CIP Core regular meeting

Date: July 21st, 2020 (30min~1h)

Time:

- timezones
- Tokyo (Japan) 17:30
- Taipei (Taiwan) 16:30
- Bangalore (India - Karnataka) 14:00
- Frankfurt (Germany - Hesse) 10:30
- London (United Kingdom - England) 09:30

Zoom

Dial-in numbers

Past meetings

Rules

- http://www.linuxfoundation.org/antitrust-policy
- Please mark with (PRIVATE) those parts that should not appear in the public version of these minutes.
- **Please write your own minutes/comments (unless you are on the phone)**

Roll Call

Participants

- Daniel Sangorrin [TOSHIBA]
- DInesh Kumar [TOSHIBA]
- Venkata [TOSHIBA]
- *Masato Minda [Plat'Home]*
- Chris Paterson [Renesas]
- Kazuhiro Fujita [Renesas]
- Kento Yoshida [Renesas]
- SZ Lin [Moxa]
- *Alvin Chen [Moxa]*
- Jan Kizka [Siemens]

- Masashi Kudo [Cybertrust]
- *John Ward [Codethink]*
- please add your name here

Discussion

Previous action items

- AI(Core group): use upstream kernel configs in ISAR
  - USE_CIP_KERNEL_CONFIG = "1"
  - Ready: hihope-rzg2m, iwg20m and simatic-ipc227e.
  - Remove local configs
- AI(Security group): submit kernel config changes upstream (nftables)
  - Kent: Please update
- AI(Security group): merge security branch into the master branch (ISAR)
  - Dinesh: Security branch patches will be shared for review in ML today (21/July)
  - We are preparing security config data and it will be shared for merging once ready
- AI(Testing group): add opt-testtools.yaml for testing
  - Separate LTP to another layer (opt-testtools.yaml)
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/merge_requests/5/commits
- AI(Security group): add debsecan (or other one) to the CI to generate CVE reports
  - SZ: No update.
- AI(Security group): add security packages to kas-security.yaml and verify (Deby).
  - Dinesh: We will verify security packages in Deby once LAVA test definition verification for CIP isar is completed
- AI(Testing group/Security group): coordinate on the integration of Security tests into Linaro test definitions
  - For single node test cases, we are facing low disk space issue, detail will be shared in email for increasing disk space for test case execution. All single node test cases modification and verification is completed except test cases related to disk space
  - For multi-node test cases verification on CIP LAVA infrastructure, waiting for Chris to configure LAVA Coordinator for multi-node test cases execution
- AI(Core group): rename opt-targz-img to opt-lava-img?
  - we need to generate lava images for full images (to test sw updates etc)
  - Jan will think about this
- AI(Core group): ping Neal/Scott/Jan-simon about the approach to release images
- AI(Security group): solve systemd problem with idle locks
  - Dinesh:No update received from upstream
- AI(Security group): backport Duplicity (using python3) to Buster

    - Dinesh: Yasin has updated to complete backporting tentatively by 21/Aug
- Q: kernel config, should we apply security configs to all?
    - option 1: fragments
        - there could be options that get enabled differently depending on the platform
    - option 2: add to the defconfig

Image releases

- What we have now (example: https://lava.ciplatform.org/scheduler/job/30376)
    - Kernel: https://s3-us-west-2.amazonaws.com/download.cip-project.org/ciptesting/ci/uImage_renesas_shmobile_defconfig_4.19.132-cip30_8cc013389/arm/renesas_shmobile_defconfig/kernel/uImage
    - Device tree: https://s3-us-west-2.amazonaws.com/download.cip-project.org/ciptesting/ci/uImage_renesas_shmobile_defconfig_4.19.132-cip30_8cc013389/arm/renesas_shmobile_defconfig/dtb/r8a7743-iwg20d-q7-dbcm-ca.dtb
    - CIP core rootfs with LTP: https://s3-us-west-2.amazonaws.com/download.cip-project.org/ciptesting/cip-lava/rfs/core-image-minimal-qemuarm-ltp.tar.bz2
- Could we restrict this to CIP members with an AWS password (or key)?
- Should we release images only for CIP members or to the public?

Response from LF

Overview: This is a complex question with several facets to it. Because of the complexities, some projects (notably the Linux kernel) simply don't provide binaries, and leave it to downstream distributions to build and use binaries however they see fit.

When a project does distribute binaries, some of the considerations are legal and some are technical. Here are a few things to consider on the legal side.

Entity: CIP is set up under the older structure for projects, where it is within The Linux Foundation legal entity. Because of that, typically we would set up a separate Series LLC to release the binary distributions (we have done this for some other projects like Open Mainframe and CDF). We can work with you on this if you plan to proceed with releasing binaries.

Process: For Zowe, a project in Open Mainframe that releases binaries, they have implemented a process we recommended where the maintainer who compiles and provides the final binary for release provides an assertion of a few statements regarding the composition of the binaries. This sign-off process helps provide transparency and responsibility for the binary release. I can provide more details around this sign-off process.

License compliance: This is unfortunately a very broad topic that has many different practical impacts, depending both on which licenses are involved and on the technical specifics of the project's code and ecosystem. Different projects may have different approaches to making available things like license notices and source code where required, particularly for third-party dependencies that are incorporated into the binaries.

Although I can't really advise project community members on specifics for requirements to comply with particular licenses, I'd encourage that in many cases much of the core requirements can be addressed by ensuring that the project is publishing the original source code for the particular versions of third-party dependencies that they incorporate into the binary – not just linking to where it can be found elsewhere, but making it available by the project. The idea is typically that for whatever version of the binary they are shipping, they would need to make available the corresponding source code of the version they incorporated into the binary. So if they're incorporating the compiled version x.y.z-rc5 of the foo dependency into what they are shipping, then they would also need to make available the source code of that specific version.

The core idea is generally that when you are giving someone a binary, you should also be giving them the corresponding source code that is actually incorporated into that binary.

License information: Being able to comply with licenses necessitates first knowing what licenses are present, and for which components. The LF's Automating Compliance Tooling (ACT) project at https://automatecompliance.org/ is supporting the development of open source tools to help with compliance. The LF also has access to various commercial / proprietary tools that can assist with this, including WhiteSource, FOSSA, Sonatype Nexus IQ, and Snyk (incorporated into CommunityBridge Security). Each of these has different strategies / purposes and none of them is perfect, but I can provide more details if you want to investigate further.

Additionally, for some of our projects I provide a license scanning service where I run periodic scans of the project's source code using some of these tools, and then provide feedback on the detected licenses and recommendations for remediation, etc. If the project is interested in this and wants to budget for it, we could discuss details of what is involved.

Security WG queries

- Any queries about exida meeting information email sent today :)
- Do we have or should we define policy in meta-debian for including packages dynamically or statically
  https://github.com/meta-debian/meta-debian/issues/220
- Can we support “CR 3.14 – Integrity of the boot process” in CIP SW ?
    - While reviewing IEC-62443-4-2 it was concluded in security WG this requirement has dependency on HW since basic root of trust is achieved by putting public key in HW
    - So here the question is can’t we support secure boot in CIP SW by having public key in SW which should be replaced later by end product owner with HW public key?

Next action items

-

Items that need approval by TSC voting members

None

Future topics

- SDK images
- Reproducibility checks