TrustedFirmware.org

Project Update

Matteo Carlini & Shebu V. Kuriakose
Trusted Firmware: Build Security Collaboratively

Open Governance Community Project

Reference open source implementation of Secure world software for Arm processors across all market segments

Membership open to all

Board

Technical Steering Committee
A year in the news!

Trusted Firmware-A & TF-A-Tests v2.3 released
Trusted Firmware-M v1.1 and Ecosystem Enablement

Linaro donates OP-TEE in Firmware Project

Hafnium, MbedTLS, PSA Crypt Project
Trusted Firmware Project

Trusted Firmware today announced that Hafnium, MbedTLS, and PSA Crypto Project transitioned into its project scope. This move is towards collaborative development of secure software for the Arm ecosystem, enabling open governance project with architected solutions which can then be easily ported to many other trusted software implementations.

Renesas Electronics and NXP Semiconductors N.V. join the Trusted Firmware Project

Cambridge – WEBWIRE – Wednesday, March 25, 2020

Trusted Firmware, the open governance community project hosted by Linaro Community Projects Division, today announced that Renesas Electronics Corporation and NXP® Semiconductors N.V. have joined the Trusted Firmware Project. Members to date include Arm, Cypress, Data IO, Futurewei, Google, Linaro, ST Microelectronics and Texas Instruments.

“The forecasted one trillion embedded devices connecting to the cloud, Renesas wants to ensure its 32-bit microcontroller solutions are as secure as possible”, said Daryl Khoo, Vice President of Marketing, IoT Platform Business Division at Renesas. “Joining the Trusted Firmware Project is the logical next step in securing our RA MCU Family featuring Arm® Cortex®-M processors.”

Security for Arm Cortex-M devices with FreeRTOS

by Shebu Varghese Kuriakose on 17 Jul 2020

Deliver Your News to the World
Trusted Firmware Security Center

New centralized Security incident process

https://developer.trustedfirmware.org/w/collaboration/security_center/

● Have you found a security vulnerability in Trusted Firmware?
  → Report it here: security@lists.trustedfirmware.org

● Coordinated disclosure with Trusted Stakeholders and ESS
  ○ https://developer.trustedfirmware.org/w/collaboration/security_center/trusted_stakeholder_registration/

● Per-project security email aliases
  ○ https://developer.trustedfirmware.org/w/collaboration/security_center/mailing_aliases/
New Maintenance Process & New Maintainers!

https://developer.trustedfirmware.org/w/collaboration/project-maintenance-process/

- Explicit and well documented code review process
- Roles definition (Contributors, Code owners, Maintainers) & expectations
- Patch lifecycle & contribution guidelines
- Platform support lifecycle (fully supported, limited support, deprecated)

- Added new core maintainers to TF-A and Hafnium
- Half of them from the developer community & partners!

