ELASTIC Project

Secure Systems Group, Aalto University

Ghazal Shenavar, Xuan-Huy Ngo, Jose Luis Martin-Navarro, Lachlan J. Gunn

Contact: *{ghazal.shenavar, huy.ngo, jose.martinnavarro}@aalto.fi, lachlan@gunn.ee*

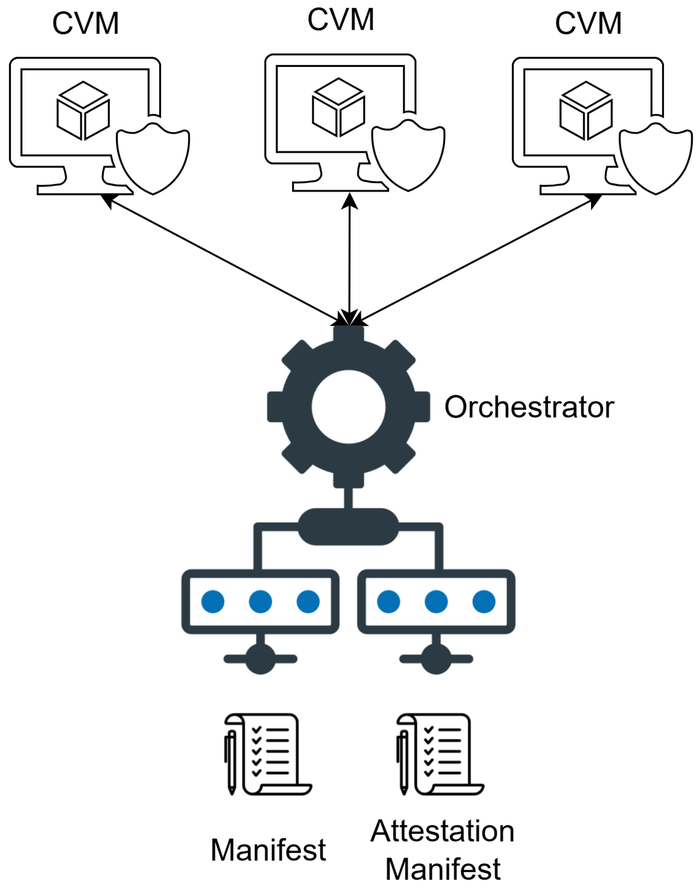
Attestation of Distributed Applications

Background

- Remote Attestation: a mechanism that allows one device to prove properties of itself to another
- Trusted Execution Environment (TEE): a secure and isolated area for authorized parties to process and execute confidential data

Problem

Current remote attestation mechanisms are limited to attesting monolithic applications that run within a single TEE

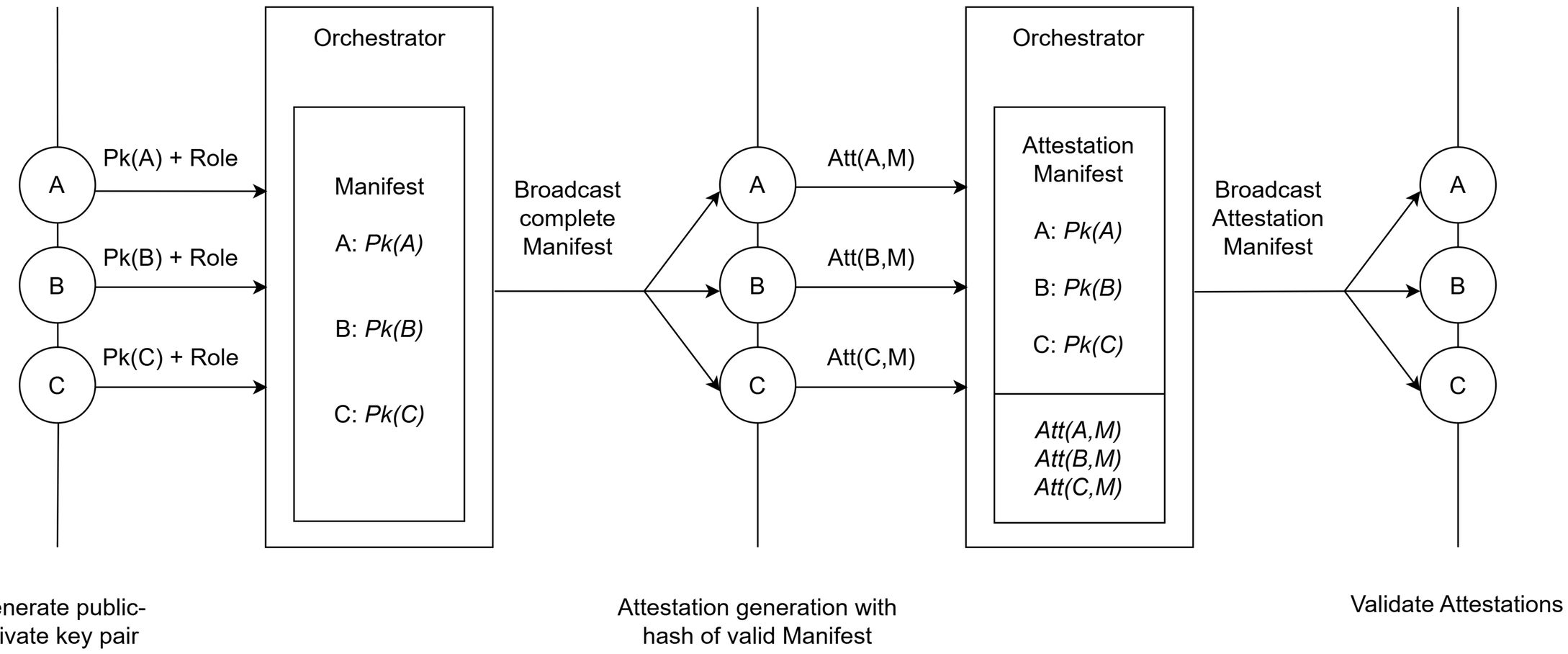


Solution

- Agree on identities of application components with consensus-like protocol
- Components attest their own identity and consensus result on individual machines
- Manifest + individual attestations attest whole application

Contributions

- A distributed application can attest itself as a single unit, ensuring all underlying components execute the right code and all configuration is correct
- Implementation with two TEEs (Intel TDX and SGX) demonstrates the practicality of the protocol



Aalto University

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS-JU. Neither the European Union nor the granting authority can be held responsible for them.