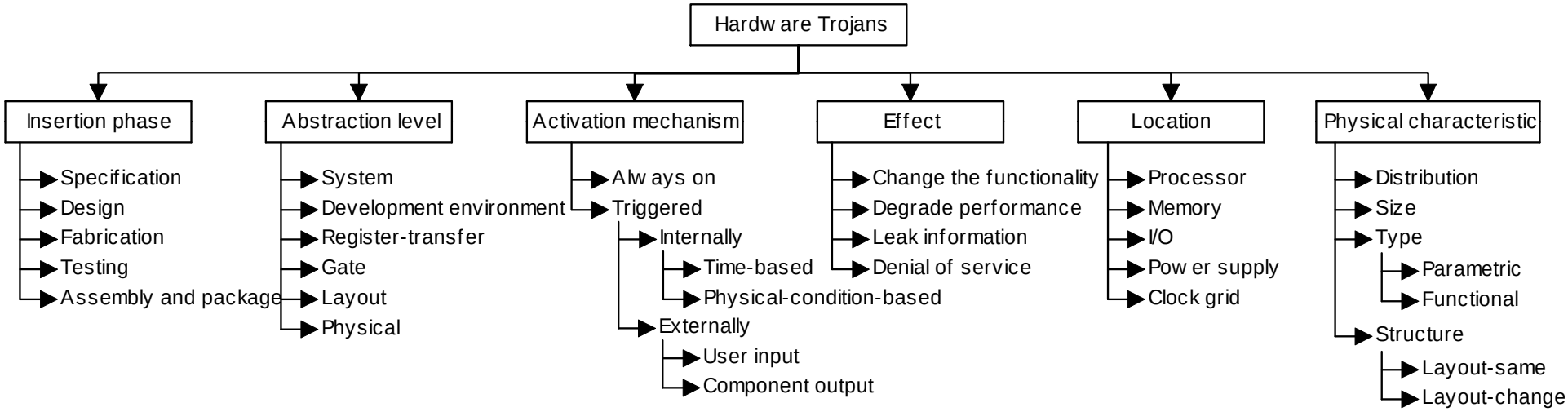
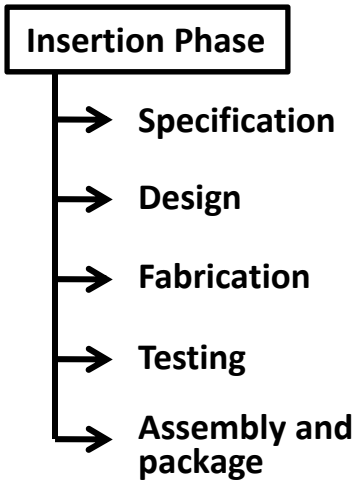
Trojan Taxonomy

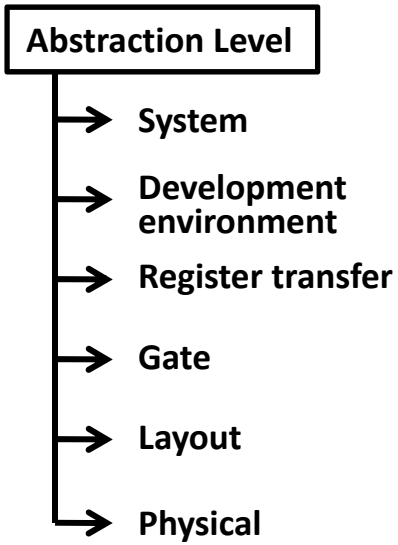


Trojan Taxonomy
Insertion phase



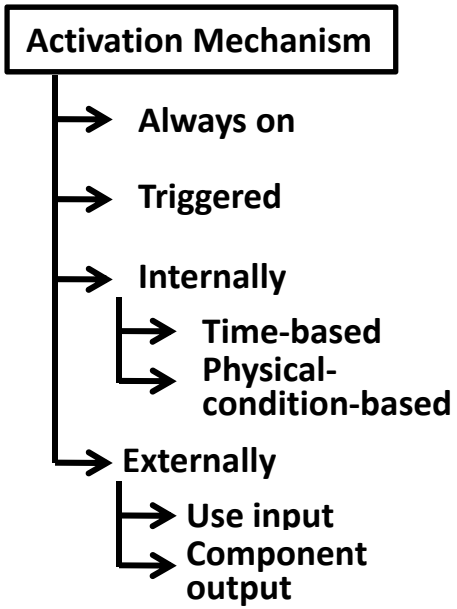
A Trojan can be introduced by changing the deign specification, like temperature, to degrade the design dependability. Design and fabrication stages are also subjected to tampering. A Trojan can be realized by adding some extra gates to a design's netlist or by changing its masks. Trojan insertion at the testing phase refers to trustworthy testing of a design after fabrication where an adversary may manipulate testing to keep an inserted Trojan undetected. Finally, unprotected interconnections between chips are prone to Trojan interference even if the chips are trustworthy by themselves. An unshielded wire connection could introduce unintended electromagnetic which an adversary can exploit for information leakage or fault injection.

