Detecting and thwarting hardware trojan attacks in cyber-physical systems

Abstract

Cyber-physical system integrity requires both hardware and software security. Many of the cyber attacks are successful as they are designed to selectively target a specific hardware or software component in an embedded system and trigger its failure. Existing security measures also use attack vector models and isolate the malicious component as a counter-measure. Isolated security primitives do not provide the overall trust required in an embedded system. Trust enhancements are proposed to a hardware security platform, where the trust specifications are implemented in both software and hardware. This distribution of trust makes it difficult for a hardware-only or software-only attack to cripple the system. The proposed approach is applied to a smart grid application consisting of third-party soft IP cores, where an attack on this module can result in a blackout. System integrity is preserved in the event of an attack and the anomalous behavior of the IP core is recorded by a supervisory module. The IP core also provides a snapshot of its trust metric, which is logged for further diagnostics.