

Secure Boot

La fine di GNU/Linux sui Desktop?

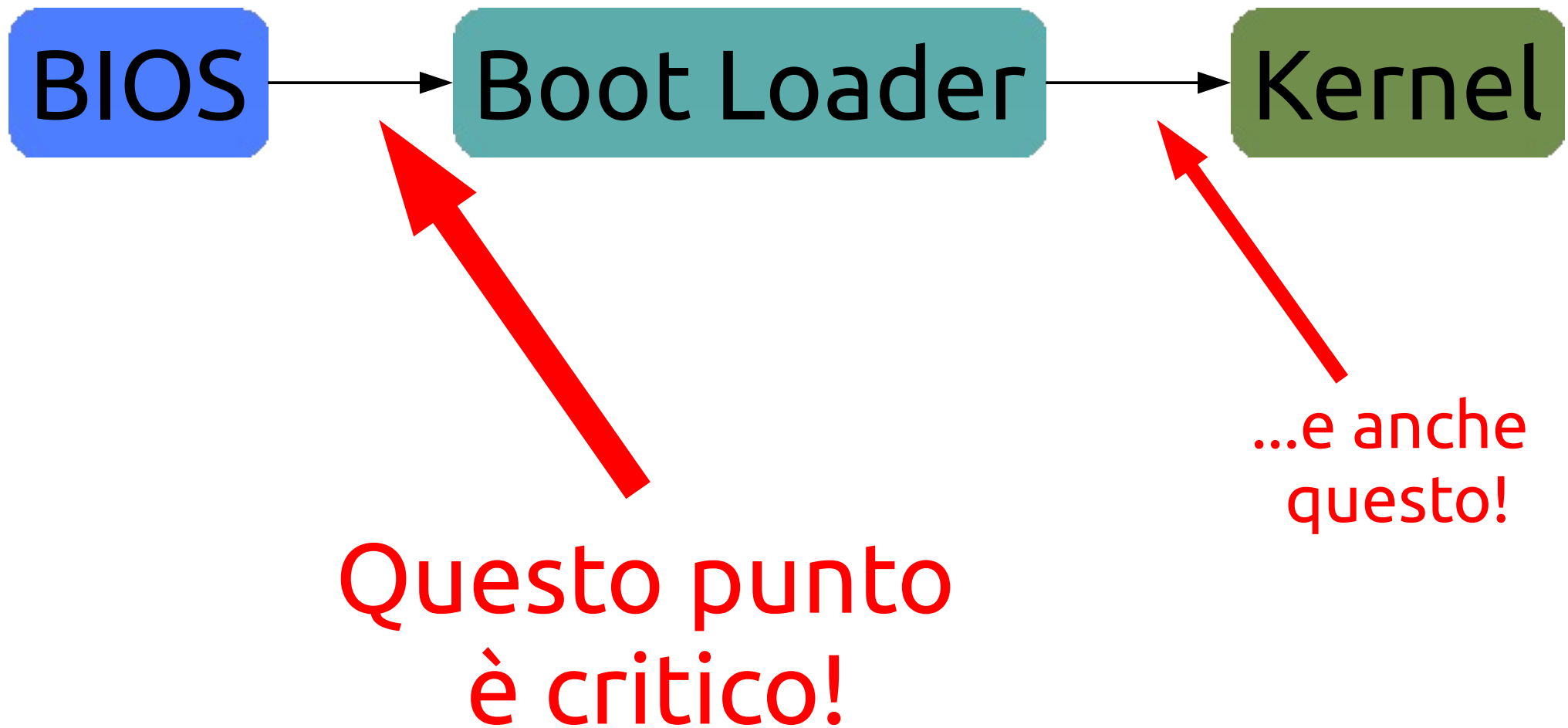
Ubuntu-it Meeting
Bologna, 17 novembre 2012

Andrea Colangelo
Ubuntu Developer

Il Boot



Il Boot, semplificato :)



