CIVIL INFRASTRUCTURE PLATFORM

CIP Technical Steering Committee Meeting

Date: 26th June 2020.

Roll Call

TSC members

- *Masashi Kudo (Cybertrust) (Representative)*
- *Takuo Koguchi (Hitachi)*
- *Hidehiro Kawai (Hitachi)*
- *SZ Lin (Moxa) (Representative)*
- *Masato Minda (Plat'Home) (Representative)*
- *Chris Paterson (Renesas)*
- *Kento Yoshida (Renesas)*
- *Takehisa Katayama (Renesas) (Representative) (Voting)*
- *Kazuhiro Fujita (Renesas)*
- *Jan Kiszka (Siemens) (Representative)*
- *Wolfgang Mauerer (Siemens) (Representative)(Voting)*
- *Urs Gleim (Siemens)*
- *Akihiro Suzuki (Toshiba)*
- *Dinesh Kumar (Toshiba)*
- *Daniel Sangorrin (Toshiba)*
- *Nobuhiro Iwamatsu (Toshiba) (Kernel Maintainer) (Voting)*
- *Yoshi Kobayashi (Toshiba) (Representative) (Voting) - Chair*
- *Pavel Machek (Denx) (Kernel Maintainer)*

Discussions

Security working group

Status updates for the last 6 month

- Conference
    - regular meeting
        - 11 bi-weekly meetings, 1 extraordinary meeting, 1 long-call
    - IRC
        - held weekly in private to proceed investigation about the standards/norm

        - temporarily changed to the conference call to investigate IEC 62443-4-1 now
- Security package proposal
    - Description:
        - Last year, we started an investigation of the requirements for IEC 62443-4-2 and that investigation had completed.
        - Selected 21 debian packages to meet their requirements. And we propose to add these 21 packages to the package lists of CIP core.
    - Status:
        - Proposal suspended with consideration that the proposal content may change depending on the assessment with the CB
        - Security packages are evaluated using the security branch on CIP core
    - Link:
        - description for the requirements and the proposed security packages
    - Plan:
        - Merge the security branch to the main branch on CIP core
        - Discuss the supporting policy for the security packages
- Test cases, self-evaluation for the security packages
    - Description:
        - We defined 55 test cases according to IEC 62443-4-2 / CSA by ISASecure certification.
        - Completed manual evaluation for the 55 test cases.
        - 1 package ('duplicity') is pending, required to backport from the upper version
        - 2 test cases (related to 'systemd' and 'nftables') are false
            - Measures are under consideration with CIP core / CIP-dev
    - Status:
        - Preparing for automated testing in LAVA environment (40/55 LAVA test definitions are done.)
    - Link:
        - final report of self-test cases according to IEC 62443-4-2
    - Plan:
        - Start automated test using LAVA environment
            - <**Question**> Do we need to submit a proposal to use LAVA?
            - <Answer> Yes.
        - Make test using the reference hardware
- Investigation for IEC 62443-4-1
    - Description:
        - Started to investigate IEC 62443-4-1, i.e. secure development process for software, for preparation of the assessment.
        - Expand the technical conference at IRC, which is one hour a week, to 1.5 hours and change it to a conference call temporarily.
    - Status:
        - 18 / 47 requirements are reviewed in working group
    - Plan:

        - Publish the investigation result to clarify what we are required
        - Define the efforts within the security WG and requirements for other groups
        - Start the assessment w/ Exida and revise the rules
- Preparing to publish the document
    - Description:
        - We need to create some documents for the assessment, and they are required to publish with all users.
    - Status:
        - Defined the required documents and preparing them now:
            - IEC-62443-4-2 test cases validation report, *issued to internal and CIP-dev*
            - APP & HW rules document, *issued to internal*
            - CIP User Manual
            - Security Capabilities Document
            - Product features document
            - IEC-62443-4-1 (development process) documents
        - Got approval to create a public repository on CIP gitlab to publish documents, and will publish these public documents on it.
    - Plan:
        - Create a repository and put these documents on it when it is completed.
- Marketing activities
    - updated the security working group wiki page
    - Planned to attend a few conference related to sec-institute, but canceled the events

Plans and Roadmap

- Refer to the above
- Next milestone:
    - Get contract with Exida in July
    - Gap assessment in this year (at least 3 months)

Discussions

- Ongoing considerations
    - Supporting with CIP core / CIP-dev
        - kernel configuration changing
        - not working session lock function in 'systemd'
        - automated CVE tracking tool investigation

Kernel team

Status updates for the last 6 month

- Contribution
    - Continue to contribute LTS kernel
- Releases

    - 4 kernels
    - Release period does not change
    - Release process is stable enough and not required to change
- Now CIP has 3 tools to maintain kernels (classify, sec, cip-kernel-config)
    - cip-kernel-sec
    - Classify-failed-patches
    - Cip-kernel-config
-

Future plan, Roadmap and Discussions

- **Please refer to the following slides.**
    - https://docs.google.com/presentation/d/1jhZQzgLAxeWzW_fUG2aUfw5Q_G6xUOJSs7ZL0pc_GK8/edit?usp=sharing
- No conclusion was made in TSC meeting
    - AI(Kernel team): Propose multiple options to start to discuss what kinds of sacrifices CIP members can accept.
        - E.g. Reducing release cycle, Support scope reduction (reduce kernel config options)
    - Expected to choose the next SLTS based on LTS this year.
    -
- Real-time patches may not merge within this year.