Trojan Taxonomy
Abstraction Level



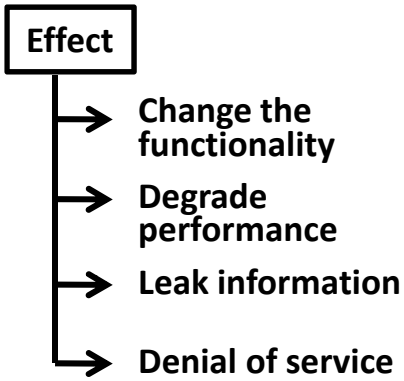
The level of abstraction determines the control of advisory on Trojan implementation. At the system level, a design is defined in terms of modules and interconnections between them, with an adversary being limited to the modules' interfaces and their interactions. At the development environment level, a Trojan can be inserted into the modules by taking advantage of CAD tools and scripting languages. In more details, each module is described in terms of signals, registers and Boolean functions at the register-transfer level. In this level, an adversary has full access to the functionality and implementation of the modules and can easily change them. A design is represented as a list of gates and their interconnections at the gate level. Here, an adversary can implement Trojans in details, and Trojans' gates and their interconnections can be decided. At the layout level, the impact of Trojans on design power consumption or its delay characteristics can be controlled. Trojans can be realized even by changing the parameters of an original circuit's transistors. Finally, all circuit components and their dimensions and locations are determined in physical level. A Trojan can be inserted in white/dead space of the design layout with the least impact on the design characteristics.

Trojan Taxonomy
Activation Mechanism



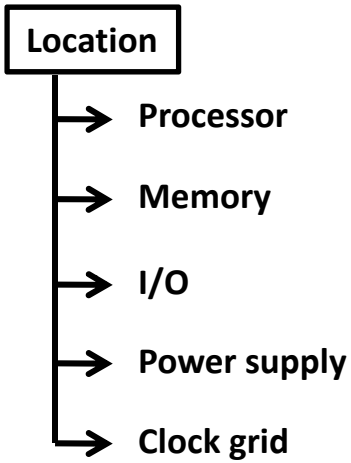
Trojans may always function, or they get conditionally activated. Always-on Trojans start as soon as their hosting designs are powered-on while conditional Trojans seek specific triggers either internally or externally to launch. The internal triggers can be timing-based (a Trojan is activated after certain time), or physical-condition-based (a Trojan is activated by certain events, e.g. specific temperature). The externally-triggered Trojans track user inputs or components' outputs, and the Trojans get activated if activation condition(s) are met.

Trojan Taxonomy
Effect



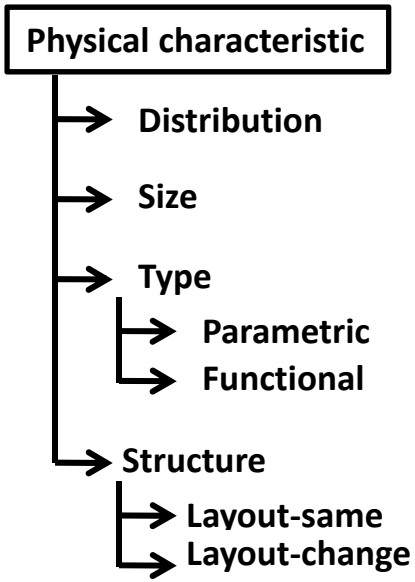
Trojans can be characterized based on their effects. They may change a design's functionality, for example, by modifying the data path of processor. Trojans can reduce the design performance or degrade its reliability by changing the design parameters. A Trojan may leak the secret key of a cryptographic processor or can cause the denial of a service for an authorized requested service at specific time.

Trojan Taxonomy
Location



Any part of a design is potentially subjected to Trojan insertion. A Trojan can be distributed over several parts or tightened in one part. A Trojan can tamper with a processor to obtain control over its controller or data path units. A Trojan in a memory can change stored values or block read/write accesses to the memory. On a Printed Circuit Board (PCB) including of several chips, an inserted Trojan on chips' interfaces can disturb communication. A Trojan can even affect the design power supply and alter current and voltage characteristics. Design delay characteristics can change with interrupting the clock grid by a Trojan. The Trojan can freeze part of clock tree and disable some functional modules.

Trojan Taxonomy
Physical characteristic



Trojan physical characteristics represent various hardware manifestations. A Trojan can be a functional or parametric type where functional Trojans are realized by transistors/gates addition or deletion and parametric Trojans by wire thickness or any other design parameter modification. The number of transistors/gates added or removed determines Trojan size. Trojan distribution indicates how loose or tight Trojan cells are placed in the physical layout. Trojan structure refers to possible modification of original physical design for Trojan cells placements.

Please send your concerns/questions to

Dr. Hassan Salmani at SalmaniHSN@gmail.com

Prof. Mohammad Tehranipoor at teharni@engr.uconn.edu