Towards Scalable SoC Security Validation
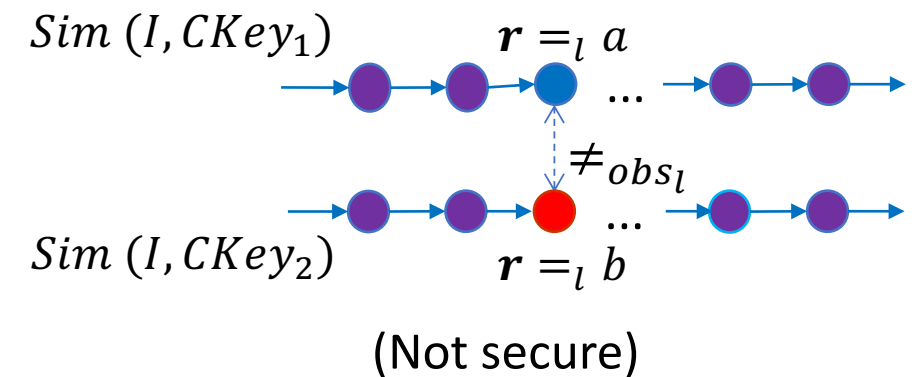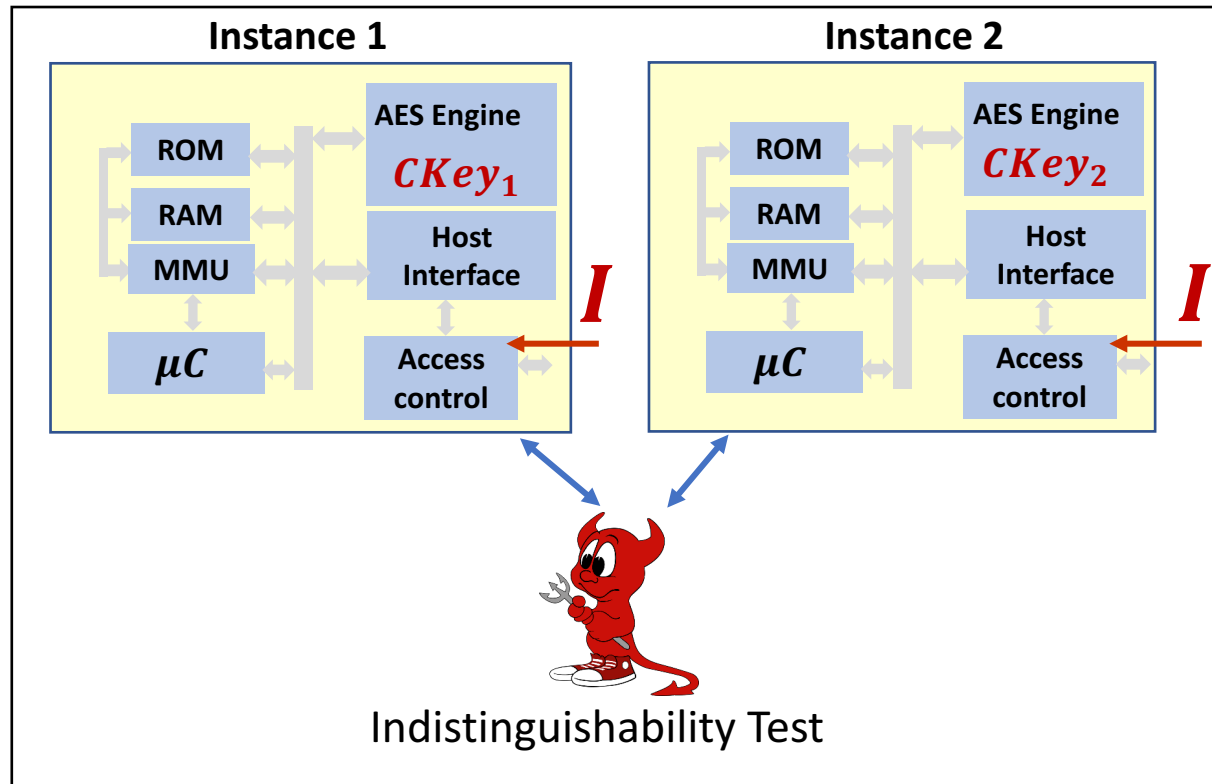
Sujit Kumar Muduli

