

## START UP

EN PARTENARIAT AVEC 

# Puce blindée pour cartes ultrasensibles

**NOM :** Secure-IC.**DATE DE CRÉATION :** janvier 2010.**DOMAINE :** nanotechnologies.**INNOVATION :** brevets en sécurité physique de composants électroniques critiques.

Concevoir une puce résistante à n'importe quelle attaque, tel est l'objectif de la start up Secure-IC. Lauréate 2010 du Concours national d'aide à la création d'entreprises innovantes du ministère de l'Enseignement supérieur et de la Recherche, cette jeune pousse s'appuie sur les huit brevets déposés en 2007 par les chercheurs de l'Institut Télécom Paris-tech. Ceux-ci visent, notamment, à empêcher l'extraction de données confidentielles sur des composants électroniques critiques : cartes bancaires, équipements de communication militaires... Soit toutes les plateformes à valeur ajoutée nécessitant intégrité et confidentialité de leur contenu.

## Associer sécurité et preuve formelle

Différentes de celles rencontrées dans l'univers informatique, les attaques connues adressant l'électronique sont dites passives ou actives. Les premières consistent en une interprétation des signaux électriques au travers de sondes électromagnétiques. Il est ainsi possible, par exemple, de découvrir le code secret d'une carte bancaire au moment de la saisie. Les secondes procèdent par injection de « fautes », à savoir des envois de surtensions, de tirs laser, voire des attaques sur l'horloge du composant électronique. Il s'agit, cette fois, d'en empêcher le bon fonctionnement.

Secure-IC vise aujourd'hui le plus haut niveau de certification de sécurité : EAL 7. « *Nous associons sécurité*

*et preuve formelle* », explique Hassan Triqui, son président. Par preuve formelle, il faut comprendre que la start up peut attester de l'efficacité de ses procédés par l'intermédiaire d'une démonstration mathématique. Une réelle innovation en électronique issue de l'univers de l'informatique, la modélisation d'un circuit électronique n'étant pas chose triviale.

## La défense intéressée

Secure-IC a malgré tout développé en parallèle un équipement afin d'évaluer la robustesse de ses algorithmes de chiffrement en mesurant leur niveau de vulnérabilité. « *Nous apportons également à nos clients tout l'environnement de développement et de débogage. Dans le cas, par exemple, d'une application de type passeport, nous fournissons les piles logicielles métier liées au marché de l'identification, tel le protocole cryptographique lié à un passage de frontière* », explique Hassan Triqui.

Travaillant sur des projets sensibles, les dirigeants de Secure-IC restent discrets quant aux noms de leurs clients, mais laissent entendre que le milieu militaire n'est jamais très loin et que le marché de l'identification s'avère être le plus porteur. « *Nous nous sommes positionnés sur ce marché car les réponses apportées actuellement ne sont pas encore satisfaisantes* », estime Hassan Triqui. ■

STÉPHANE BELLEC

## REPÈRES

**Siège :** Rennes (35).**Effectif :** 15 personnes.**Financement :** 350 k€ d'Oséo.

### L'équipe dirigeante :

**Hassan Triqui**, président.**Philippe Nguyen**, directeur technique.**Jean-Luc Danger, Sylvain Guilley**et **Laurent Sauvage**, en charge du conseil scientifique.

## DANS LES LABOS

## Mieux protéger son mot de passe



Des chercheurs de l'université américaine de Beyrouth (Liban) ont amélioré la technique de KPA

(Key Pattern Analysis), qui consiste à analyser la manière dont une personne saisit son mot de passe (vitesse de frappe, par exemple), afin d'ajouter un facteur de sécurité supplémentaire. Plus précisément, ils ont mesuré le temps pendant lequel chaque touche du clavier est enfoncée. Reste que cette technique peut compliquer la reconnaissance de la personne qui tape lorsque le mot de passe est très long.

## De la mémoire cryptée

Les mémoires NVMM (Non Volatile Main Memory) pourraient remplacer les mémoires vives des ordinateurs, car elles présentent une plus grande capacité. Mais les données étant conservées lorsque le PC est éteint, elles posent d'évidents problèmes de sécurité. Des chercheurs de l'université de Caroline du Nord ont développé une technologie de chiffrement partiel de ces données. Partiel, afin de ne pas ralentir la machine.

## Homme ou femme : l'ordinateur sait



A l'université polytechnique de Madrid, des chercheurs ont développé un algorithme reconnaissant en temps réel le sexe d'un individu sur une vidéo. Les applications sont nombreuses, telle la répartition hommes/femmes des visiteurs d'un stand de magasin. L'avancée se situe sur la méthode mathématique employée, reposant sur des techniques dites de classifieur linéaire.