

Superviseur :

Marc Frappier

Contributeurs :

Karim Nacro

Thomas Lesieur

Projet informatique I (IFT592 / IFT596)

Titre :

Comparatif des outils d'inventaire cryptographique

Sujet :

Création d'un rapport comparant les différentes solutions pour la mise en place d'inventaire cryptographique en vue de la transition vers les algorithmes post-quantiques.

Mise en contexte :

Selon les experts, ce n'est qu'une question de temps avant que les ordinateurs quantiques, capables de briser les algorithmes fondés sur la cryptographie classique, fassent leur apparition. Dans ce contexte, il est nécessaire pour les entreprises traitant des données sensibles de planifier leur migration vers des algorithmes de cryptographie post-quantique (PQC). Pour ce faire, des outils permettant d'établir l'inventaire cryptographique (CBOM) à différents niveaux ont été développés dans les dernières années.

Cependant, puisqu'il s'agit d'un sujet relativement nouveau, il n'existe pas de rapport ou de référentiel largement reconnu qui compare les solutions disponibles sur le marché. Pour combler ce manque, notre projet de recherche vise à produire un rapport sous forme de « benchmark » qui examine et compare les possibilités offertes par ces différents outils afin de faciliter la prise de décision.