A Zero Trust Architecture for Semiconductor Supply Chain

The semiconductor supply chain as depicted in Figure 1, is vulnerable to security threats from untrusted participants involved in the network. These threats involve, but are not limited to hardware Trojan insertion, cloning, intellectual property (IP) theft and piracy, bitstream tampering, insider threats, etc. There have been well-documented cases of counterfeit chips and chips implanted with Trojans infiltrating the supply chain. According to a report published by the Alliance for Gray Market and Counterfeit Abatement (AGMA) in December 2020, there has been a 254% increase in counterfeit chips. It is also reported that 15% of the spare and replacement parts purchased by the Pentagon for the U.S. Department of Defense (DoD) turn out to be counterfeits. As a result, significant research is being conducted to secure the integrity of the semiconductor supply chain.

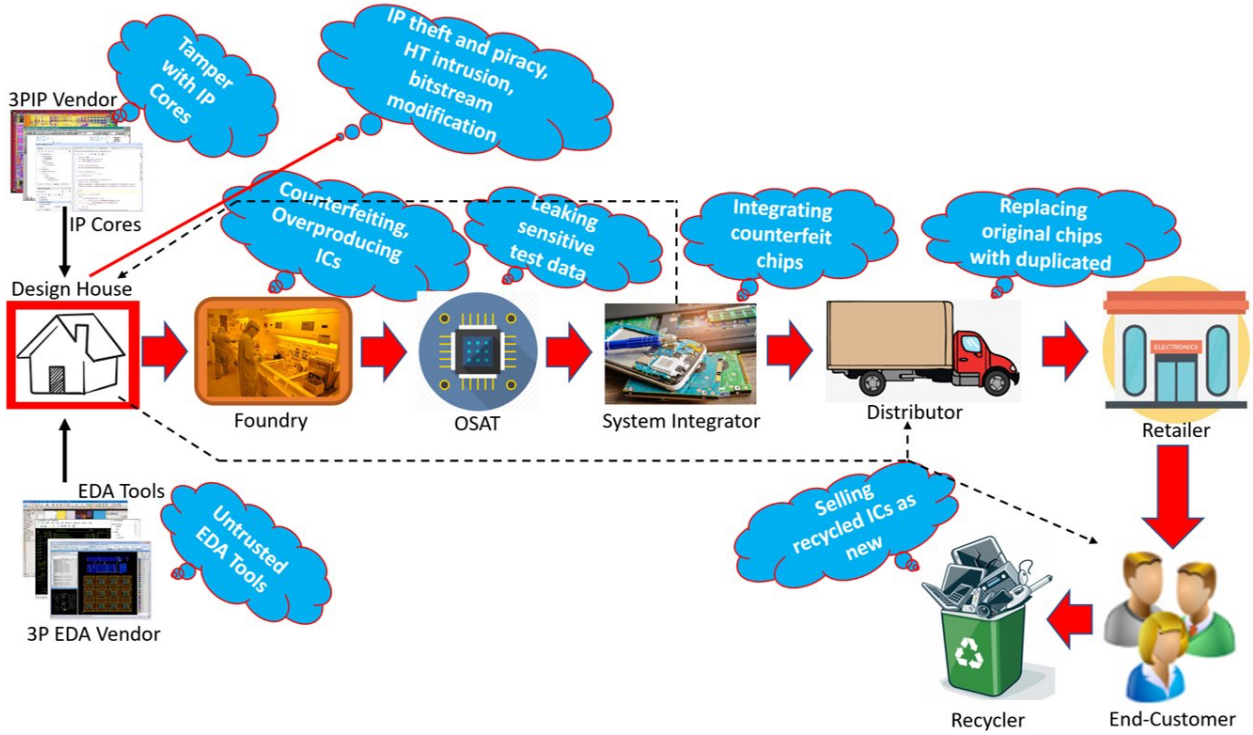

Figure 1: A typical semiconductor supply chain and security threats on it

Our work aims to establish a zero trust semiconductor supply chain by leveraging blockchain and ring oscillator physical unclonable functions (ROPUFs). The zero trust principles draw inspiration from the zero trust tenets outlined by the National Institute of Standards and Technology (NIST). Blockchain's features such as smart contracts, tracking and tracing capabilities, and immutability are used for authentication and access control of users while the unique challenge-response pairs (CRPs) generated by ROPUFs are employed to validate the semiconductors.

