04 Hardware Trojans

Engr 399/599: Hardware Security

Grant Skipper, Ph.D.
Indiana University

Adapted from: Mark Tehranipoor of
University of Florida

Agenda

- Review some of last class.
- Deep(ish) Dive into DES mechanics
- Start HT Unit.
- Next week - first project assigned (on HTs!)

SIDE QUEST: CWEs

- Common Weakness Enumeration (CWE)
  - produced and maintained by MITRE through public process (similar in vein to CVEs).

- Unlike CVEs, CWEs are not focused on identifying specific VULNERABILITIES - instead categorizes WEAKNESSES.

- Why do we care about the CWE system?

- What problems does the CWE system have?

https://cwe.mitre.org/data/definitions/1194.html

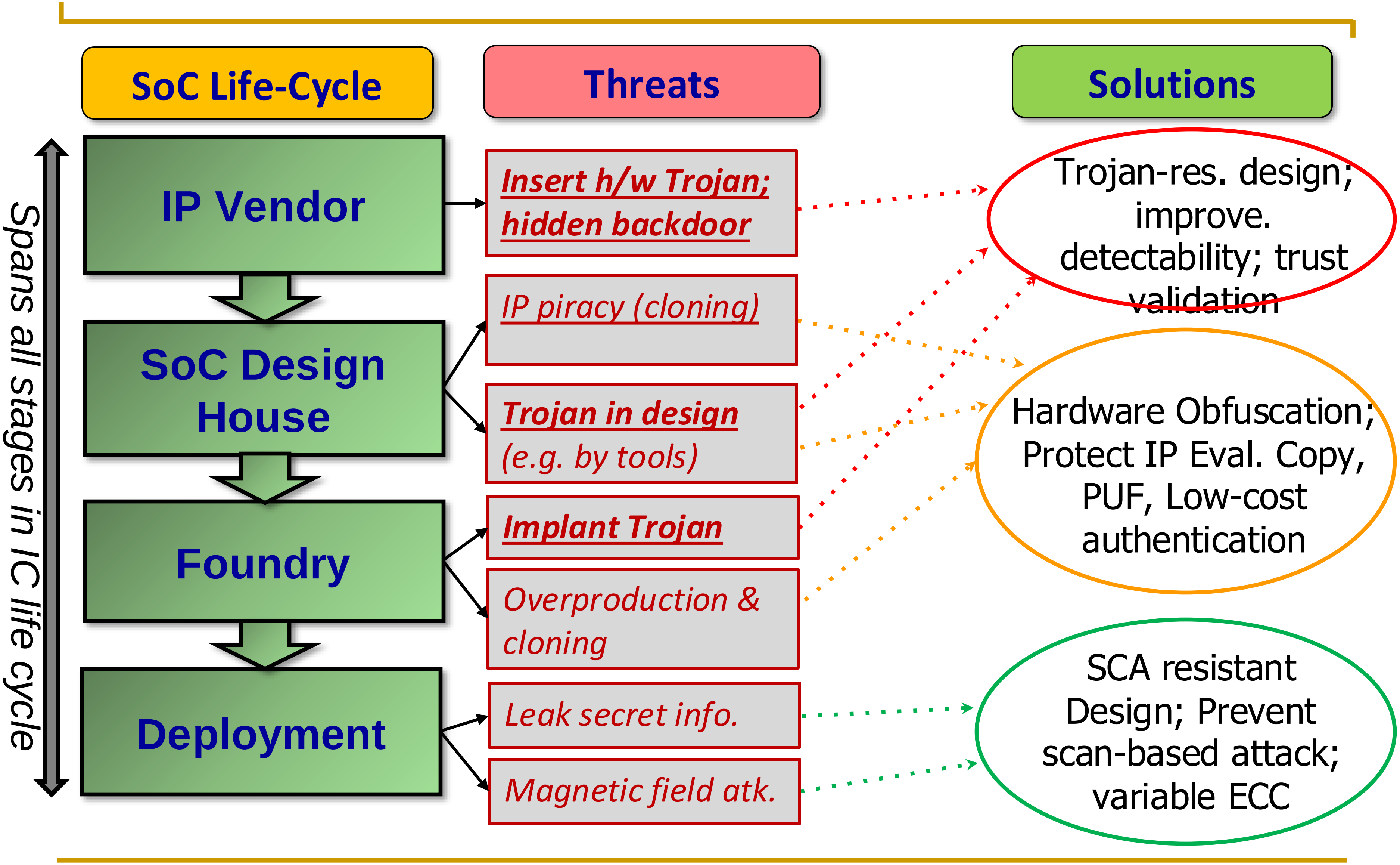
What is Hardware Trojan?

- **Hardware Trojan:**
  - A malicious addition or modification to the existing circuit elements.
- **What hardware Trojans can do?**
  - Change the functionality
  - Reduce the reliability
  - Leak valuable information

ANYTHING To ACHIEVE AN <u>OBJECTIVE</u>

- **Applications that are likely to be targets for attackers**
  - Military applications
  - Aerospace applications
  - Civilian security-critical applications
  - Financial applications
  - Transportation security
  - IoT devices
  - Commercial devices
  - More

Threats



SoC Life-Cycle

Threats

Solutions

Spans all stages in IC life cycle

IP Vendor

SoC Design House

Foundry

Deployment

Insert h/w Trojan; hidden backdoor

IP piracy (cloning)

Trojan in design
(e.g. by tools)

Implant Trojan

Overproduction & cloning

Leak secret info.

Magnetic field atk.

Trojan-res. design; improve. detectability; trust validation

Hardware Obfuscation; Protect IP Eval. Copy, PUF, Low-cost authentication

SCA resistant Design; Prevent scan-based attack; variable ECC

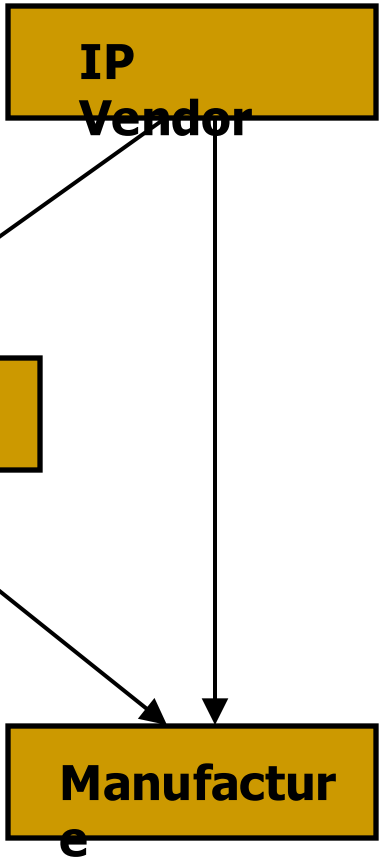
IC/IP Trust Problem

- Chip design and fabrication has become increasingly vulnerable to malicious activities and alterations with globalization.

- **IP Vendor and System Integrator:**
  - IP vendor may place a Trojan in the IP
  - *IP Trust problem*

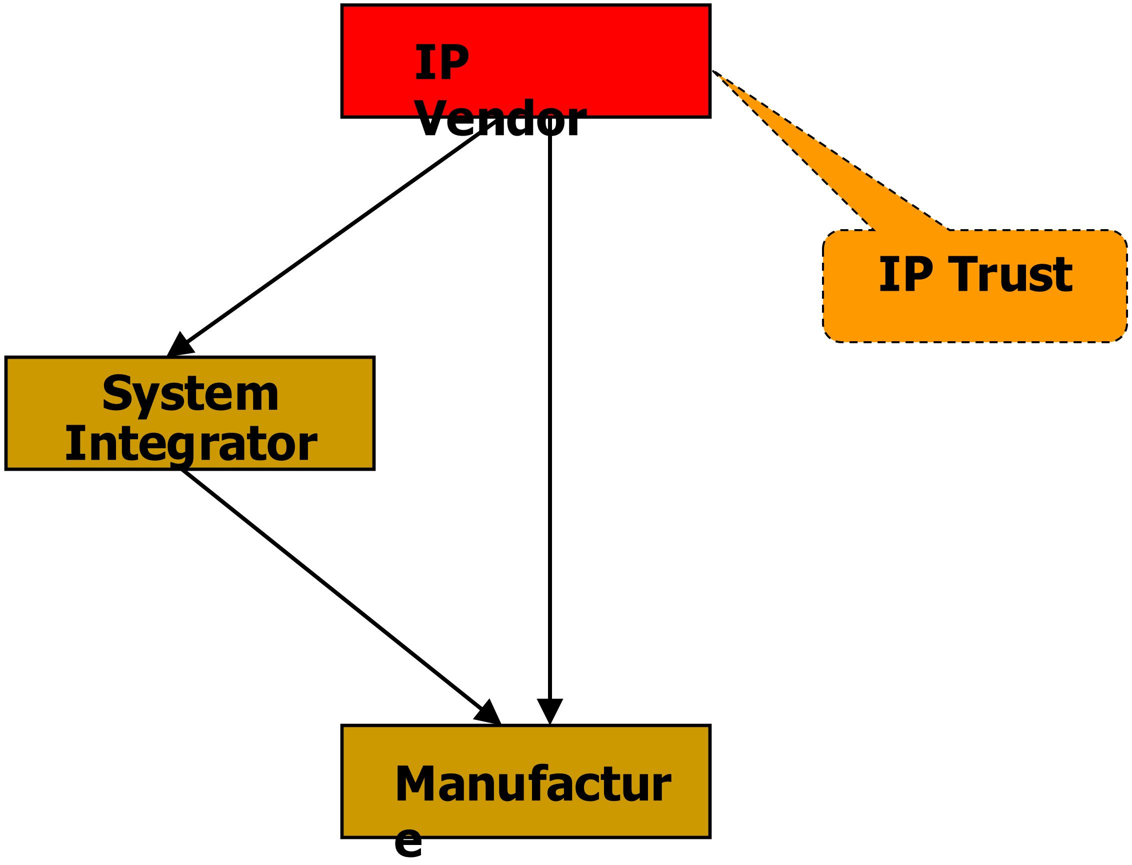
- **Designer and Foundry:**
  - Foundry may place a Trojan in the layout design.
  - *IC Trust problem*

