CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenture

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

B5

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DATA
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DGi ONE
the leading digital company

ICT CYBER CONSULTING

Hardware Trojans

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER
CHALLENGE
CyberChallenge.IT

cini
Cybersecurity
National Lab

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Prerequisites

- Lecture:
  - *HS_1.2 - Hardware Vulnerabilities*

Acknowledgments

- The presentation includes material from
  - Giorgio DI NATALE
  - Nicolò MAUNERO
  - Gianluca ROASCIO

  whose valuable contribution is here acknowledged and highly appreciated.

Goals

- Presenting an overview on the threat that Hardware Trojan pose today, providing a proper taxonomy.

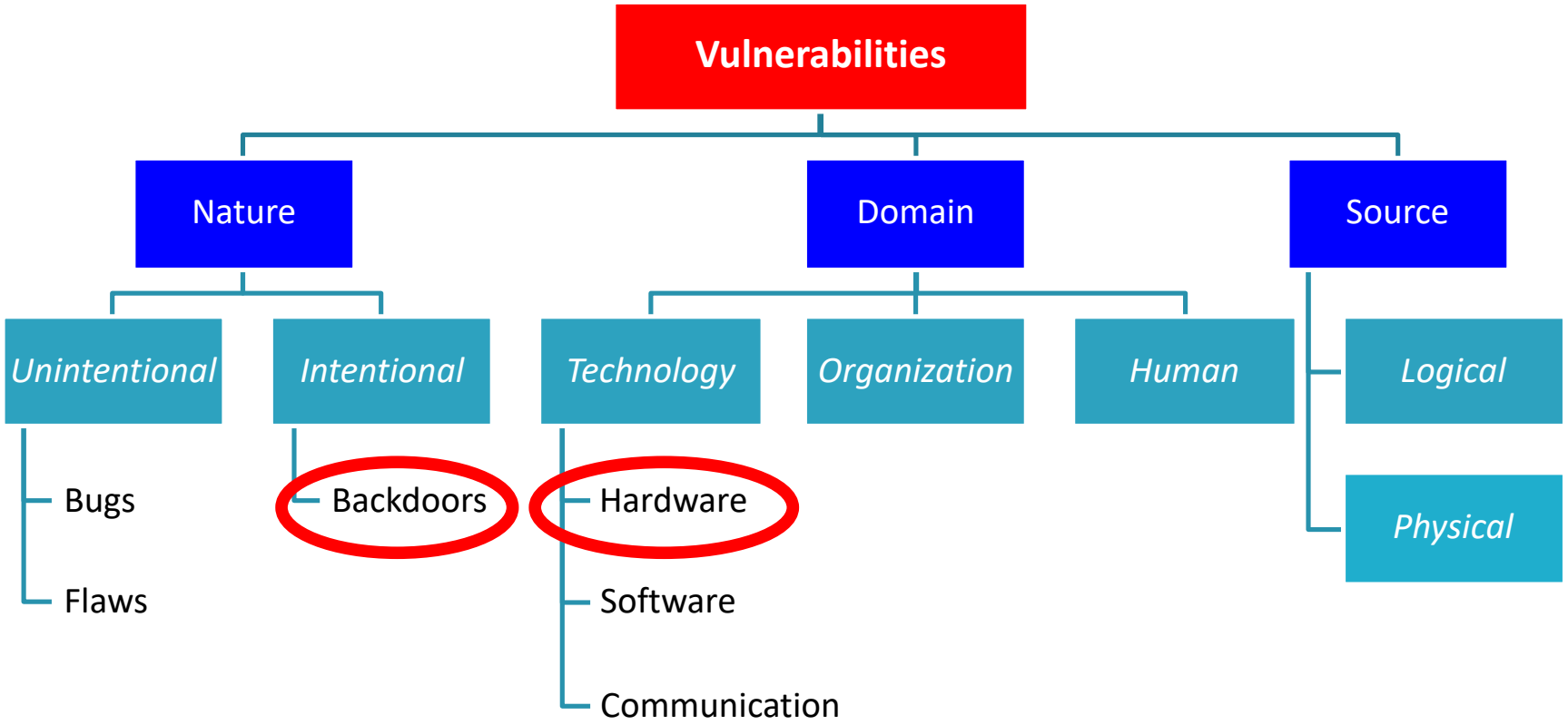
Outline

- Introduction
- Trojans Taxonomy

Outline

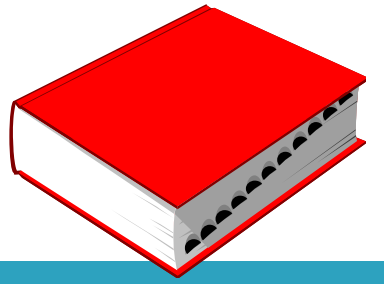
- Introduction
- Trojans Taxonomy

