UEFI-Integration und Secure Boot

Inhalt

- Motivation
- PC BIOS
  - Funktionsweise
- UEFI
  - Architektur
  - Funktionsweise
- Secure Boot
  - Architektur
  - Praxis unter Windows 8 und Linux
  - Risiken & Herausforderungen

Motivation

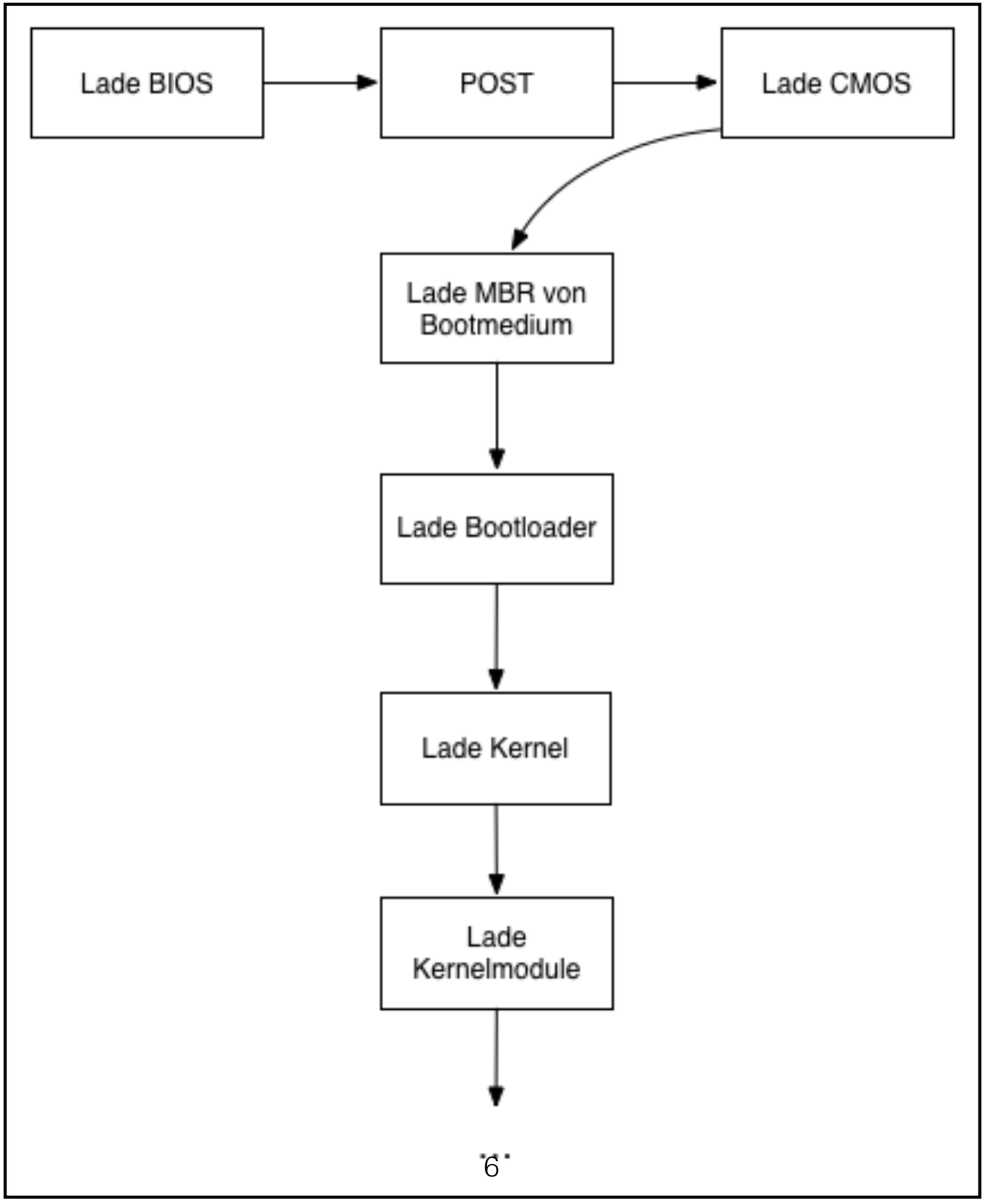
- Sicherer Systemstart
  - nur vertrauenswürdige Software ausführen
  - wird der Systemstart kompromittiert, fallen alle weiteren Sicherheitsmechanismen
- Kernel-Rootkits
  - Nachladen von Kernelmodulen

PC BIOS

Basic Input Output System

PC BIOS

- Auf Mainboard abgelegt
- initialisiert die Hardware, führt den POST aus und lädt Konfiguration aus dem CMOS
- lädt Bootsektor des Startmediums (MBR)
- Master Boot Record (MBR) enthält Partitionstabelle und Bootloader


Lade BIOS
POST
Lade CMOS
Lade MBR von Bootmedium
Lade Bootloader
Lade Kernel
Lade Kernelmodule

PC BIOS

- unterstützt nur Bootmedien kleiner 2,2TB
- langsamer Bootvorgang
- kann nur 1MB adressieren
- > 30 Jahre alte Technologie

