Purpose

After installing OpenBSD fully encrypted with keys on USB stick, let's try with Linux and Fedora 32 (that we will push to rawhide for bleeding edge experience). As reading a non-clear text key seems largely impossible on Linux… I opted for “Honeypot OS” solution: Windows 10 on 256GB drive and Linux / on second drive with /boot on USB drive. This way without the USB key, Only Windows boots :D

Hardware

Lenovo Thinkpad X230 Table with an m-SATA drive in the phone card slot and 500GB hard drive replaced by a 1TB SSD, 16GB RAM, Corei5 CPU.

Disk partitioning

SSD (1TB) = sda
m-SATA (256GB) = sdb
sdd = 16GB Usb Drive

disk	partition	type	size	mount point	install pass
sdb	sdb*	Microsoft Crap	256GB		
sdb	sdb2	EFI Partition 100MB	/boot/efi		
sdd	sdd1	ext2	10GB	/boot	
sda	/dev/mapper/Fedora	LUKS encrypted	1TB		test
sda	sda1	swap	16GB	-	
sdb	/dev/mapper/Fedora-fedora–root	ext4	915GB	/	

Install

Using Fedora Media Writer I created a live USB with Fedora 32

Boot is set to “UEFI” with Microsoft “Secure boot” (🤣 yes Secure and Microsoft in the same sentence) pure GPT crap on all devices
I first installed Windows 10 on first hard drive (m-sata 256GB)
Install goes by and when at the step of partitionning disk I choose Custom, select all devices then mount the EFI partition of the m-sata drive as /boot/efi then create /boot(ext2) on the USB key an LVM(named Fedora, encrypted) and inside create swap and / (ext4)

I put an easy passphrase as we'll change it later and put the key on a USB drive to decrypt easily.

initial pass are in the table above 🙂

After reboot it will ask for swap then LVM key

Next step put the encrypted key on the USB key to avoid typing

Rawhide

Switch to rawhide ! Rock'n roll

https://fedoraproject.org/wiki/Upgrading_Fedora_using_package_manager#To_Rawhide

```
dnf upgrade
dnf install -y dnf-plugins-core fedora-repos-rawhide
dnf config-manager --set-disabled fedora updates updates-testing
dnf config-manager --set-enabled rawhide
dnf clean -q dbcache packages metadata
dnf --releasever=rawhide --setopt=deltarpm=false distro-sync --nogpg
touch /.autorelabel


====== Missing programs/repo ======
<code bash> dnf install -y htop ccze vim zsh dfc git
```

epel

Fingerprints

```
dnf install -y fprint libfprint fprint-pam
```

LUKS key on usb drive

WORK IN PROGRESS
Reference: https://forums.centos.org/viewtopic.php?t=53452

key in /boot/trololo.key (usb drive formatted in ext2)

LUKS'key

add this key to the luks partition

```
cryptsetup luksAddKey /dev/disk/by-uuid/<lvm luks> /boot/trololo.key
```

Dracut

create a dracut config file to help mounting the key at early stage

```
vi /etc/dracut.conf.d/usb-decrypt.conf
```

content:

```
omit_dracutmodules+="systemd"
filesystems+="ext2"
```

Note: my USB drive is formatted in ext2

Re-generate initramfs

```
dracut -fv
```

GRUB

get UUID of devices to get the UUID of your USB drive

```
ls -l /dev/disk/by-uuid
```

Add in grub.cfg

```
vi /boot/efi/EFI/fedora/grub.cfg
```

add

```
rd.luks.key=/trololo.key:UUID=<UUID of USBdrive>
```

Note: the key path is relative to the device

Reboot to test

LUKS Keys

Generate

```
dd if=/dev/urandom of=/boot/trololo.key bs=1 count=1024
```

Failover key

```
cryptsetup luksAddKey /dev/sda1
```

cleaning keys

Check keys:

- list

```
cryptsetup luksDump /dev/sda1
```

- check one specific

```
cryptsetup luksOpen --test-passphrase --key-slot 0 /dev/sda2 && echo correct
```

- delete osolete

```
cryptsetup -v luksKillSlot /dev/sda1 0
cryptsetup -v luksKillSlot /dev/sda1 1
```