Hardware Vulnerabilities Taxonomy



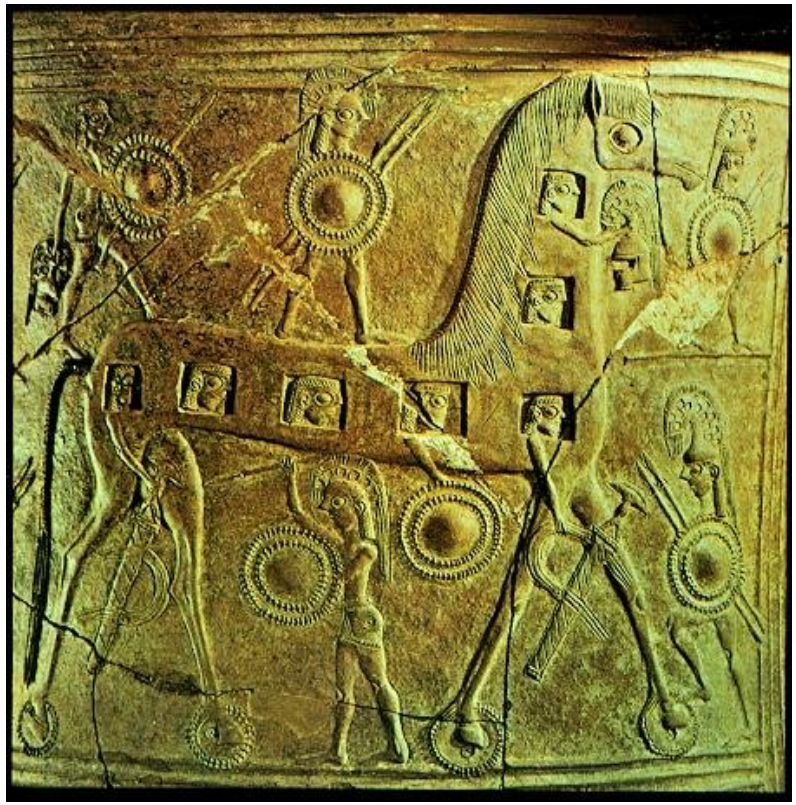
 Rel. 18.05.2020

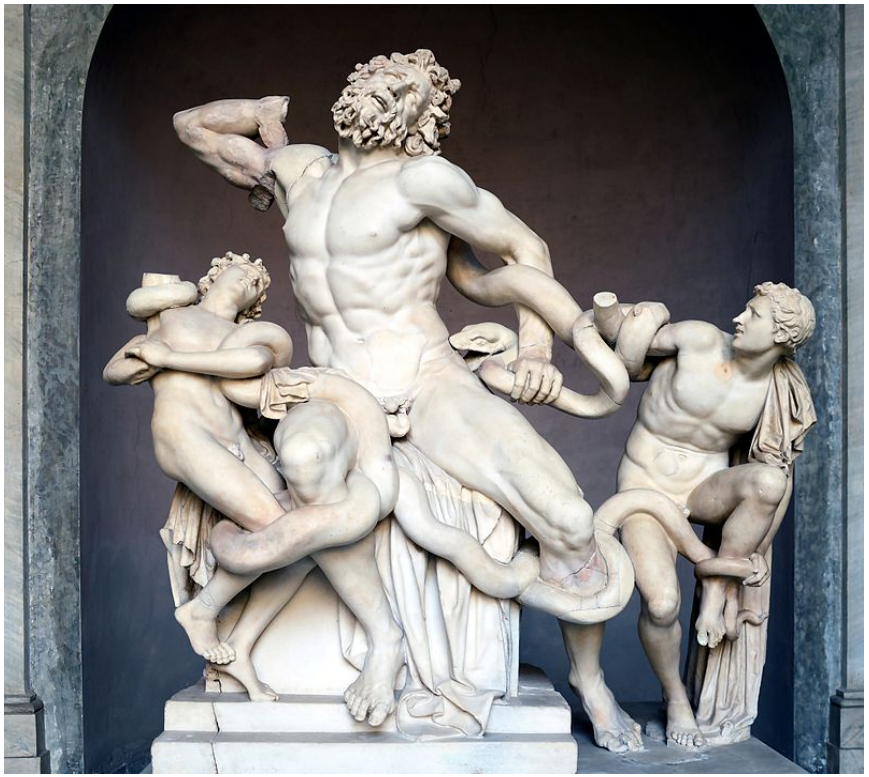
Intentional Vulnerabilities



- A vulnerability inserted intentionally inside a hardware device can be referred to as a *backdoor*, as the person who inserts them wants to guarantee her/himself (or someone else) the possibility of a later access or use that is *outside* the set of intended use cases.

Trojan Horse

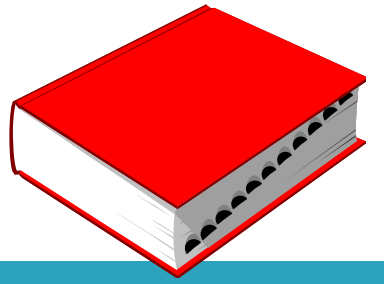




Trojan Horse

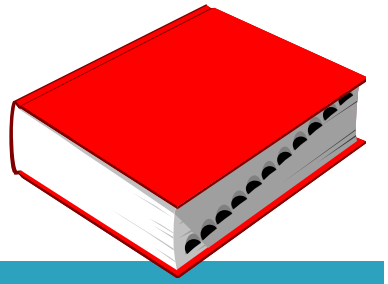
Publio Virgilio Marone - Eneide (Libro II, 49)

Hardware Trojan



- A rogue piece of circuitry fraudulently inserted during the design or production phase, which can carry out unauthorized actions when its *triggering conditions* are satisfied.

Hardware Trojan



Trigger

- The activation mechanism of the Trojan (e.g., always on, input condition, …)

Payload

- The harmful effect of Trojan activation (e.g., alter functionality, DoS, destruction, …)