Hardware Trojan Threat



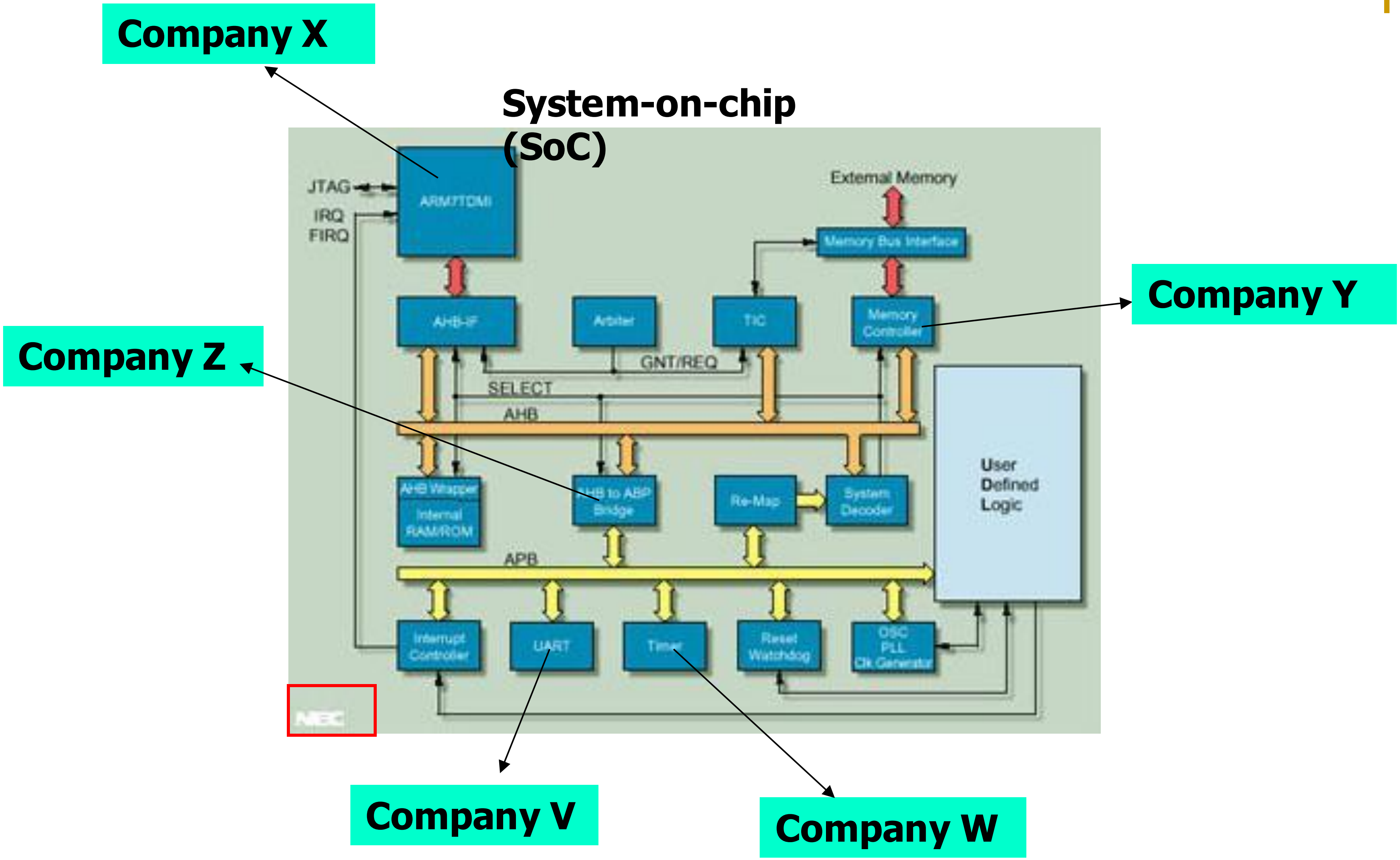
Any of these steps can be untrusted

Hardware Trojan Threat



🟥 Untrusted

Issues with Third IP Design



Company X

System-on-chip (SoC)

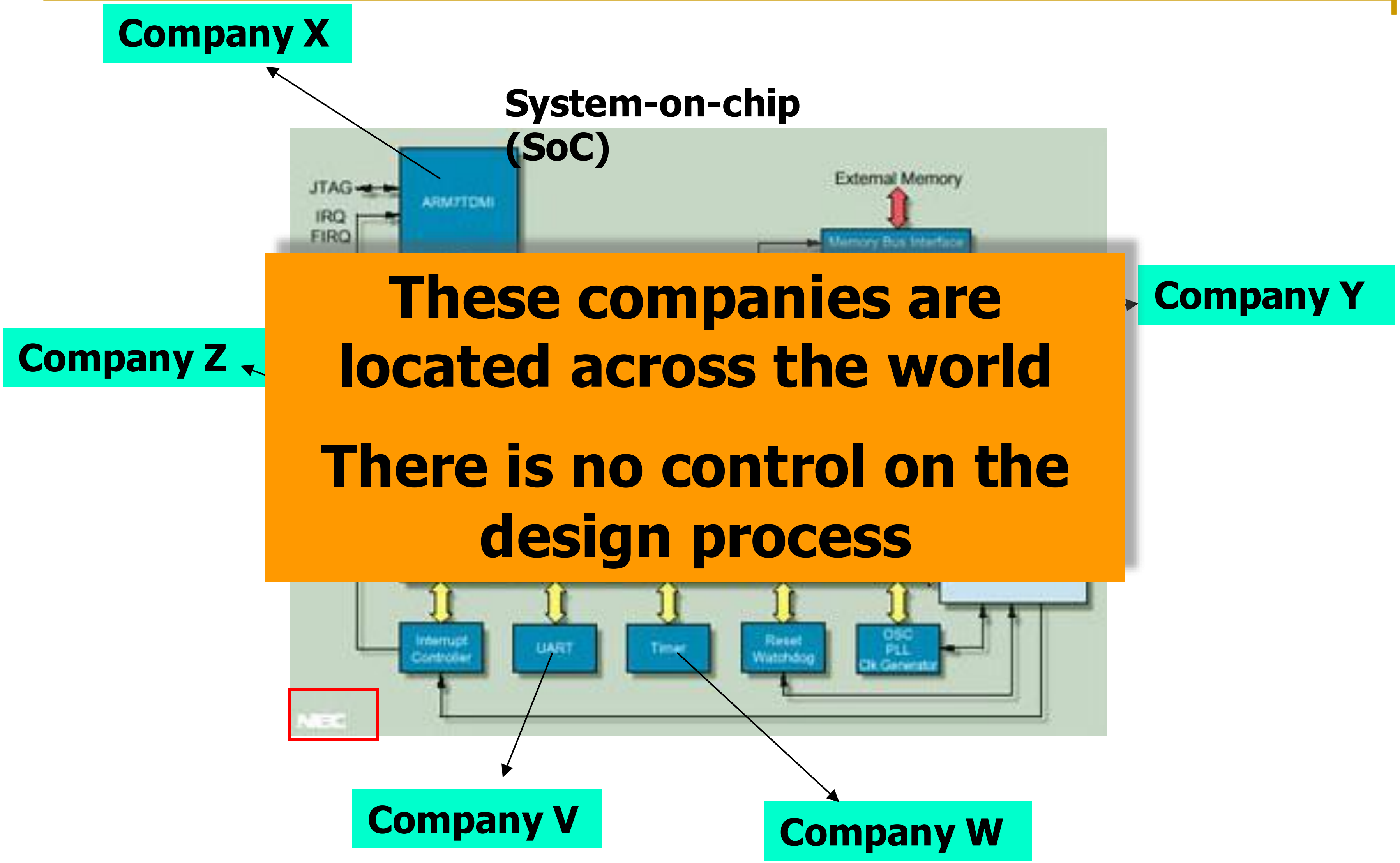
Company Y

Company Z

Company V

Company W

Issues with Third IP Design



Company X

System-on-chip (SoC)

