# Security of Heterogeneous CPU-FPGA Systems

PI: Sheng Wei (sheng.wei@rutgers.edu)

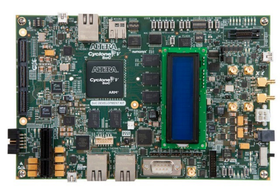
Department of ECE, Rutgers University

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

## CPU-FPGA Heterogenous System

XILINX

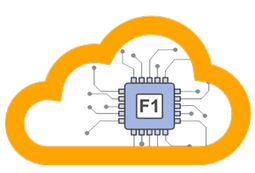
System on Chip



intel


intel

PC/Server




amazon web services

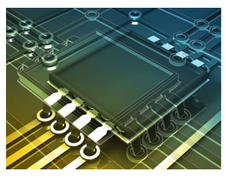

Microsoft

Cloud

## Problem Space

Traditional Hardware Security

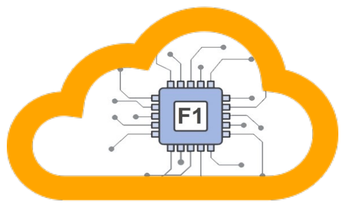
Outsource



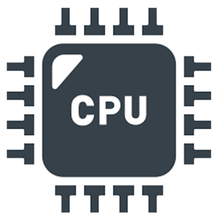
IC Manufacturing

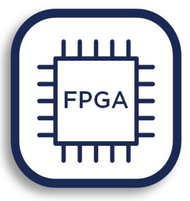
This Research

Crowdsource




