S-EL2

Secure Systems Group, Aalto University

Wojciech Geisler, Lachlan J. Gunn

Reliable migration of WebAssembly enclaves

- WebAssembly enclaves allow portable applications with strong sandboxing guarantees
- Migration must be atomic: exactly one node continues execution even under attack
- Fair exchange protocols ensure atomicity

WebAssembly (WASM)

- A portable instruction format.
- Code written in C, Rust, Go, etc.
- Designed for web: virtual machine provides highly secure sandbox

Enclave platform

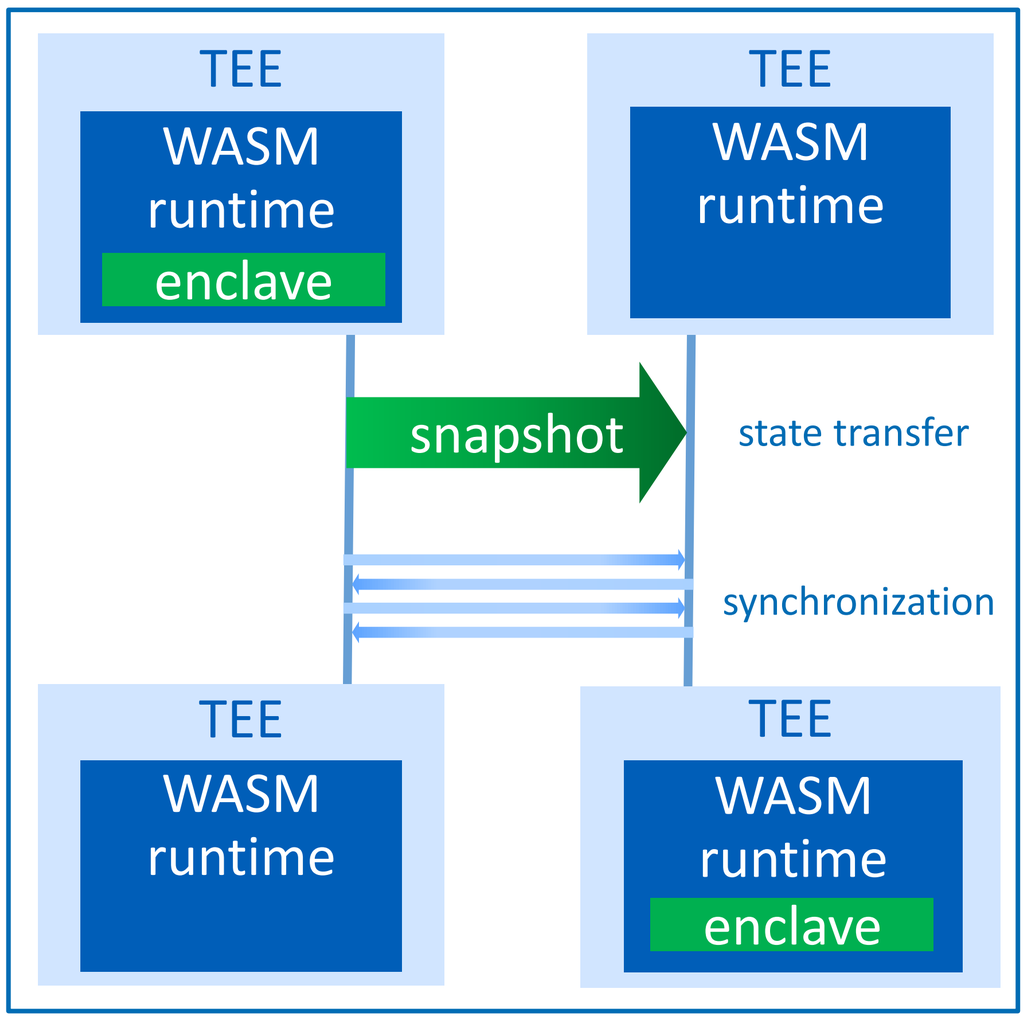
- WASM runtime running in TEE
- Platform supports remote attestation: certifying properties of an enclave
- Runtime migrates enclave between TEEs
- Problem: migration over insecure network

