



Bezpečné používání linuxového desktopu

Martin Vicián • martin.vician@nic.cz • [/ptvician](https://twitter.com/ptvician) • vician.cz

LinuxDays 2018 • 7. října 2018



Bezpečné používání linuxového desktopu

Martin Vicián • martin.vician@nic.cz • [/ptvician](https://twitter.com/ptvician) • vician.cz

LinuxDays 2018 • 7. října 2018

Máte na Linuxu antivirus? A mohla bych ho vidět?



sed -i 's|Linux|GNU/Linux|g' *

Martin Vicián

Systemový administrátor



90% notebooků na Linuxu

Člen



vpsFree.cz

Úvod do Linuxu



Implicitně:



16.04 (Unity) a 18.04 (Gnome 3)

Stačí stáhnout?

Zrcadla



launchpad.net/ubuntu/+cdmirrors

Linux Mint

2016: Beware of hacked ISOs if you downloaded Linux Mint on February 20th!

- hacknutý WordPress a phpBB
- změněné ISO - přidán Malware
- MD5 kontrolní součty



Verify your ISO

- Kontrolní součet
 - Podpis (PGP)
-
- <https://tutorials.ubuntu.com/tutorial/tutorial-how-to-verify-ubuntu>
 - <https://linuxmint.com/verify.php>
 - <https://getfedora.org/verify>
-
1. Stáhnout dodatečné soubory: kontrolní součet a podpis
 2. Získat PGP klíč
 3. Ověřit kontrolní součet
 4. Ověřit podpis kontrolního součtu

NÁVOD, JAK S POMOCÍ PGP OVĚŘIT,
ŽE JE DANÝ EMAIL DŮVĚRYHODNÝ:

ZKONTROLUJTE, ZDA
MAIL ZAČÍNÁ TAKTO



POKUD ANO, JE EMAIL ZŘEJMĚ V POŘÁDKU.

Kolik můžu zadávat hesel při bootu?

1. Heslo k odemknutí BIOSu
2. Heslo k odemknutí disku
3. Heslo k odšifrování disku (LUKS)
4. Heslo k přihlášení do systému
5. Heslo k odemknutí klíčenky
6. . . .

A která dávají smysl?



BIOS a disk heslo (Dell)

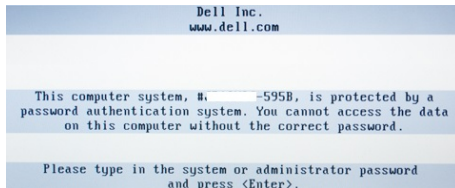
BIOS

- Master heslo odemkne BIOS



Disk

- Master heslo smaže a odemkne disk



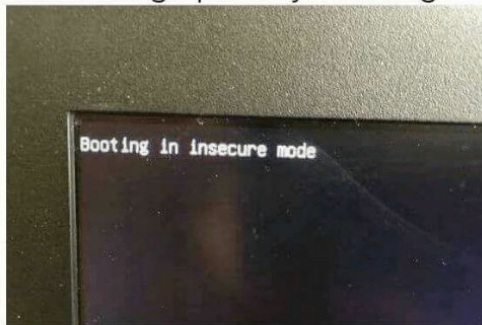
<https://bios-pw.org/>

CTRL+ENTER

Secure Boot (UEFI)

- Byl objeven škodlivý kód LoJax útočící na UEFI. Řadí i ve střední Evropě (lupa.cz)
- Secure Boot má chránit před zavedením necertifikovaného operačního systému
- Canonical (Ubuntu) má v UEFI klíče
- Lze podepsat vlastními klíči

Me waking up every morning



Secure Boot (UEFI) - instalace

- Ubuntu z továrny (a to chcete?)
- Při instalaci většinou ručně vypínáme (3rd party)
- Přeinstalace nemění stav Secure Bootu

Install third-party software for graphics and Wi-Fi hardware, Flash, MP3 and other media

This software is subject to license terms included with its documentation. Some is proprietary.

