2018-7190 Analyses des attaques sur les mémoires SRAM et conception de contremesures H/F

Informations générales

Description de l'entité	Le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) est un organisme public de recherche. Acteur majeur de la recherche, du développement et de l'innovation, le CEA intervient dans le cadre de ses quatre missions : . la défense et la sécurité . l'énergie nucléaire (fission et fusion) . la recherche technologique pour l'industrie . la recherche fondamentale (sciences de la matière et sciences de la vie). Avec ses 16000 salariés -techniciens, ingénieurs, chercheurs, et personnel en soutien à la recherche- le CEA participe à de nombreux projets de collaboration aux côtés de ses partenaires académiques et industriels.
Description de l'unité	Le Leti, institut de recherche technologique de Cea Tech, a pour mission de créer de la valeur et de l'innovation avec ses partenaires industriels. Il fait le lien entre la recherche fondamentale et la production de micro et nanotechnologies dans le but d'améliorer la qualité de vie de chacun. Fort d'un portefeuille de 2.800 brevets, le Leti façonne des solutions avancées pour améliorer la compétitivité de ses partenaires industriels: grands groupes, PME ou startups. Localisé à Grenoble (38), le Leti compte plus de 1 800 chercheurs et a des bureaux aux US et au Japon. Le LSOSP, Laboratoire sécurité des objets et des systèmes physiques, mène des activités de R&D dans le domaine des technologies de sécurité et de protection de la vie privée. Il analyse et caractérise les risques auxquels sont soumis les systèmes électroniques et les composants; il conçoit des contre-mesures s'appuyant notamment sur des techniques cryptographiques mais aussi sur des modifications dans l'architecture des systèmes pour intégrer les technologies nécessaires (composants, codes embarqués, interfaces ou protocoles de communications...). Il caractérise l'efficacité des contremesures intégrées dans des composants, des objets (communicants) et des systèmes cyberphysiques afin de résister aux attaques au niveau de leur structure, de leurs fonctions ou de leur utilisation.
Délai de traitement	2 mois

Description du poste

Site	Grenoble
Lieu	17, avenue des martyrs, 38000 GRENOBLE
Domaine	Composants et équipements électroniques
Contrat	Stage
Intitulé de l'offre	Analyses des attaques sur les mémoires SRAM et conception de contremesures H/F
Sujet de stage	Analyses des attaques sur les mémoires SRAM et conception de contremesures
Durée du contrat (en mois)	6 mois
Description de l'offre	Le CEA LETI et l'IRT NanoELec à travers le projet Nanotrust repense la sécurité des processeurs pour les systèmes embarqués que l'on trouve dans l'IoT ou les CPS à travers la conception de processeurs intrinsèquement sécurisés basés sur l'architecture RISC-V. Avec l'utilisation de filière toujours plus fine, en particulier avec des transistors ayant des tailles de grille inférieure à 10 nm, on commence à observer de plus en plus fréquemment des défaillances sur les mémoires SRAM. Elles se manifestent sous deux formes : l'apparition de fautes générées par les lectures et les écritures sur des données adjacences dans la matrice de mémorisation [1], mais aussi des phénomènes de rétention de données [2]. Ces effets indésirables ouvrent la porte à des problèmes de sécurité. L'enjeu est d'autant plus de taille que les SRAM sont utilisées dans la plupart des mémoires cache des processeurs. Il pourrait ainsi être possible de modifier des lignes de cache contenant des données ou des instructions sur lesquelles on n'a pas les droits et ainsi violer les principes d'isolation de processus. Dans un premier temps le candidat caractérisera sur la base de l'état de l'art ces erreurs avec des matrices SRAM de FPGA. On verra ensuite comment elles sont transposables à des mémoires cache de processeurs. Il s'agira ensuite de déterminer comment on peut les exploiter et enfin d'essayer de trouver des contremesures à ces attaques. Références [1] Vilas Sridharan, Nathan DeBardeleben, Sean Blanchard, Kurt B Ferreira, Jon Stearley, John Shalf, and Sudhanva Gurumurthi. Memory errors in modern systems : the good, the

	bad, and the ugly. ACM SIGARCH Computer Architecture News, 43(1) :297–310, 2015. [2] Joseph McMahan, Weilong Cui, Liang Xia, Jeff Heckey, Frederic T Chong, and Timothy Sherwood. Challenging on-chip sram security with boot-state statistics. In Hardware Oriented Security and Trust (HOST), 2017 IEEE International Symposium on, 101–105. IEEE, 2017
Moyens / Méthodes / Logiciels	VHDL sur Xylink
Profil du candidat	Etudiant en troisième année d'école d'ingénieur ou deuxième année de master
	Merci de bien vouloir transmettre votre candidature directement à Olivier SAVRY : olivier.savry@cea.fr

Critères candidat

Langues	Anglais (Courant)
Diplôme préparé	Bac+5 - Diplôme École d'ingénieurs
Formation recommandée	Etudiant en 3ème année d'école d'ingénieur ou 2ème année de master

Demandeur

Disponibilité du poste	01/02/2019