HOST 2022 Microelectronics Security Challenge: IP Security Track

Jiafeng Xie, Aviv Barkai, and Ujjwal Guin
Emails: jiafeng.xie@villanova.edu, aviv.barkai@intel.com, ujjwal.guin@auburn.edu

Overview: The threats toward hardware IP come from many malicious sources, including side-channel information leakage and fault injection attacks. The side-channel attacks using power analysis can expose a cryptosystem's secret and have been studied extensively over the past two decades. Differential power analysis exploits the correlation between leakage power with the input data. The fault attacks mainly refer to injecting malicious faults to the hardware IP by the hackers for possible critical message corruption/stealing. Both attacks are harmful to the hardware IP design community and have recently drawn significant attention from various parties. With this perspective, we propose launching a competition to enable the student community to analyze a vulnerable IP and then implement patches to address the threat.

IP overview: The IP will be an AES core. Details will be provided in the challenge directory.

Participating groups will implement the AES core into an FPGA system, using side channel analysis including different power analysis and fault injection methods, collect leakage information. The groups will then propose and implement countermeasures to defend against the proposed attack methods and demonstrate the results.

Groups will write their report in clear, brief format, either as a presentation or as a document (MS Word or any other kind).

Submission Criteria:

- The participants are required to submit a zip file containing codes, sample submission, demo, and presentation. The file name should be “team_name_HOST_2022_IPS.zip using OneDrive.
- The report should be clear. It may be prepared as a presentation or document including the following:
  - **Explanation of system setup**: At least one image, and brief explanation of the type of board, type of setups, probes and anything else used for the work.
  - **Vulnerabilities and weaknesses:** List security issues found in the AES core and its implementation. Brief explanation as necessary.
  - **Mitigations:** List of mitigations. Brief explanation as necessary.
  - **Code:** Code for mitigations (as appendices) and anything else you think necessary to understand your work.
  - **Demo:** A demo video link (upload in OneDrive). The video should demonstrate finding an issue and/or proving a mitigation.
    - **Demo time limit**: maximum - 30 mins. Recommended – few minutes.
- **In-person demonstrations:** Qualified groups will be invited to attend HOST’22 and demonstrate the designed crypto core in-person. Teams may also qualify for travel support. There will be a final evaluation as well during the in-person demonstration time.

Evaluation Criteria:

Total: 100 pts

- Vulnerabilities – 50 pts
  - Simple power analysis – 10 pts

    Details of the simple power analysis such as power variation figures, how the information leakage is obtained from power variations, etc.

  - Differential power analysis – 15 pts

    Details about how the differential power analysis is carried out and how the key information leakage is observed (etc.) need to be provided

  - Simple fault analysis – 10 pts

    Specify the fault attack model, attack procedure, and the attack outcome related to the information leakage

  - Differential fault analysis – 15pts

    Describe the fault attack model, attack strategy, and the attack result

- Mitigations and improvements – 50 pts (based on the discovery in the Vulnerabilities)
  - Countermeasures with simple power analysis – 10 pts

    Provide the strategy to defend against simple power analysis (connecting with related Vulnerability Section)

  - Countermeasures with differential power analysis – 15 pts

    Provide the countermeasure design details and the defense result (note: if this countermeasure is developed, then the points for designing countermeasure for simple power analysis is automatically awarded)

  - Countermeasures with simple fault attack – 10 pts

    Provide the strategy to defense, connecting with the corresponding simple fault attack part of the Vulnerability Section.

  - Countermeasures with differential fault attack defense – 15 pts

    Details of designing countermeasures for differential fault attack defense (note: if this countermeasure is developed, then the points for designing countermeasure for simple fault attack is automatically awarded)

Additional notes:

Evaluation criteria subject to minor changes until the beginning of competition.

Extra points may be assigned for work exceeding what was asked.

Poorly written, unclear reports may be rejected.