Hardware Trojan Taxonomy

Hardware Trojan Taxomony

- IC supply chain phase
- Activation
- Effects
- Location
- Type
- Size
- Layout
- Distribution

IC Supply Chain Phase

- **Design Phase**: Trojans introduced during the initial design, including IP cores or soft IPs.
- **Fabrication Phase**: Trojans inserted at the foundry.
- **Testing Phase**: Trojans embedded during testing, often hidden within testing patterns.
- **Packaging Phase**: Added in assembly and packaging.
- **Field Phase**: Trojans activated during the device's operational life, potentially with delayed effects.

Activation

- **Always on:** parametric HTs
- **Externally Triggered**: Activated by external inputs or signals, such as specific input patterns.
- **Internally Triggered**: Activated through internal conditions or states within the IC.
- **Environmentally Triggered**: Triggered by external environmental factors, like temperature or voltage.
- **Time-Triggered**: Activated after a specific time period or counter has been reached.

Effects or Payload

- Payload is the action or the damage that a HT will do once it is activated
- Change/ control of functionality
  - Killer switch, time bomb
- Leak sensitive information
  - Side channels: power, timing, optical, thermal, EM emission
- Reduce circuit reliability or lifetime
  - Parametric HTs, Trojans that will drain resources (power, CPU, bandwidth).

Location

- **Processing Units**: Trojans placed within the core processing units.
- **Peripheral Components**: Embedded in less secure peripherals, like I/O interfaces.
- **Memory Blocks**: Trojan circuits embedded within memory units for data access.
- **Interconnect**: Situated in data paths and interconnects, allowing manipulation of data in transit.
- **Power Supply Units:** change power supply to cause failure
- **Clock grids:** change frequency to cause fault or failure

Type

- Functional:
  - Addition/deletion of components
  - Modification of component’s functionality
- Parametric: damage reliability or increase the likelihood of performance failure
  - Thinning wires
  - Weakening of transistors or logic gates
  - Modification of power distribution network

Size

- Big functional blocks: sophisticated time bombs, powerful antenna
- Small gates: killer switch, small sensor

Layout

- **Need redu layout:** add functional blocks
- **No change:** parametric HTs

Distribution

- Tight/ centralized: big
- Loose/ distributed: small

Thankyou