Joint work with Huawei

Deterministic use of ARMv8.5-MTE

How to use ARMv8.5-A Memory Tagging Extensions without random tagging?

The setting:

- ARMv8.5-MTE provides memory tagging that can be used to detect memory errors
- Randomly assigned 4-bit tags sufficient for bug detection in large scale testing

The problem:

- Probabilistic defenses are insufficient when an attack can be repeated (e.g., to attack physically accessible device)

Approach:

- Use static analysis to realize deterministic stack tagging scheme with hard guarantees
- Can completely protect *safe* variables by using MTE to isolate memory errors

Status:

- LLVM-based MTE-aware variable safety analysis and stack tagging for ARMv8.5-A

In progress