Bezpečné používání linuxového desktopu

Martin Vician • martin.vician@nic.cz • vician.cz
/ptvician • @vician@mastodon.social

OpenAlt 2018 • 4. listopadu 2018

Máte na Linuxu antivirus? A mohla bych ho vidět?

Martin Vician

Systémový administrátor

CZ.NIC | SPRÁVCE DOMÉNY CZ

90% notebooků na Linuxu

Člen

Úvod do Linuxu

CZ.NIC AKADEMIE

Implicitně:

16.04 (Unity) a 18.04 (Gnome 3)

Obrázek: ubuntu.com

Témata

- Stažení a instalace Linuxu
- Bios a disk heslo
- Secure Boot
- Thunderbolt 3
- Firmeware aktualizace

- Linuxová distribuce Deepin

Obrázek: http://www.laptop-junction.com/toast/content/security-keeping-laptop-data-yours

Stačí stáhnout?

Zrcadla

launchpad.net/ubuntu/+cdmirrors
launchpad.net/ubuntu/+archivemirrors

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)

- tutorials.ubuntu.com/tutorial/tutorial-how-to-verify-ubuntu
- linuxmint.com/verify.php
- getfedora.org/verify

1. Stáhnout dodatečné soubory: kontrolní součet a podpis
2. Získat PGP klíč
3. Ověřit kontrolní součet
4. Ověřit podpis kontrolního součtu

Obrázek: xkcz.cz 1181

Získání GPG klíče

Ubuntu na Ubuntu

```
gpg --import \
/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg
```

Fedora na Windows a MAC OS X

Fedora Media Write

Nekontroluje

- UnetBootin
- Rufus (oficiálně doporučený)

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?

Obrázek: Stahler 2016, mvcr.cz

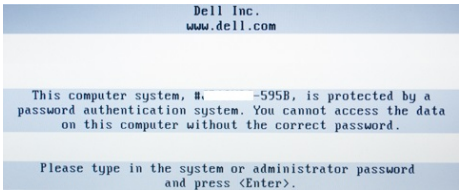
BIOS a disk heslo (Dell)

BIOS

- Master heslo odemkne BIOS

Disk

- Master heslo smaže a odemkne disk



https://bios-pw.org/

CTRL+ENTER

Obrázky: dell.com , ioffer.com

Secure Boot

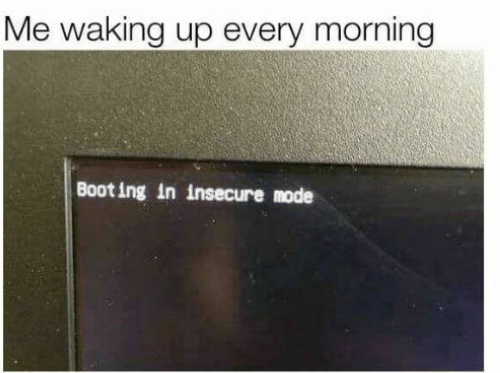
- UEFI: Dobrý sluha nebo špatný pán? (Radek Zajíc) https://youtu.be/ldNl4LivNAc
- https://mojefedora.cz/implementace-bezpecneho-bootovani-pomoci-uefi-ve-fedore/
- https://www.root.cz/clanky/secure-boot-nepodepsanym-systemum-vstup-zakazan/

- čtyři databáze klíčů:
  - `Platform Key` slouží výrobci k aktualizaci ostatních klíčů
  - `Key Exchange Key` klíče dodavatelů software, podepsané PK
  - `db` databáze klíčů/otisků povoleného softwaru
  - `dbx` databáze revokovaného softwaru

Obrázek: linuxzone.es

Secure Boot (UEFI)

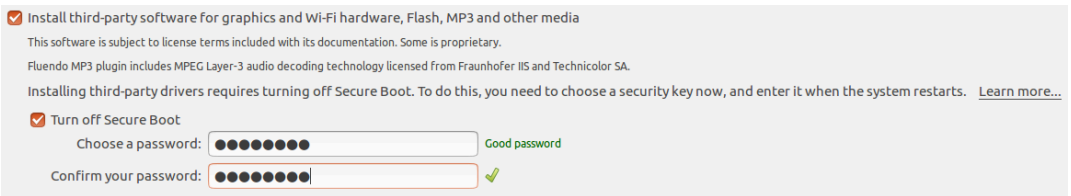
- Byl objeven škodlivý kód LoJax útočící na UEFI. Řádí i ve střední Evropě (lupa.cz)
- Secure Boot má chránit před zavedením necertifikovaného operačního systému
- Canonical (Ubuntu) má v UEFI klíče
- Lze podepsat vlastními klíči