Objectives

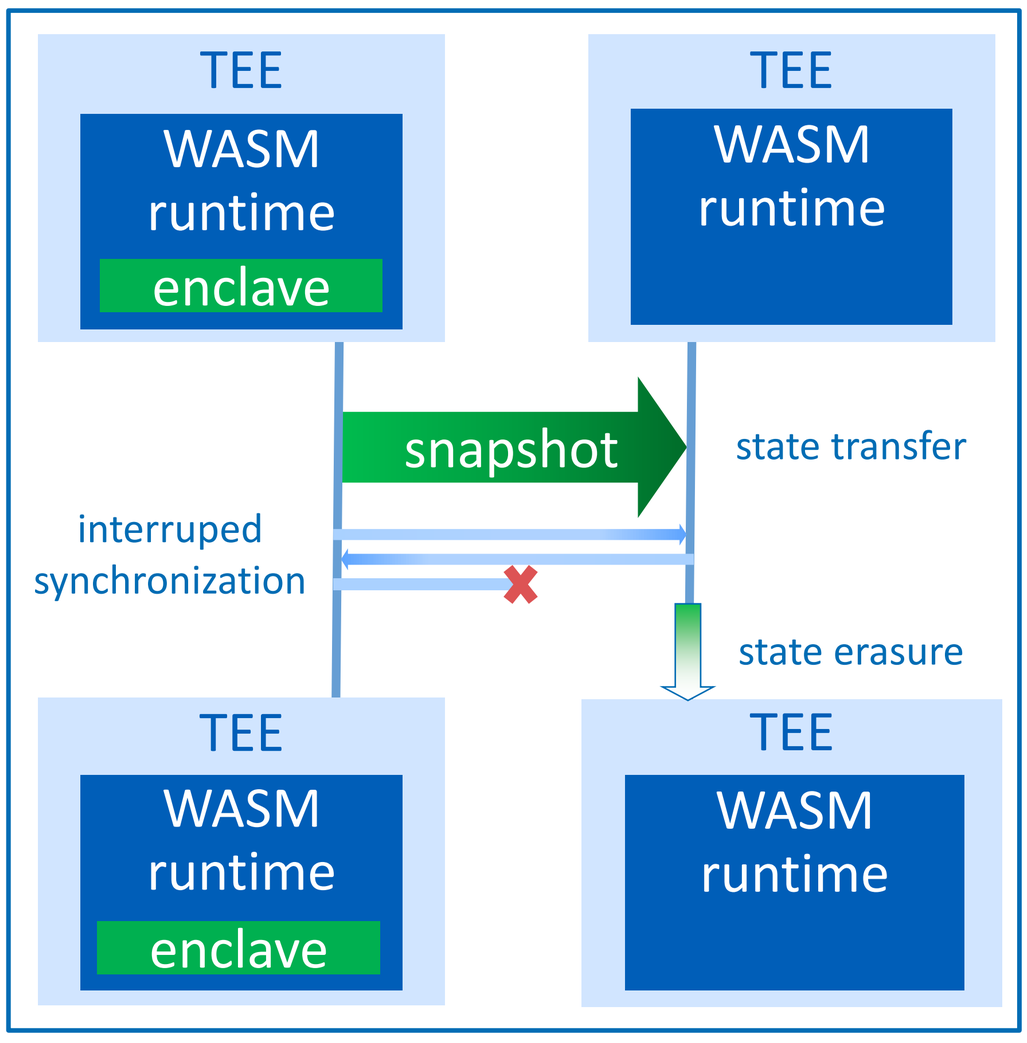
- authentication: migration target is always a trusted environment
- confidentiality: an attacker cannot learn enclave content
- reliability: migrating enclave can’t disappear
- non-duplication: enclave continues execution in only one place

Solution

- authentication: remote attestation
- confidentiality: TLS channel
- non-duplication: fair exchange protocol
- reliability: original node resumes execution if fair exchange ends in failure



successful migration



interrupted but correct migration

Aalto University

Acknowledgments

This work was funded by Huawei Technologies Oy.