UEFI

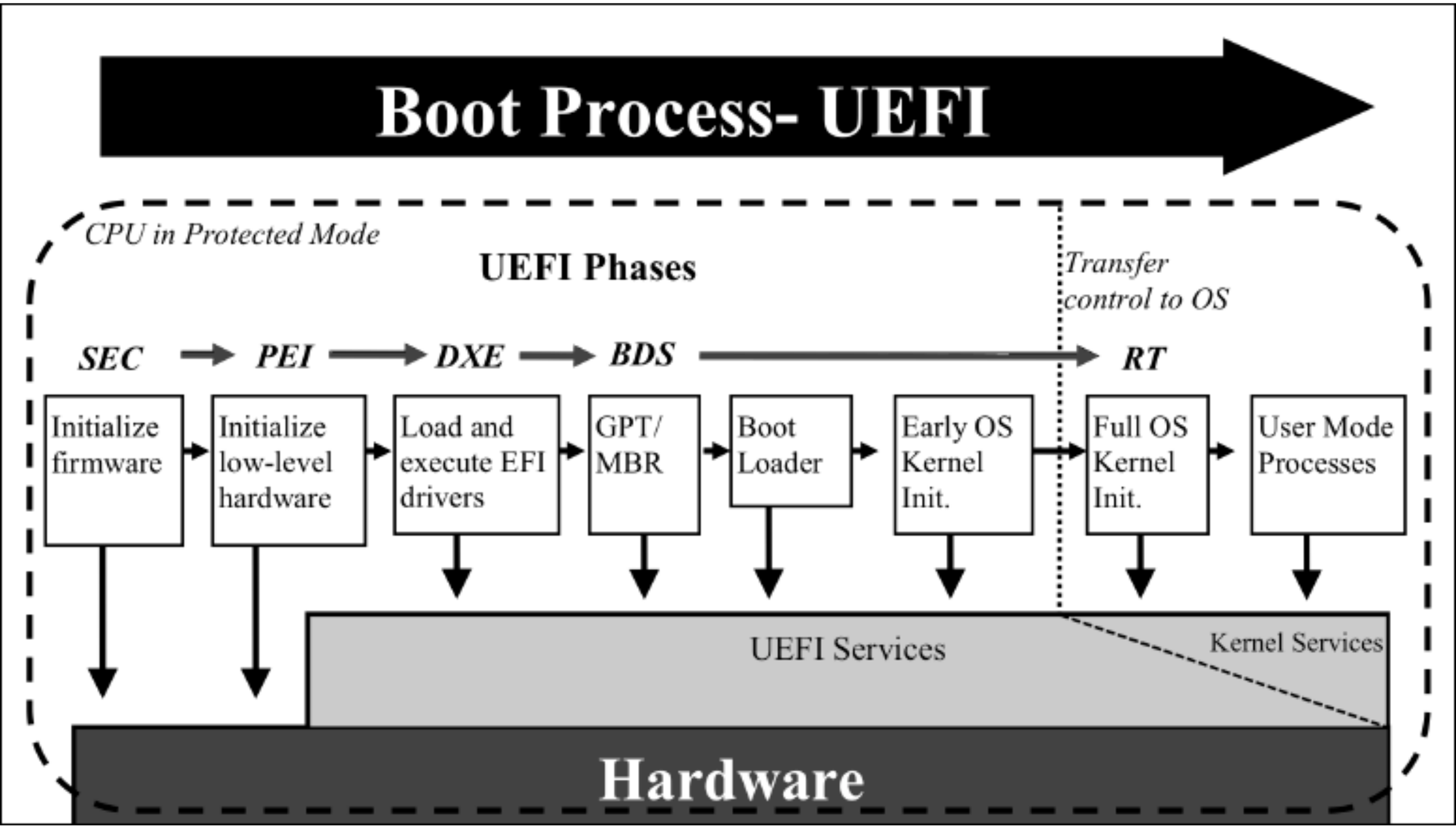
Unified Extensible Firmware Interface

Was ist UEFI?

- BIOS-Ersatz
- Soll die technischen Limitierungen vom PC-BIOS überwinden
- Anfangs bei Intel entwickelt (“Intel Boot Initiative”)
- UEFI Forum (Intel, AMD, IBM, Dell, Apple, Microsoft, Red Hat, …)
- Zunächst auf Intel Macs verwendet (2006)
- Mittlerweile auf “allen” “aktuellen” Mainboards implementiert

UEFI-Architektur

- modular, erweiterbar
- Integriertes Netzwerkmodul
- Integration von Treibern
- Integrierte Kommandozeile
- Compatibility Support Module (BIOS-Emulation)
- GUID Partition Table (GPT) ersetzt MBR
- Secure Boot



[Zimmer, Dasari, & Brogan: The UEFI PI-based Boot Process, 2009, Seite 16]