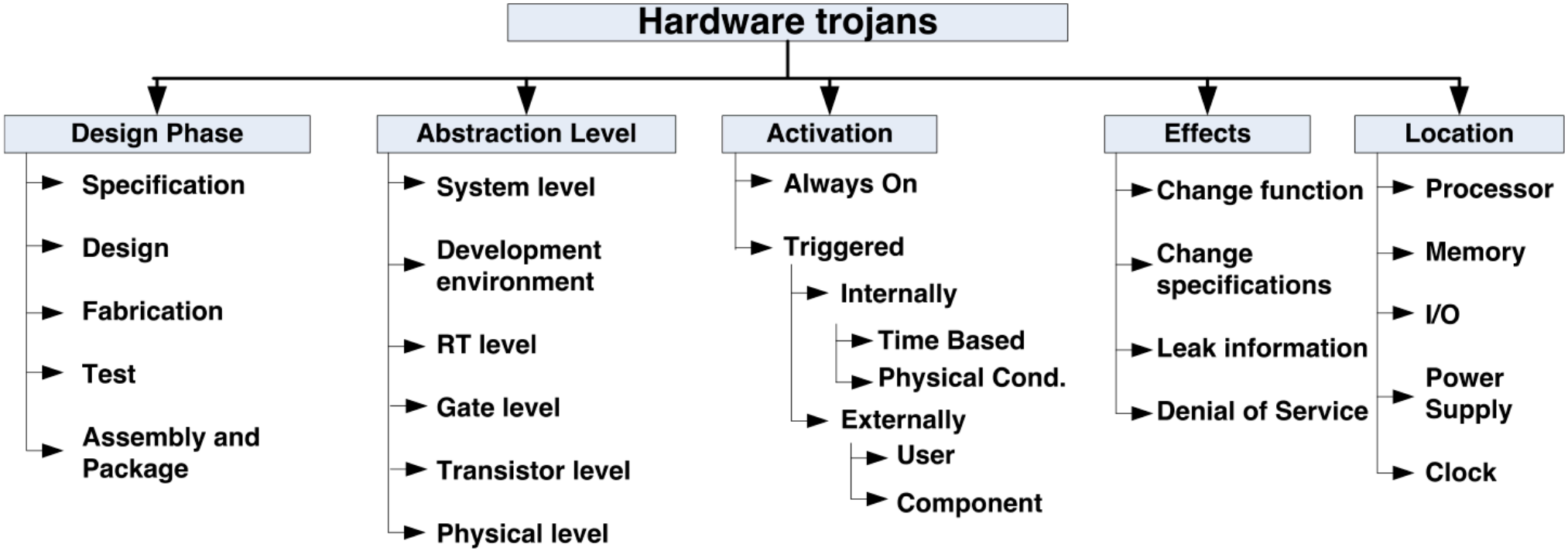
Outline

- Introduction
- Trojans Taxonomy

Hardware Trojan Taxonomy

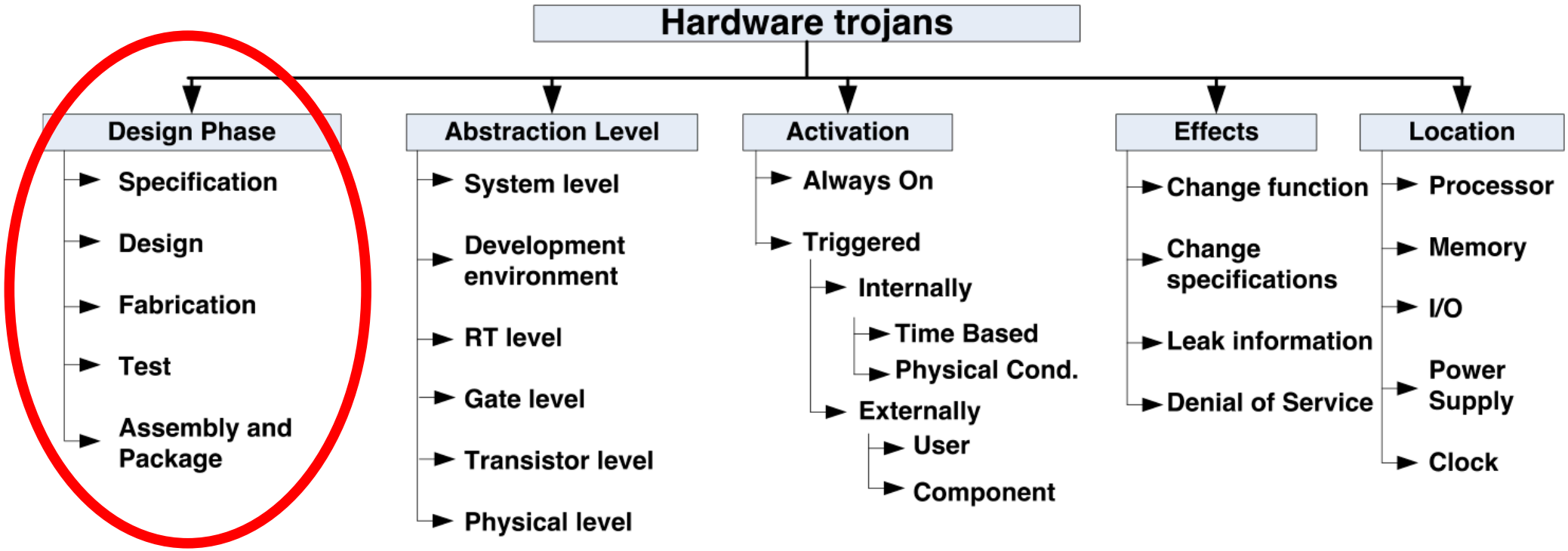
- HW Trojans can be according to several criteria:
  - When the Trojan is inserted
  - Where the Trojan is inserted
  - How the Trojan can be activated
  - Which effects the Trojan may have

Hardware Trojan Taxonomy



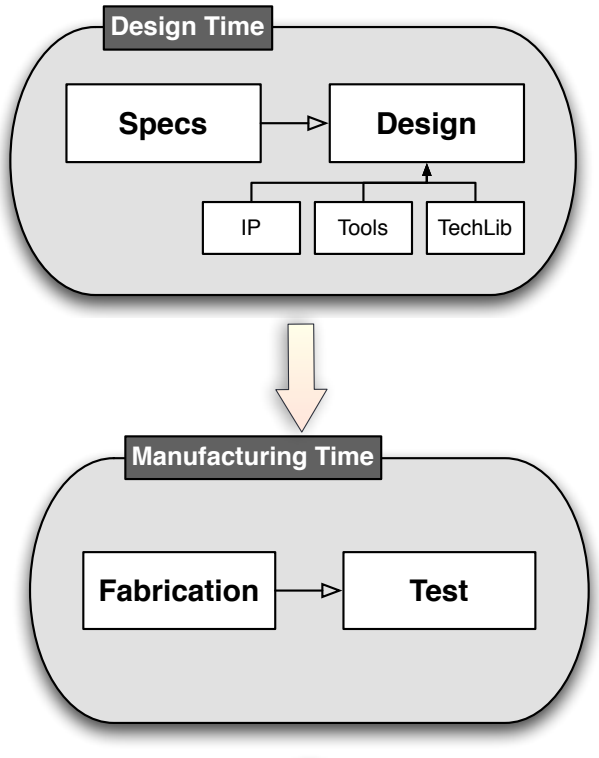
R. Karri et. al "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," IEEE Computer, vol. 43, no. 10, pp 39-46, 2010

Hardware Trojan Taxonomy



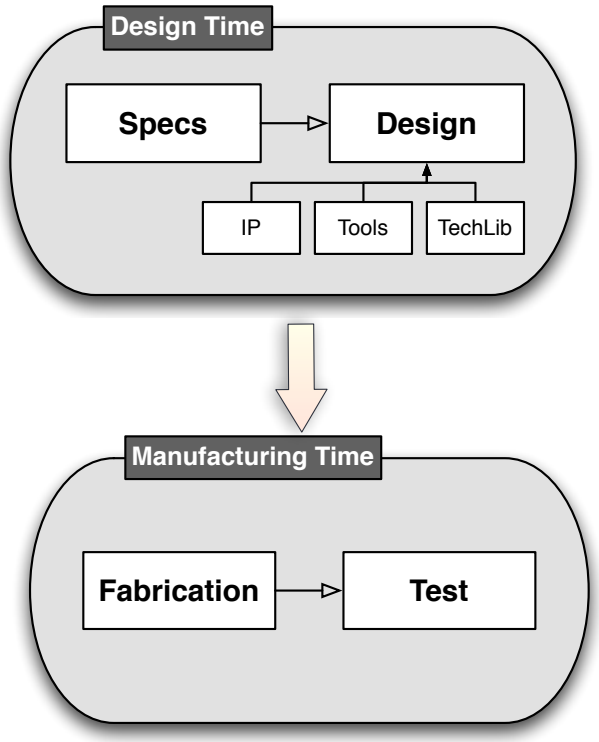
R. Karri et. al "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," IEEE Computer, vol. 43, no. 10, pp 39-46, 2010

