

Damien SAUVERON

6 Le Clos des Troubadours – 87430 Verneuil-sur-Vienne

Tél. : +33 6 61 78 55 19

Mail : damien.sauveron@unilim.fr

Web : <http://damien.sauveron.fr/>

Dossier de demande de qualification aux fonctions de Professeur en Informatique Section 27 du CNU

Table des matières :

- Déclaration de candidature.....	p. 2
- CV.....	p. 4
- Documents liés à l'HDR.....	p. 5
- Attestation de réussite à l'HDR en Informatique.....	p. 6
- Rapports de pré-soutenance.....	p. 7
- Rapport et PV de soutenance.....	p.13
- Enseignement.....	p.15
- Responsabilités pédagogiques et volumes d'enseignement.....	p.16
- Descriptif sommaire des principales unités d'enseignement..	p.17
- Détails des enseignements par année.....	p.17
- Projet d'enseignement.....	p.24
- Recherche.....	p.25
- Évolution et structuration de ma recherche.....	p.26
- Liste complète des publications.....	p.28
- Bilan d'activités résumé 2010 – 2014.....	p.35
- Encadrements et activités de direction de la recherche.....	p.39
- Responsabilités scientifiques 2010 – 2014 et rayonnement...	p.42
- Projet de recherche.....	p.45
- Charges collectives.....	p.49
- Descriptions et avis de responsables / Recommandations.....	p.51

Note : Afin de rester conforme au contenu exigé par l'arrêté du 16 juillet 2009, pour le CV, il convient de prendre le CV présenté en page 4, pour « l'exposé présentant les activités en matière d'enseignement, de recherche, d'administration et d'autres responsabilités collectives » les récapitulatifs Enseignement, Recherche et Charges collectives exposées respectivement en pages 16-17, 26-27 et 50. L'ensemble des autres informations doivent se comprendre comme des annexes de compléments d'information de nature à éclairer aux mieux les rapporteurs sur mes activités.

*Il est conseillé de joindre ce document au dossier transmis
aux rapporteurs désignés par le Conseil National des Universités*

DÉCLARATION DE CANDIDATURE À LA QUALIFICATION
AUX FONCTIONS DE PROFESSEUR DES UNIVERSITÉS,
POUR LA SECTION 27-Informatique
(Campagne 2015)
1ère demande

Je soussigné(c) M.

Nom de famille : SAUVERON

Nom d'usage : SAUVERON

Prénom : DAMIEN

Date et lieu de naissance : 23/01/1977 - LIMOGES

Nationalité : Française

Adresse postale et électronique à laquelle seront acheminées toutes les correspondances		
6 LE CLOS DES TROUBADOURS		
Code postal : 87430	Ville : VERNEUIL SUR VIENNE	Pays : FRANCE
Téléphone : 0661785519	Télécopie :	
Adresse électronique : damien.sauveron@unilim.fr		

Date de création de la candidature

08/10/2014 à 10:10

Date de dernière modification de la candidature

08/10/2014 à 10:10

Titres universitaires français :

Habilitation à diriger des recherches

Diplôme au titre duquel la qualification est demandée : HDR

Titre : Sécurité et interactions

des « smart secure devices » et des « réseaux mobiles »

Date de soutenance : 12/12/2014

Lieu de la soutenance :

Mention :

Directeur : PHILIPPE GABORIT

Composition du jury :

Liste des étabs et labos d'exercice :

Activités en matière d'enseignement :

Thème de recherche et mots clés :

Activités en matière d'administration et autres responsabilités collectives :

déclare faire acte de candidature à la qualification.

Fait à LIMOGES le 16/12/2014

Signature



Damien SAUVERON

6 Le Clos des Troubadours – 87430 Verneuil-sur-Vienne

Tél. : +33 6 61 78 55 19

Mail : damien.sauveron@unilim.fr

Web : <http://damien.sauveron.fr/>

Né le 23 janvier 1977 à Limoges (Haute-Vienne)

Nationalité Française – Marié – 1 enfant (4 ans)

