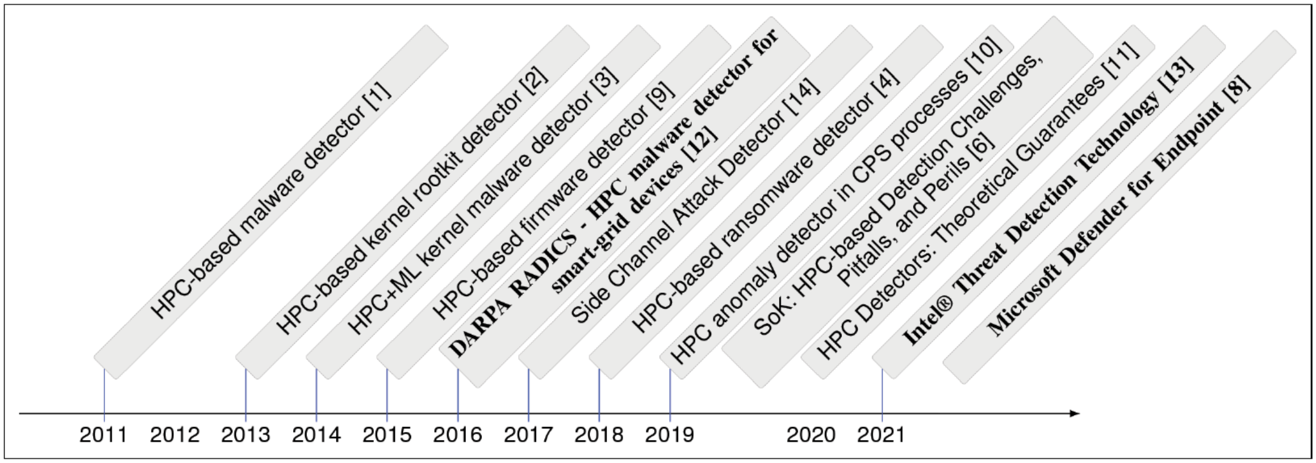
HPC-Based Malware Detectors Actually Work: Transition to practice After a Decade of Research.

Charalambos Konstantinou, Michail Maniatakos, Ramesh Karri, Xueyang Wang.

Introduction:

Modern Processor include dedicated registers, called hardware performance counters used to track the low-level microarchitectural events to monitor and measure events of processes executing on the system. Over a decade ago in 2011, researchers proposed using HPCs to evaluate static and dynamic integrity of program codes to detect malicious program modification at load time and at run time. Extending this paradigm, HPCs can be used for offensive and defensive purpose. Now they can detect malicious firmware and software, ransomware and cryptojacking.


HPC-based malware detector [1]
HPC-based kernel rootkit detector [2]
HPC+ML kernel malware detector [3]
HPC-based firmware detector [9]
DARPA RADICS - HPC malware detector for smart-grid devices [12]
Side Channel Attack Detector [14]
HPC-based ransomware detector [4]
HPC anomaly detector in CPS processes [10]
SoK: HPC-based Detection Challenges, Pitfalls, and Perils [6]
HPC Detectors: Theoretical Guarantees [11]
Intel® Threat Detection Technology [13]
Microsoft Defender for Endpoint [8]
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021

Above figure, present the chronology of transition of research, on malware detection using HPCs. Since their introduction for malware detection, HPCs have been used to detect variants of malware such as *kernel-level rootkits, firmware modifications*, and *malware in multithreaded cyber-physical system processes*.

HPC for embedded system security-

Since HPC are available in all modern processors, so they can yield near zero overhead approach to count hardware events of applications running on the platform. While it is not possible to read all available HPCs at the same time, one can multiplex the measurements to read more HPC measurement streams, albeit with the overhead of multiplexing.

1) Confirm: In 2015, researchers extended HPC-based malware detection to detect firmware modifications in embedded systems using HPCs. The motivation for ConFirm is that embedded devices are integrated in several domains, including power grid, home and automation networks, and smart/connected cars. These devices are constrained in terms of

performance and resources and hence cannot employ the same heavyweight security measures used in general-purpose computers. ConFirm is a low-cost, HPC-based technique to detect malicious modifications in the firmware of embedded control systems. Confirm was the first work to introduce HPCs to secure the firmware both as a design for secrity concept and as an add-on feature. Confirm observe that a program is a sequence of various type of instructions which during execution can be monitored by low-level hardware events. The behaviour of the firmware running on resource constrained embedded systems can be uniquely characterized by using HPCs at run time. Moreover, one can monitor the relationship between the counts of the different events.

Follow-up addtional academic research

I. HPC based monitoring for security of CPS: used for real-time monitoring of software running on embedded CPS processors.

II. Using HPCs to detect different types of attacks: used to detect return-oriented programming, ransomware, and side-channels.

III. Feasiblility of other built-in hardware components for security: Modern computer systems have on-chip sensors including thermal, voltage, and frequency sensors and associated reporting interfaces. Readings from these sensors correlate to the behavior of running programs and can be adapted for security monitoring. Combining thermal profiles of processors with HPCs can detect malicious changes due to software and hardware attacks.

IV. HPC can be used as security backdoor: This rootkit allows an attacker to redirect control flow to malicious code by using HPCs count specific events. Alam et al. present a micro-architectural side-channel attack by analyzing HPC counts when executing encryption algorithms.

Transition to Practice case studies

DARPA RADICS:

The DARPA RADICS program developed systems to restore power following a cyber-attack on the power grid. DARPA assembled several teams with over 100 participants to solve this critical problem. RADICS teams demonstrated technologies, with red-teams injecting malicous code and blue-teams detecting malware and restoring substation devices to create the crank path to restore power.

INTEL TDT:
After a decade of academic research and proof-of-concept demonstrations, Intel as a major processor vendor has taken an important step to unlock the capabilities of HPC-based malware detection. Intel developed TDT as part of its Hardware Shield suite. Intel TDT leverages HPCs and hardware acceleration of machine learning on an integrated GPU to collect profile, and detect malicious activities.

Microsoft Detender for EndPoints:

uses Intel TDT to detect unauthorized crypto mining such as cryptojacking entails maliciously co-opting computational resources of community to mine crypto currencies.Crypto mining repeatedly uses mathematical operations, and these activity patterns can be detected by monitoring HPCs. Microsoft uses Intel TDT for HPC-based monitoring in their commercial malware defense tool. By analyzing the values of the selected HPCs, the system determines whether someone is mining with or without the owner’s consent.