Design & Production Phase

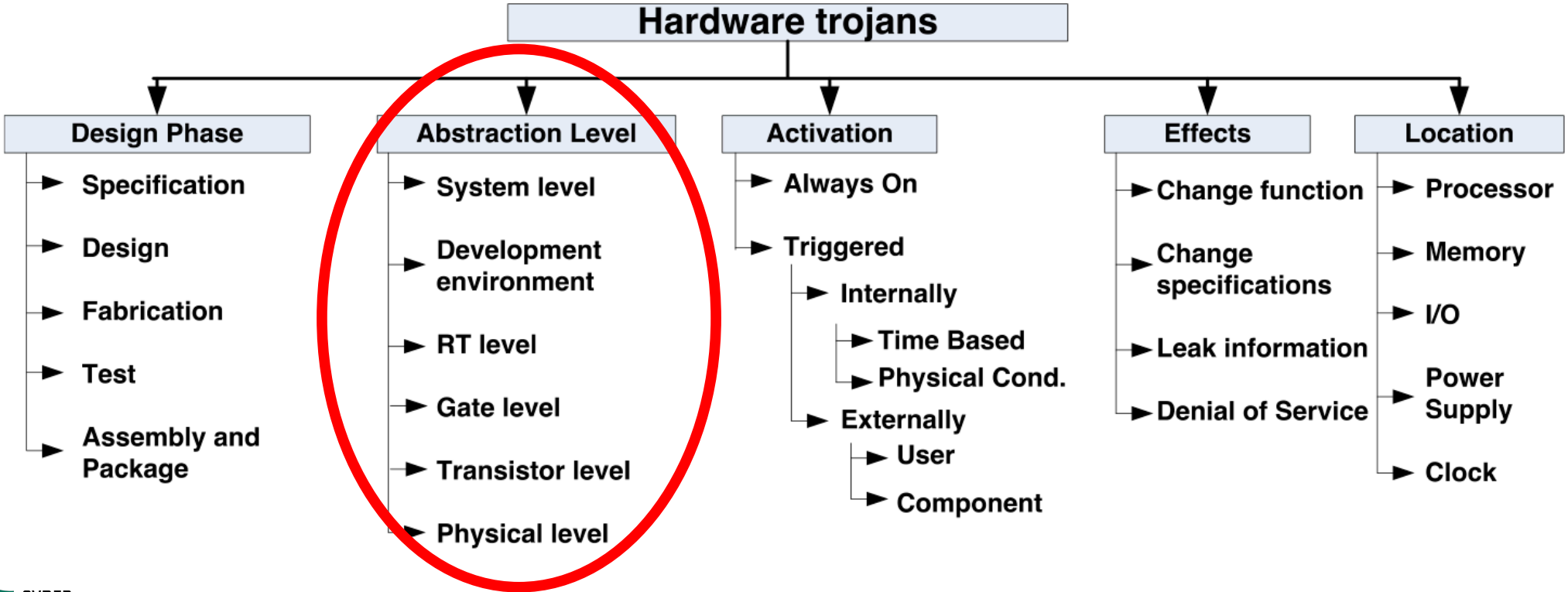


Design & Production Phase

- **Design**
  - Malicious IP core used during the design phase
  - Malicious design tools
  - Malicious designer
- **Fabrication**
  - Modification in the mask geometry and layout
  - Alteration in the chemical composition
- **Test**
  - A Trojan can be either inserted or hidden if already present
  - Untrusted Test Facilities can hide the detection of a Trojan
- **Assembly**
  - Improper termination
  - Improper shielding against phenomena such as electromagnetic interference



Hardware Trojan Taxonomy



R. Karri et. al "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," IEEE Computer, vol. 43, no. 10, pp 39-46, 2010

Abstraction Level

- *System Level*

- Alteration in the interconnections
- Modification of communication protocols
- Alteration of hardware modules
- Exploitation of *active probes* for eavesdropping

Caveat

- Not ALL hardware trojans are exploited by cyber-criminals !!
- Law enforcement agencies are extensively resorting to them

Probes for active eavesdropping

- Active interceptions are mainly conducted via active network probes, i.e., network devices that can be interposed on the user's communication channel and that, in addition to intercepting traffic, can (under specific circumstances) interact with the user pretending to be the recipient.
- This is done in order, for example, to exchange false authentication certificates or to alter the data flow appropriately.

Abstraction Level

- *System Level*
- *Architectural Level*

- The ISA (Instruction Set Architecture) of a processor can include undocumented Machine Instructions, introduced:
  - Fraudulently to enable, for instance, privilege escalations
  - For debugging purposes and then not removed in the final version

Undocumented CPU Instructions

- An undocumented machine instruction has been detected in some CPUs x86 manufactured by VIA Technologies
- The instruction ALTINST (0F 3F) forces the CPU to execute an alternative ISA and directly accessing the RISC core available within the CPU by executing a JMP EAX, i.e., a jump to the memory location whose address is stored into the EAX register

