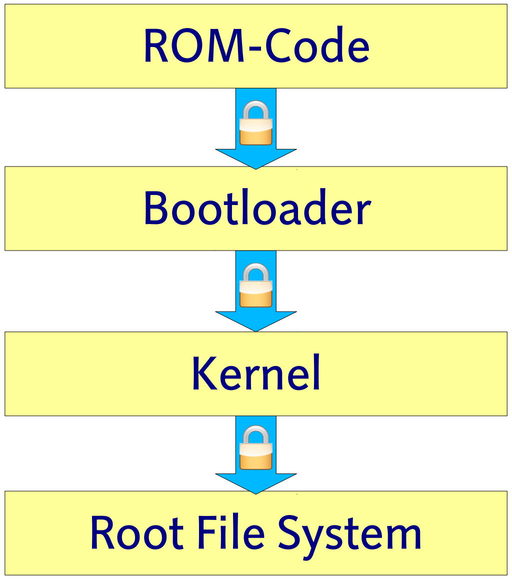
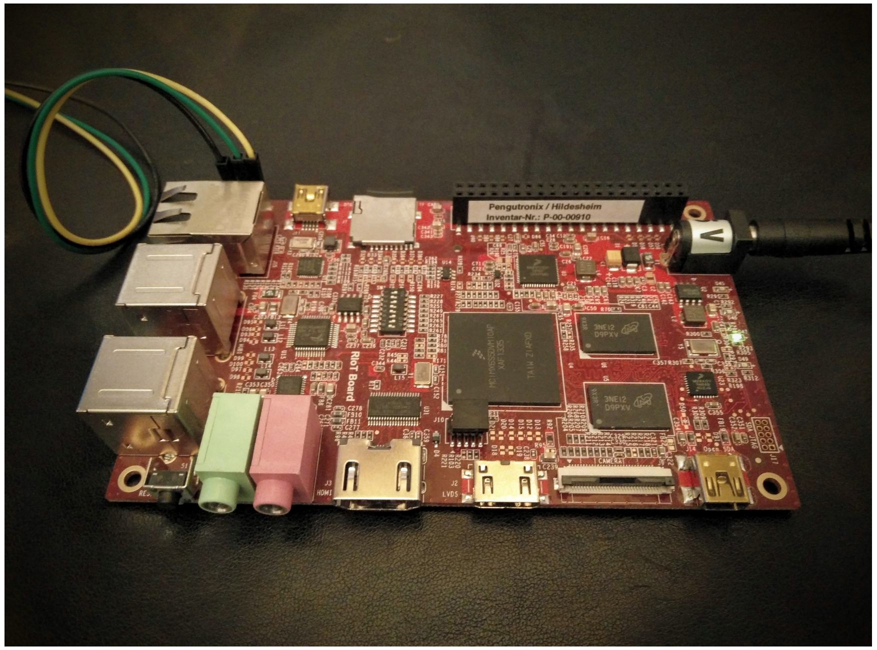
Verified Boot: From ROM to Userspace





ELC Europe 2016, 12.10.2016

Marc Kleine-Budde <mkl@pengutronix.de>

Why Verified Boot?

Attractive hacking target:

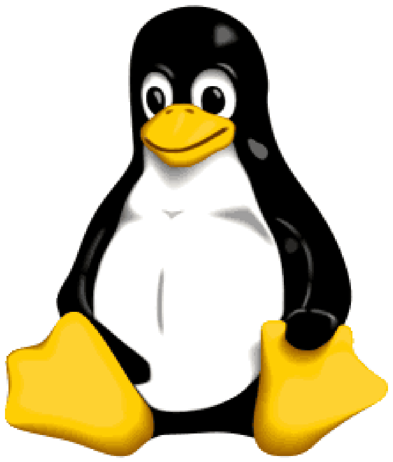
- Linux systems control critical industrial processes
- Compared to servers, embedded systems receive poor maintenance

Complex Software:

- Every Linux system has undiscovered vulnerabilities
- Commercial control software (closed source)
- Defense in Depth is important!

We can do it ourselves:

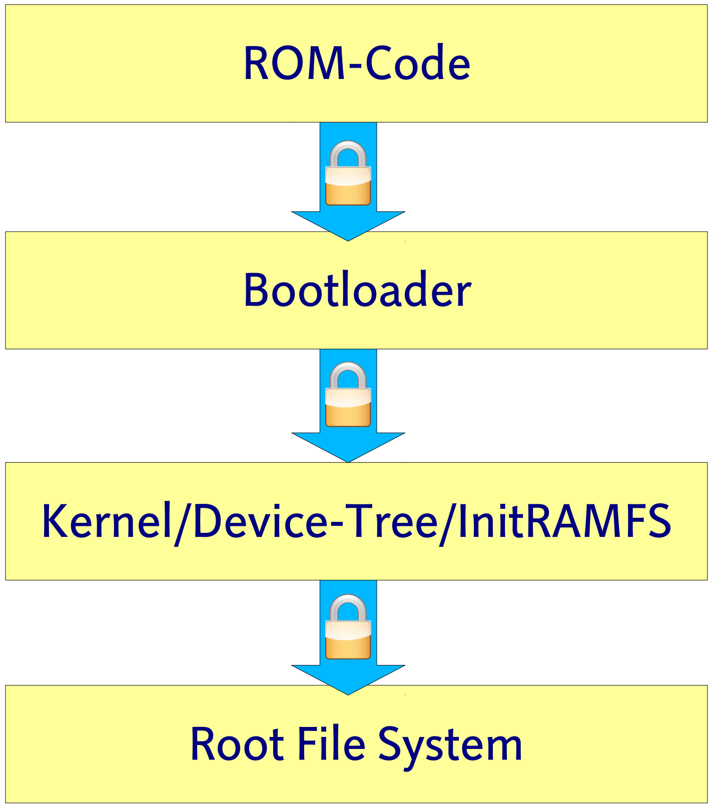
- SoC with hardware support are available everywhere
- Software components are available as FOSS



