TrustedFirmware.org

Project Update

Matteo Carlini & Shebu V. Kuriakose

Linaro Connect VIRTUAL 2020

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

Increasing Collaboration, Accelerating Technology

arm

FUTUREWEI Technologies

NXP

Google

CYPRESS EMBEDDED IN TOMORROW™

Linaro

Data I/O

ST life.augmented

RENESAS

TEXAS INSTRUMENTS

Linaro Connect VIRTUAL 2020

A year in the news!

Trusted Firmware-A & TF-A-Tests v2.3 released

Trusted Firmware-M v1.1 and Ecosystem Enablement

WebWire®
News and Press Release Distribution, Since 1995

Deliver Your News to the World

Home | News | How We Work | Compare Services | FAQ

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

LinkedIn | Twitter | Facebook | Reddit | Pinterest

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.

"With a 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."

> "The Trusted Firmware Project was founded for the Arm ecosystem to collaborate on building secure software and solving the complexity of security at scale. New platinum members, Renesas and NXP, bring extensive and valuable experience to the project.

WebWire®
News and Press Release Distribution, Since 1995

Deliver Your News

Home | News | How We Work | Compare Services

Hafnium, MbedTLS, PSA Cry Trusted Firmware Project

Trusted Firmware today announced that Hafnium, M Crypto Project transitioned into its project scope. Thi towards collaborative development of secure softwa Trusted Firmware, the open governance community project hosted by Linaro Community Projects Division, to date include Arm, Cypress, Data IO, Futurewei, Google, Linaro, NXP® Semiconductors N.V., Renesas Electronics Corporation, ST Microelectronics and Texas Instruments.

WebWire®
News and Press Release Distribution, Since 1995

Deliver Your N

Home | News | How We Work | Compare Services

Linaro donates OP-TEE in Firmware Project

LinkedIn | Twitter | Facebook | Reddit | Pinterest

San Diego – WEBWIRE – Monday, September 23, 2019

Linaro Ltd, the open source collaborative engineering organization developing software for the Arm ® ecosystem, today announced that OP-TEE (Open Portable TEE, an open source Arm TrustZone® solution) is moving to become part of the Trusted Firmware open project managed by Linaro.

OP-TEE is a Trusted Execution Environment (TEE) designed as a companion to a non-secure Linux kernel running on Arm Cortex®-A cores using the Arm TrustZone technology. OP-TEE implements TEE Internal Core API v1.1.x which is the API exposed to Trusted Applications and the TEE Client API v1.0, which is the API describing how to communicate with a TEE. Those APIs are defined in the GlobalPlatform API specifications. OP-TEE is designed primarily to rely on the Arm TrustZone technology as the underlying hardware isolation

governance project, with architected solutions which can then be easily ported to many other trusted software implementations.

Security for Arm Cortex-M devices with FreeRTOS

by Shebu Varghese Kuriakose on 17 Jul 2020

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/

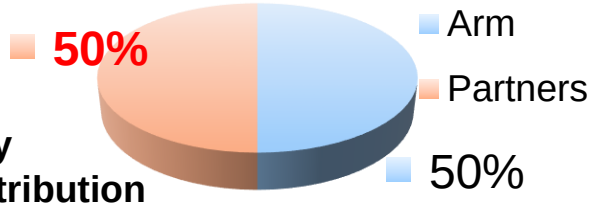
- Per-project security email aliases
  - https://developer.trustedfirmware.org/w/collaboration/security_center/mailing_aliases/

New Maintenance Process & New Maintainers!