Abstraction Level

- *System Level*
- *Architectural Level*
- *RT Level*

- An attacker can gain control over the hardware functionality

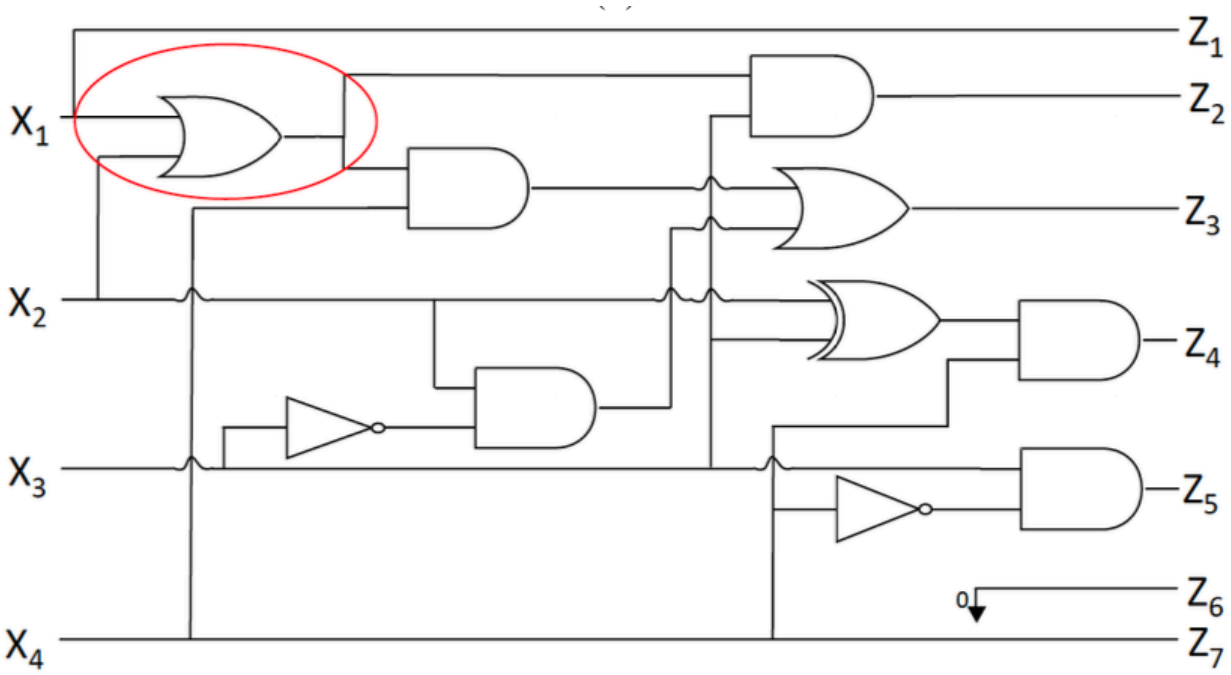
Abstraction Level

- *System Level*
- *Architectural Level*
- *RT Level*
- *Netlist Level*

- Logic gates and flip-flops are added in order to modify or inhibit some of the device functionalities

Netlist Level Trojan

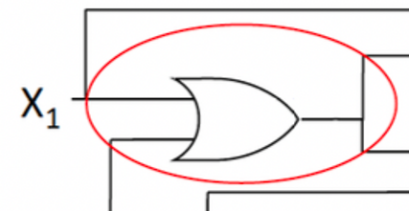
- Circuit without the Trojan

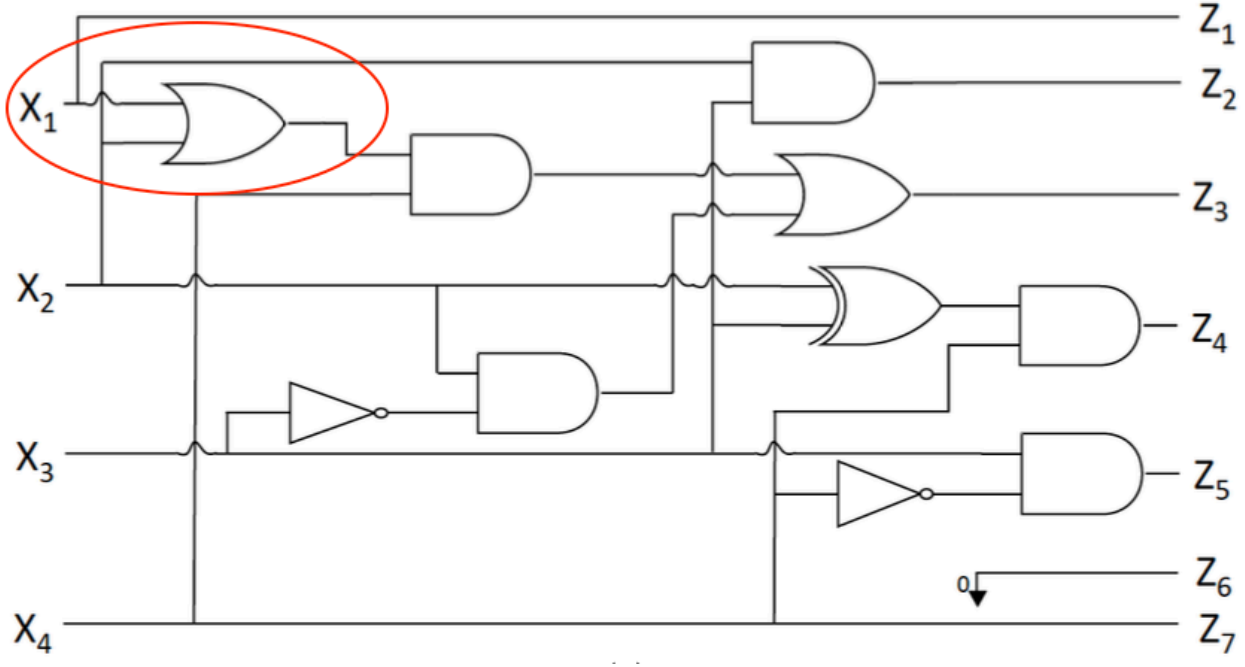


 Rel. 18.05.2020

Netlist Level Trojan

- Circuit with the Trojan



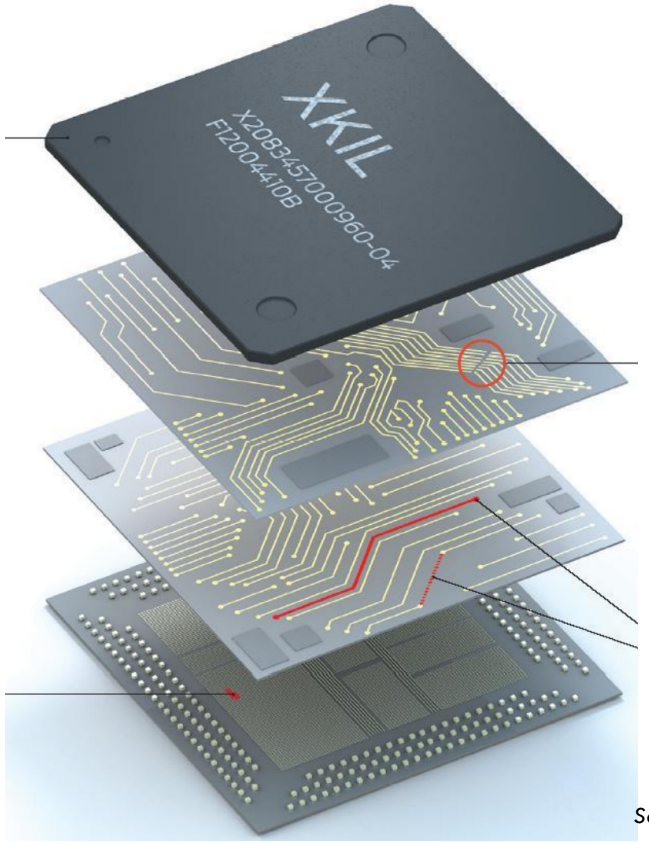


Abstraction Level

- *System Level*
- *Architectural Level*
- *RT Level*
- *Netlist Level*
- *Transistor Level*

- Resizing or deletion of existing transistors

Transistor Level Trojan



Source: *IEEE Spectrum*

ADD EXTRA TRANSISTORS

Adding just 1000 extra transistors during either the design or the fabrication process could create a kill switch or a trapdoor. Extra transistors could enable access for a hidden code that shuts off all or part of the chip.

