The Center for Cyber Defenders

Expanding computer security knowledge

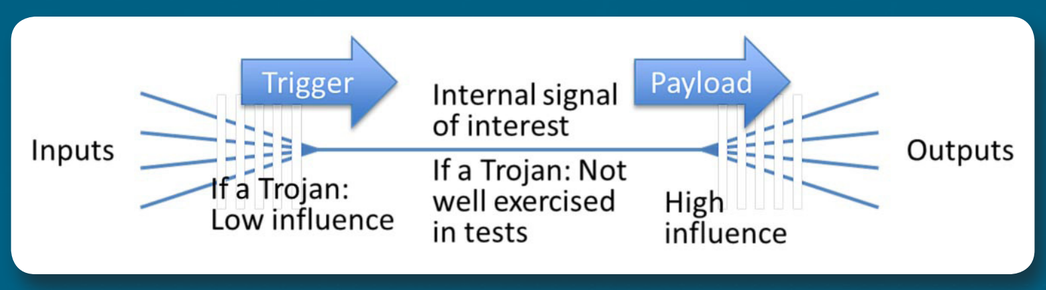
# FPGA Trust and Vulnerability Assessment using Network Criticality Metrics

Megan Boscarillo, University of Tulsa;
Zachary Silva, Rose-Hulman Institute of Technology

**Project Mentor: Vivian G. Kammler, Org. 5645**

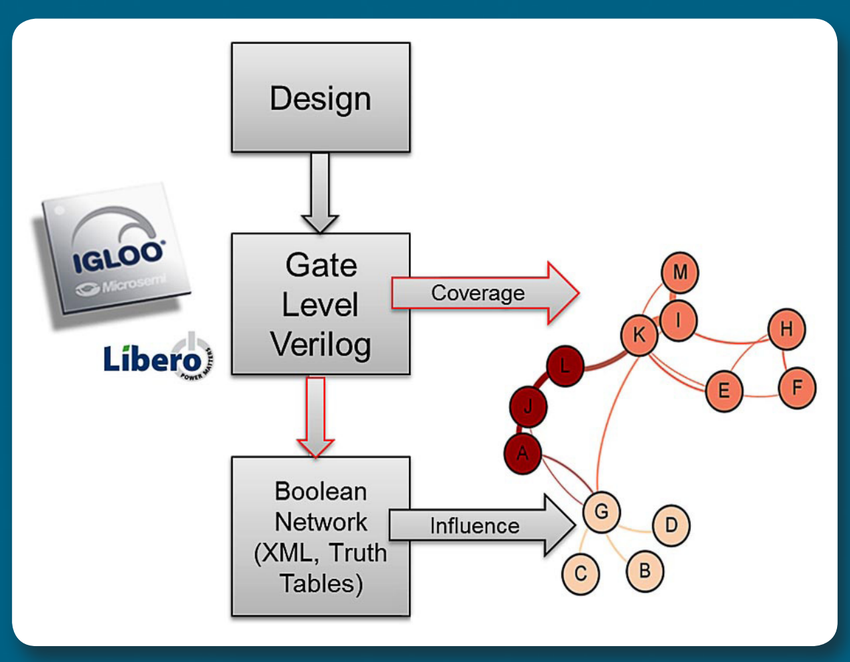
## Problem Statement:

Traditionally trusted hardware has recently been called into question as attackers aim to make stealthy modifications  to integrated circuits. These modifications are designed to both evade detection and trigger an attack using obscure, untested input. Hence, diminishing options for trusted manufacturing cause a major security concern and metrics to engineer trust into hardware using untrusted design tools are needed, but do not exists.



