Hans WINDERIX – Résumé de la thèse

Les ordinateurs sont omniprésents dans notre société numérisée. Ainsi, nous sommes devenus dépendants des systèmes informatiques qui gèrent notre infrastructure critique et nous confions des informations sensibles à un nombre croissant d'applications. Nous pourrions donc nous attendre à ce qu'ils se comportent de manière correcte et sûre. Malheureusement, la réalité brosse un tableau plutôt sombre en ce qui concerne la sécurité de nos systèmes informatiques actuels.

La cause de ces vulnérabilités est souvent due aux hypothèses formulées par les développeurs lors de la conception et de la mise en œuvre de logiciels mais qui ne se sont plus valables lorsque le programme est exécuté par un ordinateur.

L'abstraction est une technique importante pour gérer la complexité des systèmes informatiques. Les programmes informatiques sont généralement écrits dans des langages de programmation de haut niveau. Ces langages proposent un certain nombre de concepts qui devraient permettre aux développeurs d'exprimer plus facilement les fonctionnalités des programmes informatiques et de raisonner sur les propriétés des programmes qu'ils conçoivent. Un compilateur est un programme informatique qui a pour tâche de réduire ces concepts (ou abstractions) à une représentation appropriée pour être exécutée par une machine ne disposant d'aucune notion des abstractions réalisées par les développeurs.

Cependant, cette approche présente un certain nombre d'inconvénients. Lors de la traduction entre ces deux mondes, un certain nombre de propriétés - souvent implicites - relatives à la sécurité, qui s'appliquent au niveau d'abstraction supérieur utilisé par le programmeur lorsqu'il étudie la sécurité de son programme, disparaissent. Cela rend le code machine vulnérable aux attaquants qui interagissent avec le système au niveau d'abstraction inférieur.

Avec une compilation sécurisée, l'objectif est de préserver les caractéristiques de sécurité exprimées par les concepts dans un langage de programmation de plus haut niveau une fois les programmes convertis en code machine exécutable. Cette technique permet aux développeurs de réfléchir à la sécurité des applications informatiques à un niveau d'abstraction confortable.

Le mémoire de maîtrise de Hans Winderix examine la faisabilité d'une plate-forme ouverte pour une compilation sécurisée, dans laquelle les propriétés de sécurité peuvent être présentées et traitées de manière explicite et générique aux différents niveaux d'abstraction. Une plate-forme où des modèles et algorithmes communs soutiennent de nombreux langages de programmation et architectures informatiques.

La contribution la plus importante de sa thèse est la proposition d'une telle plate-forme unifiée. Il a développé un prototype qui conserve la propriété d'isolation, exprimée dans les langages de programmation C et Rust, après compilation sur Sancus et Intel SGX, deux architectures de sécurité offrant des primitives matérielles permettant de maintenir efficacement l'abstraction de l'isolation après compilation.