Hardware Trojans
Detect and React?

A. Dabrowski, P. Fejes, J. Ullrich, K. Krombholz, H. Hobel, E. Weippl

secure
sba-research.org

Hardware Development Cycle

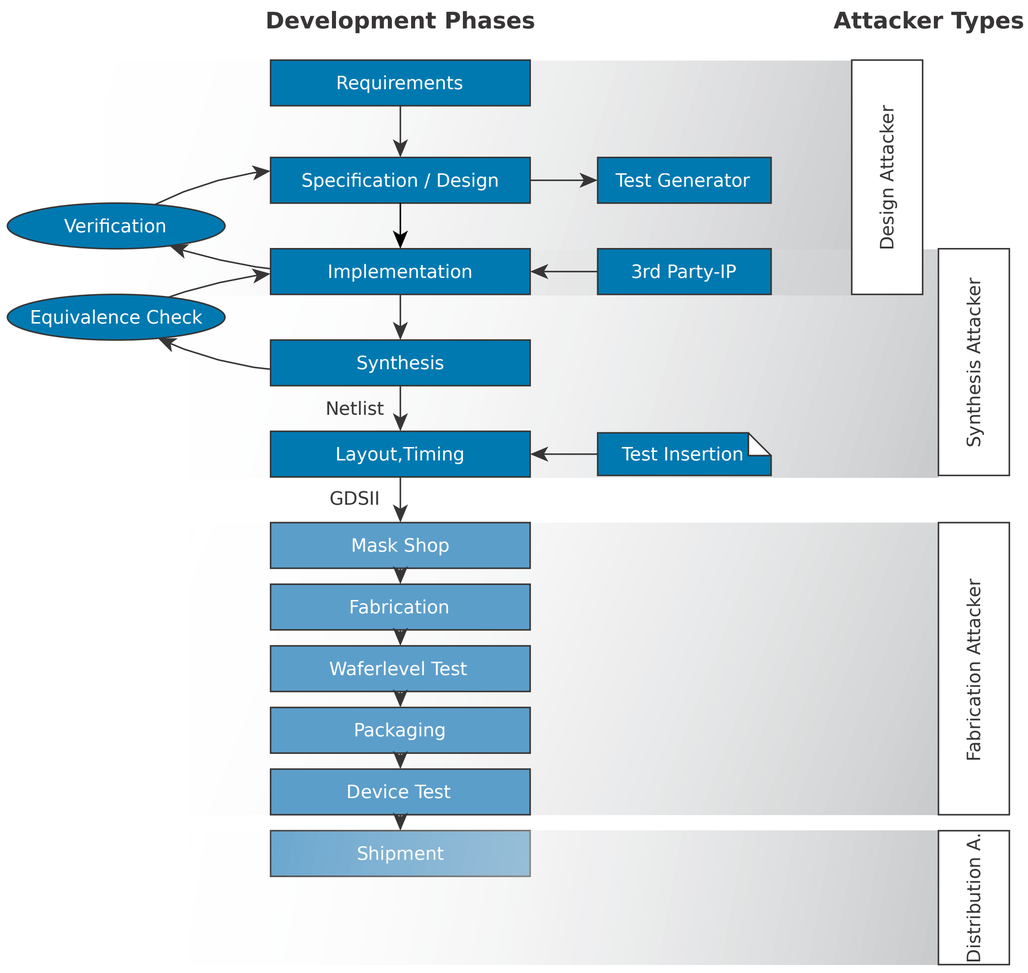

Figure 1: Industrial Hardware Development Lifecycle

Problem & Motivation

- Hardware Trojans are malicious hardware changes which might result in changing functionality of the device.
  - *Integrated Circuits* are essential parts of everyday life
  - Lack of real-world examples
  - Need of Trojan implementations for development of detection methods

Methodology: Hardware Trojan Kit

The kit is assembled in a modular way and it bases on four charact-eristics: activation, covert communication, payload and detection.

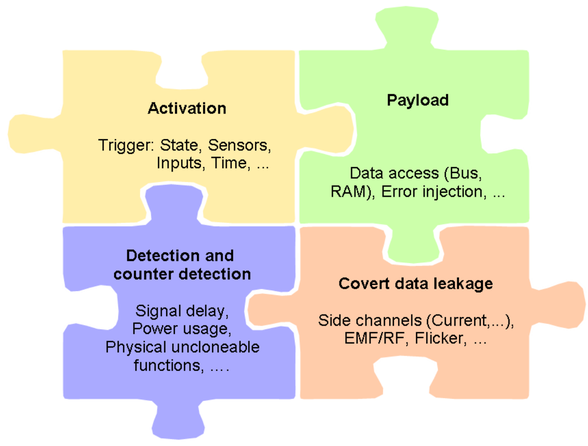

Figure 2: Classification of Modules

Methodology: Malware Structures

- An analysis on HDL/RTL as well as netlist level showed that the following characteristic structures are of interest for Hardware Trojan detection:
  - Asynchronous latches
    unclocked, self-clocked or externally clocked flip-flops
  - Gated wire or output signals
    signal which is influenced by means of a gate
  - Ring oscillator
    combinatorial loop without constant frequency
  - Unused pins or bond wires
    convient for covert channel dissemination
  - Additional states
    dependent on the encoding scheme
  - Gated reset signal
    resets, which are independent from the global reset
  - Local or gated clocks
    clocks, which are independent from the global clock

	Extra slices	Extra LUTs	Specifc elements	Async. latch	Gated wire/output	RO	Unused pin/bond	Hidden FSM state(s)	Latch/FF wo/gated reset	Local/gated clock
Activation										
Thermal trigger	101 (27+RO)	186 (7)	RO and a measurement circuit		x	x				
Synchronous counter	37/46	1								
Asyncronous counter	15	6		x	x					(x)
Hybrid counter	21	14		x	x				x	
UART parity error	54	57	Extra comparator/gates		x					
Character counter	10	10	Extra comparator			x				
Character FSM	0	65	Extra FSM					x		
ADC trigger	30	45	FSM /monitoring circuit					x		
Covert channel										
AM radio	292	521	Unused bond				x			
Modifed UART idle	6(tx) 14(rx)	8 / 25	Mod. FSM, mod. baud rate					x		
Modifed UART character	9(tx) 2(rx)	16 / 2	Mod. RS232 character, extra shift-register		x			x		
LED transmission	85	83	Blinking LED	x		(x)				
Power side channel			Measurement device	x						
Payload										
Mod. FSM	0	0	Extra state					x		
UART with mod. reset	10	10	Gated reset						x	
UART with mod. tx data	0	65						x		
Clock division mod.	2	1	Local clock							x
Mod. carry lookahead adder	0	2	Gated signal		x					
Mod. memory enable signal	1	6	Extra comparator/gates	x						
Mod. memory content	8	5	Mod. latch	x						
Mod. sync. divider	3	6								
Mod. case-divider	5	7	Extra state					x		
Mod. combinatorial divider	0	0	XOR instead of OR		x					
Detection										
Ring Oscillator						x				
Physically Unclonable Function						x				
Shadow Circuit			Exact copy of the circuit							

Table 1: Malware Structures in Kit Modules

Future Work

- Enhancement of the development process to mitigate the threat of Hardware Trojans
- Provision of the Trojan kit to the scientific community

FFG

This work was supported by the FIT-IT program (project number 835922) and the COMET K1 program by FFG (Austrian Research Funding Agency).