Company Y

Company Z

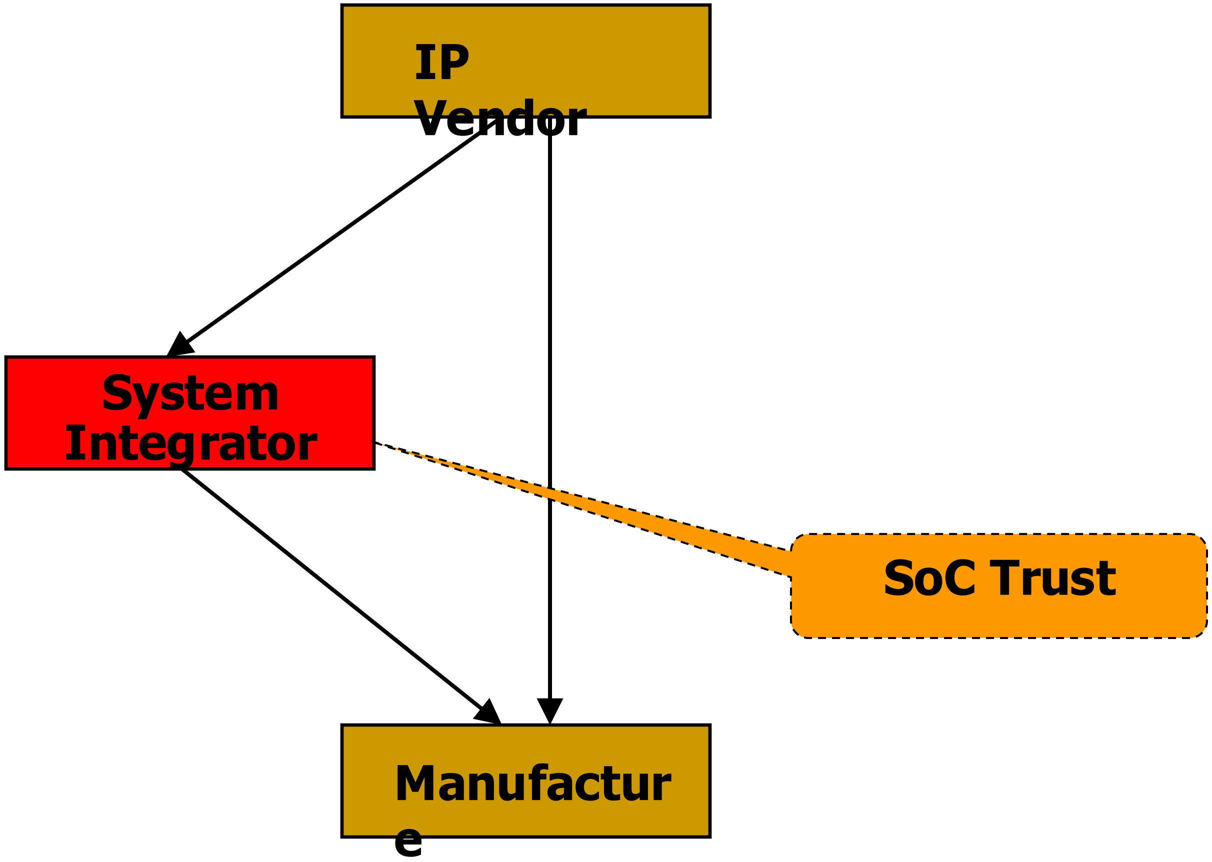
These companies are located across the world

