CALL FOR PAPERS

Springer International Journal of Parallel Programming

Special Issue on "Side-channel and fault analysis of high-performance computing platforms."

GUEST EDITORS:
Rosario Cammarota, ro.c@qti.qualcomm.com, Qualcomm Research, San Diego.
Patrick Schaumont, schaum@vt.edu, Virginia Tech.
Yunsi Fei, yfei@coe.neu.edu, Northeastern University.

AIMS and SCOPE:

This IJPP Special Issue covers both attack and defense mechanisms in the context of emerging concerns of side-channel, covert-channel and fault analysis applied to modern computing systems.

The scope of this Special Issue includes security analysis of highly parallel computing systems and their compilation and run-time environments. Such systems may include many on-die computing cores, hardware accelerators, complex interconnect and memory hierarchy, facilitating high-performance computation via leveraging multiple levels of parallelism and resource allocation at both compilation and run-time.

High-performance architectures and their compilers traditionally focus on maximizing the system performance through micro-architectural optimizations such as pipelining, caches, and hyper-threading, bootstrapped by the corresponding compilation and run-time supports. However, such performance considerations introduce biases in the micro-architecture and its software. Once the biases and their dependency on the instruction and data are observed by an adversary and exploited, critical or secret information can be leaked, and the system confidentiality and security will be subverted.

Despite physical security and tamper resistance included in computer systems, micro-architecture attacks can be executed remotely, across virtual machines (e.g., in the case of cloud infrastructures), and can result in key extraction of cryptographic implementations and information leakage across computing system compartments. Such attacks effectively extend the realm of physical attack to the cyberspace, and their severity directly correlates with the increasing importance or criticality of the contents being processed on the target hardware, e.g., processing premium contents, transaction in the FinTech domain.

We invite manuscripts that address the multiple aspects of information leakage through shared resources in high-performance micro-architecture, and/or due to compiler assisted optimizations. At the same time, we invited manuscript that investigate the use of high-performance architecture and compilation techniques to defend against micro-architectural attacks, a research space which is largely unaddressed.

We are soliciting original manuscripts covering the state-of-the-art principles and practices in attacks and mitigations, but also including theoretical foundations. We are also looking to complement the research-focused content with technology surveys and case studies. We welcome broader aperture surveys as well as case studies in micro-architecture attacks. Contributions from industry are welcome.

We aim to gather a valuable set of resources for both the high-performance computing and computer security community for setting and pursuing, with more clarity, further advances in this new field.

TOPICS OF INTEREST:
The topics of interest for this special issue include, but are not limited to, the following hardware related topics:

- Micro-architecture side-channel and fault analysis metrics, principles and practices (fault intensity analysis).
- Hardware assisted mitigations and their design and evaluation (side-channel resistant memory hierarchy, datapath, controlpath).
- Software assisted mitigation techniques and their design and evaluation (forms of randomization, use of redundancy) at different levels, source code, compile time, and run-time.
- Attacks and mitigations (in the cloud, for specific micro-processor features, for accelerators).
- Application specific attacks and mitigations (to cryptographic implementations, non-cryptographic implementations, e.g., deep learning).

Given that the goal of the issue is to provide an authoritative starting point for future research, we encourage authors to provide a comprehensive description of related research and state of practice, from the perspectives of both attack and countermeasure.

IMPORTANT DATES:
Open for submissions in Springer Manuscripts: December 1, 2017
Closed for submissions: February 1, 2018
Results of first round reviews: April 1, 2018
Submission of revised manuscripts: July 1, 2018
Results of second round reviews: August 1, 2018
Publication material due: September 1, 2018

SUBMISSION GUIDELINES:
Prospective authors are invited to submit their manuscripts electronically after the "open for submissions" date, adhering to the International Journal of Parallel Programming guidelines (http://www.springer.com/computer/theoretical+computer+science/journal/10766?detailsPage=pltci_2519840) .

Please submit your papers through the online system (https://www.editorialmanager.com/ijpp/default.aspx) and be sure to select the special issue or special section name. *Manuscripts should not be published or currently submitted for publication elsewhere.* Please submit only full papers intended for review, not abstracts, to the Editorial Manager portal. If requested, abstracts should be sent by e-mail to the Guest Editors directly.