macOS in QEMU

ARM edition

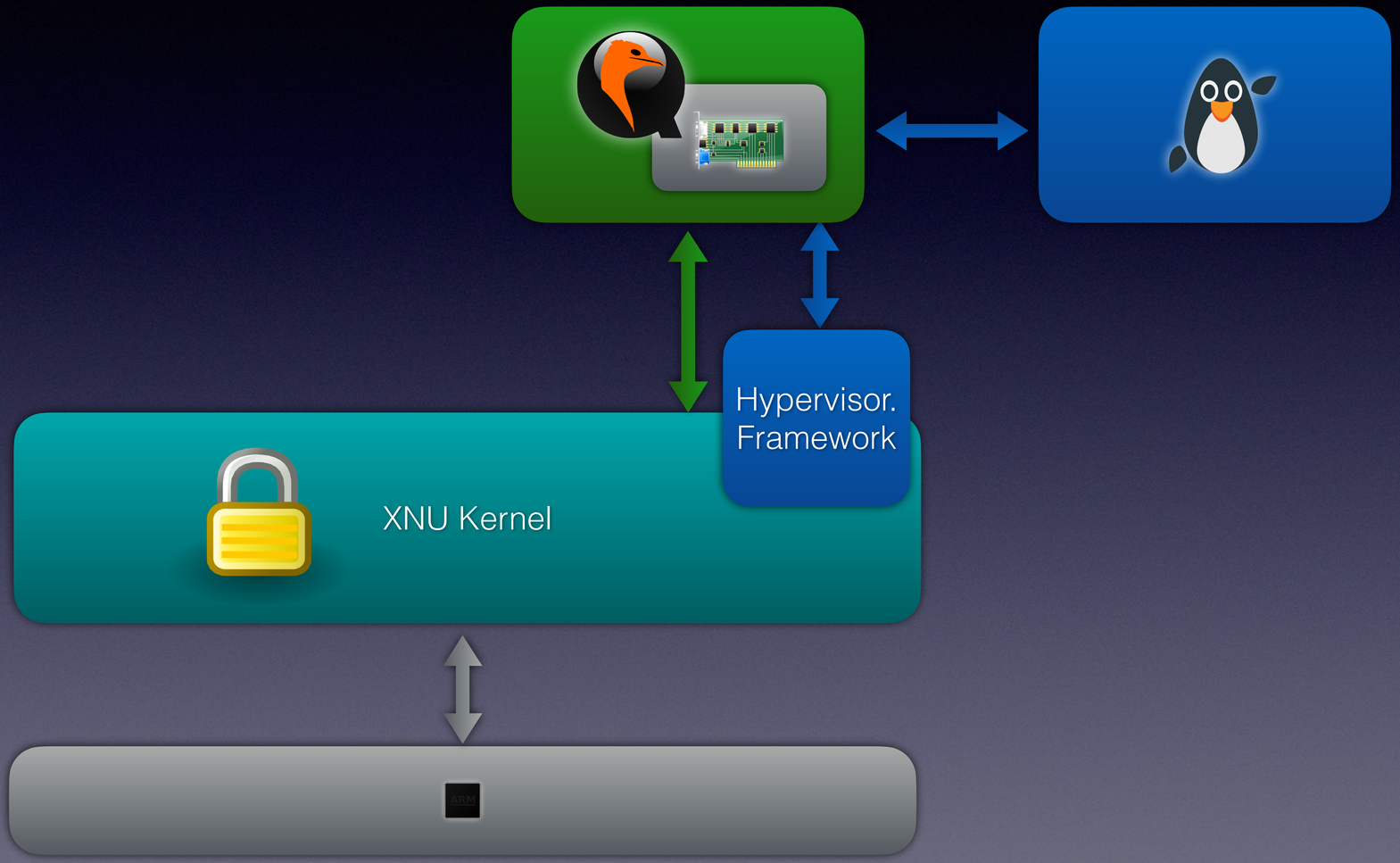
About Me

- Alexander Graf
- EC2 developer at Amazon
- Opinions my own

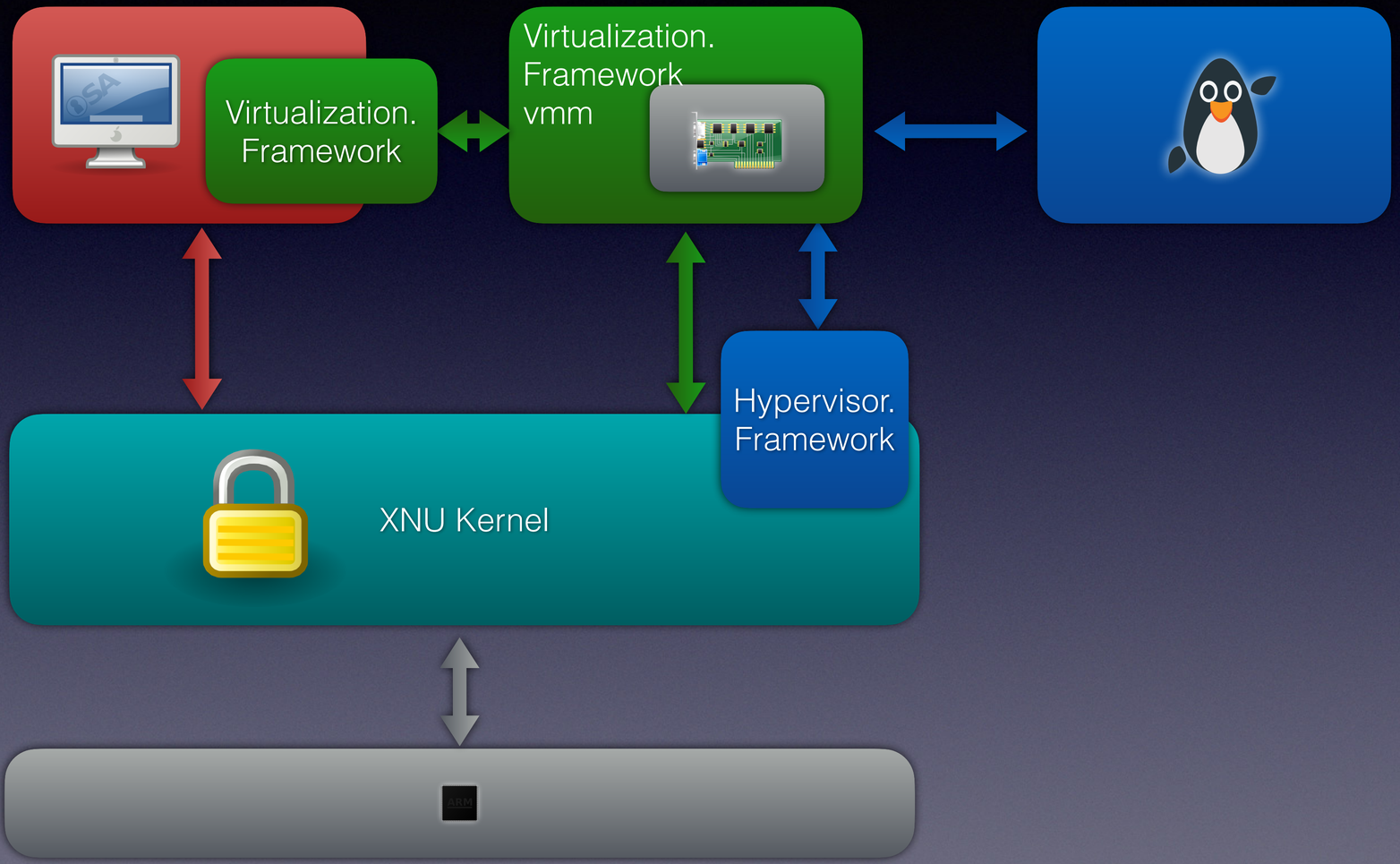
Flashback

QEMU on macOS

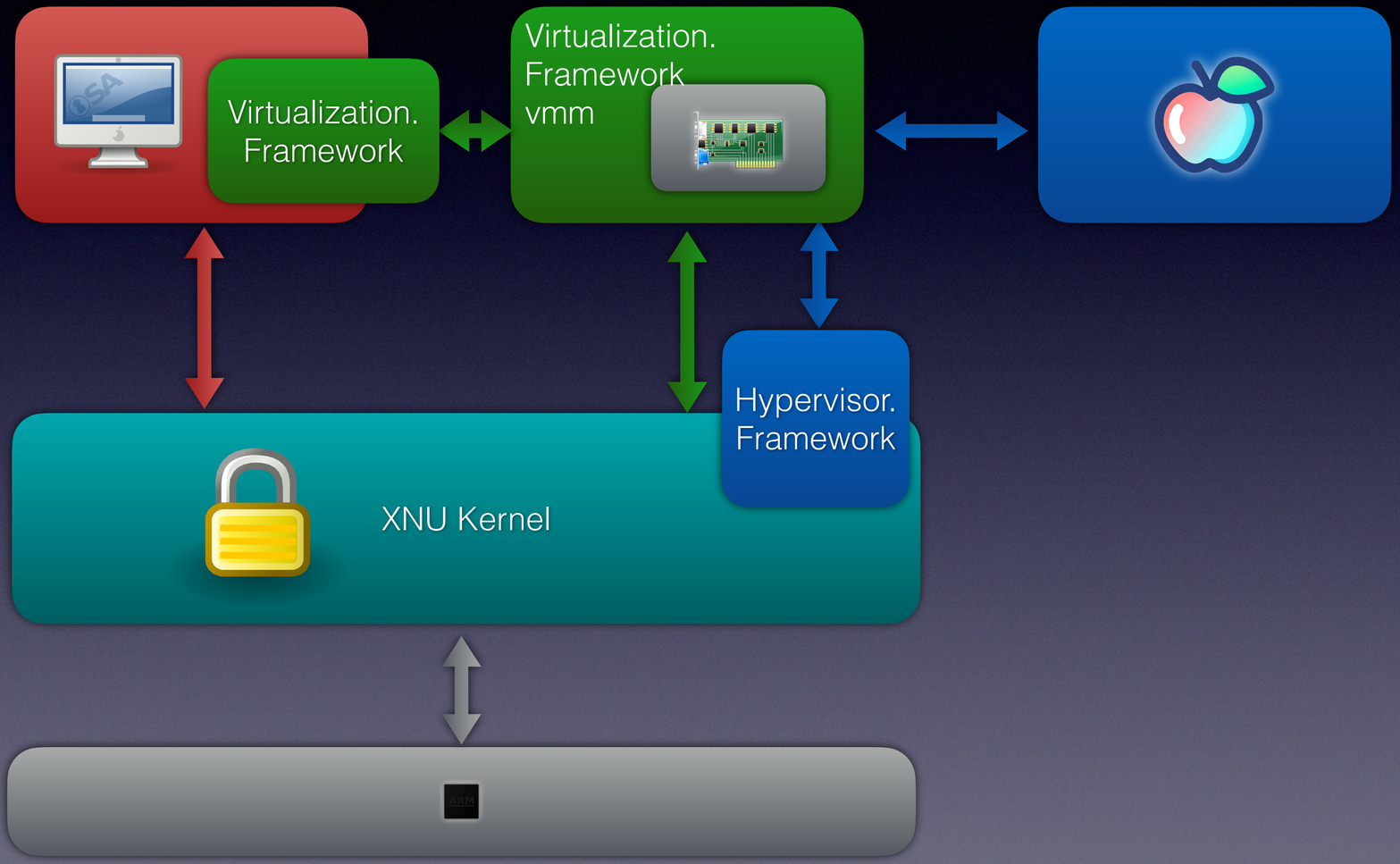
QEMU



Virtualization.Framework



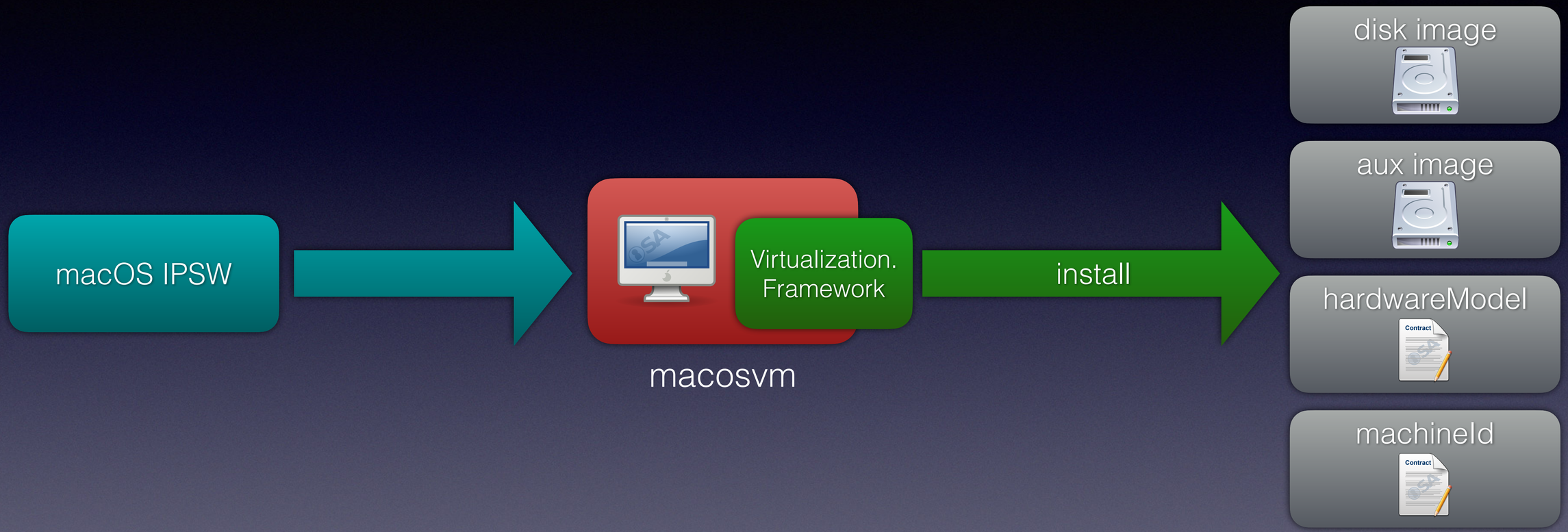
Virtualization.Framework



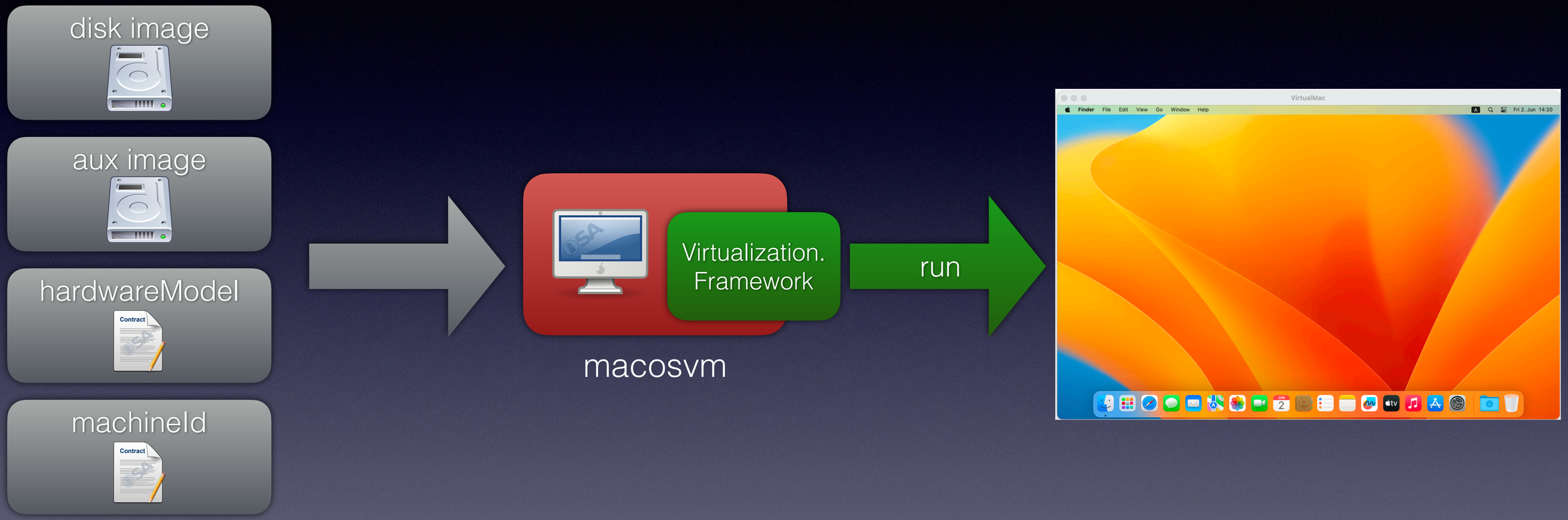
Virtualization.Framework

- macosvm
- UTM
- Parallels
- VirtualBuddy