What do we want to protect?

- Bootloader
- Kernel
- File system
  - Programs
  - Configuration files
  - Application data
- The attacker can manipulate all stored data
  → we want to detect any tampering

Boot Stages



vendor dependent
(here: Freescale/NXP i.MX6 HABv4, SHA and RSA)

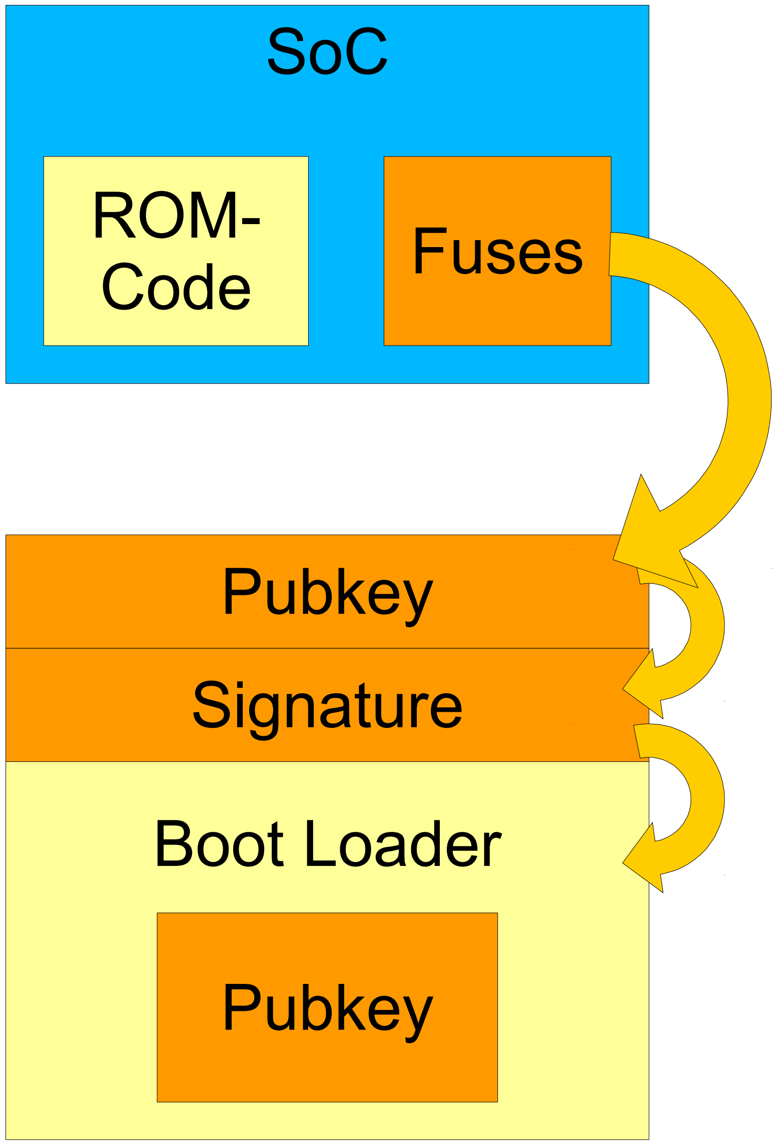
FIT-Image (SHA and RSA)

IMA & EVM (HMAC and RSA)

Boot Loader

- Usually on unprotected storage (NAND, eMMC, SD)
- Has full control over the system
- Must be verified by the ROM code
  - Hash of the certificate is burned to on-chip fuses
- Contains the public key to verify the Kernel image