Indian Institute of Technology, Kanpur

Objective

Proving confidentiality and integrity
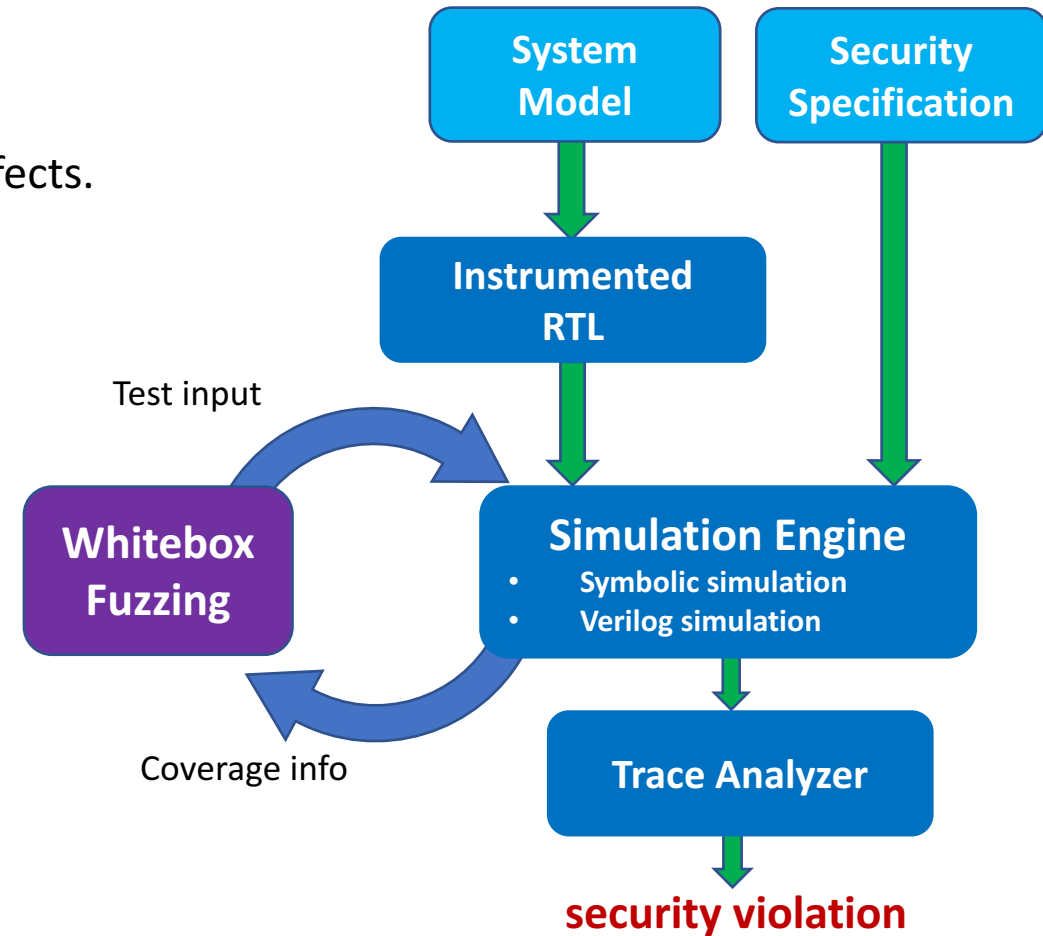
show execution traces are indistinguishable to untrusted entity

Goal : automated technique for finding 2-safety hyperproperty violations

Challenges

1. Specifying properties for end-to-end security.

2. Specification and Model must capture adversarial effects.

3. Scalability issue in verification process.

A semi-formal technique to find 2-safety violations