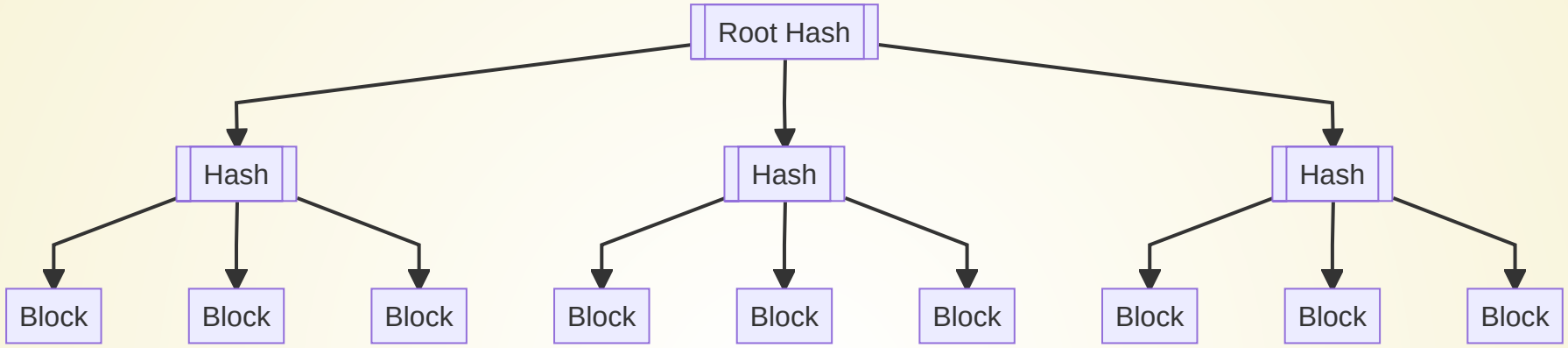


DM-VERITY ROOTFS INTEGRITY

Presented by frehberg <Frank Rehberger> (fr@frehberg.com)
FOSDEM 2023

Demonstrator: https://opencritis.org

WHAT IS DM-VERITY?

Family of Kernel Device Mapper (DM) Modules

mapping physical block devs onto higher-level virtual block devs, for example

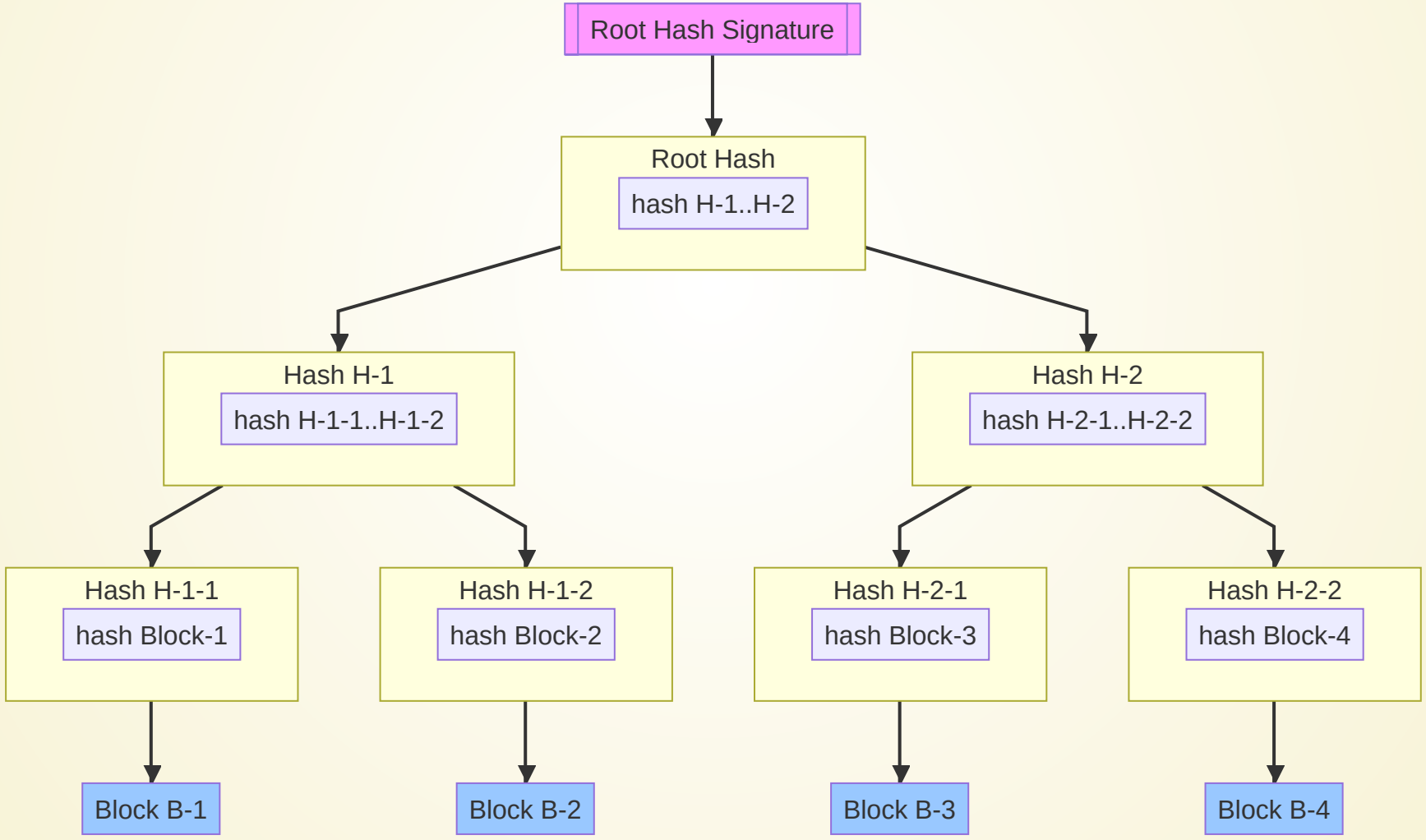
- dm-crypt: encryption/confidentiality (rw)
- dm-integrity: journaling (rw)
- **dm-verity: authenticity/integrity (ro)**