- …

Virtualization.Framework



Virtualization.Framework



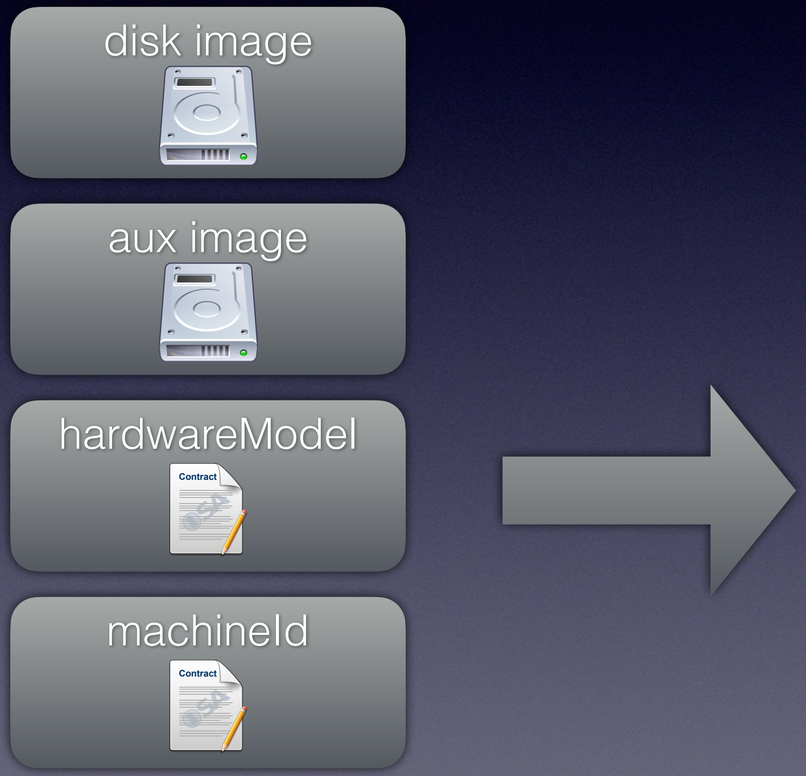
Virtualization.Framework

- Raw disk image
- Root volume encrypted

Virtualization.Framework

- Raw disk image with 16kb header
- “NVRAM” contents
- Copy of iBoot for bootstrap

Virtualization.Framework




```
{
    "DataRepresentationVersion": 1,
    "PlatformVersion": 2,
    "MinimumSupportedOS": [
        13,
        0,
        0
    ]
}
```

