Setting the Scene

- Trustedfirmware.org
- Who All Are Here?
- What Do We Want to Achieve?, What Next?
- TF-M Today, What’s Coming?
Trustedfirmware.org
Trusted Firmware History

- Oct 2013: Arm Trusted Firmware
- Mar 2018: Trusted Firmware-M
- Oct 2018: Trusted Firmware-A
- Today: TrustedFirmware.org
Trustedfirmware.org

- NOT Linaro OR Arm’s Project, HOSTED BY Linaro
Current members

- ARM
- Google
- Data I/O
- Cypress
- TrustedFirmware.org
- Linaro
- Texas Instruments
Build Security Collaboratively

- Security by Scale
- Shared Ownership
- Complexity solved once for all
- Faster TTM & Reduced Cost
- Less Individual Maintenance & Minimised TCO

TrustedFirmware.org
How to Get Involved

● Contribute to the open source codebase!

● Join the project mailing lists!

● ...and last but not the least: become a project member! (enquiries@trustedfirmware.org)
  ○ Own the strategic and technical direction of the project
  ○ Have your board supported and maintained by the open CI
  ○ Become a Trusted Firmware ambassador!
Who All Are Here?
What Do We Want to Achieve?, What Next?
Build TF-M Community...

- **Inception**
  - Invite members to join
  - Create Discussions
  - Relationship building
  - Transparency & Openness

- **Established**
  - Content
  - Hackathons
  - Conferences
  - Meetups

- **Maturity**
  - Growing Influence
  - Community Ownership
  - Streamlining

- **Mitosis**
  - Focussed Subgroups
Workshop & Beyond...

● Each Slot is NOT a ‘death by power point’ by presenters

● 2-3 slides to kick off each topic, followed by Open Discussion

● Active participation by attendees

● Not an opportunity to ask Arm to do more ☺, but to solve problems jointly

● Starting point for more involved mailing list discussions on design/implementation

● Opportunity for
  ○ Follow up on important topics in a bi-weekly TF-M Technical Forum
  ○ Making this workshop an annual event
TF-M – Today & Future
Growing up as a Toddler....

With a Lot of Friends and Toys!!!
TF-Mv1.0-RC2: Enabling L1,2 and Functional API Certification

- F.INITIALIZATION
- F.FIRMWARE_UPDATE
- F.ISOLATION
- F.SECURE_STORAGE
- F.SECURE_CRYPTO
- F.SECURE_ATTESTATION
- F.SECURE_AUDIT
- F.SECURE_STATE
- PSA Dev. APIs

Non-Secure

Secure/TF-M

RTOS

PSA Dev APIs

PSA Test Suite*

TF-M Core (IPC, SPM, Interrupt Handling)

Secure Boot

TBSA-M HAL

HAL

TBSA-M Hardware

PSA Storage API

PSA Crypto APIs

mbed Crypto (IPC/Lib)

PSA Attestation APIs

Audit APIs

Audit (Lib)
Enablement in RTOSes

- mbedOS 5.12 (March’19) onwards integrated TF-M
  - PSA Level1 and Functional API certified
  - Several PSA Level1 certified platforms supported

- Zephyr PR integrating TF-M
  - For MuscaA, B1e and AN521 on MPS2
  - PSA L1 certified

- Integration of FreeRTOS 10.2.1 and TF-M under evaluation by FreeRTOS team
  - Investigating how best TF-M can integrate with Amazon: FreeRTOS

- Collaboration kicked off with RT-Thread on integration
TF-M – Current Roadmap

**Today**
- Library, IPC Mode, L1,L2 Isolation, PSA APIs, mbedcrypto

**H2 2019**
- Enabling L2 Certification, Dual v7-M, PSA 1.0.0, Crypto HW, Zephyr/TFM

**H1 2020**
- TF-M Profiles, Level3 Isolation
- Crypto HW, TF-M Profiles, Level3 Isolation, FreeRTOS/TFM

**H2 2020+**
- More Secure Services
- Provisioning, Secure Debug, Scheduler, Platform Services, PSA API 1.1
Workshop & Beyond…