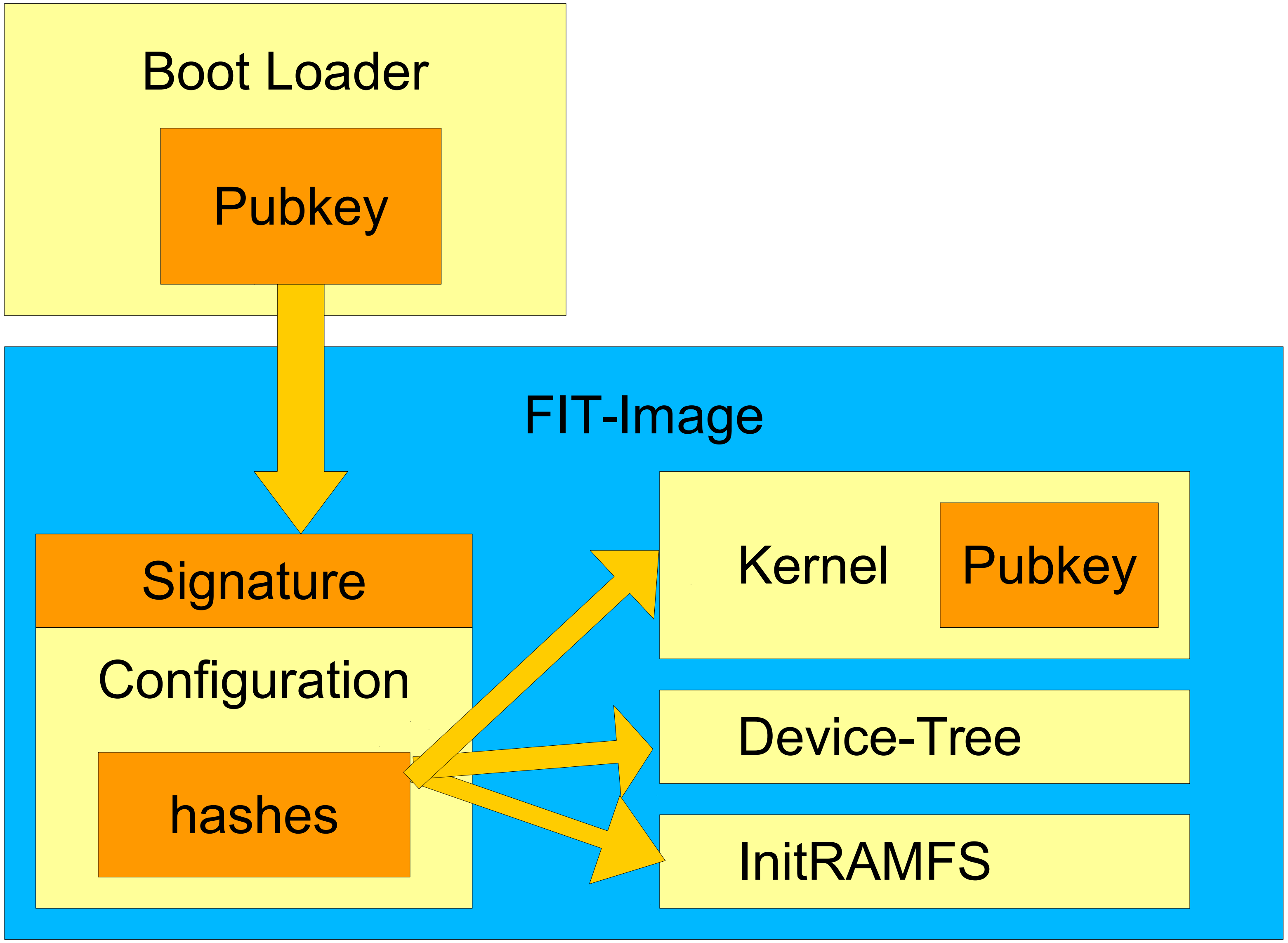
Boot Loader



FIT-Image

- In separate partition or on root file system
- Consists of Kernel, Device-Tree and InitRAMFS
  - May contain several variants
  - Always signs a complete “configuration” of kernel, DT and InitRAMFS to prevent mix-and-match attacks
- Must be verified by the boot loader
  - Signature matches the public key in the boot loader
- Contains the public key to check the root file system

