DUZÉS Florian
63 avenue de la République
94800 Villejuif
07.50.64.15.22
florian.duzes@inria.fr

CentraleSupélec - Campus de Rennes,
Av. de la Boulaie,
Cesson-Sévigné

Conception et Vérification formelle de méchanisme de sécurité matériel/logiciel

Bonjour Monsieur Hiet,

Bonjour Messieurs Courousse, Jean et Wilke.

Je suis actuellement en stage au sein de l'équipe PROSECCO, au centre Inria Paris, sous la supervision joins de M.Aymeric fromherz & des Messieurs Sebastien Bardin et Yanis Sellami du centre CEA Nano-Innov de Saclay. Ce poste d'ingénieur de recherche me permet de terminer mon master "Cryptologie et Sécurité Informatique" de Bordeaux.

Mon plan à l'origine était d'entrer dans le privé à la fin de ce master, mais les échanges avec mes professeurs et collègues de bureaux m'ont ouvert à la possiblité qu'il existe une autre voie. Cette voie, c'est la thèse. Dans cet objectif, je prend contact avec différents centre de recherche français pour recueillir des informations et me préparer à cette possibilité.

Ce chemin de la thèse, je le vois comme une possiblité offerte à une jeune personne d'essayer pendant trois ans, puis, de présenter un retour sur son parcours pour faire avancer la recherche. C'est une chance que je voudrais saisir. Pour moi, la thèse, c'est un travail personnel, où on cultive un savoir, qui est ensuite rendu impersonnel. C'est un travail où il y a moins de contrainte de retour sur investissement que dans une société privée. Un espace de liberté proposé dans un but de recherche et développement, mais un travail quand même.

J'aime le travail de recherche que je fais actuellement. Il consiste à "industrialiser" le processus de détection de faille pour des attaques temporelles. Je vérifie la sureté, selon ce prisme, d'une bibliothèque cryptographique. J'aimerai pouvoir élargir ce prisme. Dans cette optique, votre sujet propose de descendre encore d'une couche dans la sécurité. Je voulais poursuivre en cherchant un travail au niveau de la sécurité du code, je n'avais pas conscience qu'il était possible d'augmenter en précision. Cette offre me permet de découvrir un nouveau aspect de la sécurité que je ne percevais pas. J'ai envie de me lancer dans cette nouvelle aventure et je serais heureux de pouvoir le faire avec vous.

Je serais heureux de travailler avec vous car vos travaux me plaise. J'ai rapidement parcouru les productions réalisées par l'ancienne équipe CIDRE, les travaux de SUSHI et les sujets des anciens thésards, et certains sont l'idée que je me suis faîte du travail futur que je voudrais réaliser. La détection automatique des failles par canal auxiliaire, vérifier l'éxécution d'un programme; c'est que j'avais en tête en consultant la page de l'équipe SUSHI. En parallèle, mes travaux actuels m'ont sensiblisé à RiscV. Pour moi, il est clair qu'il est possible d'améliorer/développer la sécurité de cette nouvelle architecture, cela laisse donc de la place pour de nouvelles personnes. Je voudrais faire partie de ces personnes.

Cette offre de thèse est donc pour moi une possibilité que je souhaite explorer. Je réalise la quantité de travail à abattre, l'ensemble des articles et pages de documentation à lire pour bien cerner le projet et planifier les trois années à venir. Ce travail ne m'effraie pas, il est clair et précis. Avec de la discipline et de la régularité tout peur être réalisé. Je vais pouvoir côtoyer des personnes très savantes, développer la sécurité embarqué d'une nouvelle technologie et entrer dans la cours des grands.

J'ai hâte de pouvoir discuter avec vous, de vos attentes, de nos visions, durant notre entretien, concernant cette proposition de travail. Je vous remercie pour le temps accordez à la lecture de cette lettre,

En vous souhaitant une agréable journée,

Cordialement

Duzés Florian