La sécurité de millions de cartes à puce sans contact sérieusement remise en question

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 21 juillet 2008

Selon une étude dont NXP a tenté d'interdire la publication, des failles sur ses cartes Mifare Classic permettent de les cloner.

C'est finalement la liberté d'expression qui l'a emporté. La justice néerlandaise vient d'autoriser des chercheurs de l'université Radboud de Nimègue, aux Pays-Bas, à révéler les failles de sécurité qu'ils ont découvertes dans des cartes à puce sans contact Mifare, cartes déjà vendues à plusieurs centaines de millions d'exemplaires dans le monde (1).

Ces chercheurs avaient démontré depuis quelque temps qu'ils étaient en mesure de casser la sécurité des puces dites Mifare Classic, commercialisées par le fondeur néerlandais NXP. Ces puces, qui utilisent la technologie NFC (Near Field Communication, qui opère à moins de dix centimètres) pour communiquer, équipent des cartes servant à sécuriser une multitude de services (transport, accès à des locaux, services administratifs, etc.). Les transports londoniens l'emploient par exemple pour une carte de transport électronique rechargeable (le système Oyster) utilisée par quelques 17 millions d'usagers.

Pour la justice, NXP est responsable de la sécurité de ses puces

Selon les chercheurs néerlandais, il est possible, grâce à un scanner, de récupérer la clé de chiffrement contenue dans les cartes de ce type et dans les lecteurs correspondants. Les données récupérées par le scanner sont ensuite exploitées pour dupliquer des cartes existantes ou en créer de nouvelles et ainsi pénétrer dans des locaux ou voyager gratuitement sans être inquiété.

Dénonçant les risques qu'entraînerait la divulgation de ces secrets, NXP avait saisi la justice néerlandaise afin que les chercheurs ne puissent publier leur étude. Ces derniers comptaient en effet profiter d'une conférence dédiée à la sécurité en Espagne en octobre prochain pour présenter leurs travaux. « Les dommages éventuellement subis par NXP ne résulteraient pas de la publication de cette étude mais de la production et de la vente d'une puce apparemment défectueuse », a fait valoir le tribunal d'Arnhem qui a rejeté vendredi dernier la requête de NXP.

Un secret de Polichinelle pour les experts en sécurité

Depuis plusieurs mois déjà, la sécurité des puces Mifare Classic était de plus en plus sujette à caution. En mars dernier, un analyste du Burton Group avait tiré la sonnette d'alarme sur son blog, citant notamment les travaux du chercheur Karsten Nohl. Selon les experts, c'est l'algorithme Crypto1 utilisé par les puces Mifare qui serait défaillant. Le fait que la clé de chiffrement utilisée ne mesure que 48 bits faciliterait en outre le travail des pirates. « Si l'algorithme est bien sécurisé, il faut essayer toutes les clés [ici au nombre de 2^48 , NDLR], ce qui est très long. Mais, s'il présente des failles, les pirates peuvent gagner un temps considérable », explique François Vacherand, chef du service architecture et sécurité des technologies de l'information au Léti (2).

NXP a fait l'erreur de garder secret l'algorithme Crypto1, qui est intégré aux lecteurs et aux cartes Mifare Classic. « Si l'algorithme reste secret, la communauté des chercheurs ne peut pas tester sa fiabilité. Aujourd'hui, une tendance forte est d'utiliser des algorithmes publics éprouvés avec des clés secrètes », note François Vacherand. Selon lui, la publication de l'étude néerlandaise confirmant l'existence de failles dans les puces Mifare Classic amènera forcément les clients de NXP à reconsidérer leur analyse de risque lors de la mise en oeuvre de ces cartes - autrement dit à reconsidérer leur choix.

Pour les clients déjà équipés, NXP proposera d'ici à la fin de l'année une solution plus sécurisée, baptisée Mifare Plus, utilisant l'algorithme public AES. Cependant, la migration de la technologie actuelle à la nouvelle sera évidemment très coûteuse. Reste à savoir qui paiera l'addition.

(1) Les puces Mifare Classic sont utilisées partout en Europe, notamment en France mais surtout au Royaume-Uni, aux Pays-Bas et en Belgique.

(2) Laboratoire d'électronique et de technologie de l'information du Commissariat à l'énergie atomique (CEA).

Post-scriptum :

http://www.01net.com/editorial/3871...