Polytech network form for PhD Research Grants from the China Scholarship Council

This document describes the PhD subject and supervisor proposed by the French Polytech network of 14 university engineering schools. Please contact the PhD supervisor by email or Skype for further information regarding your application.

Supervisor information	
Family name	Pillement
First name	Sebastien
Email	Sebastien.pillement@univ-nantes.fr
Web reference	http://pillement.polytech.univ-nantes.fr
Lab name	I.E.T.R.
Lab web site	www.ietr.fr
Polytech name	Polytech Nantes
University name	University of Nantes
Country	France

PhD information	
Title	Statistical modeling and analysis methods for system-level design of secured multi-core architectures
Main topics regards to CSC list (3 topics at maximum)	IC design, structure of new computer systems, understanding models and intelligent systems

Required skills in science and engineering	Computer systems, programming languages…

Subject description (two pages maximum)

Context and main object of this project

The recent processor security vulnerabilities such as SPECTRE [KOC19] and MELTDOWN [LIP18], have shown the great extend and relevance of the possible attacks on current multi-core systems. These vulnerabilities directly result from performance oriented architectural choices from the last decades. The performance improvement relies on the implementation of highly parallel architectures including shared resources. Indeed, performance systems offer and encourage resource sharing between applications. However, malicious applications can take advantage of these shared hardware resources (memories, caches, buses, networks), by observing and exploiting their influence on sensitive applications in order to gain information otherwise not accessible (i.e., a cryptographic key).

In order to cope with current and future security vulnerabilities, security constraints need to be taken into account in the early stages of the architecture design. This project aims at proposing innovative modeling and analysis methods of multi-core architectures taking into account security as a particular non-functional design constraint. This PhD thesis will particularly consider cache-based multi-cores architectures and will focus on logical side-channel attacks exploiting shared caches.

One of the main issues that will be addressed by this project is the ability to propose fast yet accurate models to efficiently evaluate and improve the security level of future multi-core architectures.

Existing work

System-level modeling and analysis of hardware/software architectures have strongly been considered during the last decades [GER09]. System-level models correspond to high level representation of application tasks allocated to a set of hardware/software components. These models are used to evaluate the efficiency of architectures with respect to timing and power constraints. However, security has not yet been considered as a constraint in existing system-level frameworks. A first effort in order to guide the design of architectures from a security point of view has been made in [TAN'17]. However, this work does not take into account indirect illegal access to data through logical side channel attacks. The proposed project will particularly focus on these latter attacks, as their great extend the last year have shown their great impact in current multi-core systems [KOC19][LIP18]. `

Expected contributions

The main idea of the project is then to develop a new methodology for system-level evaluation of secured multi-core architectures. In this context and among all the possible threat, this PhD thesis will focus on the cache design and protection.

The first contribution of this work rely then on the definition of a new modeling approach to appropriately capture at high level of abstraction cache management effects and potential attacks. The

proposed model would then serve as evaluation metric of security. For that purpose, the existing logical cache-based attacks will be studied. Specifically we will concentrate on multiple cache-based attacks (i.e. Flush and Reload [YAR14], Flush and Flush [GRU16], Prime and Probe [LIU15]…). After their theoretical study and their real implementation in an hardware FPGA based prototype, the considered architecture resources and related attacks will be characterized through execution traces (execution time, resource utilization, communication traces…). Statistical learning approach represents an interesting method that could help to deliver fast yet accurate models [ZHE15] to characterize and detect these attacks.

The second targeted contribution concerns the definition of an appropriate system-level analysis method to estimate the architecture security level. The models of architecture resources proposed in the first phase of the thesis will be considered here. In this scope, Statistical Model Checking or machine learning approaches could represent good candidates to deliver reliable estimations. Robustness of these approaches to allow potential attacks to be detected will thus be evaluated. The established analysis framework would be used to evaluate different optimisation strategies to increase the architecture security level.

In the scope of this thesis, a multi-core architecture will be implemented and tested on a FPGA-based prototype. This prototype will be used to generate the processed execution traces. The studied attacks will be tested and the accuracy of the estimation delivered by the proposed analysis framework will be evaluated. At this step the modification on the cache structure implementation and management (i.e. secured-by-design) will be implemented on the prototype for evaluation.

References

[KOC19] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz and Y. Yarom, "Spectre Attacks: Exploiting Speculative Execution", Proc. IEEE Symposium on Security and Privacy (S&P), 2019.

[LIP18] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom and M. Hamburg, "Meltdown: Reading Kernel Memory from User Space", Proc. USENIX Security Symposium, 2018.

[YAR14] Y. Yarom and K. Falkner, “FLUSH+ RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack”, Proc. USENIX Security Symposium, 2014.

[GRU16] D. Gruss, C. Maurice, K. Wagner and S. Mangard, “Flush+Flush: A Fast and Stealthy Cache Attack”, Proc. Springer Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), 2016.

[LIU15]F. Liu, Y. Yarom, Q, Ge, G. Heiser and R. B. Lee, “Last-Level Cache Side-Channel Attacks are Practical”, Proc. Symposium on Security and Privacy (S&P), 2015.

[TAN’17] B. Tan, M. Biglari-abhari and Z. Salcic, “An automated Security-Aware Approach for Design of Embedded Systems on MPSoC”, Transactions on Embedded Computing Systems, Vol. 16, No. 5s, 2017.

[GER09] A. Gerstlauer et al., “Electronic system-level synthesis methodologies”, IEEE Transactions on computer-aided design of integrated circuits and systems, ol. 28, no. 10, October 2018.

[BUL12] P. Bulychev et al., “Statistical model checking for priced timed automata”, Proc. Workshop on quantitative aspects of programming languages and systems (QAPL), 2012.

[ZHE15] X. Zheng, P. Ravikumar, L.K. John, A. Gerstlauer, “Learning-based analytical cross-platform performance prediction”, Proc. International Conference on embedded systems (SAMOS), 2015.