CIP Core regular meeting

- **Date: May 10th, 2022**
- Time: Tokyo (Japan) JST 17:30 (30min~1h)
    - **Please check your local time in timeanddate.com**
- Zoom
    - Meeting URL
    - Dial-in numbers
    - Meeting ID: 917 9128 4612
    - Passcode: 248841
- 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

Roll Call

Attendees (Please change to **Bold**, if you attend this meeting) (Key shortcut: Ctrl+b)

Company	Members
Cybertrust	**Hiraku Toyooka** Alice Ferrazzi
Hitachi	
IoT.bzh	
Linutronix	
Moxa	Jimmy Chen
Plat'Home	**Masato Minda**
Renesas	Chris Paterson Kento Yoshida Kazuhiro Fujita **Hung Tran** Nhan Nguyen

Siemens	**Jan Kiszka** **Christian Storm** Raphael Lisicki
Toshiba	**Kazuhiro Hayashi (WG chair)** Dinesh Kumar **Venkata Pyla** **Shivanand Kunijadar**
VES Solutions	
Denx	

Discussion

Action items updates

- AI(Kazu): Consider to write a blog post about bullseye based CIP Core image (from TSC meeting)
    - Writing... need some references https://www.cip-project.org/blog
- AI(Kazu): Update WG wiki page
- Debian Extended LTS
    - AI(Kazu): Package proposal for Debian jessie
    - AI(Kazu): Start discussion about kernel collaboration in cip-members
- IEC-62443-4-1
    - AI(Kazu): Create the package proposal for bullseye minimal packages
    - AI(Kazu): Suggest ideas in cip-dev to get feedback from isar-cip-core maintainers
    - AI(all): Consider the direction of “Debian repository for CIP Core”tgith
- Reproducible builds
    - AI(Toshiba): Fix reproducible failures due to debconf cache file
- isar-cip-core
    - Support 5.10.y + Debian 11
        - AI(Kazu): Check isar-cip-core CI if the combination is included
    - AI(Toshiba): Test CIP kernel (built with the updated config) + isar-cip-core + SWUpdate on BBB
- CIP Core testing
    - No OpenBlocks IoT device available in LAVA
        - AI(Plat’Home):
            - Check the kernel command line in LAVA is expected one
            - Test the images in S3 can boot using NFS in local environment
- cip-core-sec
    - AI(Toshiba): Update the ISAR gitlab-ci integration branch
    - AI(Toshiba): Support bullseye

- Software Updates
    - No action item

Debian Extended LTS

- Current plan (confirmed by TSC): CIP will fund **1,530 EUR / 6 months**
    - **425 EUR**: Cost for Debian 8 package maintenance
        - "Priority: Required" and their dependencies + CIP's requests (busybox, binutils, openssl, openssh)
    - Remaining(1,105 EUR): Used to improve infrastructure of Debian (ELTS)
- Next step
    - AI(Kazu): Package proposal for Debian jessie
        - WIP: Create "pkglist_jessie.yml" like buster then send the proposal
- Updates from ELTS
    - Freexian is willing to support each Debian release up to 10 years
    - Changed the pricing scheme to be able to announce up-front the cost for the whole support period
        - The documentation updated
    - The change impacts CIP because the package list was very short and the "base price" include all base packages
    - ...
- The collaboration with ELTS in long-term supported kernel
    - AI(Kazu): Start discussion in cip-members
    - ELTS does not provide kernel package support, but it seems there are several requests from their sponsors to provide kernel package as well
    - Raphael is interested in if ELTS could rely on CIP kernel to provide kernel to their customers (sponsors)
    - They require generic kernel (compiled with generic configs) like Debian kernel, so they are wondering how the current CIP kernel maintenance activities work for their customers' requirements and what kind of possibilities for the collaboration are there
    - This discussion is on-going

IEC-62443-4-1 requirements

- Plan of Security WG about package proposal
    - Wants to wait for the conclusion of the target Debian version
        - Debian version is concluded to be Debian bullseye
    - AI(Kazu): Create the package proposal for bullseye minimal packages
- CIP Core release image and release process
    - Requirements:
        - CIP Core image is required for running tests and producing evidence
        - The versions of CIP Core (and CIP kernel) are required for the final assessment certificate

        - CIP Core images should be released after security related issues are resolved
        - Define a procedure for testing security patches to make sure they fix the issue and don't introduce new ones
    - AI(Kazu): Suggest ideas in cip-dev to get feedback from isar-cip-core maintainers
- Debian repository for CIP Core
    - Requirements:
        - Keep all packages required to reproduce CIP release images generated in the past
    - AI(all): Consider the direction:
        - Reuse existing Debian infra (e.g. snapshot, archive)
        - Create CIP's own (e.g. aptly)
        - Others?
- Bug tracking system in CIP
    - Requirement: Lifetime of all bugs should be managed
      => Should be discussed in TSC

Reproducible builds

- Status summary (2022-04-04)
    - Issue-1: changelog file contains date and is not reproducible **[Solved]**
        - This is fixed in 'isar' upstream, below are the references.
            - https://github.com/ilbers/isar/commit/19c31264f5860cf46076558f4425bdb3092ecc18
            - https://github.com/ilbers/isar/commit/53d315fdd3f3dcf70ac3f257d9431ba522e86eb4
    - Issue 2: /var/log/ file contents are not reproducible **[Solved]**
        - This is also fixed in 'isar' upstream, below is the reference
            - https://github.com/ilbers/isar/commit/2eb778680150b8577ee7b19357495e0d5c81e430
    - Issue 3: /var/cache/debconf/config.dat is not reproducible **[Under Investigation]**
        - currently investigation and considering the below two approaches
            - remove '/var/cache/debconf/config.dat' file if no one is interested in this file.
                - **[2022/05/10]** Requested for comments to the patch for removing the debconf cache files in isar image

                  https://groups.google.com/g/isar-users/c/5H0-SfWiu6Q/m/jiikUykBAgAJ
                - Any update required in isar-cip-core side when this patch is merged in isar? => No, just need to update isar commit ID

