



Paris, août 2008

## Actualité Recherche

### > Un concours international de cryptologie, organisé par l'Institut Télécom, pour aider à parer aux attaques sur les cartes à puce

Depuis plusieurs mois, des chercheurs de Télécom ParisTech ont lancé un concours international d'évaluation de la sécurité des composants cryptographiques embarqués : le *DPA Contest*. Un événement majeur pour les chercheurs mais aussi les professionnels, notamment de la banque, dans un univers où la culture du secret domine. Les premiers résultats seront restitués du 6 au 9 septembre 2009 lors de la conférence CHES (*Workshop on Cryptographic Hardware and Embedded Systems*).

#### Quelle sécurité pour nos cartes bleues et nos téléphones ?

Les composants de cryptographie embarqués sont très présents dans notre quotidien car on les retrouve dans les puces de carte bleue ou de téléphone pour protéger les données et les communications. Pour autant, ils sont vulnérables face à des attaques via le courant électrique consommé ou les ondes électromagnétiques.

Différentes parades théoriques ont été publiées du côté des chercheurs, mais leur réelle efficacité reste délicate à jauger. Du côté des industriels, chacun a sa recette secrète mais les attaques ont au moins une longueur d'avance sur les contre-mesures. Il devient dès lors primordial de disposer d'une méthodologie standard d'évaluation sécuritaire.

#### Décloisonner en mettant en commun les méthodes et les résultats

Pour Jean-Luc Danger et Sylvain Guilley, chercheurs à Télécom ParisTech, « dans un univers où la culture du secret domine, il est difficile de confronter des approches concurrentes. Ce concours vise à remédier au cloisonnement actuel en promouvant l'examen critique des recettes propriétaires par un accès complet à leurs spécifications, un peu comme dans le domaine du logiciel libre ». La démarche du *DPA Contest* est donc imprégnée du désir d'établir davantage de transparence dans le domaine émergent de la sécurité des implémentations.

Le passage d'une standardisation des primitives cryptographiques à celle de leurs implémentations est à la clé ! Et intéressera autant les banques que les domaines de la sécurité d'Etat...

Pour atteindre cet objectif, le site web <http://www.dpacontest.org/> propose des mesures de canaux auxiliaires accessibles publiquement. Elles font office de référence pour évaluer la force d'une attaque. Dans le moyen terme, elle pourrait servir de support standardisé. Plus de 100 000 mesures de référence peuvent être ainsi téléchargées depuis un serveur de base de données. Toute personne ou établissement désireux de profiter de cette dynamique est invité à participer.

Pour Francis Jutand, directeur scientifique de l'Institut Télécom « c'est une façon pour l'Institut Télécom de faire profiter la communauté internationale de son expérience cumulée dans le domaine de la sécurité des composants cryptographiques, et plus particulièrement pour les laboratoires de Télécom ParisTech d'affirmer leur expertise dans la conception de systèmes de sécurité ». L'Institut Télécom joue ainsi pleinement son rôle académique en suscitant un travail ouvert (basé sur l'accès aux codes sources) et collaboratif (chacun peut contribuer librement en déposant en ligne son algorithme d'attaque).

#### Chercheurs et spécialistes se retrouvent à Lausanne pour les résultats du concours 2009

Depuis le lancement du concours en août 2008, 3700 personnes ont consulté le web et/ou téléchargé les données de recherche depuis 43 pays, comme la France, le Japon, l'Allemagne, les Pays-Bas, les Etats-Unis, la Belgique, la Chine, la Corée du Sud... A ce jour, 30 soumissions originales ont été reçues. Les participants au concours sont autant des laboratoires publics que privés.

Les résultats du DPA Contest seront annoncés lors de la session plénière de la conférence phare du domaine (CHES) qui aura lieu à Lausanne du 6 au 9 septembre et à laquelle plus de 250 personnes, chercheurs et spécialistes de la cryptographie, participeront. Sylvain Guilley présentera le vainqueur du concours avant de lancer l'édition 2010.

Plus d'information sur la conférence : <http://www.chesworkshop.org/>

**Contact presse : Pleon**

Julie Ferroux – +33 (0)1 53 04 24 02 – [julie.ferroux@pleon.com](mailto:julie.ferroux@pleon.com)

Esla Portal - +33 (0)1 53 04 23 10 – [elsa.portal@pleon.com](mailto:elsa.portal@pleon.com)

**Institut Télécom**

Jérôme Vauselle - +33 (0)1 45 81 75 05 – [jerome.vauselle@institut-telecom.fr](mailto:jerome.vauselle@institut-telecom.fr)