CIP Core regular meeting

- **Date: November 22nd, 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
Bosch	
Cybertrust	**Hiraku Toyooka** Alice Ferrazzi
Hitachi	
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 Tho Nguyen Dat

Discussion

Action items updates

- AI(Kazu): Update WG wiki page => Started
  - Need to add the following information that was discussed in CIP Core
  - 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)
- Debian Extended LTS
  - AI(Kazu): Package proposal for Debian jessie
    - WIP: Have an issue in script
  - AI(Kazu): Start discussion about kernel collaboration in cip-members
- IEC-62443-4-1
  - AI(Kazu): Create the package proposal for bullseye minimal packages
    - WIP Have an issue in script
  - AI(Dinesh): Ask Chris (Testing WG) “how frequently the CIP Core needs to be built for kernel CI testing”
    - Whenever new commit is pushed
    - Current situation: Always using the latest commit in master
    - CIP Core can go to the next step (suggest to use the latest CIP Core release version in testing WG)
- Isar-cip-core
  -
- CIP Core testing
  - No OpenBlocks IoT device available in LAVA

        - AI(Plat'Home): Update kernel configs
        - Summary: (as of 2022-10-11)
          The kernel update for LAVA has been completed.
          USB error is occurring in Iwamatsu-san's environment.
          But, no errors have occurred in Plat'home
            - I am discussing it with Iwamatsu-san.
        - (as of 2022-11-22) I invited Iwamatsu-san to Slack. I thought about using CIP's Slack, but it was better not to use CIP's Slack because the communication would be in Japanese (advice from Iwamatsu-san). We do it on Slack at Plat'home.
- cip-core-sec
    - AI(Toshiba): Add improvements to solve some issues and make the project official (move to cip-project)
    - AI(Toshiba): Update the ISAR gitlab-ci integration branch
- SWG AI
    - CIP Secure Storage
        - No update
        - Started to create template for CIP Secure Storage
        - https://docs.google.com/document/d/1sMeKBi11SJr2TpWP4b6EQKJGneMMjE-zPZIcHqUhvbA/edit
    - CIP Security hardening document
        - Draft document is shared for review at https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/49
    - Remote session termination investigation update
        - [cip-security-tests/Issues/#1]: [WIP] Updating tests in IEC layer
        - https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/merge_requests/1/diffs?commit_id=2580019f4802073b9f8e2989c0f91b5e9e8051cb
    - Add data encryption packages in isar-cip-core
        - No update
        - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/29
        - Patches for adding package are in local branch but they are for ARM64 architecture
            - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/blob/2de2aaa5331b2094137779c4375ff877394415c9/doc/README.information-confidentiality.md
    - Defining minimum CIP HW specification or selecting reference hardware for IEC-62443 certification
        - This is something to be decide by CIP members, it seems without reference hardware CIP can not be considered as platform but as Software Application
    - SWG to send email to check other members opinion for following topics based on BV response

        - What's the desirable security level for CIP IEC-62443-4-2 certification, BV suggested SL-1 or SL-2
        - Any specific protocol support should be added e.g. below list (it affects SVV testing cost)
            - https、opc、ftp、ntp、ssh、telnet、modbus、canbus、profibus、profinet

Debian Extended LTS

- AI(Kazu): Package proposal for Debian jessie
    - WIP: Create "pkglist_jessie.yml" like buster then send the proposal
- 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

- 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
    - Related conversation
    - The current idea
        - When: Regularly releases just after Debian point release (e.g. 11.1, 11.2...)
        - What:
            - Recipes
            - Images for each CIP reference hardware
            - Test results
            - Security reports (by cip-core-sec)

