Théorie et pratique de la cryptographie en boite blanche.

Azevedo Oliveira Paco*[1,2]

[1]Laboratoire de Mathématiques de Versailles – Université de Versailles Saint-Quentin-en-Yvelines, Université Paris-Saclay, Centre National de la Recherche Scientifique – France
[2]Thales – Thales (France) – France

Résumé

Historiquement, la cryptographie s'est concentrée sur la sécurité des communications face à des adversaires "mathématiques",
qui ont accès à l'entrée et la sortie de l'algorithme. Depuis les années 2000, certain travaux ont mis en évidence que ce modèle n'était
pas le plus adéquat lorsqu'un algorithme est exécuté sur un appareil physique, par nature imparfait.
L'objectif de cette présentation est d'introduire le modèle de la boite blanche, dans lequel l'adversaire a un contrôle total de l'environnement d'exécution de l'algorithme. Dans un tel modèle, particulièrement favorable à l'attaquant, aucune implémentation publique connue de standards tels que AES ou ECDSA ne résiste à des attaques automatiques.

Pourtant, en parallèle, de nombreuses entreprises (parmi lesquelles Thales) vendent des implémentations boite blanche de standards cryptographiques, validées par des laboratoires d'attaques.
Dans cette présentation je propose de définir le modèle théorique de la boite blanche et d'expliciter les différences entre la boite blanche théorique et son application en pratique dans les entreprises. Finalement, je présente un schéma de masquage dans le modèle de la boite grise, CAPA censé offrir une résistance combinée (contre les attaques passives et actives) à un implémentation d'un algorithme. Je montre que cet algorithme de masquage n'offre en réalité aucune sécurité, ce qui le rend impossible à utiliser dans le modèle de la boite blanche.

*Intervenant