Secure Boot

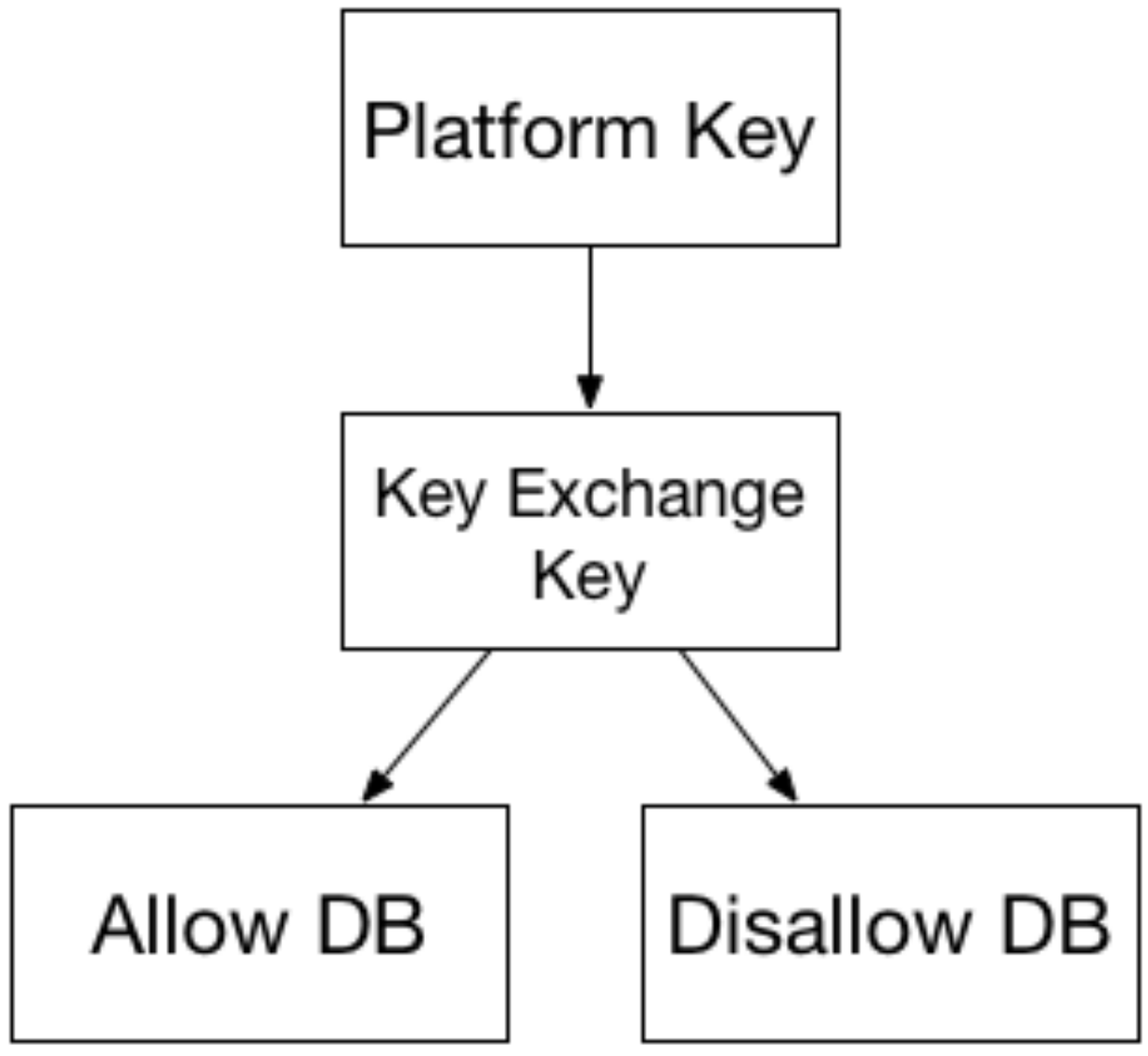
Secure Boot - Ziele

- Sicherer Systemstart
- verhindert das Ausführen unsignierter Binärdateien (Bootloader, Kernel, Kernelmodule)
- verhindert NICHT die Installation von modifizierten Bootloadern

Secure Boot - Architektur

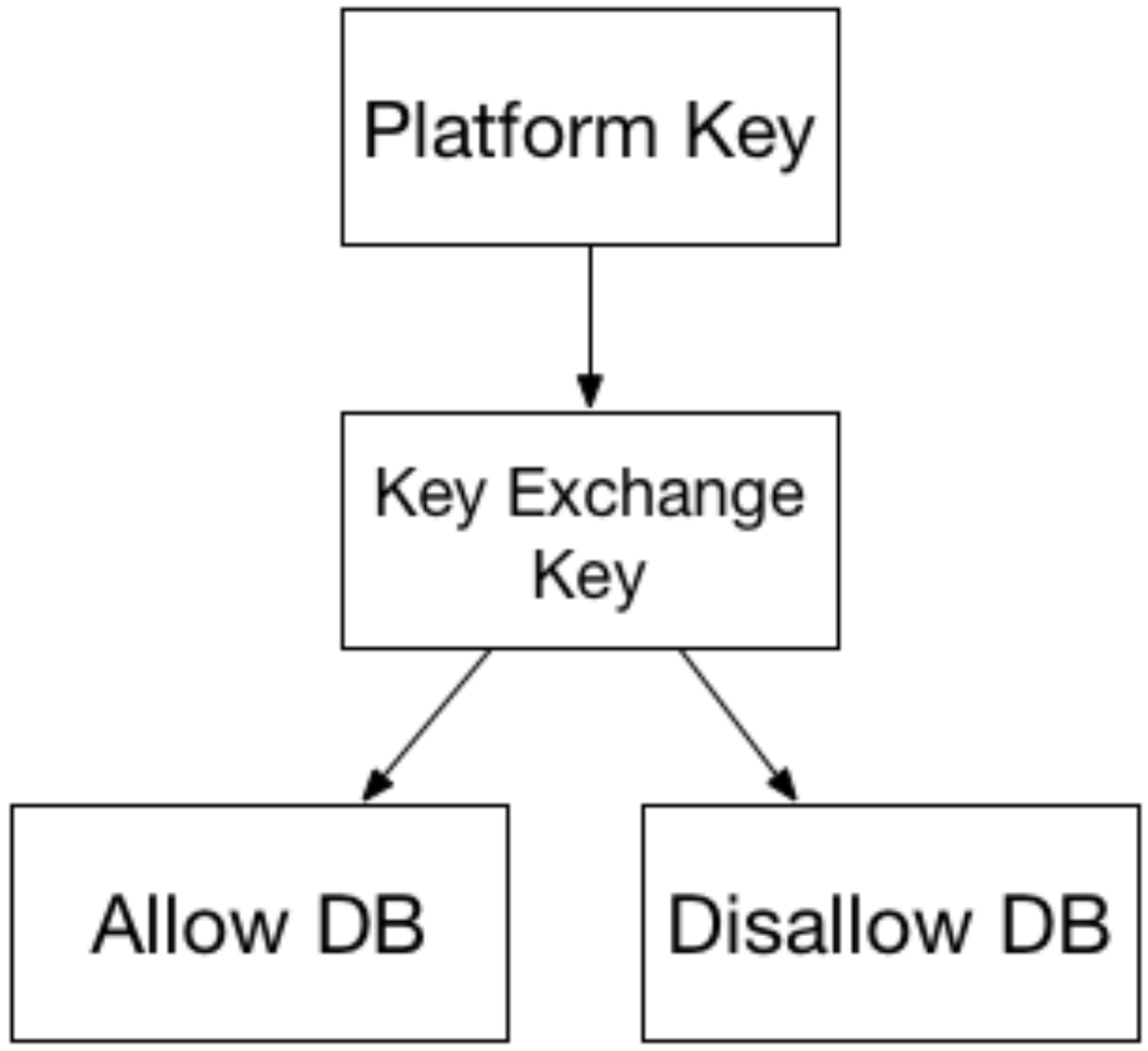
- Programmierschnittstelle für den Zugriff auf Variablen
- X.509-Zertifikate
- Validierung von Bootloader/Treibern durch Signaturen
- Widerruf von Zertifikaten und Signaturen
- Setup- und User-Modus

