Le paiement par carte sous la loupe du Chaos Computing Club

Sécurisé les lecteurs de cartes bancaires utilisés par les commerçants ? Peut-être suffisamment pour le commun des consommateurs mais pas autant qu'il le faudrait aux yeux des hackers réunis lors la récente conférence du Chaos Computing Club. Karsten Nohl (de la firme berlinoise Security Research Labs) et son associé Fabian Braünlein ont profité de l'événement organisé par l'association allemande d'experts en sécurité informatique pour exposer leurs trouvailles sur deux protocoles de communication exploités par les lecteurs de cartes : ZVT (Zahlungverkehrsterminal) et Poseidon. Le premier est utilisé en jonction avec les systèmes de caisses en point de vente. Le second fait le lien avec les banques, en tant qu'implémentation du standard ISO 8583 (spécifications d'échange de messages dans le cadre de transactions financières), détaille *ITespresso.fr*.

ZVT était, à l'origine, conçu pour gérer le transport de données sur connexion série. Aujourd'hui utilisé sur protocole Ethernet, y compris sans fil (essentiellement en Wi-Fi), il n'embarque pas de mécanisme d'authentification : si un tiers arrive à se positionner sur le même réseau, il peut, par une attaque de type « man-in-the-middle », obtenir les informations associées à une carte – y compris le code PIN – pour ensuite la cloner. Les lecteurs disposent en théorie d'une zone sécurisée dont le code PIN ne sort jamais. Mais il existe une faille dans l'une des fonctions de ZVT, qui permet d'afficher du texte sur l'écran. Une faille qui pourrait typiquement être exploitée pour demander la saisie du PIN, lequel serait donc transmis en clair.

Car les caractères affichés sont liés à un code d'authentification de message (MAC), destiné à prouver que les données proviennent d'un tiers de confiance et qu'elles n'ont subi aucune modification. Mais ce MAC est mal implémenté : il est possible de le récupérer par le biais d'une attaque temporelle, qui consiste à estimer et analyser le temps mis pour effectuer certaines opérations cryptographiques. Dans le cas présent, le terminal de paiement met un peu plus de temps à accepter le bon MAC qu'à en rejeter un mauvais…

S'attaquer aux lecteurs de cartes

ZVT peut aussi être détourné pour s'en prendre directement à un commerçant plutôt qu'au porteur de carte. Chaque lecteur dispose d'un identifiant unique qui permet de déterminer son propriétaire. Il a aussi un numéro de port pour la communication des données, le tout étant configuré par la banque, en association avec un compte où sont déposés les fonds collectés. ZVT permet de reconfigurer ces éléments dès lors que l'on se trouve sur le même réseau que le terminal.

Modifier l'identifiant requiert un mot de passe, mais celui-ci est fixe et largement accessible en ligne. Une réinitialisation modifie des éléments comme le nom du magasin, mais le protocole Poseidon permet de restaurer l'ensemble pour cacher plus efficacement l'attaque.

Copier les lecteurs

La troisième démonstration effectuée par Karsten Nohl et Fabian Braünlein se base uniquement sur Poseidon. Elle implique l'achat, par le pirate, de n'importe quel lecteur de cartes qui sera configuré à l'identique de celui de la victime. Pour faire la jonction avec l'organisme qui traite les paiements, le terminal du marchand envoie son identifiant via un port de communication particulier et reçoit, en réponse, des données de configuration chiffrées.

Communiqués de manière séquentielle, les identifiants sont de surcroît lisibles sur chaque reçu imprimé. Une aubaine pour des tiers malveillants. Quant aux données chiffrées, elles sont protégées par un mot de passe qui est généralement le même pour tous les marchands associés à un même organisme de gestion des paiements (on trouve les principaux sur le Web).

Force brute

Pour ce qui est de la configuration des communications, il suffit de procéder par force brute, en testant chaque port jusqu'à trouver celui qui répond. Reste alors à reprogrammer le lecteur de cartes acheté. Ce lecteur peut ensuite être utilisé pour des « remboursements » abusifs : en d'autres termes, débiter de l'argent sur le compte du marchand, sans forcément qu'il y ait eu auparavant une transaction en sens inverse.

ZVT est surtout utilisé en Allemagne, mais quelques autres pays d'Europe l'ont adopté. L'alternative OPI (Open Payment Initiative) est plus récente, mais ne propose toujours pas d'authentification alternative. Quant aux fonctions de commande et de configuration à distance, elles ne sont pas nativement disponibles… mais de nombreux marchands les ont ajoutées via des extensions, note Reuters.

Lire également
Enquête : Le paiement mobile NFC sécurisé, vraiment ?

crédit photo : LDprod / Shutterstock