CIP Core

Status updates for the last 6 month

- Started regular meetings on Zoom
    - https://wiki.linuxfoundation.org/civilinfrastructureplatform/cip-core-meetings
- ELTS (Jessie)
    - Fund an arbitrary amount for some infrastructure projects to help their security workflow.
- Work on Lifecycle/EOL definitions and scripts/plots
    - https://gitlab.com/cip-playground/cip-lifecycle

		Debian version (Projected EOL)		
		8 (jessie)	9 (stretch)	10 (buster)
CIP kernel version	4.4	2025-04-26	2027-01-17	Unsupported
	4.19	Unsupported	2027-06-17	2029-01-11

* CIP may decide to extend the supported period based on member feedback

- Package list

    - We created a Package Decision Process (PDP) to manage the list of packages that will receive CIP's long-term maintenance
        - https://gitlab.com/cip-project/cip-core/cip-pkglist/-/blob/master/doc/pdp.md
    - We created an initial package list for Debian 10 (Buster)
        - https://gitlab.com/cip-project/cip-core/cip-pkglist/-/blob/master/pkglist_buster.yml
    - We created scripts to manage package proposals and registration
        - https://gitlab.com/cip-project/cip-core/cip-pkglist
    - Metrics
        - 5 GitLab issues (closed)
        - Commits: 33
            - Authors: Hayashi-san, Venkata-san, Punit-san
            - 10 files changed, 1701 insertions(+), 396 deletions(-)
- cip-core/deby
    - Changelog
        - Remove all local kernel configs and use the ones from cip-kernel-config
        - Add support for simatic-ipc227e (and gitlab-ci build job)
        - Add lava job templates for each board
        - Add code to submit jobs to LAVA from gitlab-ci (uname boot test)
        - Add instructions to build each target's image for LAVA
        - LTP support
            - https://gitlab.com/iwamatsu/meta-cip-test-support.git
            - opt-smc.yaml
        - Add opt-dhcp.yaml (installs busybox-udhcpc)
            - used by LAVA jobs that require internet
        - Update to Kas version 2.0
        - Comment LAVA BBB block until the device is available
        - meta-debian
            - Add recipes for 21 security packages to meet IEC-62443-4-2 security requirements
                - acl, adduser, aide, audit, duplicity, google-authenticator, openssh, openssl, pam, pam-pkcs11, pam-shield, shadow, sudo, tpm2-abrmd, tpm2-tools, tpm2-tss, util-linux, chrony, nftables, suricata, syslog-ng
    - Metrics
        - Commits: 39
            - Authors: Hayashi-san, Iwamatsu-san
            - 30 files changed, 400 insertions(+), 144 deletions(-)
- isar-cip-core
    - Changelog
        - Add 24 binary packages to meet IEC-62443-4-2 security requirements
            - openssl, libssl1.1, fail2ban, openssh-server, openssh-sftp-server, openssh-client, syslog-ng-core, syslog-ng-mod-journal, aide aide-common, libnftables0, nftables, libpam-pkcs11, chrony,

tpm2-tools, tpm2-abrmd, libtss2-esys0, libtss2-udev, libpam-cracklib, acl, sudo, libauparse0, audispd-plugins, auditd, uuid-runtime
        - Add opt-targz-img.yml (tarballs for LAVA)
        - Use cip-kernel-config (iwg20m, hihope-rzg2m, simatic-ipc227e)
        - install.tmpl for 4.4 arm kernels (patch for ISAR)
        - LTP support
    - Metrics (not counting the latest Quirin patches)
        - Commits: 12
            - Authors: Jan, Quirin
            - 12 files changed, 107 insertions(+), 6 deletions(-)
- Method to obtain metrics
    - number of commits: git log --oneline --after="2020-01-01" | wc -l
    - code changes: git diff $first2020commit..HEAD --stat
    - authors: git shortlog -s --after="2020-01-01"

Plans and Roadmap

- Image releases
    - Goal: try/test images locally on the reference hardware
    - Can serve as a basis for hands-on to CIP Core on a future mini-summit
- More testing
    - Use isar-cip-core for testing the kernel (LTP, etc), and deby for kernel boot tests
        - https://gitlab.com/cip-project/cip-testing/linux-cip-ci/-/issues/11
    - Test CIP Core (isar-cip-core and deby) on LAVA
        - Security tests
        - Other tests
    - Add back support for BBB once available in LAVA
- Merge security layer into CIP Core (isar-cip-core and deby)
- Finish work on CIP Core lifecycle and reflect the result on the wiki page
- Finish support for cip-kernel-config in isar-cip-core
    - qemu-amd64, bbb
    - remove local configs
    - allow extending cip-kernel-config in exceptional cases
- Future topics:
    - SDK, Reproducible builds

Discussions

- Image releases
    - What level of security and license compliance is required?
        - Security: e.g. Signature
            - AGL does not use signatures.
            - If we use signatures, that requires some additional development resources.

