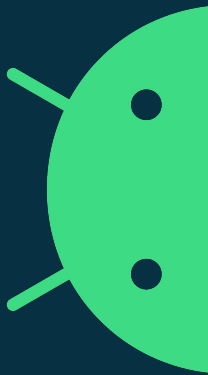


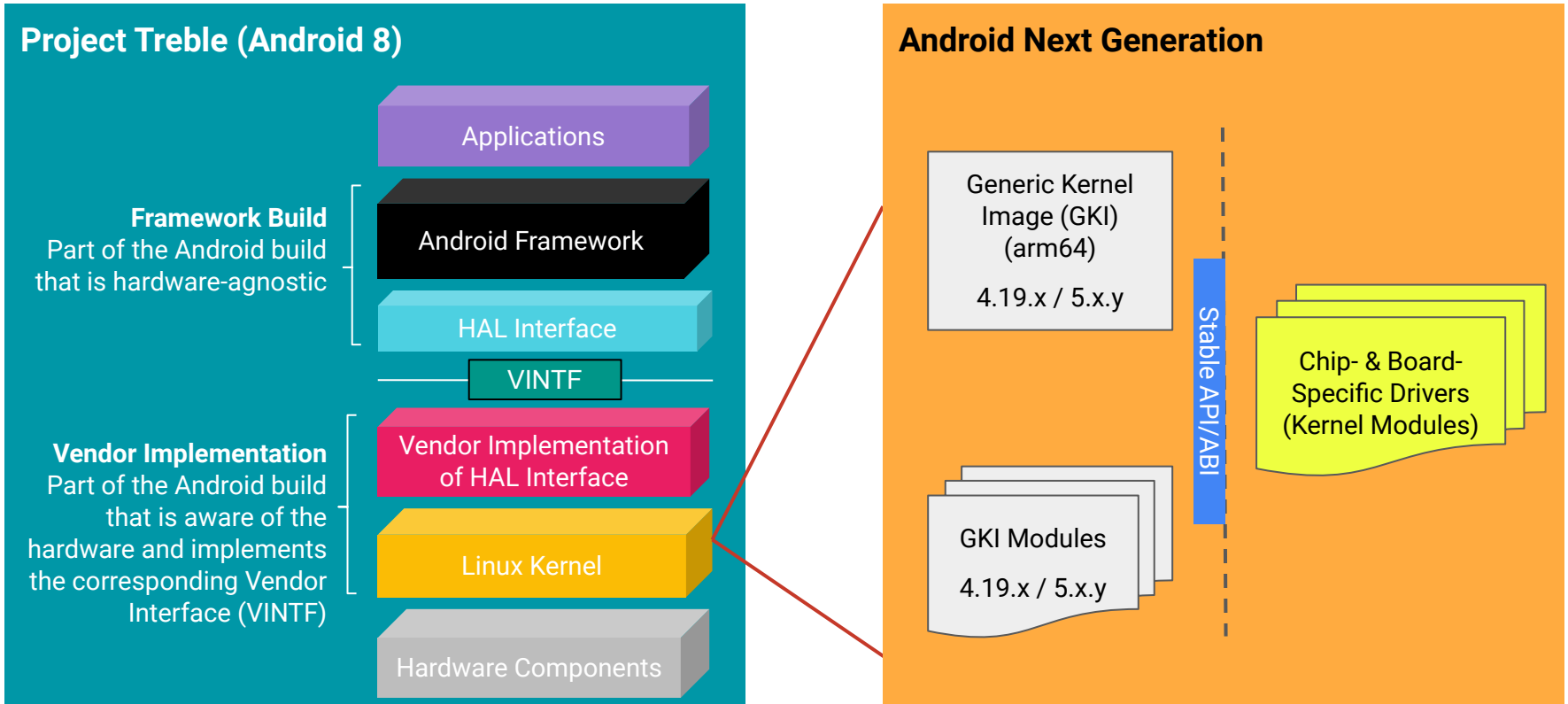
# GKI Enforcement Tools

An update on ABI Monitoring

Matthias Männich - Linux Plumbers 2020



# Stable ABIs for Android Kernels



# Stable ABI within Boundaries

and how Android implements that

## Branches

- Only keep ABI stable within major upstream branch
- Stable per Android version
- E.g. LTS 4.19, 5.4, 5.y