    - SWG: Needs to define “version”
    - AI(Dinesh): Ask Chris (Testing WG) “How frequently the CIP Core needs to be built for kernel CI testing”
        - Discussion in ML in progress, Chris yet to answer this question
- Discussion with Exida
    - https://docs.google.com/spreadsheets/d/1PEdWzSrm3i2Dn3VLP0ho36HHKhLl2H6V/edit?usp=drive_web&ouid=109781914047697344061&rtpof=true
    - AIs
        - Exida: How to do static analysis, etc.
            - Waiting for exida response, basically for mainline kernel SCA not needed but need to clarify what’s done for CIP specific changes
        - CIP Core/SWUpdates: None?
    - Questions about kernel?
        - CIP specific changes in CIP kernel
        - Static analysis
    - CIP specific changes in CIP Core (e.g. bullseye)
        - Packages
            - SWUpdate
            - EFI Boot Guard
        - Features
            - Integration of SWUpdate and related functions
                - Remote / local
            - What features do we need to commit?
        - Required information
            - Security issue
            - ...
    - Define minimum requirements about the environment?
        - Dinesh will make a discussion about this on CIP ML => Done
            - Minimum RAM requirements
            - Minimum persistent store (Flash/SSD/magnetic drive) storage requirements
            - Minimum NIC (network interface card) requirements (such as 100baseT, 1000 baseT etc.)
            - Whether a TPM is required. It is recommended that you require a TPM and most platforms these days have TPMs.
            - Requirement for a hardware RNG (random number generator). This is required to meet cryptography requirements
    - Effective way at the moment: Collect questions then check in CIP afterwards
        - No questions just need to clarify and document how CIP specific changes are tested

- (ON-HOLD) 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?

Reproducible builds

- Open issues
    - #31[file system time stamps are not identical]:
        - [WIP] shared patch to upstream (isar) and discussing further.
        - created a test case to check the reproducibility in the isar and shared the patch2 with upstream.
- Future topics
    - Fix remaining issues #35 and #31
    - CI for regularly check the reproducible problems
    - 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
    - Update cip-kernel to the latest
- WIP: Patch series to build a QEMU setup which uses OP-TEE to use RPBM (Replay protected memory) of an EMMC for a secure storage are under review
    - ARM specific
    - Dinesh: Any plans to add demo / test applications to test the feature?
        - Jan: No, but we can discuss if someone has requirements about app

deby

- (No update)

CIP Core Testing

- deby has the copy of linux-cip-ci's LAVA functions
    - (No update)

    - Plan: Create a separated repository to provide the LAVA functions => Other projects like linux-cip-ci, deby (and isar-cip-core?) reuse the repository
    - Created the draft project in playground
    - Implemented the draft and validating
- No OpenBlocks IoT device available in LAVA
    - The recipes for the device have been implemented in development branch and the OS images (kernel & rootfs) are built by CI
    - AI(Plat'Home): Update kernel configs

cip-core-sec

- (No update)
- AI(Toshiba): Add improvements to solve some issues and make the project official (move to cip-project)
- AI(Toshiba): Update the ISAR gitlab-ci integration branch

RISC-V Investigation

- "qemu-riscv64" image generation is supported in isar-cip-core master
    - Used to test CIP kernel with KernelCI
    - This is an exceptional target and not in WG's maintenance scope in official because it's based on Debian riscv64 packages in sid-ports which are not included in Debian official release (yet)

Software Updates WG

- Related updates in isar-cip-core
    - WIP: An issue & RFC to fix issues about UUID
- Support ARM targets
    - Supporting physical ARM64 boards?
        - Toshiba: MPSoC ZCU102 is a preferred option, but no requirement at the moment
    - Any boards that can be used to implement secure boot & secure storage?
        - CyberTrust (MPSoC ZCU102): No requirement, not sure about H/W features
        - Renesas: No requirement
- Request(Jan): Support data encryption (secure storage)
    - Pre-condition for security WG activities
    - AI(SWG): Discuss about requirements about secure storage
        - Currently lacking contribution in SWG to take up the pending work items
    - We'd like to have some common parts to support the feature among the multiple targets (in isar-cip-core)
    - Targets

        - QEMU (ARM): WIP
        - QEMU x86
            - TPM emulation configuration required
        - Physical boards
- 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
    - SystemReady is targeting on ARM
        - RISC-V is not included

Q&A or comments

- (Dinesh)
    - Are there any sessions by CIP Core/CIP Kernel WG members at OSS Japan?
        - Kazu: No WG specific topic I found
    - Are we planning to have the next CIP Core meeting on 06th Dec ?
        - Waiting for the decision of the next TSC meeting. If it will be held in the same week, I will hold the WG meeting on the same day

Items that need approval by TSC voting members

- None