CYBER CHALLENGE
CyberChallenge.IT

 Rel. 18.05.2020

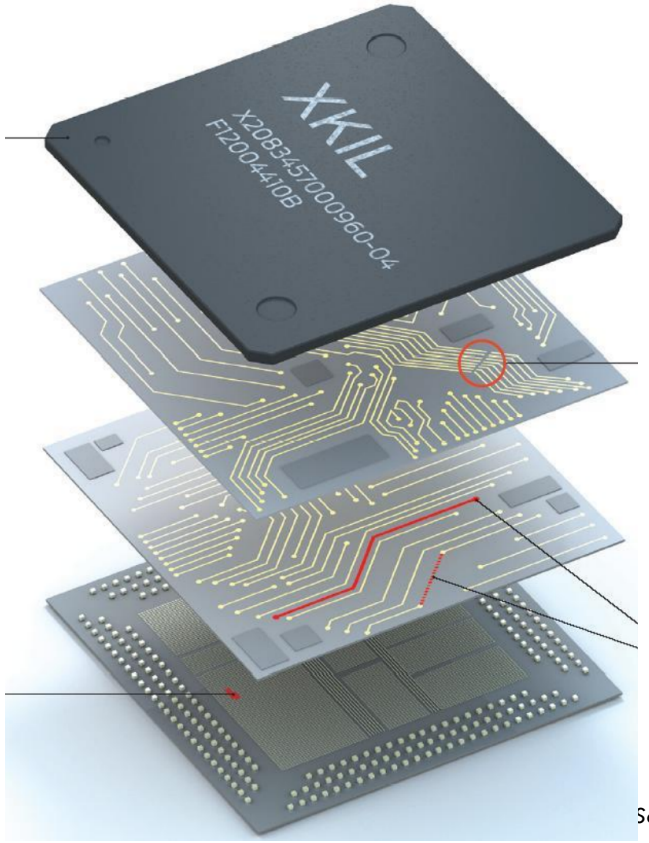
cini Cybersecurity National Lab

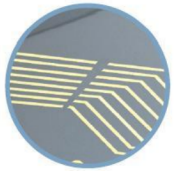
Abstraction Level

- *System Level*
- *Architectural Level*
- *RT Level*
- *Netlist Level*
- *Transistor Level*
- *Layout Level*

- Modification in transistors or layout
- Circuit is altered to affect reliability or correct functionality

Layout Level Trojan





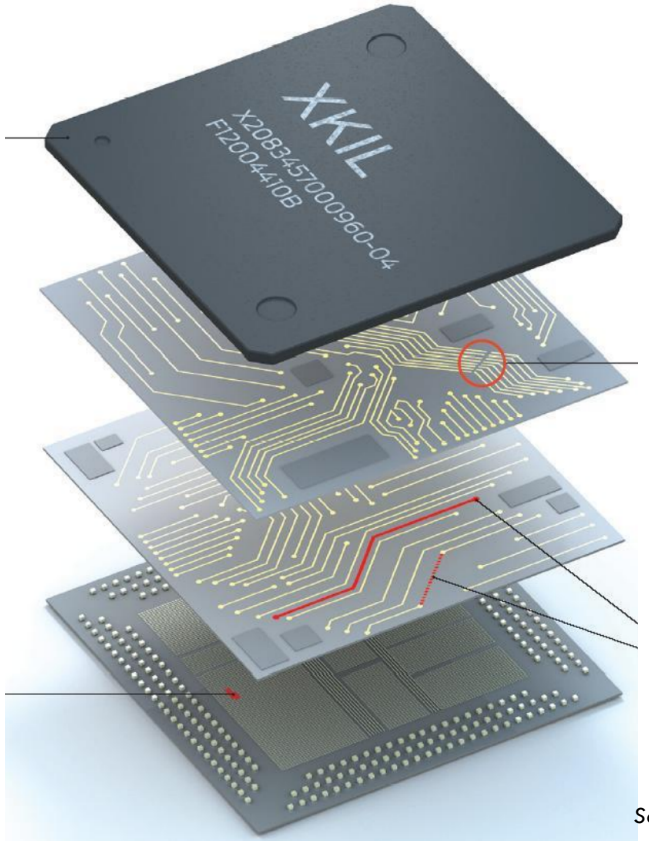
NICK THE WIRE

A notch in a few interconnects would be almost impossible to detect but would cause eventual mechanical failure as the wire became overloaded.

