Lanzaboote

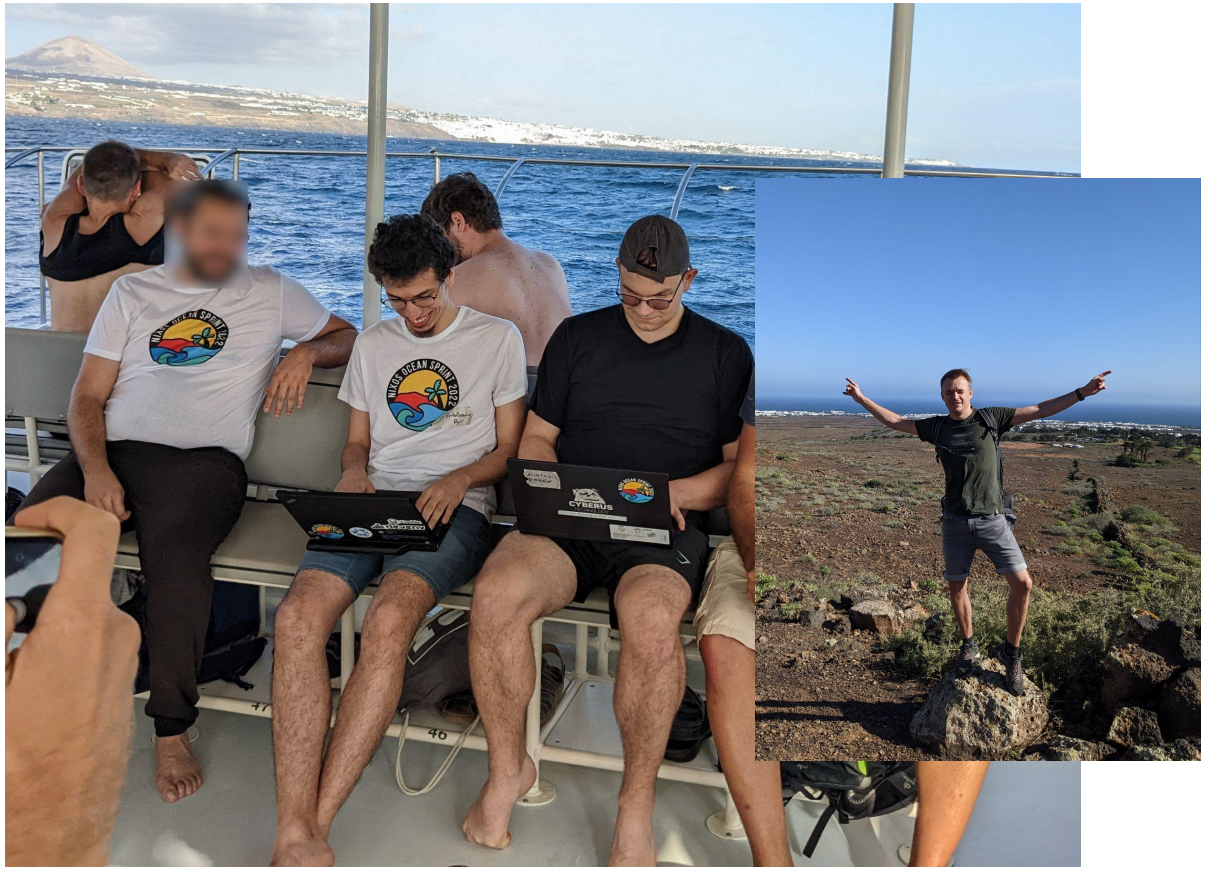
Towards Secure Boot for NixOS

The Lanzaboote Team

Julian Stecklina @js:ukvly.org

The Lanzaboote Team

@raitobezarius
@nikstur
@blitz

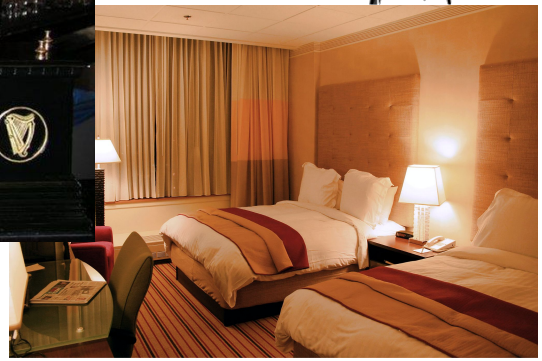


Agenda

- What’s Secure Boot?
- What’s lanzaboote? And why is NixOS special?
- What’s the status?
- How do I contribute?