Formation – Diplômes – Carrière industrielle et universitaire

Depuis 2006	Maître de Conférences en Informatique à l'Université de Limoges Composante de rattachement : Faculté des Sciences et Techniques Laboratoire : XLIM (UMR 7252 Université de Limoges/CNRS) Habilitation à Diriger des Recherches en Informatique de l'Université de Limoges soutenue le 6/12/2014 sur le projet : <i>Sécurité et interactions des « smart secure devices » et des « réseaux mobiles »</i> Lieu : XLIM, Limoges, France Jury : • Pr Philippe Gaborit, Université Limoges, Garant et Examinateur, CNU27 • Pr Mohamed Mosbah, Institut Polytechnique de Bordeaux, Rapporteur et Président, CNU27 • Pr Keith Mayes, Royal Holloway, University of London, Rapporteur • Dr HDR Samia Bouzefrane, Conservatoire National des Arts et Métiers, Rapporteur, CNU27 • Pr Serge Chaumette, Université de Bordeaux, Examinateur, CNU27 • Pr Maryline Laurent, Telecom SudParis, Examinateur, CNU27 • Pr Pascal Urien, Telecom ParisTech, Examinateur, CNU27
2004-2006	Post-doctorant au sein de l'Information Security Group – Smart Card Centre du Royal Holloway, University of London (01/02/2006 – 31/07/2006) ATER à l'Université de Limoges (03/09/2004 – 31/01/2006)
2001-2004	Doctorat d'Informatique au LaBRI, Université Bordeaux 1 (Mention Très Honorable) soutenu le 3/12/2004 Thèse sous convention CIFRE intitulée « <i>Étude et réalisation d'un environnement d'expérimentation et de modélisation pour la technologie Java Card. Application à la sécurité.</i> » et réalisée sous la direction du Professeur Serge Chaumette. Ingénieur R&D au sein du Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) de SERMA Technologies
2000-2001	DEA d'Informatique au LaBRI, Université Bordeaux 1 (Mention Assez Bien) Mémoire intitulé « <i>Sécurité et vérification d'applications embarquées en environnement Java Card</i> » et réalisé sous la direction du Professeur Serge Chaumette
1999-2000	Maîtrise Informatique, Université de Limoges (Mention Assez Bien)

- Titulaire de la Prime d'Excellence Scientifique depuis janvier 2012
- Qualification CNU 27 (Informatique) aux fonctions de Maître de conférences en 2005 (MCF-2005-27-05227152536)
- Récipiendaire de l'[IFIP Silver Core award](#) délivré par l'assemblée générale de l'IFIP (International Federation for Information Processing) en décembre 2013.

Thèmes de recherche :

40 Réseaux

- 41 Architecture, gestion, sécurité

- 42 Protocoles, QoS, multimédia, mobilité

60 Systèmes informatiques

- 64 Systèmes répartis et distribués

- 65 Sécurité des systèmes informatiques

voire B3 Architectures spécialisées, systèmes numériques intégrés sur la puce, systèmes embarqués

Mots clés : Sécurité, cartes à puce, RFID, réseaux sans fil, réseaux véhiculaires (drones)

Documents liés à l'HDR

UNIVERSITÉ DE LIMOGES

ATTESTATION DE REUSSITE AU DIPLOME

Madame le Doyen de la Faculté des Sciences et Techniques atteste que

le diplôme d'habilitation à diriger des recherches Informatique
a été décerné à

Monsieur SAUVERON DAMIEN

né le 23 janvier 1977 à LIMOGES (087)

au titre de l'année universitaire 2014/2015

Date de soutenance : 6 décembre 2014

Etablissement soutenance : UNIVERSITE de LIMOGES

Jury : M. MOHAMED MOSBAH, Président du jury, PROFESSEUR DES UNIVERSITES
Institut Polytechnique de Bordeaux
Mme SAMIA BOUZEFRANE, Rapporteur du jury, MAITRE DE CONFERENCES/HDR
C.N.A.M. Paris
M. KEITH MAYES, Rapporteur du jury, PROFESSEUR
University of London (UK)
M. SERGE CHAUMETTE, Membre du jury, PROFESSEUR DES UNIVERSITES
UNIVERSITE BORDEAUX 1 SCIENCES ET TECHNO
M. PHILIPPE GABORIT, Membre du jury, PROFESSEUR DES UNIVERSITES
UNIVERSITE de LIMOGES
Mme MARYLINE LAURENT, Membre du jury, PROFESSEUR DES UNIVERSITES
Telecom SudPARIS
M. PASCAL URIEN, Membre du jury, PROFESSEUR DES UNIVERSITES
TELECOM ParisTech

