Bureau d'étude - Mise en place d'une enclave sécurisée sur un processeur

La sécurisation de l'exécution des programmes tournant sur un système fait partie intégrante du processus de conception des processeurs modernes. Celle-ci passe le plus souvent par l'isolation de programmes vis-à-vis des autres, généralement de manière logicielle et reposant sur des mécanismes matériels bas niveaux. La première avancée déterminante dans le domaine a été l'invention du mécanisme de mémoire virtuelle, permettant ainsi d'isoler l'espace mémoire d'une application à l'autre, avec la mise en place d'un mode de fonctionnement privilégié (le mode noyau) inaccessible par les applications afin d'empêcher d'accéder au programme et aux données des autres applications tournant sur la machine.

Cette approche suppose une confiance pleine et entière dans ce fameux noyau, qui malheureusement peut se retrouver compromis par des vulnérabilités tant logicielles que matérielles. De plus, dans un contexte d'externalisation des services vers le "Cloud", cette confiance envers le noyau peut se réduire en la confiance dans le Cloud lui-même, avec un risque de fuite d'information sensible.

Dans ce bureau d'étude, nous nous proposons d'étudier et de concevoir un mécanisme complémentaire d'isolation des données sensibles sur une machine, à savoir une enclave. L'objectif sur le papier est simple : Avoir la garantie que même en cas de noyau malveillant, les données sensibles résidant sur la machine ne peuvent pas être compromises.

Pour ce faire, on se propose de faire évoluer le jeu d'instructions du processeur afin de permettre une telle isolation. Ci-dessous les considérations de conception de base que vous devez prendre en compte (elles seront raffinées au fur et à mesure que l'on ajoutera des fonctionnalités) :

> Les programmes et les données sensibles sont stockés dans la mémoire centrale au niveau d'une "zone isolée", c'est-à-dire une plage d'adresses contiguë non accessible aux applications non-isolées. Une représentation schématique de la mémoire centrale est présentée figure 1.

> On considère comme hors de porté d'un attaquant de lire manuellement le contenu de la mémoire centrale. Ainsi, seul le processeur peut lire et écrire dans cette mémoire.

> Toute information stockée dans la mémoire de masse est considérée comme parfaitement accessible par un attaquant.

> On considère que le processeurs possède, en parallèle du classique mode noyau/utilisateur, un mode enclave qui ne peut s'activer que si le processeur est en mode utilisateur et qui permet d'accéder à la zone isolée.

Question 1

A votre avis, pourquoi impose-t-on que le mode enclave ne puisse pas être activé lorsque le processeur est en mode noyau ?

Partie 1 - Intégration d'un mécanisme d'éviction de pages dans la zone isolée

Le mécanisme d'éviction de page est un mécanisme fondamental dans la gestion d'un système d'exploitation. Il permet, en cas de manque d'espace mémoire disponible dans la mémoire centrale, de faire migrer une page de la mémoire centrale vers la mémoire de masse. Compte tenu que la zone isolée à une taille fondamentalement bien inférieure à la taille de la mémoire centrale, il est indispensable de mettre en place un tel mécanisme au niveau de cette zone. Dans les systèmes courants, cette gestion incombe au noyau, qui a une vision globale de l'état d'utilisation de la mémoire. On souhaite, pour des raisons d'efficacité, maintenir cette gestion par le noyau, y compris de la zone isolée. Il faut néanmoins garder en tête que celui-ci n'est pas considéré de confiance.

L'objectif de cette partie est de proposer un mécanisme d'éviction assurant les propriétés de confidentialité, d'intégrité et d'authentification (en particulier vis-à-vis du noyau).

On se fixe une éviction en deux étapes, une première de la zone isolée vers la zone partagée, puis de la zone partagée vers le SWAP de la mémoire de masse. Une représentation schématique est proposé figure 2.

Question 2

(A faire valider par un enseignant) A partir des informations du cahier des charges, proposez un mécanisme permettant l'éviction d'une page de la zone isolée. Vous préciserez en particulier les étapes fondamentales à respecter (avec les différents modes du processeurs sollicités) ainsi que les algorithmes cryptographiques permettant d'assurer les propriétés de sécurité demandées.

Partie 2 - Intégration d'un mécanisme d'attestation à distance

Une autre propriété déterminante que doit proposer un processeur gérant la gestion d'enclaves sécurisées est de prouver que l'application s'exécute effectivement dans la zone isolée et non dans la zone partagée. Pour se fixer les idées, on considère que vous avez développé un service Cloud proposant une analyse des données génomiques de vos clients (Cf. RGPD). En parallèle, vous proposez une application cliente à télécharger sur un smartphone permettant d'envoyer le génome au service Cloud pour traitement.

L'objectif de cette partie est de mettre en place un mécanisme d'attestation à distance permettant de prouver que l'application s'exécute dans la zone isolée ainsi que la mise en place d'une connexion sécurisée avec l'application cliente.

Question 3

(A faire valider par un enseignant) A partir des informations du cahier des charges, proposez un mécanisme d'attestation à distance ainsi que le protocole d'échange associé afin d'assurer la confidentialité, l'intégrité et l'authentification de l'échange entre votre service Cloud et l'application cliente.

Annexe

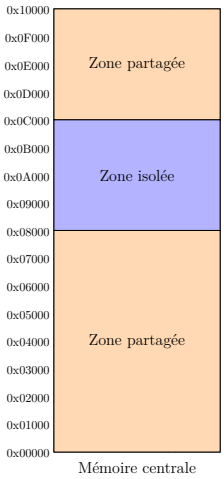

Figure 1: Représentation schématique d'un découpage possible de la mémoire centrale entre zone isolée et non-isolée.

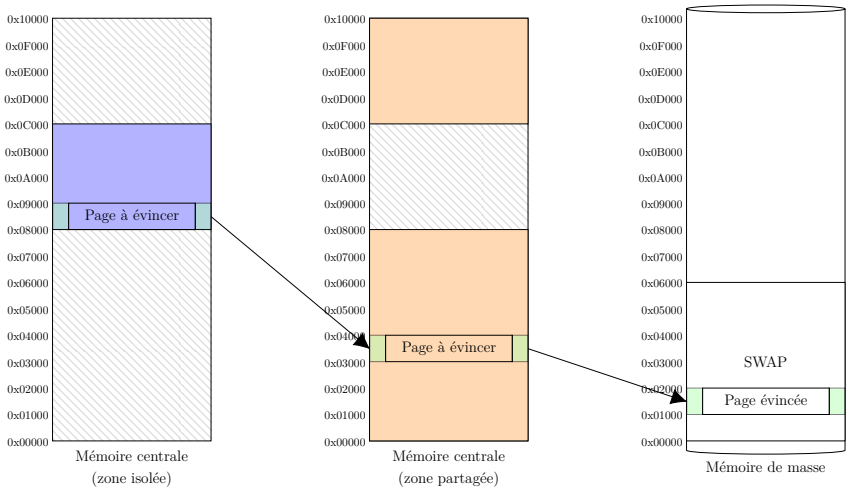

Figure 2: Représentation schématique de le l'éviction d'une page vers la mémoire de masse.