HardSec
Hardware Trojan Lab

Lab#1

Due by 2/14/2017 (12:25 PM)

Contact TA: vj338@nyu.edu at ANY time

Lab#1: Hardware Trojan Lab

- GOAL: Insert Hardware Trojans in RC5 Design
  - At least 1 Key leaking Trojan
  - At least 1 temporary Denial of Service or Functionality changing Trojan
  - Be creative
- Trojan cannot be in behavioral code – Needs to be described in LUTs, FFs, or any Xilinx primitives
- 2 students per team (Submit only 1 submission)

Lab#1: Hardware Trojan Lab

- STEPS:
  - Get the initial mapping of RC5 design on your FPGA
    - → Submit screenshot of Planahead/FPGA Editor
  - Insert the Trojan in the areas not occupied by the original design
    - → Study and report the effects of Trojan on original design
      - Area Impact: Increase in LUTs, FFs, IO Pins, and etc
      - Performance Impact: Change in critical path delay/max freq, and etc
  - Get the mapping of Trojan-infected RC5
    - Study and report how the Trojan changes the original mapping
    - Try to get the RC5 to remain in its originally mapped place
      - → If the mapping of RC5 in Trojan-infected design is same as original RC5 mapping (full points)

Lab#1: Deliverables

- **A single PDF report with the following contents:**
  - Trojan design details
    - How it is activated
    - What it does
    - Resources utilized
  - Screenshot of Planahead/FPGA Editor:
    - → The initial mapping of RC5 design on your FPGA
    - → After Trojan insertion
  - Analysis of RC5 with Trojan
- **VHDL/Verilog Codes in a Zip file (Original RC5 design and Trojan-infected RC5)**

Lab#1: Study Materials

- CLB Architecture:
  http://www.xilinx.com/support/documentation/user_guides/ug474_7Series_CLB.pdf
  - See Page 9, 17-22
- Xilinx primitives and library guide:
  http://www.xilinx.com/support/documentation/sw_manuals/xilinx14_1/7series_hdl.pdf
  - See Page 65-70 for list of primitives. For LUT6: See Page 269
- Xilinx Constraints Guide:
  http://japan.xilinx.com/support/documentation/sw_manuals_j/xilinx14_7/cgd.pdf
  - See page 142- 144, 147-157 for LOC constraint
  - See page 57-59 for BEL constraint
- Sample low level modelling code can be found at:
  https://github.com/IamVNIE/Hardware-Security
- Presentation used in Lecture (1/31):
  http://isis.poly.edu/~vinayakj/documents/Hardware%20Security%20Trojan%20Presentation.ppt