Microelectronics Security Challenge

1. Objective: The microelectronics security challenge 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. Engineering disciplines such as Electrical and Computer Engineering and Computer Science are actively involved in ensuring the design, fabrication, and security of electronic hardware and providing a critical workforce to build and maintain the U.S. semiconductor supply chain. To promote security awareness among the students enrolled in engineering, it is essential to gain necessary hardware security skills such as a theoretical understanding of threats from untrusted semiconductor design, manufacturing, and test, and then design preventive measures to mitigate the threats. This microelectronics security challenge plans to include security assessments from intellectual properties (IP), system on a chip (SoC), and electronic supply chain.

2. IP Security Track (Track Co-Chair: Jiafeng Xie): 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.

3. SoC Security Track (Track Co-Chair: Kanad Basu): 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. The individual IP cores may contain security-threatening bugs. However, when they are connected within an SoC, additional security bugs may arise even if the individual IP cores are verified as secure. A vulnerable design results from a security bug that escapes the verification phase. 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. An adversary can exploit these vulnerabilities to launch an attack on a secure system. MITRE maintains a Common Weakness Enumeration (CWE) database [2] for vulnerabilities exploited by adversaries. These include issues in debug and test, peripherals and on-chip fabric, core and computing, etc. It is thus imperative to perform a thorough security assurance before a product is shipped. Trust-Hub also includes 50+ security properties to be checked [3]. With this perspective, we propose launching a competition so that students can analyze SoC and perform security analysis.

4. Supply Chain Security Track (Track Co-Chairs: Navid Asadi and Yousef Iskander): 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 optical images from various SoC components and perform security analysis with this perspective.

5. Eligibility

Graduate and undergraduate students

6. Competition Process

Step 1: 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 2: 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 3: Phase-2. Additional tasks will be given to the selected groups at the HOST venue. Judges will test and evaluate the performance.

7. Important Dates

April 15, 2022: Phase-1 starts
May 15, 2022: Phase-1 report due
May 18, 2022: Phase-1 result
June 27: Phase-2 starts
June 28: Phase-2 ends, and winners will be declared at the social event.

8. Submission Site: https://easychair.org/conferences/?conf=ieeehost2022 (Please make a new submission and choose one of the **HOST 2022 Microelectronics Security Competition – IP Security/ SoC Security/Supply Chain Security** tracks)

9. Contact Information

HOST Microelectronics Security Competition Chair: Ujjwal Guin

E-mail: ujjwal dot guin at auburn dot edu