

Louvain-la-Neuve, jeudi 8 septembre 2011

Recherche UCL

Un chercheur UCL s'attaque à la sécurité de nos données personnelles

François-Xavier Standaert est professeur au pôle en ingénierie électrique de l'UCL. Ses recherches ont pour but d'analyser et d'évaluer la sécurité de systèmes cryptographiques. La cryptographie s'intéresse à la sécurité de l'information. Elle s'attache à protéger des messages, assurant leur confidentialité et leur intégrité lors de communications électroniques (e-mails, services bancaires,...). L'objectif du chercheur UCL ? Limiter l'information disponible aux adversaires éventuels, et rendre son exploitation la plus difficile possible. Il vient d'ailleurs de décrocher une bourse européenne ERC (Conseil européen de la recherche), pour la poursuite de ses recherches.

En cryptographie, la protection des données ne se base jamais sur le secret des méthodes utilisées, mais bien sur celui d'une clé numérique (similaire à un mot de passe). Dans les modèles classiques (exclusivement mathématiques), il s'agit de quantifier la sécurité face à un adversaire qui espionne les messages chiffrés échangés sur un canal de communication. On parle d'attaques physiques lorsqu'un pirate espionne non seulement les entrées et sorties d'une carte à puce, mais profite aussi d'autres canaux de communication. Par exemple, la consommation électrique d'un circuit peut être utilisée pour réaliser une sorte d'électro-encéphalogramme, qui donne à l'adversaire des informations supplémentaires pour retrouver les clés de protection.

Il en résulte de nombreuses questions, notamment liées à la difficulté de quantifier exactement l'information contenue dans ces électro-encéphalogrammes. Car à l'instar des applications médicales, une extraction optimale de l'information est ici cruciale. Si le concepteur d'un système ne le prémunit pas contre la totalité des fuites d'informations physiques, il devient impossible de garantir qu'un adversaire ne tirera pas parti d'un excédent d'information.

Cette recherche s'organise en deux axes principaux. Dans un premier temps, il s'agira de développer de nouveaux outils qui permettront d'analyser la sécurité physique d'un circuit de façon objective. Cette partie de la recherche a donc de fortes connections avec les applications réelles. Pour l'utilisateur final, elle devrait permettre d'augmenter la confiance en différents objets cryptographiques, en augmentant la transparence de leurs évaluations. Ensuite, l'objectif sera de concevoir de nouvelles techniques de chiffrement, mieux connectées à la réalité physique. La sécurité d'un système n'étant jamais absolue, ce second objectif se mesurera en termes de compromis entre sécurité mathématique, sécurité physique et efficacité des mises en œuvre.

En parallèle de ses recherches, François-Xavier Standaert s'intéresse au caractère parfois intrusif des technologies de l'information et de leurs applications quotidiennes, impliquant une réflexion en termes d'éthique et de respect de la vie privée.

INFOS PRATIQUES

Infos : <http://perso.uclouvain.be/fstandae>

Qui ? François-Xavier Standaert, professeur au pôle en ingénierie électrique de l'UCL : 010 47 25 65