Paiement par smartphone : des chercheurs exposent une faille de sécurité

Des spÃ©cialistes en cryptographie de lâ€™ETH Zurich, en Suisse, viennent de publier un article scientifique dÃ©crivant comment ils sont parvenus Ã contourner les sÃ©curitÃ©s du protocole de paiement par carte bancaire EMV pour rÃ©gler sans contact, par smartphone, nâ€™importe quel achat dans un commerce Â« physique Â».

Une application Android crÃ©Ã©e Â« sur mesure Â» pour tromper le terminal de paiement

La validation des rÃ¨glements par carte bancaire au moyen dâ€™un code secret est un gage de sÃ©curitÃ© dont la robustesse a Ã©tÃ© prouvÃ©e au fil des dÃ©cennies. Mais rÃ©cemment, avec la gÃ©nÃ©ralisation du paiement sans contact, il a Ã©tÃ© dÃ©cidÃ© de ne plus la rendre systÃ©matique. Comme le montre cette Ã©tude suisse, cette dÃ©marche a ouvert une boÃ®te de Pandore, permettant Ã des escrocs (pourvu quâ€™ils se soient prÃ©alablement prÃ©parÃ©s) Ã effectuer des rÃ¨glements avec des cartes bancaires dont ils ne sont pas les porteurs.

Au cours de leur expÃ©rience, les chercheurs de lâ€™ETH Zurich ont reliÃ© leur carte Visa Ã un smartphone, puis ont transfÃ©rÃ© les donnÃ©es de cette carte sur un autre smartphone, oÃ¹ Ã©tait installÃ©e lâ€™application Â« frauduleuse Â» quâ€™ils avaient conÃ§ue. Lorsque le terminal de paiement demandait un rÃ¨glement, ils approchaient du terminal ce dernier smartphone. Le terminal envoyait alors une requÃªte dâ€™authentification du porteur (en dâ€™autres mots, une requÃªte de saisie du code secret). Lâ€™application Â« frauduleuse Â» rÃ©pondait alors que le porteur avait dÃ©jÃ Ã©tÃ© identifiÃ© en locale, Â« hors ligne Â» (en dâ€™autres mots, sur le smartphone client - il nâ€™y avait donc pas besoin de lâ€™authentifier Â« en ligne Â» auprÃ¨s de la banque Ã©mettrice de la carte).

La validation Â« hors ligne Â» des transactions, un terreau fertile pour monter des escroqueries

Cette combine a pour effet dâ€™exclure complÃ¨tement lâ€™authentification Â« en ligne Â», Ã savoir lâ€™authentification du porteur de carte auprÃ¨s de la banque Ã©mettrice (qui, normalement, a lieu lorsque le terminal renvoie Ã la banque Ã©mettrice les paramÃ¨tres de la carte et le code secret saisi). La transaction est donc validÃ©e Â« hors ligne Â», par le seul terminal de paiement. Le client peur repartir avec son achat.

Ensuite, Ã la fin de la journÃ©e par exemple, le terminal communique Ã la banque le registre des transactions ayant Ã©tÃ© effectuÃ©es Â« hors ligne Â». Câ€™est Ã ce moment-lÃ que la fraude se dÃ©couvre, car la banque voit que la Â« clÃ© Â» censÃ©e authentifier le porteur (communiquÃ©e en lâ€™occurrence par le smartphone) nâ€™est pas la bonne, elle nâ€™est pas la mÃªme que la vraie Â« clÃ© Â», dont la banque a connaissance. Mais Ã ce moment-lÃ le client est bien sÃ»r dÃ©jÃ parti, impossible pour le commerÃ§ant de faire quoi que ce soit...