What's the Problem?

- Laptop disk is encrypted.
- Laptop is left alone.
- You type in your password.



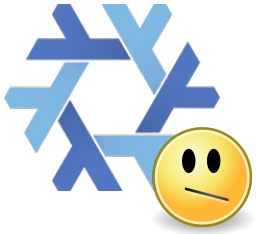
Are you sure this password prompt does what you think it does?

Secure Boot to the Rescue

Chain of Trust

Verifies Signatures with what?

Typically Microsoft and OEM keys are trusted.



Secure Boot and NixOS

No signed binaries on cache.nixos.org.

But we can enroll our own Secure Boot keys!

But then we have to manually sign things?

What is Lanzaboote?

NixOS Secure Boot tooling developed in Lanzarote at OceanSprint.

Lanzaboote takes care of:

- Automatic signing of boot files on nixos-rebuild.

You **once** take care of:

- Manual generation of keys.
- Manual enrolling of keys in firmware.

-> Quick Start Docs

Unified Kernel Images (UKI)

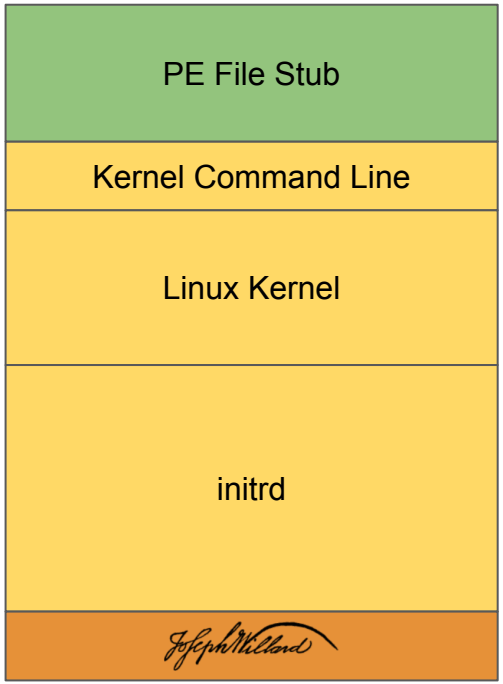
We focus on systemd-boot* and use UKIs:

- Is a normal UEFI PE binary to the firmware.
- Self-contained. Bundles:
  - Kernel
  - Kernel Command Line
  - Initrd
- Contains Metainformation for Bootloader (os-release)
  - Name, Version, …
  - Used to show user a bootloader entry
- Signing the UKI is sufficient.

*Grub and extlinux support are planned.