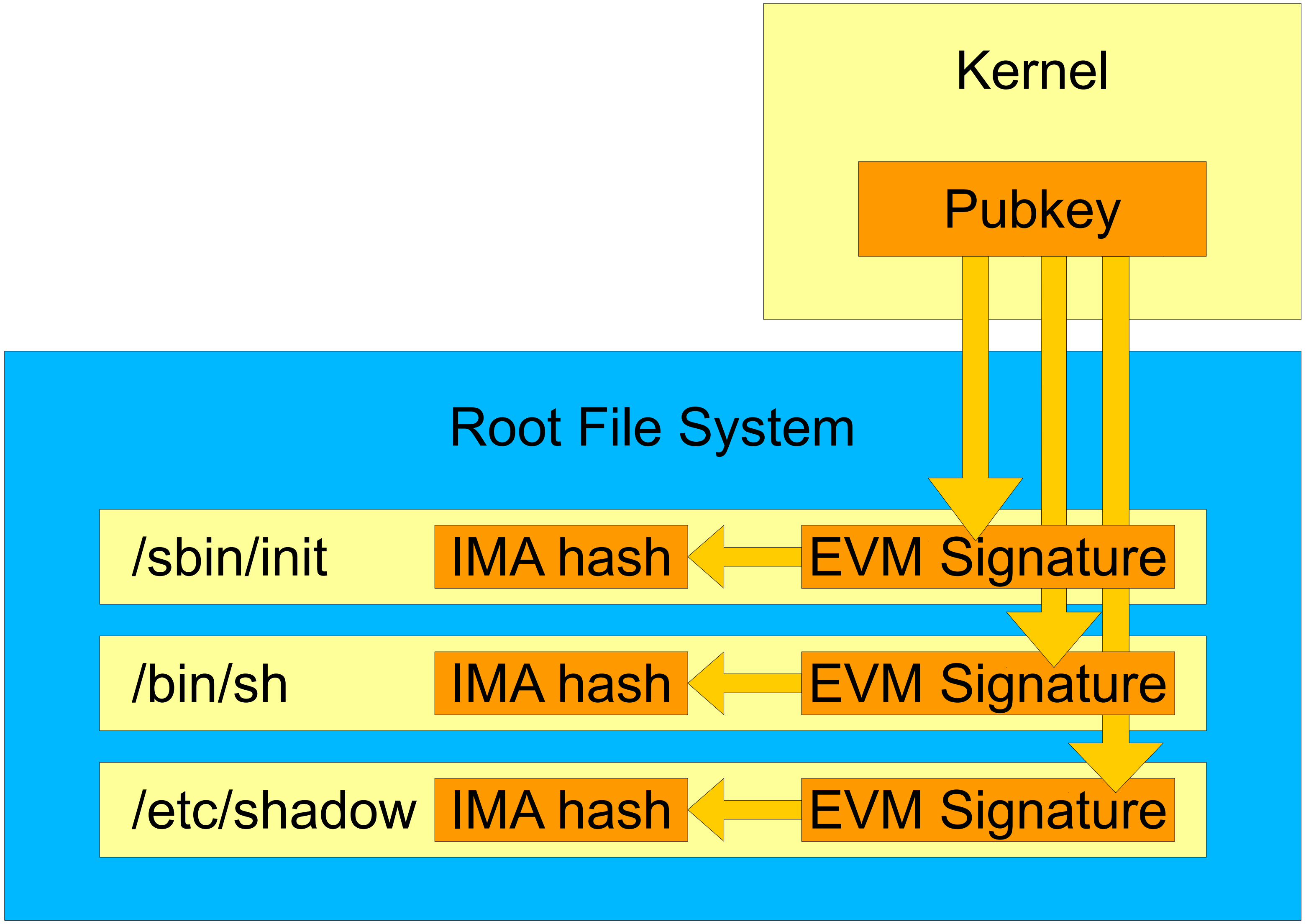
FIT-Image


Boot Loader
Pubkey
FIT-Image
Signature
Configuration
hashes
Kernel
Pubkey
Device-Tree
InitRAMFS

Root File System (initial)

- ext4 oder UBIFS
    - File System needs Extended Attributes
- Every file has an IMA hash
    - SHA1 or SHA256 of the file content
    - Extended Attribute: security.ima
- Every file has an EVM signature
    - Secures Security Extended Attribues
    - Is signed on the development computer with a private key
    - RSA signature matches the public key in the kernel
    - Extended Attribute: security.evm

Root File System (initial)



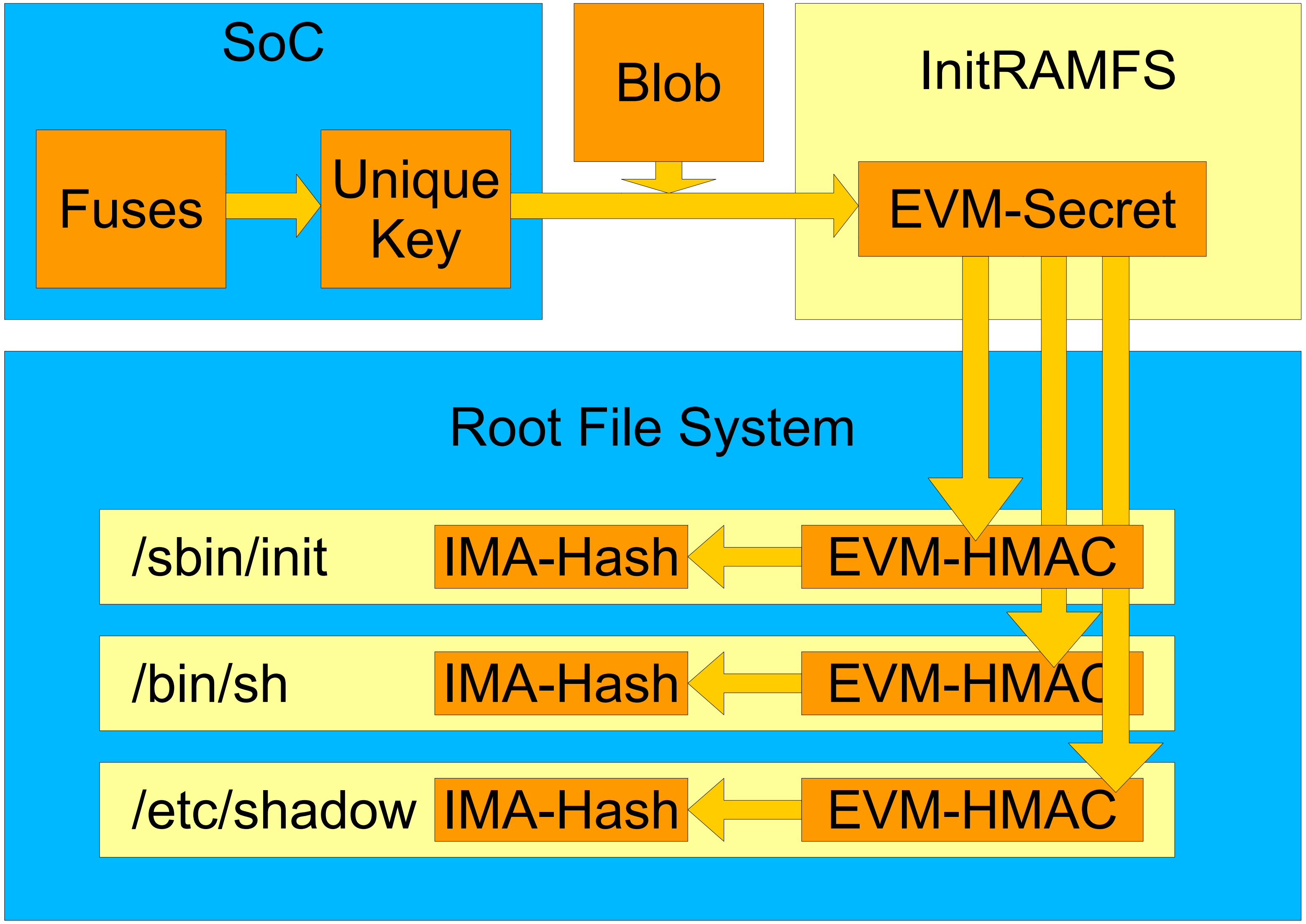
Root File System (writable)

