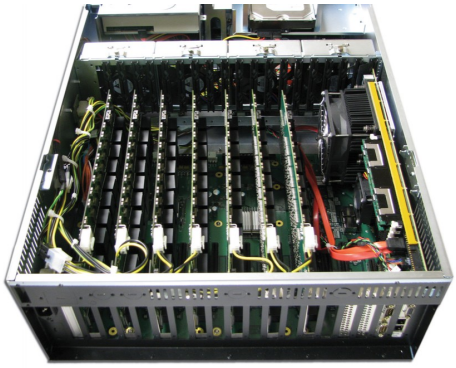
h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

RÉSUMÉ

Lorsqu'un utilisateur doit s'authentifier auprès d'un service, il doit fournir un mot de passe préalablement défini. Pour des raisons de sécurité, le système stocke ce mot de passe en le passant par une fonction de hachage. Ainsi, lors de l'authentification, le système compare le hash du mot de passe entré par l'utilisateur avec le hash stocké pour vérifier son identité. Une fonction de hachage qui est souvent utilisé pour le stockage de mots de passe est le Bcrypt, qui a comme particularité d'être assez lente, rendant les mots de passe assez résistante aux attaques par bruteforce. Ce rapport a pour but de détailler la mise en oeuvre d'un système visant à attaquer les mots de passe protégés par l'algorithme bcrypt en utilisant un Field-Programmable Gate Array (FPGA). L'objectif principal est de créer une solution extensible et plus performante que les approches traditionnelles basées sur Graphics Processing Unit (GPU). Le système repose sur plusieurs cœurs de calcul parallèles sur le FPGA pour générer les hashs bcrypt. Ce projet présente deux solutions distinctes pour l'implémentation d'une attaque par bruteforce. La première solution génère les mots de passe directement sur le FPGA, accompagnée d'une interface Universal Asynchronous Receiver Transmitter (UART) qui permet à l'utilisateur d'interagir avec le système. La seconde solution, encore en développement, repose sur l'utilisation de l'interface Peripheral Component Interconnect Express (PCIe) pour permettre des transferts de données rapides, rendant ainsi possible une attaque par dictionnaire. Après l'implémentation, des mesures ont été effectuées pour évaluer les performances et l'utilisation des ressources sur le FPGA. Bien que la solution basée sur l'interface PCIe ne soit pas encore entièrement opérationnelle, les résultats obtenus jusqu'à présent ouvrent la voie à des optimisations et des améliorations futures.



Candidat-e :

ABIVARMAN KANDIAH

Filière d'études : ISC

Professeur-e(s) responsable(s) :

ANDRES UPEGUI POSADA

En collaboration avec : ELCA Security

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

Travail soumis à un contrat de confidentialité : non