- Each Slot is NOT a ‘death by power point’ by presenters
- 2-3 slides to kick off each topic, followed by Open Discussion
- Active participation by attendees
- Not an opportunity to ask Arm to do more 😊, but to solve problems jointly
- Starting point for more involved mailing list discussions on design/implementation
- Opportunity for
  - Follow up on important topics in a bi-weekly TF-M Technical Forum
  - Making this workshop an annual event
Thank You!

arm
TF-M, PSA, CMSIS, mbed

CYPRESS
EMBEDDED IN TOMORROW™

Linaro

NXP

RENESAS

TrustedFirmware.org

Texas Instruments

life.augmented
My Company is a trustedfirmware.org member - A Testimony

- Eric Finco, Technical Director & Fellow, STMicroelectronics & trustedfirmware.org Board member
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Host(s)/Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 31st (Thursday)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.30-9.00am</td>
<td>Registration &amp; Welcome Drinks</td>
<td>Host(s)/Presenter(s)</td>
</tr>
<tr>
<td>9.00-9.25am</td>
<td>Setting the Scene</td>
<td>Shebu V. Kuriakose</td>
</tr>
<tr>
<td>9.25-9.45am</td>
<td>Keynote - Collaborating in trustedfirmware.org</td>
<td>Eric Finco</td>
</tr>
<tr>
<td>9.45-10.30am</td>
<td>Scheduler Design Ideas</td>
<td>Ken Liu/Mate Toth-Pal/Summer Qin</td>
</tr>
<tr>
<td>10.30-11am</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>11.00-12.30pm</td>
<td>Interrupt Handling, What Else in TF-M Core</td>
<td>Ken Liu/Mate Toth-Pal/Summer Qin</td>
</tr>
<tr>
<td>12.30-1.30pm</td>
<td>Lunch</td>
<td>Host(s)/Presenter(s)</td>
</tr>
<tr>
<td>1.30-2.15pm</td>
<td>Secure Storage Service</td>
<td>Jamie Fox/Antonio De Angelis</td>
</tr>
<tr>
<td>2.15-3.00pm</td>
<td>mbedcrypto</td>
<td>Jaeden Amero/Janos Follath</td>
</tr>
<tr>
<td>3.00-3.45pm</td>
<td>Crypto Hardware Integration</td>
<td>Jamie Fox/Tamas Ban</td>
</tr>
<tr>
<td>3.45-4.05pm</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>4.05-4.50pm</td>
<td>mcuboot &amp; Attestation Service</td>
<td>Tamas Ban</td>
</tr>
<tr>
<td>4.50-5.30pm</td>
<td>Dual CPU Design</td>
<td>David Hu</td>
</tr>
<tr>
<td>Nov 1st (Friday)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.30-9.00am</td>
<td>Welcome Drinks</td>
<td>Host(s)/Presenter(s)</td>
</tr>
<tr>
<td>9.00-9.45am</td>
<td>Build System</td>
<td>David Wang</td>
</tr>
<tr>
<td>9.45-10.30am</td>
<td>Tooling Support</td>
<td>Abhishek Pandit/Shebu V. Kuriakose</td>
</tr>
<tr>
<td>10.30-11am</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>11.00-11.45am</td>
<td>RTOS Enablement</td>
<td>David Wang</td>
</tr>
<tr>
<td>11.45-12.30pm</td>
<td>Open CI</td>
<td>Minos Galanakis</td>
</tr>
<tr>
<td>12.30-1.30pm</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>1.30-2.15pm</td>
<td>TF-M Profile Proposal</td>
<td>Shebu V. Kuriakose/Antonio De Angelis</td>
</tr>
<tr>
<td>2.15-3.00pm</td>
<td>HAL - Change Proposal</td>
<td>Antonio De Angelis</td>
</tr>
<tr>
<td>3.00-3.30pm</td>
<td>Break</td>
<td>Shebu V. Kuriakose</td>
</tr>
<tr>
<td>3.30pm-4pm</td>
<td>Wrap Up</td>
<td></td>
</tr>
</tbody>
</table>