# Microelectronics Security Competition

**1. Objective:** The microelectronics security competition at HOST aims to promote hardware security, provide the students with exposure to the community and prospective employers, and support interaction between academia and industry. The vision of this competition is to bring the stakeholders together in a unique experience, in which experts from industry and government will craft security challenges which represent real problems with genuine interest in their solutions. These challenges will be given to different research teams from academia to find innovative solutions. Successfully implemented solutions will be demonstrated at HOST, reviewed with team of experts, and best solutions will be awarded. This microelectronics security competition plans to include security assessments from intellectual properties (IP), system on a chip (SoC), and microelectronic supply chain.

**2. IP Security Track:** 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 power consumptions and 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.

**3. SoC Security Track:** Modern computing systems extensively use System-on-Chips (SoCs), usually integrated with multiple Intellectual Property (IP) cores. The integration of different IPs has created distinctive security challenges while interacting among themselves. When IPs cores are connected within an SoC, additional security bugs may arise even if the individual IPs are verified to be secure. Hardware vulnerabilities can be introduced within a design due to incorrect/ambiguous specifications, which results in designers misinterpreting the design functionality, design mistakes such as setting a global variable to true when it should be false, and/or flawed implementations such as including knowingly insecure cryptographic cores that can be easily attacked. MITRE maintains a Common Weakness Enumeration (CWE) database [1] for vulnerabilities exploited by adversaries. These include issues in debug and test, peripherals and on-chip fabric, core and computing, etc. Trust-Hub also includes 50+ security properties to be checked [2]. With this perspective, we propose launching a competition so that students can analyze SoC and perform security analysis to identify SoC vulnerabilities and propose effective countermeasures.

**4. Supply Chain Security Track:** The lack of traceability in the globalized electronics supply chain results in the infiltration of various counterfeit electronic parts, including recycled, remarked, overproduced, cloned, out-of-spec/defective, forged documentation, and tampered types and pose a severe threat to the security of our critical infrastructures. Among them, recycled, remarked, and cloned parts constitute most counterfeit incidents. Over the years, a class of solutions has been proposed to mitigate the widespread infiltration of these fake parts. Physical Inspection methods have gained a lot of attention due to their one-size-fits-all nature as the same methods can be applied to all types of parts (analog, digital, memory, FPGAs. etc.). Among various modalities, including optical, X-ray, thermal, electron beam microscopy, etc., optical imaging is one of the fastest and most affordable modalities. We propose a competition to analyze different modalities images from various SoC

components and perform security analysis with this perspective. Competitors are encouraged to collect and use their own images for the competition. A dataset will be also provided by the committee.

## Eligibility

Graduate and undergraduate students

## Competition Process

**Step1: Registration.** Research groups are invited to register as "***teams***" for "***one or more***" of the tracks.

**Step2: Phase-1**. The competition materials for different tracks will be released to all the participants. Each participating group will be required to perform the respective tasks for their tracks. The participating groups are required to prepare a detailed report.

**Step 3: Judges' first-round review**. The returned reports and codes will be evaluated by experts and go through specific criteria to determine the final candidates. The selected teams will then be invited to attend Phase-2. The students may be eligible for travel grants.

**Step 4: Phase-2**. Additional tasks will be given to the selected groups at the HOST venue. Judges will test and evaluate the performance.

## Important Dates

**Current:** Registration is open. See submission information below.

**February 1st, 2023:** Phase-1 starts

**March 1st, 2023:** Phase-1 report due

**April 1st, 2023:** Phase-1 result

**May 1st, 2023:** Phase-2 starts

**May 4th, 2023:** Phase-2 ends, and winners will be declared at the social event

## Travel Support and Recognition

Finalist teams will be provided with some travel support. Winning teams will be recognized at the HOST closing session.

## Submission Information

Please make a new submission to one of the **HOST 2023 Microelectronics Security Competition – IP Security, SoC Security, or Supply Chain Security** tracks at https://easychair.org/conferences/?conf=host2023 with the following **required** information.

Title: Name of your team

Abstract: NA

Keywords: Mention three keywords

Files: Not required

## Contact Information

**HOST Microelectronics Security Competition Chairs:** Eslam Tawfik and Mohamed El-Hadedy (Aly)

**E-mail:** tawfik.10 at osu.edu; mealy at cpp.edu