Secure Boot Variablen



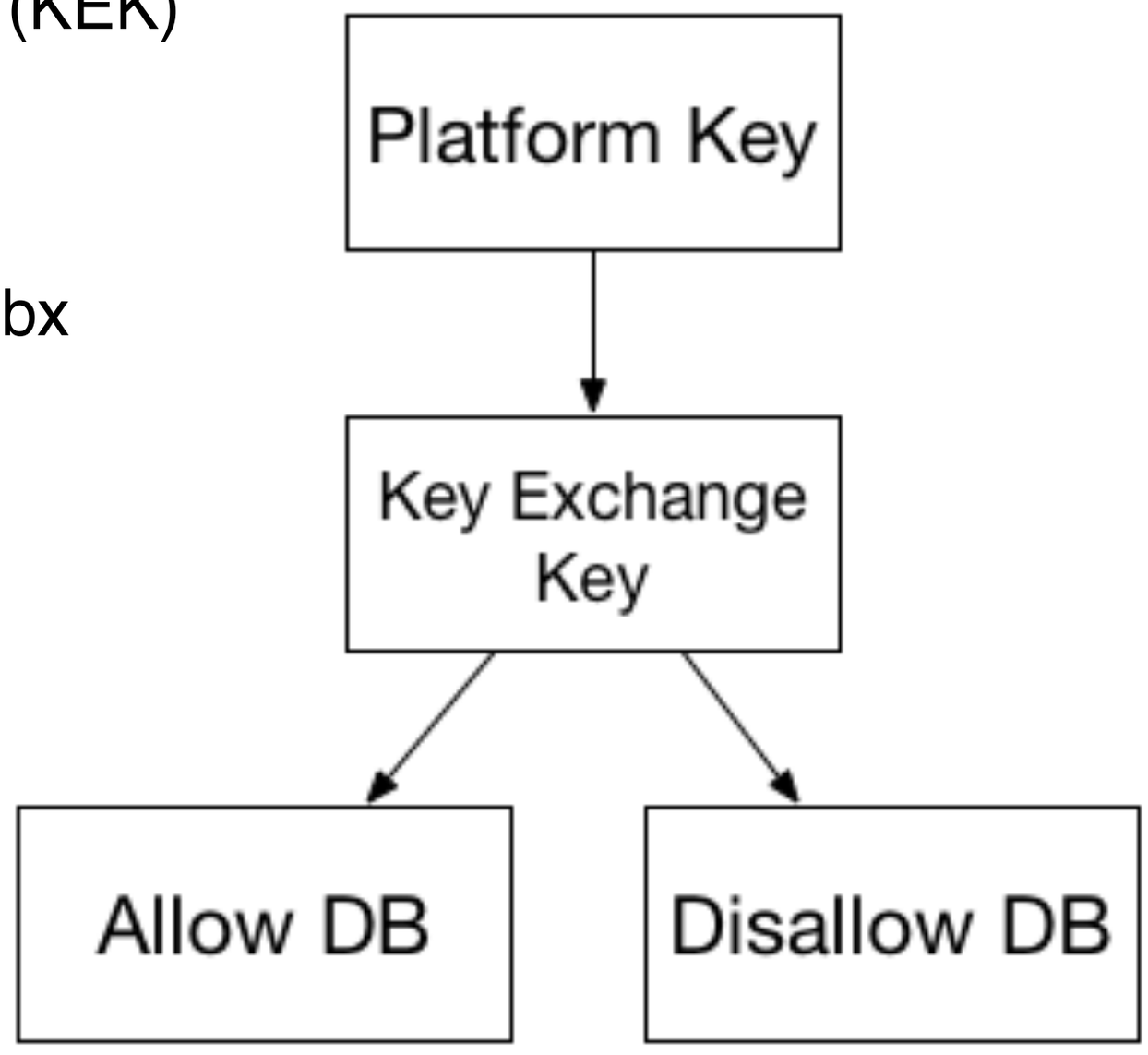
Secure Boot Variablen

- Platform Key (PK)
  - nur ein einzelner PK möglich
  - Schlüssel des Hardware-Herstellers (OEM)
- Erlaubt der Modifikation der KEK
- Löschen -> Setup Mode