The proposed zero trust architecture for the semiconductor supply chain, as depicted in Figure. 2, integrates various components and mechanisms to ensure authentication, access control, traceability, and security. The authentication and access control of the users is mainly done through the blockchain enabled MFA while the semiconductor chip is authenticated using the

unique CRPs obtained from ROPUF. The transactions performed in the network are updated on the shared blockchain ledger and hence are trackable and traceable. To maintain confidentiality and integrity of the assets, features offered by the blockchain are utilized. Furthermore, this work enforces that all the devices used in the network are updated with the latest security patches and all source codes are developed taking into consideration the concepts of secure coding, thus adhering to the ZT compliance. The zero trust policy engine evaluates and enforces all the policies formulated for the architecture. Upon enforcement of the protocols, access to the network resources is either allowed or blocked, depending upon the evaluation of the policies laid and their implementation. With these protocols in place, everything that enters the network to fetch access to the resources is verified and authenticated, with the aim to ideally leave no room for an untrusted element to enter the network.

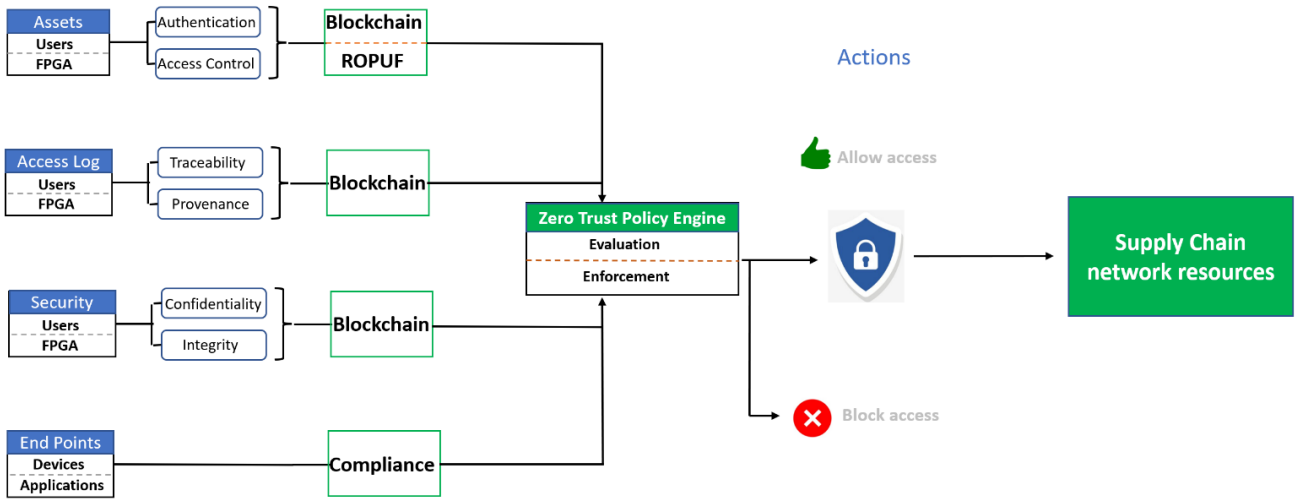

Figure 2: The Zero Trust Architecture for semiconductor supply chain security

Bios

Dr. Akshay Kulkarni works as a postdoctoral research associate at the ECE department at University of Florida, Gainesville, FL. He earned his Ph.D. from the University of Toledo, OH under the supervision of Dr. Mohammed Niamat. His research interests include IC supply chain, application of Blockchain, Zero Trust, and NFTs for assured and trusted digital microelectronics.

Dr. Mohammed Y. Niamat received the bachelor's degree in electrical engineering from the Aligarh Muslim University, India, the master's degree in electrical engineering from the University of Saskatchewan, Canada, and the Ph.D. degree from the University of Toledo, OH, USA. During 1996-1997, he was a Visiting Associate Professor at Stanford University. He has supervised more than 50 graduate students including Akshay Kulkarni.