UNIVERSITÉ DE RENNES 1

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2022

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : **POLE DE RECHERCHE :**

Unité de recherche d'accueil

Unité de Recherche : IRISA

Equipe : Taran

Encadrement

Directeur de thèse : Steven Derrien **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes 1

HDR : ☐ oui ☐ ~~non~~ **Nb de thèses en cours** : 5 au 1er septembre 2022

Mail : sderrien@irisa.fr **Tél.** :

Co-encadrant de thèse : Simon Rokicki **Unité de recherche** : IRISA

Employeur/Établissement d'origine : ENS Rennes

HDR : Ξ ~~oui~~ ☐ non **Nb de thèses en cours** : 1

Mail : simon.rokicki@irisa.fr **Tél.** :

Sujet

Titre : Security of DBT based processors

Mots clés : DBT, Hardware Security, fault attacks

Cotutelle internationale (~~oui~~/non) : **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

The use of micro-architectures based on Dynamic Binary Translation (DBT), also called Hardware/Software Co-Designed machines, allow to completely decouple the micro-architecture from the Instruction Set. In a DBT based processor a guest ISA is executed on the its micro-architecture through the use of a dynamic compilation layer embedded within the processor.

For example, Hybrid-DBT is capable of transparently executing RISC-V binaries on an explicitly parallel architecture [3]. The underlying micro-architecture can then be freely customized, as long as the DBT layer is retargeted to support it.

Transmeta and NVidia Denver[1,2] are two examples of such an architecture, and experiments have demonstrated that the Hybrid-DBT architecture is up to three times more energy-efficient compared to an equivalent Out-of-Order processor [5]. The interest in DBT processors has recently been revived by the Apple M1 processor which rely on these techniques to dynamically translate x86 binaries to the Arm ISA.

The use of HW/SW co-designed machines raises novel security issues. For example, recent work demonstrated that a simple software update on the DBT engine can protect against several variants of the Spectre vulnerability [4]. Moreover, the DBT engine and the ability to modify the processor offer a simple way to transparently insert complex mechanisms in the processor. For example, DBT makes it possible to

dynamically apply compiler transformation for protecting against fault attacks (instruction duplication/triplication, generation of randomized schedules, etc.). It also enables hardware support for protecting against security attacks (for example by supporting Information Flow Tracking) .

However, DBT processors may also create new vulnerabilities linked to the dynamic translation and optimization process. Therefore, it is crucial to also build a better understanding of these approach from a security perspective.

The goal of this PhD is to evaluate the type of security issues raised by DBT architecture, and propose suitable mechanisms to address them.

[1] J. C. Dehnert et al., "The Transmeta Code Morphing™ Software: Using Speculation, Recovery, and Adaptive Retranslation to Address Real-Life Challenges," in Proceedings of the international symposium on Code generation and optimization: feedback-directed and runtime optimization, 2003, pp. 15–24.
[2] D. Boggs, G. Brown, N. Tuck, and K. S. Venkatraman, "Denver: Nvidia's First 64-bit ARM Processor," in IEEE Micro, Mar. 2015, vol. 35, pp. 46–55.
[3] S. Rokicki, "Hybrid-DBT: Hardware/Software Dynamic Binary Translation Targeting VLIW.," IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol. 38, no. 10, pp. 1872–1885, 2019, doi: 10.1109/TCAD.2018.2864288.
[4] S. Rokicki, "GhostBusters: Mitigating Spectre Attacks on a DBT-Based Processor.," pp. 927–932, 2020, doi: 10.23919/DATE48585.2020.9116402.
[5] S. Rokicki, "Accélération matérielle pour la traduction dynamique de programmes binaires". Thèse. Université Rennes 1, 2018