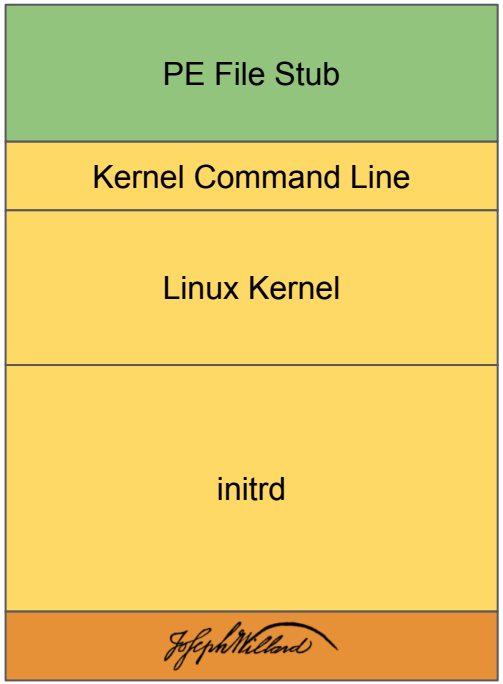
systemd-stub

/EFI/Linux/very-big-uki.efi



systemd-stub

/EFI/Linux/very-big-uki.efi

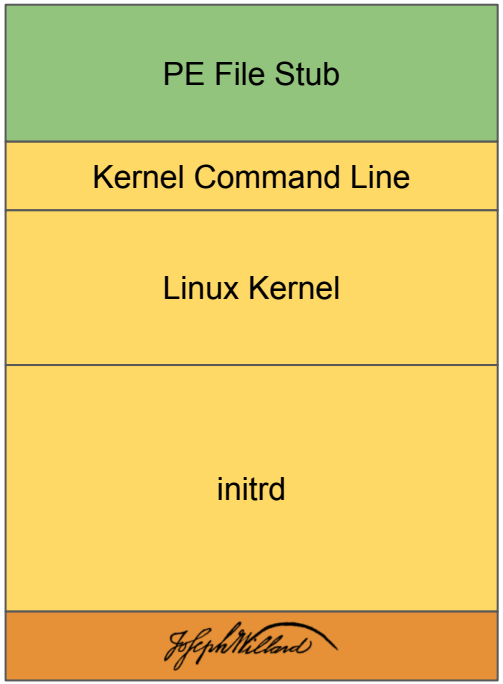


init=/nix/store/aw2…-nixos-system-23.05.20230120.5ed4819/init …

Changes for *every* generation!

systemd-stub

/EFI/Linux/very-big-uki.efi



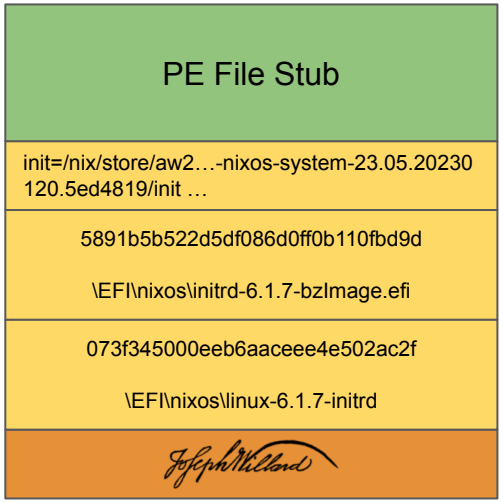
init=/nix/store/aw2…-nixos-system-23.05.20230120.5ed4819/init …

Changes for *every* generation!

~40 MiB, but don’t change for every generation.