- android-4.19-stable
- android11-5.4
- android12-5.4
- android12-5.yx

## Configuration

- Single Kernel Configuration
- Suitable for all vendors
- Configuration changes allowed if they don't break ABI

- Generic Kernel Image (GKI) configuration  
(gki\_defconfig)

## Toolchain

- Single Toolchain
- Hermetic Build

- Clang Build (only)
- Clang tools (nm, objcopy, ...)
- Hermetic Toolchain

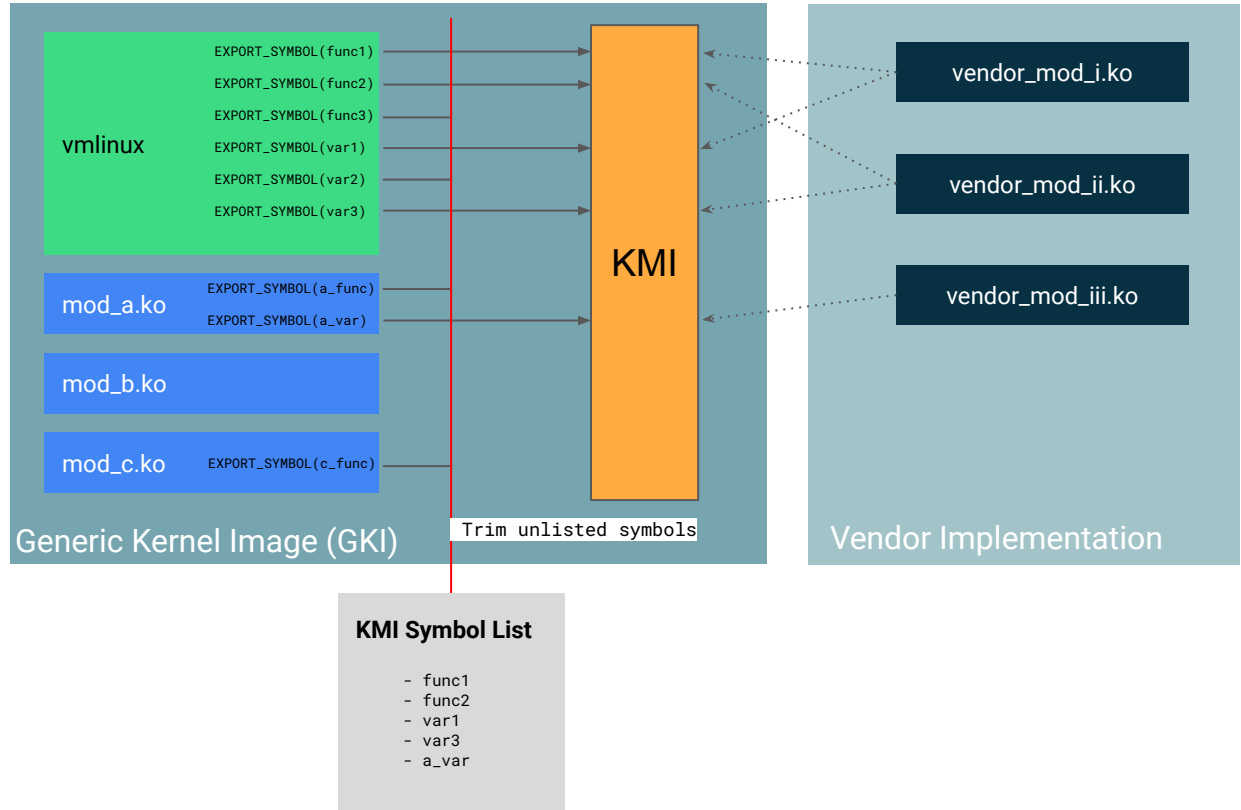
