Linux Day 2012

27 OTTOBRE 2012
FERMO - BUC Machinery

Secure Boot

La fine di GNU/Linux sui Desktop?

Andrea Colangelo

Ubuntu Developer – Debian Maintainer

FermoLUG
Gruppo Utenti Linux
del Fermano

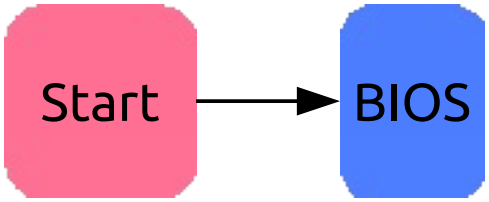
www.linuxfm.org

Il Boot

Start

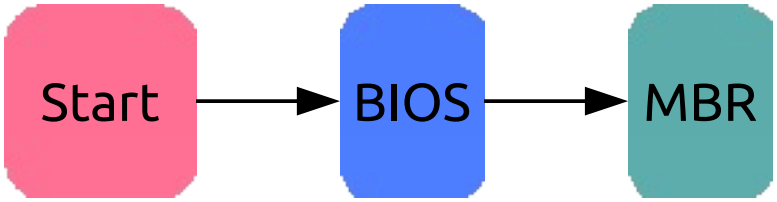
T0 Accensione CPU

Il Boot



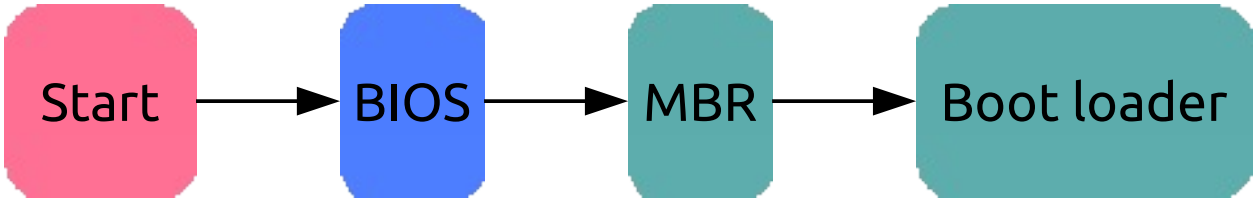
T+2 POST, Avvio BIOS

Il Boot



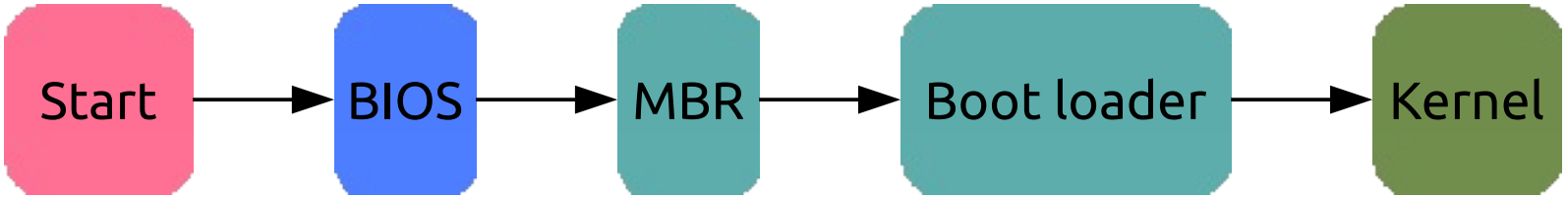
T+2.1 Primo stadio del boot loader (*MBR, settore 0 HD*)