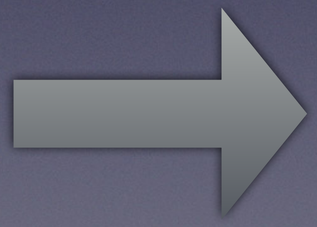
Virtualization.Framework

disk image

aux image

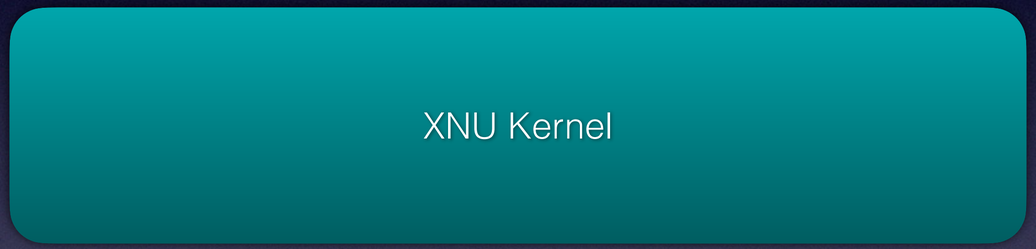
hardwareModel

machineId



```
{
    "ECID": 6058536491512803386
}
```

Virtualization.Framework



Virtualization.Framework

Virtualization.Framework

M1 Pro
M1 Max
M1 Ultra

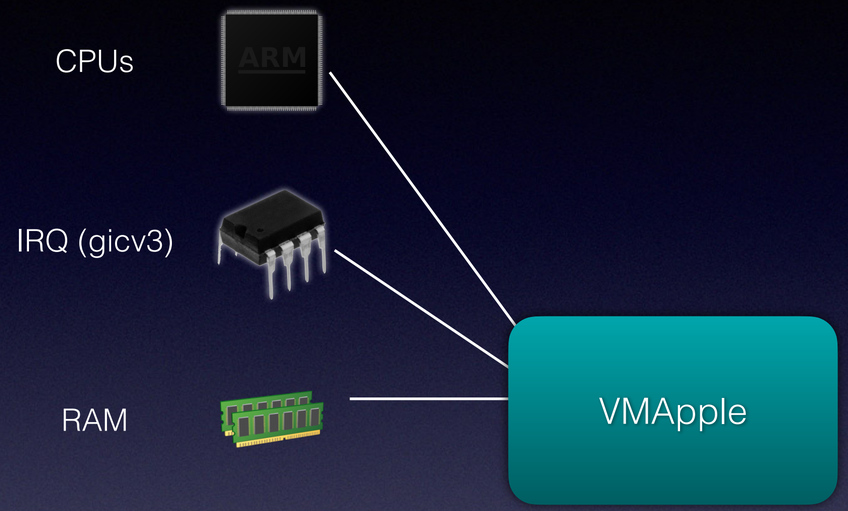
M2 Pro
M2 Max
M2 Ultra

M1

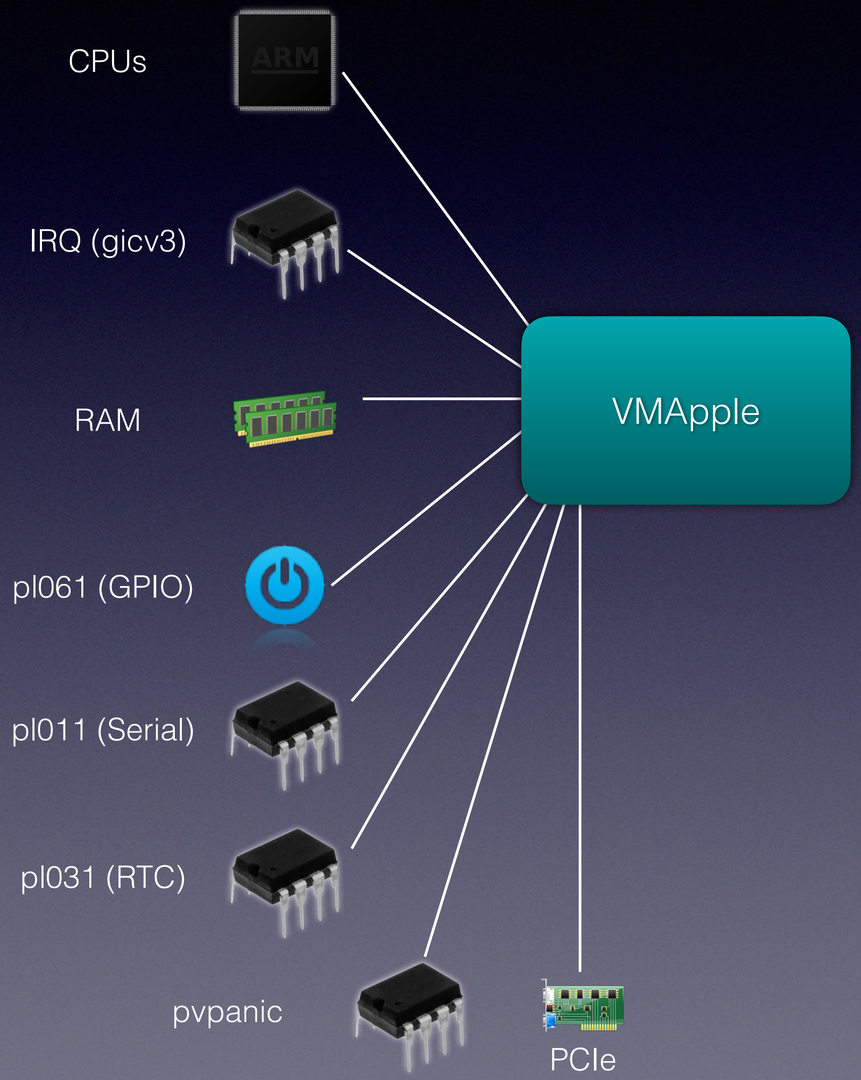
M2

Virtualization.
Framework

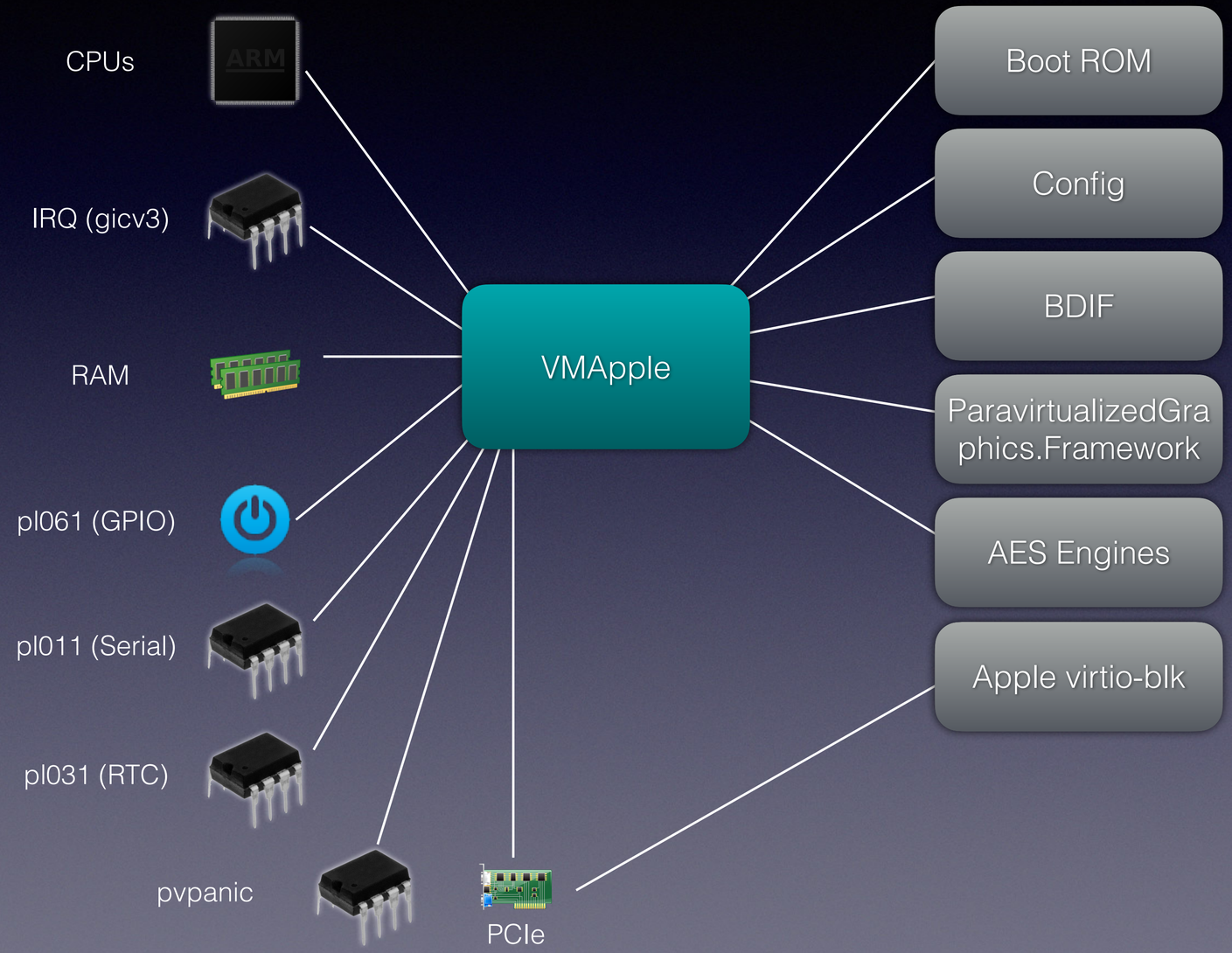
VMApple



VMApple


CPUs
ARM
IRQ (gicv3)
RAM
VMApple
pl061 (GPIO)
pl011 (Serial)
pl031 (RTC)
pvpanic
PCIe

VMApple


CPUs
IRQ (gicv3)
RAM
pl061 (GPIO)
pl011 (Serial)
pl031 (RTC)
pvpanic
PCIe
VMApple
Boot ROM
Config
BDIF
ParavirtualizedGraphics.Framework
AES Engines
Apple virtio-blk

VMApple

Boot ROM

Config

BDIF

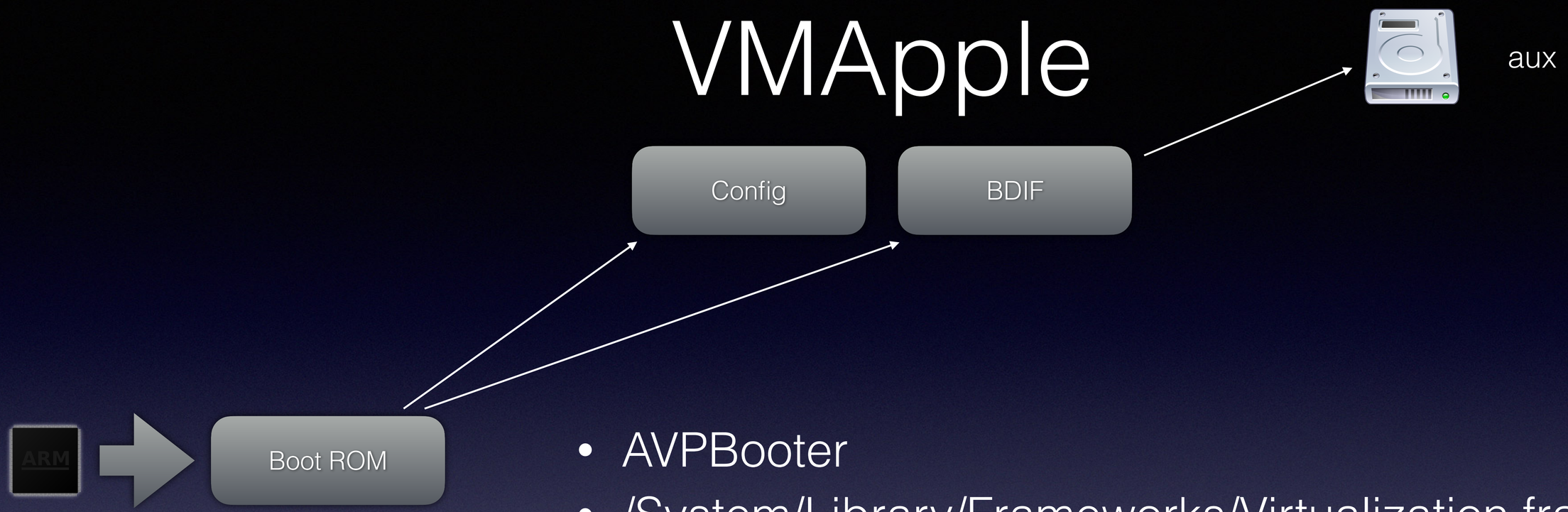
VMApple

Config

BDIF

Boot ROM

VMApple



- AVPBooter
- /System/Library/Frameworks/Virtualization.framework/Resources/AVPBooter.vmapple2.bin
- Special build of iBoot
- Loads stage1 from aux volume