## Scope

- Define what is part of the ABI
- Symbols

- Observable ABI
- Symbol Lists
- Symbol Namespaces

# Defining the Kernel Module Interface (KMI)

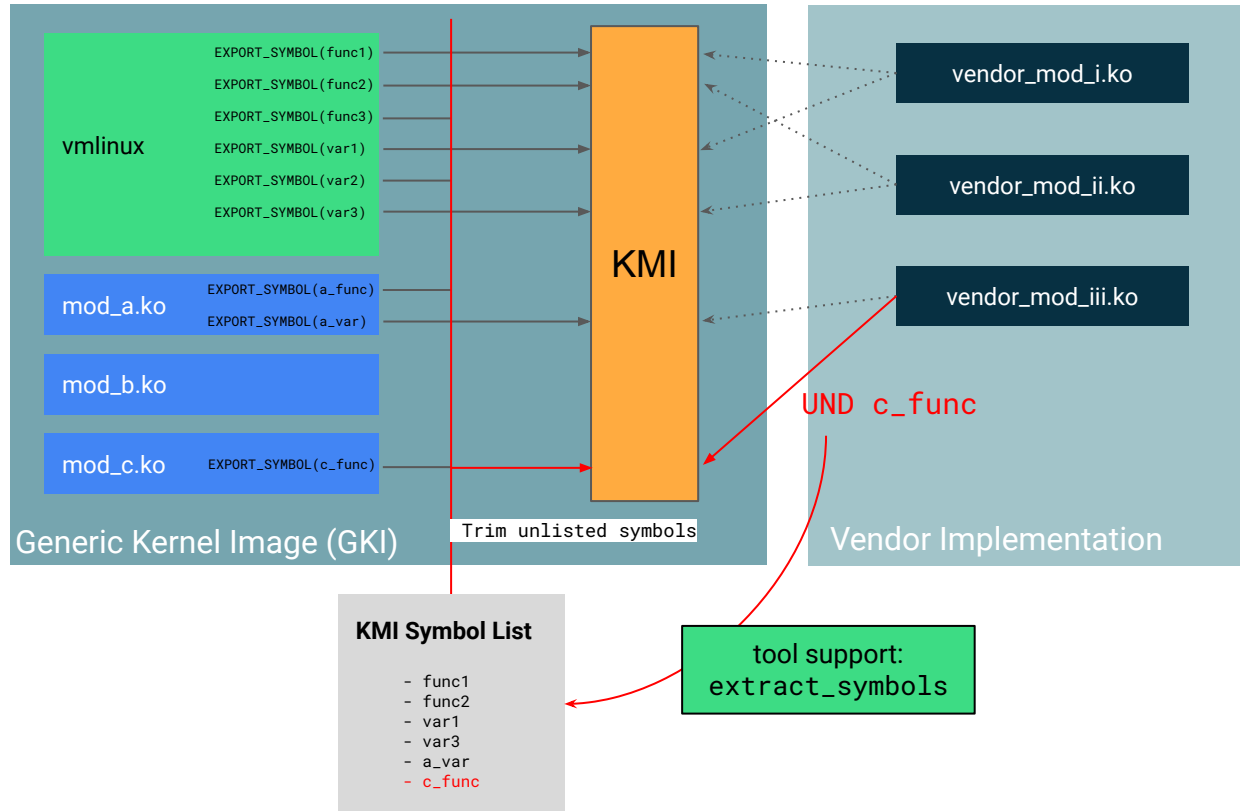
- Symbols used by Vendor modules need to be
  - EXPORTed
  - Listed in a symbol list
- The GKI binaries export only listed symbols. (trimmed)
- KMI symbols kept ABI stable
- Additions to the KMI possible even after the release.