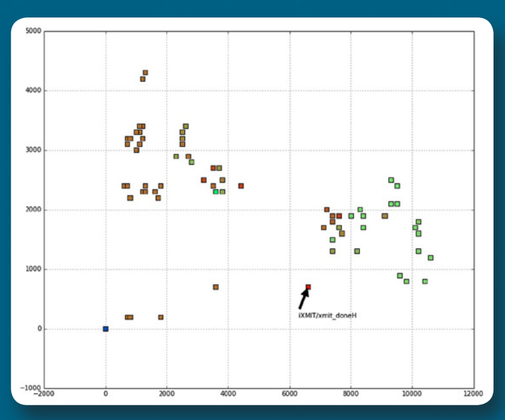

## Objective and Approach:

- Heat maps: Using synthesized output of FPGA design tools we combined influence and coverage to create a heat maps that identify areas that might harbor Trojans or other vulnerabilities.
- Equivalence check: Formal equivalence checking is a mathematical technique to prove that two representations of a logic circuit exhibit exactly the same functional behavior. Formal equivalence checking will ensure that no unexpected logic was inserted into the design or no intended logic was removed from it.




## Results:

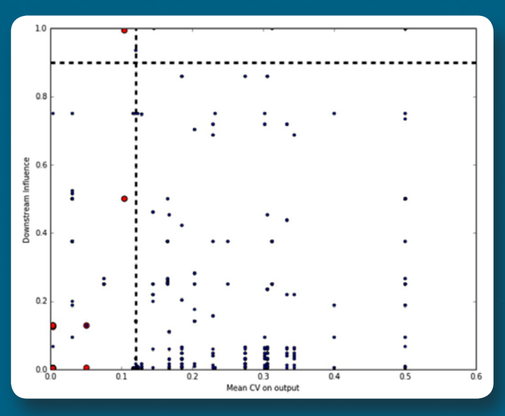
T-900 Heat map:




trust-HUB

*Using a heat metric where red indicates a node with high influence and a low control value*

T-900 Trojan Influence Plot:




*Note: Red nodes on influence plot corresponds to the red nodes in the heat map.*

Equivalency Checking:

Reference (Trojan free) output

```
-R- Outputs: HOLD= 33
-R- States:  HOLD=586
-R- The designs are equivalent.
```

Trojan introduced output:

```
-R- Outputs: HOLD= 33
-R- States:  HOLD=550 FAIL=32
-R- The designs are not equivalent
```

## Impact and Benefits:

**Sandia**

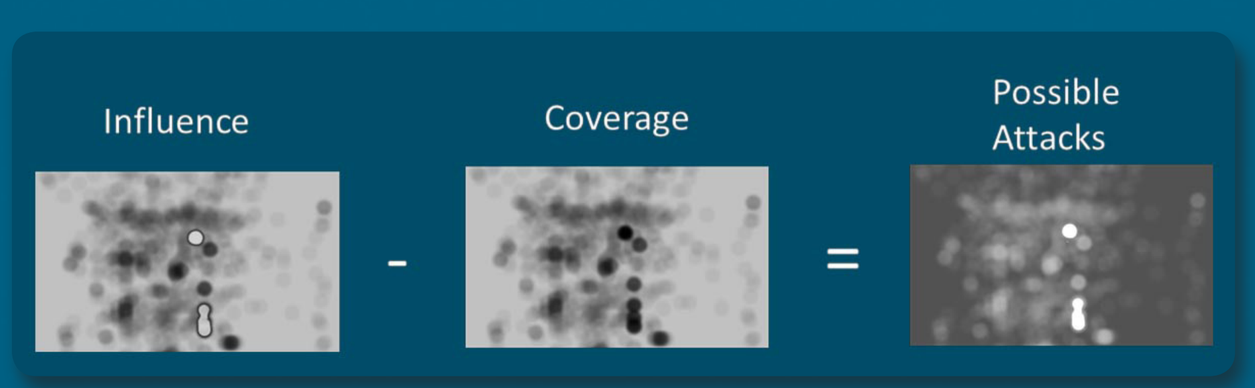
- Design of high consequence ICs: Risk mitigation for use of EDA tools. Engineered robustness of designs.
- Verification of high consequence ICs: Trust-related coverage metrics for achieving completeness. Independent validation of efforts to achieve high quality functional tests.

**USG**

- Risk mitigated use of FPGAs, and ASICs, using untrusted design tools

**Commercial**

- FPGA/EDA vendor incentives to assist in development of trust solutions




Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-6805D.