La sécurité des données numériques : gestion des identités, de la confiance et de la vie privée dans un univers numérique

IBM *Software Group*

Nous sommes heureux de vous accueillir pour le podcast sur la sécurité des données numériques. Christian Achermann s'entretient avec Jan Camenisch, scientifique au laboratoire de recherche d'IBM à Rüschlikon.

Christian Achermann : «Pouvez-vous nous donner quelques informations sur vous-même et sur votre fonction chez IBM ?»

Jan Camenisch : «Je fais partie de l'équipe des chercheurs de ce laboratoire et je suis cryptographe. Mais je suis également responsable du projet européen PrimeLife qui concerne la protection des informations personnelles sur Internet et qui porte sur la gestion des identités, de la confiance et de la vie privée dans un univers numérique.»

Christian Achermann : «Aujourd'hui, lorsqu'on utilise des services en ligne, on vous demande souvent de communiquer un grand nombre de données personnelles. Quels sont les risques inhérents à cette pratique ?»

Jan Camenisch : «D'un côté, vous risquez que les données que vous communiquez tombent entre de mauvaises mains, soit simplement parce qu'elles se perdent comme on le lit tous les jours dans la presse, soit parce qu'elles sont utilisées abusivement par les employés de la société à qui vous les transmettez. De l'autre, il existe aussi le risque que les données soient utilisées à des fins de « profilage ». Par exemple, si vous divulguez une information personnelle sur un réseau social, celle-ci pourra servir à un employeur potentiel pour décider de vous embaucher ou non.»

Christian Achermann : «Dans la dernière édition de THINK!, le magazine clients d'IBM, on peut lire que vous et votre équipe travaillez à une solution novatrice destinée à protéger les données sensibles, appelée « Identity Mixer ». Pourriez-vous nous dire où en est actuellement ce projet et nous expliquer les fonctions de votre solution ?»

Jan Camenisch : «Grâce à cette solution, nous cherchons à nous attaquer au problème de la divulgation d'un excès d'informations, et ce, sous trois angles. Nous essayons, premièrement, de réduire au minimum les données que les gens doivent divulguer, deuxièmement, d'aider les utilisateurs à faire confiance à leurs partenaires en ligne et, troisièmement, de redonner aux utilisateurs le contrôle de leurs données. Voici un exemple de minimisation du nombre de données : si vous possédez une carte d'identité électronique et que vous désirez prendre une bière dans un bar, vous devez souvent prouver que vous avez l'âge requis. Avec une carte d'identité électronique, vous divulguez toutes les informations qu'elle contient, y compris vos données personnelles. Grâce à notre technologie, vous pourriez révéler au barman que vous avez plus de 18 ans et rien d'autre. C'est cela la minimisation du nombre de données. A l'inverse, lorsque vous entrez dans un bar, vous voulez avoir l'assurance qu'il s'agit bien d'un bar et que vous parlez réellement à un barman.

Bien sûr, dans le cas du bar, c'est facile. Mais sur Internet, on n'est jamais certain du site avec lequel on communique et si on peut lui faire confiance. Les applications que nous sommes en train de développer permettent de créer facilement cette confiance. En ce qui concerne les données personnelles dont la divulgation est évidemment inévitable dans certains cas, nous informons d'abord l'utilisateur du sort qui leur est réservé – seront-elles conservées pendant dix ans ou au contraire effacées dès la fin de la transaction ? – et qui est autorisé à les utiliser et à quelle fin.
Certaines de ces solutions sont déjà disponibles pour téléchargement et une partie du code de base existe. Nous sommes toutefois encore en phase de construction et d'expansion. Nous recherchons un mode de standardisation et des interfaces utilisateurs rendant la technologie accessible au plus grand nombre possible et permettant au secteur industriel d'intégrer ces technologies dans ses logiciels, à mesure qu'elles évoluent vers une solution standard.»

Christian Achermann : «Quelles difficultés avez-vous rencontrées pendant le processus de développement ? Qu'avez-vous fait pour éviter ces inconvénients ?»

Jan Camenisch : «Cela fait plus de dix ans que nous travaillons à ces solutions et lorsque nous avons commencé, il s'agissait principalement de relever les défis mathématiques auxquels nous sommes confrontés en matière de cryptographie. Si j'ai une carte d'identité numérique qui confirme ma date de naissance, comment puis-je l'utiliser pour convaincre le barman que j'ai plus de 18 ans sans révéler ma date de naissance ? Comment élaborer les mécanismes cryptographiques nécessaires ? Une fois les solutions trouvées, le plus difficile a été d'expliquer leur fonctionnement à nos collègues afin qu'ils développent des interfaces utilisateurs permettant l'utilisation intuitive de ces technologies. Je pense qu'il s'agit là de la partie la plus importante. Sans bonnes interfaces utilisateurs, cette technologie ne sera jamais mise en œuvre et je pense que nous sommes encore au milieu du gué en matière de recherche dans ce domaine. Nous avons quelques ébauches de solutions, mais je suis persuadé que nous pouvons faire beaucoup mieux.»

Christian Achermann : «Dans une perspective d'avenir, comment votre solution continuera-t-elle d'être développée au cours des mois et des années à venir ?»

Jan Camenisch : «Je dirais que nous sommes plutôt arrivés au bout en ce qui concerne la technologie de base des algorithmes cryptographiques. Nous savons comment émettre des cartes d'identité électroniques et des certificats. S'agissant de la phase suivante, à savoir comment transmettre les données, nous sommes en train de standardiser les choses et de produire des normes et des protocoles de communication. Ici, nous parlons des instances de standardisation. Au niveau supérieur, celui des interfaces utilisateurs, nous avons les premières solutions, mais la recherche n'est pas terminée dans ce domaine. Par ailleurs, si nous considérons la façon dont les gens utilisent Internet aujourd'hui, par exemple en envoyant une grande quantité de données à travers les réseaux sociaux et les wikis, notre technologie ne s'applique pas facilement à ce domaine et nous devons poursuivre nos recherches afin d'imaginer la meilleure manière de protéger les gens. Ainsi, un futur employeur ne tombera pas obligatoirement sur les images de la dernière beuverie.»

Christian Achermann : «Pour conclure, dans la mesure où aucun produit de ce type n'existe actuellement sur le marché, comment peut-on protéger au mieux ses données personnelles ? Pouvez-vous faire quelques suggestions ?»

Jan Camenisch : «Je pense que la meilleure chose que vous puissiez faire est de faire très attention aux partenaires avec qui vous communiquez et aux données que vous portez à leur connaissance. Vous pouvez essayer de lire leurs règles en matière de respect de la vie privée, mais elles sont parfois très difficiles à trouver. Sinon, il me semble que j'utiliserais des cartes de crédit et des adresses e-mail à usage unique et que je ne donnerais pas d'informations personnelles exactes quand ce n'est pas nécessaire. Naturellement, si vous désirez vous faire expédier quelque chose chez vous, il faudra bien indiquer votre véritable adresse.»

Christian Achermann : «Merci beaucoup du temps que vous nous avez consacré et des nombreuses informations que vous nous avez données.»