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

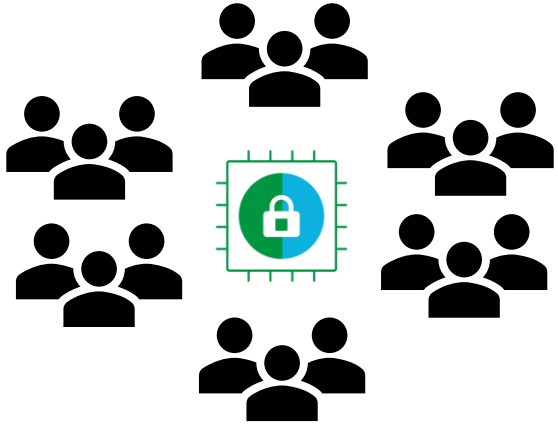
- Explicit and well documented code review process
- Roles definition (Contributors, Code owners, Maintainers) & expectations
- Patch lifecycle & contribution guidelines
- Platform support lifecycle (fully supported, limited support, deprecated)

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



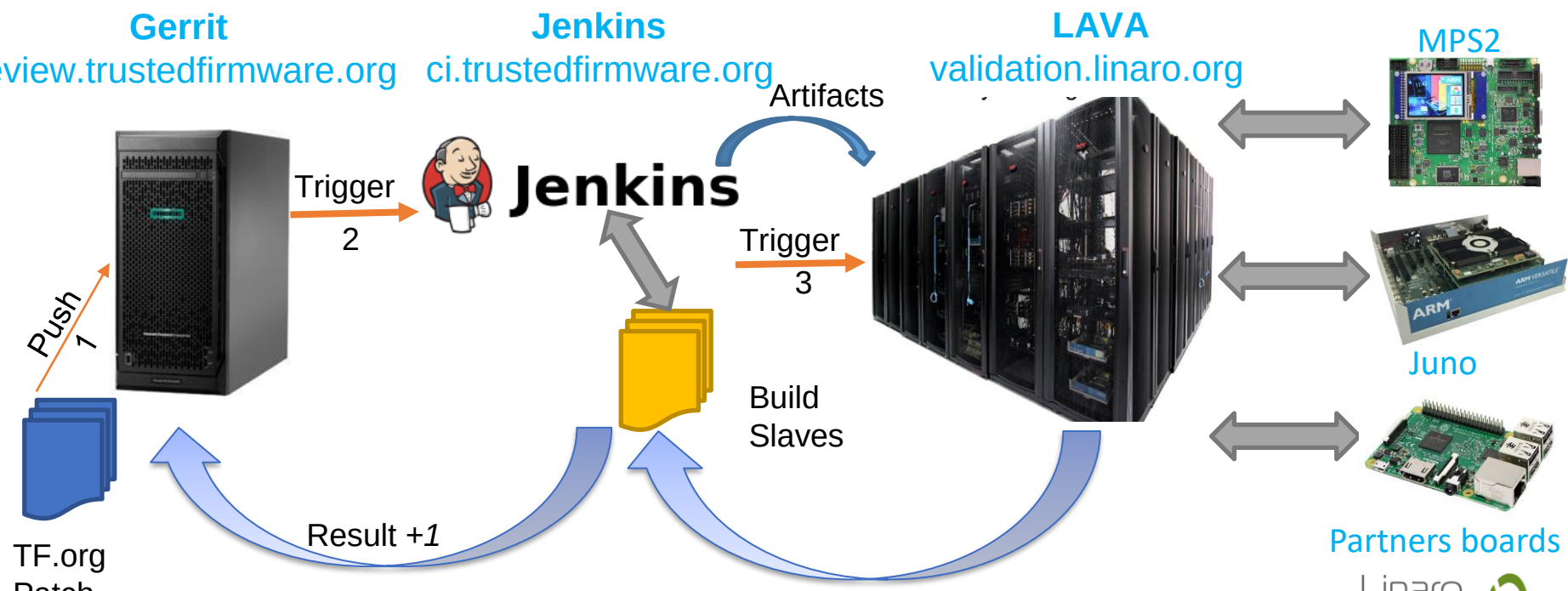
2020 TF-A & Hafnium newly appointed maintainers distribution

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)



Dashboard [Jenkins]

ci.trustedfirmware.org

Jenkins

search

log in

Jenkins

- People
- Build History
- Project Relationship
- Check File Fingerprint
- Open Blue Ocean

Build Queue

No builds in the queue.

