# Capability-Based Efficient Data Transmission Mechanism for Serverless Computing

## Paper summary:

Existing isolation mechanisms for serverless functions are mainly VMs and containers, each which pros and cons regarding security guarantees and overheads. In this context, the paper proposes a security mechanism relying on capability-based data transmission. Building upon the CHERI capabilityies, the paper proposes to run multiple serverless functions in different compartments in a single address space while performing data transmission between compartments with zero-copy.

## Strengths:

- Good background section that concisely exposes the CHERI architecture and capability mechanism

## Weaknesses:

- While Section 2 provides a substantial background, it does not quite convince on the inefficiency of the existing capability-based communication mechanisms

## Comments to the authors:

- Given that a capability cannot be shared among multiple functions simultaneously (due to the sealing and revocation), doesn't this limit communication between multiple (more than 2) functions compared to shared memory, for example?
- What type is the SCST log? Is it a 4KB page?
- Section 3.3 stipulates that when the SCST log is full, addresses are flushed to the capability-ordered list, while Section 3.1 states that the monitor records the sender's shared capabilities in the SCST log. So, is the SCST log per shared capability? Or per function? Or unique for the whole system?
- Concerning the log backup ordered list, what is it used for? Does the monitor use it each time it traverses the SCST log (since it is a backup of the latter)? If so, what type is it? Is it optimized for memory scan upon revocation/sealing?
- In the *time measurement* description, it is unclear which methodology do you finally adopt? Do you use the `rdtime` instruction for all configurations? Or only for the CHERI-enabled one? For equity purposes, as you stated, why not use it for all configs?
- As a more general comment, I would recommend that the context and the problem in the introduction are more specifically restrained to data transmission which is really the scope of the paper. Because one might be confused when reading about the cost and lack of security guarantees of VMs and containers and then suddenly falling back to inter-function communication by passing hardware capabilities. I would suggest that the authors directly point out the problem of the function communication and heavy data transmission and therefore present the limitations of existing solutions more closely in this precise context. Otherwise, you may have compared your solution to VM-based isolation techniques.

## Is this paper thought provoking?

Strong but narrow appeal. Thought provoking only for people already working in this particular topic.

## Is this paper convincing?

Good. The evidence is not bullet-proof but is acceptable for papers in the area.

## Writting Quality

Well-written

## Merit

Accept