ELASTIC Project

Secure Systems Group, Aalto University

Kha-Luan Pham, Parsa Sadri Sinaki, Lachlan J. Gunn

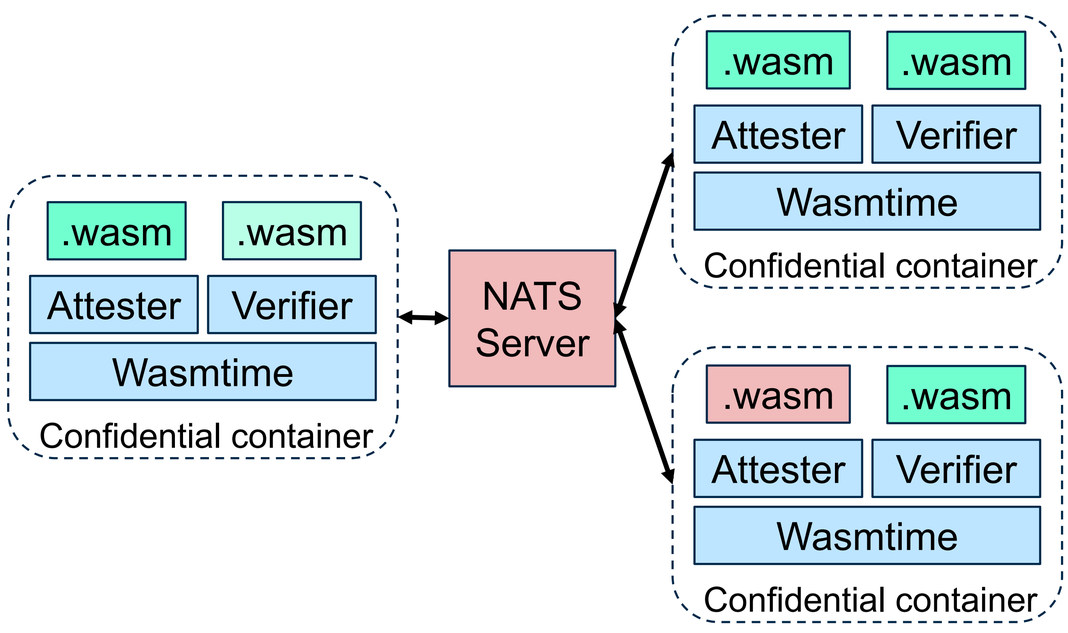
Secure, attested communication for serverless WebAssembly applications

Introduction

- The **WebAssembly (WASM)** component model defines interoperable software components using **Wasm Interface Type (WIT) interfaces**.
- **WIT interface** specifies exported and imported interface of a WASM component

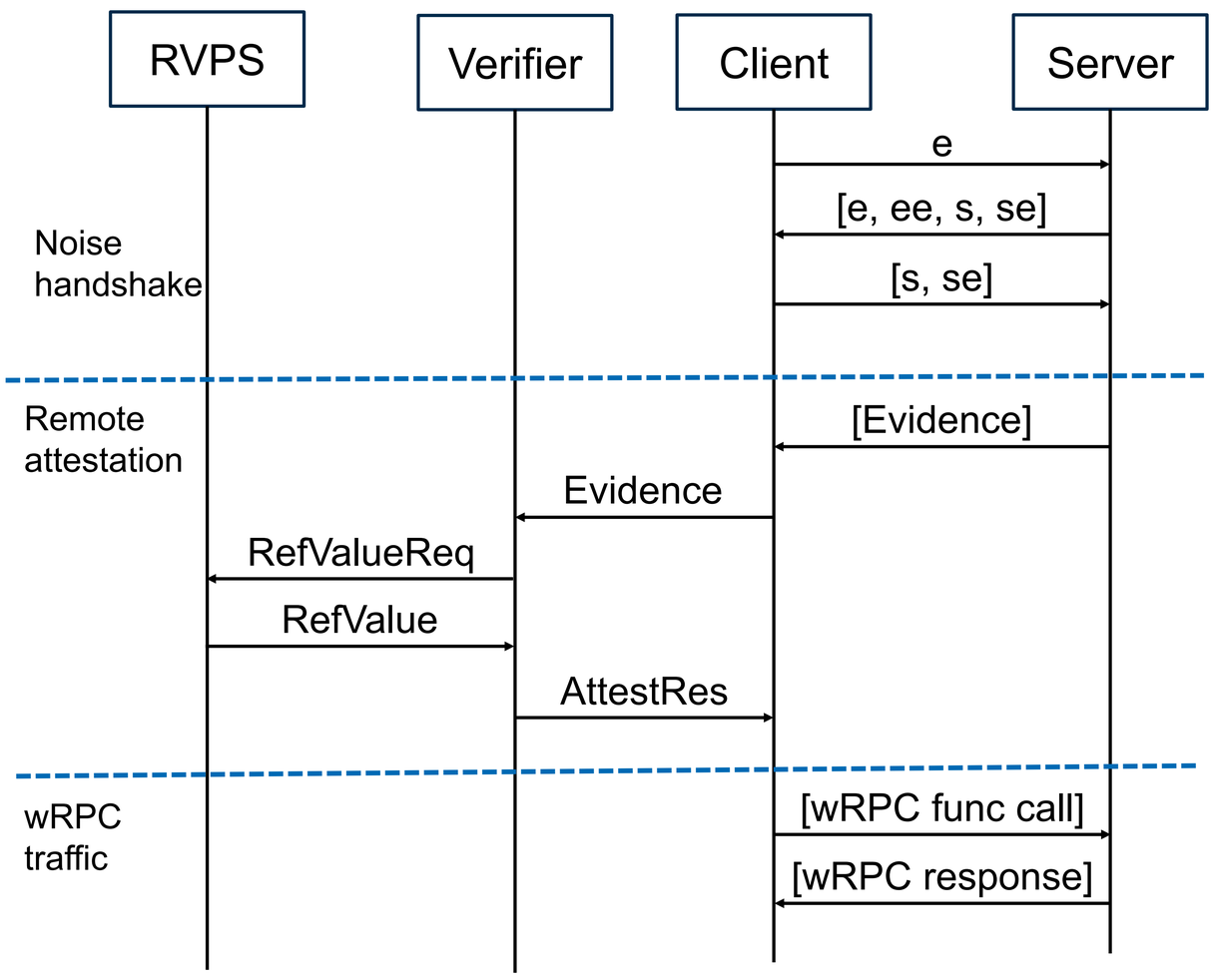
```
package demo:example;
world calculator-world {
    export calculator;
    interface calculator {
        add: func(a: u32, b: u32) → u32;
    }
}
```