There is no control on the design process

Company V

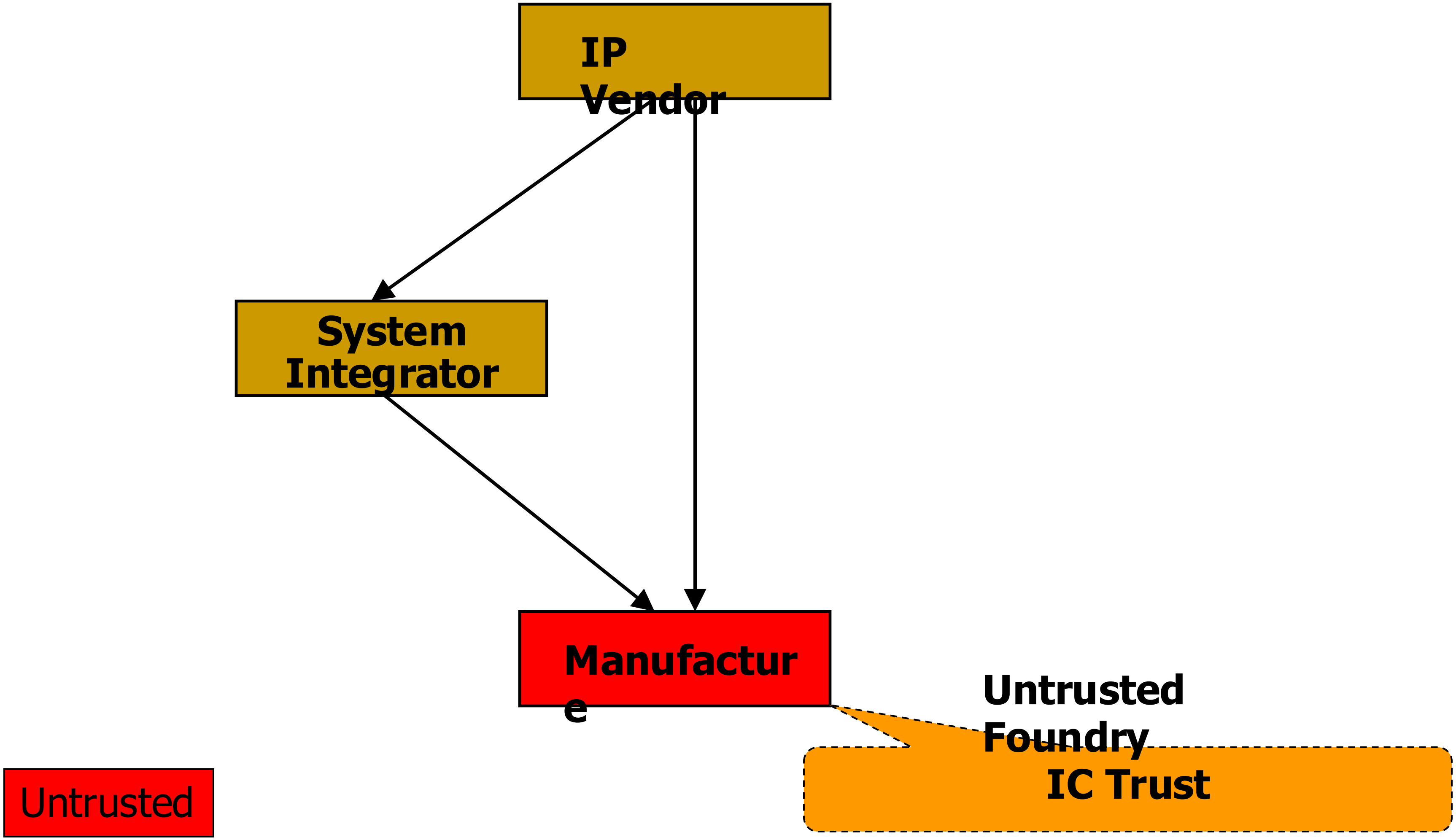
Company W

Hardware Trojan Threat



Untrusted

Hardware Trojan Threat



IP Vendor

System Integrator

Manufacture

Untrusted Foundry

IC Trust

🟥 Untrusted

ASIC Design Process – Untrusted Foundry

Design Process

IP

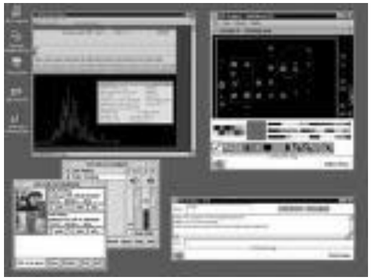
CAD Tools

STD Cells

Models

Design Specification

Design

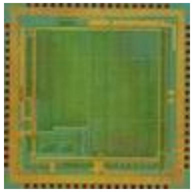


Fabrication Process

Fab Interface

Mask

Fab



Manufacturing Test Process

Wafer Probe

Dice & Package

Package Test

Deploy and Monitor

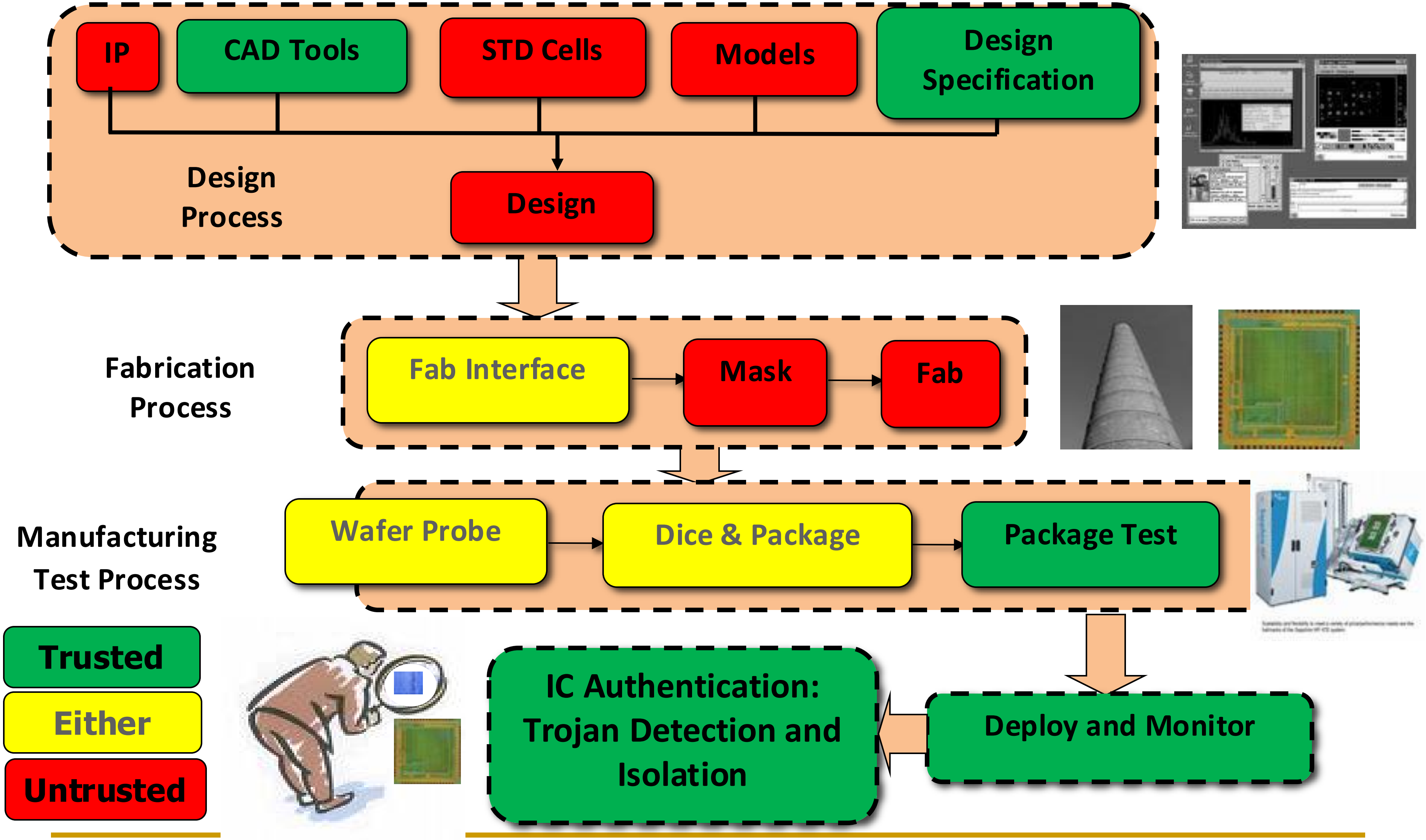
IC Authentication: Trojan Detection and Isolation