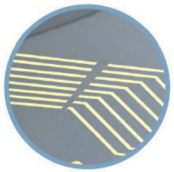
Source: *IEEE Spectrum*

 Rel. 18.05.2020

Layout Level Trojan



Source: *IEEE Spectrum*



ADD OR RECONNECT WIRING

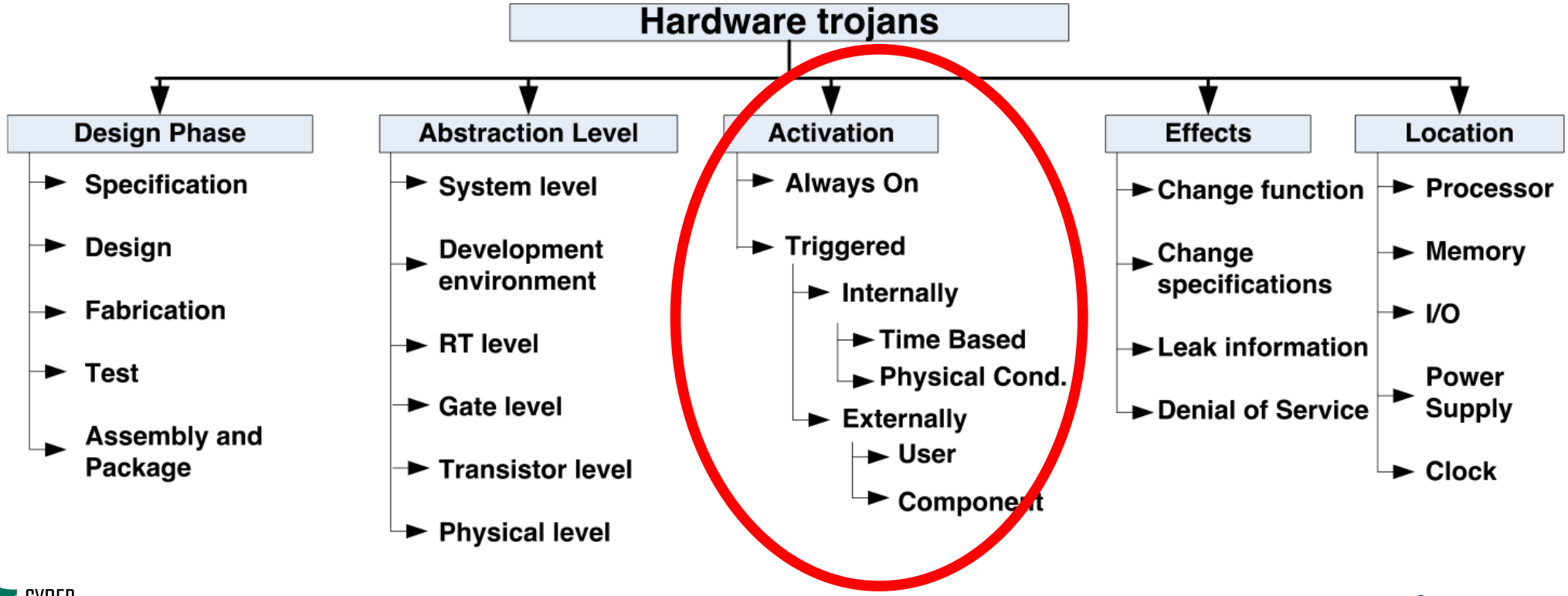
During the layout process, new circuit traces and wiring can be added to the circuit. A skilled engineer familiar with the chip's blueprints could reconnect the wires that connect transistors, adding gates and hooking them up using a process called circuit editing.

CYBER CHALLENGE
CyberChallenge.IT

 Rel. 18.05.2020

cini Cybersecurity National Lab

Hardware Trojan Taxonomy

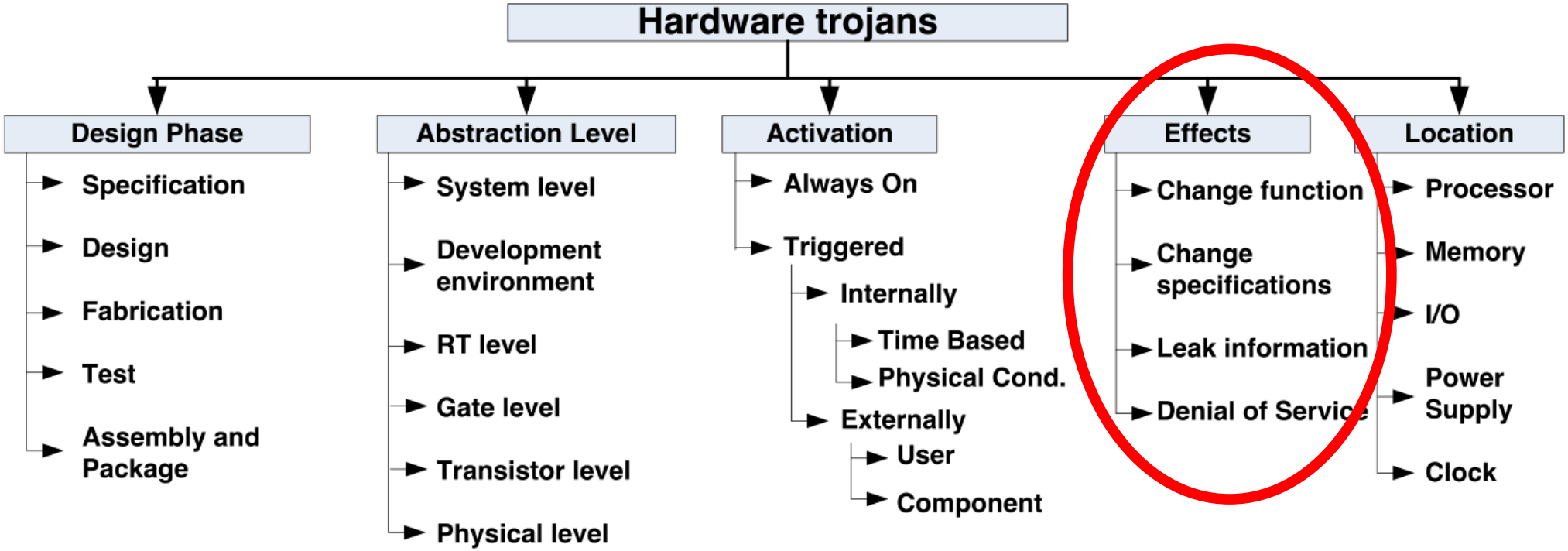


R. Karri et. al "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," IEEE Computer, vol. 43, no. 10, pp 39-46, 2010

Activation

- **Always On**:
  the Trojan is always active
- **Triggered**:
  the Trojan shows its effects only when activated.
  The activation condition can be
  - **Internal**: the Trojan waits for a sequence of one or more events that occur in the system. This condition is typically an internal logic state or a pattern of input/output signals.
  - **External**: the Trojan is activated by an external signal received, e.g., from an antenna or a sensor.