Il Boot



T+3 Secondo stadio del boot loader (*partizione di boot)*

Il Boot

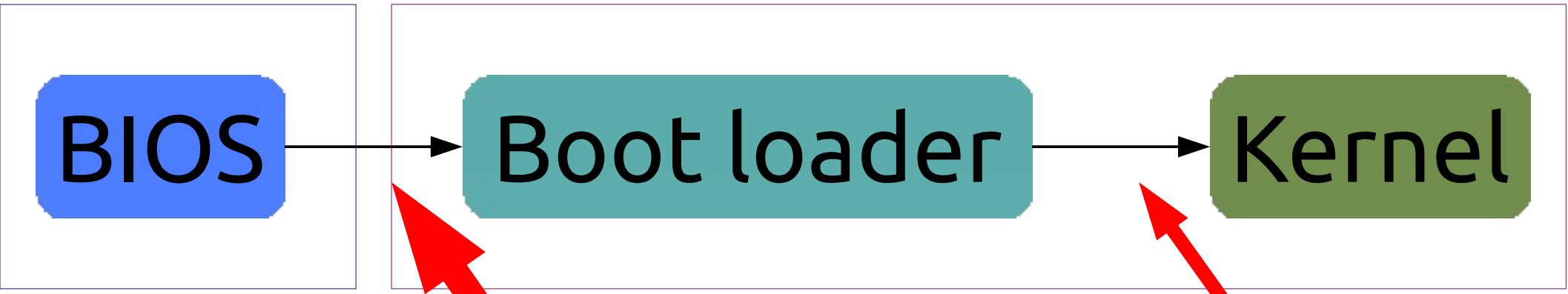


T+6 Esecuzione kernel

Il Boot

T+∞ Completamento avvio OS

Il Boot, semplificato :)



Scheda madre
Non modificabile
OS-indipendente

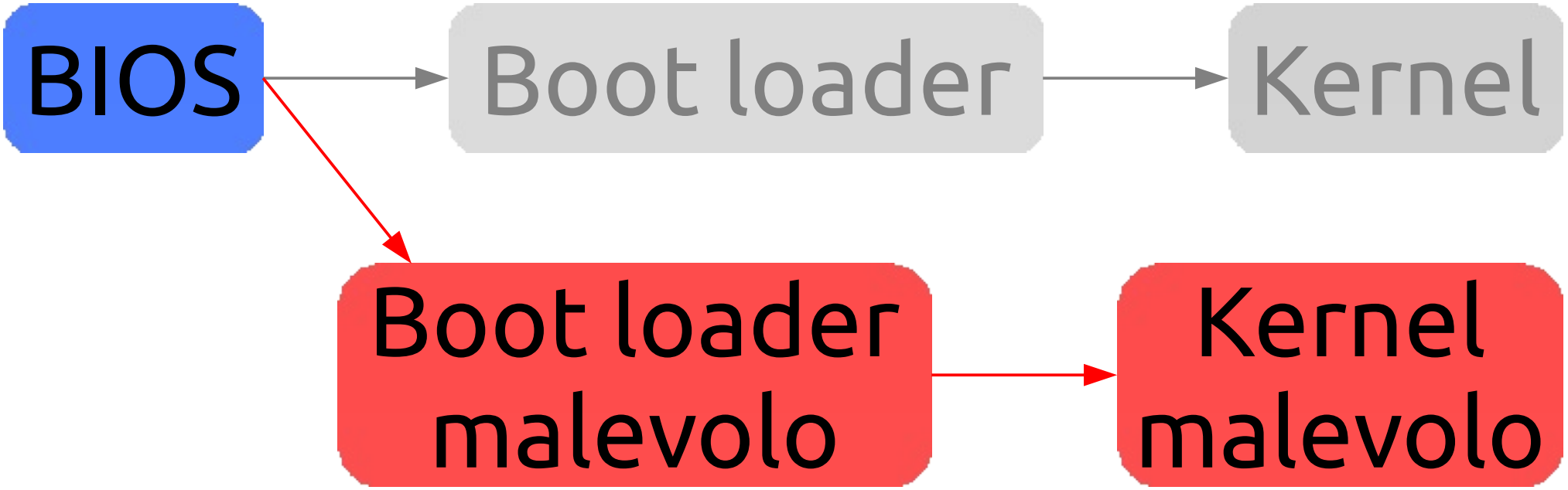
Hard Disk
Modificabile
OS-dipendente

...e anche
questo!

Questo punto
è critico!