- No RSA-Signatures
  - There is no private key on the system
  - RSA is quite slow

- Instead SHA-HMAC
  - Requires a different shared Secret for each system
  - On first file access the signature is replaced by the HMAC

- Every file has an IMA hash and a EVM HMAC
  - Only a correctly booted system has access to the EVM Secret
  - Attackers cannot manipulate files and calculate a matching HMAC

Root File System (writable)

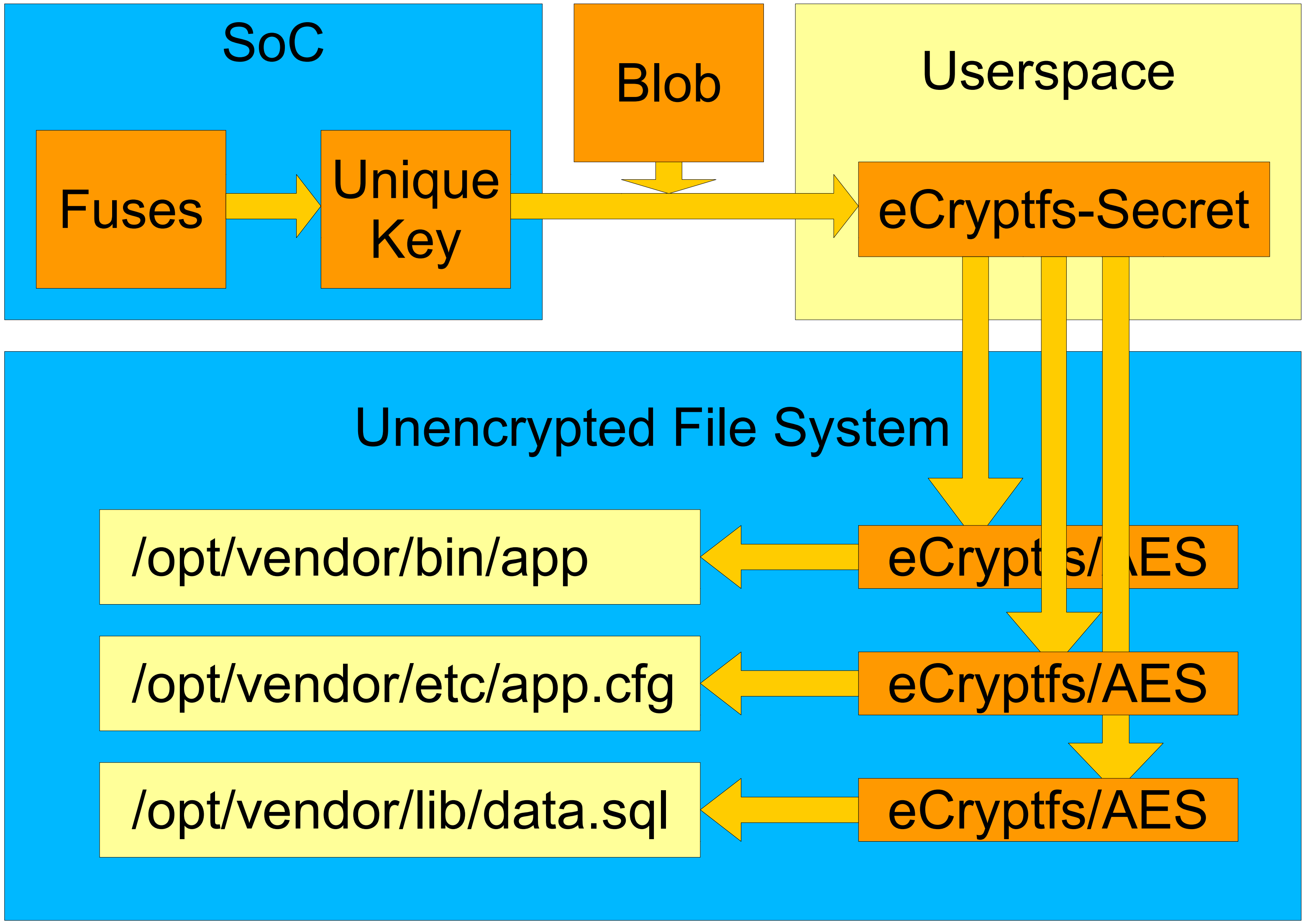


Pengutronix.