Hardware Trojan Taxonomy

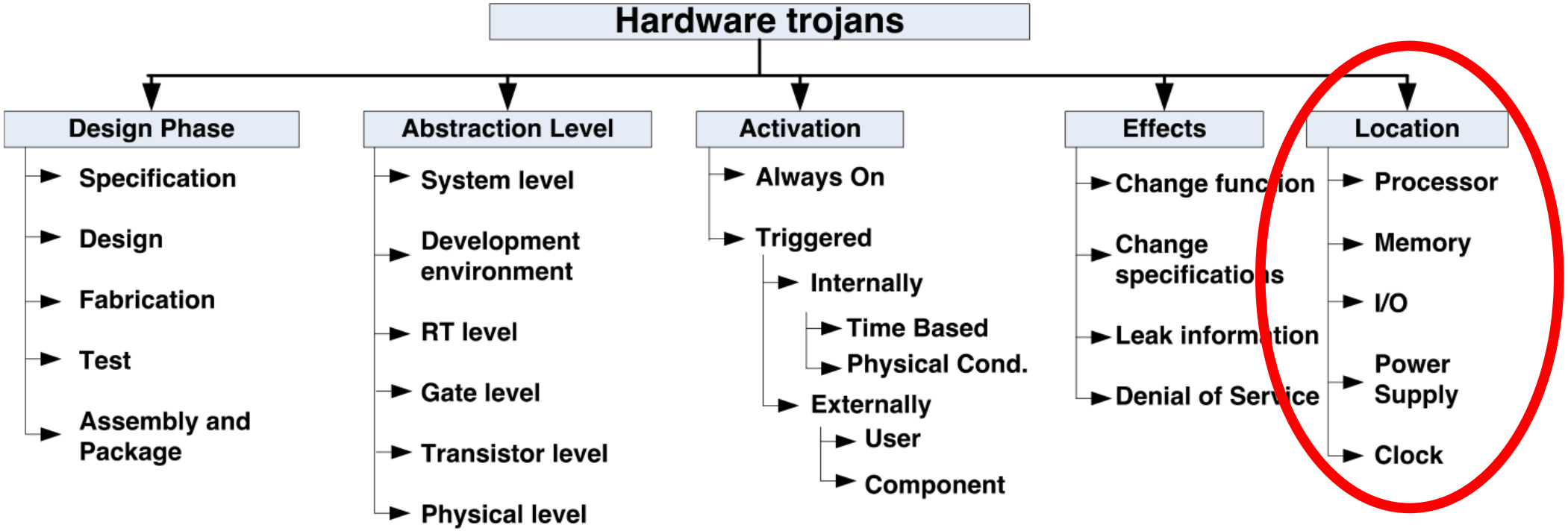


R. Karri et. al "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," IEEE Computer, vol. 43, no. 10, pp 39-46, 2010

Effects

- **Change in the functionality**:
  The Trojan can bypass, modify or delete existing logic, changing one or more of the device's functionalities
- **Reduced reliability**:
  The Trojan can alter the reliability of the chip by modifying characteristics of the circuit such as the length of a critical path or the power consumption
- **Denial of Service (DoS)**:
  The Trojan can alter some parameters of a device to exhaust resources or introduce computational delays.

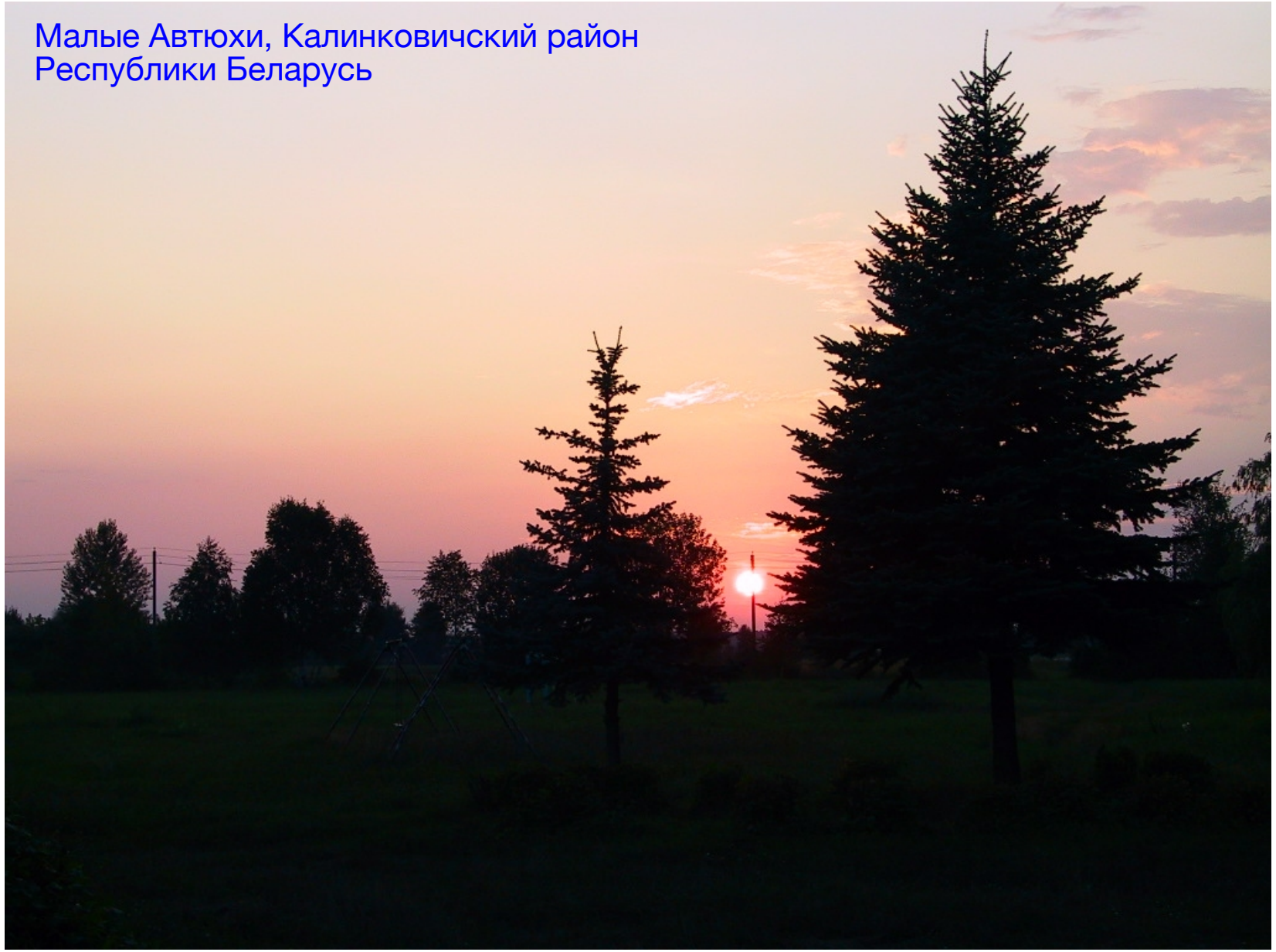
Hardware Trojan Taxonomy



R. Karri et. al "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," IEEE Computer, vol. 43, no. 10, pp 39-46, 2010

Location

- **Processor/microcontroller**:
  can be placed in the power or clock distribution grid to reduce reliability of or cause DoS attacks
- **Memory**:
  can modify address or enable/disable read/write operations
- **Input/output**:
  A Trojan placed here may have access to information exchanged between two devices, modify the communication or change the content of the exchanged data.



Малые Автюхи, Калинковичский район
Республики Беларусь

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE
CyberChallenge.IT

cini Cybersecurity National Lab

https://cybersecnatlab.it

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenture

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

B5

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DATA
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DGi ONE
the leading digital company

ICT CYBER CONSULTING