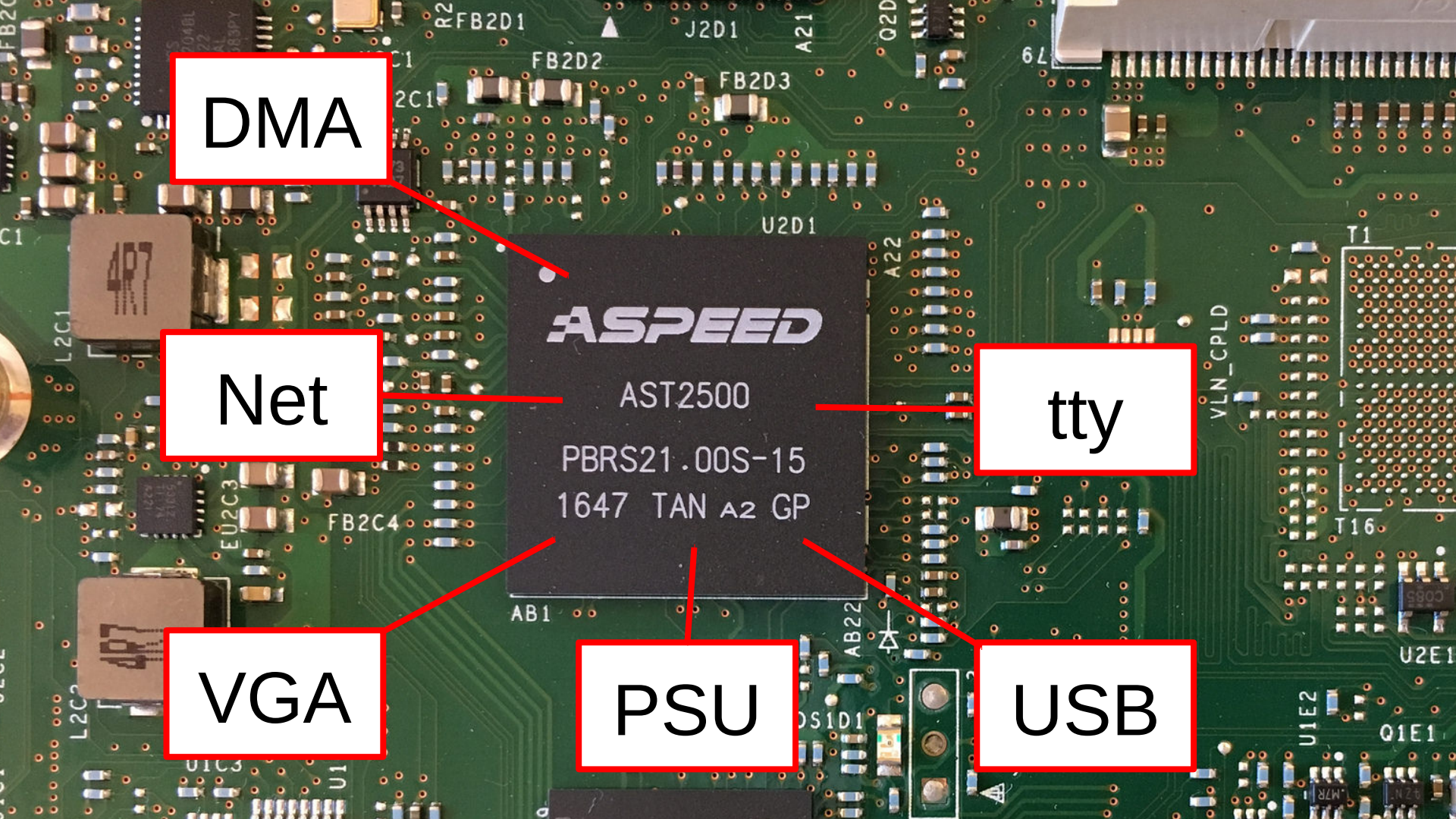
PBR521.00S-15

1647 TAN A2 GP

PSU

tty

USB



DMA

SPI

Net

tty

VGA

PSU

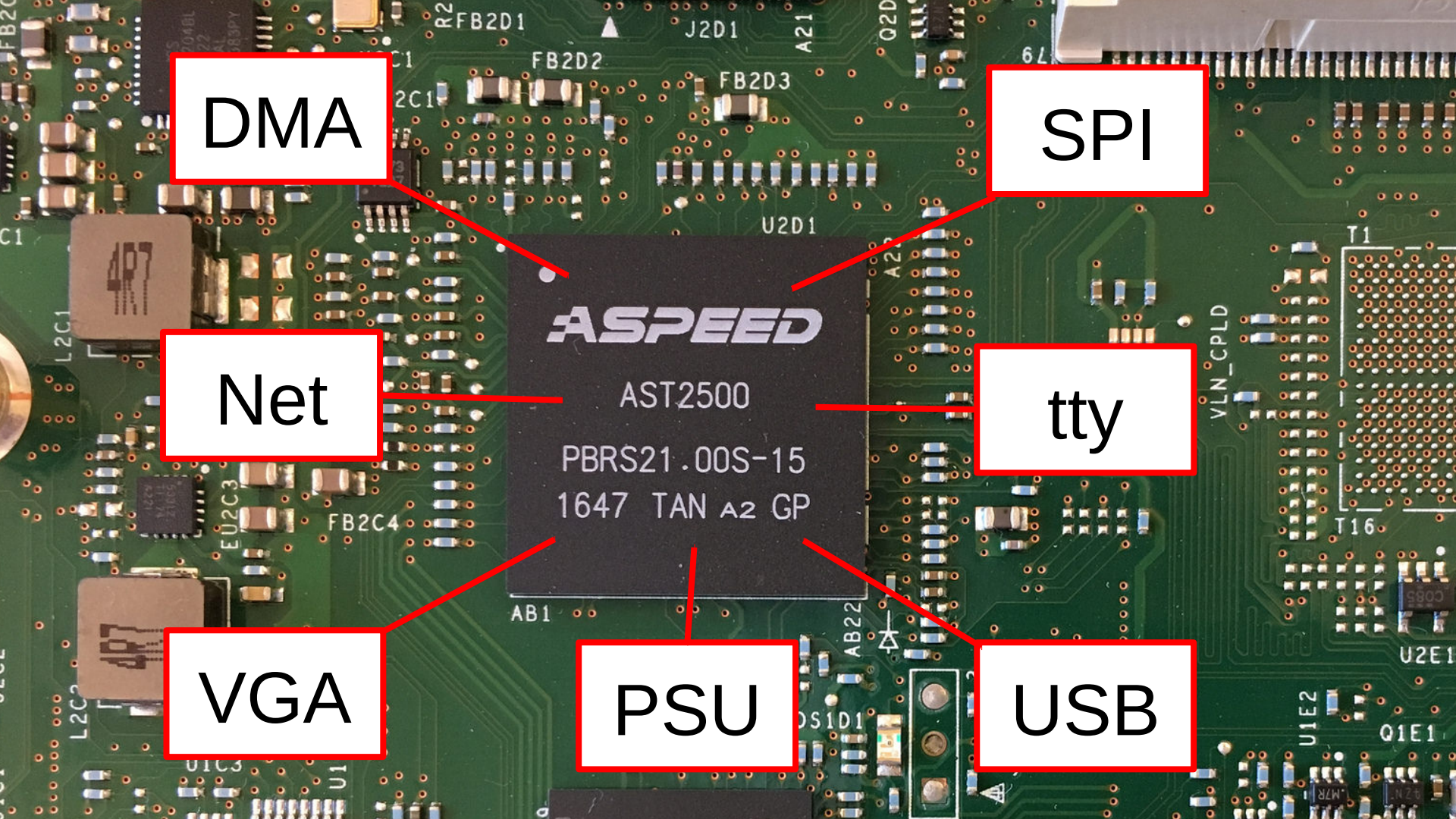
