A Joint Venture of TÜV Austria and TU Wien

Safety and Security in Industry Research Lab „SafeSecLab“

#SafeSecLab

PhD7: Design-time hardware-security verification

Attackers can leverage the unsecure SoC supply chain in order to introduce malicious functionality (hardware Trojans) in hardware designs. Thus, critical devices can be subjected to possible attacks as DoS, sensitive information leakage, etc. The digitalization of the industry provides a profitable attack surface for such scenario.

Our goal is to develop a tool that detects such malicious functionality at the design time.

Sofia Maragkou

Education

Technical University of Crete - School of Electrical and Computer Engineering

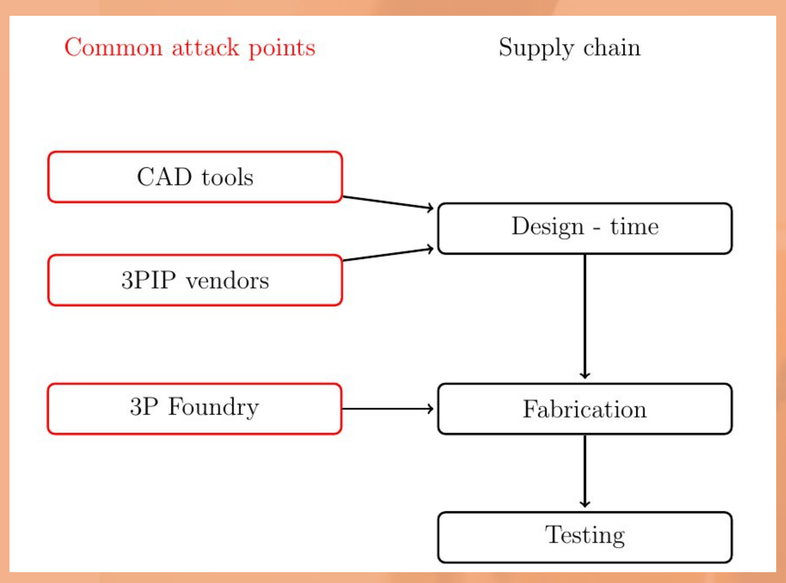
Experience

Project assistant at Fraunhofer Institute

Contact: sofia.maragkou@tuwien.ac.at

Motivation

SoC supply chain



Why verification at the design time?

Disadvantages

- Still entry points in the design process
- The verification of the final product is not guaranteed

Advantages

- Post-fabrication attacks are very expensive
- Attacks at design time can affect more designs
- If a Trojan is found after fabrication, recovery is very expensive

Challenges of the current market

1. M2M communication
   - Malicious functionality (e.g. Hardware Trojans) included in the chips can leak sensitive information such as authentication keys.
   - Relevant for TTTech Industrial Automation AG

2. Critical parts are outsourced without verification after the purchase
   - Such components purchased from third party vendors can hide malicious functionality (e.g. Hardware Trojans)
   - Relevant for Frequentis AG

3. Digital transformation
   - Retrofitting on legacy systems could create security breach which malicious functionality could take advantage of
   - Relevant for TTTech Industrial Automation AG

Picture by Michal Jarmoluk

Project goals

1. Identification of HW authentication methods
   - Challenge 2
2. Recognition of HW Trojan patterns
   - Challenge 1
3. Prototype a (semi-)automatic detection tool
   - Challenge 1
4. Identification of unwanted communication via hardware backdoors
   - Challenge 1
5. Investigation on protective measures against HW Trojans
   - Challenge 1,2

Supervisor
Axel Jantsch (TU Wien)
Contact person
Christoph Schwald (TÜV)

Current results

- The SoA of hardware design authentication methods has been defined

The SoA of communication means for hardware Trojans has been analyzed

Expected results in 2022

- Specify the threat model for hardware Trojans
- Define use case
- Define the concept and method of verification

Upcoming steps

- Implementation of the concept
- Implementation of the method and the algorithm for hardware Trojan identification
- Tool validation
- Draft catalogue of countermeasures