NXP embarrassé face au piratage de sa carte à puce sans contact Mifare Classic

- Technologie -

Date de mise en ligne : mercredi 12 mars 2008

Spyworld Actu

NXP reconnait implicitement que la protection de sa carte Mifare Classic 4K a été compromise. Il étudie les contre-mesures réalisables dans un système global afin que des couches de sécurité différentes détectent les éventuelles attaques dues à la carte.

Alors que les transports publics Néerlandais ont finalement décidé de conserver la carte de paiement sans contact de technologie Mifare Classic 4K dont l'algorithme de protection a été piraté, NXP Semiconductors le concepteur de la carte, a pour sa part réagi le 6 mars. Pour résumer, le fondeur ne dément pas le fait que la protection de la carte ait été effectivement compromise, il dialogue même avec les « chercheurs » qui ont brisé les protections, afin d'évaluer les contre mesures à déployer dans le cadre d'un système global. Il procède de même avec des intégrateurs spécialisés. NXP insiste sur le fait que la sécurité d'un système de paiement dans les transports doit s'appréhender dans son ensemble. La faiblesse d'un composant doit être compensée par d'autres couches de sécurité. On détecte même dans le propos de NXP une légère possibilité de se dédouaner de ses éventuelles responsabilités, puisqu'il évoque le fait qu'un responsable d'un système de transports fait usuellement appel à des consultants en sécurité afin d'évaluer l'ensemble des risques et des contre-mesures nécessaires. Enfin, NXP rappelle que le niveau de sécurité doit aussi résulter d'un compromis entre les performances et les coûts.

Un communiqué émis par NXP

Dans le détail, le fondeur a émis un communiqué qui rappelle que ses puces Mifare Classic sont utilisées dans le monde entier dans des systèmes de transport. Il décrit la carte Mifare Classic comme un composant d'entrée de gamme (NDLR : la carte embarque essentiellement de la mémoire, et non un processeur comme dans le cas d'une carte bancaire) faisant partie d'une famille de produits destinés aux applications de cartes à puce sans contact. Elle n'est utilisée ni dans les passeports électroniques, ni dans les cartes bancaires traditionnelles ni dans la sécurisation de véhicules. De plus, NXP souligne que le travail réalisé pour obtenir l'algorithme de chiffrement de la carte Mifare Classic a été entrepris par des chercheurs très compétents qui ont effectué le « reverse engineering » du composant ; une tâche qui a réclamé beaucoup de temps et de ressources.

Un dialogue ouvert avec les chercheurs

NXP affirme qu'il a établi un dialogue ouvert avec ces chercheurs et qu'il évalue les attaques possibles et les contre mesures qui puissent être prises dans un système global. NXP travaille activement avec des intégrateurs qui ont l'expertise nécessaire pour prendre les mesures appropriées dans les infrastructures qui utilisent la carte Mifare Classic. NXP ajoute que la puce sans contact n'est qu'un élément dans un système complet, qui comprend habituellement différentes couches de sécurité. En pratique, les systèmes ayant de multiples couches de sécurité de bout en bout, ont le moyen de détecter des cartes falsifiées et de réagir rapidement. Même si une couche est compromise, les autres couches empêcheront tout usage détourné.

Equilibrer les coûts et les performances

NXP poursuit en indiquant que de manière usuelle, les responsables des transports demandent à des experts en sécurité d'identifier les attaques potentielles autant que les contre-mesures. En matière de système, l'établissement d'une infrastructure appropriée, les risques potentiels, les performances et les coûts doivent être étudiés avec soin, afin d'obtenir un compromis équilibré entre l'investissement et les fonctions. NXP rappelle qu'il propose une large gamme de puces avec différents niveaux de chiffrement de sécurité, afin que les intégrateurs puissent retenir la solution adaptée en termes de sécurité du composant et du back office et de répondre aux contraintes de

confidentialité et de sécurité. NXP travaille avec de nombreux responsables des transports globalement afin d'aider leurs intégrateurs de systèmes à concevoir et à bâtir des systèmes qui soient appropriés. NXP prend au sérieux les revendications (NDLR : au sujet du piratage) et continue de suivre la situation, évalue ses produits et ses mesures de sécurité, et reste ouvert à la discussion avec toutes les parties intéressées. Affaire à suivre.

Post-scriptum :

http://www.reseaux-telecoms.net/act...