World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:18, No:01, 2024

Investigating Message Timing Side Channel Attacks on Networks on Chip with Ring Topology

Authors : Mark Davey

Abstract : Communications on a Network on Chip (NoC) produce timing information, i.e., network injection delays, packet traversal times, throughput metrics, and other attributes relating to the traffic being sent across the chip. The security requirements of a platform encompass each node to operate with confidentiality, integrity, and availability (ISO 27001). Inherently, a shared NoC interconnect is exposed to analysis of timing patterns created by contention for the network components, i.e., links and switches/routers. This phenomenon is defined as information leakage, which represents a 'side channel' of sensitive information that can be correlated to platform activity. The key algorithm presented in this paper evaluates how an adversary can control two platform neighbouring nodes of a target node to obtain sensitive information about communication with the target node. The actual information obtained is the period value of a periodic task communication. This enacts a breach of the expected confidentiality of a node operating in a multiprocessor platform. An experimental investigation of the side channel is undertaken to judge the level and significance of inferred information produced by access times to the NoC. Results are presented with a series of expanding task set scenarios to evaluate the efficacy of the side channel detection algorithm as the network load increases.

Keywords : embedded systems, multiprocessor, network on chip, side channel
Conference Title : ICSOC 2024 : International Conference on System on Chip
Conference Location : London, United Kingdom
Conference Dates : January 15-16, 2024