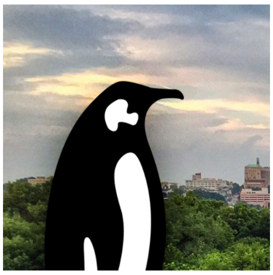

Contribution ID: **200**   Type: **not specified**

Proposal of porting Trusted Execution Environment Provisioning (TEEP) Protocol with WorldGuard

Monday, November 13, 2023 10:40 AM (20 minutes)

The objective of TEEP Protocol is to install and update the target device or server to have the latest critical software and data which is called Trusted Component (TC) at the IETF.
In the procedure, the server checks the trustworthiness of the target devices remotely whether it is compromised or not, and only installs and updates the software components if confirmed it is not compromised.

I would like to propose possibilities of porting from existing TEEP Protocol implementation on RISC-V relies on only PMP to using WorldGuard which was recently donated to RISC-V International from SiFive.
The current TEEP implementation only uses PMP hardware feature and the Keystone software stack.
It will have much practical value to have TEEP working on better hardware support which WorldGuard provides for the hardware isolated region.

I am standardizing the TEEP protocol and released the open-source reference implementation of it at the end of April 2023 at the Internet Engineering Task Force (IETF). I am also an Author which enables life cycle management of software packages as a Trusted Components (TC). The TC consists of Trusted Applications and Personalization data covers from IoT/Edge/Network devices, to drone, automotive and heavy industry equipment.

Maintaining the security bugs in the software packages is becoming challenging, while the number of software packages required for developing products is dramatically increasing every year.

The development of TEEP Protocol implementation started in late 2018.
It was a deadly psychological difficulty to repeat the approval request for releasing the source code for four years which took until April 2023.

It was initially planned to disclose in March 2019, so I could collaboratively develop with the people with Keystone project at UC Berkeley and Open Enclave project by Confidential Computing Consortium at the Linux Foundation. And making it worse, every time Keystone project releases new versions or the TEEP Protocol evolves at every IETF meeting, I had to revise the internal implementation only with limited engineers in AIST because the people of Keystone and Open Enclave do not know we was developing TEEP Protocol on top of their software stack. If I could have collaborated the implementation with the people of Keystone and the Open Enclave, then the development efforts would be much less, and the quality of the implementation would be improved by having their expertise. It was a typical bad example of working on open collaboration community like RISC-V without using the benefit of collaboration.
I hope Japanese organization will learn the good practice sometime in the future.

Primary author: TSUKAMOTO, Akira

Presenter: TSUKAMOTO, Akira

Session Classification: RISC-V MC

Track Classification: LPC Microconference: RISC-V MC