🟩 Trusted

🟨 Either

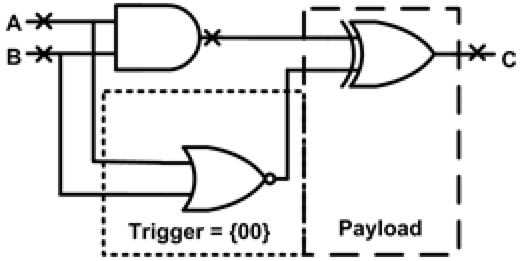
🟥 Untrusted

Untrusted Designer and Foundry

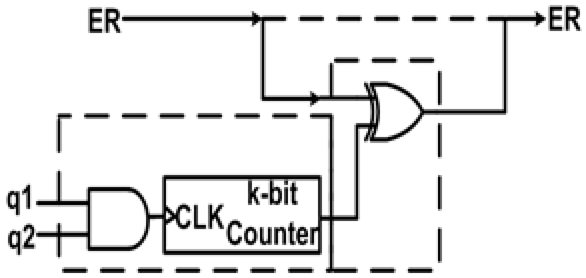


HW Trojan Examples / Models

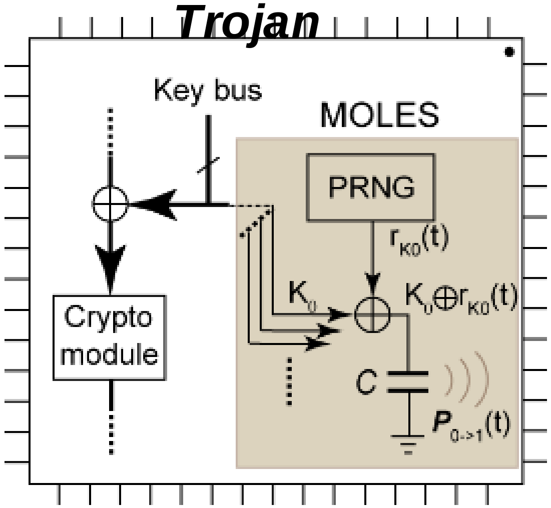
Comb. Trojan Example



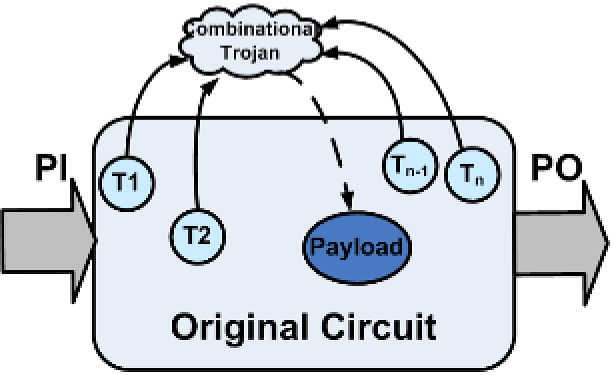
Seq. Trojan Example



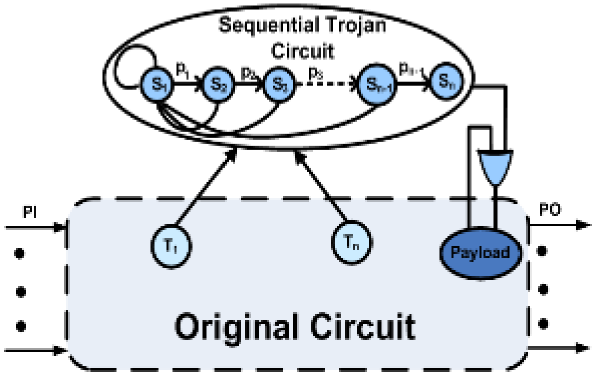
MOLES: Info Leakage Trojan*



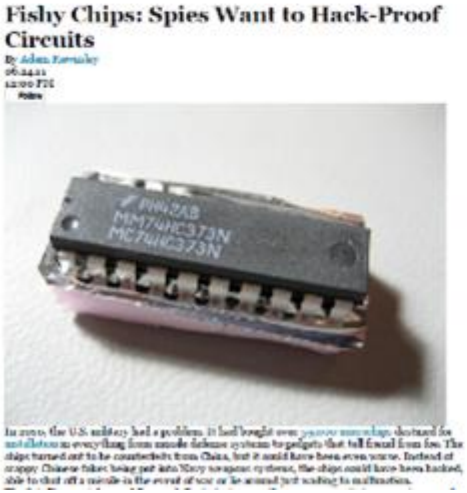
Comb. Trojan model



Seq. Trojan Model



**Lin et al, ICCAD 2009*



Fishy Chips: Spies Want to Hack-Proof Circuits

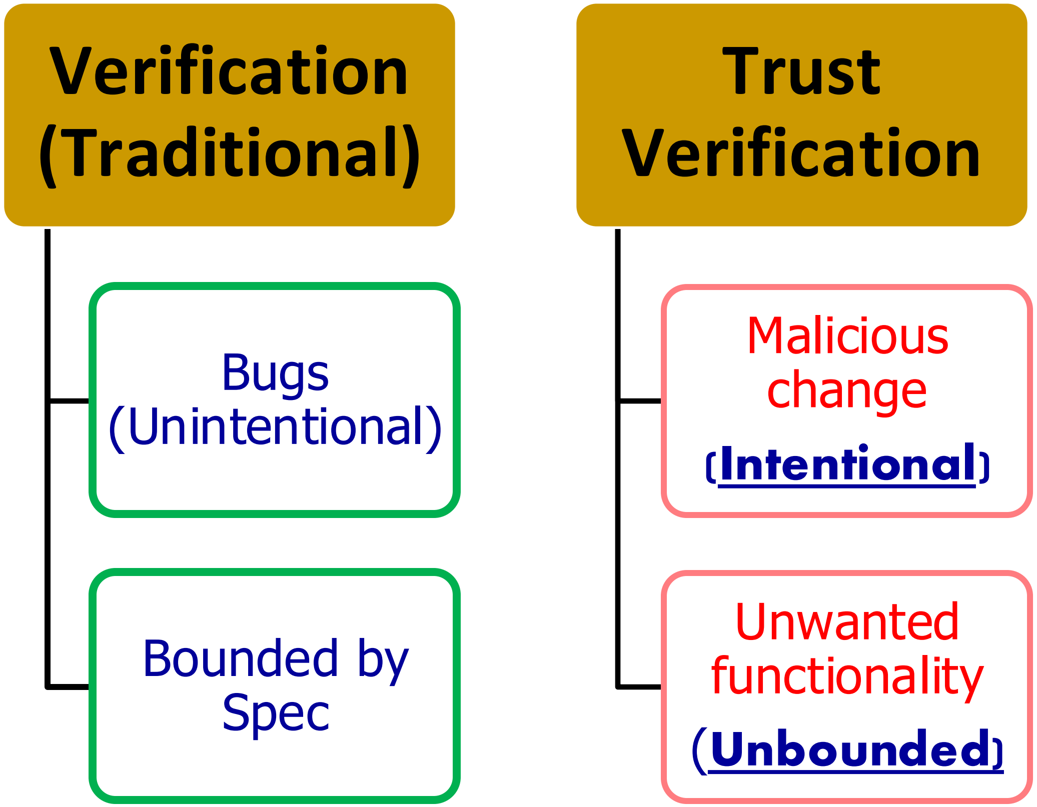
By Adam Rawnsley
06.24.11
12:00 PM
Follow

In 2010, the U.S. military had a problem. It had bought over 59,000 microchips destined for installation in everything from missile defense systems to gadgets that tell friend from foe. The chips turned out to be counterfeits from China, but it could have been even worse. Instead of crappy Chinese fakes being put into Navy weapons systems, the chips could have been hacked, able to shut off a missile in the event of war or lie around just waiting to malfunction.

HW Trojan evidence!

Why is detection of hardware Trojans very difficult?

Bug vs. Malicious Change



Verification (Traditional)

Bugs (Unintentional)

Bounded by Spec

Trust Verification

Malicious change

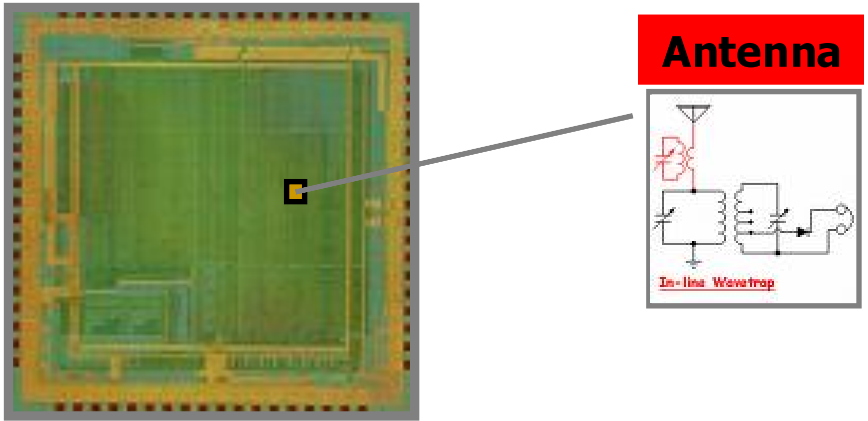
(**Intentional**)

Unwanted functionality

(**Unbounded**)

Trojan Attacks → BIGGER verification challenge!

Silicon Back Door



Untrusted Hardware

- Adversary can send and receive secret information
- Adversary can disable the chip, blowup the chip, send wrong processing data, impact circuit information etc.

- Adversary can place an Antenna on the fabricated chip
- Such Trojan cannot be detected since it does not change the functionality of the circuit.

Silicon Time Bomb

Untrusted Hardware

Counter

Finite state machine (FSM)

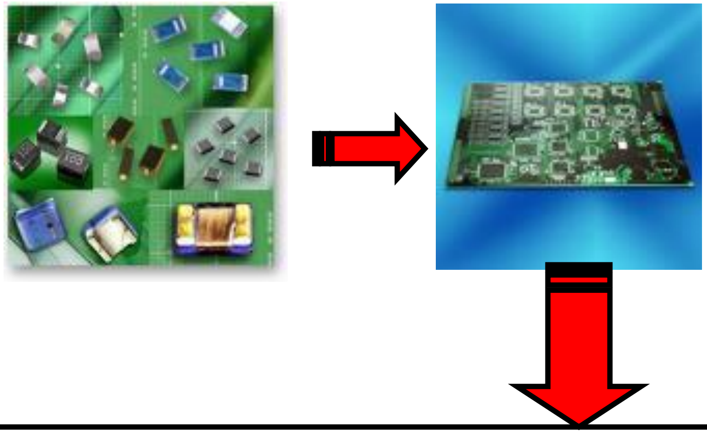
Comparator to monitor key data

Wires/transistors that violate design rules

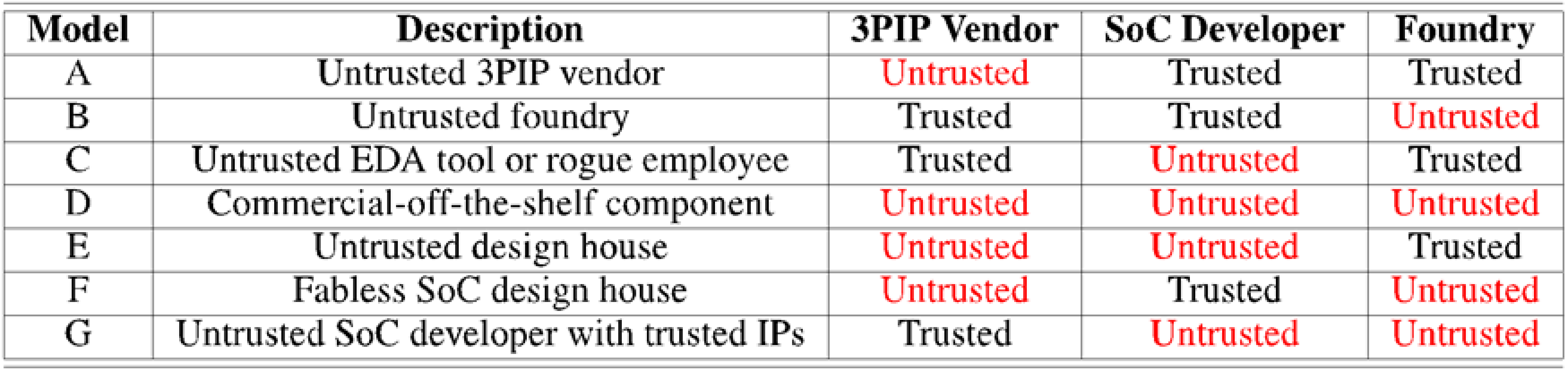
- Such Trojan cannot be detected since it does not change the functionality of the circuit.
- In some cases, adversary has little control on the exact time of Trojan action
- Cause reliability issue

Applications and Threats

Thousands of chips are being fabricated in untrusted foundries



Comprehensive Attack Model



Model	Description	3PIP Vendor	SoC Developer	Foundry
A	Untrusted 3PIP vendor	Untrusted	Trusted	Trusted
B	Untrusted foundry	Trusted	Trusted	Untrusted
C	Untrusted EDA tool or rogue employee	Trusted	Untrusted	Trusted
D	Commercial-off-the-shelf component	Untrusted	Untrusted	Untrusted
E	Untrusted design house	Untrusted	Untrusted	Trusted
F	Fabless SoC design house	Untrusted	Trusted	Untrusted
G	Untrusted SoC developer with trusted IPs	Trusted	Untrusted	Untrusted

Trojan Taxonomy

What is a Taxonomy?

