UEFI Secure Boot:
The story behind and where Linux stands

Dr. Udo Seidel
Linux-Strategy @ Amadeus

To my Mum

Agenda

- Introduction
- Keys and Signatures
- Linux and Opportunities
- What else?
- Summary

Introduction

Me ;-)

- Teacher of mathematics & physics
- PhD in experimental physics
- Started with Linux in 1996
- Linux/UNIX trainer
- Solution engineer in HPC and CAx environment
- Head of the Linux Strategy team @Amadeus

Basic Input Output System

- Around for a while
- Insecure
  - Easy to hack
  - Executes anything
- Problems with big disks

(U)EFI

- Unified Extensible Firmware Interface
- First version called EFI
  - HP Itanium systems
  - UEFI kind of EFI NG
- Replaces BIOS
- Emulates BIOS
- See talk from Thorsten Leemhuis

Secure Boot

- Part of UEFI Specification v2.2+
- Addresses BIOS security issues
- Mandate by Microsoft
  - For Windows 8
  - Not only x86
- See keynote from Matthew Garrett

Keys and Signatures

Trust

- Parties
  - Platform
  - Firmware
  - Operating System
- Technique
  - Asymmetric keys
  - Public one part of implementation

Key master

- Platform Key (PK)
- Key Exchange Key (PK)
- Signature database (db)
- Forbidden signature database (dbx)
- Signed EFI executables

EFI instead of ELF

- Subset of PE32 specification
- Portable Executable (PE)
- See also Common Object File Format (COFF)
- PE/COFF header
  - Optional part
  - List of pointers
- Signatures tailing file

Firmware

- Legacy (CSM)
- UEFI
  - Without Secure Boot

    OR
  - With Secure Boot
    - Setup modus
    - User modus

Typical scenario

- Since last autumn
- UEFI Secure Boot
  - Enabled if not even forced
  - Microsoft 'keys' implemented

Linux locked out ?!?

Linux: Options and Opportunities

Options

- Setup modus
- Replace keys
- MS signed Linux bootloader

Option I – Setup modus

- Insecure
- Not always possible
- Facing backward

Option II – Replace keys

- Linux distribution ...
  - ... specific
  - ... independent
- 3rd party support needed
- Tools needed

Replacing keys – more details

- X.509 certificates
- Generation via openssl
- Tools for EFI binary signing
- Multi O/S configuration tricky

Replacing keys – tools

- pesign
- sbsigntools
- efitools

Option III – MS signed bootloader

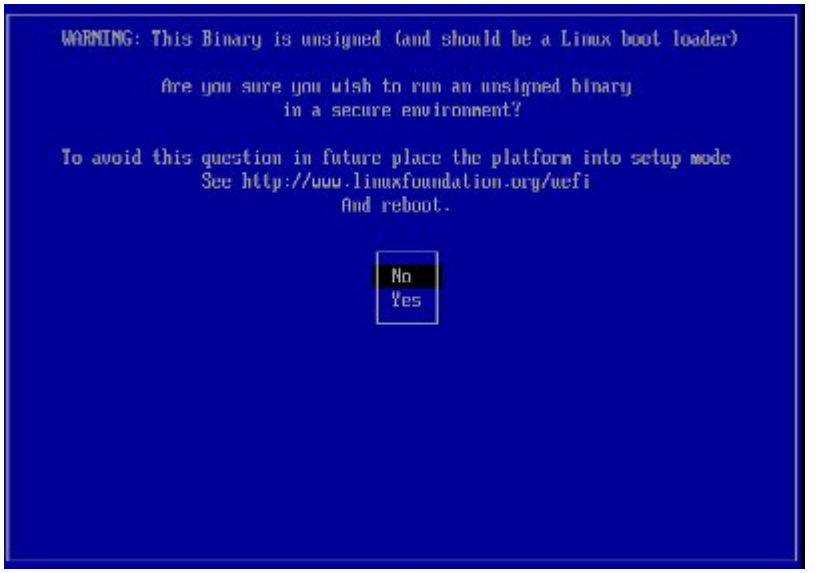
- MS support needed
- Again: Linux distribution ...
  - ... specific
  - ... independent
- Bootloader maintenance?

MS signed bootloader - Idea

- Phased bootloader
- Small & static
- Between UEFI and Linux bootloader

MS signed bootloader – Loader.efi

- Linux Foundation
- To enable ALL Linux bootloaders
- No additional security
- Recently reworked
- Helper tools
  - Preloader.efi
  - Hashtool.efi