VMApple

aux

Config

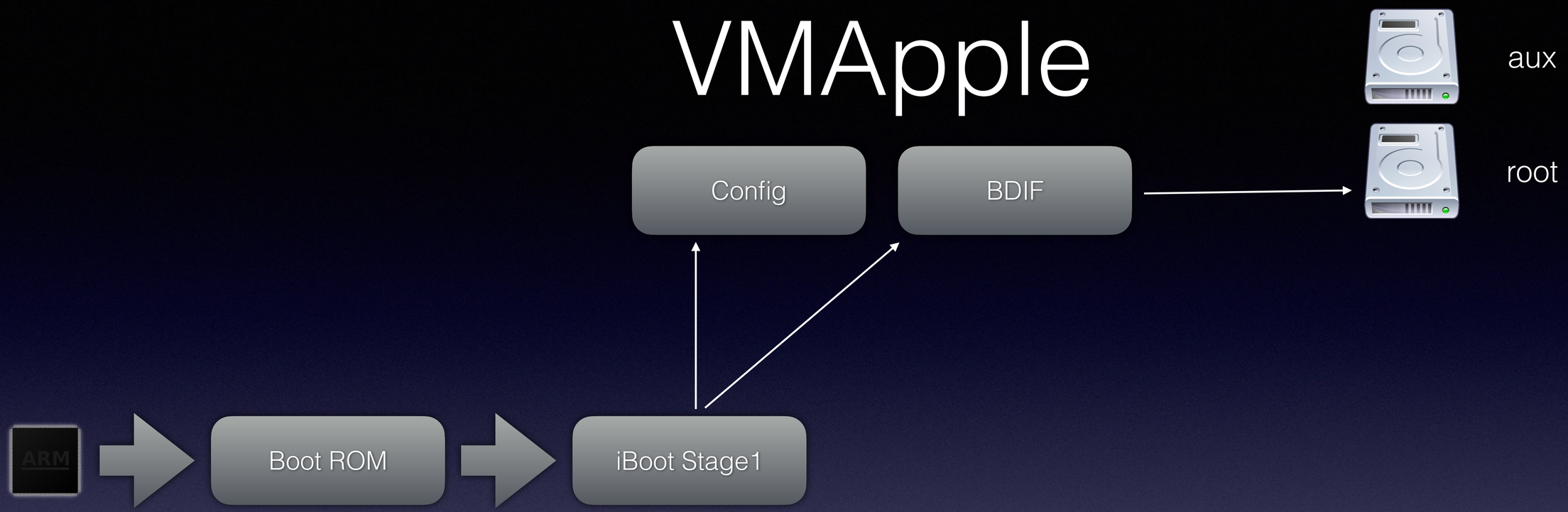
BDIF

Boot ROM

iBoot Stage1

```
=======================================
::
:: 🔥🌸 Supervisor iBootStage1 for vma2, Copyright 2007-2023, Apple Inc.
::
::      Local boot, Board 0x20 (vma2ap)/Rev 0x0
::
::      BUILD_TAG: iBoot-10151.0.82.0.1
::
::      BUILD_STYLE: RELEASE
::
::      USB_SERIAL_NUMBER: SDOM:01 CPID:FE00 CPRV:00 CPFM:03 SCEP:01 BDID:20 ECID:569A2CF311F49B3D IBFL:FD
::
=======================================
```

VMApple




```
========================================
::
:: 🔥🌸 Supervisor iBootStage1 for vma2, Copyright 2007-2023, Apple Inc.
::
::      Local boot, Board 0x20 (vma2ap)/Rev 0x0
::
::      BUILD_TAG: iBoot-10151.0.82.0.1
::
::      BUILD_STYLE: RELEASE
::
::      USB_SERIAL_NUMBER: SDOM:01 CPID:FE00 CPRV:00 CPFM:03 SCEP:01 BDID:20 ECID:569A2CF311F49B3D IBFL:FD
::
========================================
```

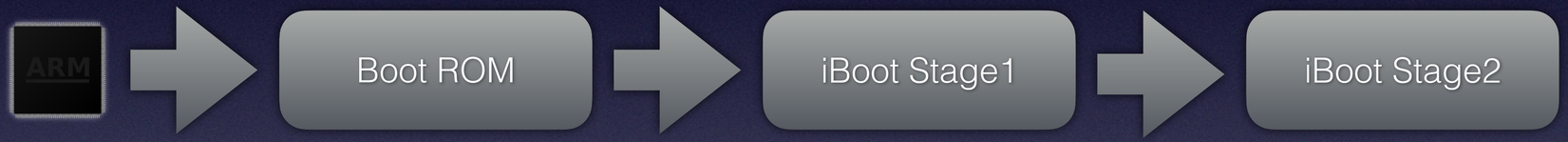
VMApple

aux

root

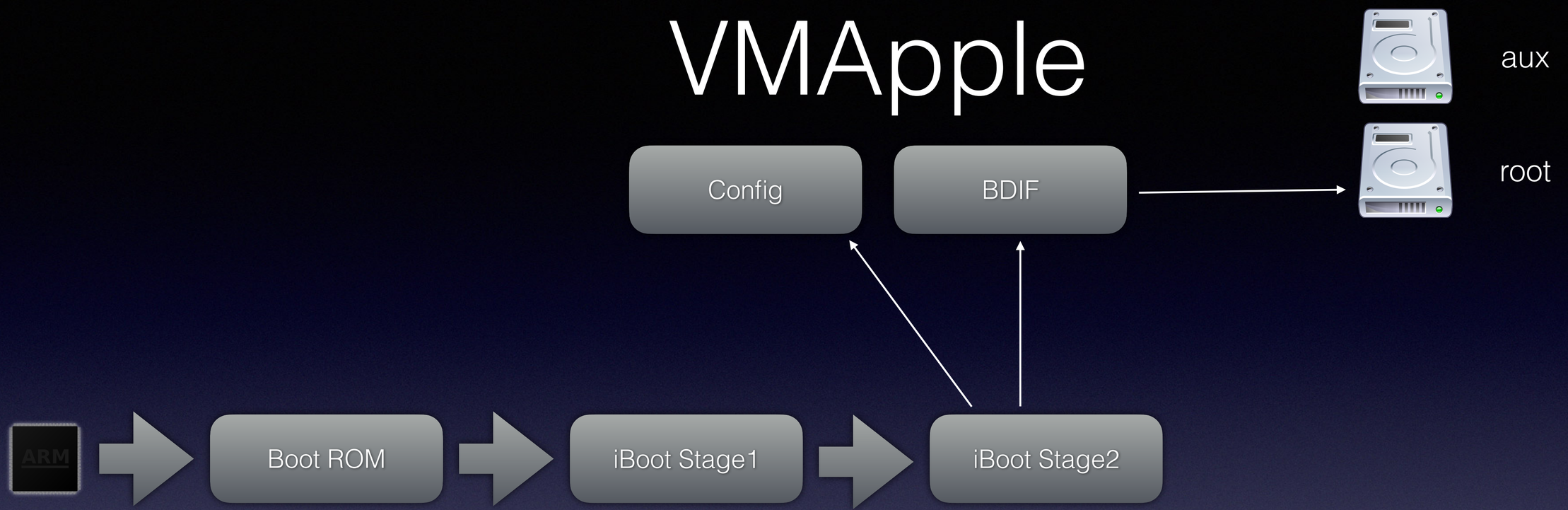
Config

BDIF




```
=======================================
::
:: 🔥🌸 Supervisor iBootStage2 for vma2, Copyright 2007-2023, Apple Inc.
::
::      Local boot, Board 0x20 (vma2ap)/Rev 0x0
::
::      BUILD_TAG: iBoot-10151.0.82.0.1
::
::      BUILD_STYLE: RELEASE
::
::      USB_SERIAL_NUMBER: SDOM:01 CPID:FE00 CPRV:00 CPFM:03 SCEP:01 BDID:20 ECID:569A2CF311F49B3D IBFL:BC SRNM:[1234]
::
=======================================
```

VMApple




```
========================================
::
:: 🔥🌸 Supervisor iBootStage2 for vma2, Copyright 2007-2023, Apple Inc.
::
::      Local boot, Board 0x20 (vma2ap)/Rev 0x0
::
::      BUILD_TAG: iBoot-10151.0.82.0.1
::
::      BUILD_STYLE: RELEASE
::
::      USB_SERIAL_NUMBER: SDOM:01 CPID:FE00 CPRV:00 CPFM:03 SCEP:01 BDID:20 ECID:569A2CF311F49B3D IBFL:BC SRNM:[1234]
::
========================================
```