2020 TF-A & Hafnium newly appointed maintainers distribution

50% Arm
50% Partners
Trusted Firmware Community Manager

- Help build a collaborative Trusted Firmware community
- Understand and Resolve Barriers to Collaborate
- Organize Community Initiatives – Tech Forums, Open CI
- Promote Trusted Firmware, Support Members
- Welcome Don Harbin to the Trusted Firmware Family!
Open Continuous Integration (ci.trustedfirmware.org)
<table>
<thead>
<tr>
<th>Name</th>
<th>Last Success</th>
<th>Last Failure</th>
<th>Last Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1 Dockerfile build/publish deployment</td>
<td>4 days 23 hr - #556</td>
<td>1 mo 5 days - #650</td>
<td>10 min</td>
</tr>
<tr>
<td>C1 jobconfigs sanity check</td>
<td>3 days 18 hr - #222-23a0e091a</td>
<td>10 days - #211-f0b0b02</td>
<td>6.2 sec</td>
</tr>
<tr>
<td>C1 VAP config builder</td>
<td>18 days - #f13-9db07b75</td>
<td>28 days - #f3-e033109</td>
<td>2.3 sec</td>
</tr>
<tr>
<td>C1 VAP config builder sanity check</td>
<td>18 days - #f13-9db07b75</td>
<td>27 days - #f3-46c9999</td>
<td>5.2 sec</td>
</tr>
<tr>
<td>Demo hours use fastmovie</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Hafnium builder</td>
<td>3 days 17 hr - #321-7b0123aa</td>
<td>10 days - #314-801b050w</td>
<td>10 min</td>
</tr>
<tr>
<td>Post build to Lib</td>
<td>11 days - #3744</td>
<td>1 hr 3 min - #3905</td>
<td>2.7 sec</td>
</tr>
<tr>
<td>th-m-build-and-test</td>
<td>1 hr 1 min - #4684</td>
<td>11 days - #483</td>
<td>15 min</td>
</tr>
<tr>
<td>th-m-build-config</td>
<td>1 hr 0 min - #48002</td>
<td>2 hr 26 min - #48030</td>
<td>2 min 11 sec</td>
</tr>
<tr>
<td>th-m-build-doc</td>
<td>1 hr 0 min - #502</td>
<td>2 hr 26 min - #729</td>
<td>1 min 43 sec</td>
</tr>
<tr>
<td>th-m-build-doc-nightly</td>
<td>13 hr - #59</td>
<td>11 days - #320</td>
<td>15 min</td>
</tr>
<tr>
<td>th-m-check patch</td>
<td>1 hr 7 min - #467</td>
<td>6 days 23 hr - #480</td>
<td>5 min 10 sec</td>
</tr>
<tr>
<td>th-m-checkcheck</td>
<td>1 hr 5 min - #4697</td>
<td>N/A</td>
<td>5 min 28 sec</td>
</tr>
<tr>
<td>th-m-infra-health</td>
<td>1 hr 46 min - #143</td>
<td>2 hr 26 min - #3810</td>
<td>48 min</td>
</tr>
<tr>
<td>th-m-log-submit</td>
<td>57 min - #31178</td>
<td>1 hr 27 min - #9126</td>
<td>30 sec</td>
</tr>
<tr>
<td>th-m-magpie</td>
<td>4 hr 43 min - #151</td>
<td>9 days 13 hr - #117</td>
<td>39 min</td>
</tr>
<tr>
<td>th-m-nightly-code-coverage</td>
<td>13 hr - #333</td>
<td>10 days - #85</td>
<td>25 min</td>
</tr>
<tr>
<td>th-m-release</td>
<td>7 hr 17 min - #9</td>
<td>7 days 8 hr - #9</td>
<td>41 min</td>
</tr>
<tr>
<td>th-m-static</td>
<td>1 hr 7 min - #466</td>
<td>11 days - #467</td>
<td>21 min</td>
</tr>
<tr>
<td>th-m-static-shards</td>
<td>N/A</td>
<td>1 hr 7 min - #13</td>
<td>5 min 5 sec</td>
</tr>
<tr>
<td>Tripper for TF-A, script events</td>
<td>11 days - #4649</td>
<td>1 hr 21 min - #5010</td>
<td>2 min 21 sec</td>
</tr>
<tr>
<td>Trusted Firmware A (TF-A) builder</td>
<td>11 days - #4663</td>
<td>1 hr 21 min - #6294</td>
<td>2 min 7 sec</td>
</tr>
</tbody>
</table>

Legend: Atom feed for all, Atom feed for failures, Atom feed for just latest builds
More Capabilities Coming to Open CI

- FVP, QEMU Support, Silicon Platforms
- Dashboards
- Static Analysis
- Staging Instances
- Open CI for Mbed TLS, OP-TEE
- User Guides
TF-M, Mbed TLS Virtual Workshops – Coming Soon!

- Regular Tech Forums happening for TF-M, TF-A, OP-TEE.
- TF-M, Mbed TLS Virtual Workshop with Talks, Design Discussions being planned
- ½ Day Event Open to All
- Look Out for more info. In the TF-M, Mbed TLS Mailing lists
We’ve Got a New Look

TrustedFirmware

OPEN SOURCE SECURE WORLD SOFTWARE

EASY NAVIGATION
STREAMLINED CONTENT
IMPROVED READABILITY
**Trusted Firmware** provides a reference implementation of secure world software for Armv8-A and Armv8-M. It provides SoC developers and OEMs with a reference trusted code base complying with the relevant Arm specifications.

The code on this website is the preferred implementation of Arm specifications, allowing quick and easy porting to modern chips and platforms. This forms the foundations of a Trusted Execution Environment (TEE) on application processors, or the Secure Processing Environment (SPE) of microcontrollers.

---

**Available Trusted Firmware Projects**

- Hafnium
- Mbed TLS
- OP-TEE
- TF-A
- TF-M

---

**Our Members**
The Trusted Firmware-A project provides a reference implementation of secure world software for Armv7-A and Armv8-A class processors.

Contribution guidelines can be found in the documentation.

Please subscribe to the project email list to participate in development discussions.

A bi-weekly Technical Forum call is held to discuss technical subjects.
LVC20 Trusted Firmware Talks

- **Tuesday September 22\(^{nd}\)**
  - PSA Secure Partitions in OP-TEE

- **Wednesday September 23\(^{rd}\) (11.45am – 12.10pm UTC)**
  - Scalable Security Using Trusted Firmware-M Profiles

- **Thursday September 24\(^{th}\) (3.45-4.10pm UTC)**
  - Enable UEFI Secure Boot using OP-TEE as Secure Partition

- **Thursday September 24\(^{th}\) (4.15-4.40pm UTC)**
  - Secure Partition Manager (SEL2 firmware) for Arm A-class devices
Visit Our New Home – Trustedfirmware.org

Subscribe to the Mailing Lists
Attend Regular Tech Forums and Upcoming Workshops
Thank you

Accelerating deployment in the Arm Ecosystem

enquiries@trustedfirmware.org