



Paris, le 11 décembre 2008

COMMUNIQUE DE PRESSE

> L'Institut TELECOM dévoile ses circuits cryptographiques les plus robustes

Le retrait d'espèces à un distributeur de billets, le passage à un portique de transports en commun avec un badge sans contact, l'identification chez un médecin par le biais d'une carte Vitale, ou encore le téléchargement d'une chanson sur un baladeur numérique sont autant d'actes quotidiens qui font intervenir des circuits cryptographiques (clés mathématiques) nécessaires à la sécurisation des données. Mais ces circuits doivent être protégés contre les attaques « physiques » qui tirent partie de l'information véhiculée par le courant électrique et le rayonnement électromagnétique qu'il émet.

Protéger les circuits cryptographiques grâce à des logiques électroniques sécurisées

Qu'ils revêtent la forme d'une carte à puce ou d'un terminal électronique portable, les circuits cryptographiques permettent d'engager des transactions en toute confiance. Pourtant, de nombreux acteurs malveillants sont en permanence tentés d'abuser de ces facilités dans l'optique de se faire passer de façon illégitime pour quelqu'un d'autre ou simplement pour contourner une mesure technique de protection. Même si les algorithmes utilisés sont mathématiquement robustes, il est possible de compromettre la sécurité d'un circuit cryptographique en espionnant son fonctionnement interne à l'aide de matériel de laboratoire (sondes de courant, antennes, oscilloscopes, etc.).

Les chercheurs de TELECOM ParisTech développent précisément des contre-mesures visant à rendre les circuits cryptographiques aussi immunes que possible à ce type d'assauts de cybercriminels. Des styles de logique électronique, dont la consommation électrique est rendue aussi équilibrée que possible, ont ainsi été conçus et testés pour garantir la sécurité des systèmes.

La meilleure résistance aux attaques de l'état de l'art

Les cartes à puces actuellement disponibles sur le marché proposent de nombreux chausse-trappes et autres mécanismes de prévention d'attaques. Parmi toutes les solutions possibles pour lutter contre les attaques en observation de la carte, TELECOM ParisTech a exploré et perfectionné celle qui garantit une consommation constante ; dans ce créneau, les contre-mesures inventées à l'Institut TELECOM résistent le mieux aux attaques de l'état de l'art. Les parades à l'introspection maligne mises en œuvre, rassemblées sous le terme de SecLib (Secured Library), combinent une logique de calcul à activité constante avec une complète symétrisation des chemins de données et un soin extrême apporté à l'équilibrage de l'apport d'énergie et à l'isolation électrique des signaux contre la diaphonie.

L'évaluation sécuritaire la plus poussée montre que la logique SecLib est au moins dix fois plus solide que la logique sécurisée WDDL, très étudiée dans le monde académique, et que la puissance d'une attaque, en nombre de mesures à effectuer, pour (éventuellement) mettre à mal SecLib est d'au moins 350 fois supérieure à celle d'un style de logique de référence.

[Référence bibliographique : <http://doi.ieeecomputersociety.org/10.1109/TC.2008.109>]

Une collaboration de plusieurs années avec STMicroelectronics

Fruit de 5 années de collaboration avec le fabricant de circuits intégrés Franco-Italien STMicroelectronics, la logique SecLib a été validée sous diverses formes dans les circuits durcis de la famille "SecMat" (Sécurité du Matériel), ASIC en technologie 130 nanomètres. Ces « cartes à puces académiques » ont permis de mettre en œuvre nombre d'attaques sur des prototypes matériels et d'évaluer la robustesse des contre-mesures.

De la recherche à la création d'entreprise innovante

Profitant de leur expertise dans le domaine de la sécurité, 4 chercheurs de TELECOM ParisTech se sont rassemblés pour créer Secure-IC (<http://www.secure-ic.com/>). Cette *spin-off* a pour objectif de

fournir des services aux grandes entreprises de la Défense afin de protéger, au-delà des cartes à puces, les circuits à "haute performance", tels que les FPGA, contre des menaces similaires.

Contact presse : Agence Point Virgule

Chrystel Libert – +33 (0)1 73 79 50 63 – clibert@pointvirgule.com

Solenn Morgon – +33 (0)1 73 79 50 70 – smorgon@pointvirgule.com

Institut TELECOM

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

A propos de l'Institut TELECOM www.institut-telecom.fr

L'Institut TELECOM est un organisme d'enseignement supérieur et de recherche en sciences et technologies de l'information et de la communication (STIC). Il regroupe les grandes écoles TELECOM ParisTech, TELECOM Bretagne, TELECOM SudParis et TELECOM Ecole de Management ainsi que deux filiales TELECOM Lille1 et EURECOM soit 5000 étudiants, 600 enseignants-chercheurs et 800 doctorants, post-docs et sabbatiques. Depuis mai 2008, l'Institut TELECOM, acteur européen de référence en STIC, compte également deux écoles associées : TELECOM Saint-Etienne et l'ENSPS.

TELECOM ParisTech : première grande école française d'ingénieurs dans le domaine des sciences et des technologies de l'information et de la communication (STIC), TELECOM ParisTech forme les ingénieurs de la société de l'information. L'enseignement prépare les étudiants à devenir acteurs du domaine des STIC, aujourd'hui omniprésent et facteur de croissance rapide de l'économie. L'école, membre fondateur de ParisTech, aux côtés de onze des plus prestigieuses grandes écoles françaises, est aussi un centre de recherche reconnu internationalement et héberge deux incubateurs.