Security and Boot Architecture

- PI/MM on ARM discussions tomorrow (Tues)
  - UEFI members only
- Brief Trusted Firmware update
  - Where is the upstream for 96Boards TF platform code?
  - Potential requirements
- GICv3 impact on secure world architecture
- Improving AArch32 secure world support
  - More library support for Secure OS integration (PSCI + IP drivers)
- Common support for boot path verification
- Secure firmware interfaces
  - Standard secure world -> normal world cold boot interface
  - Or, more standard SMCs
  - For example, to pass Secure DRAM region info
Security and Boot Architecture (2)

• Segment specific use-cases
  – Trusted OS / Secure-EL1 payload on Enterprise systems?
  – Boot architecture on Cortex-A class IoT systems

• Missing secure services/drivers/features
  – Especially for OPTEE

• Security hardening
  – Threat models, code audits, Pen testing, etc...

• Non-functional requirements
  – Performance, RAM budget on IoT or many core systems
  – Trace format for use-cases touching multiple components

• Anything else?
ARM Trusted Firmware Update

Dan Handley
Linaro Connect San-Francisco 2015
ARM Trusted Firmware for 64-bit ARMv8-A

- Reference boot flows
  - For 64-bit ARMv8-A systems
- Open Source at GitHub
  - BSD License
  - Contributors welcome
- BL31 runtime is compatible with other boot firmware
- Trusted OS is optional
- Applicable to all segments

https://github.com/ARM-software/arm-trusted-firmware
Feature evolution

- **PSCI v1.0**
  - Platform porting interface overhaul for flexible topology and enhanced CPU_SUSPEND support
  - Now upstream including compatibility support for existing platform ports

- **Trusted Board Boot**
  - Futureproof interface supporting alternative Crypto Libs, Certificate structures and Chains of Trust
  - Mandatory features nearly complete: Firmware Update (Recovery Mode) coming soon

- **System IP**
  - CCN-xxx driver complete (pull request pending)
  - Full GICv3 support coming soon (see later)

- **Firmware interoperability (entrypoint rework, programmable reset address)**

- **Platform ports**
  - NVidia has upstreamed ports for Tegra T210 and T132
  - Mediatek has upstreamed a port for MT8173
GIC versions

GICv2

- Features
  - Up to 8 cores
  - Up to 1020 interrupt IDs
  - Up to 8 bits of priority
  - Software Generated Interrupts
  - TrustZone support
  - Virtualization support

- Implemented by:
  - CoreLink™ GIC-400

GICv3

- Adds:
  - Support for many more than 8 cores
  - Message Based Interrupts
  - Enhanced security model
  - System register interface
  - Vastly expanded interrupt ID space
  - Optional support for legacy GICv2 compatible operation

- Implemented by:
  - CoreLink™ GIC-500
## GICv3 Security Groups

<table>
<thead>
<tr>
<th>Group 0</th>
<th>Secure Group 1</th>
<th>Non-Secure Group 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always secure</td>
<td>FIQ if in Non-Secure state</td>
<td>FIQ if in Secure state</td>
</tr>
<tr>
<td>Always FIQ</td>
<td>IRQ if in Secure state</td>
<td>IRQ if in Non-Secure state</td>
</tr>
<tr>
<td>Typically used by EL3 firmware</td>
<td>Typically used by Trusted OS</td>
<td>Typically used by Rich OS or Hypervisor</td>
</tr>
</tbody>
</table>
GIC Interrupt Groups, Lines and Usage models

- “Canonical” model (trap other world interrupt to EL3) is rare in practice
  - Most Trusted OS always trap Group0 (S) interrupts to S-EL1
  - Some (for example OPTEE) also trap Group1 (NS) interrupts to S-EL1
    - For example, save task state, before forwarding to normal world via SMC
  - Other Trusted OS do not enable Group1 interrupts at S-EL1 (symmetric model)
  - TSPD supports both models

- GICv3 S-Group1 interrupts will be useful to enable dedicated EL3 interrupts
  - Avoids having to shoe-horn use-cases into GICv2 systems
- But expect S-EL1 initial handling of Group0/NS-Group1 will continue with GICv3
  - Substantial design/implementation churn in Trusted OS required to switch to trap-to-EL3 model
GICv3 Software Migration Strategy
Hardware and Software System compatibility

<table>
<thead>
<tr>
<th>Software Architectures</th>
<th>GICv2 (e.g. GIC-400)</th>
<th>GICv3+v2 (e.g. GIC-500)</th>
<th>GICv3 (no legacy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric GICv2</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>all ARE=0, SRE=0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric GICv3 + GICv2</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>ARE_NS=1, ARE_S=0, all SRE=1 except SRE_EL1(S)=0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric GICv3</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>all ARE=1, SRE=1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## GICv3 Software Migration Strategy

**Current support in ARM Trusted Firmware**

### Current GIC driver

<table>
<thead>
<tr>
<th>Software Architectures</th>
<th>GICv2 (e.g. GIC-400)</th>
<th>GICv3+v2 (e.g. GIC-500)</th>
<th>GICv3 (no legacy)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symmetric GICv2</strong></td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>all ARE=0, SRE=0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Asymmetric GICv3 + GICv2</strong></td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>ARE_NS=1, ARE_S=0, all SRE=1 except SRE_EL1(S)=0</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Symmetric GICv3</strong></td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>all ARE=1, SRE=1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Hardware Systems

- Symmetric GICv2: all ARE=0, SRE=0
- Asymmetric GICv3 + GICv2: ARE_NS=1, ARE_S=0, all SRE=1 except SRE_EL1(S)=0
- Symmetric GICv3: all ARE=1, SRE=1

Not supported: ✓

<table>
<thead>
<tr>
<th>Hardware Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>GICv2 (e.g. GIC-400)</td>
</tr>
<tr>
<td>✓</td>
</tr>
<tr>
<td>✗</td>
</tr>
<tr>
<td>✗</td>
</tr>
</tbody>
</table>
## GICv3 Software Migration Strategy

### Proposed GIC driver support

<table>
<thead>
<tr>
<th>Software Architectures</th>
<th>GICv2 (e.g. GIC-400)</th>
<th>GICv3+v2 (e.g. GIC-500)</th>
<th>GICv3 (no legacy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric GICv2</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>all ARE=0, SRE=0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric GICv3 + GICv2</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ARE_NS=1, ARE_S=0,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>all SRE=1 except SRE_EL1(S)=0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric GICv3</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>all ARE=1, SRE=1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Hardware Systems**

- **New GICv2 driver**
- **New GICv3 driver**
- **Deprecate**