- **wRPC** enables WASM components to connect over the network.



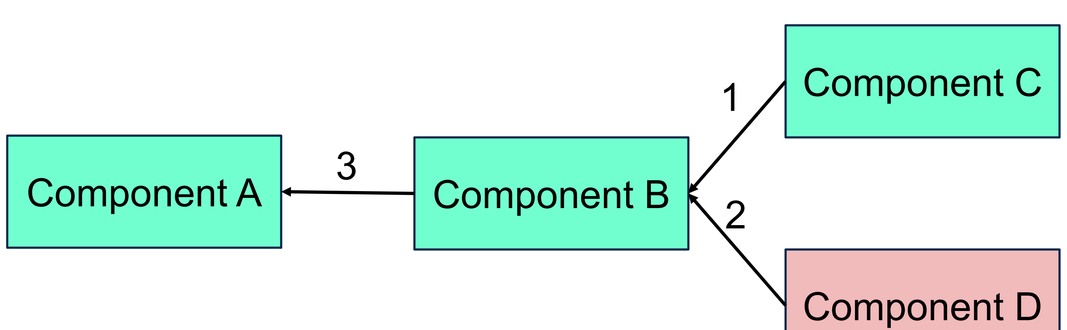
Solution

- Combine **remote attestation** with **Noise protocol**
- Bind the evidence with the active session with **transcript hash**
- A workload generates evidence if **all** dependencies are successfully attested



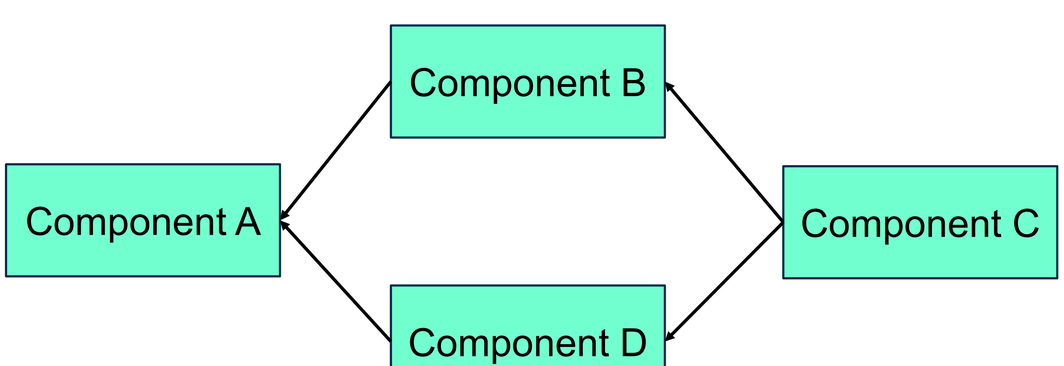
Problem

- How to verify which WASM component is at the other end of a wRPC connection before making wRPC call?
- How to ensure **end-to-end encryption** for wRPC traffic?
- How to extend remote attestation from individual workload to **dependency-aware trust establishment**?



Discussion

- How to handle **circular dependencies, diamond dependency**?
- **Component identity** related issue: component duplication?
- How to extend for **mutual attestation**?



Aalto University

Co-funded by the European Union

6GSNS

elastic

The ELASTIC project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe programme, Grant Agreement No. 101139067. 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.