Lanzaboote Stub

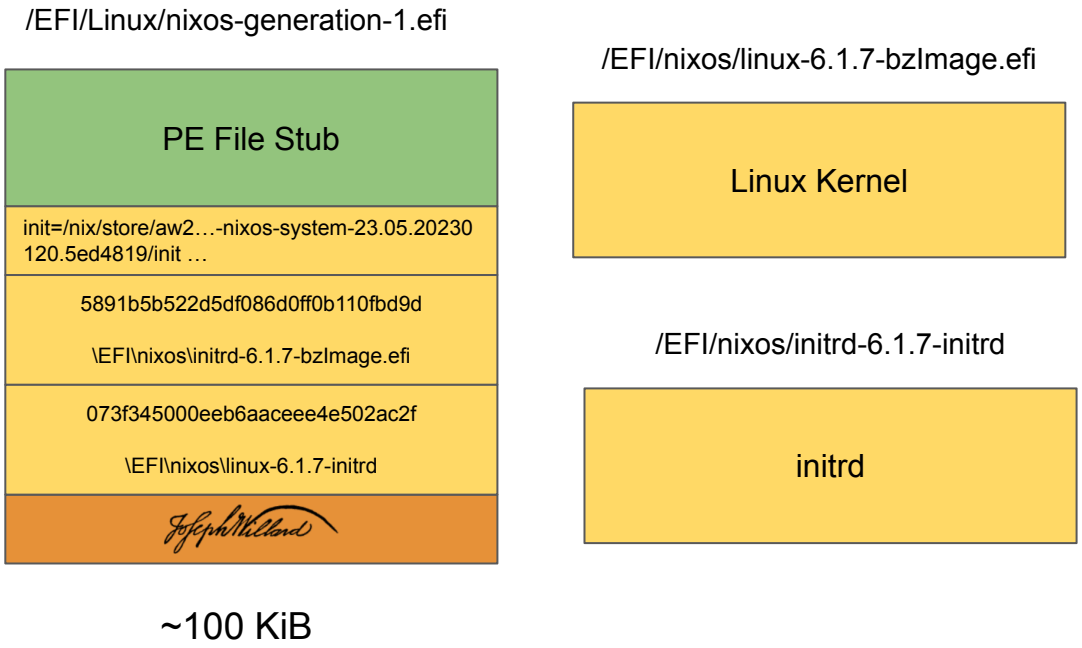
/EFI/Linux/nixos-generation-1.efi



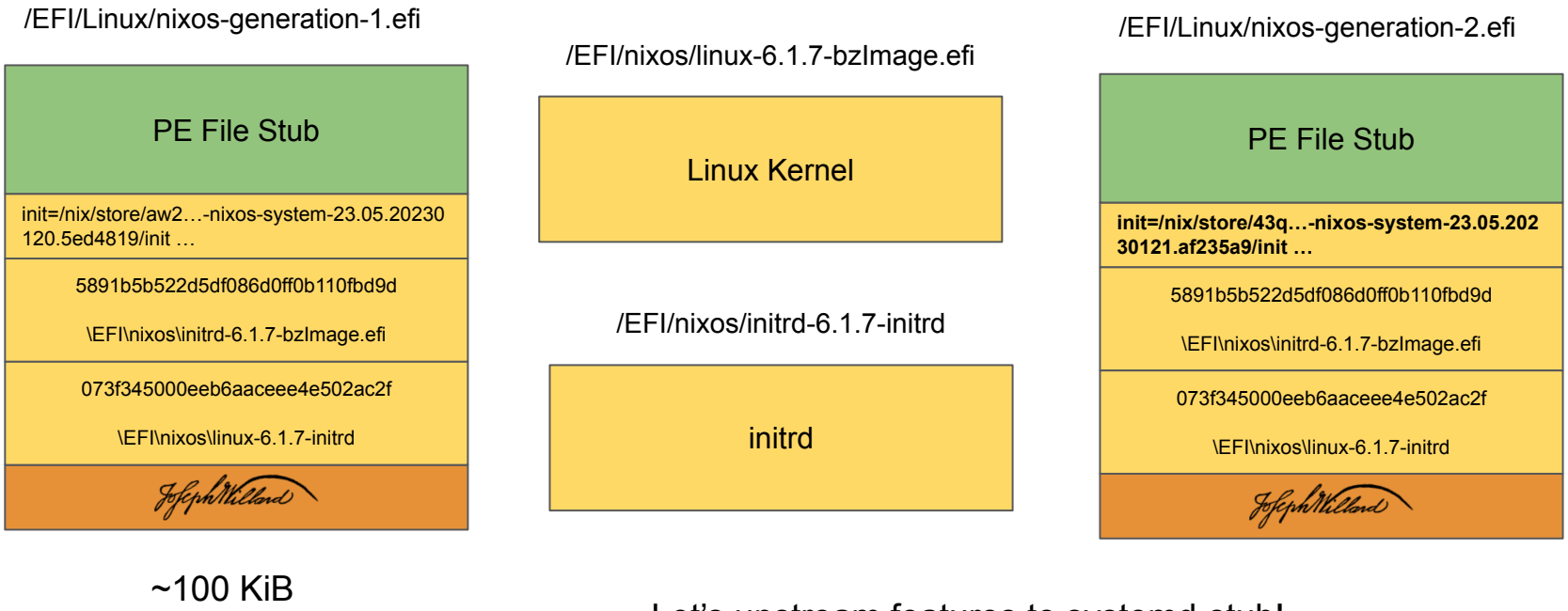
Path + Hash instead of file contents.

