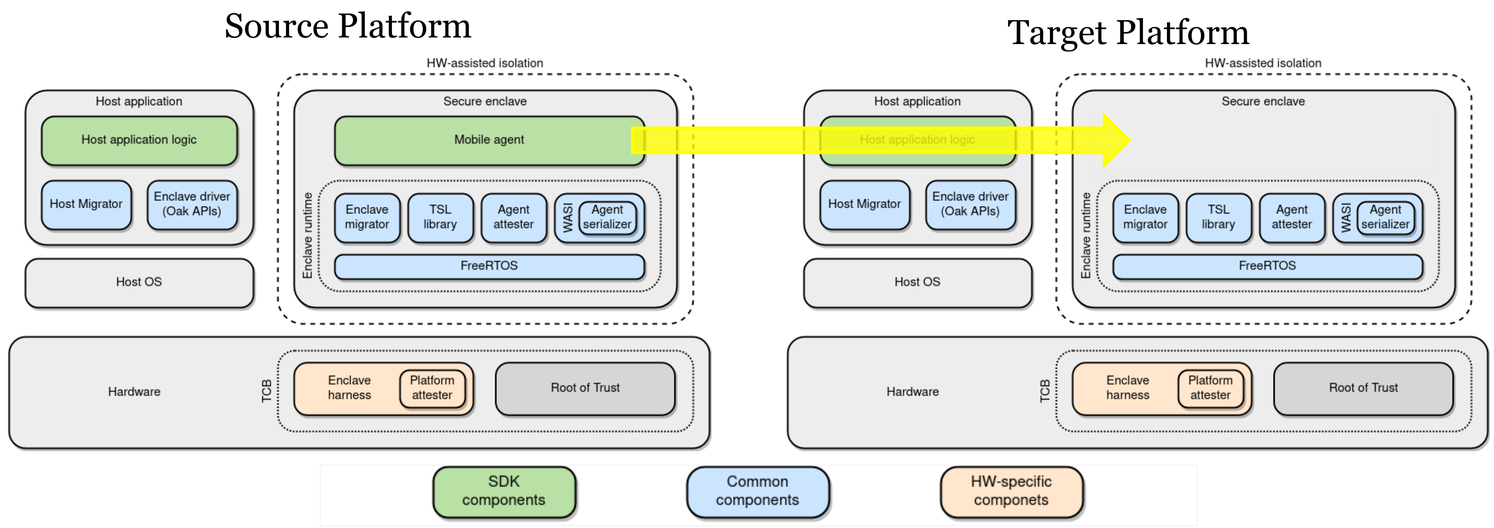
Securely migrating WebAssembly Mobile Agents between secure enclaves

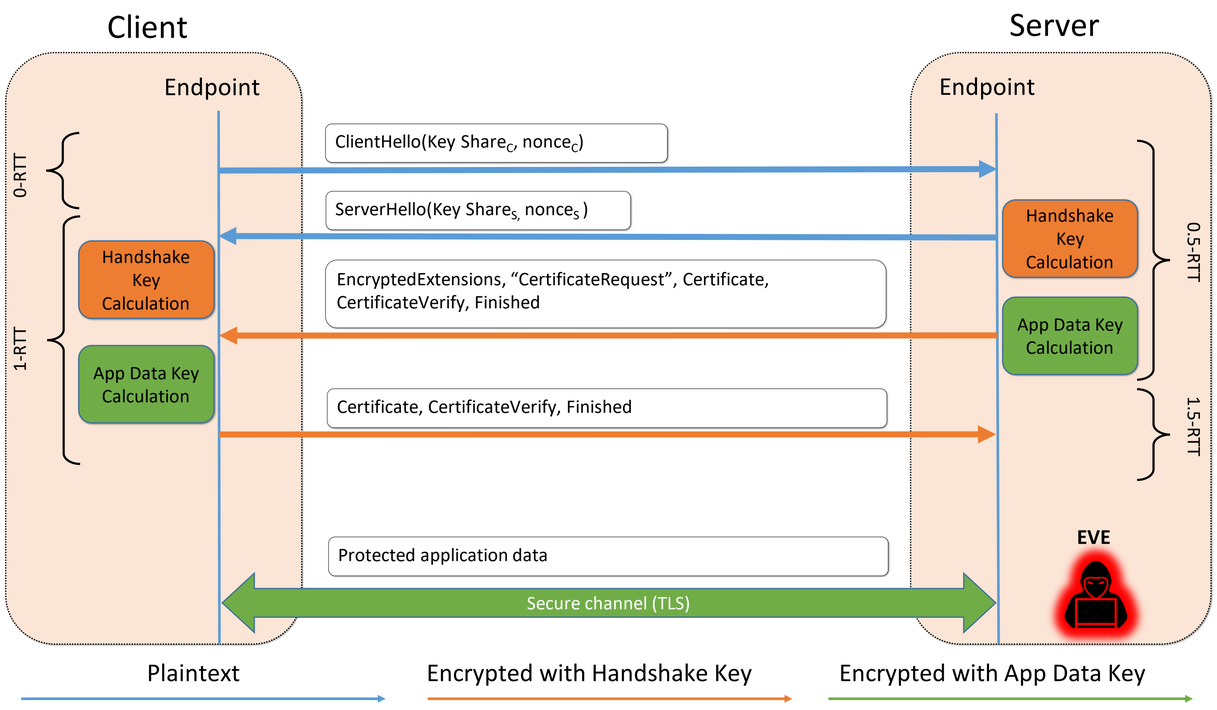
A secure enclave (SE) uses hardware-assisted isolation techniques to provide a trusted execution environment where the executed code cannot be tampered with by the surrounding unknown environment. SEs are strongly bounded by hardware isolation to the processor architecture they are implemented on. Hence, SEs cannot be easily moved between platforms with different architectures.