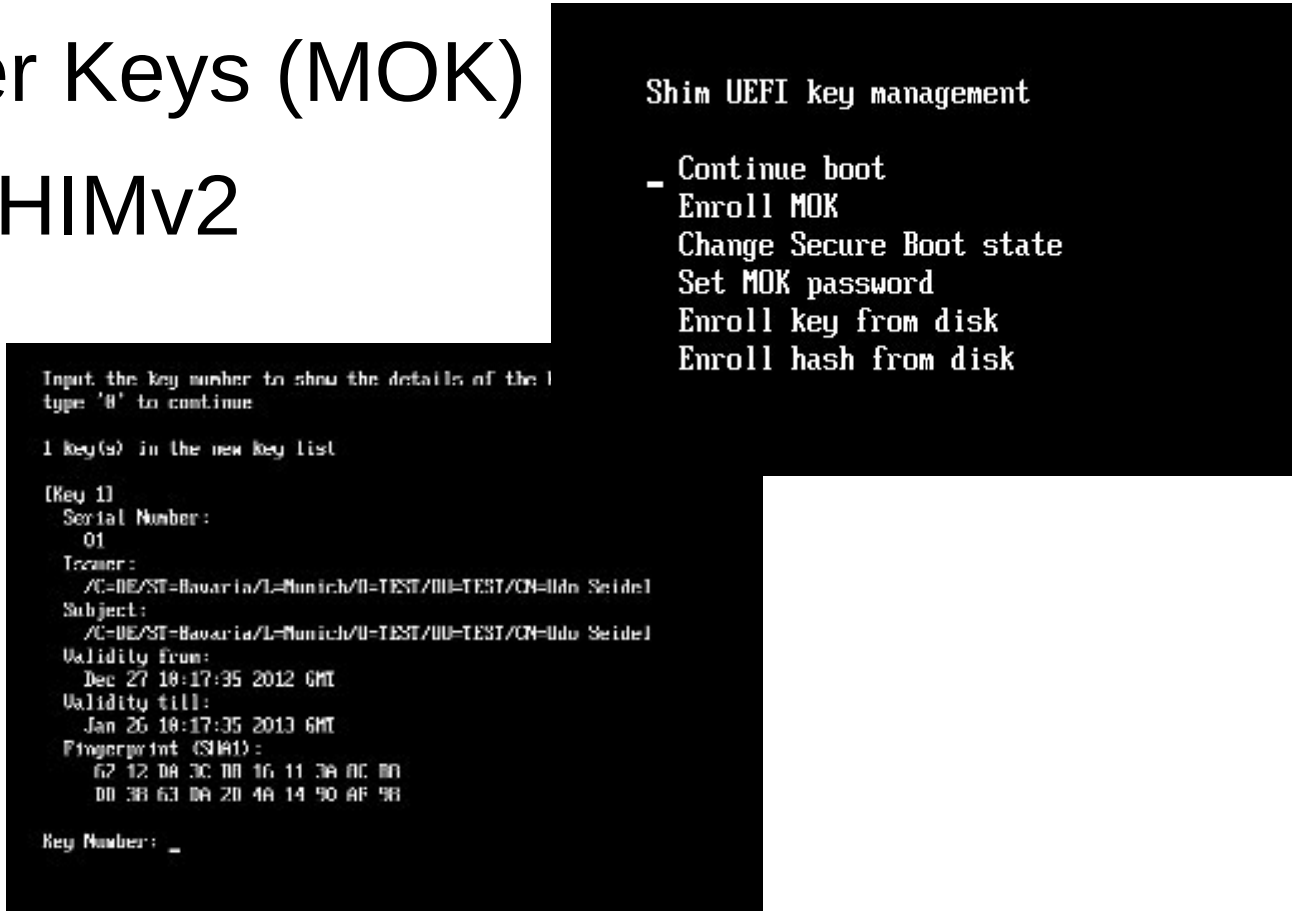


MS signed bootloader – the SHIM

- Originally RedHat'ish
- First version quite static
- Does not support all bootloaders
  - Yes: eLILO, GRUB, GRUB2
  - No: Gummiboot, efilinux

Machine Owner

- Originally from SUSE
- Machine Owner Keys (MOK)
- Integrated in SHIMv2



Extending SB trust chain

- Several certificates
  - Microsoft
  - Linux distribution
- Signed bootloader
- Signed kernel core binary
- Signed kernel modules
- ..?!?

Distributor approaches

- Enterprise
  - In place: Ubuntu LTS
  - Announced: SUSE
  - Unknown: RedHat, Oracle

- Community
  - In place: Ubuntu, Fedora, openSUSE, ...
  - Announced: ...
  - Unknown: Debian and derivatives

What else?

ARM

- UEFI Forum since 2008
- More strict Microsoft mandate
- UEFI ARM boards available but ...

Problems

- Samsung: firmware death
- Toshiba: Missing keys
- Lenovo: Only Windows 8 and RHEL
- Microsoft: leaked keys

Summary

Take aways

- Linux almost ready
  - In general
  - Enterprise sector
- Opportunity not pain
- Homework to be done

References

- http://www.uefi.org
- http://mjg59.dreamwidth.org
- http://blog.hansenpartnership.com
- http://www.sxc.hu

Thank you!

UEFI Secure Boot:
The story behind and where Linux stands

Dr. Udo Seidel
Linux-Strategy @ Amadeus