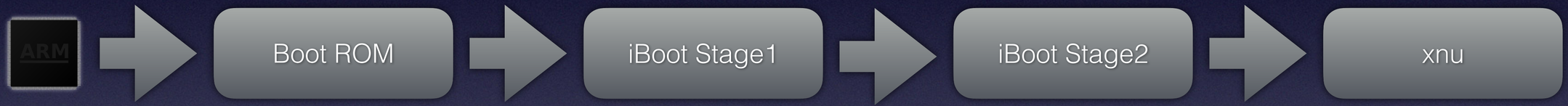
VMApple

Config

BDIF

aux

root



VMApple

Boot ROM

BDIF

aux

root

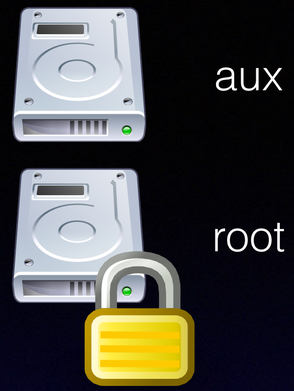
Config

- # of CPUs
- RAM size
- boot mode
- serial
- CPU name
- ECID

VMApple

Boot ROM

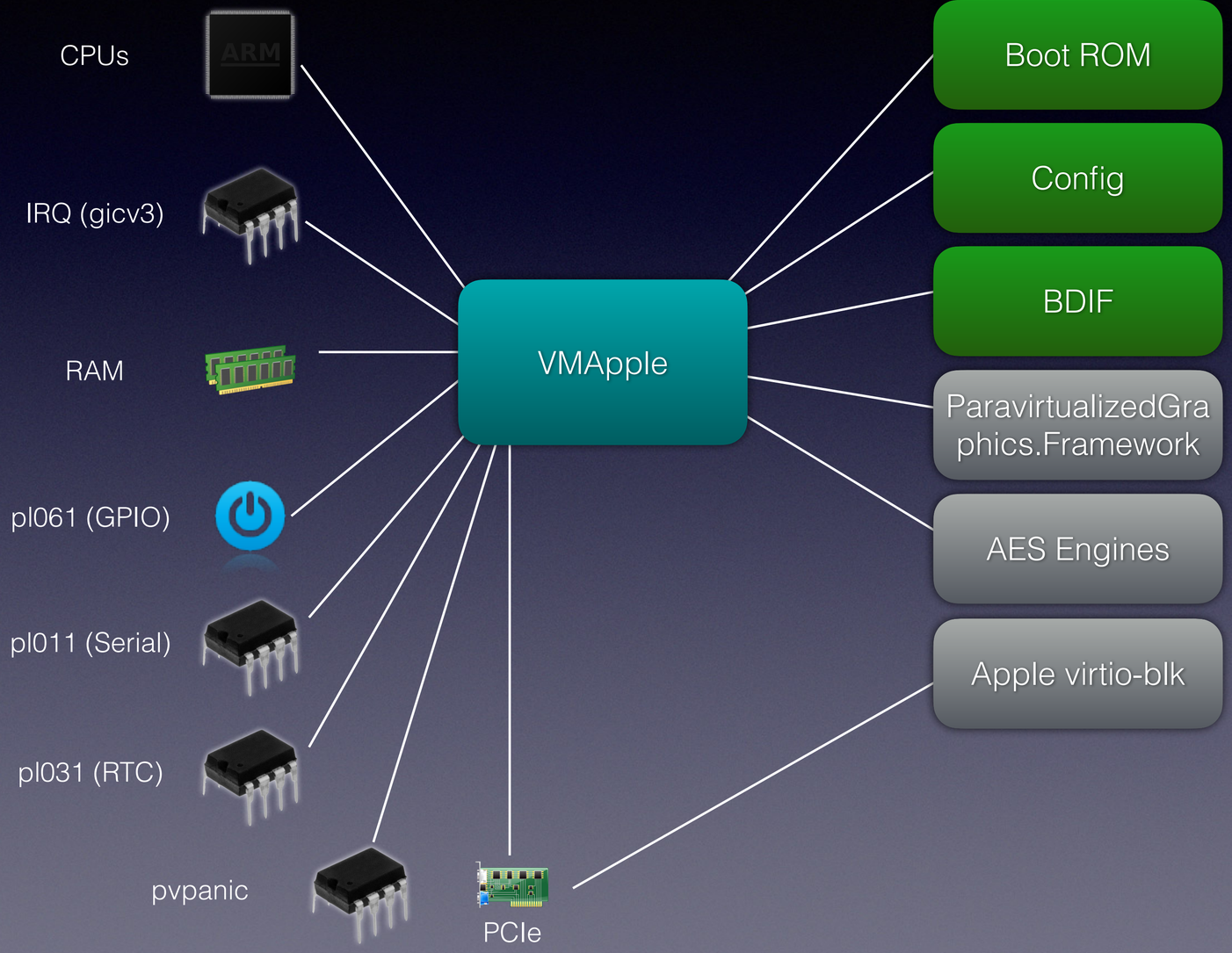
BDIF



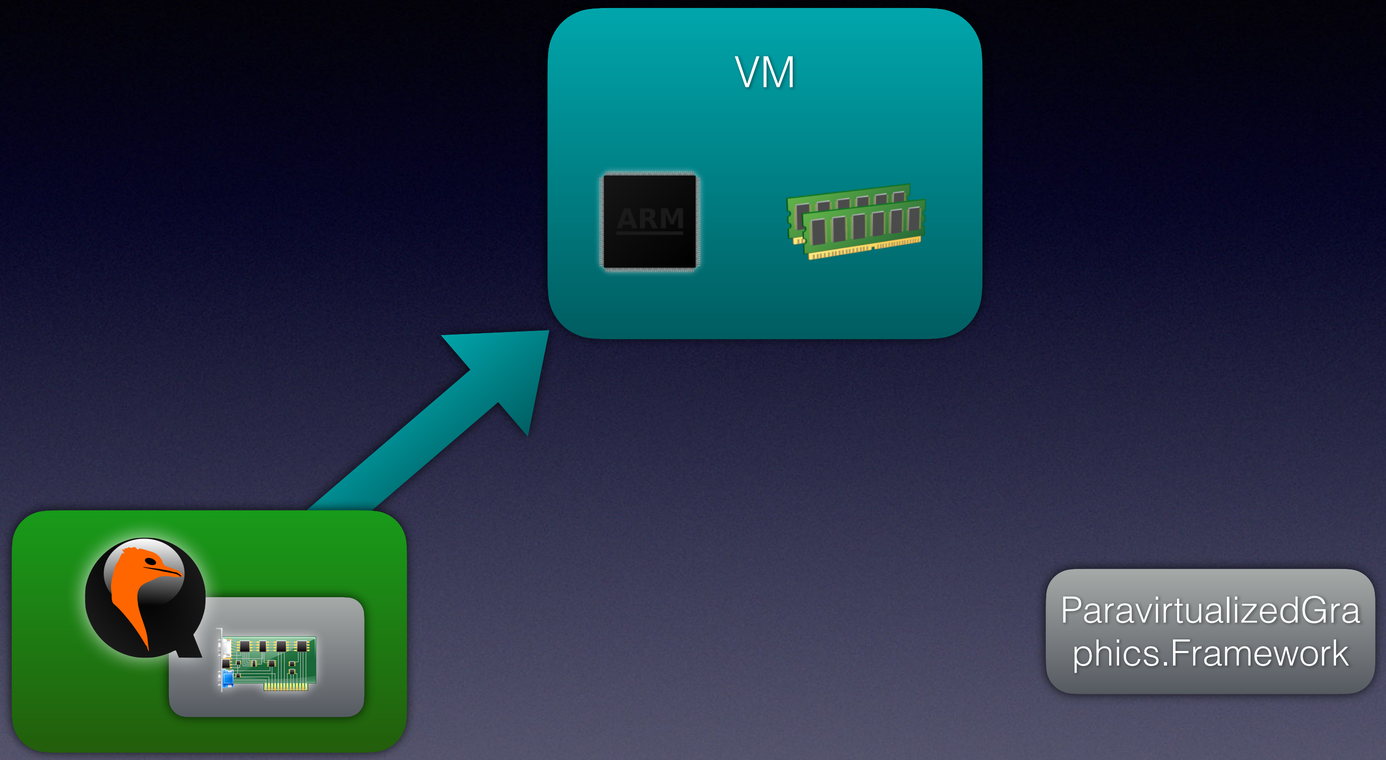
Config

- "Exclusive Chip Identification"
- Unique Chip ID on real devices
- Used as encryption key for the root volume

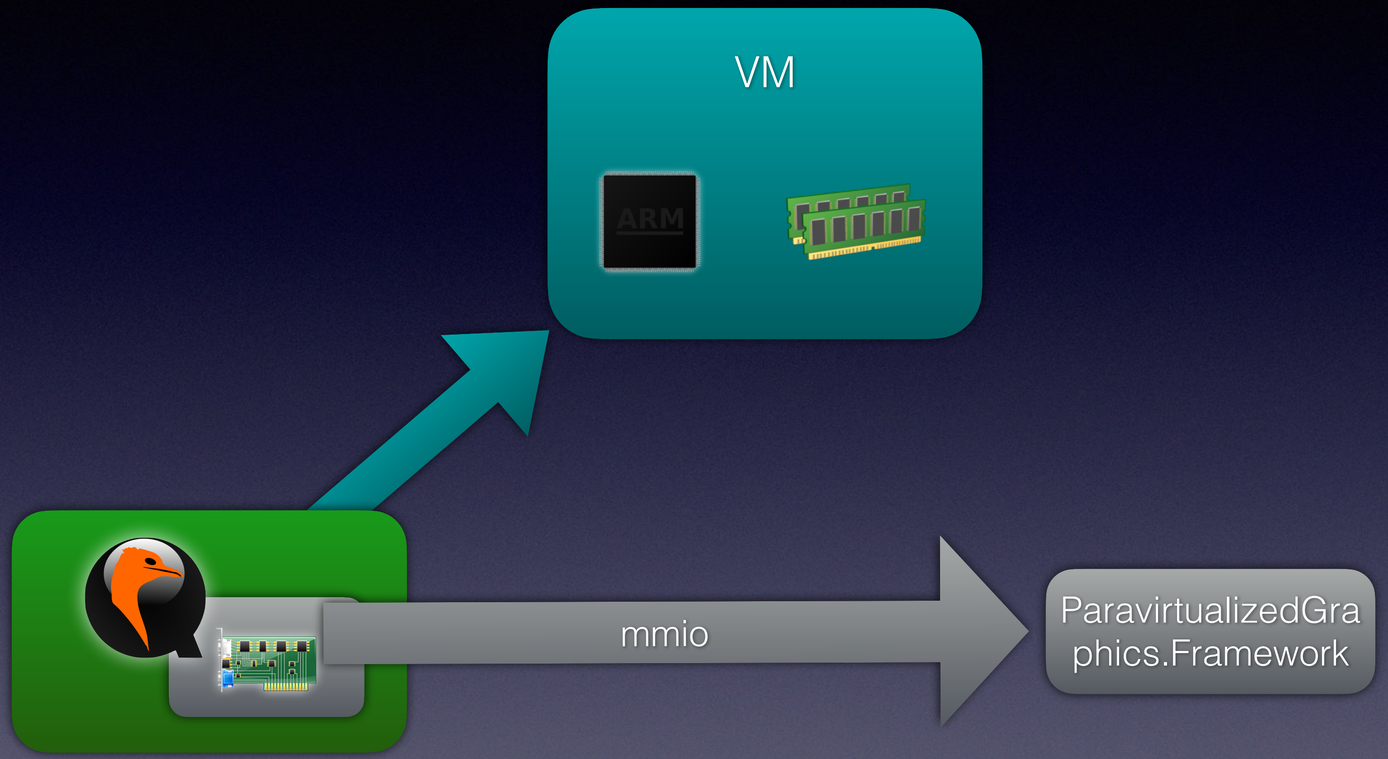
VMApple


CPUs
IRQ (gicv3)
RAM
pl061 (GPIO)
pl011 (Serial)
pl031 (RTC)
pvpanic
PCIe
VMApple
Boot ROM
Config
BDIF
ParavirtualizedGraphics.Framework
AES Engines
Apple virtio-blk

