

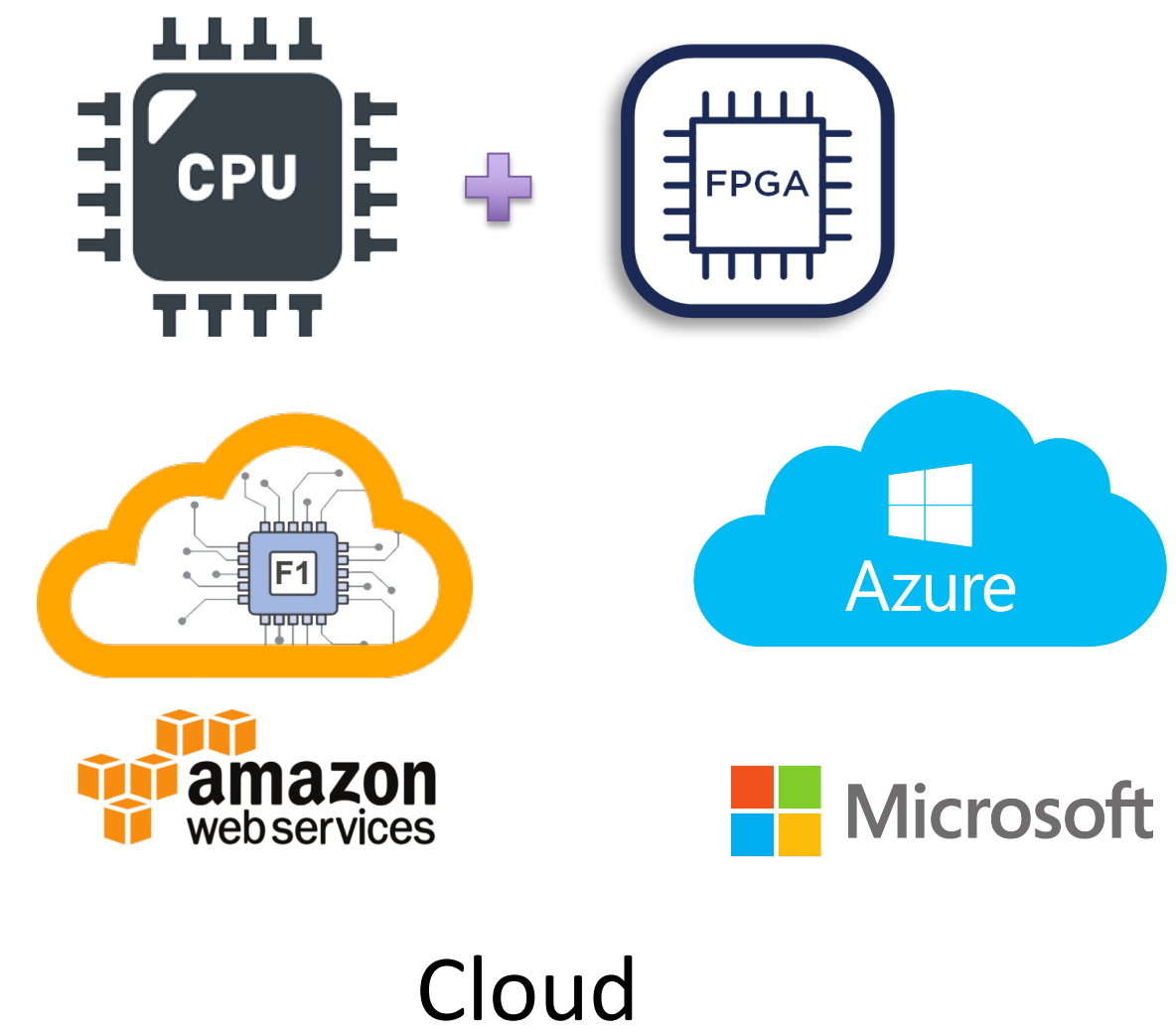
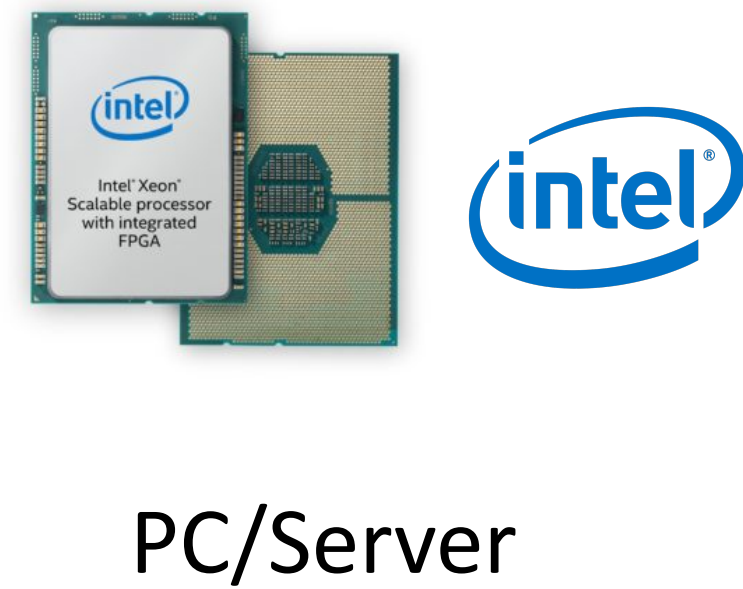
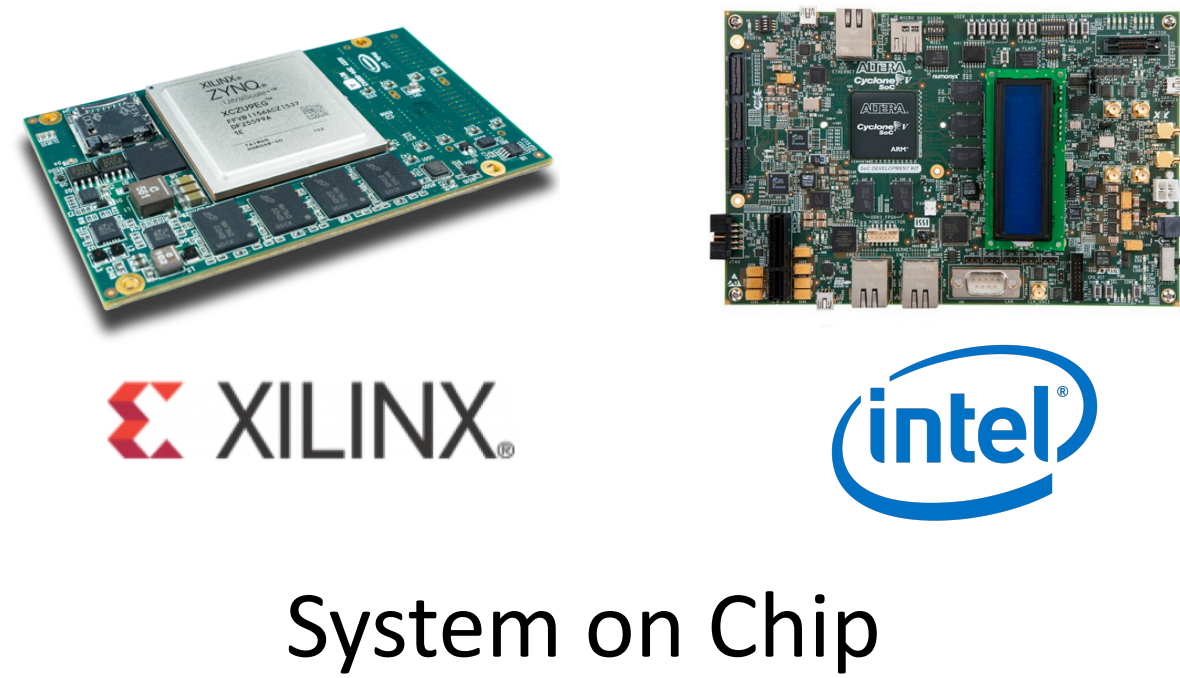
HISA: Hardware Isolation-based Secure Architecture for CPU-FPGA Heterogenous Systems