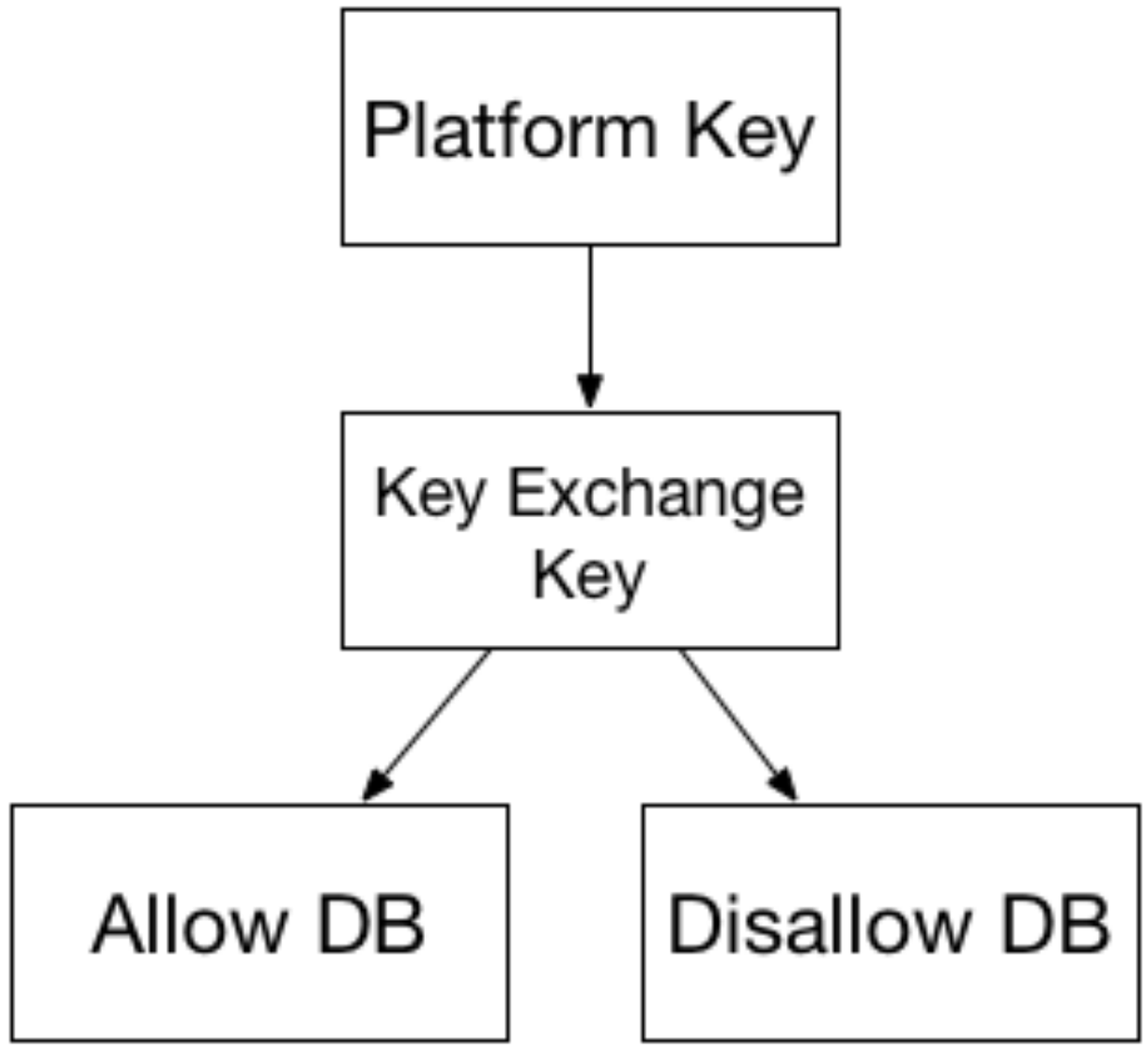
Secure Boot Variablen

- Key Exchange Key Datenbank (KEK)
  - mehrere Zertifikate möglich
  - erlaubt Modifikation von db/dbx



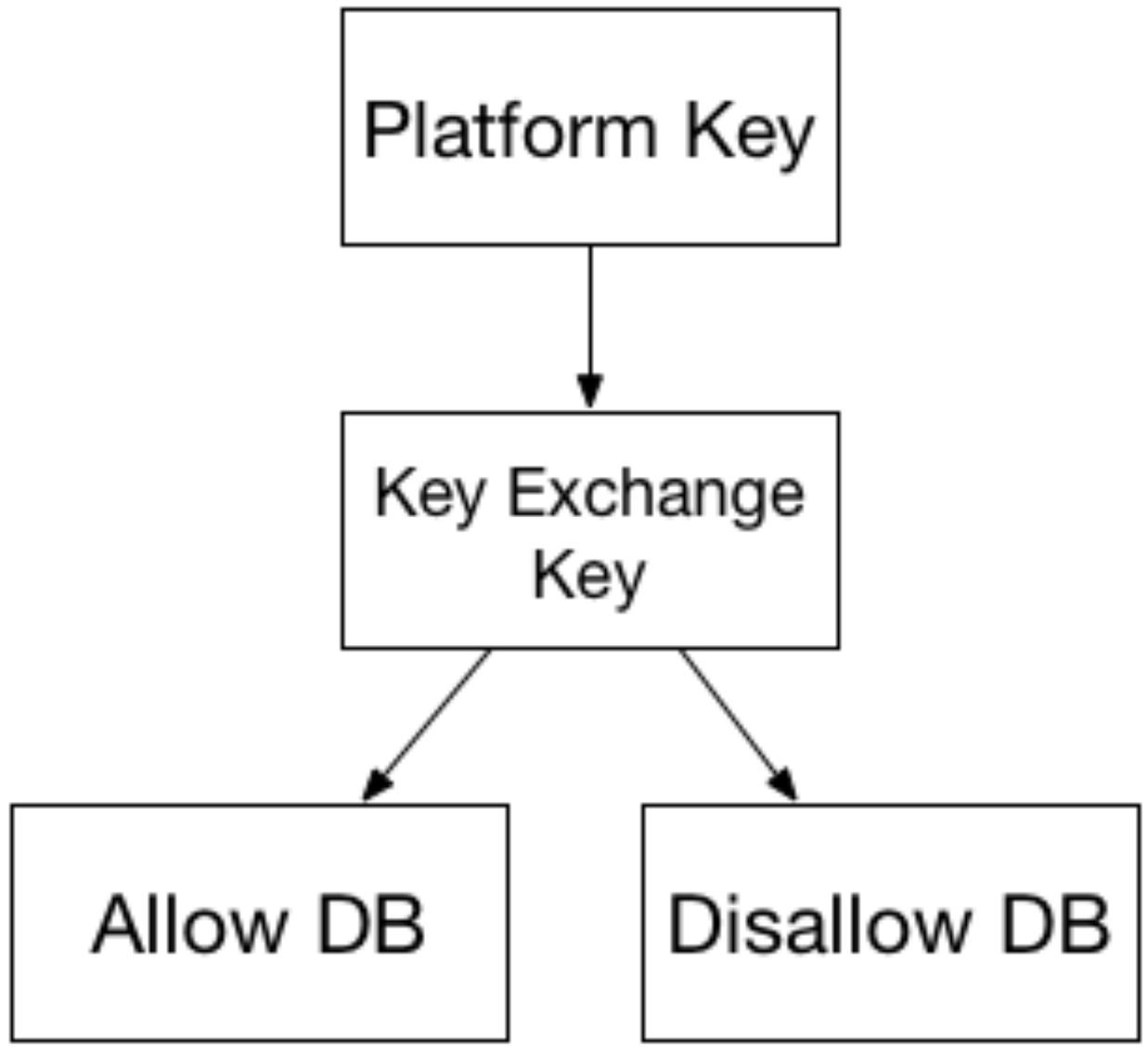
Secure Boot Variablen

- Authorisierte DB (db)
  - Zertifikate und Hashes
  - identifiziert vertrauenswürdige Binärdateien



Secure Boot Variablen

- Nicht authorisierte DB (dbx)
  - Zertifikate und Hashes
  - identifiziert nicht vertrauenswürdige Binärdateien
- hat Vorrang vor db



