Class Project

Due No Due Date **Points** 0

Purpose

This assignment introduces students to the design and assessment of hardware security. Students will implement, as a team, a functional design on an FPGA and compromise it with a stealthy Trojan circuit. This will improve both their ability to implement hardware and ability to think adversarially. Finally, students will expand their ability to detect threats by trying to find a Trojan implemented by a peer team.

Task

Students will design a novel and stealthy hardware Trojan which they will implement into a circuit design. A good Trojan should have a clear trigger (i.e. there should be some way to activate the Trojan, it should not always be on), contain a payload that compromises the normal operation of the circuit (i.e. should do something with adverse effects to the circuits users), and should be stealth (i.e. the Trojan should not be trivially detectable).

Students will try and discover another teams Trojan horse.

Working in your lab groups, students will do the following:

- Milestone 1: Choose a logic block, interactive environment on the basis board, and a future Trojan to implement into the design. Function(s) and Trojans must be approved by instructors and should be of sufficient complexity to be interesting. Get verbal approval for your design and Trojan.
  - A set of basic modules will be provided for students to use. Additional functionality will needed to be added to these circuits to make them useful in some way.
  - Students may select other designs of their own creation or from those found online. All designs must be approved by the professor.
  - The Trojan should have a clear trigger, interesting payload, and attempt to remain stealthy.
  - Get verbal approval for your design and Trojan! Your professor will mark you off for credit for this milestone.
- Milestone 2: Two short write-ups
  - A short 1-2 page write up of the above, detailing your logic block's specification and how to interact with it on the Basis board. Think of this as your project's user manual. This will be provided to the student team that will hunt for your Trojan.
  - A second write-up (either as a separate document or as additional text in the above) detailing your Trojan's trigger and payload.
  - You will submit both documents through Canvas for this milestone.

- Milestone 3: Implement your designed block correctly.
  - Demonstrate your working circuit to your professor for credit for this milestone.
- Milestone 4: Implement and test your Trojan.
  - Demonstrate your working circuit to your professor for credit for this milestone.
  - Additionally, you will submit your project through Canvas to be distributed to other teams. Include a short write-up detailing the location of the Trojan in your implementation.
- Milestone 5: Search for the Trojan horse in another other team's project! Students will be given the specifications, code, and implementation of another teams logic-block with a Trojan. They will use test techniques to search for and identify discovered vulnerabilities.
  - To put a sane limit on the time spent on the Hunt, teams will only be expected to hunt for the Trojan during Tuesday Lab in the last week of class.
  - For credit, you will give a short presentation on Thursday of the last week of class on the circuit you received, how you went about hunting for the Trojan, and what you believe to be the Trojan circuit in your given design.
- Milestone 6: Write-up results. Write a report with all relevant results from above. Include a discussion on how the Trojan could be used in an attack, i.e. what type of attacker would use this to attack what type of system to accomplish what? If in doubt, discuss with instructors and err on the side of including things.
  - This will be submitted through Canvas during Finals Week.

See Course Schedule (https://canvas.calpoly.edu/courses/111634/pages/course-schedule) for timeline