PI: Sheng Wei; Department of ECE; Rutgers University

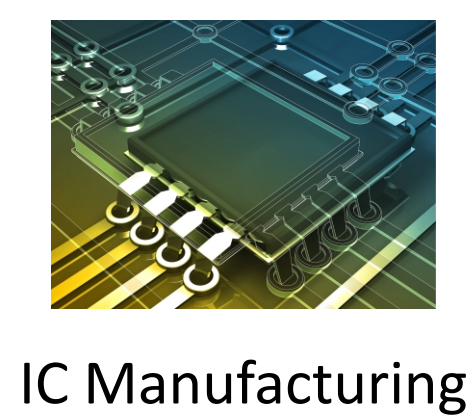
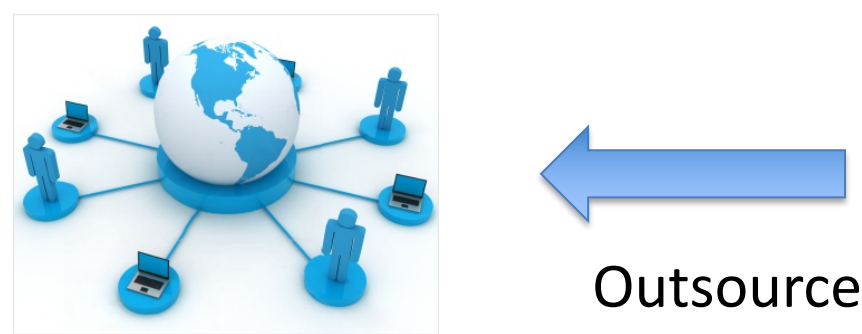
Project URL: <https://github.com/hwsel/hisa>