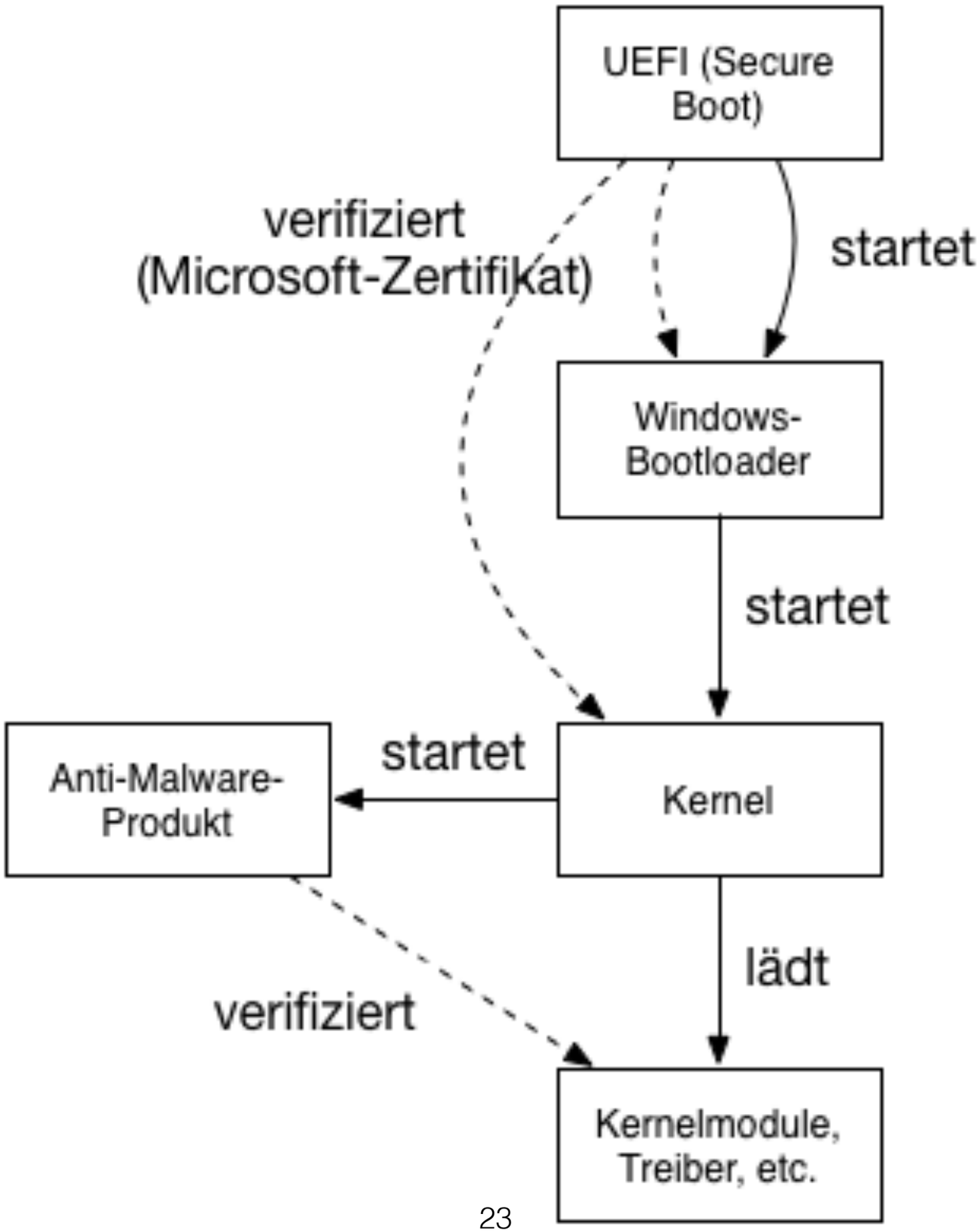
Secure Boot - Modi

- Setup Mode
  - erlaubt Modifikation der Secure Boot Variablen aus dem Betriebssystem heraus
  - dient zur Einrichtung von Secure Boot
- User Mode
  - Modifikation von db/dbx setzt privaten Schlüssel eines Zertifikates im KEK voraus
  - Modifikation von PK/KEK setzt privaten Schlüssel des PK voraus

Secure Boot und Windows 8

Secure Boot und Windows 8

- Vom OEM hinterlegte Schlüssel Voraussetzung für “Windows 8 Logo”
- Secure Boot ist keine Voraussetzung
- Start von kompromittierter Software soll durch Anti-Malware-Produkt verhindert werden
- Vorinstalliert: Windows Defender
- “Early Launch Anti-Malware”-Technik (ELAM)


UEFI (Secure Boot)
verifiziert (Microsoft-Zertifikat)
startet
Windows-Bootloader
startet
Anti-Malware-Produkt
startet
Kernel
lädt
verifiziert
Kernelmodule, Treiber, etc.

Secure Boot und Windows 8

- Sicherheitsgewinn ist vom Anti-Malware-Produkt abhängig
- ELAM kann deaktiviert werden

Secure Boot und Linux

	HP	Dell	Lenovo	Medion
PK	HP UEFI Secure Boot Platform Key	Dell Inc. UEFI Platform Key	Lenovo Ltd. PK CA 2012	MEDION Certificate
KEK	MS KEK CA 2011 HP UEFI Secure Boot Key Exchange Key	MS KEK CA 2011	MS KEK CA 2011 Lenovo Ltd. KEK CA 2012	MS KEK CA 2011
db	MS UEFI CA 2011 MS Windows Production PCA 2011	MS UEFI CA 2011 MS Windows Production PCA 2011	MS UEFI CA 2011 MS Windows Production PCA 2011 ThinkPad Product CA 2012 Hash: 14 e6 ... f4 36	MS UEFI CA 2011 MS Windows Production PCA 2011
dbx	Hash: 00 00 ... 00 00	MS Windows PCA 2010	Hash: 14 e6 ... f4 36	Hash: e3 b0 ... b8 55

[Bundesamt für Sicherheit in der Informationstechnik: Sicherheitsanalyse der UEFI-Integration und „Secure Boot“- Implementierung von Windows 8, Seite 45, abgerufen Dezember 2014]

Secure Boot und Linux

- Problemstellung:
  - OEMs hinterlegen die für das “Windows 8 Logo” notwendigen Schlüssel
  - … und meistens auch nur die
  - fehlende Marktmacht von Linux-Distributoren

Secure Boot und Linux

- Eigener Key Exchange Key
  - OEMs müssten KEK hinterlegen
- Eigener Platform Key
  - aufwändig
  - physischer Zugriff nötig
- Signierung des Bootloaders durch Microsoft

Signierung des Bootloaders durch Microsoft

- Betriebssystem-Hersteller schickt seinen Bootloader an Microsoft
- Microsoft prüft den Bootloader
- Microsoft schickt den signierten Bootloader zurück
- Risiken?

