Earthquake ? A NoC-based optimized differential cache-collision attack for MPSoCs

Title	Earthquake ? A NoC-based optimized differential cache-collision attack for MPSoCs
Publication Type	Conference Paper
Year of Publication	2018
Authors	Reinbrecht, Cezar, Forlin, Bruno, Zankl, Andreas, Sepulveda, Johanna
Conference Name	2018 Design, Automation Test in Europe Conference Exhibition (DATE)
Keywords	attack efficiency, cache activity, cache line, cache location, cache memories, cache storage, Computer architecture, cryptography, earthquake attack, Earthquakes, Encryption, Glass, Metrics, microprocessor chips, MPSoC configurations, MPSoC Glass, multiprocessing systems, network on chip security, network-on-chip, Network-on-Chip communication structure, NoC, on-chip connectivity, optimized differential cache-collision attacks, optimized variant, programming flexibility, pubcrawl, resilience, Resiliency, Scalability, security concerns, Security NoC, system-on-chip, Systems-on-Chips, Timing, Timing attack, timing measurements, Timing Side-channel Attack
Abstract	Multi-Processor Systems-on-Chips (MPSoCs) are a platform for a wide variety of applications and use-cases. The high on-chip connectivity, the programming flexibility, and the reuse of IPs, however, also introduce security concerns. Problems arise when applications with different trust and protection levels share resources of the MPSoC, such as processing units, cache memories and the Network-on-Chip (NoC) communication structure. If a program gets compromised, an adversary can observe the use of these resources and infer (potentially secret) information from other applications. In this work, we explore the cache-based attack by Bogdanov et al., which infers the cache activity of a target program through timing measurements and exploits collisions that occur when the same cache location is accessed for different program inputs. We implement this differential cache-collision attack on the MPSoC Glass and introduce an optimized variant of it, the Earthquake Attack, which leverages the NoC-based communication to increase attack efficiency. Our results show that Earthquake performs well under different cache line and MPSoC configurations, illustrating that cache-collision attacks are considerable threats on MPSoCs.
DOI	10.23919/DATE.2018.8342090

Citation Key reinbrecht_earthquake_2018

pubcrawl network on chip security Scalability Resiliency resilience Metrics attack efficiency cache activity cache line cache location cache memories cache storage computer architecture Cryptography earthquake attack Earthquakes encryption Glass microprocessor chips MPSoC configurations MPSoC Glass multiprocessing systems network-on-chip Network-on-Chip communication structure NoC on-chip connectivity optimized differential cache-collision attacks optimized variant programming flexibility security concerns Security NoC system-on-chip Systems-on-Chips timing Timing attack timing measurements Timing Side-channel Attack