Fluendo MP3 plugin includes MPEG Layer-3 audio decoding technology licensed from Fraunhofer IIS and Technicolor SA.

Installing third-party drivers requires turning off Secure Boot. To do this, you need to choose a security key now, and enter it when the system restarts. [Learn more...](#)

Turn off Secure Boot

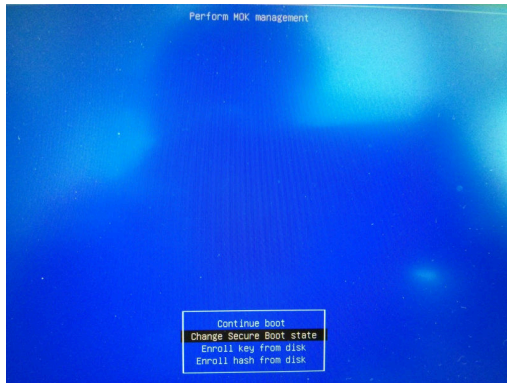
Choose a password: Good password

Confirm your password: ✓

Secure Boot (UEFI) - ruční zapnutí

```
sudo mokutil --enable-validation
```

- jednorázové heslo 8 - 16 znaků
- restart počítače
- MOK - máte 10 vteřin
- Change Secure Boot state
- tři náhodné znaky z dočasného hesla



Thunderbolt 3

Zařízení:

- Dell Thunderbolt Dock (TB16)
- Thunderbolt adaptér

Periferie:

- Ethernet
- HDMI, VGA, DisplayPort
- USB (3.0)

- Bezpečnostní nastavení v BIOSu:
 - **none**
 - **dponly** - Display Port a USB
 - **user** - uživatel řeší ručně
 - **secure** - jako **user**, navíc umožňuje uložit pro pozdější identifikaci

DMA (direct memory access) útok



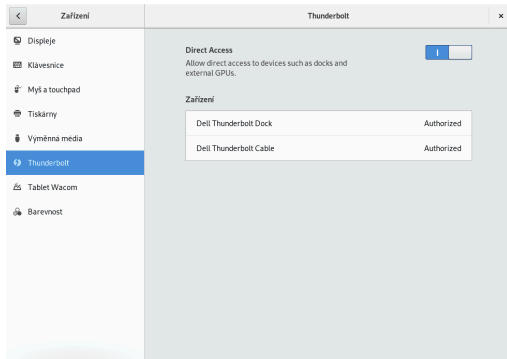
Thunderbolt 3

Správa:

- bolt (bo1tct1) - GUI v Gnome3:
 - user level je třeba schvalovat po každém bootu
- thunderbolt-tools
 - tbtadm

Problémy:

- zadávání hesel, např. LUKS (USB klávesnice)
- ethernet připojení
- pomalá autorizace



Deepin

- První verze únor 2004
- Poslední verze spren 2018
- Stojí na Debian unstable
- Vyvíjí: *Wuhan Deepin Technology Co., Ltd.*
- Vlastní Deepin Desktop Environment (DDE) v Qt
- Nejpopulárnější distribuce v Číně
- 23. distribuce na distrowatch (posledních 12 měsíců)



K zamyšlení

- Chybí podpisy checksum souborů
- Stahování několik dní, nebo:
 - zrcadla
 - mega.nz, drive.google.com, ...
- Nejde zvolit celošifrovaný disk (LUKS)
- Nekontroluje sílu hesla
- Nemá `systemd-resolved`
- Automaticky spuštěná samba



K zamyšlení

- Nainstalovaný gnome-keyring, ale ne seahorse
- Obsahuje nestandardní balíky
 - google-chrome: nainstalovaný a podepsaný Google klíči
 - spotify: přidalo repozitář a expirovaný klíč
 - atom: z webupd8 z ppa pro ubuntu bez klíčů
 - skypeforlinux: přidalo repozitář a správný klíč
- Přidává starší verze, případně s repozitáři pro aktualizace
- Mirror repozitářů:
 - <https://www.deepin.org/en/mirrors/packages/>



2001:1488:ffff::456