Phased-Guard: Multi-Phase Machine Learning Framework for Detection and Identification of Zero-Day Microarchitectural Side-Channel Attacks

Title	Phased-Guard: Multi-Phase Machine Learning Framework for Detection and Identification of Zero-Day Microarchitectural Side-Channel Attacks
Publication Type	Conference Paper
Year of Publication	2020
Authors	Wang, H., Sayadi, H., Kolhe, G., Sasan, A., Rafatirad, S., Homayoun, H.
Conference Name	2020 IEEE 38th International Conference on Computer Design (ICCD)
Date Published	Oct. 2020
Publisher	IEEE
ISBN Number	978-1-7281-9710-4
Keywords	composability, defense, detection, Detectors, feature extraction, Hardware, Identification, machine learning, Metrics, microarchitecture, Monitoring, pubcrawl, resilience, Resiliency, side-channel attacks, Zero day attacks, Zero-day attacks

Abstract

Microarchitectural Side-Channel Attacks (SCAs) have emerged recently to compromise the security of computer systems by exploiting the existing processors' hardware vulnerabilities. In order to detect such attacks, prior studies have proposed the deployment of low-level features captured from built-in Hardware Performance Counter (HPC) registers in modern microprocessors to implement accurate Machine Learning (ML)-based SCAs detectors. Though effective, such attack detection techniques have mainly focused on binary classification models offering limited insights on identifying the type of attacks. In addition, while existing SCAs detectors required prior knowledge of attacks applications to detect the pattern of side-channel attacks using a variety of microarchitectural features, detecting unknown (zero-day) SCAs at run-time using the available HPCs remains a major challenge. In response, in this work we first identify the most important HPC features for SCA detection using an effective feature reduction method. Next, we propose Phased-Guard, a two-level machine learning-based framework to accurately detect and classify both known and unknown attacks at run-time using the most prominent low-level features. In the first level (SCA Detection), Phased-Guard using a binary classification model detects the existence of SCAs on the target system by determining the critical scenarios including system under attack and system under no attack. In the second level (SCA Identification) to further enhance the security against side-channel attacks, Phased-Guard deploys a multiclass classification model to identify the type of SCA applications. The experimental results indicate that Phased-Guard by monitoring only the victim applications' microarchitectural HPCs data, achieves up to 98 % attack detection accuracy and 99.5% SCA identification accuracy significantly outperforming the state-of-the-art solutions by up to 82 % in zero-day attack detection at the cost of only 4% performance overhead for monitoring.

URL https://ieeexplore.ieee.org/document/9283602
DOI 10.1109/ICCD50377.2020.00111
Citation Key wang_phased-guard_2020

composability defense detection Detectors feature extraction Hardware Identification machine learning Metrics microarchitecture Monitoring pubcrawl resilience Resiliency side-channel attacks Zero day attacks Zero-day attacks