2. Les dossiers d'attractivités

2.1. SECUREIOT_

Titre : **Sécurité des systèmes multicoeurs**

Porteur du projet : Maria MENDEZ REAL
Etablissement : Polytech Nantes, université de Nantes
Laboratoire : IETR UMR CNRS 6164, Equipe SysCom,

Origine : Université Bretagne Sud, laboratoire Lab-STICC UMR CNRS 6285

2.1.1. Objectif du recrutement

L'université de Nantes recrute en 2018 d'un enseignant chercheur sur la thématique des systèmes embarqués avec un adossement recherche dans l'équipe SysCom de l'IETR.
L'enseignante chercheure, Maria MENDEZ REAL, recrutée lors de cette campagne développera et renforcera les compétences en informatique embarquée et architecture matérielle du département ETN (Electronique et Technologies Numériques) de Polytech Nantes dans le domaine de la conception de systèmes embarqués communicants.
Les domaines d'application envisagés sont les télécommunications, l'électronique professionnelle, avec l'intégration des contraintes de consommation d'énergie et la fiabilité.

Concernant les systèmes embarqués communicants, les enjeux identifiés sont :

- La sécurité dès la conception (Security-by-design) ;
- L'analyse des menaces (Threat modeling) ;
- La cyber-résilience (Cyber-resilience) : tout système est et sera attaquable.

Le dossier attractivité a incité la candidate à venir à Nantes en ayant en plus du poste de maître de conférences, la possibilité de démarrer rapidement une activité de recherche et de collaborations en accordant le financement d'une allocation de recherche doctorale, ainsi qu'un budget de fonctionnement couvrant des achats d'équipements et des frais de missions aussi bien pour la dissémination de ses travaux que pour le montage de futures collaborations de recherche.

2.1.2. Thèse associée au projet Attractivité

Titre : **Evaluation et considération de la sécurité dans les systèmes de gestion d'architectures multicoeurs**

Laboratoire : IETR UMR CNRS 6164, Université de Nantes

Laboratoire associé :

Doctorant : Safouane NOUBIR
Encadrant : Maria Méndez Real, Sébastien Pillement

Mots clés : Sécurité matérielle, multi et "many-" cœurs, gestionnaires de ressources

Verrous scientifiques ou technologiques levés :

- Le principal verrou à traiter est l'identification et la mise en évidence de vulnérabilités de sécurité des systèmes de gestion des architectures actuelles. En effet ce verrou n'a été que très peu traité

(un seul article publié en 2017), cependant ces gestionnaires sont vulnérables et peuvent être attaqués constituant ainsi un frein important à l'adoption à grande échelle des architectures multi et «many-»cœurs ;
- Le deuxième verrou à traiter sera la sécurisation des gestionnaires de ressources actuels.

Etat : Début de thèse 1/10/2018, soutenance en décembre 2021

2.1.2.1. Résumé grand public du projet

Les architectures complexes intégrant un nombre important de ressources de calcul, de mémoire, dites multicœurs sont aujourd'hui une réalité. Si ces architectures offrent une puissance de calcul et un degré de parallélisme importants, elles sont également très complexes et nécessitent des gestionnaires dynamiques afin de gérer et d'optimiser l'utilisation de ces ressources. Cette complexité rend difficile le contrôle d'une utilisation malveillante des ressources et services. Dans cette thèse nous proposons d'étudier dans un premier temps les différents vecteurs d'attaques de ces gestionnaires de ressources et de mettre en évidence ces vulnérabilités de sécurité par l'implémentation d'attaques. Dans un deuxième temps, des pistes pour la sécurisation de ces gestionnaires seront investiguées.

2.1.2.2. Résultats du projet

2.1.2.2.1. Résumé des travaux de thèse

Lors de la première année de thèse, nous avons étudié l'état de l'art et investigué la reproduction de seule attaque existante sur les gestionnaires d'énergie des architectures multicœurs "clkscrew", publié en 2017. Des limites de cette attaque sur les architectures actuelles ont été identifiées. Ce travail s'est poursuivi par l'implémentation d'une nouvelle attaque de type déni de service visant les gestionnaires DVFS d'architectures multicœurs. Cette attaque a été entièrement implémentée sur deux architectures très récentes largement utilisées dans le monde de la téléphonie mobile montrant ainsi un vrai enjeu nécessitant d'être traité. Ce travail a été valorisé par une publication dans une conférence de rang A en 2020.
Lors de la deuxième année de thèse nous avons investigué les possibles exploitations malicieuses de capteurs embarqués (de température, de consommation) des systèmes actuels. Les données de ces capteurs sont nécessaires pour la prise de décision dynamiques des gestionnaires de ressources, néanmoins elles pourraient également permettre la déduction d'informations sensibles/secrètes par exemple lors du chiffrement de données. Ce travail est actuellement en cours mais les premiers résultats montrent que les données des capteurs de température fuitent des informations sur les instructions et les données manipulés qui ne pourraient être autrement déduites. L'exploitation complète de ces fuites est actuellement investiguée.

2.1.2.2.2. Publications

"Towards Malicious Exploitation of Energy Management Mechanisms", S. Noubir, M. Méndez Real and S. Pillement, at The Design, Automation, and Test in Europe (DATE), 2020.

2.1.2.2.3. Dissémination

Présentation à la Journée du laboratoire IETR en 2019.

2.1.2.2.4. Equipement et ressourcement

- Salaire du doctorant
- Achat d'une station de travail pour les travaux ;
- Frais d'inscription à la conférence DATE où les premiers travaux ont été présentés.