Section CNU : 27 - Informatique



Fait à Limoges, le 8 décembre 2014

Anne-Mercedes BELLIDO

N° étudiant : 9501212



Rapport sur le mémoire d'habilitation présenté par

Damien Sauveron

Damien Sauveron présente ses activités de recherche dans un document intitulé « Sécurité et interactions des *smart secure devices* et des réseaux mobiles ». Le fil conducteur de ces travaux de recherche concerne la mise au point de techniques pour sécuriser les systèmes informatiques. Plus précisément, les contributions des travaux ont pour objectifs de sécuriser les réseaux mobiles à la fois au niveau des nœuds que des communications inter-nœuds. Les solutions utilisées sont principalement basées sur les cartes à puce ou technologies RFID, avec des applications aux réseaux mobiles, aux réseaux ad hoc, aux flottes de drones, etc. Le manuscrit présente deux parties : *smart secure devices* composée des 3 premiers chapitres et les réseaux mobiles formée des 3 chapitres suivants. Le document contient également des annexes avec quelques articles et un descriptif des activités pédagogiques et des responsabilités.

Après une introduction, le document commence par une présentation des travaux sur la sécurité et les applications des cartes multiapplicatives. L'une des contributions principales a été d'introduire la notion de cartes à puce multiapplicatives ouvertes. Le principe est de permettre au porteur de la carte de charger des applications après l'émission, et de proposer des méthodes pour tester leur sécurité. Un modèle de cartes semi-ouvertes, qui permet d'installer des applications après l'émission par des tiers de confiance, a été proposé. Ce modèle a eu une importante capitale puisqu'il a été utilisé dans les technologies NFC.

Le second chapitre présente des travaux sur la sécurité de système RFID. L'un des principaux résultats est la mise au point de protocoles d'authentification légers et efficaces pour protéger la vie privée, pour des tags RFID bas-coûts. Une autre contribution dans ce domaine concerne le développement de plusieurs prototypes de systèmes d'attaques sur des RFID. Ce travail s'est déroulé dans le cadre d'un projet MIRES (fédération de laboratoires du PRES Limousin-Poitou-Charentes).

Le chapitre 3 concerne des travaux sur l'évaluation et la certification, qui s'inscrivent dans la continuité des travaux de la thèse. Une méthodologie proposée consiste à isoler physiquement un motif à observer dans une trace d'exécution. Une fois le motif isolé, les évaluations peuvent s'appliquer plus facilement. Cette méthode a été proposée pour Java Card, et peut également s'appliquer à d'autres technologies, mais cette extension n'a pas été effectuée. Une autre retombée souhaitée de l'utilisation de cette méthode est de construire un dictionnaire de bytecodes Java Card pour analyser une trace d'exécution capturée par l'intermédiaire de paramètres physiques sur une carte Java Card comme la consommation électrique ou les émissions électromagnétiques, mais ce travail n'a pas été achevé. Toutefois, des extensions intéressantes sont

envisagées notamment dans le cadre d'une plate-forme ouverte pour augmenter davantage le niveau de confiance.

La seconde partie du manuscrit concerne les travaux sur les réseaux mobiles. Le chapitre 4 donne des extensions d'un travail fait en thèse sur le développement d'une grille de calcul totalement sécurisée et dont les ressources des calculs sont les cartes à puce. Ces techniques ont été utilisées pour retrouver de l'information privée entre nœuds ne se faisant pas confiance, et ont été appliquées à des cartes SIM embarquées sur des téléphones portables communicants via un réseau GSM.

Les réseaux de capteurs sont traités dans le chapitre 5. Il s'agit de travaux récents qui présentent un état de l'art dans le domaine de la sécurité des réseaux de capteurs ainsi que sur la prise en main de réseaux de capteurs/actionneurs. Les perspectives dans cette direction sont de s'appuyer sur les résultats précédents notamment sur une plate-forme semblable à MADNESS pour sécuriser un réseau de capteurs. Par ailleurs, Damien Sauveron a piloté l'édition de deux numéros spéciaux de journaux sur les réseaux de capteurs et la sécurité.