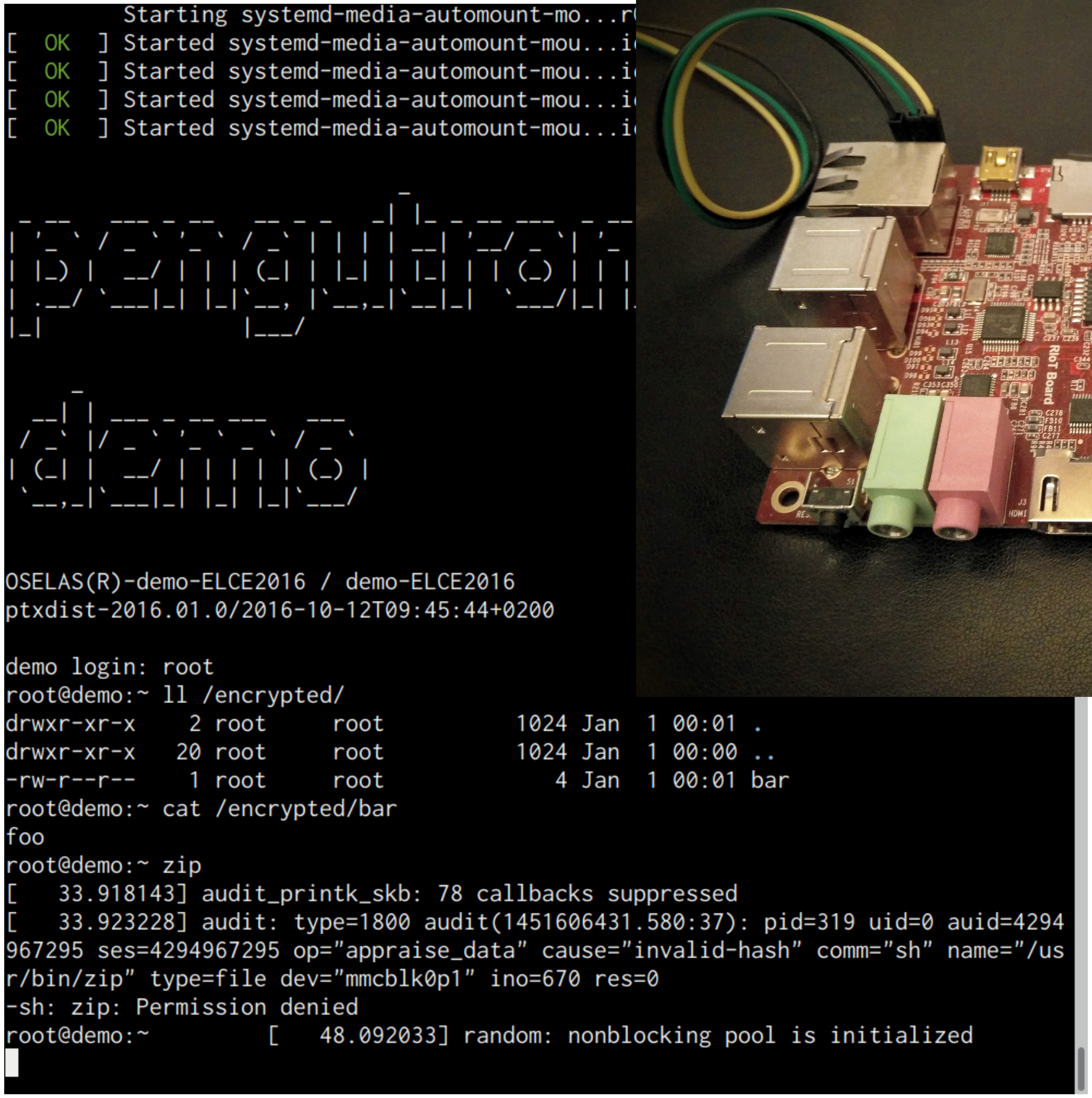
Encrypted File System - eCryptfs

- File system level encyption
    - Works both on NAND and block devices
    - Every file corresponds to an unencrypted file
    - File names and content encrypted
    - Directory layout and permissions are clear text
- Requires a different shared Secret for each system
- IMA/EVM not needed
    - Integrity is provided by AES in GCM mode

Encrypted File System - eCryptfs



Demo Time!



