La cryptographie basée sur l'identité

Au service de la confidentialité des données

Introduction

La cryptographie basée sur l'identité (ou IBC pour « *Identity-Based Cryptography* ») est un domaine récent de la cryptographie moderne. Imaginée en 1984 par Shamir, célèbre mathématicien et cryptographe à l'origine de l'algorithme RSA lors d'un exercice de pensée, l'IBC ne restera pour l'essentiel qu'une fiction jusqu'en 2001, lorsque deux chercheurs de l'université de Stanford proposèrent un algorithme de chiffrement basée sur l'identité (*Identity-Based Encryption from the Weil Pairing* Franklin, D. Boneh (1)). Depuis, ce domaine est en pleine effervescence dans le monde académique : de très nombreuses équipes de recherche à travers le monde ont proposé successivement depuis le début des années 2000 nombre d'algorithmes basés sur « l'identité » de plus en plus sophistiqués et sécurisés (chiffrement, signature, broadcast, *etc.*). Ainsi, la première partie de ce rapport aura pour objectif premier de faire un état de l'art du domaine pour donner aux lecteurs les éléments de compréhensions, les enjeux et les contraintes essentielles de ce domaine prometteur.

Aujourd'hui, les processus cryptographiques traditionnels (la cryptographie symétrique et la cryptographie asymétrique) ne nécessitent plus autant qu'auparavant d'avoir une connaissance précise des éléments techniques fondamentaux sur lesquels ils reposent pour être utilisés en pratique au stade industriel et applicatif. En effet, la couche applicative est suffisamment dense et les algorithmes suffisamment matures pour pouvoir faire quasi abstraction des connaissances plus fondamentales. A rebours, la cryptographie basée sur l'identité repose sur des concepts et des objets mathématiques beaucoup plus jeunes, tout du moins concernant leur utilisation en cryptographie. C'est le cas des courbes elliptiques, et c'est encore plus le cas des « couplages » que nous introduirons dans la première partie du rapport (cf. page **Error! Bookmark not defined.**). Ces objets, encore peu connus et utilisés en comparaison avec les « robustes » corps finis utilisés par l'algorithme RSA, posent encore de nombreuses interrogations vis-à-vis de la sécurité.

Si l'IBC semble être un domaine prometteur, en témoigne l'importante activité à son sujet encore aujourd'hui, elle reste pour le moment à un niveau essentiellement académique et de recherche appliquée. Malgré quelques expérimentations à travers le monde (Voltage Security, HP Labs, Microsoft Recherche) très peu d'applications utilisant l'IBC ont pour le moment vu le jour. **La véritable motivation du travail effectué pendant six mois sur ce sujet était donc de franchir le cap entre le stade de recherche et le stade industriel en développant une solution innovante reposant sur l'IBC.**

Ainsi, dans la seconde partie du rapport, qui constitue **la véritable valeur ajoutée du travail effectué** pendant six mois, nous présenterons notre solution basée sur l'IBC, laquelle permet, entre autres, de sécuriser les échanges d'information dans les entreprises et organisations de tout type de manière plus simple, efficace et économique en comparaison avec les solutions actuelles du marché. A titre d'illustration, nous montrerons que notre solution pourrait permettre de garantir la confidentialité des données personnelles de santé, tout en conservant un haut niveau de praticité, dans un contexte où celles-ci sont de plus en plus amenées à être numérisées, transférées et partagées entre les différents praticiens et professionnels de santé dans ce qu'il est commun d'appeler aujourd'hui le « *Cloud* Santé ».

Conclusion

A l'heure de l'espionnage numérique de masse, il devient de plus en plus urgent pour les entreprises d'agir. Le chiffrement des données est un moyen efficace pour réduire l'impact et les conséquences éventuelles du cyber espionnage. Hélas, nous avons vu que les systèmes actuels, reposant sur l'utilisation d'une infrastructure à clé publique, étaient actuellement trop couteux et trop complexes à utiliser et à administrer pour la plupart des entreprises, à commencer par les PME/PMI et certaines administrations de l'Etat.

A la lumière de ce rapport, nous pouvons affirmer que la cryptographie basée sur l'identité, bien plus qu'un simple domaine de recherche académique foisonnant, représente dès aujourd'hui un terreau extrêmement fertile pour des innovations majeures. La cryptographie basée sur l'identité, et plus particulièrement l'algorithme d'IBE proposé en 2001 par Franklin et Boneh peut aujourd'hui être implémenté avec succès afin d'aboutir à de réelles applications industrielles. Ainsi, la solution que nous avons développée, permettant le chiffrement des données dans un contexte d'usages nouveaux, tel le *cloud computing* et les espaces de travail collaboratifs, n'est qu'une illustration du potentiel d'innovation de l'IBC.

Notre solution permet nous semble-t-il de réduire la « barrière à l'entrée » que doivent aujourd'hui franchir les organisations pour installer, utiliser et administrer un système complet de chiffrement des données (emails, documents partagés, *etc*.). Il nous a semblé également que la gestion des droits d'accès aux données numériques était aujourd'hui un enjeu majeur pour des organisations toujours plus dynamiques et complexes. C'est la raison pour laquelle, nous avons voulu mettre à profit le fort potentiel de l'IBE pour concevoir et développer une solution de chiffrement des données basée sur les rôles et les attributs des individus. Dans notre solution, la « clé » servant à chiffrer et la politique de divulgation des données ne font qu'un. C'est cette propriété de l'IBC qui permet à notre solution de réduire drastiquement les contraintes actuelles. En effet, les technologies du marché à base de PKI sont mal adaptées à la gestion de droits d'accès du type RBAC, car elles souffrent d'un problème de flexibilité et sont difficiles à administrer.

Un enjeu majeur nous semble également être celui de la confidentialité de données personnelles de Santé. Alors que le gouvernement souhaite relancer ce chantier important, à travers la généralisation du Dossier Médical Personnel (DMP), nous pensons que l'IBC ferait un excellent candidat pour en garantir la sécurité tout en permettant une gestion facilitée tant pour les praticiens que pour les patients.

Deux mouvements aujourd'hui antagonistes se font parallèlement : d'un côté la bataille pour la sécurisation des données dans un contexte d'espionnage mondial, et de l'autre la volonté des individus de pouvoir partager et s'échanger toujours plus facilement leurs données. Nous pensons que la cryptographie basée sur l'identité est une solution pour réconcilier ces deux mouvements apparemment contradictoires.