How are Taxonomies useful?

Trojan Taxonomy

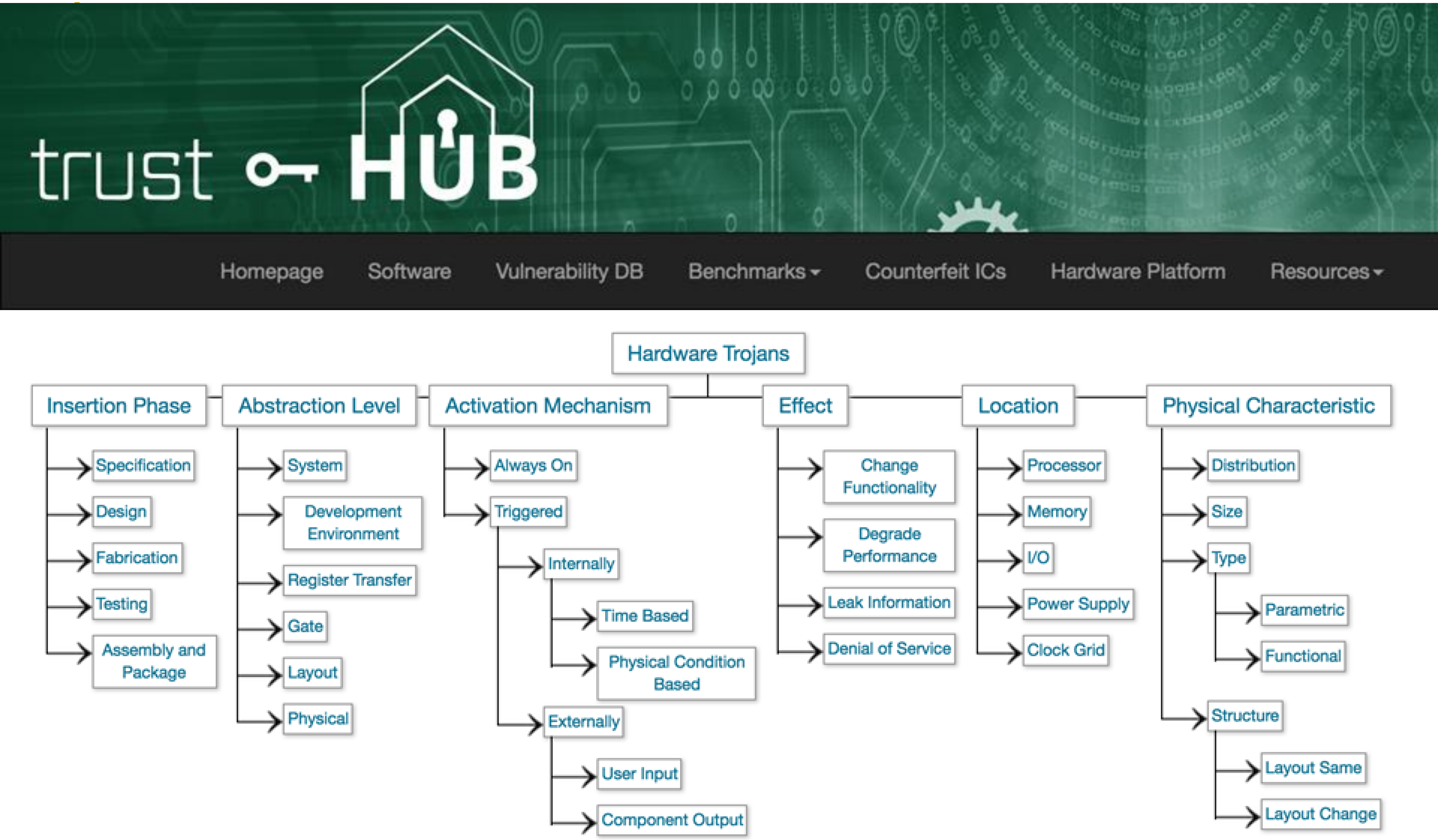
What is a Taxonomy?

A system of classification!

How are Taxonomies useful?

Provides structure for understanding and communicating ideas for complex (diverse) subject matter.

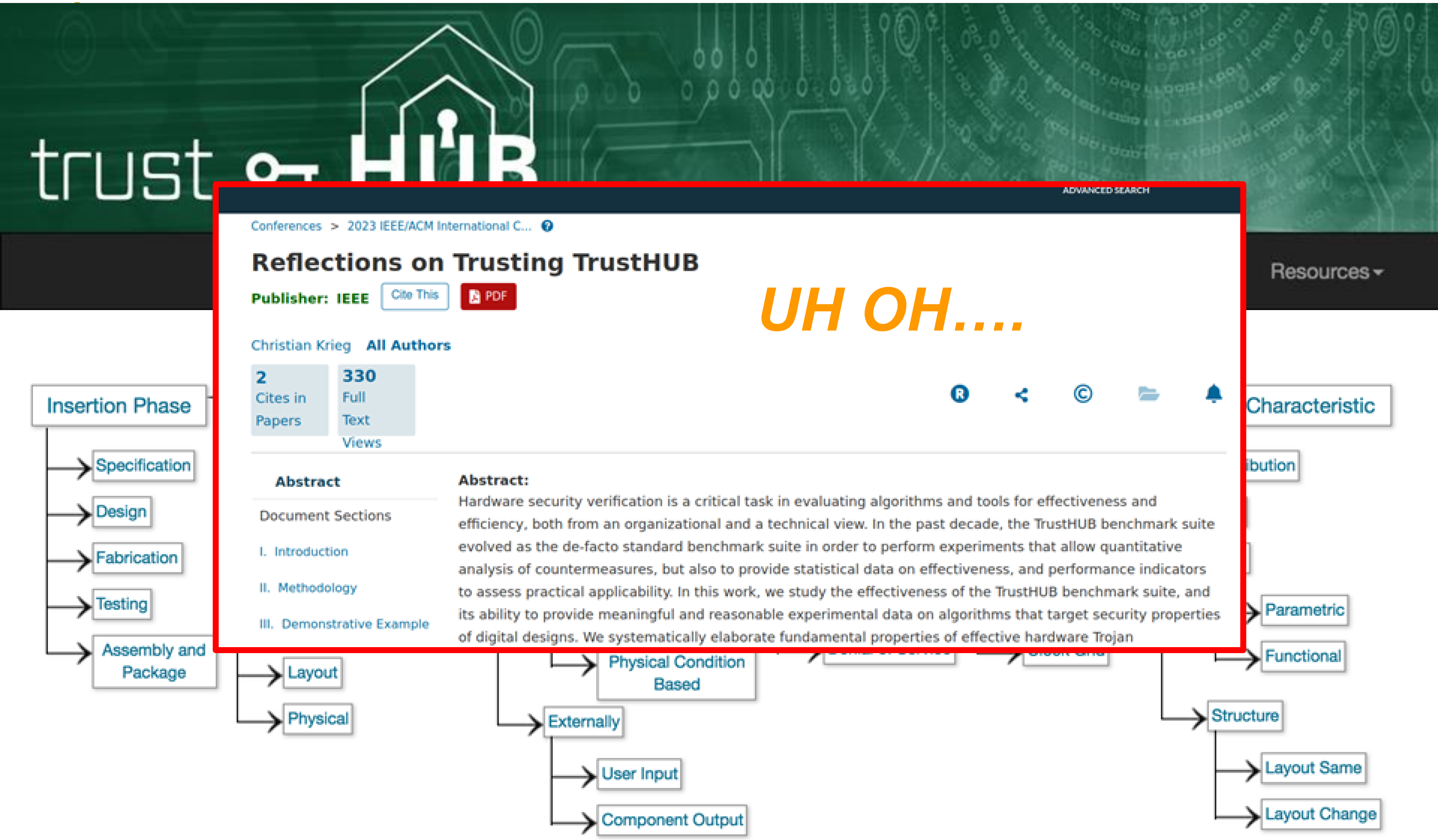
Trojan Taxonomy



Hardware Trojans

- Insertion Phase
  - Specification
  - Design
  - Fabrication
  - Testing
  - Assembly and Package
- Abstraction Level
  - System
  - Development Environment
  - Register Transfer
  - Gate
  - Layout
  - Physical
- Activation Mechanism
  - Always On
  - Triggered
    - Internally
      - Time Based
      - Physical Condition Based
    - Externally
      - User Input
      - Component Output
- Effect
  - Change Functionality
  - Degrade Performance
  - Leak Information
  - Denial of Service
- Location
  - Processor
  - Memory
  - I/O
  - Power Supply
  - Clock Grid
- Physical Characteristic
  - Distribution
  - Size
  - Type
    - Parametric
    - Functional
  - Structure
    - Layout Same
    - Layout Change

Trojan Taxonomy



Conferences > 2023 IEEE/ACM International C...