CPU-FPGA Heterogenous System

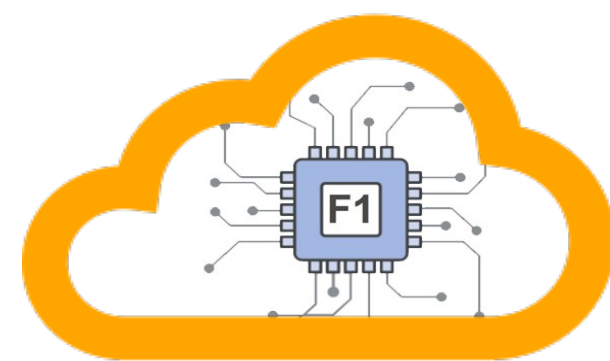


Problem Space

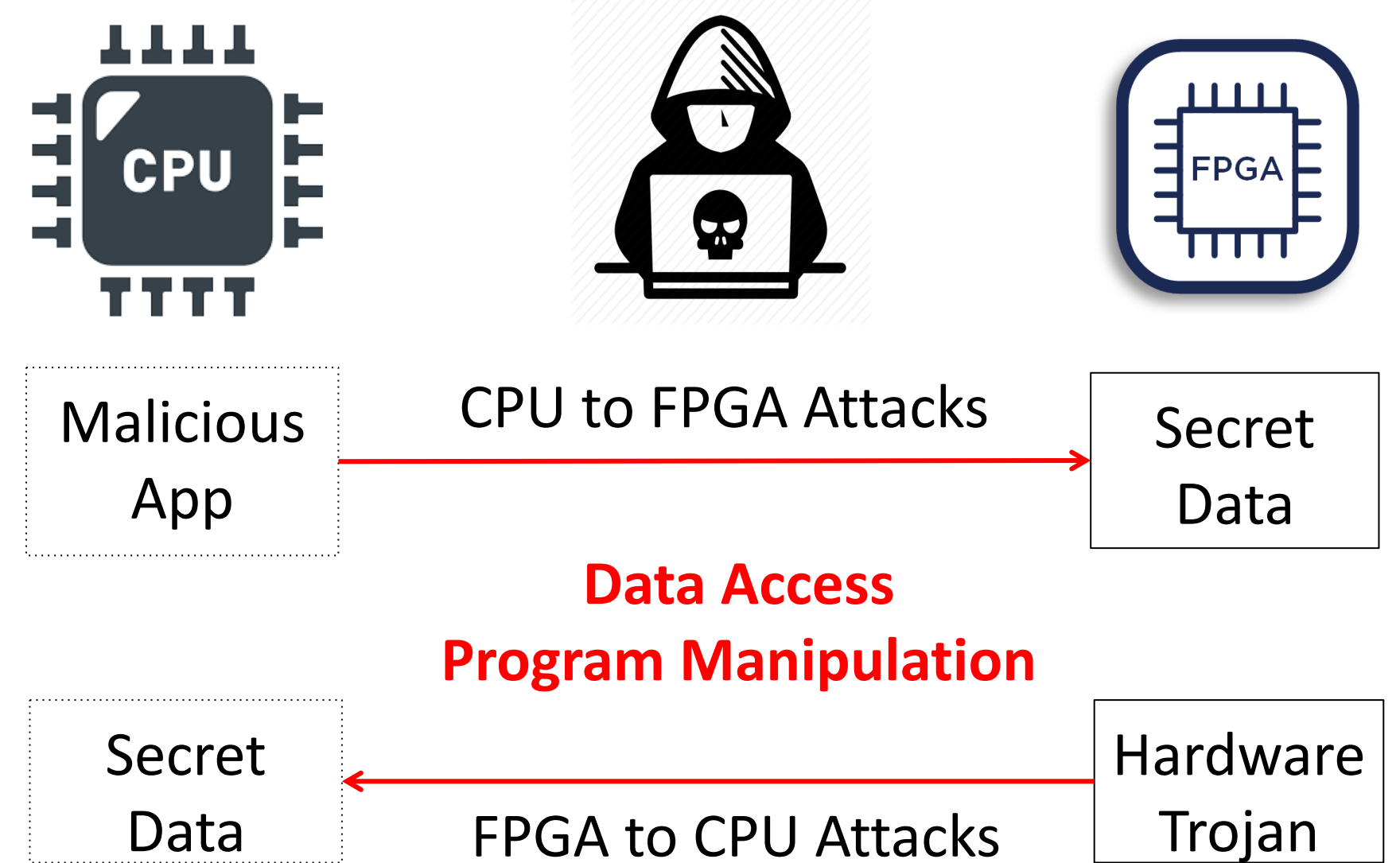
Traditional Hardware Security



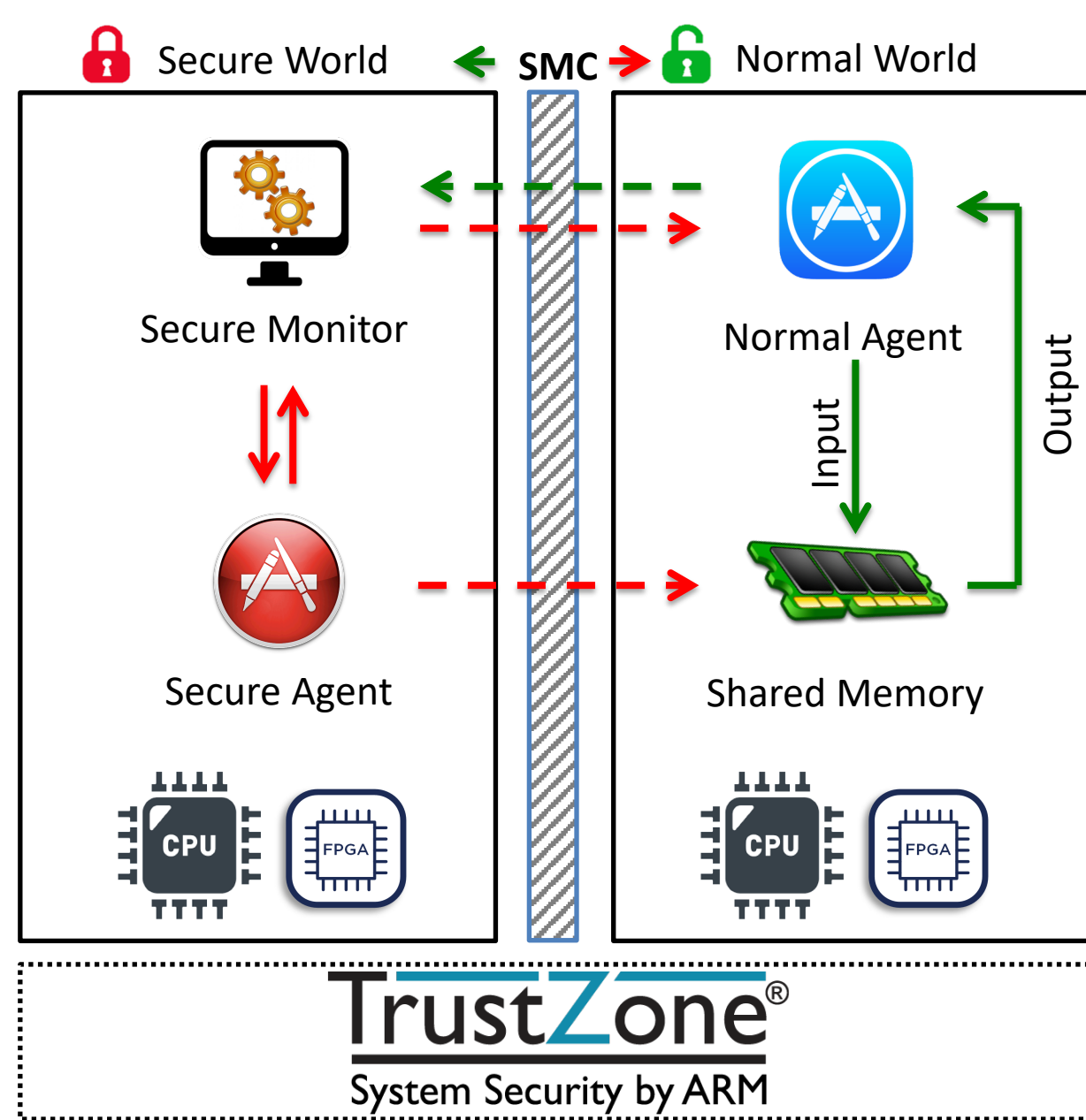
This Research



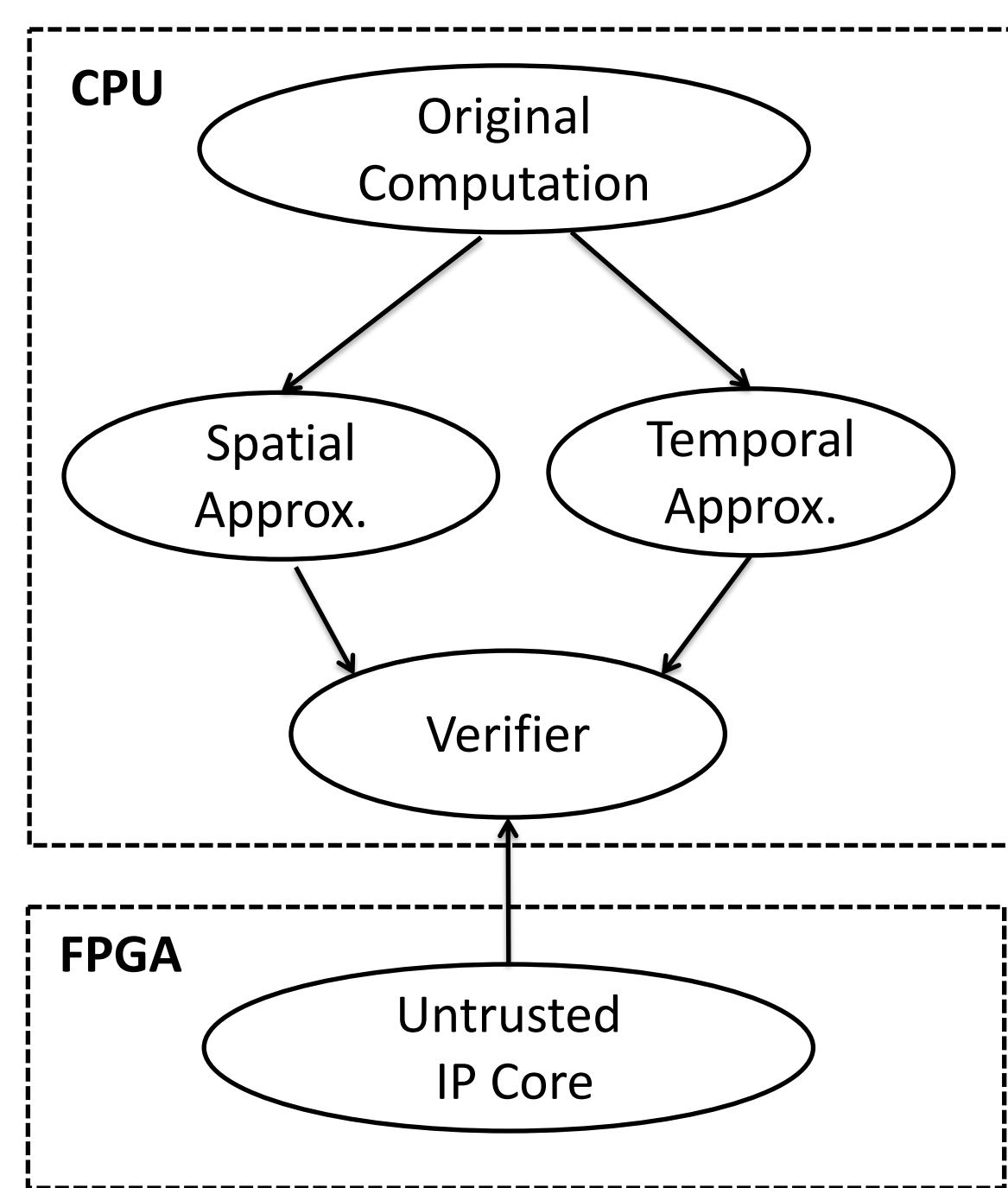