Migration of Mobile Agents

Goals:
- Trusted execution environments for end developers
- Hardware architecture independence
- Small runtime code-size footprint
- Migration capabilities

Use case examples:
- Off-loading mechanisms in Mobile Edge computing
- IoT move a DRM decoder from the mobile phone to a smart TV for a better experience





Secure channel – TLS 1.3

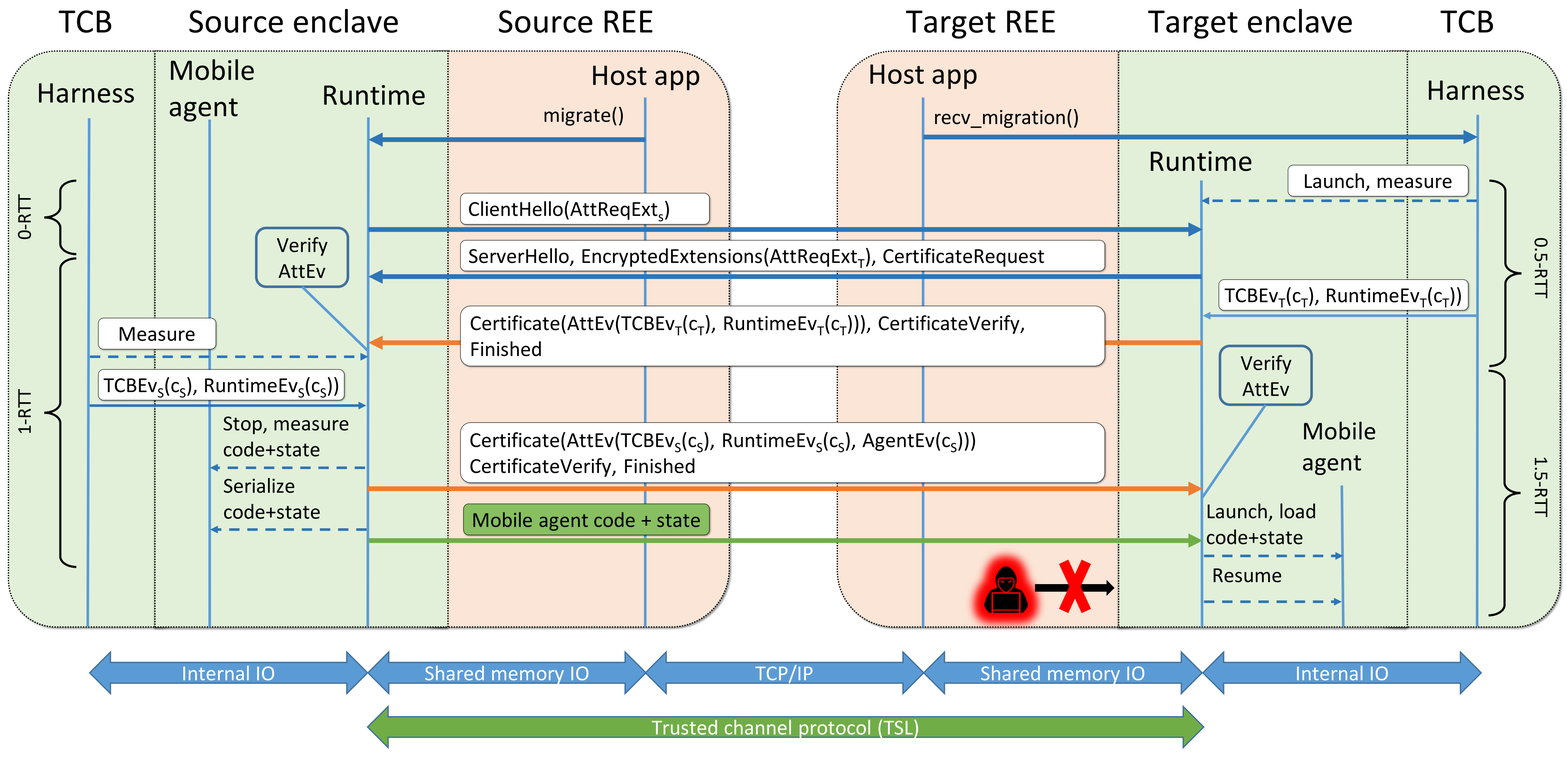
A secure channel ensures data integrity, data confidentiality, authentication of the endpoints, replay protection, and key confirmation between the entities involved in the communication. The TLS 1.3 protocol implements a secure channel and is the most secure to our knowledge.