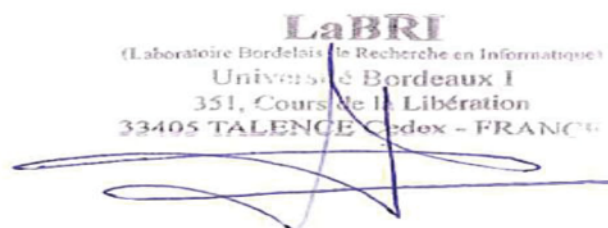
Le dernier chapitre présente les travaux sur les flottes de drones. La principale contribution a été d'introduire un modèle de l'adversaire qui dispose d'un potentiel d'attaque élevé et qui prend en compte la capture d'un drone pour extraire des informations secrètes. Pour résister à ces menaces, il faut que les drones embarquent des éléments inviolables. Une solution basée sur un mélange des caractéristiques des cartes à puce et des RFID actifs est en cours d'étude.

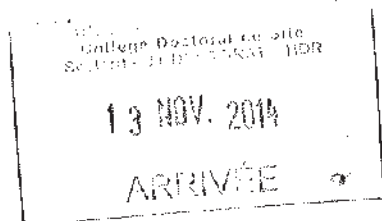
La dernière partie du document contient des annexes présentant les publications, un projet scientifique et une synthèse des activités de Damien Sauveron, en termes de contrats, encadrement, responsabilités, ainsi que les activités pédagogiques.

Le matériel de recherche présenté dans ce mémoire est d'ampleur. L'activité de recherche est dense et maintenue depuis de nombreuses années, avec des encadrements de jeunes chercheurs et une activité de publication régulière. Par ailleurs, Damien Sauveron a une activité pédagogique assez riche et des responsabilités pédagogiques et scientifiques importantes, ce qui témoigne de sa grande maturité universitaire et d'une visibilité internationale dans le domaine de la sécurité informatique. En bref, il ne fait aucun doute que Damien Sauveron est totalement autonome pour définir des sujets de recherche originaux, pour encadrer des jeunes chercheurs, pour mener à bien des activités contractuelles, etc. En conséquence, je propose d'accepter sans réserve que Monsieur Damien Sauveron présente son travail en vue d'obtenir une Habilitation à Diriger des Recherches.

Bordeaux, le 19 novembre 2014

Mohamed Mosbah, Professeur
LaBRI, Institut Polytechnique de Bordeaux
Université de Bordeaux





Rapport sur le dossier de Damien Sauveron présenté en vue de l'obtention de l'Habilitation à Diriger des Recherches de l'Université de Limoges

Damien Sauveron est Maître de Conférences à l'Université de Limoges depuis Septembre 2006, et est chercheur au Laboratoire XLIM de Limoges. Notons qu'après l'obtention de son Doctorat en Informatique à l'Université de Bordeaux 1 en 2004 qui portait sur « L'étude et la réalisation d'un environnement d'expérimentation et de modélisation pour la technologie Java Card. Application à la sécurité », il a été ATER à l'Université de Limoges durant 1 an et demi puis il a effectué un post-doc à Royal Holloway, University of London.

Il est titulaire de la PEDR (PES) depuis Janvier 2012, et a bénéficié au second semestre de l'année 2013/2014 d'un CRCT.

En plus de son implication dans les responsabilités pédagogiques en particulier comme co-directeur des études, Damien Sauveron possède incontestablement une grande expérience dans l'enseignement (10 ans) dans divers domaines de l'informatique avec une charge importante durant les premières années.

Dans ce dossier, Damien Sauveron fait valoir ses travaux de recherche menés depuis la fin de sa thèse de Doctorat jusqu'à maintenant, pour obtenir une Habilitation à Diriger des Recherches. La sécurité constitue le fil conducteur de ses travaux à travers d'une part l'étude de failles de sécurité dans des objets sécurisés comme dans les plates-formes Java Card, et d'autre part en introduisant des mécanismes de sécurité dans des objets non sécurisés comme les tags RFID ou plus généralement dans des systèmes basés sur l'Internet des objets.

Le dossier de Damien Sauveron se décompose en deux parties, la première partie traite des objets sécurisés intelligents (« smart secure devices ») et la seconde partie traite des réseaux mobiles.