CPU-FPGA Security Challenges



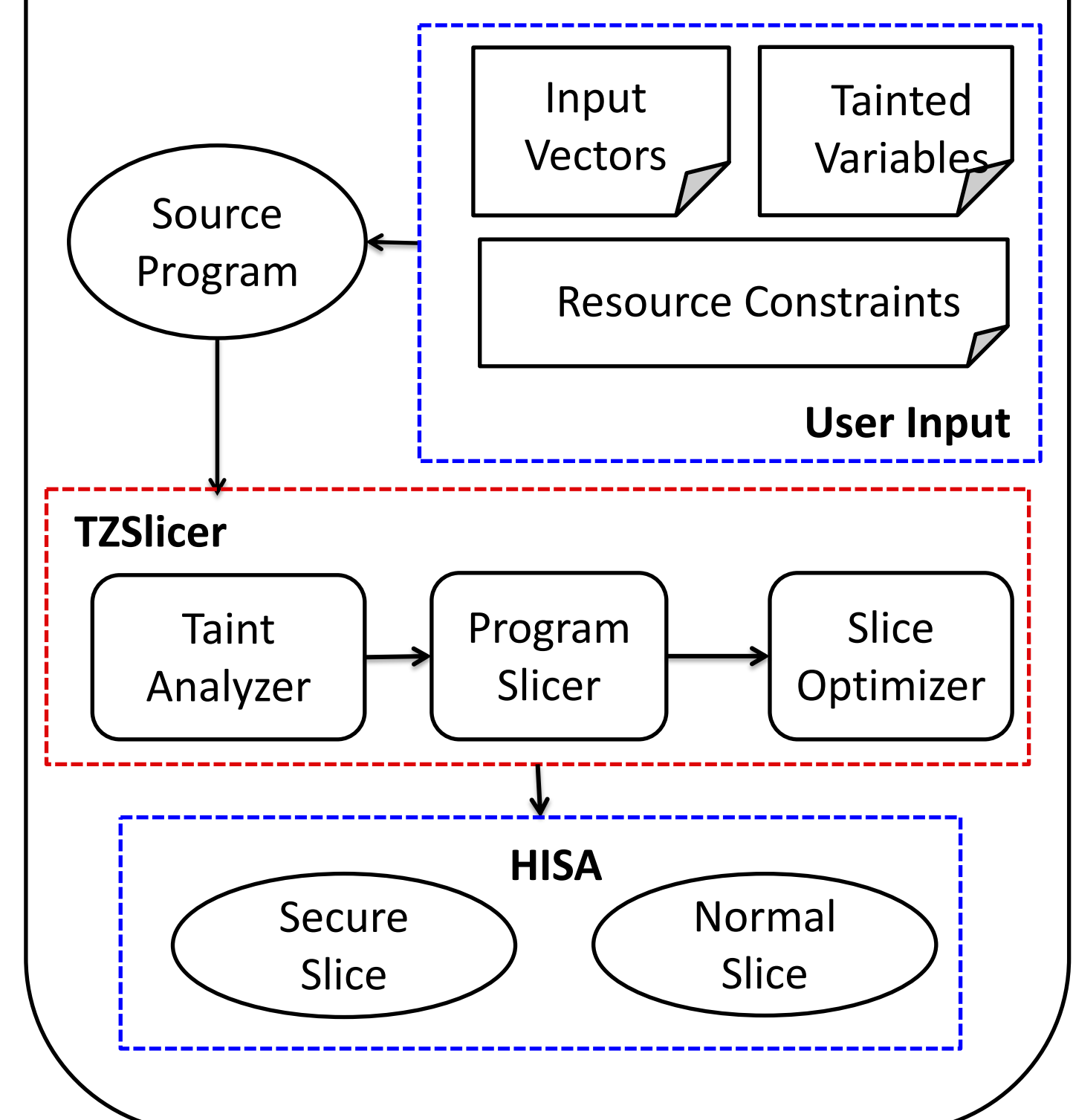
HISA: Build the Fence



ApproVer: Approximate Verification

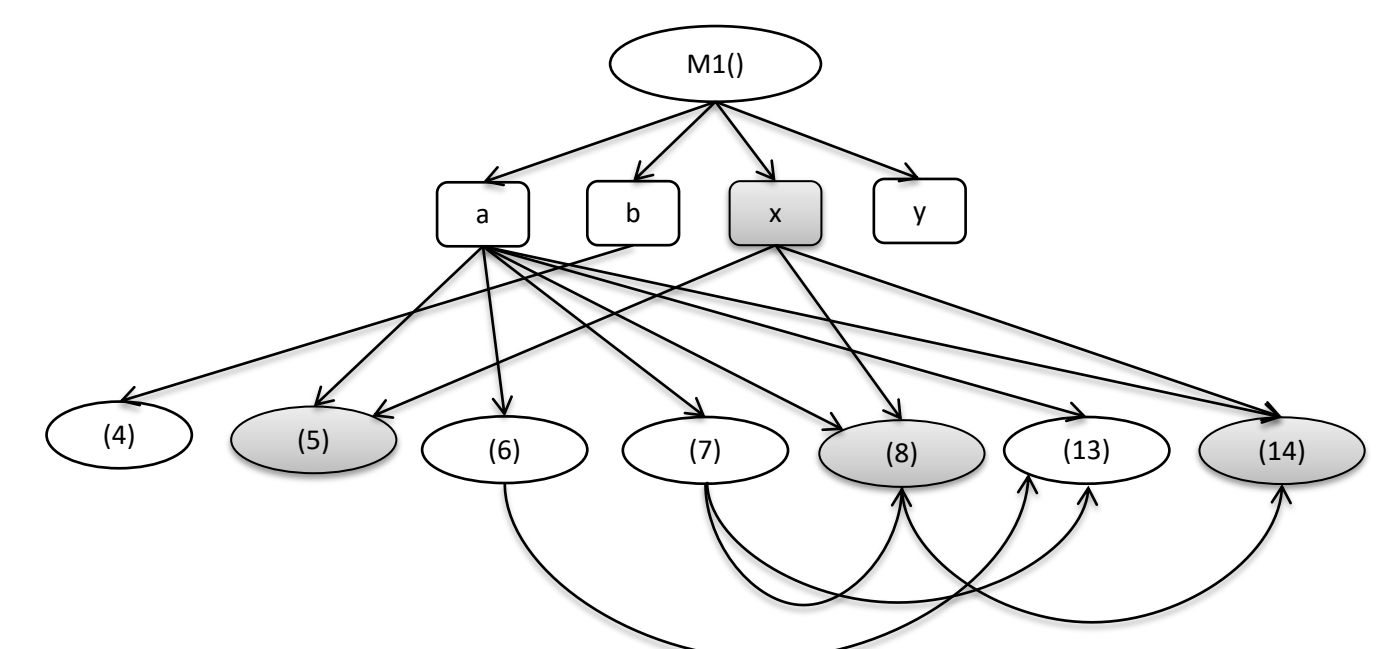


TZSlicer: Easy Programming



Security Performance Usability

	Spatial Defense	Temporal Defense
Baseline	36	1
NoTrojan	31.84 (-11.56%)	1.02 (+2.00%)
STrojan	0 (-100%)	0 (-100%)



Broader Impact: Society

- Cloud service providers
- Accelerator designers
- End users requiring secure high performance computing

Broader Impact: Education

- Hardware security course at Rutgers University
- Two female PhD students focusing on this research

Broader Impact: Applications

- Secure multimedia systems
- Secure AI/machine learning
- Secure scientific computing