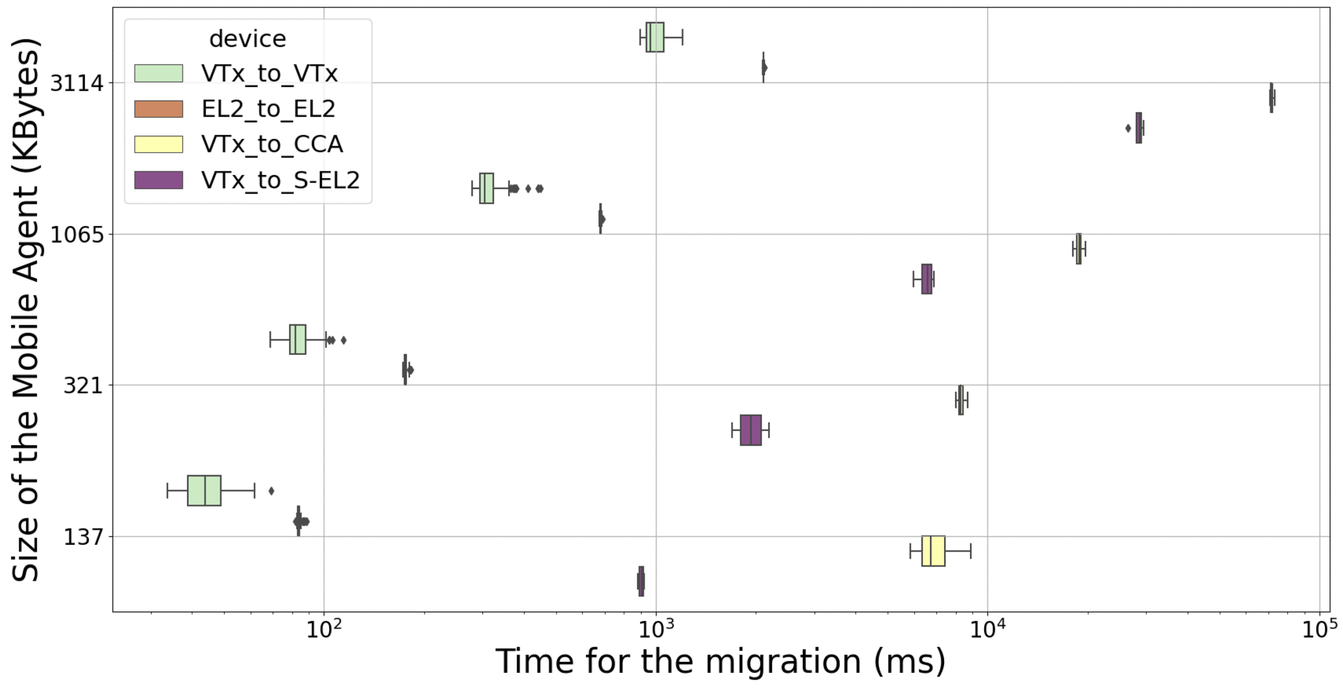
Problem: migration between SEs requires guarantees of endpoint integrity and trustworthiness. However, TLS 1.3 only provides protection for the data *in-transit* and authentication of the endpoints but it does not give any guarantee on the trustworthiness of the entities involved in the communication. As such, it leaves the door open to attacks from compromised endpoints.

Secure Migration on a Trusted Channel

Solution: A trusted channel adds remote attestation on top of a secure channel in order to establish trust into the endpoints of the communication.

Implementation: *Trusted Sockets Layer* (TSL) protocol is an example of such a trusted channel and it is used within the Huawei's secure enclave framework. The TSL extends the certificate-based authentication of TLS 1.3 with mutual attestation by using the callbacks provided by traditional TLS libraries. Hence, the TSL protocol gives the ability to securely migrate the mobile agent just on trusted platforms.





Architecture independent migrations

We implemented the Huawei's secure enclave framework on several architectures and secure enclave technologies like Intel VTx, ARM EL2, ARMv8.4 (S-EL2), and ARMv9 (CCA).

Results: In our benchmarks over a LAN network, migration time ranged from 44.57ms on powerful processors with Intel VTx up to 7041.84ms on emulated processors like ARMc9 CCA.

The project produced two papers that have been already published:
- Niemi, A., Pop, V. A. B., & Ekberg, J. E. (2021, November). Trusted Sockets Layer: A TLS 1.3 based trusted channel protocol. In Nordic Conference on Secure IT Systems (pp. 175-191). Springer, Cham.
- Pop, V. A. B., Niemi, A., Manea, V., Rusanen, A., & Ekberg, J. E. (2022, April). Towards securely migrating webassembly enclaves. In Proceedings of the 15th European Workshop on Systems Security (pp. 43-49).

Bogdan Pop, Valentin Manea, Arto Niemi, Antti Rusanen, Jan-Erik Ekberg
Huawei Technologies Oy Co. Ltd., Finland

HUAWEI