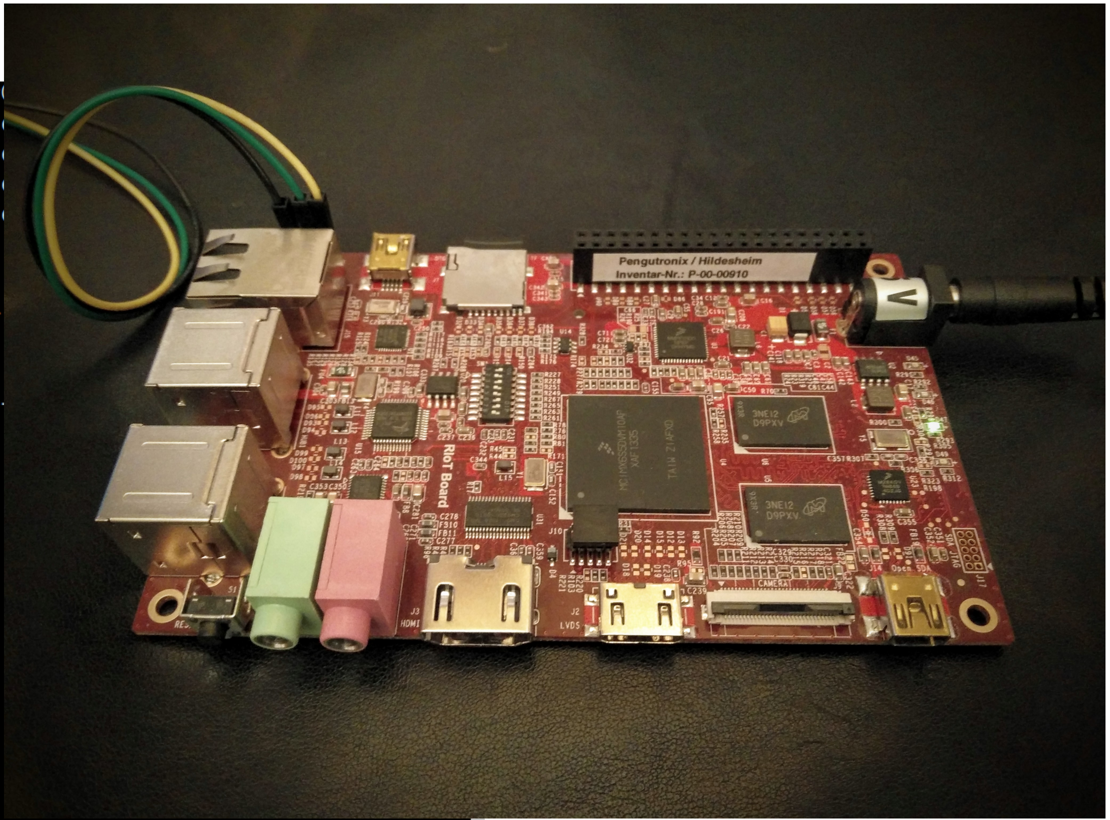
```
         Starting systemd-media-automount-mo...r
[  OK  ] Started systemd-media-automount-mou...i
[  OK  ] Started systemd-media-automount-mou...i
[  OK  ] Started systemd-media-automount-mou...i
[  OK  ] Started systemd-media-automount-mou...i

                             _
 _ __   ___ _ __   __ _ _   _| |_ _ __ ___  _ __
| '_ \ / _ \ '_ \ / _` | | | | __| '__/ _ \| '_
| |_) |  __/ | | | (_| | |_| | |_| | | (_) | | |
| .__/ \___|_| |_|\__, |\__,_|\__|_|  \___/|_| |.
|_|               |___/

     _
  __| | ___ _ __ ___   ___
 / _` |/ _ \ '_ ` _ \ / _ \
| (_| |  __/ | | | | | (_) |
 \__,_|\___|_| |_| |_|\___/


OSELAS(R)-demo-ELCE2016 / demo-ELCE2016
ptxdist-2016.01.0/2016-10-12T09:45:44+0200

demo login: root
root@demo:~ ll /encrypted/
drwxr-xr-x    2 root     root          1024 Jan  1 00:01 .
drwxr-xr-x   20 root     root          1024 Jan  1 00:00 ..
-rw-r--r--    1 root     root             4 Jan  1 00:01 bar
root@demo:~ cat /encrypted/bar
foo
root@demo:~ zip
[   33.918143] audit_printk_skb: 78 callbacks suppressed
[   33.923228] audit: type=1800 audit(1451606431.580:37): pid=319 uid=0 auid=4294
967295 ses=4294967295 op="appraise_data" cause="invalid-hash" comm="sh" name="/us
r/bin/zip" type=file dev="mmcblk0p1" ino=670 res=0
-sh: zip: Permission denied
root@demo:~       [   48.092033] random: nonblocking pool is initialized
█
```



Do It Yourself!