Signierung des Bootloaders durch Microsoft

- Microsoft kann das Zertifikat widerrufen
- Die Signatur ist nur eine bestimmte Zeit gültig

Shim

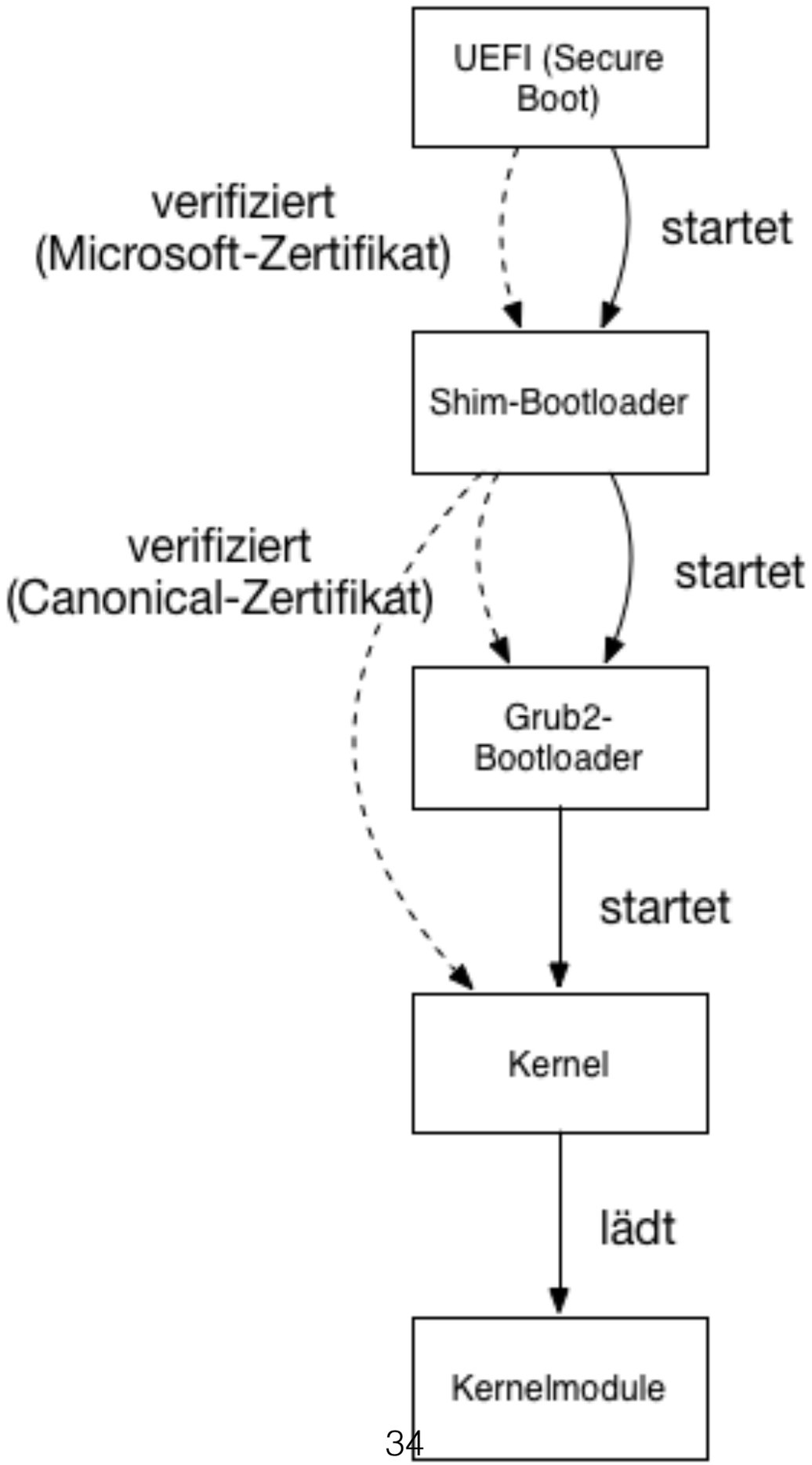
- Open-Source Bootloader
- von Microsoft signiert
- “Bootloader vor dem eigentlichen Bootloader”
- ermöglicht das Ausführen unsignierter Bootloader

Shim

- Verifikation des eigentlichen Bootloaders durch
  - Eintrag in db/dbx
  - eigenen Zertifikats-/Hash-Speicher
  - im Shim-Binary hinterlegtes Zertifikat/Hash

Ubuntu 13.04

- von Microsoft unterschriebener Shim-Bootloader
- Canonical-Zertifikat in Shim-Binary integriert
- eigentlicher Bootloader: Grub2