Bootkit

BIOS

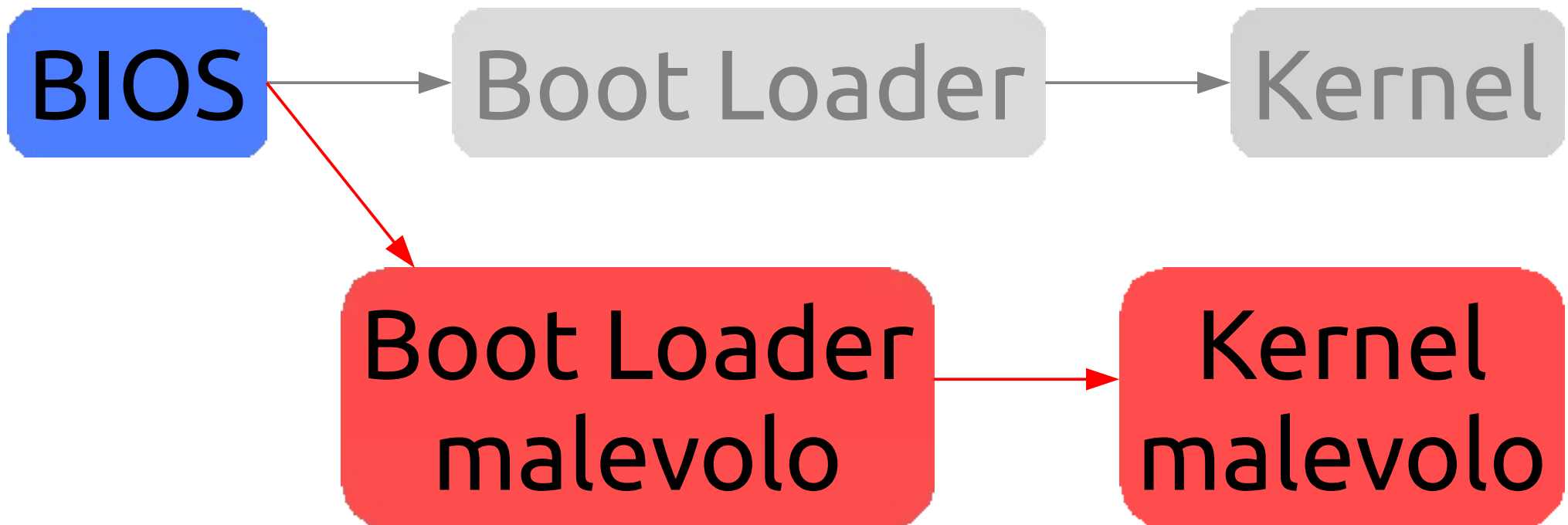


Boot Loader



Kernel

Bootkit





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

Secure Boot



(*non obbligatorio)

Secure Boot





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?

1: Il Kernel deve essere firmato?

UEFI impone firme solo
fino a `ExitBootServices()`

2: Chi certifica le chiavi?

UEFI non prevede
un'autorità 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?

fedoraTM



- Fedora 18 firma il bootloader con la chiave Microsoft
- Bootloader: 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
- Bootloader: shim + GRUB2
- Kernel e moduli non firmati



SUSE

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

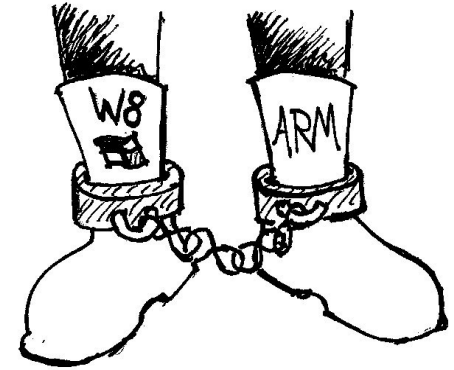


- Pre-Bootloader firmato con chiave Microsoft
- Pre-Bootloader avrà un “Present User” test
- Pre-Bootloader caricherà un Bootloader (e poi kernel) non firmato



Restricted Boot :)

WE PROUDLY PRESENT:



RESTRICTED BOOTSTM®

IT'S FOR
YOUR
SAFETY!

ES'12

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

Per approfondire...

Il blog di Matthew Garrett:

<http://mjg59.dreamwidth.org10>

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>