# Defining the Kernel Module Interface (KMI)

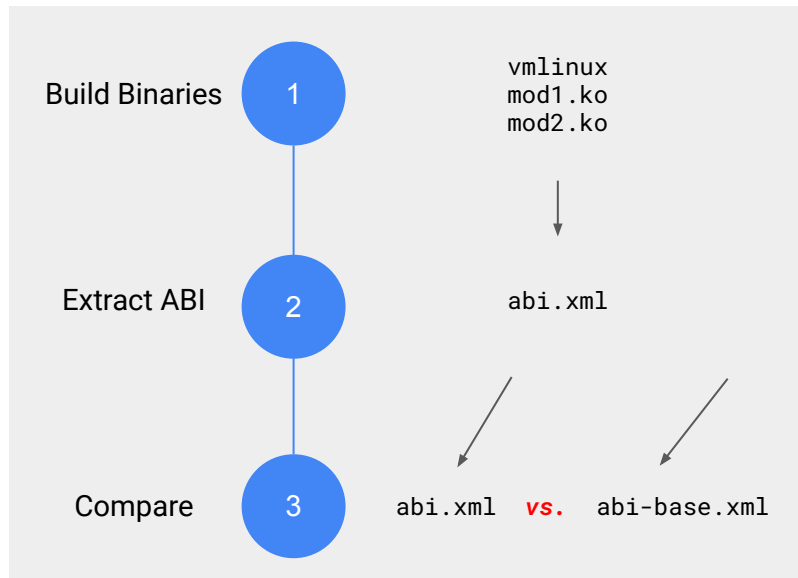
## Adding Symbols to the KMI

1. Source code modification in vendor\_mod requires new symbol. (build failure)
2. Vendor submit symbol list updates to AOSP
3. Subsequent updates of GKI
  - o export `c_func` for modules
  - o keep `c_func` ABI stable



# Libabigail

"Application Binary Interface Generic Analysis and Instrumentation Library"  
<https://sourceware.org/libabigail/>



## What's new?

- Support for
  - Clang-built 64bit ARM Kernels
  - Linux 4.19+
  - Modversions (CRC)
  - LTO / CFI
  - Symbol Namespaces
  - Multiple Symbol Lists
- Bugfixes
  - Type equality
  - Textual reporting
  - ...
- Maintainability fixes
  - towards ABI change ↔ XML change

# Tracking KMI breakages

File	Comments	Size	Delta
Commit message			
drivers/iommu/io-pgtable.c		<div style="width: 100%; height: 10px; background-color: green;"></div>	+33 -0
drivers/iommu/io-pgtable-arm.c		<div style="width: 100%; height: 10px; background-color: red;"></div>	+20 -17
include/linux/io-pgtable.h		<div style="width: 100%; height: 10px; background-color: green;"></div>	+46 -0 Reviewed
			+99 -17

Presubmit passed.

Failing: 1

Lint KernelABI - ABI is broken for 'kernel\_aarch64' on 'aosp\_kernel-common-android11-5.4!': rc=4, please visit go/kernel-abi-monitoring

Successful/Info: 23

```
diff --git a/include/linux/io-pgtable.h b/include/linux/io-pgtable.h
index ec7a134..cd6b768 100644
--- a/include/linux/io-pgtable.h
+++ b/include/linux/io-pgtable.h
@@ -95,6 +110,7 @@
     unsigned int          oas;
     bool                  coherent_walk;
     const struct iommu_flush_ops *tlb;
+    const struct iommu_pgtable_ops *iommu_pgtable_ops;
     struct device          *iommu_dev;

/* Low-level data specific to the table format */
```

KernelABI - ABI is broken for 'kernel\_aarch64' on 'aosp\_kernel-common-android11-5.4!': rc=4, please visit go/kernel-abi-monitoring

1 function with some sub-type change:

[C] 'function io\_pgtable\_ops\* alloc\_io\_pgtable\_ops(io\_pgtable\_fmt, io\_pgtable\_cfg\*, void\*)' at io-pgtable.c:29:1 has some sub-type changes:

- CRC value (modversions) changed from 0xe49d2ea to 0x153c3f3b

'struct io\_pgtable\_cfg at io-pgtable.h:64:1' changed:

- type size changed from 704 to 768 (in bits)
- 1 data member insertion:
  - 'const iommu\_pgtable\_ops\* io\_pgtable\_cfg::iommu\_pgtable\_ops', at offset 320 (in bits) at io-pgtable.h:113:1

there are data member changes:

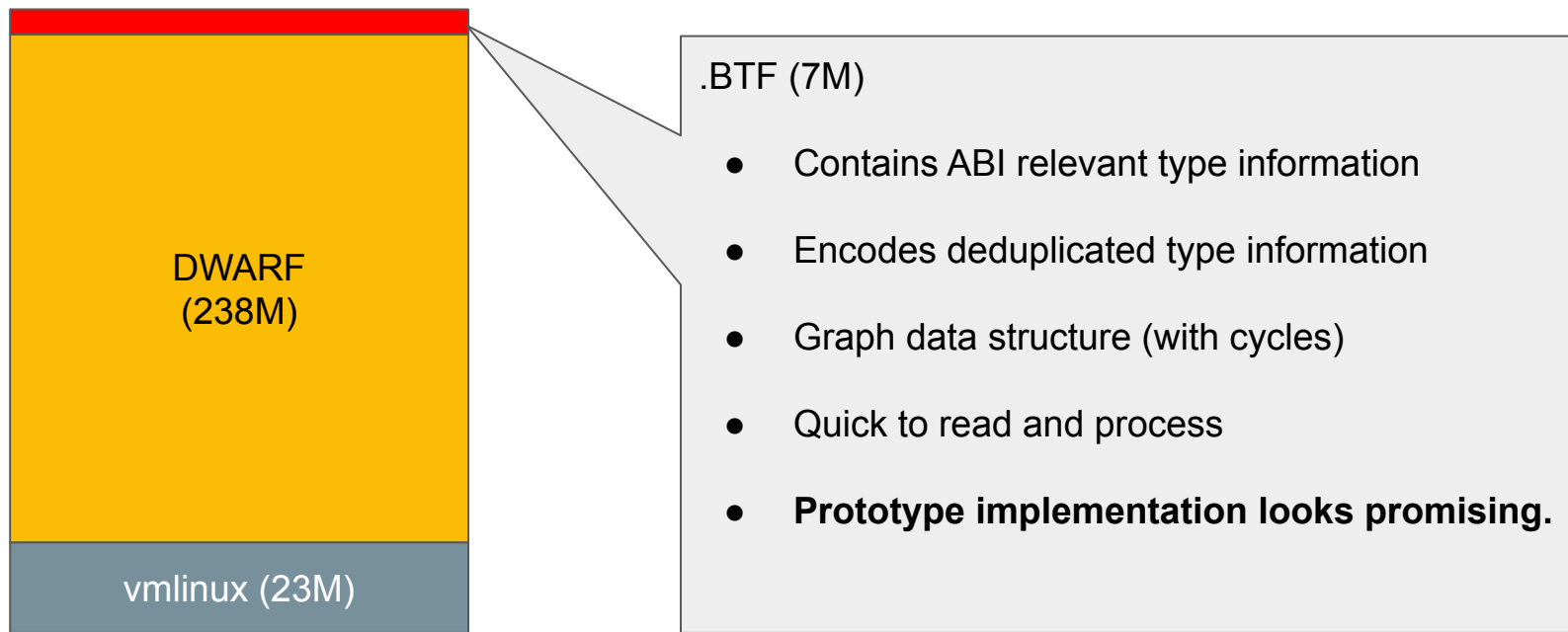
- 'device\* io\_pgtable\_cfg::iommu\_dev' offset changed from 320 to 384 (in bits) (by +64 bits)
- anonymous data member 'union {u64 tthr[2]; u64 tcr; u64 mair[2];} arm\_lpae\_s1\_cfg; struct {u64 vttbr; u64 vtcrr;} arm\_lpae\_s2\_cfg; struct {u32 ttbr[2]; u32 tcr; u32 nmrr; u32 prrr;} arm\_v7s\_cfg; struct {u64 transtab; u64 memattr;} arm\_mali\_lpae\_cfg;' offset changed from 384 to 448 (in bits) (by +64 bits)
- one impacted interface

## Example:

- [v5 of the change](#) affected the KMI
- [A change](#) was added to the series to update the KMI definition (branch was still open for incompatible changes)

# Bonus: Using BTF Type Information

CONFIG\_DEBUG\_INFO\_BTF=y





# Question?

Matthias Männich <[maennich@android.com](mailto:maennich@android.com)>