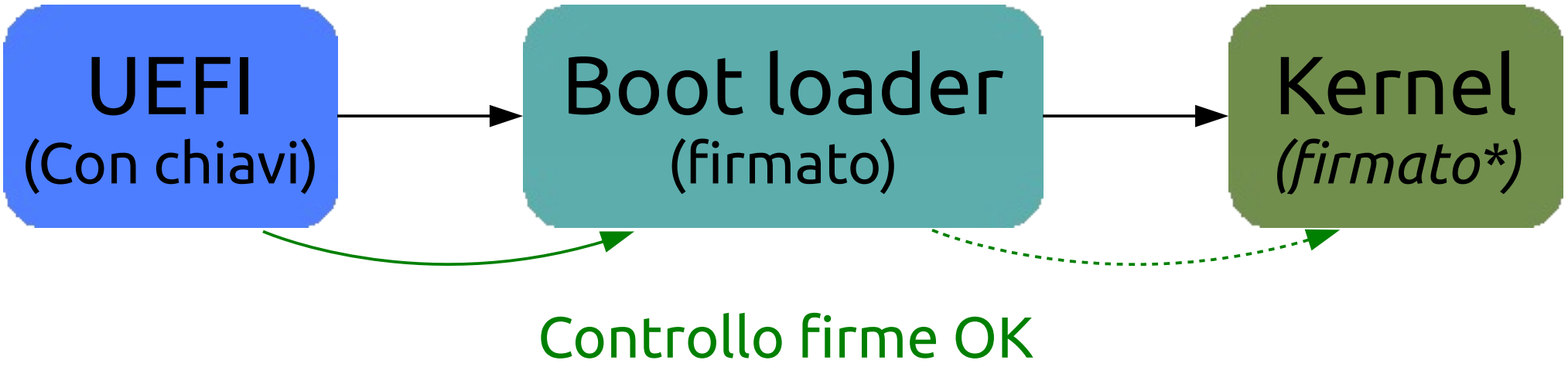
Bootkit

Bootkit


BIOS
Boot loader
Kernel
Boot loader
malevolo
Kernel
malevolo

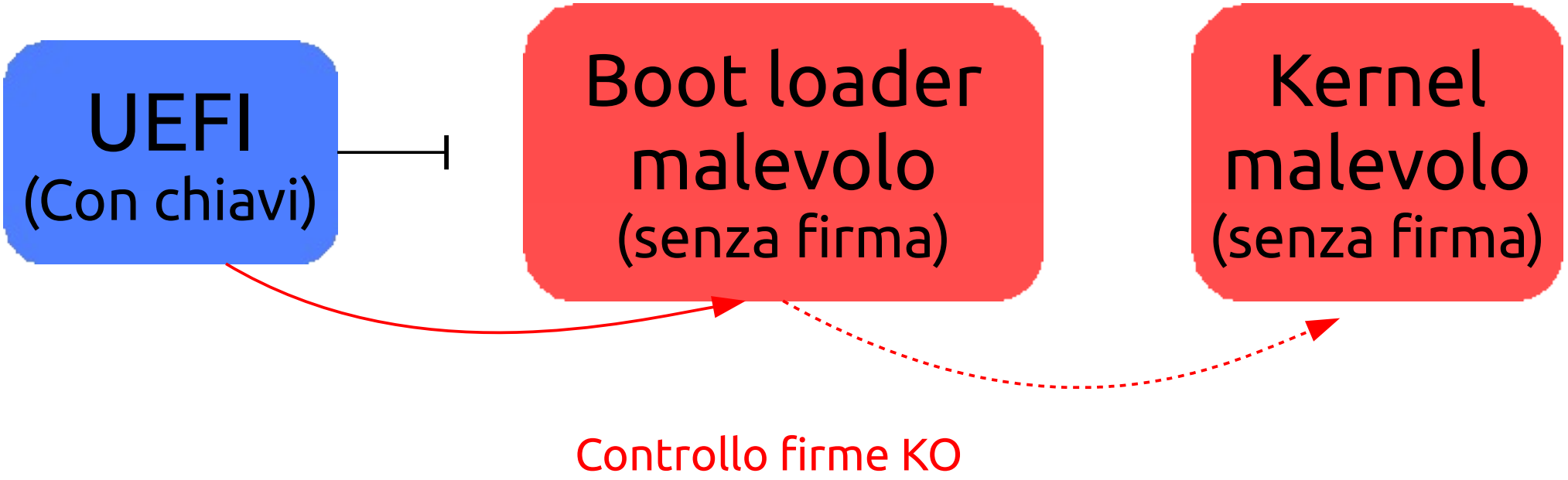

ASUS EFI BIOS Utility - Advanced Mode
Exit
Main
Ai Tweaker
Advanced
Monitor
Boot
Tool
BIOS Information
BIOS Version 1053 x64
Build Date 01/03/2011
EC Version MBECE-0017
ME Version 7.0.1.1141
CPU Information
Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz
Speed 3519 MHz
Memory Information
Total Memory 8192 MB
Speed 1648 MHz
System Language English
System Date [Monday 01/17/2011]
System Time [13:55:17]
Access Level Administrator
Security
Choose the system default language
UEFI
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F5: Optimized Defaults
F10: Save ESC: Exit
Version 2.00.1201. Copyright (C) 2010 American Megatrends, Inc.