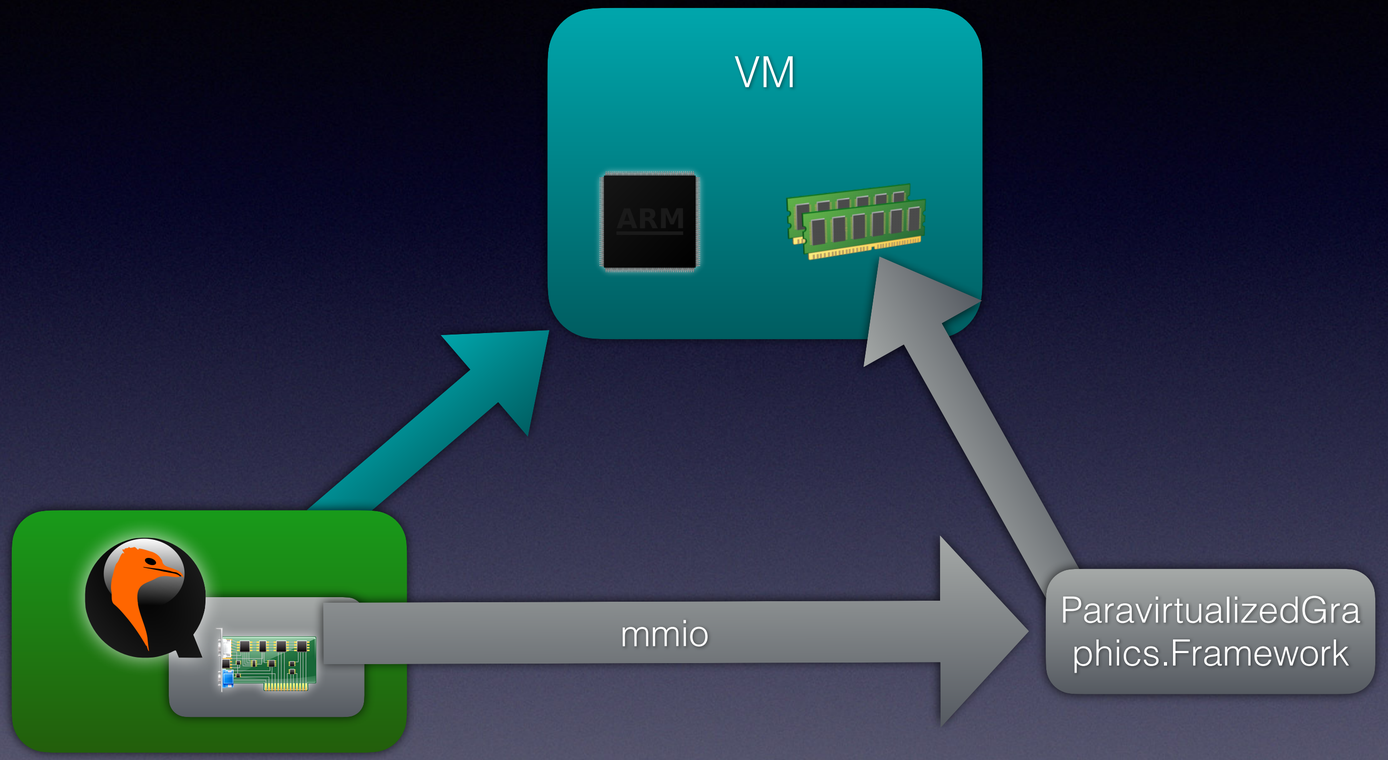
VMApple



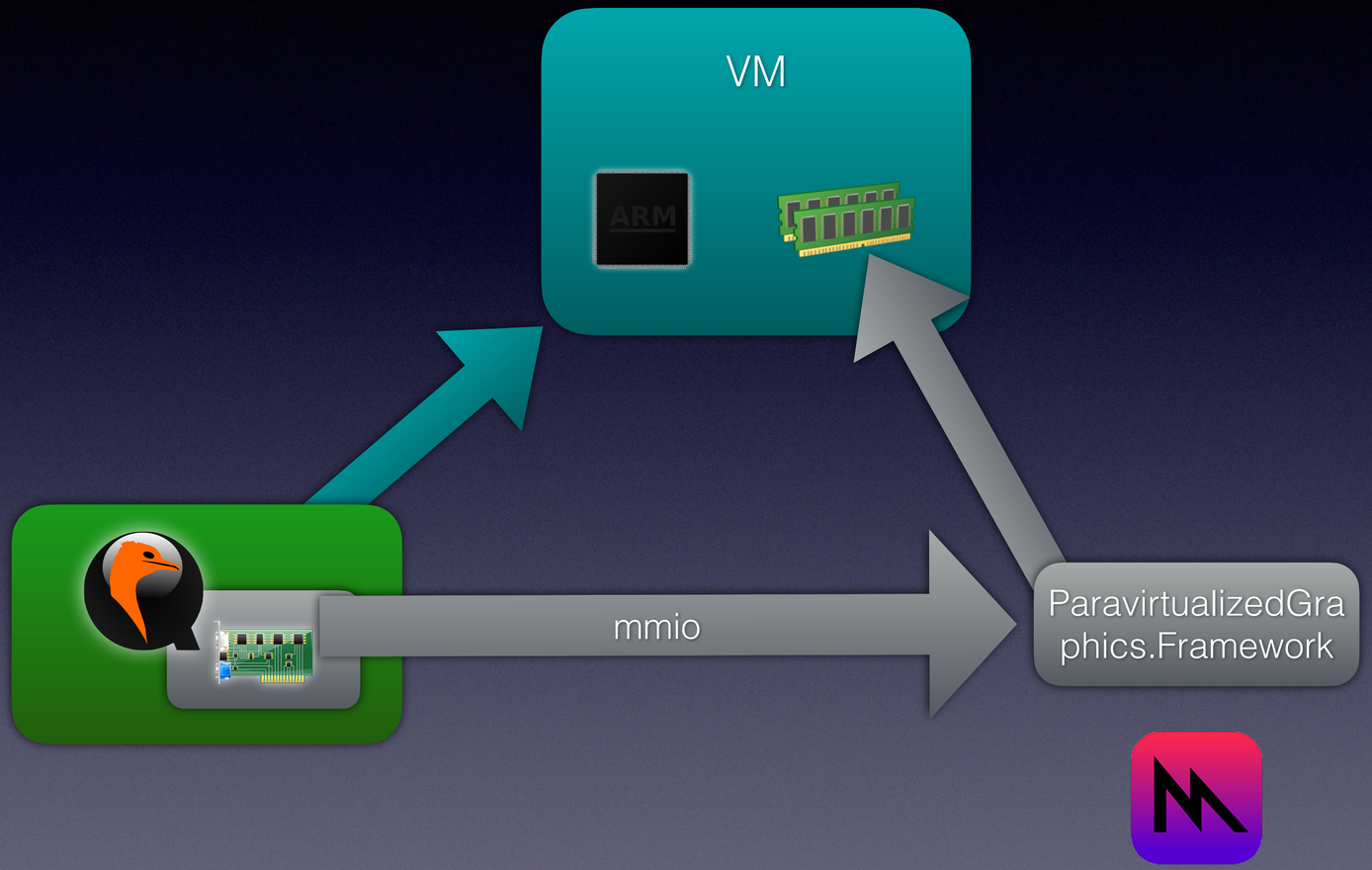
VMApple



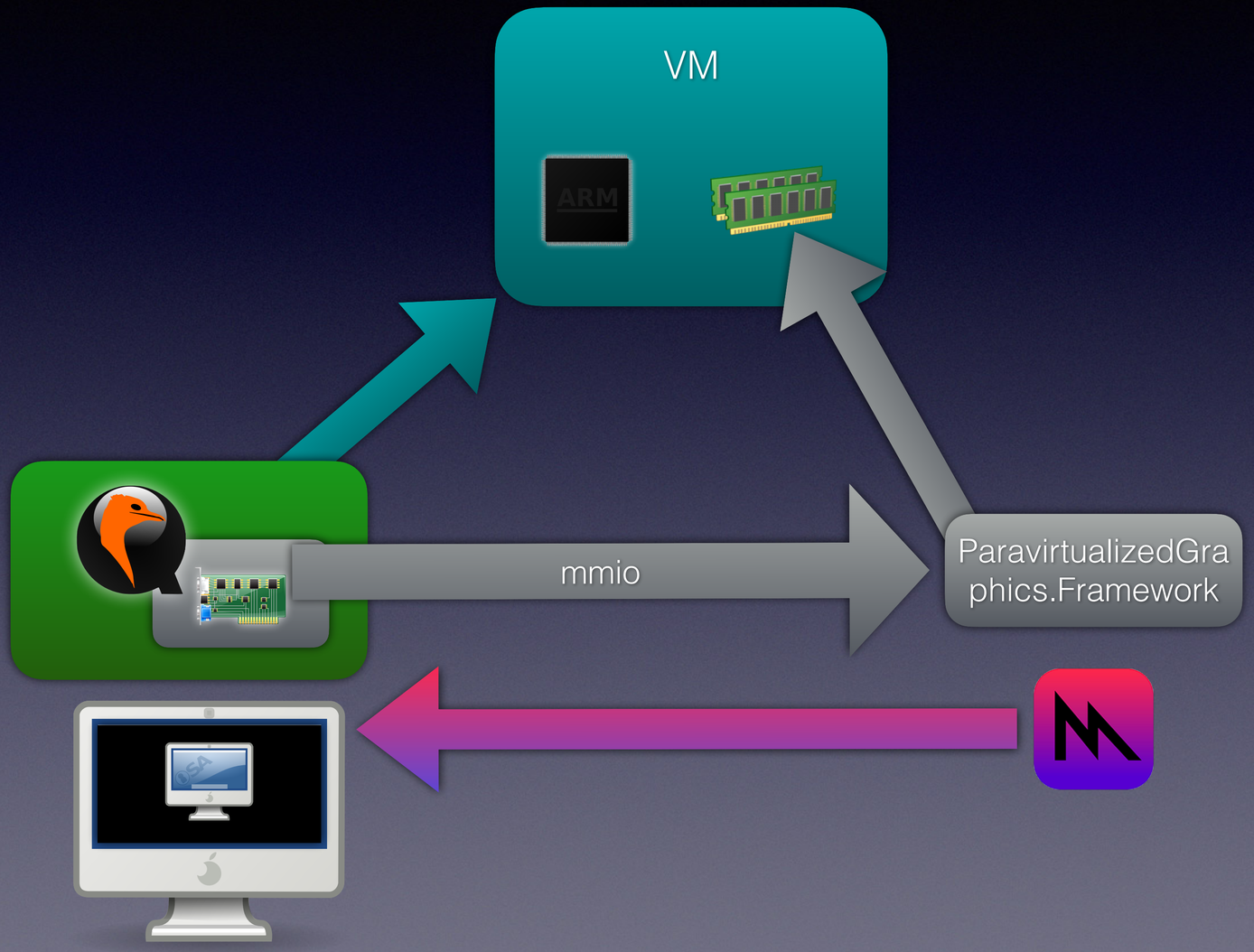
VMApple



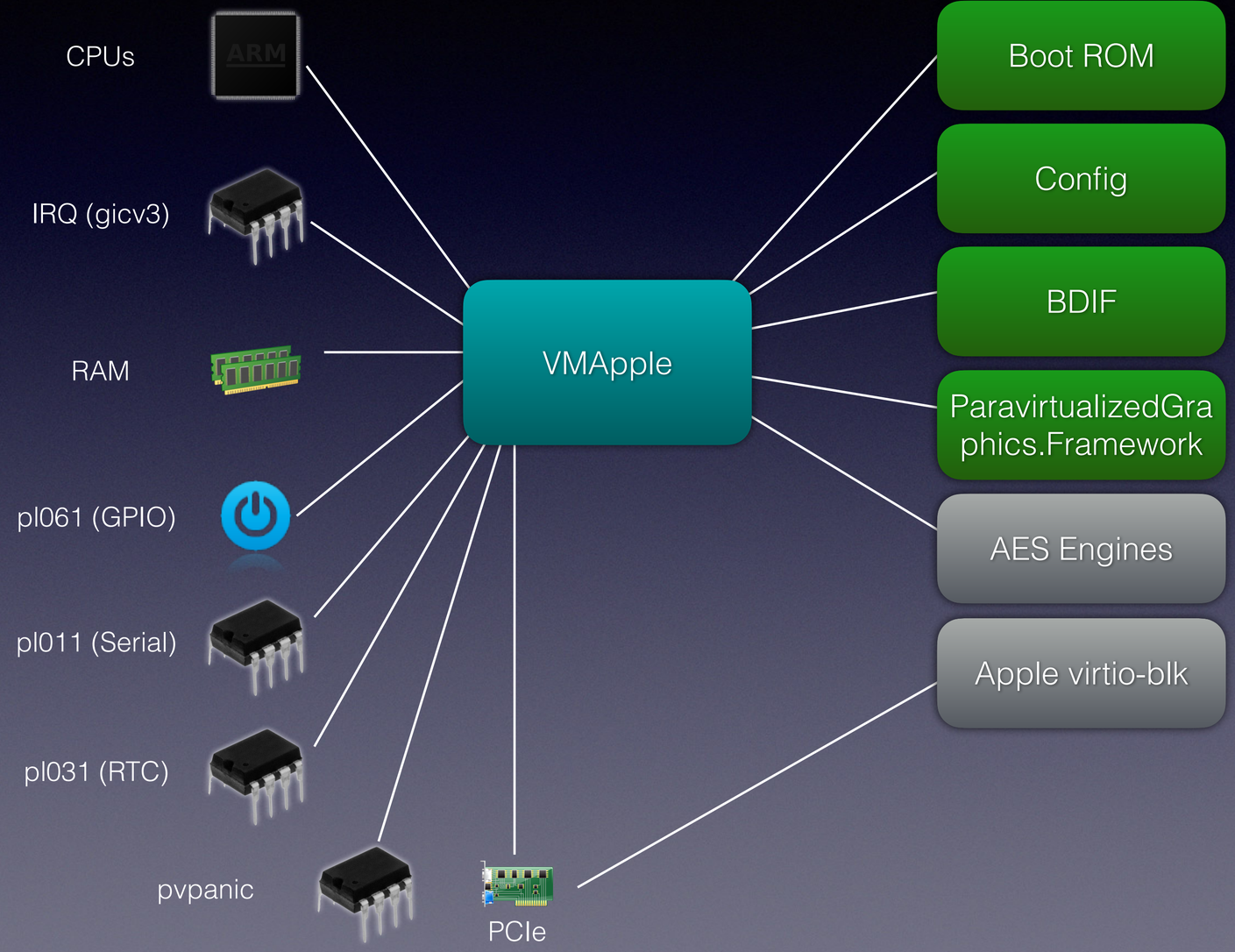
VMApple



VMApple



VMApple


CPUs
IRQ (gicv3)
RAM
pl061 (GPIO)
pl011 (Serial)
pl031 (RTC)
pvpanic
PCIe
VMApple
Boot ROM
Config
BDIF
ParavirtualizedGraphics.Framework
AES Engines
Apple virtio-blk

VMApple

AES Engines

- Same device as in iPhones / iPads
- Used for hashing of data, including root volume
- Contains embedded keys. On real hardware hopefully random.

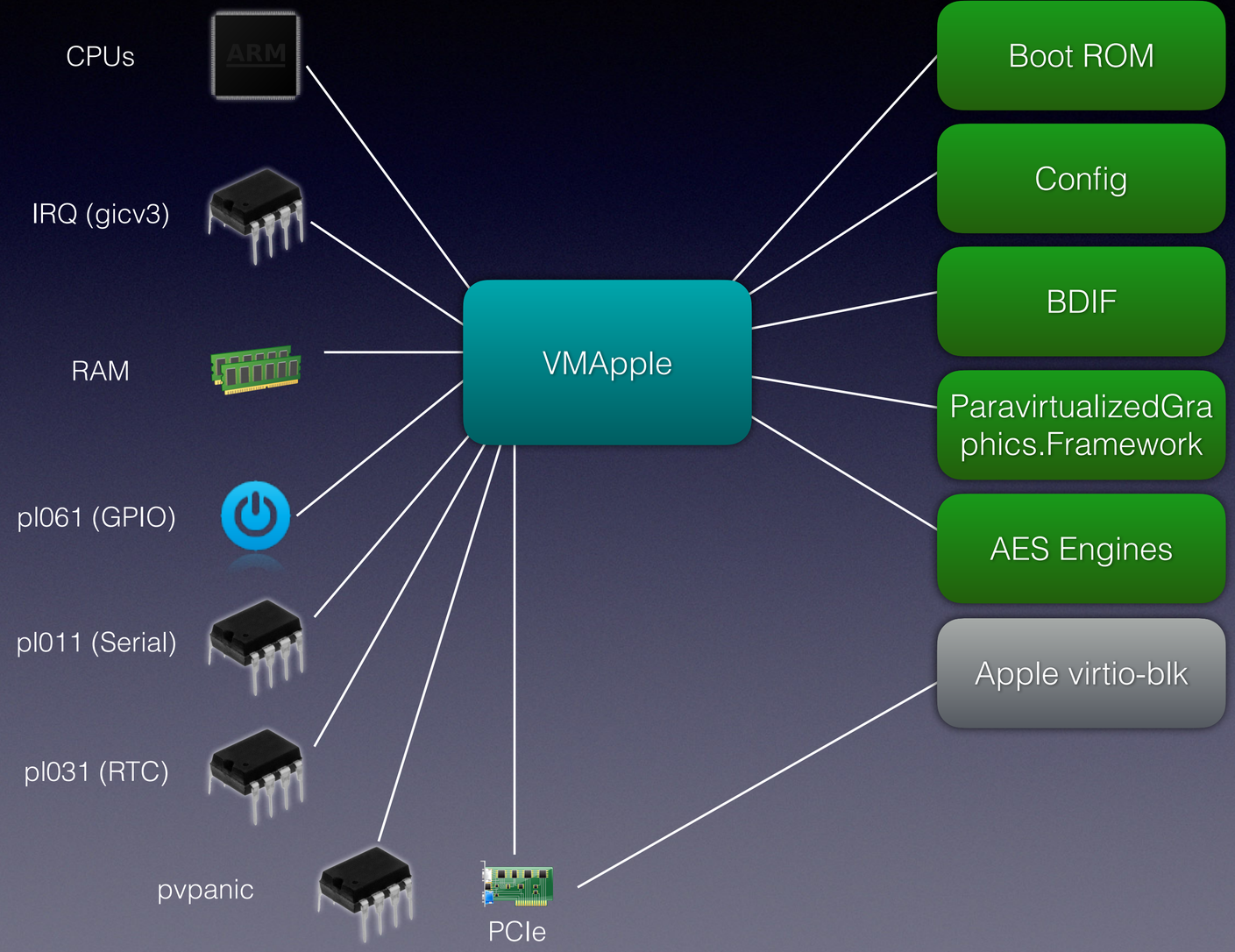
VMApple

AES Engines

- Same device as in iPhones / iPads
- Used for hashing of data, including root volume
- Contains embedded keys. On real hardware hopefully random.

```
static struct key builtin_keys[7] = {
    [1] = { .key_len = 32, .key = { 0x1 }, },
    [2] = { .key_len = 32, .key = { 0x2 }, },
    [3] = { .key_len = 32, .key = { 0x3 },
    }
};
```

VMApple


CPUs
IRQ (gicv3)
RAM
pl061 (GPIO)
pl011 (Serial)
pl031 (RTC)
pvpanic
PCIe
VMApple
Boot ROM
Config
BDIF
ParavirtualizedGraphics.Framework
AES Engines
Apple virtio-blk

VMApple

Apple virtio-blk

- Different PCI device/vendor ID
- Hard coded "Apple Device Type (aux/root)" offset in cfg space, collides with zone extension
- New blk command, probably a special variant of "TRIM" with zeroing semantics