Build Executor Status

1 Idle
2 Idle

All | All | TF-A | TF-M

S	W	Name ↓	Last Success	Last Failure	Last Duration
		CI Dockerfiles build/publish deployment	4 days 22 hr - #66	1 mo 5 days - #60	10 min
		CI job configs sanity check	3 days 18 hr - #222-83ae081a	10 days - #211-fa3b0b69	6.2 sec
		CI YADP config builder	18 days - #13-da6b7e75	28 days - #3-e0331808	2.3 sec
		CI YADP config builder sanity check	18 days - #15-da6b7e75	27 days - #8-4fcf9969	5.2 sec
		Demo howto use fastmodel	N/A	N/A	N/A
		Hafnium builder	3 days 17 hr - #321-74017ece	10 days - #314-8d3b599e	10 min
		Post build to LAVA	11 days - #3744	1 hr 3 min - #3905	2.7 sec
		tf-m-build-and-test	1 hr 1 min - #494	11 days - #485	15 min
		tf-m-build-config	1 hr 0 min - #40092	2 hr 26 min - #40030	2 min 11 sec
		tf-m-build-docs	1 hr 0 min - #802	2 hr 26 min - #799	1 min 43 sec
		tf-m-build-docs-nightly	13 hr - #39	11 days - #28	1 min 23 sec
		tf-m-checkpatch	1 hr 7 min - #487	6 days 23 hr - #480	5 min 10 sec
		tf-m-cppcheck	1 hr 7 min - #487	N/A	5 min 28 sec
		tf-m-infra-health	1 hr 46 min - #143	2 hr 26 min - #140	48 min
		tf-m-lava-submit	57 min - #33798	1 mo 27 days - #14206	30 sec
		tf-m-nightly	4 hr 43 min - #151	9 days 13 hr - #117	39 min
		tf-m-nightly-code-coverage	13 hr - #55	10 days - #45	25 min
		tf-m-release	7 hr 17 min - #6	7 days 8 hr - #5	41 min
		tf-m-static	1 hr 7 min - #486	11 days - #477	21 min
		tf-m-static-checks	N/A	1 hr 7 min - #15	5 min 9 sec
		Trigger for TF-A gerrit events	11 days - #4849	1 hr 21 min - #5010	2 min 21 sec
		Trusted Firmware A (TF-A) builder	11 days - #4663	1 hr 6 min - #4824	2 min 7 sec

Icon: S M L

Legend | Atom feed for all | Atom feed for failures | Atom feed for just latest builds

Type here to search

ENG 12:08 PM 9/15/2020

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

EASY NAVIGATION

STREAMLINED CONTENT

IMPROVED READABILITY

OPEN SOURCE SECURE WORLD SOFTWARE

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

arm CYPRESS EMBEDDED IN TOMORROW Data I/O FUTUREWEI TECHNOLOGIES Google Linaro

Enhanced User Experience

About News & Blogs Security Contact

Trusted Firmware A (TF-A)

TF-A Testing TF-A

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 to participate in development discussions.

A bi-weekly Technical Forum call is held to discuss technical subjects.

DOCS	Trusted Firmware-A Documentation
REVIEW	Gerrit review
CODE	View source code
SUBSCRIBE	Subscribe to the TF-A mailing list

CONTRIBUTE/SUBMIT CODE

JOIN THE TF-A TECH FORUM

Other Trusted Firmware Projects

Hafnium Mbed TLS OP-TEE TF-M

https://trustedfirmware-a.readthedocs.org/

LVC20 Trusted Firmware Talks

- Tuesday September 22nd
  - PSA Secure Partitions in OP-TEE
- Wednesday September 23rd (11.45am – 12.10pm UTC)
  - Scalable Security Using Trusted Firmware-M Profiles
- Thursday September 24th (3.45-4.10pm UTC)
  - Enable UEFI Secure Boot using OP-TEE as Secure Partition
- Thursday September 24th (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