Since kernel v3.4, Android version 4.4, (late 2013)

https://docs.kernel.org/admin-guide/device-mapper/verity.html

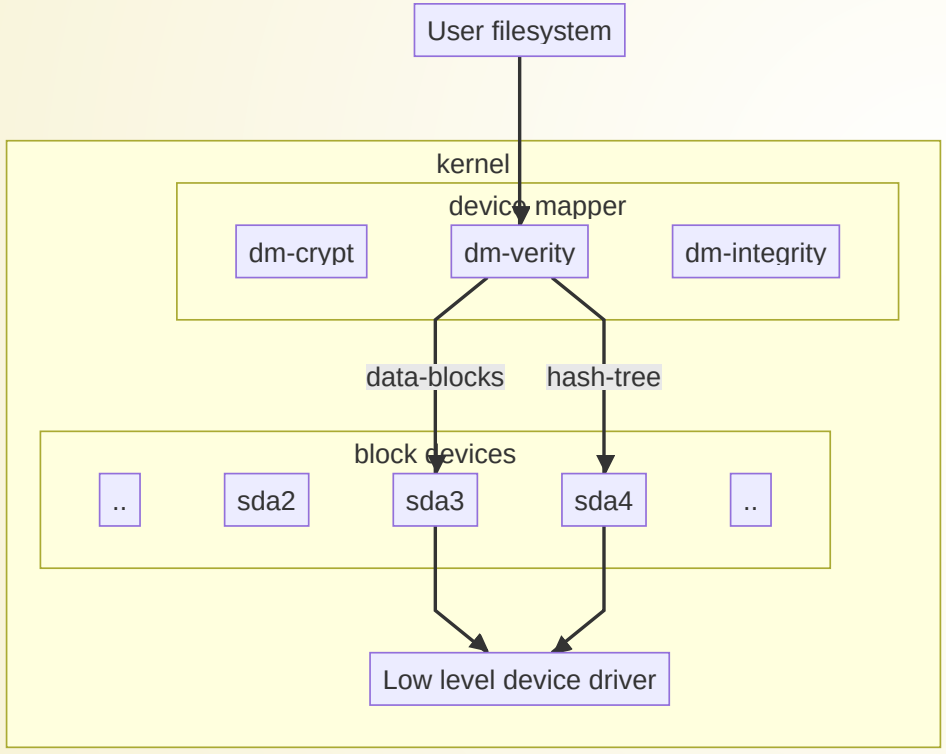
DM-VERITY HASH TREE FORMATTING

$ veritysetup format rootfs.ext2 hash.img



DM-VERITY MAPS VIRTUAL BLOCK DEVICE

kernel device mapper module



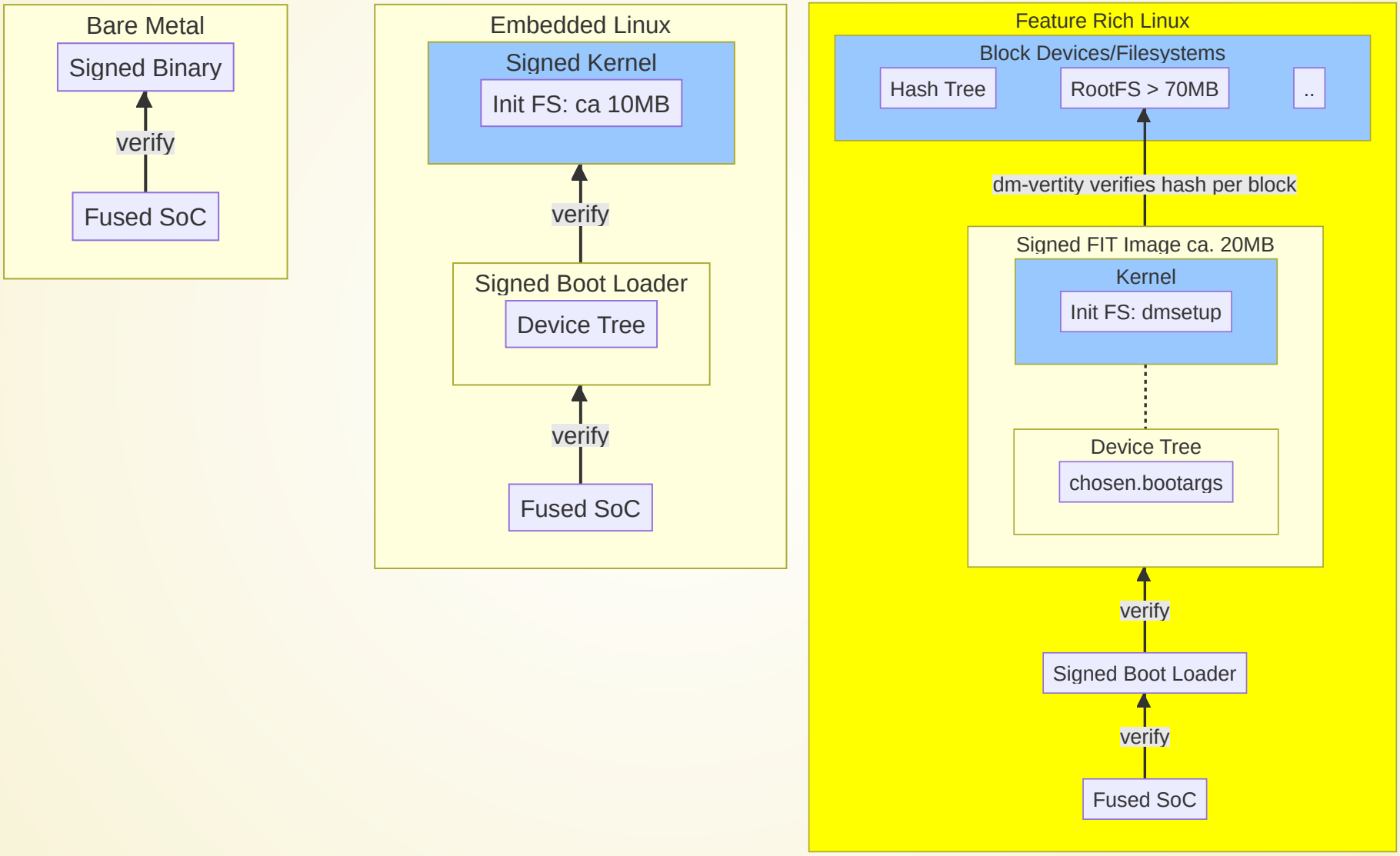
- integrity checking root filessytem
- (authenticity) with signed root hash

DM-VERITY AS COUNTER MEASURE

Major threat: Manipulation of rootfs

- Detect Manipulation at startup
- Detect manipulation **during runtime**
- Terminate execution if manipulation is detected
- Deal with forward error correction (FEC)
- Minimal runtime overhead, ~Zero latency at startup. (compare to full image hash 15MB/s)

