MINES Saint-Étienne
Une école de l'IMT

AVIS DE SOUTENANCE DE THESE DE DOCTORAT

Le **06-12-2019**
A **14h** Amphi Minatec (Grenoble)

CEA Grenoble
17 Rue des Martyrs
38054 Grenoble

Soutiendra en vue de l'obtention du titre de Docteur de l'Ecole Nationale Supérieure des Mines de Saint-Etienne dans la spécialité : MICROELECTRONIQUE

Maxime **MONTOYA**

Une thèse ayant pour sujet :

Sécurité adaptative et énergétiquement efficace dans l?Internet des Objets

MEMBRES DU JURY :

Président
(Le président est désigné le jour de la soutenance)

Rapporteurs :

Tisserand	Arnaud	Directeur de recherche	Centre de recherche Huygens
Hély	David	Maître de conférences	LCIS

Examinateurs :

Guilley	Sylvain	Professeur	Inst. MINES-TELECOM
Bossuet	Lilian	Professeur	Laboratoire Hubert Curien
Moro	Nicolas	Ing. de recherche	IMEC - Holst Centre
Rouzeyre	Bruno	Professeur	Univ. Montpellier 2 - LIRMM
Fournier	Jacques	Ing. de recherche	CEA
Bacles-Min	Simone	Ing. de recherche	CEA

Thèse préparée dans le centre CMP-GC à l'Ecole Nationale Supérieure des Mines de Saint-Etienne.
Travail co-encadré par : FOURNIER Jacques

BACLES-MIN - CEA Leti Simone

Destinataires : DRI, Accueil, SCIDEM, Centre,
D.CORTIAL « Le Progrès », 24 rue de la robotique – 42000 Saint-Etienne

Résumé

La sécurité des circuits intégrés pour l'IoT est généralement incompatible avec la faible consommation énergétique attendue de ces circuits.

Cette thèse a donc pour but de proposer de nouvelles manières de concilier sécurité et efficacité énergétique pour les circuits intégrés.

Dans un premier temps, la sécurisation d'un mécanisme de gestion de l'énergie est étudiée. Les radios de réveil permettent de gérer la sortie de veille d'objets connectés, en réveillant un tel objet lors de la réception d'un code de réveil spécifique, mais elles sont vulnérables aux attaques par déni de sommeil, qui consistent à réveiller constamment l'objet en répétant un même code de réveil de sorte à vider sa batterie.

Une nouvelle manière de générer des codes de réveils est proposée, qui permet de contrer efficacement ces attaques avec un coût négligeable en énergie.

Dans un second temps, l'efficacité énergétique des contre-mesures contre les attaques matérielles est améliorée à travers deux approches différentes. Une nouvelle contre-mesure mixte, ayant une consommation énergétique plus faible que les protections mixtes existantes, est proposée ; elle consiste en un lissage algorithmique de la consommation offrant une détection intrinsèque des fautes. L'implémentation adaptative de contre-mesures matérielles est également proposée ; elle consiste à moduler le niveau de protection fourni par ces contre-mesures au cours du fonctionnement d'un algorithme protégé, afin d'optimiser la sécurité et la consommation énergétique.

Une évaluation de la sécurité des contre-mesures montre qu'elles fournissent une protection efficace contre les attaques matérielles existantes.

Maxime MONTOYA, CMP