        -
    - We might need a snapshot mirror (filtered) faster than snapshot.debian.org
        - In this case we will need a new contributor and a server
- New contributors apart from Siemens and Toshiba
    -

CIP Testing Workgroup

Items need to be approved by TSC voting members

Status updates for the last 6 month

- Added lab-cip-cybertrust and lab-cip-denx
- We now have 21 devices (covering 12 device-types) in our LAVA environment
- Added LTP testing support
- Added RT testing support
- Added rebase branch comparison support
- Added build support for all CIP Kernel configurations
- Added test support for most CIP reference platforms
- Added build support for stable-rc 4.4/4.19 Kernels using CIP Kernel configurations, boot/SMC tests are run on supported boards
- Created staging-lava.ciplatform.org
- Linked lava.ciplatform.org with kernelci.org
    - Currently 'baseline' tests on upstream/stable Linux Kernels are run on qemu, BBB, r8a774a1-hihope-rzg2m-ex, r8a774b1-hihope-rzg2n-ex and r8a774c0-ek874 devices
    - Support for other platforms is in progress

Plans and Roadmap

- Get at least 1 of each reference platform hosted in 2 or more LAVA labs
- Use cip-core-tiny and cip-core-generic for all Kernel testing
- Finish test support for all reference platforms
- Improve Kernel test results front end
    - Setup and configure kernelci.ciplatform.org (or perhaps cip.kernelci.org?)
    - Integrate CIP's GitLab based Kernel builds with KernelCI's backend
    - Automatic test regression detection
- Test case expansion
    - LTP for all reference boards
    - kSelftest
- Add 'small instance' support to gitlab-cloud-ci for test jobs
- Speed up build times
    - Use ccache
- Speed up test times
    - Move s3 storage to EU
    - Integrate squid cache into cip-lava-docker

- Add monitoring for the various CI components (LAVA master, LAVA workers etc.)
- Add support for the next SLTS Kernel
- Add support for the next CIP Core versions
- Sort out the mess of repositories/projects in https://gitlab.com/cip-project/cip-testing

Discussions

- Any requests for items to be added to the backlog?
- Test case expansion
  - Any tests that would help with Kernel testing?
- What support do the non-Kernel WGs need?
  - CIP Core package tests?
    -
  - Security certification tests?
    - Proposed above
  - Remote update tests?
    - Planed in next iteration
  - Daniel commented u-boot test as a part of CIP testing
    - Jan also commented this is relate to software update activity
- Static Analysis tools?
  - Not sure

Software update workgroup

Status updates for the last 6 month

- Make development environment open
  - Make cip-sw-updates group
  - Make cip-sw-updates-demo for managing demo scripts
  - Make cip-sw-updates-tasks for managing our tasks
- List up our tasks
- Work on the tasks in order of priority
  - Integrate CIP SW Updates mechanism into deby
    ---> This was suspended to work on other high priority tasks
  - Prepare minimum required development environment
    - Clean a branch relevant to SWUpdate on isar-cip-core

Plans and Roadmap

- Remaining 3rd iteration tasks (- the end of July 2020)
  - Commit source codes that already exists in my local machine
    - Add a demo of ELCE 2019 regarding a safe update feature
  - Fix what should have been integrated into the current software update mechanism
    - Enable u-boot environment redundancy so that software updates can continue if a power failure occurs
    - Fix how to use binary delta update

    - The remaining tasks will move to the next iteration
- Plan of 4th iteration (the beginning of August 2020 - the end of January 2021)
    - Support new basic features
        - Support kernel update feature
        - Support HTTPS connection between client and server
        - Support rollout feature
    - Make a demo better
        - Fix bug of hawkBit dashboard regarding screen refresh
        - Add multiple ways to trigger software updates such as push update and arbitrary polling time
        - Automate a demo
    - Integrate the software updates mechanism into other WGs
        - Integrate the CIP software updates mechanism into CIP Core properly
        - Integrate the CIP software updates mechanism into CIP Testing properly

Discussions

- Need contributors to make our progress better
- Comments
    - Patches sent recently by Quirin to provide updatable secure boot for UEFI (via efibootguard)
    - Patches to do something similar with U-Boot native means under development, will follow at some later point
    - Those two paths should cover the main use cases for swupdate on devices and should carry most recent pattern -> goal is to use isar-cip-core in project layer as source
    - We need to also add the backend part (hawkbit) and test it during the software updates

Other topics

- Upcoming events
    - OSS Japan CFP deadline: 12 July
        - CIP will not sponsor this event.
    - ELC Europe CFP deadline: 26 July
- Hong-Kong Open Source Conference
    - Expect more than 100
- Linux Plumbers virtual event
    - Chris will attend
- DebConf will be a virtual event
- Debian mini-conf Europe
    - Undecided yet