IEEE CTSoc Chapter MP- section: Technical Talk

28th April 2023, 2.00 PM IST

1. **Speaker name: Dr. Chester Rebeiro**

2. **Speaker Bio:** Dr. Chester Rebeiro is an Associate Professor at the Indian Institute of Technology, Madras. Prior to this he was a postdoctoral researcher at Columbia University. He has a Ph.D. from IIT Kharagpur in the area of hardware security. Before joining IIT Kharagpur, he worked as a Member Technical Staff at CDAC, Bangalore. His area of interests includes security aspects in the operating system, architecture, and VLSI. He is particularly interested in applying learning algorithms and formal methods to analyze the security of systems. He is an author of a book entitled "Timing Channels in Cryptography" and also holds two patents. He is an associate editor of Springer Journal of Hardware and Systems Security (HASS).

3. **Title of talk:** Hardware Security and Side Channel Analysis

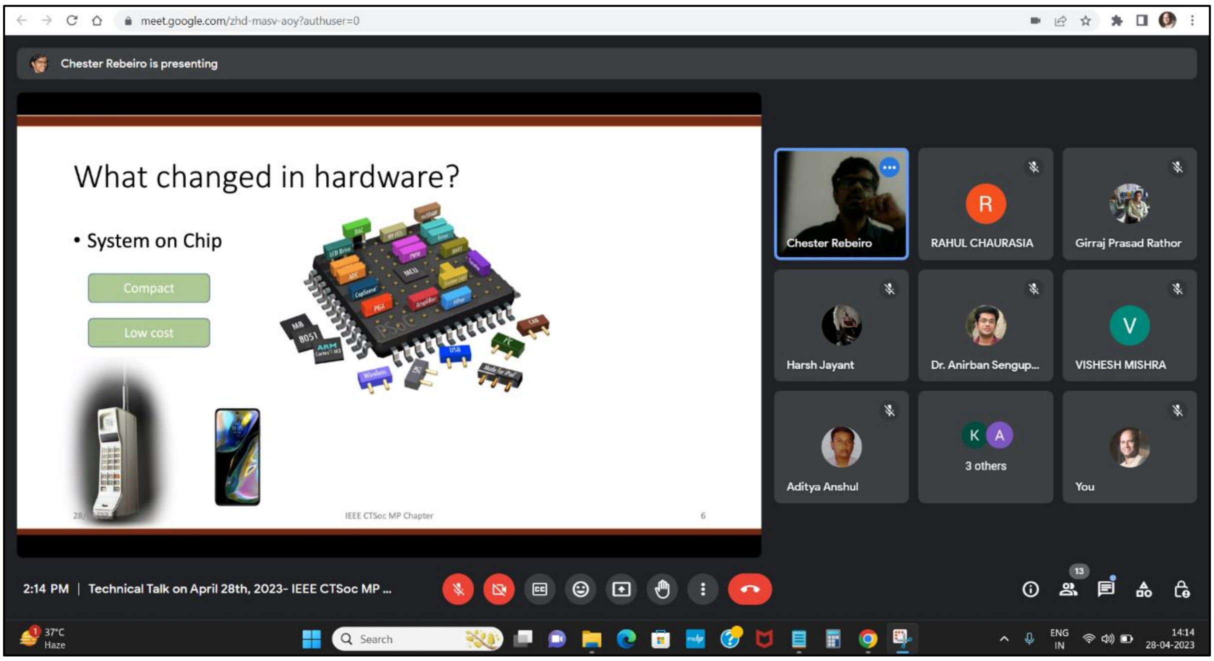
4. **Abstract of talk:** The design and development of semiconductor chips is a vastly complex and involved process. The recent trend is to involve several organizations from chip design to fabrication. While this has greatly reduced costs and time to market, it has opened new security threats. The first part of the talk will discuss various attack vectors that originate due to the distributed hardware security development process. We will dwell into the various causes of the attacks and discuss potential solutions. The second part of the talk will discuss side-channel analysis attacks. These potent attacks make use of a device's power consumption to glean secret information. These attacks can break cryptographic keys from ciphers like the AES or RSA, within a few hours. We will discuss recent works from IIT Madras, where we identify the root cause of side-channel leakage in a processor, and present the first side-channel resistant processor.

5. **Date and time:** April 28th, 2023, Time: 2:00 PM IST

6. **Meeting Venue:** meet.google.com/zhd-masv-aoy

7. **Number of participants: 13**

8. **Event Photo:**



What changed in hardware?

- System on Chip

Compact

Low cost

IEEE CTSoc MP Chapter 6

*****