USB

ASPEED

AST2500

PBR21.00S-15

1647 TAN A2 GP



DMA

TPM

SPI

Net

tty

VGA

PSU

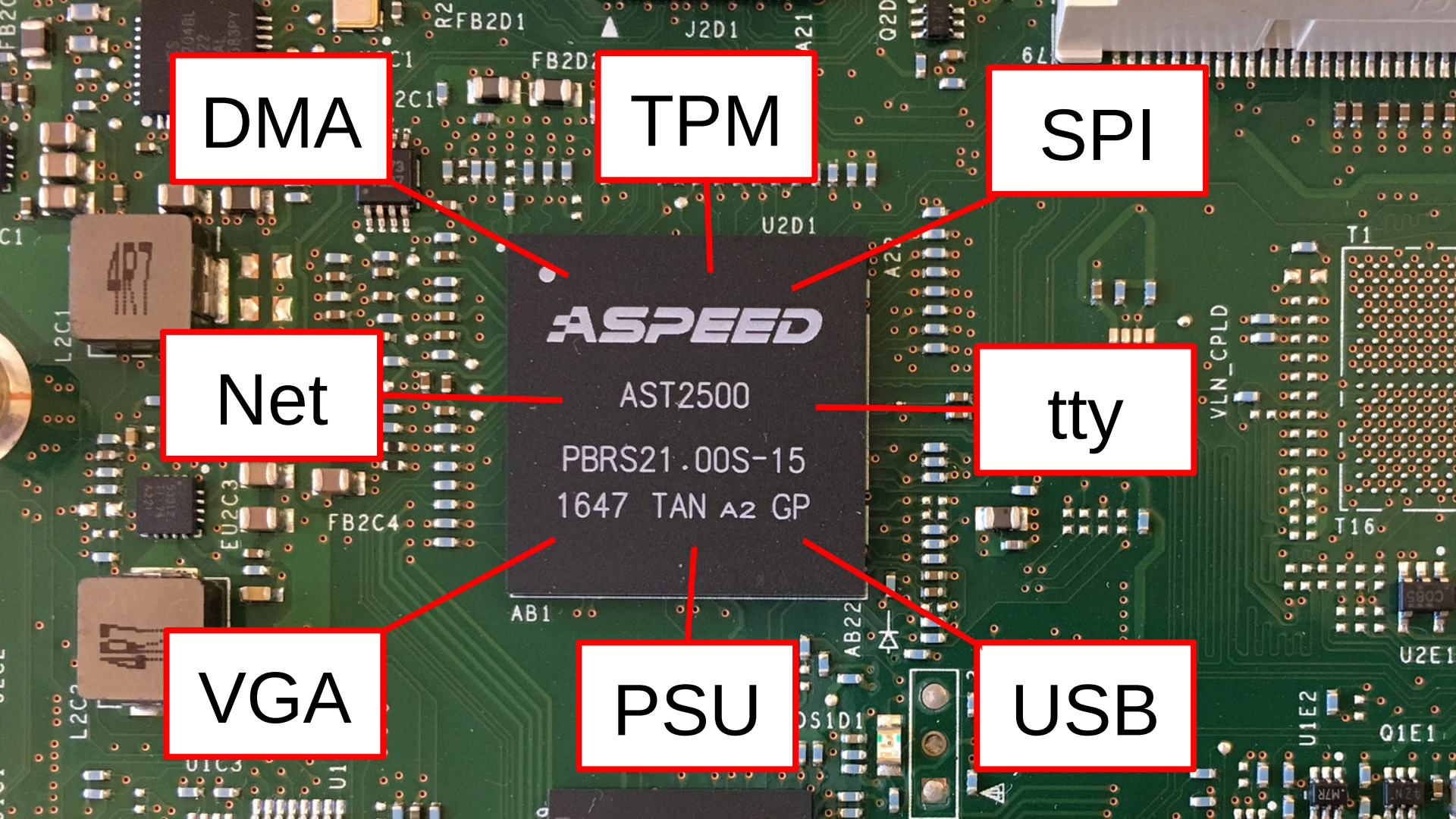