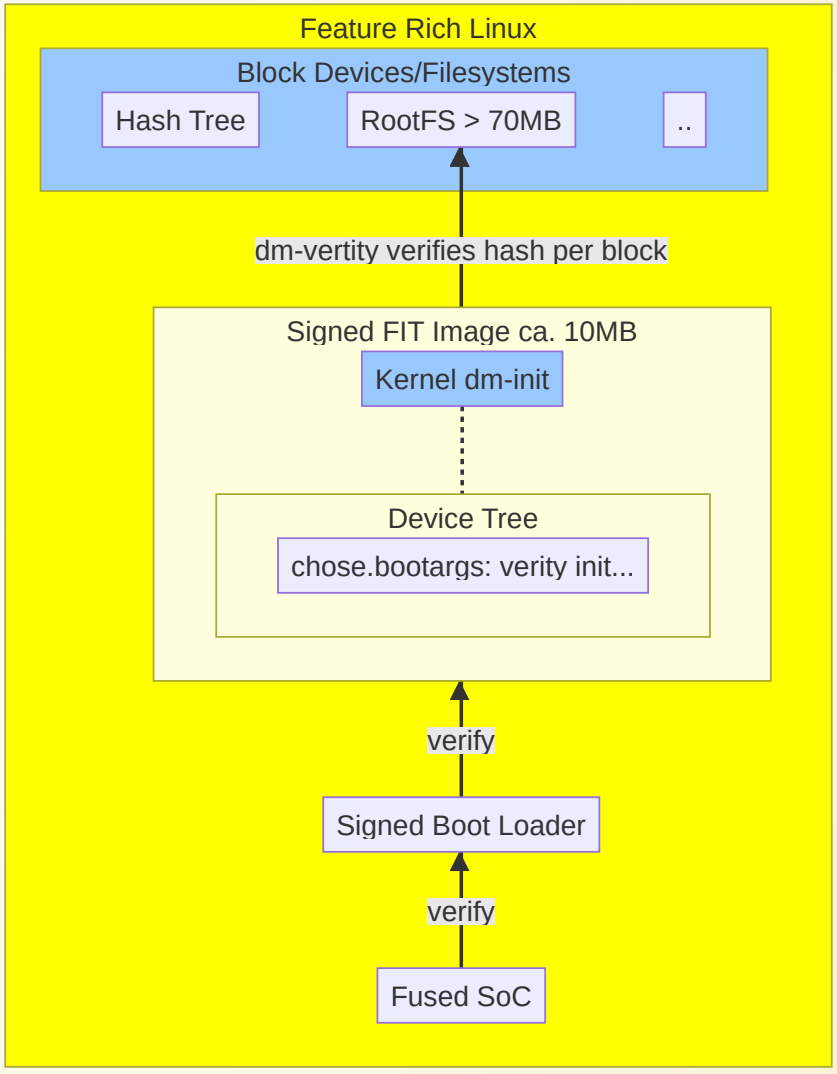
DM-VERITY USE CASE: RICH LINUX



INIT DM-VERITY WITHOUT INITFS

Kernel patch by Nathan Barrett-Morrison(Timesys)

DM-Verity Without an Initramfs



KERNEL COMMAND LINE

```
console=ttyAMA0,115200 ro rootwait
root=/dev/dm-0
systemd.volatile=overlay
dm-mod.create="verity,,,ro,0 122880 verity 1
/dev/sda4 /dev/sda5 1024 4096
61440 1 sha256
a100bab0d2e49b665bb18a0ee202b0fb78d084e0d6cfe3b115b6e3908b8ac1
5027c03524f90fdf6e71f623ce059591a0aa3b48a39807826244c5f5e1db3a
3 ignore_zero_blocks
root_hash_sig_hex
3081df06092a864886f70d010702a081d13081ce020101310f300d06096086
dm_verity.require_signatures=1 rauc.slot=B
```

KERNEL OPTIONS

```
CONFIG_BLK_DEV=y
CONFIG_BLK_DEV_LOOP=y
CONFIG_MD=y
CONFIG_BLK_DEV_DM=y
CONFIG_BLK_DEV_MD=y
CONFIG_DM_INIT=y
CONFIG_DM_VERITY=y
CONFIG_DM_VERITY_FEC=y
CONFIG_DM_VERITY_VERIFY_ROOTHASH_SIG=y
CONFIG_SYSTEM_TRUSTED_KEYRING=y
CONFIG_SYSTEM_TRUSTED_KEYS="rootfs_cert.pem"
```

BENEFITS

- Rootfs Integrity during startup
- Rootfs Integrity during run-time
- Termination in case kernel detects manipulation
- Almost zero cost

THANK YOU