Obrázek: me.me

Secure Boot (UEFI) - instalace

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

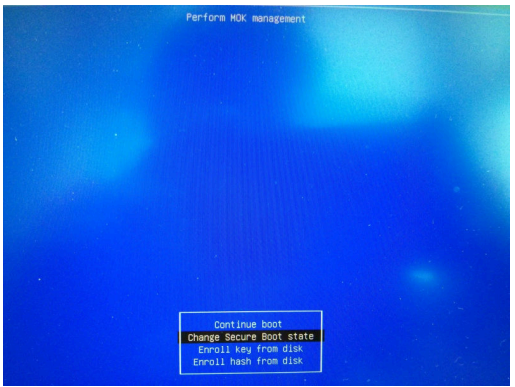


Obrázek: askubuntu.com/questions/765697/why-was-i-asked-to-create-a-password-in-order-to-disable-secure-boot-on-initial

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



Obrázek: fourdollars.blogspot.com

Dell dokovací stanice

Obrázek: discountelectronics.com, ebay.com

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

Obrázek: amazon.com

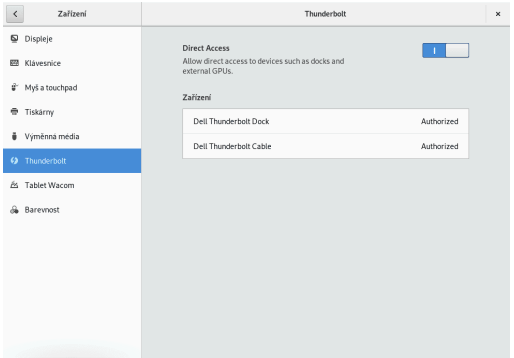
Thunderbolt 3

Správa:

- bolt (`boltctl`) - 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



Obrázek: root.cz

Thunderbolt 3 - rychlost Live USB

https://youtu.be/7tDfwKIFj4Y

Thunderbolt 3 - rychlost kancelář

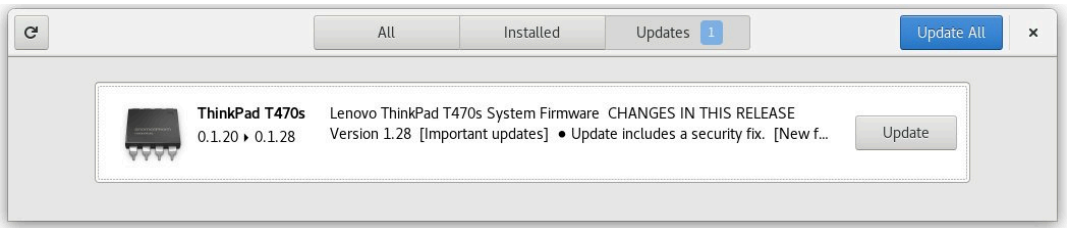
https://youtu.be/ZoS_LZ3eh50

BIOS aktualizace

- Firmware:
  - BIOS
  - Thunderbolt Controller
  - ...

- Použití: GNOME Software nebo:

```
sudo fwupdmgr refresh
sudo fwupdmgr update
```



Obrázek: twitter,com/mmmmmmpc

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)

https://youtu.be/FsDjsRXzTMs

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

Obrázek: deepin.org

K zamyšlení

- Nainstalovaný `gnome-keyring`, ale ne `seahorse`
- Obsahuje nestandardní balíky
  - `google-chrome`: nainstalovaný a podepsaný Google klíči
  - `spotify`: přidalo repozitář, jeden expirovaný a jeden už nepoužívaný klíč
  - `atom`: z webudp8 z ppa pro ubuntu bez klíčů
  - `skypeforlinux`: přidalo repozitář a správný klíč
- Přidává starší verze, případně s repozitáři pro aktualizace
- `firefox`: 60.0.1 z května 2018
- Mirror repozitářů:
  - https://www.deepin.org/en/mirrors/packages/

Nebuďme sami sobě hrozbou

Zdroj: facebook.com/spaze