Reflections on Trusting TrustHUB

Publisher: IEEE Cite This PDF

Christian Krieg All Authors

2 Cites in Papers

330 Full Text Views

Abstract

Document Sections

I. Introduction

II. Methodology

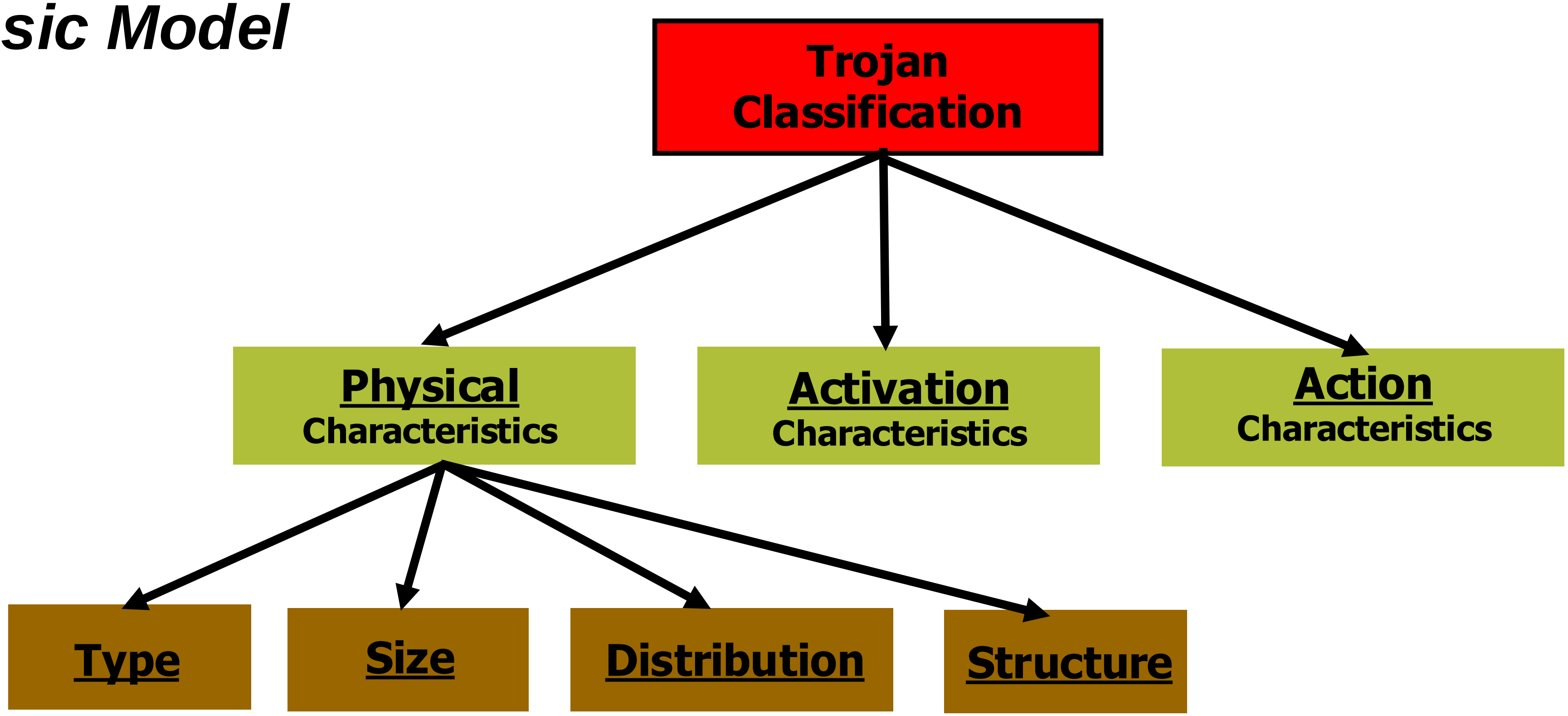
III. Demonstrative Example

Abstract: Hardware security verification is a critical task in evaluating algorithms and tools for effectiveness and efficiency, both from an organizational and a technical view. In the past decade, the TrustHUB benchmark suite evolved as the de-facto standard benchmark suite in order to perform experiments that allow quantitative analysis of countermeasures, but also to provide statistical data on effectiveness, and performance indicators to assess practical applicability. In this work, we study the effectiveness of the TrustHUB benchmark suite, and its ability to provide meaningful and reasonable experimental data on algorithms that target security properties of digital designs. We systematically elaborate fundamental properties of effective hardware Trojan

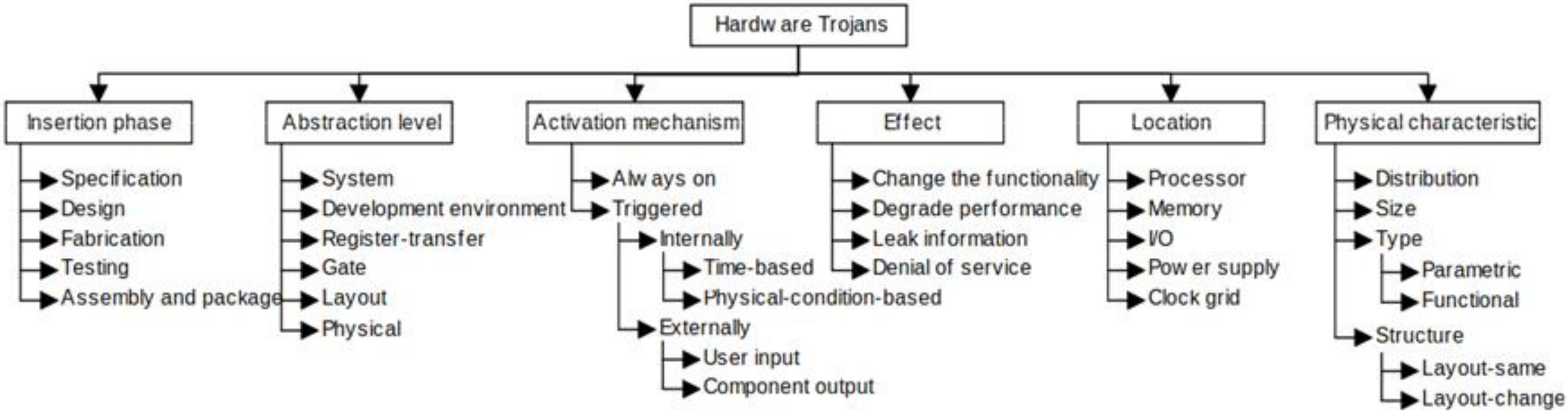
UH OH….

