Transcription de l'entretien audio de Guillaume Hiet

Je suis Guillaume Hiet, professeur à Centrale Supélec et je suis le responsable de la nouvelle équipe-projet Inria Sushi qui veut dire *SecUrity at the Software-Hardware Interface*. C'est une équipe commune entre Centrale Supélec qui fournit le gros des troupes, mais également l'ENS et donc c'est une équipe Inria et qui fait partie du laboratoire Irisa et donc le CNRS est une des tutelles également.

On travaille sur des aspects sécurité à l’interface entre logiciel et matériel. On voit cette interface à la fois comme une menace. Il y a des échanges complexes entre le logiciel de bas niveau et le matériel et de ces échanges complexes peuvent naître des vulnérabilités. Et puis, c'est également une opportunité. On peut définir des nouveaux mécanismes de sécurité qui vont faire appel à des interactions entre logiciel et matériel.

Aujourd'hui, on regarde les architectures matérielles notamment. C'est plus ce qu'on apprend traditionnellement à l’école, où¹ on a un processeur, de la mémoire, des entrées-sorties. Aujourd'hui, il y a plusieurs unités de calcul hétérogènes qui collaborent entre elles avec un stack logiciel assez complexe. Donc oui, il y a de plus en plus de complexité. Donc l'évaluation des produits de sécurité qu'on va retrouver dans les produits tous les jours, c'est un vrai défi, en particulier quand ces produits sont censés implémenter des fonctions de sécurité fortes. Par exemple, tout ce qui est gestion de l’identité.

Un des projets phares aujourd'hui dans lequel on est impliqué, c'est le projet, c'est *SecurEval*. Donc c'est un projet du PEPR *Cybersécurité*. Il y a plusieurs projets dans ce PEPR, et *SecurEval* s’intéresse, comme le nom l'indique, aux évaluations de sécurité, donc les évaluations de sécurité, aujourd'hui, c'est quelque chose qui est normé. On parle des critères communs, qui est une norme ISO que l'on retrouve dans plusieurs pays. C'est une norme qui permet à des laboratoires indépendants de faire des évaluations de sécurité de produits qui sont ensuite reconnus au niveau étatique, donc en France, par l'ANSSI. Donc, l'objectif de ce projet, c'est de fournir des analyses et de l'outillage plus poussés pour favoriser les évaluations de sécurité, donc pour permettre de diminuer leur coût, notamment vis-à-vis des laboratoires d'évaluation.

Dans le projet, *SecurEval* qui est principalement mené par le CEA, le CEA agit à la fois en tant qu'organisme de recherche, mais également en tant que fournisseur de solutions, puisque le CEA possède un laboratoire d'évaluation un CESTI. Donc, *in fine*, les retombées de ce projet elles visent bien évidemment les CESTI, les laboratoires d'évaluation, mais aussi les industriels qui ont vocation, *in fine*, de faire évaluer leurs propres produits. L'industriel doit être impliqué dans la démarche d'évaluation et donc on pense que ce que l'on développe comme recherche dans ce projet-là pourra servir également aux industriels français et européens.

L'équipe est impliquée dans deux lignes de travail qui correspondent à deux axes forts de l'équipe. D'une part, l'analyse de vulnérabilités sur des codes binaires. Alors ça, c'est important parce qu'un certain nombre d'évaluations aujourd'hui se font en boîte noire, on ne dispose pas du code source et donc il est important de développer des analyses qui puissent être faites directement sur le code binaire pour trouver des vulnérabilités. C'est un des points forts du CEA et de son équipe Binsec qui développe un outil d'analyse binaire. Et donc c'est une opportunité pour nous de collaborer avec cette équipe pour développer de nouvelles analyses.

Et d'autre part, une des originalités fortes de notre équipe, c'est de proposer des analyses et de l'outillage pour appliquer des méthodes formelles à des mécanismes de sécurité qui, au moins en partie, s'appuient sur du matériel, donc prouver des mécanismes de sécurité logicielle matériel. Et ça, c'est un des points forts de l'équipe.