Secure Boot

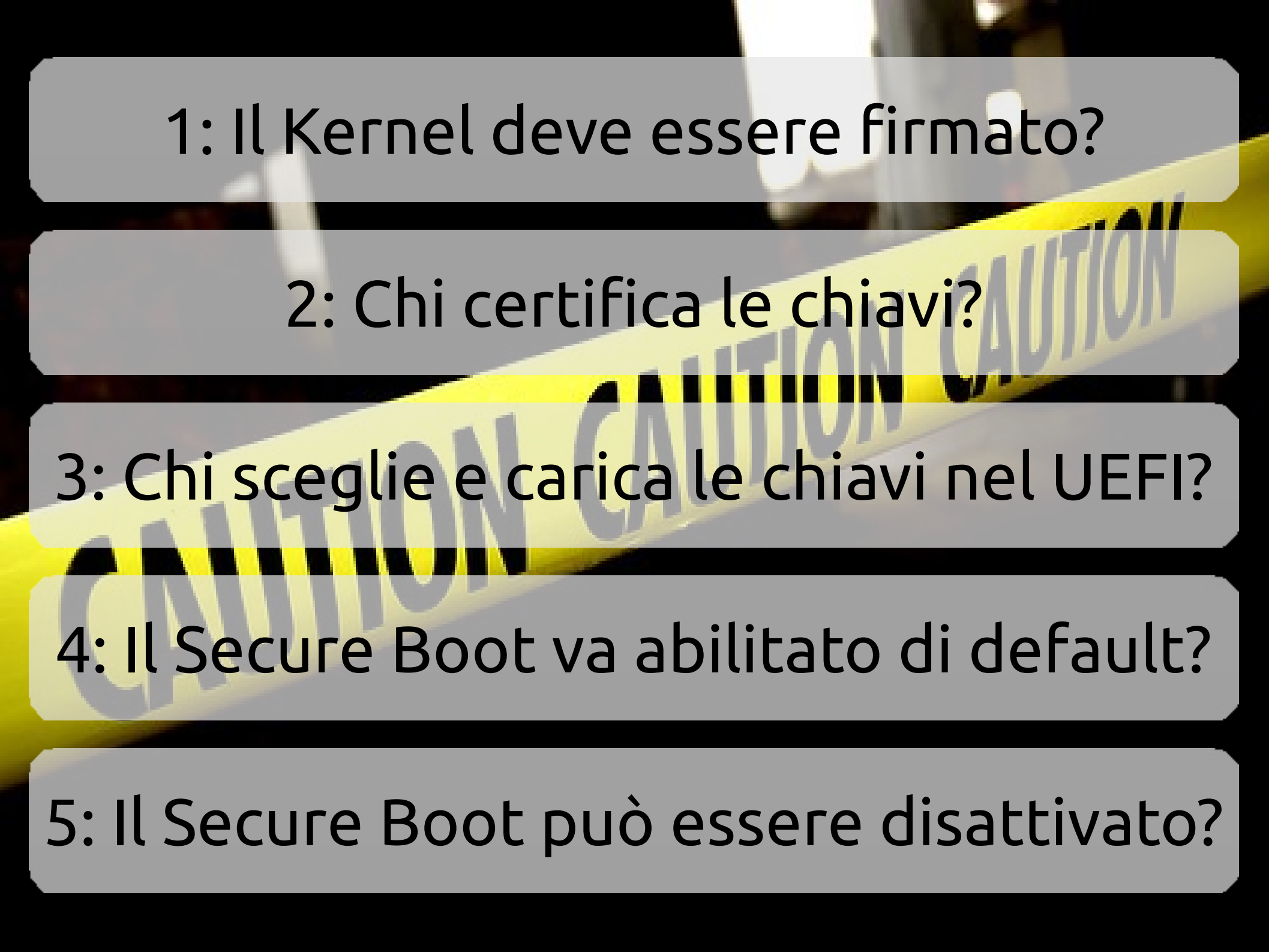


(*non obbligatorio)

Secure Boot


UEFI
(Con chiavi)
Boot loader
malevolo
(senza firma)
Kernel
malevolo
(senza firma)
Controllo firme KO

E vissero tutti felici e contenti?


1: Il Kernel deve essere firmato?
2: Chi certifica le chiavi?
3: Chi sceglie e carica le chiavi nel UEFI?
4: Il Secure Boot va abilitato di default?
5: Il Secure Boot può essere disattivato?
CAUTION CAUTION CAUTION

1: Il Kernel deve essere firmato?

UEFI impone firme solo
fino a ExitBootServices()

2: Chi certifica le chiavi?

