IE-Cache: Counteracting Eviction-Based Cache Side-Channel Attacks Through Indirect Eviction

Khurram Bhatti
Information Technology University (ITU), Lahore, Pakistan
Co-authors: Muhammad Asim Mukhtar, Guy Gogniat,
Lab-STICC, Universite Bretagne Sud, France

Abstract

Protecting critical information against eviction-based cache side-channel attacks has always been challenging. In these attacks, the attacker reveals secrets by observing cache lines evicted by the co-running applications. A precondition for such attacks is that the attacker needs a set of cache lines mapped to memory addresses belonging to the victim, called eviction set. Attacker learns eviction-set by loading the cache lines at random and then it observes their evictions as a result of victim access. We have found that the relation between the incoming memory location and the resulting evicted cache line eases the learning of an eviction set. In this presentation, we will present our proposed *Indirect Eviction Cache (IE-Cache)* that is based on the principle of indirect eviction to harden the building of eviction-set. In an eviction process of IE-Cache, incoming memory triggers a series of replacements based on the cached memory addresses and a secure-indexing function, and the last replaced cache line is evicted. This increases the set size and introduces non-evicting cache lines in the eviction set. Through experimental results, we have shown that a 4-way set associative IE-Cache having 1MB and up to 3 replacements per eviction would require an attacker to generate 2^{59} memory accesses to learn an eviction set with 99 % confidence. Moreover, it achieves 1 to 3 % speedup compared to set-associative cache with a random-replacement policy on PARSEC benchmarks.

This work has been published at the IFIP International Conference on ICT Systems Security and Privacy Protection (IFIP SEC'2020) and awarded the Best Paper Award as well.