Trojan Taxonomy

Basic Model



Trojan Taxonomy



- Hardw are Trojans
  - Insertion phase
    - Specification
    - Design
    - Fabrication
    - Testing
    - Assembly and package
  - Abstraction level
    - System
    - Development environment
    - Register-transfer
    - Gate
    - Layout
    - Physical
  - Activation mechanism
    - Alw ays on
    - Triggered
      - Internally
        - Time-based
        - Physical-condition-based
      - Externally
        - User input
        - Component output
  - Effect
    - Change the functionality
    - Degrade performance
    - Leak information
    - Denial of service
  - Location
    - Processor
    - Memory
    - I/O
    - Pow er supply
    - Clock grid
  - Physical characteristic
    - Distribution
    - Size
    - Type
      - Parametric
      - Functional
    - Structure
      - Layout-same
      - Layout-change

UF Model a.k.a Grandaddy of HTH Taxonomies

04 Hardware Trojans

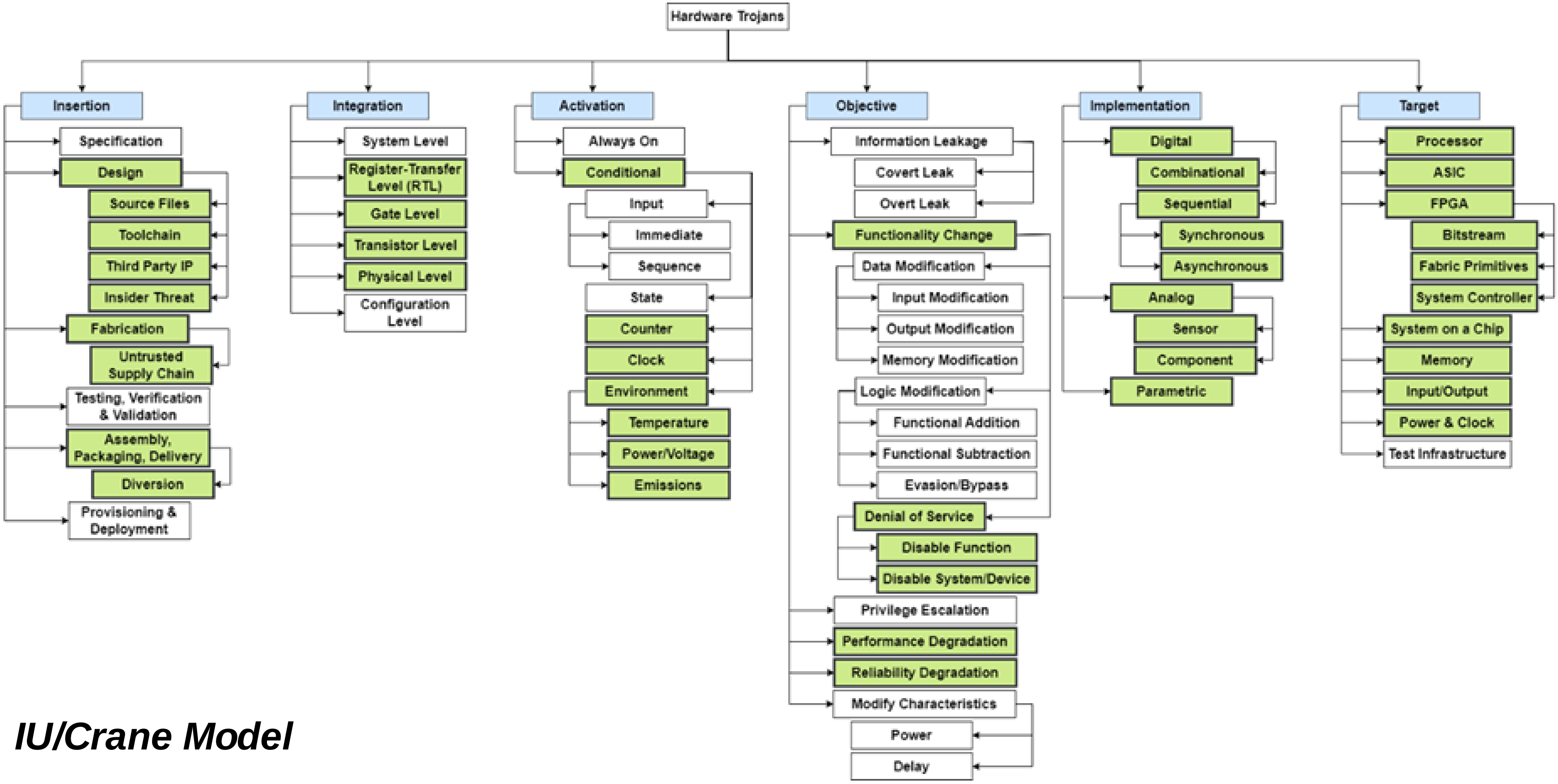
Engr 399/599: Hardware Security

Grant Skipper, Ph.D.

Indiana University

Adapted from: Mark Tehranipoor of University of Florida

Trojan Taxonomy



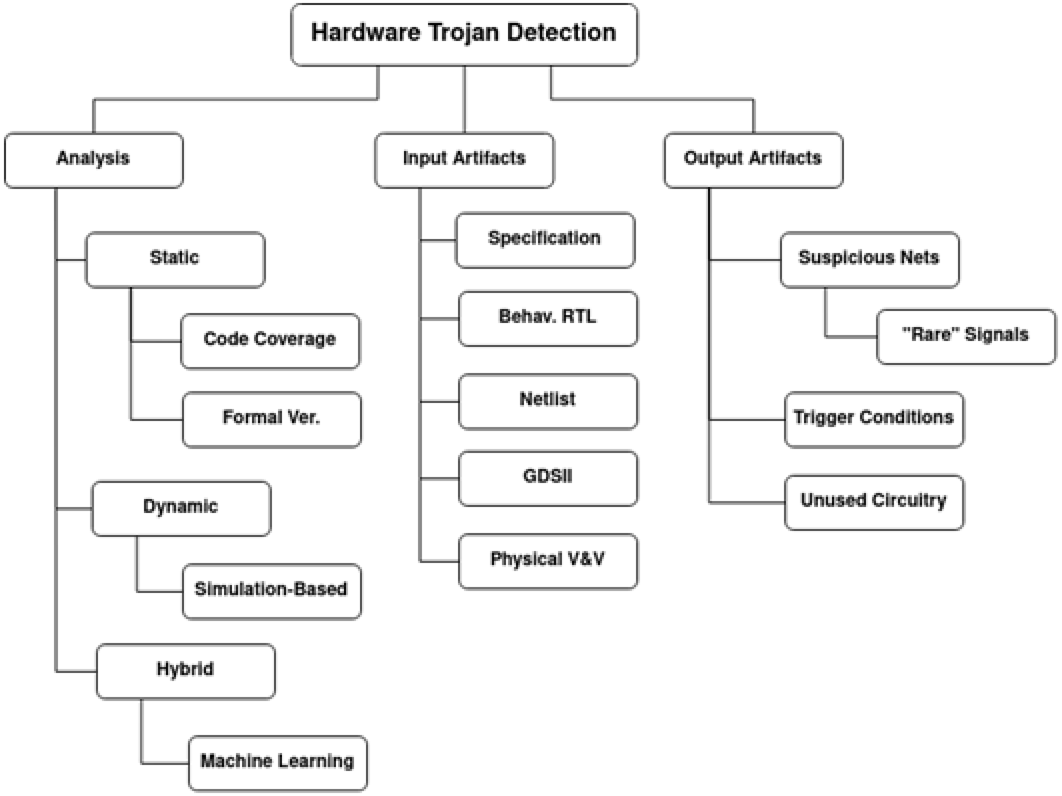
- Hardware Trojans
  - Insertion
    - Specification
    - Design
      - Source Files
      - Toolchain
      - Third Party IP
      - Insider Threat
    - Fabrication
      - Untrusted Supply Chain
    - Testing, Verification & Validation
    - Assembly, Packaging, Delivery
      - Diversion
    - Provisioning & Deployment
  - Integration
    - System Level
    - Register-Transfer Level (RTL)
    - Gate Level
    - Transistor Level
    - Physical Level
    - Configuration Level
  - Activation
    - Always On
    - Conditional
      - Input
        - Immediate
        - Sequence
      - State
      - Counter
      - Clock
      - Environment
        - Temperature
        - Power/Voltage
        - Emissions
  - Objective
    - Information Leakage
      - Covert Leak
      - Overt Leak
    - Functionality Change
      - Data Modification
        - Input Modification
        - Output Modification
        - Memory Modification
      - Logic Modification
        - Functional Addition
        - Functional Subtraction
        - Evasion/Bypass
      - Denial of Service
        - Disable Function
        - Disable System/Device
    - Privilege Escalation
    - Performance Degradation
    - Reliability Degradation
    - Modify Characteristics
      - Power
      - Delay
  - Implementation
    - Digital
      - Combinational
      - Sequential
        - Synchronous
        - Asynchronous
    - Analog
      - Sensor
      - Component
    - Parametric
  - Target
    - Processor
    - ASIC
    - FPGA
      - Bitstream
      - Fabric Primitives
      - System Controller
    - System on a Chip
    - Memory
    - Input/Output
    - Power & Clock
    - Test Infrastructure

IU/Crane Model

Iterating on previous models; balancing abstraction and specificity.

Hardware Trojan (Detection) Taxonomy

HT Detection methods can be roughly taxonomized via the general approach used to perform detection, the inputs used, and the output analysis provided.



(U)