UEFI non prevede un'authority centrale

3: Chi sceglie e carica le chiavi nel UEFI?

La responsabilità
è dei vendor...

...ma chiave Microsoft è imposta
da Certificazione Windows 8

4: Il Secure Boot va abilitato di default?

UEFI:
Nessuna indicazione

Microsoft:
Sì, obbligatorio

5: Il Secure Boot può essere disattivato?

UEFI:
Nessuna indicazione

Microsoft:
Sì, obbligatorio...

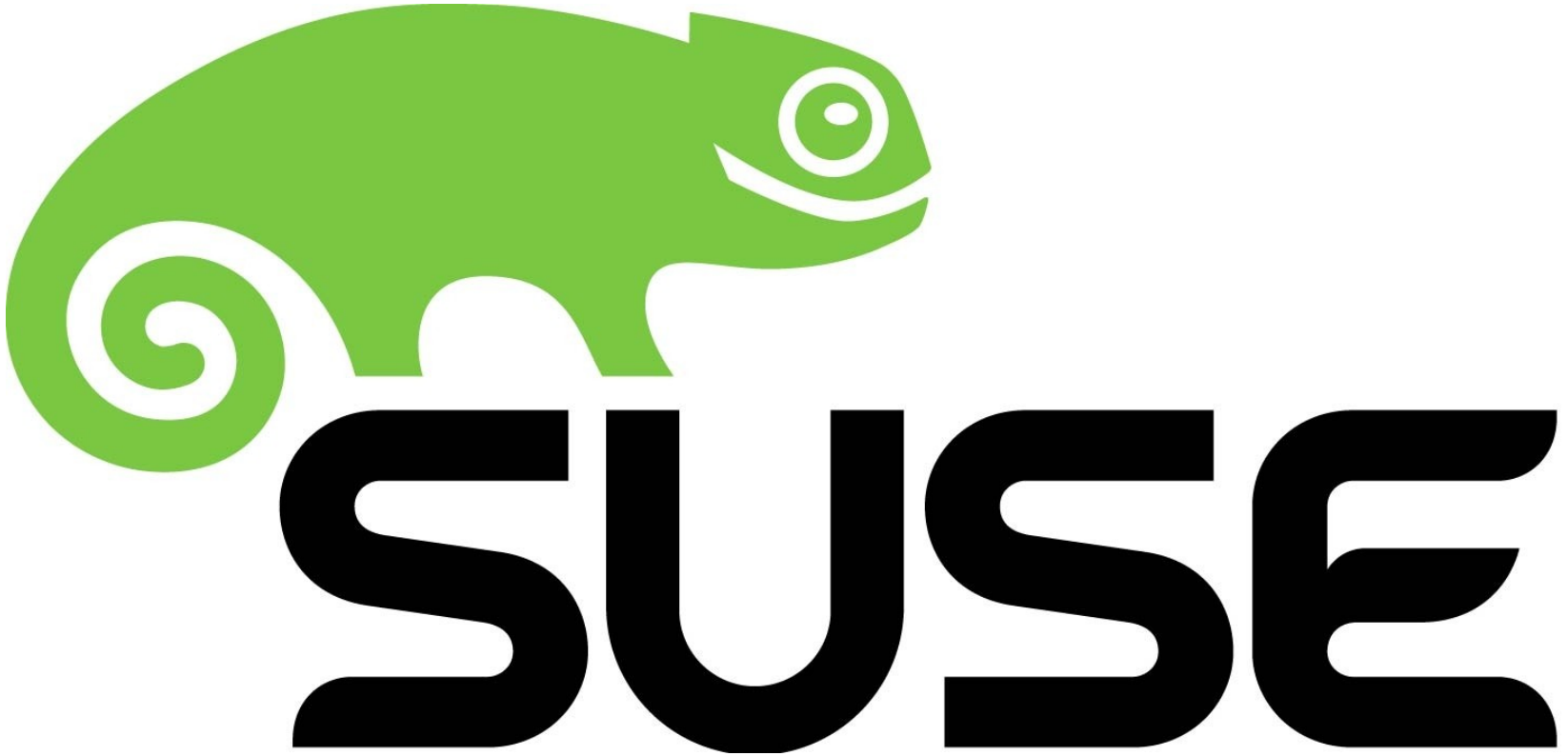
...ma non su ARM!


...e Linux?

