LA SÉCURITÉ DES PAIEMENTS, un enjeu primordial !

Le commerce électronique connaît un essor rapide au niveau mondial. Si ses avantages sont indéniables, il apparaît que celui-ci se heurte à certains obstacles. Un de ses principaux freins est lié à la sécurité des transactions et à la résilience des systèmes. Aujourd'hui, il existe une solution pour répondre à la problématique assez connue à laquelle les métiers de paiement font face, à savoir la sécurité cryptographique. Rencontre avec *Bruno Sanglé-Ferrière, président de Marbeuf Conseil et Recherche.*

Bruno Sanglé-Ferrière

Depuis 2018, vous concevez des systèmes de sécurité permettant d'améliorer la sécurité des systèmes de paiement dans une ère post-informatique quantique. Qu'en est-il ?
En effet, comme en témoignent les nombreuses attaques sur les sites informatiques, les dispositifs utilisés pour sécuriser internet ne sont plus aussi sûrs qu'ils l'étaient et le seront de moins en moins. Le système de signature électronique qui, par exemple repose sur des algorithmes dits de hash tels que MD5 ou SHA1 sont désormais réputés obsolètes. L'algorithme qui leur succède, SHA2 est encore considéré comme sûr, mais pour combien de temps ? Par ailleurs, la venue des ordinateurs quantiques sur lesquels de nombreuses sociétés et états travaillent d'arrache-pied pourra cracker non seulement ces algorithmes de hash mais aussi les systèmes de cryptages, notamment les systèmes de clés asymétriques, encore une fois nécessaires à la sécurité d'internet.

Vous avez donc créé un produit révolutionnaire pour le secteur bancaire…
Dans l'intention de créer un moyen de porter sur des moyens digitaux une monnaie, nous avons conçu un système permettant de garantir l'authenticité de fichiers inscrits dans des cartes de crédit et de transférer ces fichiers de carte à carte directement, sans internet, ou à travers internet. Souhaitant que la sécurité d'un tel système survive aux ordinateurs quantiques et aux progrès venant du travail des chercheurs en cryptographie, nous avons développé des techniques permettant de ne pas se reposer sur l'utilisation telle que nous la connaissons des signatures de type SHA ni sur les systèmes de cryptages.

Cette technologie ne nécessite pas beaucoup de puissance de calcul et peut donc fonctionner sur une puce ou un appareil différents de celles et ceux utilisés couramment pour les téléphones ou ordinateurs individuels. De plus, pouvant fonctionner en mode hors réseau elle a une capacité de résilience importante aux manques de couvertures des réseaux de téléphones, voire à leurs indisponibilités éventuelles.

Quels en sont les avantages et à quelles problématiques répondez-vous ?
La sécurité cryptographique est une véritable problématique. Elle est attaquée sur deux fronts : la possibilité de forger des données similaires ayant une même signature électronique ; et la capacité qu'ont les ordinateurs quantiques de défier les ordinateurs classiques pour inverser en un temps bref des fonctions utilisées en cryptographie que l'on croyait quasiment impossibles à inverser. Notre système est capable d'utiliser des signatures électroniques modifiées qui permettent d'éviter le premier problème, et d'utiliser des clés à usages uniques pour éviter le second problème, une telle clé cryptant une signature une seule fois avant de pouvoir être effacée, et ne nécessitant pas de fonctions soi-disant « non inversibles ». Il est conçu pour qu'une carte qui aurait utilisé toutes ses clés à usage unique pour communiquer avec une autre carte puisse obtenir de nouvelles clés, sans que l'autre carte n'ait à faire quoi que ce soit. Par ailleurs, ces clés, typiquement de 116 bits, sont plus petites que les clés asymétriques de chiffrement et permettent d'émettre des milliards de cartes pouvant s'échanger entre elles de l'argent ou des documents tout en réduisant à presque zéro la probabilité qu'il existe même une possibilité d'altérer le montant transféré au cours d'une communication en forgeant un message frauduleux.

Vos systèmes ont-ils d'autres avantages ?
Notre système permet en outre la vérification d'identité à distance, et en particulier si des cartes d'identité ou des passeports y étaient inscrits. Bien entendu, il incorpore des moyens de vérification biométriques permettant de renforcer la sécurité. Par ailleurs, nous proposons des procédures de mise à jour des documents permettant aux différents documents transférés de pouvoir évoluer au gré des technologies et aux éditeurs de documents de faire vivre leurs publications. Nous avons aussi imaginé une autre technologie permettant de protéger l'affichage des regards indiscrets ainsi que la possibilité de géolocaliser la contrepartie à laquelle on fait un paiement. ×