                - report this issue to applicable community like Debian reproducible org,
            - Discussions
                - Isar: Fix non-reproducible issue due to localepurge
                - Bug report to localepurge
                    - Waiting for the feedback
                - Started discussion in Reproducible-builds.org community
- Future topics
    - Adding tooling (or methods at least) to detect non-reproducibility

isar-cip-core

- Repositories & mailing list
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/commits/master/
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/tree/next
    - https://lore.kernel.org/cip-dev/
- Updates (master)
    - Improve initramfs recipes
    - Update kernel configs, versions
    - Update SWUpdate SRCREV
    - Key updates: update efibootgurad, support QEMU arm64
- AI(all): Support 5.10.y-cip + Debian 11
    - AI(Kazu): Check isar-cip-core CI if the combination is included
        - If not, create a MR
- isar-cip-core/cip-kernel-config: Update kernel configs for BBB
    - Discussions: #1 #2
    - The required changes are in development branches:
        - cip-kernel-config (dev branch) with v2 patches
        - isar-cip-core (dev branch) to build with cip-kernel-config above
        - Can be tested for booting
    - AI(Toshiba): Test CIP kernel (built with the updated config) + isar-cip-core + SWUpdate (no secureboot) on BBB
        - Recently latest isar-cip-core master branch image is booted on BBB successfully
        - Updating recipes to try swupdate on BBB
    - If the tests are OK, ask to merge the v2 patches for cip-kernel-config

deby

- Updates
    - **cip-core-jessie**
        - Upgrading (old) recipes to support LAVA tests, use the same recipe structure as cip-core-buster => Done

CIP Core Testing

- deby has the copy of linux-cip-ci's LAVA functions
    - Plan: Create a separated repository to provide the LAVA functions => Other projects like linux-cip-ci, deby (and isar-cip-core?) reuse the repository
    - Designing of the new project
- No OpenBlocks IoT device available in LAVA
    - The recipesfor the device have been implemented in development branch and the OS images (kernel & rootfs) are built by CI
    - Chris tried boot test with deby images but failed
        - https://lava.ciplatform.org/scheduler/job/658983
    - AI(Plat'Home):
        - Check the kernel command line in LAVA is expected one
            - https://lava.ciplatform.org/scheduler/job/658983#L251
        - Test the images in S3 can boot using NFS in local environment
        - **(minmin as of 2022-05-10)**
          Due to busy with other matters, I have not started the work yet, and will start after 2022-05-13.

cip-core-sec

- Investigating https://salsa.debian.org/security-tracker-team/security-tracker/ to see if we can avoid web-scraping the official site for reserved CVEs
- AI(Toshiba): Update the ISAR gitlab-ci integration branch
- AI(Toshiba): Support bullseye
    - "Buster" is hard-coded in some places

(KEEP) Policies about development target of CIP Core

- AI(Kazu): Move this kind of policies to CIP Wiki
- In CIP, some development works (e.g. adding autopkgtest) are on-going but they (mostly?) target on bullseye(stable) or older
- CIP Core should have clear policies about which Debian release that CIP mainly develops new features
    - Development: sid (= testing until soft freeze)
    - Maintenance: stable or older
- This would prevent CIP from having their own infrastructure (=additional efforts) to maintain their custom (backported) features and would make more chances to discuss / contribute with/to upstream (Debian)

Software Updates WG

- **Updates in related repositories (e.g. isar-cip-core)**
  - [(v2) swupdate: Update SRCREV] => Applied
    - Update SWUpdate to commit https://salsa.debian.org/debian/swupdate/344548c816b555c58ec199f31e45703897d23fb5
  - [(v2) Fixes and improvements for SWUpdate images, kernel/config update] => in master
    - qemu-arm64 enabling for SWUpdate/secure boot using the UEFI pattern
    - update to EFI Boot Guard 0.11
    - switch to unified kernel images built by EFI Boot Guard
    - fix for verity setups with CONFIG_DM_VERITY=m
    - improve error handling when mounting /etc overlay
    - update to latest CIP kernels and cip-kernel-config
- **Support ARM targets**
  - Trying to build & boot isar-cip-core image on BBB
    - QEMU arm64 is now enabled isar-cip-core next
    - QEMU armhf (Jan started the porting)
      - U-Boot is fine
      - EFI Boot Guard needs more works
        - Compilation (Solved)
        - Run on QEMU (Not yet, crashes early) => now it's running
        - Unified kernel image generation
      - Issue: https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/26
- SystemReady (from ETSC meeting on 2022-04-04)
  - Jan had a discussion with ARM
  - If the interface is very well implemented, it make simplify our implementation
    - IoT profile
  - CIP members have interest on this, but the details need to be checked
  - Related to SWUpdate/secure boot story
  - Clarify and share the basic features, check how it's related to CIP members' use cases

Q&A or comments

- How to approach meeting CIP kernel security hardening requirement
  - https://gitlab.com/cip-project/cip-documents/-/blob/master/security/security_hardening_guidelines.md
- Do we already know what all kernel configs applied from security hardening perspective
- Are there any best practices for kernel security hardening ?

Items that need approval by TSC voting members

- None

Future topics

- SDK images
- Next tiny profile