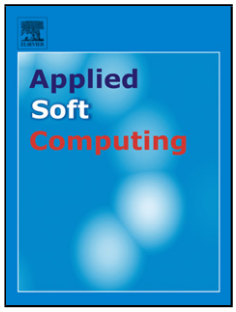

Title: Real time detection of cache-based side-channel attacks using Hardware Performance Counters

Author: Marco Chiappetta Erkay Savas Cemal Yilmaz

PII: S1568-4946(16)30473-2
DOI: http://dx.doi.org/doi:10.1016/j.asoc.2016.09.014
Reference: ASOC 3813

To appear in: *Applied Soft Computing*

Received date: 31-12-2015
Accepted date: 4-9-2016

Please cite this article as: Marco Chiappetta, Erkay Savas, Cemal Yilmaz, Real time detection of cache-based side-channel attacks using Hardware Performance Counters, *<![CDATA[Applied Soft Computing Journal]]>* (2016), http://dx.doi.org/10.1016/j.asoc.2016.09.014

Real time detection of cache-based side-channel attacks using Hardware Performance Counters

Marco Chiappetta[a,*], Erkay Savas[a], Cemal Yilmaz[a]

[a]*Sabanci University*
Universite Cd. No: 27
34956 Tuzla
Istanbul (Turkey)

Abstract

In this paper we analyze three methods to detect cache-based side-channel attacks in real time, preventing or limiting the amount of leaked information. Two of the three methods are based on machine learning techniques and all the three of them can successfully detect an attack in about one fifth of the time required to complete it. We could not experience the presence of false positives in our test environment and the overhead caused by the detection systems is negligible. We also analyze how the detection systems behave with a modified version of one of the spy processes. With some optimization we are confident these systems can be used in real world scenarios.

Keywords: cache-based, side-channel, hardware performance counter, machine learning

1. Introduction

Side-channel attacks are a particular class of attacks, usually targeting cryptographic algorithms, which do not exploit a flaw in the design of the algorithms themselves but rather in their implementation.

*Corresponding author
Email addresses: marcoc@sabanciuniv.edu (Marco Chiappetta), erkays@sabanciuniv.edu (Erkay Savas), cyilmaz@sabanciuniv.edu (Cemal Yilmaz)