Embedded Confidential Computing

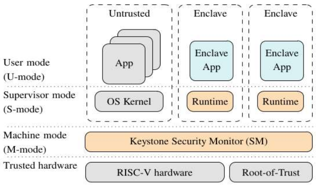
Author: Markku Kylänpää

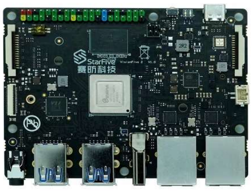
What is confidential computing?

- Confidential computing.is protecting data in use in addition to in transit and at rest
- Confidential computing building blocks:
  - Encryption, isolation, remote attestation, confidential virtual machines (CVMs)
- Cloud services utilizing AMD SEV, Intel TDX (or SGX),…

Why embedded confidential computing?

- Constraints:
  - Latency, narrowband connections, performance, memory, storage, communications
- Resource constrained platforms:
  - Instead of CVMs using split app model (e.g., ARM TrustZone)
  - Heterogenous platforms, e.g., ARM, RISC-V



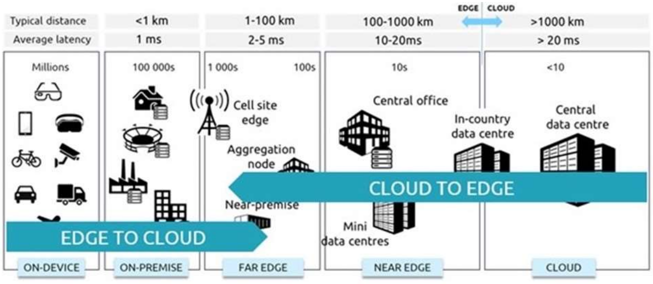


Experimenting with an embedded platform

- Using RISC-V based confidential computing framework Keystone that is utilizing low-level Physical Memory Protection (PMP) framework for isolation
- Rust programming language SDK for building Keystone enclave and host applications for the RISC-V architecture
- Utilizing existing Keystone kernel, OpenSBI, enclave runtime, and enclave loader components, but allows the use of Rust in enclave apps and host programs
- The code has been tested with QEMU and StarFive VisionFive2 development board. Open source:
  - https://github.com/vector-sdk/vector-keystone
  - https://github.com/vector-sdk/rust-sdk
- (Old) publication:
  - J. Julku and M. Kylänpää, “Towards a Rust SDK for Keystone Enclave Application Development,” Proceedings of the 9th International Conference on Information Systems Security and Privacy, pp. 29–37, 2023, doi: 10.5220/0011611900003405.

Use case: Secure edge computing

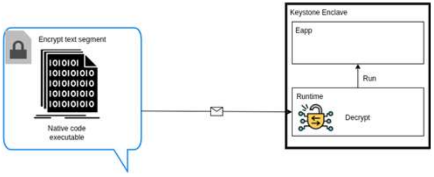
- Continuum Cloud-Edge-IoT – workload orchestration to optimal location



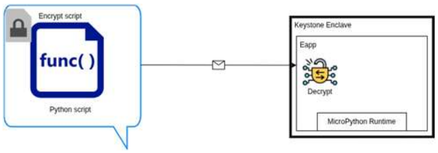
Source: EU

Use case: Confidential algorithm protection

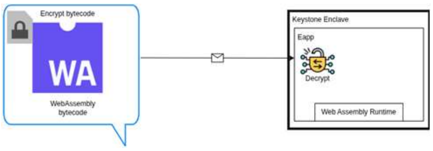
- Experiment with flexible alternatives to provide encrypted code to Keystone enclaves:
  - Encrypted native code enclave apps (eapps)



  - Encrypted Python script and MicroPython runtime



  - Encrypted WebAssembly bytecode and tinyWASM runtime



Conclusion

- **Confidential computing is not just for cloud services. It can be extended to Cloud-Edge-IoT continuum.**
- **Optimized location for workload execution may depend on latency or data transfer constraints.**
- **In addition to confidential data, confidential algorithm may need protection as well.**
- **Resource constraints require the use of the protected app model instead of confidential virtual machine.**
- **Experiments with Keystone enclave apps using Rust, Python, WebAssembly (and optional encrypted app support)**

www.vttresearch.com

Contact: Markku Kylänpää, Senior Scientist
Tel. +358 40 546 4427, markku.kylanpaa@vtt.fi

beyond the obvious

Co-Funded by the European Union GA 101096435