VMApple in QEMU

Patches are on the list, please review!

```
f02f4b0103c5:qemu graf$ git log --oneline origin/master..vmapple2-v1
aa142d5ccc (HEAD -> vmapple2-v1) hw/vmapple/vmapple: Add vmapple machine type
01f7b9ff6f hw/vmapple/apple-gfx: Introduce ParavirtualizedGraphics.Framework support
279e9304ae hw/vmapple/cfg: Introduce vmapple cfg region
dacc991e0a hw/vmapple/bdif: Introduce vmapple backdoor interface
dd69093b78 hw/vmapple/aes: Introduce aes engine
4538784d04 gpex: Allow more than 4 legacy IRQs
7682dc62f4 hw: Add vmapple subdir
340d6b94da hw/virtio: Add support for apple virtio-blk
53b8581614 hvf: arm: Ignore writes to CNTP_CTL_EL0
bdec441d8a hvf: Increase number of possible memory slots
6ea339cff8 hw/misc/pvpanic: Add MMIO interface
32fb67ee30 build: Only define OS_OBJECT_USE_OBJC with gcc
```

```
$ git diff --stat origin/master..vmapple2-v1
 accel/hvf/hvf-accel-ops.c                          |   2 +-
 configs/devices/arm-softmmu/default.mak            |   1 +
 hw/Kconfig                                         |   1 +
 hw/arm/sbsa-ref.c                                  |   2 +-
 hw/arm/virt.c                                      |   2 +-
 hw/block/virtio-blk.c                              |  23 +
 hw/i386/microvm.c                                  |   2 +-
 hw/loongarch/virt.c                                |   2 +-
 hw/meson.build                                     |   1 +
 hw/mips/loongson3_virt.c                           |   2 +-
 hw/misc/Kconfig                                    |   4 +
 hw/misc/meson.build                                |   1 +
 hw/misc/pvpanic-mmio.c                             |  66 +++
 hw/openrisc/virt.c                                 |  12 +-
 hw/pci-host/gpex.c                                 |  36 +-
 hw/riscv/virt.c                                    |  12 +-
 hw/virtio/virtio-blk-pci.c                         |   7 +
 hw/vmapple/Kconfig                                 |  29 ++
 hw/vmapple/aes.c                                   | 582 ++++++++++++++++++++++
 hw/vmapple/apple-gfx.m                             | 578 ++++++++++++++++++++++
 hw/vmapple/bdif.c                                  | 244 ++++++++++
 hw/vmapple/cfg.c                                   | 105 +++++
 hw/vmapple/meson.build                             |   5 +
 hw/vmapple/trace-events                            |  47 ++
 hw/vmapple/trace.h                                 |   1 +
 hw/vmapple/vmapple.c                               | 658 ++++++++++++++++++++++++
 hw/xtensa/virt.c                                   |   2 +-
 include/hw/misc/pvpanic.h                          |   1 +
 include/hw/pci-host/gpex.h                         |   7 +-
 include/hw/pci/pci_ids.h                           |   1 +
 include/hw/virtio/virtio-blk.h                     |   1 +
 include/hw/vmapple/bdif.h                          |  31 ++
 include/hw/vmapple/cfg.h                           |  68 +++
 include/standard-headers/linux/virtio_blk.h        |   3 +
 include/sysemu/hvf_int.h                           |   2 +-
 meson.build                                        |   9 +-
 target/arm/hvf/hvf.c                               |   7 +
 37 files changed, 2527 insertions(+), 30 deletions(-)
```

How to use

disk image

aux image

hardwareModel

machineId

How to use

disk image

aux image

hardwareModel

machineId

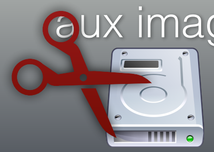
-drive if=pflash,index=0

-drive if=none,id=root -device virtio-blk-pci,drive=root,x-apple-type=1

How to use

disk image

aux image



hardwareModel

machineId

-drive if=pflash,index=0

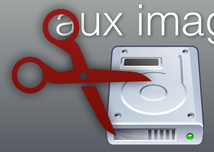
-drive if=none,id=root -device virtio-blk-pci,drive=root,x-apple-type=1

```
$ dd if=aux.img of=aux.img.trimmed bs=$(( 0x4000 )) skip=1
```

How to use

disk image

aux image



hardwareModel

machineId

-drive if=pflash,index=0

-drive if=none,id=root -device virtio-blk-pci,drive=root,x-apple-type=1

-drive if=pflash,index=1

-drive if=none,id=aux -device virtio-blk-pci,drive=aux,x-apple-type=2

How to use

-drive if=pflash,index=0

-drive if=none,id=root -device virtio-blk-pci,drive=root,x-apple-type=1

-drive if=pflash,index=1

-drive if=none,id=aux -device virtio-blk-pci,drive=aux,x-apple-type=2

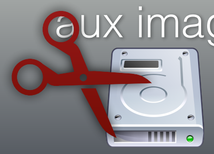
How to use

disk image

-drive if=pflash,index=0

-drive if=none,id=root -device virtio-blk-pci,drive=root,x-apple-type=1

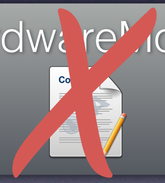
aux image



-drive if=pflash,index=1

-drive if=none,id=aux -device virtio-blk-pci,drive=aux,x-apple-type=2

hardwareModel



machineId


```
$ cat "$DIR/macosvm.json" |                                                  \
  python3 -c 'import json,sys;obj=json.load(sys.stdin);print(obj["machineId"]) |  \
  base64 -d |                                                                \
  plutil -extract ECID raw -
```

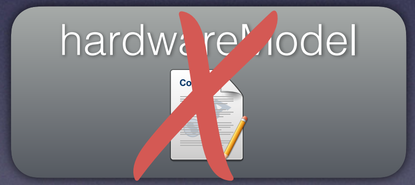
How to use

-drive if=pflash,index=0

-drive if=none,id=root -device virtio-blk-pci,drive=root,x-apple-type=1

-drive if=pflash,index=1

-drive if=none,id=aux -device virtio-blk-pci,drive=aux,x-apple-type=2



-M vmapple,uuid=1234

How to use

```
$ qemu-system-aarch64 -serial mon:stdio                                                  \
  -m 4G                                                                                  \
  -M vmapple,uuid=6240349656165161789                                                    \
  -bios /System/Library/Frameworks/Virtualization.framework/Resources/AVPBooter.vmapple2.bin  \
  -pflash aux.img.trimmed                                                                \
  -pflash disk.img                                                                       \
  -drive file=disk.img,if=none,id=d -device virtio-blk-pci,drive=d,x-apple-type=1         \
  -drive file=aux.img.trimmed,if=none,id=a -device virtio-blk-pci,drive=a,x-apple-type=2  \
  -accel hvf
```

Demo


QEMU
Finder File Edit View Go Window Help
Tue 13. Jun 04:39
JUN
13
tv

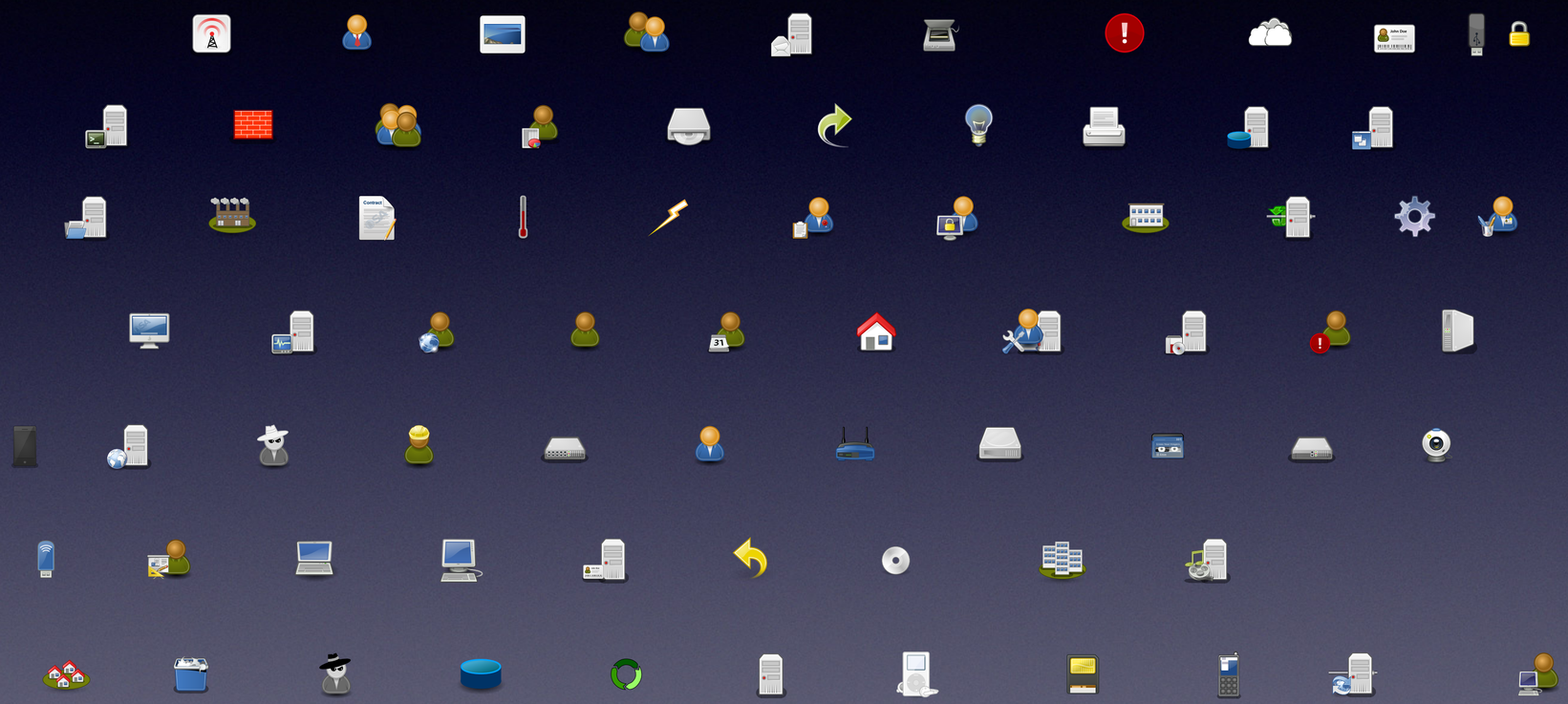
Issues

- Interrupts not always stable (no keyboard)
- No access to Total Store Ordering -> no Rosetta
- MacOS host only
- Should do an OSS rewrite of AVPBooter

Questions?

Thank You

OSA Icons



Icons received from http://www.opensecurityarchitecture.org/cms/library/icon-library

Other Icons

http://findicons.com/icon/202613/folder_library

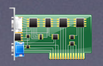
http://findicons.com/icon/download/234261/clock/128/png

http://findicons.com/icon/439269/button_power

https://fosdem.org/2017/schedule/event/grub_new_maintainers/attachments/slides/1768/export/events/attachments/grub_new_maintainers/slides/1768/slides.pdf

https://de.wikipedia.org/wiki/BeagleBoard#/media/File:Beagle_Board_big.jpg

https://thenounproject.com/term/folder-tree/27307/



https://commons.wikimedia.org/wiki/File:Crystal_Project_Hardware.png

https://developer.apple.com/assets/elements/icons/metal/metal-96x96_2x.png

emojione Icons



Icons received from http://www.opensecurityarchitecture.org/cms/library/icon-library

DALL-E

Icons generated with https://www.bing.com/images/create

External Sources

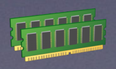
https://commons.wikimedia.org/wiki/File:Spectre_logo_with_text.svg

https://commons.wikimedia.org/wiki/File:USB_icon.svg

https://commons.wikimedia.org/wiki/File:150-8-DIP.jpg

https://commons.wikimedia.org/wiki/File:Hdd_icon.svg

https://commons.wikimedia.org/wiki/File:ARM_CPU_icon.svg



http://findicons.com/icon/177982/memory#

https://www.linux-kvm.org/page/Main_Page

https://commons.wikimedia.org/wiki/File:Keyboard-icon_Wikipedians.svg