- Fedora 18 firma il boot loader con la chiave Microsoft
- Boot loader: Shim + GRUB2
- Kernel e moduli firmati con chiave Fedora
- Piani identici per RHEL

ubuntu

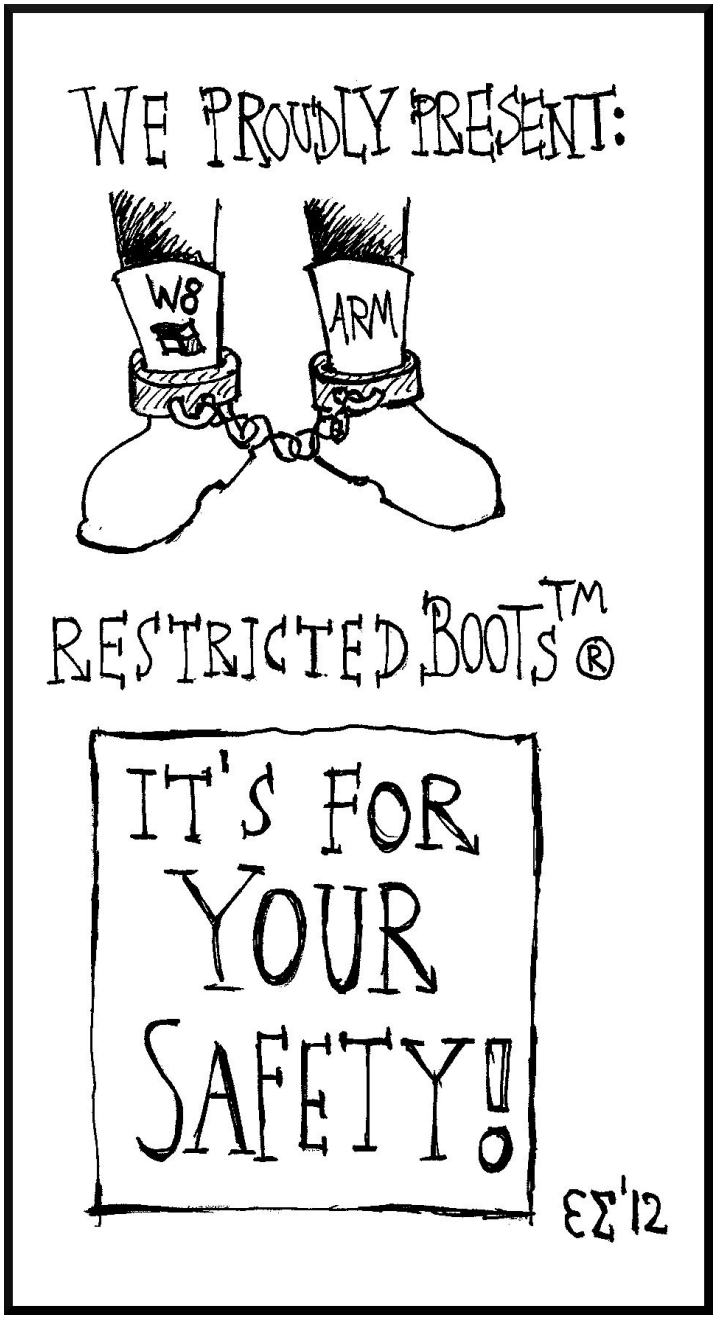
- Macchine Ubuntu Certified:
  chiave Ubuntu + chiave Microsoft
- ISO: firmate con chiave Microsoft
- Boot loader: GRUB2
- Kernel e moduli non firmati



- Piani solo per SUSE Linux Enterprise
- Shim firmato da MS, con database chiavi
- GRUB2 + Kernel firmati con chiavi nel db

- Pre-Bootloader firmato con chiave Microsoft
- Pre-Bootloader avrà un “Present User” test
- Pre-Bootloader caricherà un Boot loader (e kernel) non firmato

Restricted Boot :)



http://www.fsf.org/campaigns/secure-boot-vs-restricted-boot

Per approfondire:

Il blog di Matthew Garrett:
http://mjg59.dreamwidth.org

White paper RedHat/Canonical:
http://ozlabs.org/docs/uefi-secure-boot-impact-on-linux.pdf

Fedora
http://mjg59.dreamwidth.org/12368.html

Ubuntu
https://lists.ubuntu.com/archives/ubuntu-devel/2012-June/035445.html
http://tinyurl.com/cmynf2q

SUSE
https://www.suse.com/blogs/uefi-secure-boot-details/

Linux Foundation
http://tinyurl.com/9ccumyv

Andrea Colangelo

warp10@ubuntu.com
http://andreacolangelo.com