Practical use of Treble on DevBoards

Vishal Bhoj <vishal.bhoj@linaro.org>
Project Treble Goal

- Reduce Fragmentation
- Faster Updates
Treble Implementation

- Vendor Partition
- Kernel Changes
- HIDL/HAL
- Vndk/Linker-namespace
- SELinux
Partitioning (jstultz)
Vendor / Framework Separation (jstultz)
Hardware Interface Definition Language (HIDL)

- Specify the interface between a HAL and its users
- Intended to be used for inter-process communication
- Modes
  - Passthrough Mode
    - Generated passsthrough Header file
    - Header defines functions to be `dlopen`ed
    - Runs in the same process
  - Binderized Mode
    - `a.b.c.d@M.N::IFoo-impl`. Contains the implementation of the HAL
    - `a.b.c.d@M.N::IFoo-service`. Opens the passthrough HAL and registers itself as a binderized service.
HAL

- **Binderized HALs**
  - android.hardware.biometrics.fingerprint@2.1
  - android.hardware.configstore@1.0
  - android.hardware.dumpstate@1.0
  - android.hardware.graphics.alloca...3
  - android.hardware.radio@1.0
  - android.hardware.usb@1.0
  - android.hardware.wifi@1.0
  - android.hardware.wifi.supplier@1.0

- **Passthrough HALs**
  - android.hardware.graphics.mapper@1.0
  - android.hardware.renderscript@1.0

- **SP-HALs (Same Process HAL)**
  - openGL
  - Vulkan
  - android.hidl.memory@1.0
  - android.hardware.graphics.mapper@1.0
  - android.hardware.renderscript@1.0
Vendor Native Development Kit (VNDK)

- Set of libraries exclusively for vendors to implement their HALs
- Ships in `system.img` and is dynamically linked to vendor code at runtime
- Build Time Restrictions and Runtime Restriction through linker-namespace
- FW libraries have been labeled to restrict the access by vendor components
Linker-namespace

- **Issues**
  - SP-HAL shared libraries and their dependencies, including VNDK-SP libraries, are loaded into framework processes. There should be some mechanisms to prevent symbol conflicts.
  - `dlopen()` and `android_dlopen_ext()` may introduce some run-time dependencies that are not visible at build-time and can be difficult to detect using static analysis.
- [https://android.googlesource.com/platform/system/core/+/master/rootdir/etc/ld.config.txt](https://android.googlesource.com/platform/system/core/+/master/rootdir/etc/ld.config.txt)
SELinux with Treble

- Split Sepolicy
  - plat_*
  - nonplat_*
- Plays important role in restricting system/vendor processes accessing files on other partition.
- Sepolicy rules wrapped under “full_treble_only” section in domain.te
Vendor Interface Object (VINTF)

- The **device manifest** describes the static component of what the device can provide to the framework.
- The **framework compatibility matrix** describes what the Android framework expects from a given device. The matrix is a static entity whose composition is determined manually during development of the next release of the Android framework.
- The **framework manifest** describes high-level services the framework can provide to the device.
- The **device compatibility matrix** describes the services the vendor image requires of the framework. Its composition is determined manually during the development of the device.

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE MANIFEST</td>
<td>FRAMEWORK COMPATIBILITY MATRIX</td>
</tr>
<tr>
<td>HAL information</td>
<td>HALs section</td>
</tr>
<tr>
<td>Other sections</td>
<td>Other sections</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE COMPATIBILITY MATRIX</td>
<td>FRAMEWORK MANIFEST</td>
</tr>
<tr>
<td>HALs section</td>
<td>HAL information</td>
</tr>
<tr>
<td>Other sections</td>
<td>Other sections</td>
</tr>
</tbody>
</table>

**KEY**

- Provided → Required
- Retrieved by VINTF Object
Kernel

- Enable Modules
- Mounting partitions during early init (GPT mandatory)
Treblizing HiKey /HiKey960

● Add a Vendor Partition
● Move vendor Hals and components into vendor partition
● Fix device manifest to be compliant with Treble
● SELinux changes for Treble compliance
  ○ Start with selinux permissive mode
  ○ Build working with Treble configuration
  ○ Generate sepolicies for the denials in permissive mode + Treble
  ○ Enable enforcing mode and selectively add the needed sepolicies for Android with treble.
Treblizing DragonBoard

- Work driven by Sumit Semwal
  - Issue: Blocked with using Mesa3d in Treble environment
  - Runtime dependency on libexpat (can’t be loaded by sphal since it is a vndk component)
  - WIP: working with upstream to resolving libexpat dependency.
Resources

https://source.android.com/devices/architecture/

Credits

Portions of this slide deck are modifications based on work created and shared by the Android Open Source Project and used according to terms described in the Creative Commons 3.0 Attribution License.
Thank You!