

Comment on a sécurisé

Jean-Jacques Quisquater et Jean-Louis Desvignes

Dans les années 1980, on s'est aperçu que la carte à puce n'était pas sans faille. Un mariage avec la cryptographie, domaine alors en pleine renaissance, s'imposait d'urgence...

la carte à puce

Depuis son lancement il y a quatre ans, le paiement sans contact connaît un succès croissant. Trois milliards de transactions ont eu lieu en Europe avec une carte Visa sans contact entre mai 2015 et mai 2016, soit près de trois fois plus qu'un an plus tôt, a annoncé la société Visa Europe. Dans les commerces de proximité, une transaction sur cinq est effectuée par ce moyen, contre une sur soixante en 2013. En France, l'adoption de ce mode de paiement a augmenté de 230 % en un an, conduisant à 194 millions de transactions sur douze mois, concernant plus de 2 milliards d'euros. La confiance accordée à ce mode de paiement est grande. Pourtant, fondé sur une communication en champ proche (un lecteur communique par ondes radio avec la puce de la carte bancaire à l'aide d'une minuscule antenne si la distance qui les sépare est inférieure à 10 centimètres), il est loin d'être inviolable : certes, des précautions empêchent que l'on vide votre compte (plafond de retrait à 20 euros, nombre de paiements sans contact limité par jour...), mais aucune mesure de sécurité n'a été installée au sein de la carte pour bloquer ce type d'attaque. Rien non plus n'empêche un hacker d'intercepter vos données bancaires en passant un lecteur près de la poche où vous conservez votre carte.

L'ESSENTIEL

- À son apparition dans les années 1980 en France, la carte à puce était considérée comme inviolable.
- Mais bien vite, les premières attaques sont venues et il a fallu sécuriser davantage cette invention, d'autant que le ministère de la Défense envisageait son utilisation pour renforcer la sécurité de certains équipements de chiffrement.
- A commencé alors une course pour intégrer à la puce, malgré sa faible capacité, des algorithmes de cryptographie suffisamment puissants.

© Gettyimages/David Gould

Un million de dollars sur un plateau

En fait, le paiement sans contact n'est que le dernier rebondissement d'une longue histoire, celle de la sécurisation de la carte à puce, dont nous avons été tous deux des témoins et acteurs, l'un (Jean-Jacques Quisquater) pour la partie technologique, l'autre (Jean-Louis Desvignes) en tant que gardien de l'usage de la cryptographie, alors dédiée à des utilisations militaires et gouvernementales. Ce qu'il montre surtout, c'est que l'histoire se répète. Au début de l'usage de la carte à puce, dans les années 1980, il était commun de croire que celle-ci était incassable et digne d'une confiance totale. Cette confiance était si ancrée qu'elle nous offrit un million de dollars sur un plateau.

Lors d'une grande exposition à Bruxelles, vers 1985, un directeur de Philips avait imaginé de distribuer plusieurs dizaines de milliers de cartes à puce, avec comme mission pour les participants de trouver le code d'accès de quatre chiffres, le code PIN. Le premier qui réussirait gagnerait un million de dollars. Or un simple calcul de probabilités montrait que, statistiquement, vu le nombre de cartes distribuées et le nombre de participants,