## CPU-FPGA Security Challenges




Malicious App

CPU to FPGA Attacks

Secret Data

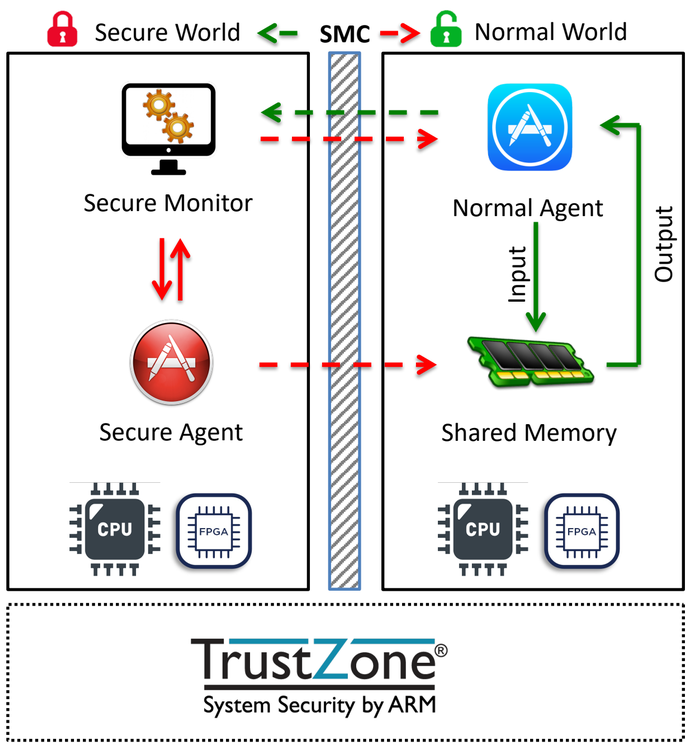
**Confidentiality**
**Integrity**

Secret Data

FPGA to CPU Attacks

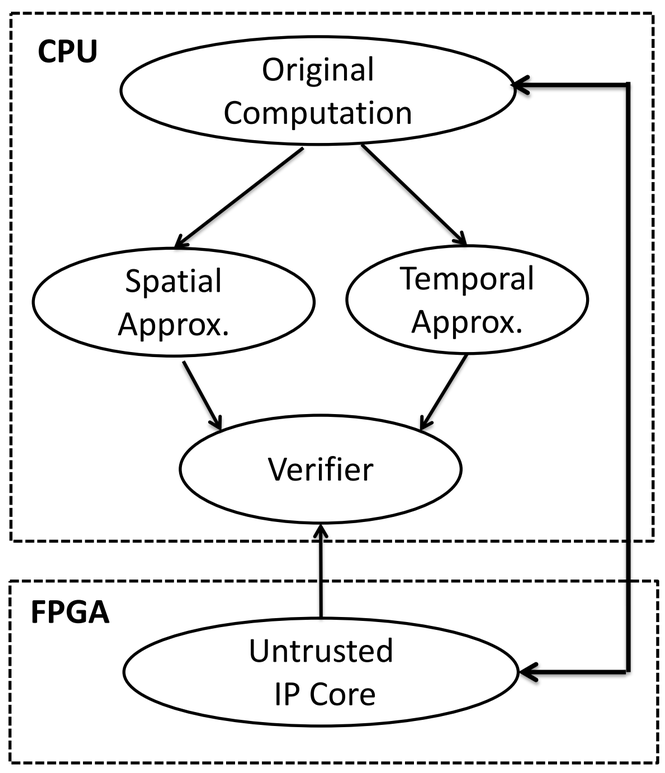
Hardware Trojan

## Build the CPU-FPGA Fence



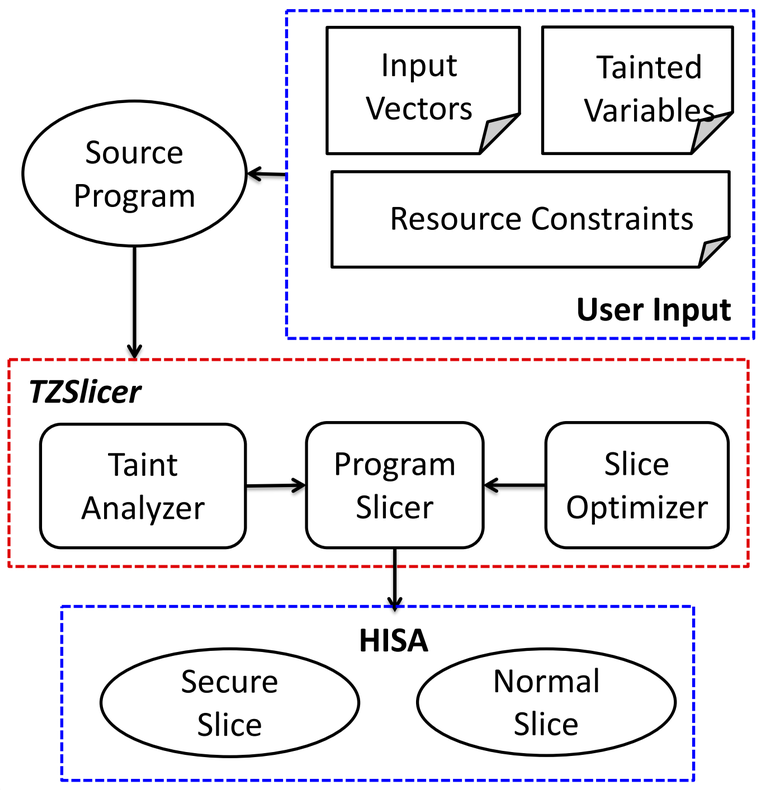

***HISA*** [ICCAD'18]

## ***ApproVer***: Approximate Verification



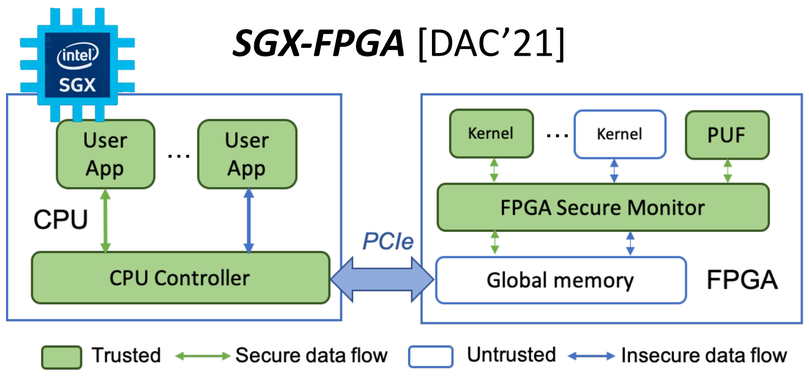

[AsianHOST'19]

## ***TZSlicer***: Easy Programming

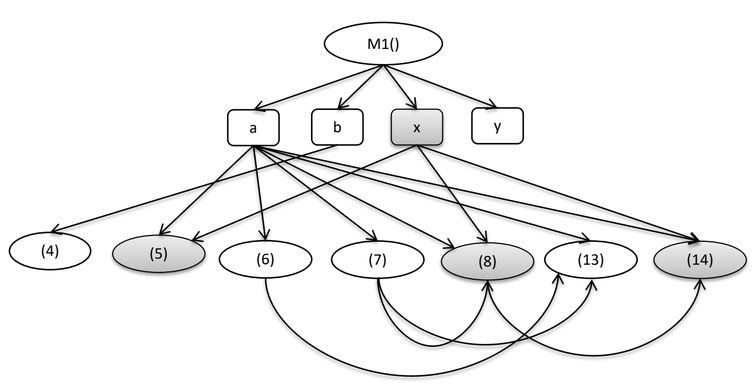



[HOST'18]

## ***SGX-FPGA*** [DAC'21]




| | 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
- 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