Securing against Malicious Hardware Trojans

Sanjay Goel  
School of Business  
University at Albany, SUNY  
Albany, New York

John Hartley  
Nanoengineering Constellation  
Colleges of Nanoscale Science and Engineering  
Albany, New York

Yuan Hong  
School of Business  
University at Albany, SUNY  
Albany, New York

Hardware Trojans are malicious components of integrated circuits that are inserted into chips during the design and fabrication process. These Trojans can make the chip fail at critical moments, generate false signals or create a backdoor that helps in stealing information. Hardware Trojans have existed for at least a decade and an oft-cited example is the failure of Syrian radars of an incoming airstrike through a backdoor inserted into the radar chip. The architecture of the chips is very complex resulting in an intricate supply chain where multiple parties are involved in the design and fabrication of chips; consequently, there are multiple vulnerable points where hardware Trojans can be inserted. There is ongoing research on identifying Trojans in the hardware through testing of properties of the chips or at the design level by examining the integrity of the design at different stages. In this paper, we lay out the design and manufacturing processes of the chips and discuss the vulnerabilities in the process that can lead to compromise of the chips. We also discuss the current research in detection of hardware Trojans and securing the design. Finally, we lay out a research agenda for the future.

The full version will be made available online through the ASIA website at: http://www.albany.edu/iasymposium