VirTEE Annual Review 2025

Tyler Fanelli <tfanelli@redhat.com>
Larry Dewey <Larry.Dewey@amd.com>

Contents

- Intro, project goals
- Key milestones since joining
- Plans for current year
- Annual review

Intro, project goals

- Repository of FLOSS tools and libraries to enable the construction of TEEs.
- Command line tools, libraries, and attestation components.
- Common abstractions to be used by developers and admins of TEEs.
    - Libraries used by:
        - Hypervisor developers abstracting common Linux APIs for confidential computing.
        - Attestation developers to produce and evaluate TEE evidence for trustworthiness.
    - CLI tools used by:
        - Administrators of TEE hosts for management.
        - Guest owners for navigation and attestation of TEE-protected VM guests.
- Donated to CCC in beginning of 2024.

Progression status, key milestones since joining

- Support for more TEE architectures
  - Upon joining, VirTEE only had full support for AMD SEV-SNP with contribution from Red Hat and AMD.
  - Desired to support other TEE architectures.
  - Projects started since joining:
    - `tdx` (Intel TDX) Rust library.
    - `cca` (ARM CCA) Rust library.
    - `tdxhost`: CLI administrative tool for Intel TDX.
    - `tdxguest`: CLI navigation and attestation utility for Intel TDX guests.
- Adoption
  - Libraries adopted by:
    - `libkrun`, `crun-krun` container runtime project.
    - `Confidential containers` cloud native confidential computing project.
    - `Trustee` attestation server.
    - Azure CVM tooling.
    - Many more.
  - CLI tools packaged for RHEL, Fedora, and openSUSE.

Plans for current year, growth goals

- Support for more TEE architectures
  - Preliminary support for other architectures begun. Still much progress to be made for both system libraries and attestation components to reach full support for:
    - Intel TDX
    - ARM CCA
  - Continue to follow and iterate over TEE architecture and subsystem changes in Linux.
  - Discuss and plan for RISC-V TEE support.
- Drive more adoption
  - Continue bug fixes and new TEE features as they arrive within the Linux API.
  - Invite more developers within the CCC and CNCF communities to become involved with the project.

Annual review

- Basic info:
  - Current stage: **Incubation**
  - Mentor: **Yash Mankad**
- Technical charter → **Unchanged**
- Progression status
- License scans → **Unchanged**
- Budget allocation

Thanks!