Cache Attacks: From Cloud to Mobile

Thomas Eisenbarth

University of Lübeck & Worcester Polytechnic Institute
thomas.eisenbarth@uni-luebeck.de

1 Abstract

The microarchitecture of modern CPUs features many optimizations that result in data-dependent runtime behavior. Data-dependent execution behavior can result in information leakage, enabling malicious co-located processes to overcome logical isolation boundaries of hypervisors and operating systems. For instance, cache attacks that exploit access time variations when retrieving data from the cache or the memory are a powerful tool to extract critical information such as cryptographic keys from co-located processes.

This tutorial introduces several methods of how to exploit cache-based side channels. Modern attacks and their behavior in various application scenarios, from cloud to mobile and embedded processors will be discussed. It will be shown of the introduced techniques can be applied to extract sensitive information from a co-located processes or VMs across cores and even across processor boundaries and how such attacks can be prevented.