- Freescale MX28
  - I2SE Duckbill (~100€)
  - MYIR Tech MYD-IMX28X (~100+40€)
- Freescale MX53
  - USB Armory (~130$)
- Freescale MX6
  - Cubox-i (~110€)
  - RioT-Board (~85€)

- Without Hardware-Support: Read-Only SPI-NOR or eMMC + TPM

Used Components

- Supported SoCs:
  - MX25
  - MX6
- Bootloader: barebox-2016.09
- Kernel: linux-4.0.9 + patches
- offline image signing:
  - e2fsprogs (+patches)
  - ima-evm-utils (+patches)
- integrated everything with ptxdist

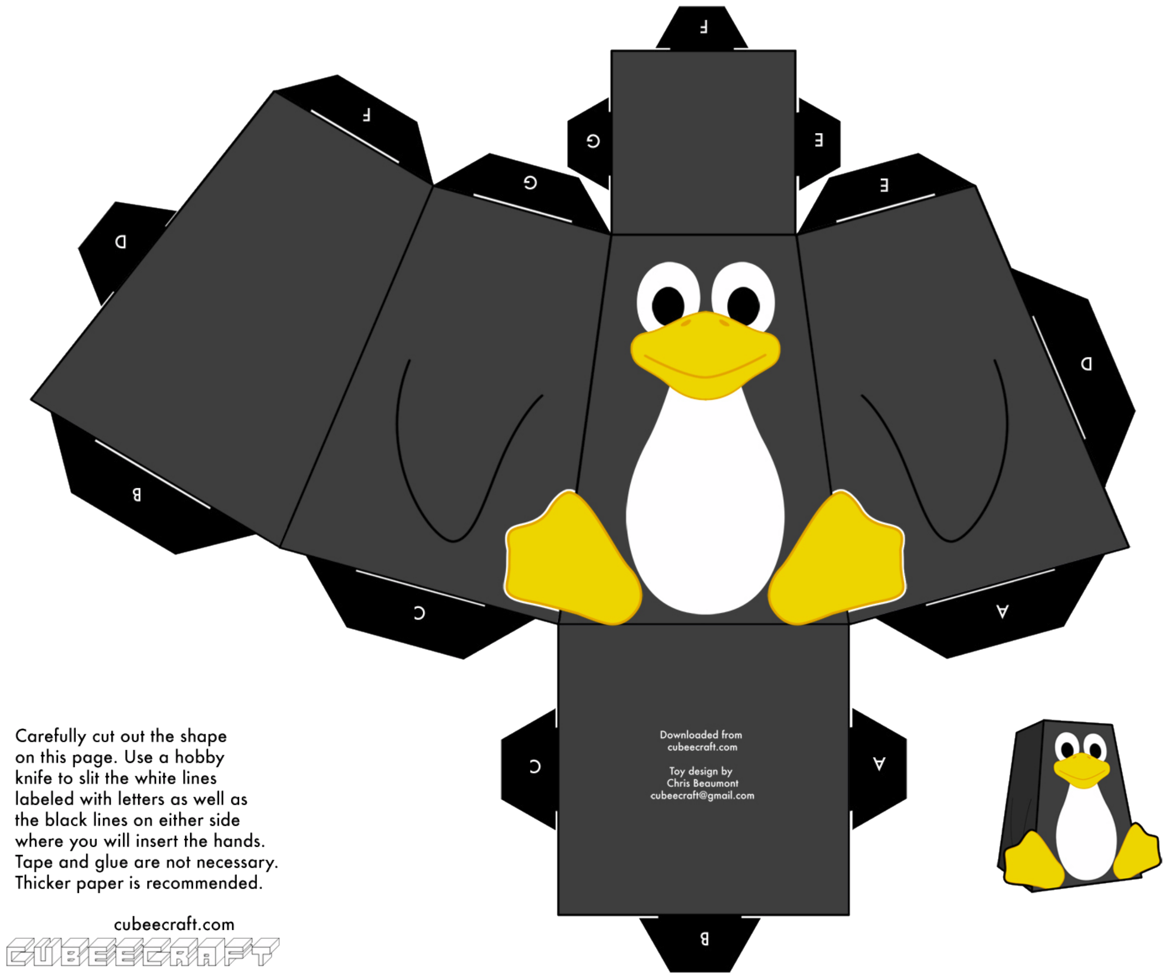
What's Missing?

- Protection of Directories
  - Prevents to move, delete and create files
  - There are already patches "directory integrity protection"
- Mainlining
  - Offline image creation via mkfs.ext4 and ima-evm-utils
  - blob drivers for imx6 crypto engine (CAAM)
  - blob drivers for mx25 crypto engine
- Support for other SoCs:
  - MX53
  - Other Vendors (Dokumentation?)

Best Practices / Lessons Learned

- Development Keys in BSP
- Access to Production Keys via pkcs#11
- Some packages in two configuration variants (Development/Production):
  - bootloader
  - Kernel/InitRAMFS
- Regularly turn on more security features during integration
- Once activated, debugging (field returns) becomes a pain
- UBIFS with IMA/EVM doesn't like sudden power cuts

Q & A


F
G
E
D
B
C
A
Downloaded from cubeecraft.com
Toy design by Chris Beaumont cubeecraft@gmail.com
Carefully cut out the shape on this page. Use a hobby knife to slit the white lines labeled with letters as well as the black lines on either side where you will insert the hands. Tape and glue are not necessary. Thicker paper is recommended.
cubeecraft.com
CUBEECRAFT

@marckleinebudde

Pengutronix.