SafeNet Black Box, Solution de protection des logiciels par cryptographie
Sécurité
Posté par : JulieM
Publiée le : 4/4/2012 11:00:00

SafeNet, l'un des leaders mondiaux de la protection de données, annonce la première solution de protection des logiciels incluant une fonction de cryptographie en « **White Box** ».

La gamme de solutions de protection et de gestion des licences logicielles SafeNet Sentinel s'enrichit de nouvelles fonctionnalités qui protègent les algorithmes de sécurité contre les attaques visant les environnements en « white box », dans lesquels les agresseurs peuvent observer librement et modifier à leur guise l'exécution dynamique du code et les éléments internes détaillés des algorithmes.

Traditionnellement, dans le domaine de la protection des logiciels, la cryptographie - ou chiffrement - a toujours été virtuellement exécutée de façon directe, face à l'agresseur. Aucune «black box» n'a jamais protégé les clés secrètes et l'exécution des applications peut en fait être observée étape par étape par l'agresseur, lequel bénéficie d'une visibilité complète des données auxquelles il souhaite accéder.

Afin de mieux sécuriser les clés secrètes et de les protéger contre les actions malveillantes, une nouvelle approche s'avère par conséquent indispensable.

« *Notre solution en «white box» suppose que l'agresseur bénéficie d'une visibilité totale. Les clés de chiffrement et les algorithmes exposés à la vue des pirates sont remplacés par des bibliothèques d'applications spéciales qui minimisent la surface d'attaque* », explique **Michael Zunke**, directeur technique de SafeNet en charge des solutions de monétisation de logiciels.

« *Grâce à cette méthodologie, les clés protégées restent cachées des agresseurs et peuvent moins facilement être reconstituées au cours des attaques.* »

Avec la solution en «white box» de SafeNet, les communications entre les applications protégées et les tokens matériels sont totalement chiffrées, de sorte que les données qui empruntent le canal sécurisé ne peuvent être « réexécutées ». Contrairement aux solutions traditionnelles qui se contentent de masquer les clés de chiffrement, la solution de SafeNet est centrée sur la cryptographie en «white box», qui suppose que les agresseurs ont la possibilité de suivre les applications et les environnements d'exécution protégés pendant qu'ils recherchent les clés de chiffrement. Cette hypothèse faisant partie intégrante de la conception, les clés de chiffrement et des algorithmes sont remplacées par des bibliothèques d'interfaces API (Application Programming Interface) propriétaires qui appliquent le même chiffrement, mais en enfouissant la clé dans l'algorithme. La clé n'est ainsi jamais présente en mémoire et à ce titre, elle ne peut pas en être extraite. Chaque bibliothèque d'applications est générée de façon unique et rendue

impénétrable par obfuscation ou obscurcissement pour chaque éditeur de logiciels, rendant ainsi les exécutions d'attaques génériques virtuellement impossibles.