USB

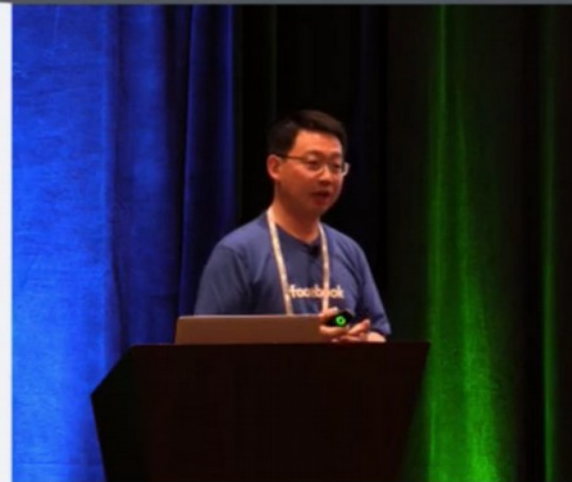
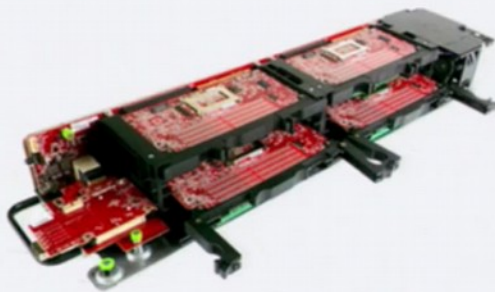
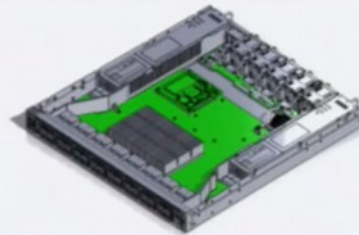
ASPEED


