h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Printemps 2024
Session de bachelor

ATTAQUE BRUTE-FORCE SUR FPGA POUR BCRYPT

ORIENTATION : SYSTÈMES INFORMATIQUES EMBARQUÉS

Descriptif :
Le projet vise à développer un accélérateur de calcul basé sur des circuits FPGA pour attaquer les mots de passe protégés par l'algorithme bcrypt, surpassant les performances des approches traditionnelles basées sur CPUs et GPUs. L'étudiant implémentera un cœur de calcul compact afin d'instancier plusieurs cœurs de calcul dans un seul FPGA, avec des interfaces de communication intégrées pour interagir avec l'hôte. Le système inclura une interface UART pour une communication série simple et économique, ainsi qu'une interface PCIe offrant des vitesses de transfert élevées pour les besoins de performances intensives. Un protocole adapté sera mis en place pour gérer les différents types de messages entre le PC et le FPGA.

Deux stratégies seront explorées pour la génération des mots de passe. La première consiste à utiliser un compteur interne au FPGA pour optimiser la vitesse et l'efficacité. La seconde permettra d'implémenter des attaques par dictionnaire, gérées par un PC qui enverra les mots de passe via l'interface PCIe. Cette configuration tirera pleinement parti des capacités de parallélisation du FPGA, offrant une solution extensible et performante pour le cassage de mots de passe.

Travail demandé : Dans le cadre de ce projet l'étudiant devra :

- Implémenter un cœur de calcul compact pour bcrypt en utilisant VHDL ou réutiliser des cours déjà existants.
- Instancier et paralléliser plusieurs cœurs de calcul sur le FPGA.
- Analyser des performances et les comparer avec des résultats sur CPU et/ou GPU.
- Proposer et implémenter des solutions pour la génération de mots de passe (compteur et dictionnaire)
- Mise en place des communications et le protocole nécessaire pour garantir la fiabilité.
- Effectuer des tests unitaires et des tests d'intégration pour vérifier le bon fonctionnement du système.
- Optimiser les performances.

Candidat-e :

KANDIAH ABIVARMAN

Filière d'études : ISC

Professeur-e(s) responsable(s) :

UPEGUI ANDRES

En collaboration avec : ELCA Security

Travail de bachelor soumis à une convention de stage en entreprise : non

Travail de bachelor soumis à un contrat de confidentialité : non