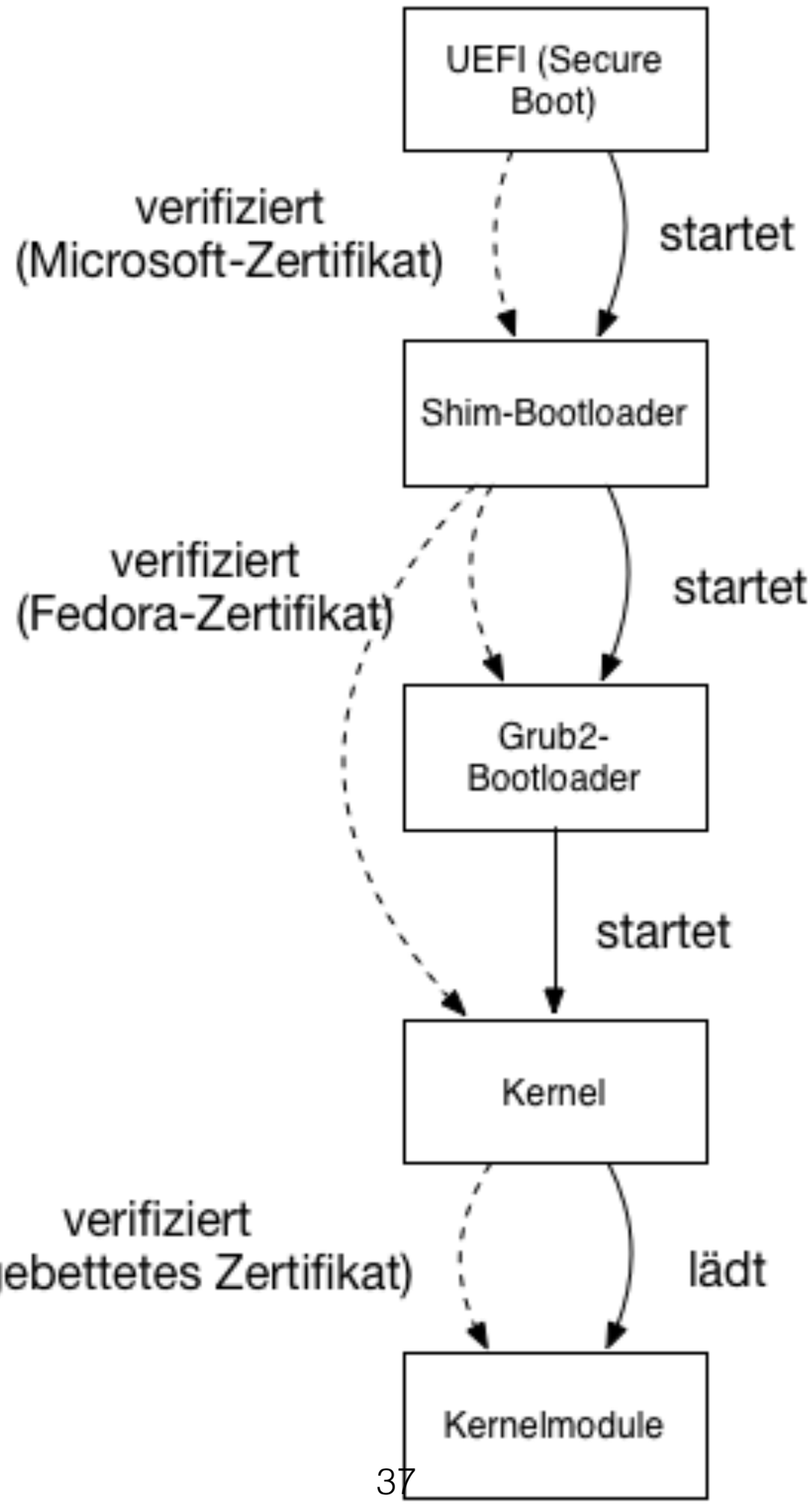

UEFI (Secure Boot)
verifiziert (Microsoft-Zertifikat)
startet
Shim-Bootloader
verifiziert (Canonical-Zertifikat)
startet
Grub2-Bootloader
startet
Kernel
lädt
Kernelmodule

Ubuntu 13.04

- Kernelmodule werden nicht verifiziert
- kein signifikanter Sicherheitsgewinn

Fedora 19

- von Microsoft unterschriebener Shim-Bootloader
- Fedora-Zertifikat in Shim-Binary integriert
- eigentlicher Bootloader: Grub2


UEFI (Secure Boot)
verifiziert (Microsoft-Zertifikat)
startet
Shim-Bootloader
verifiziert (Fedora-Zertifikat)
startet
Grub2-Bootloader
startet
Kernel
verifiziert (eingebettetes Zertifikat)
lädt
Kernelmodule

Fedora 19

- Kernelmodule werden verifiziert
- Sicherheitsgewinn: vorhanden

Secure Boot und Linux

- Debian 7, Red Hat Enterprise Linux 6.4
  - Secure Boot nicht unterstützt
  - kann durch Shim nachgerüstet werden

Risiken und Herausforderungen

Risiken & Herausforderungen

- Kompromittierung kryptographischer Verfahren
  - RSA-2048 bisher sicher
  - Gegen md5 und sha1 sind Kollisionsangriffe bekannt
  - auf starke Crypto-Verfahren achten

Risiken & Herausforderungen

- Kompromittierung von Zertifikatsstellen
  - Zertifikatsstellen stark zentralisiert (Microsoft, OEMs)
  - mehrere Einträge im KEK möglich

AMI BIOS Source Code and UEFI Signing Key Found on Public FTP Server

By Wong Chung Wee on 9 Apr 2013, 11:45am

Risiken & Herausforderungen

- Schwachstellen im Kernel
- Kompromittierung des Userspaces
- Physischer Zugang zum System
- Fehlerhafte Implementierung von UEFI/Secure Boot

Extreme Privilege Escalation: Gefährliche Sicherheitslücken in UEFI-Firmware UPDATE

vorlesen / MP3-Download

Forscher entdeckten Lücken in Intels UEFI-Implementierung, durch die sich Rootkits einschleusen lassen. HP hat daraufhin Firmware-Updates für über 1500 Varianten von PCs, Notebooks, Server etc. veröffentlicht. Das ganze Ausmaß ist noch nicht absehbar.

Eigenes Schlüsselmaterial?

- Wir setzen unseren eigenen Platform Key!
- hoher bis sehr hoher Aufwand
- dafür hoher Sicherheitsgewinn
- im Privaten/kleinen Unternehmen: möglich
- für größere Unternehmen: unrealistisch

Quellen/Literatur

- Sicherheitsanalyse der UEFI-Integration und „Secure Boot“- Implementierung von Windows 8 (BSI)
  - [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/SUSIv8/SUSIv8.pdf] (Dezember 2014)
- BIOS Boot Specification Version 1.01
  - [http://www.intel-assembler.it/portale/5/bios-boot-specification/intel-phoenix-compaq-boot-specification.asp] (Dezember 2014)
- UEFI Secure Boot in Windows 8.1
  - [http://answers.microsoft.com/en-us/windows/forum/windows8_1-security/uefi-secure-boot-in-windows-81/65d74e19-9572-4a91-85aa-57fa783f0759] (Dezember 2014)
- UEFI and the TPM: Building a foundation for platform trust
  - [http://resources.infosecinstitute.com/uefi-and-tpm-2/] (Dezember 2014)