AST2500

PBR521.00S-15

1647 TAN A2 GP





 Embedded Linux
Conference

 OpenIoT Summit

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



quanta

1009.15

720
MAG1
544834
630307

2E20MA000
19-000591

P/N: DAF20TB18C0 Rev. 1.0
CSA
30F20L80010
BPL60200135

P/N: 20F20BU0150

quanta
ARTFBF2008701059S2A 00LS
05000236

quanta

VP150R005
CE
RoHS
RECYCLED

1009.15
MAG1
544834
630307
19-000591
2E20MA000
P/N: DAF20TB18C0 Rev. 1.0
CSA
30F20L80010
BPL60200135

2x 819
picks

Getting started with 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

osresearch / heads

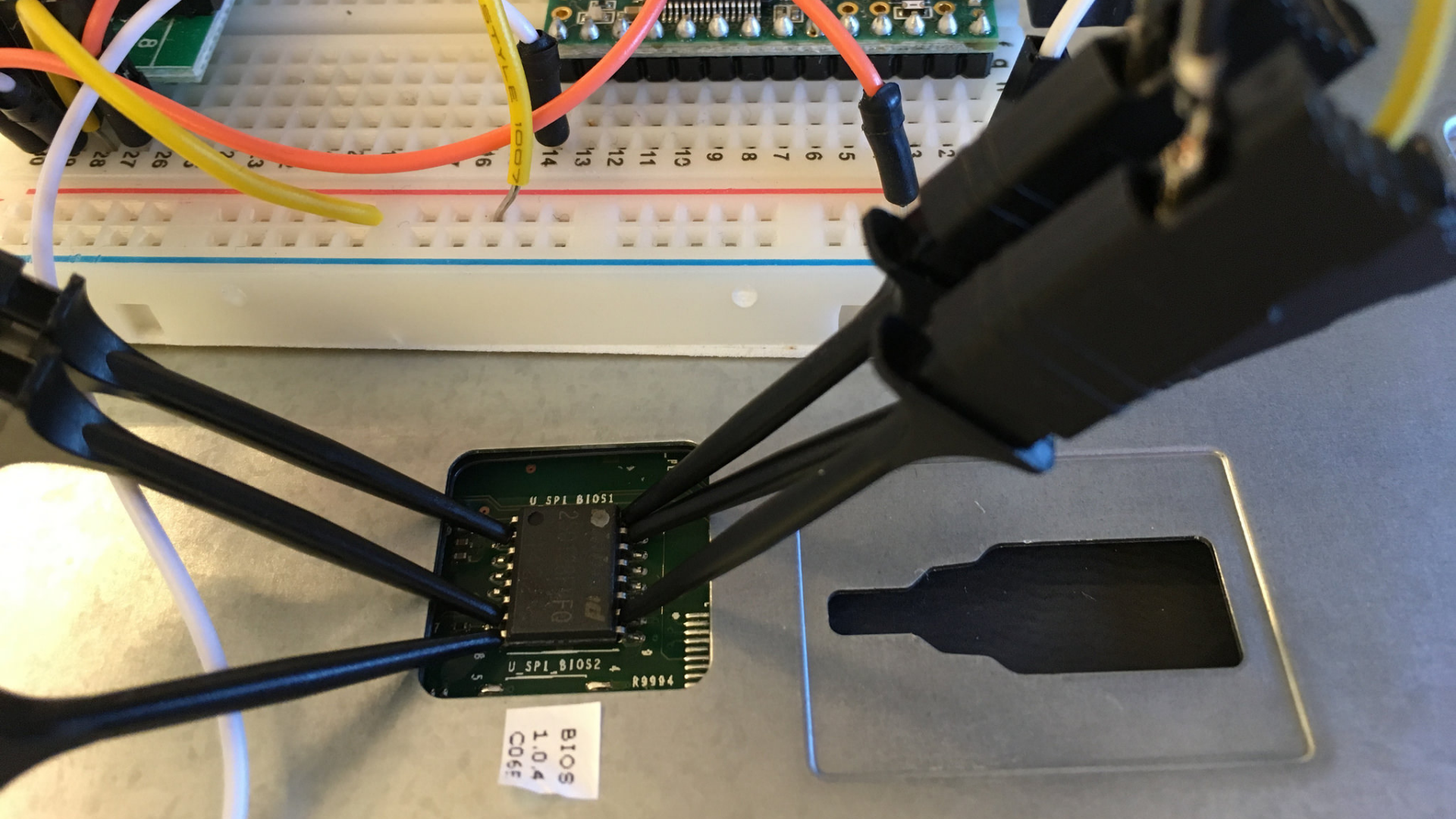
Watch 45 Star 516 Fork 54

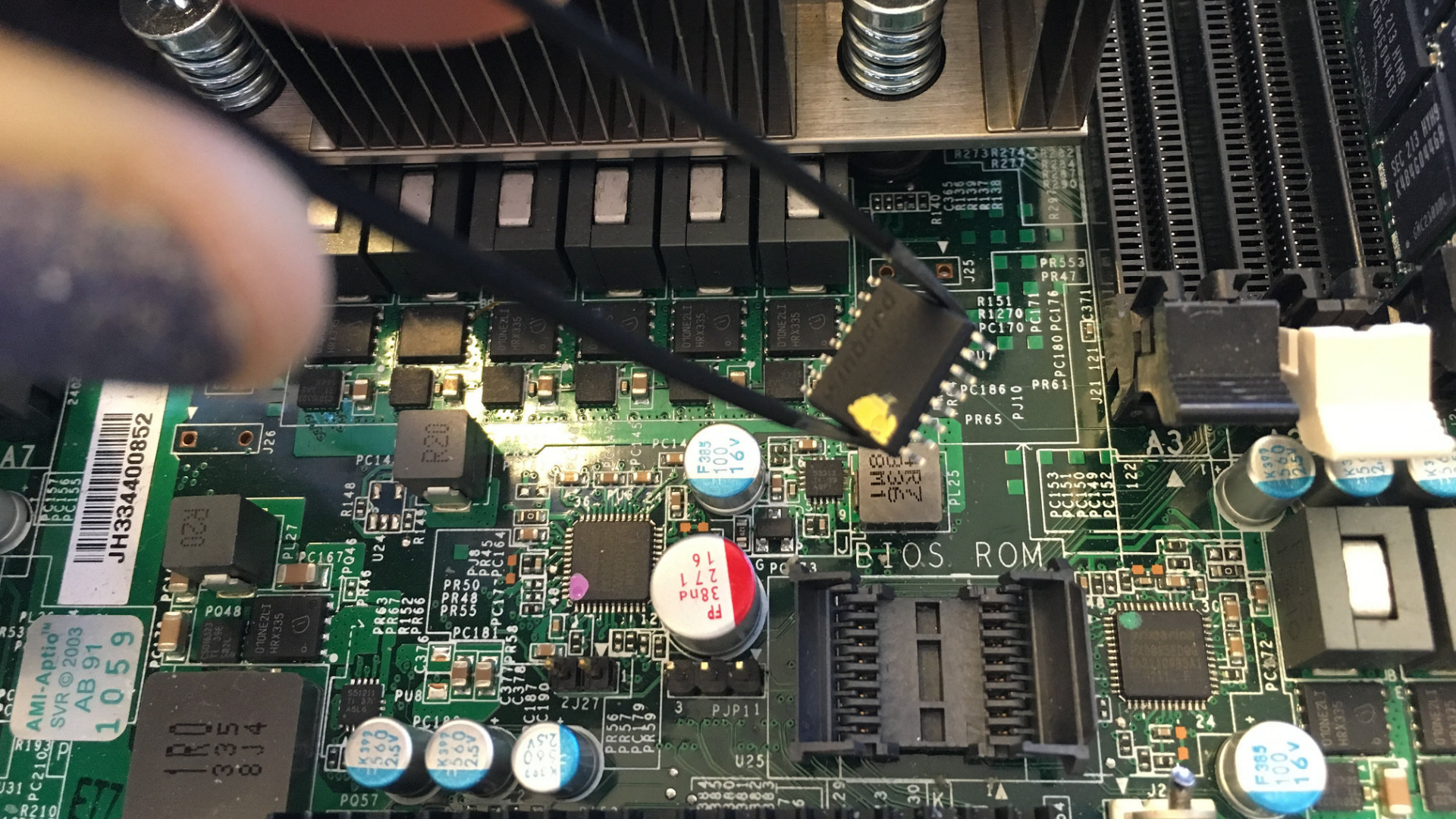
Code Issues 73 Pull requests 10 Projects 0 Wiki Insights

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





AMI-Aptio™
SVR © 2003
AB 91
1059

JH334400852

1R0
3814

BIOS ROM

FP
38nd
271
16

F385
100
16V

K390
250
25V

A503
250
25V

F385
100
16V

K390
250
25V

K390
250
25V

K390
250
25V

LW8
220
22

AMI
Aptio
BIOS
ROM

A7

240

R53

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210

R210



Secure

Flexible

Resilient

Open

Reproducible

Measured



LinuxBoot.org