~100 KiB

Lanzaboote Stub



Lanzaboote Stub



~100 KiB

Let’s upstream features to systemd-stub!
https://github.com/systemd/systemd/issues/26096

Lanzaboote Tool (lzbt)

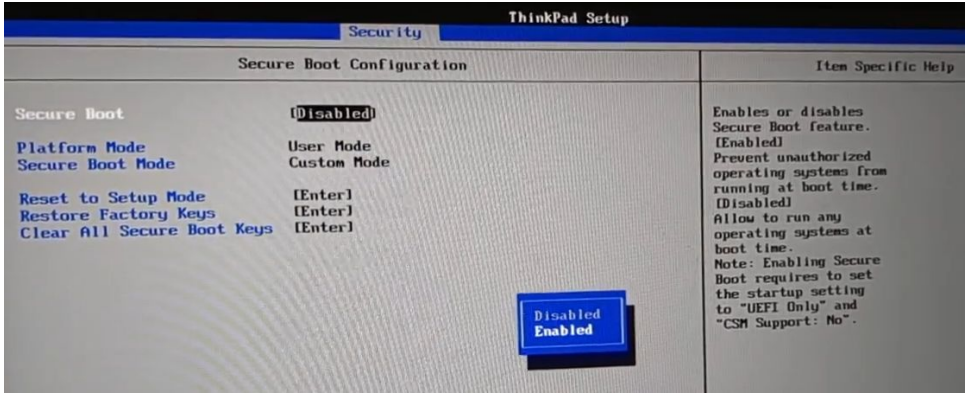
- “Behind the nixos-rebuild scenes” tooling
- Turns generation links into signed boot files
- Uses bootspec RFC: https://github.com/NixOS/rfcs/pull/125

/nix/var/nix/profiles/system-*-link

```
boot
├── EFI
│   ├── BOOT
│   │   └── BOOTX64.EFI
│   ├── Linux
│   │   ├── nixos-generation-365.efi
│   │   ├── nixos-generation-366.efi
│   │   └── nixos-generation-367.efi
│   ├── nixos
│   │   ├── hzwybyvchpkb6kr67zyq5xlqk4zbssy5-linux-6.1.7-bzImage.efi
│   │   └── qnlisq3g2vx6hawnjdp2xzhf880x0r84-initrd-linux-6.1.7-initrd.efi
│   └── systemd
│       └── systemd-bootx64.efi
❯ sudo sbctl verify
Verifying file database and EFI images in /boot...
✓ /boot/EFI/BOOT/BOOTX64.EFI is signed
✓ /boot/EFI/Linux/nixos-generation-365.efi is signed
✓ /boot/EFI/Linux/nixos-generation-366.efi is signed
✓ /boot/EFI/Linux/nixos-generation-367.efi is signed
✓ /boot/EFI/nixos/hzwybyvchpkb6kr67zyq5xlqk4zbssy5-linux-6.1.7-bzImage.efi is signed
✓ /boot/EFI/systemd/systemd-bootx64.efi is signed
```

How to Use

- Quick Start Docs
- BIOS Password
- Full Disk Encryption




```
$ sudo sbctl create-keys
[sudo] password for julian:
Created Owner UUID 8ec4b2c3-dc7f-4362-b9a3-0cc17e5a34cd
Creating secure boot keys...✓
Secure boot keys created!
```

```
boot.loader.systemd-boot.enable = lib.mkForce false;

boot.lanzaboote = {
  enable = true;
  pkiBundle = "/etc/secureboot";
};
```

Summary

You can use UEFI Secure Boot for NixOS today! You can help, if you know Rust or Nix or write beautiful documentation or …!

Github: https://github.com/nix-community/lanzaboote

Current focus: Release 1.0 Milestone

matrix **#secure-boot:nixos.org**

#bootspec:nixos.org

#rust-osdev_Lobby:gitter.im

@js:ukvly.org

astodon @blitz@infosec.exchange