Chaque partie comporte plusieurs chapitres. Chaque chapitre présente de manière brève les contributions, les perspectives ainsi qu'en annexe les publications les plus significatives dans le thème considéré.

Ce rapport de HDR aborde de manière cohérente d'abord la sécurité des objets intelligents, ensuite celle des réseaux mobiles. Les réseaux décrits ici correspondent à des réseaux basés sur des nœuds mobiles pouvant communiquer via des connexions sans fil.

La première partie sur les objets intelligents et sécurisés intègre trois chapitres :

- Dans le chapitre 1 sur la sécurité et application des cartes multi-applicatives, Damien Sauveron introduit la notion de cartes multi-applicatives ouvertes et semi-ouvertes permettant respectivement au porteur ou à un tiers de confiance de rajouter des applications dans une carte après émission, avec l'objectif de proposer une approche centrée sur l'utilisateur. Cette notion a été reprise et étendue dans la thèse de Raja Naeem Akram du Royal Holloway University of London, pour laquelle Damien Sauveron a été rapporteur. Dans cette approche centrée utilisateur, un TSM appelé Consumer Oriented Trusted Service Manager – CO-TSM a été proposé conjointement avec une étude sur les menaces qui en découleraient ainsi que la manière de les minimiser. Le chapitre se termine avec des perspectives, comme par exemple, la sauvegarde du contenu de la carte sur un serveur ou la migration du contenu de la carte vers une autre carte.

- Le chapitre 2 adresse la sécurité dans les systèmes RFID en proposant des protocoles d'authentification légers adaptés aux tags RFID bas coût. Ces protocoles sont comparés avec les solutions de l'état de l'art et semblent être plus intéressants car moins coûteux notamment en termes de nombres d'opérations côté base de données des tags. Ce travail a été complété par l'étude de la résistance à différentes attaques des solutions existantes et des protocoles proposés. Toujours dans le même thème, la participation à des projets collaboratifs régionaux comme SoRFID (Security of RFID) ou DIL (Détection Innovation Laboratoire) ont permis à Damien Sauveron de développer des prototypes d'attaques pour les tags RFID dans le projet SoRFID, et d'utiliser la technologie NFC pour assister le patient à domicile dans le projet DIL. Une des perspectives de ce chapitre concerne l'étude de la sécurité des tags RFID actifs qui sont en général dotés de capacités plus importantes en termes de mémoire et de processeur.
- Le chapitre 3 traite de l'évaluation et de la certification sécuritaires, une thématique qui s'inscrit dans la continuité des travaux de thèse de Doctorat de Damien Sauveron, en proposant une méthodologie qui facilite l'évaluation de la sécurité des plates-formes Java Card. Damien Sauveron a tenté de pointer sur la faiblesse des méthodes classiques de certification et d'évaluation pour faire en sorte que le porteur de la carte soit un acteur. Ces travaux convergent avec ceux du modèle centré utilisateur appelé UCOM présenté dans le chapitre 1. En termes de perspective, l'utilisation des PUF (Physical Unclonable Functions) semble une nouvelle piste à explorer pour bâtir un système de confiance depuis le niveau matériel des puces. Par ailleurs, une méthodologie d'évaluation de la sécurité des capteurs est intéressante à investiguer.

Les réseaux mobiles, présentés dans la deuxième partie, peuvent être définis comme des systèmes résultant de la convergence de l'Internet des objets et des systèmes cyber-physiques avec toujours l'objectif de sécuriser ces systèmes.

- Dans le chapitre 4 qui s'intitule « Du Grid computing à la mobilité », Damien Sauveron montre comment il a étendu ses travaux de thèse sur les grilles de plates-formes Java Card en considérant des cartes SIM embarquées sur des téléphones communiquant via le réseau mobile GSM. Ces travaux ont fait l'objet d'une collaboration avec Royal Holloway University of London. Les plates-formes Java Card ont été par la suite utilisées pour sécuriser des réseaux mobiles ad hoc (MANET en Anglais).
- Le chapitre 5 sur les réseaux de capteurs est un domaine abordé depuis peu par Damien Sauveron puisque les contributions pour le moment se résument à des articles sur l'état de l'art. Notons que ces réseaux dotés de capteurs et d'actionneurs et soumis à des contraintes d'énergie et de sécurité correspondent davantage à ce qu'on appelle aujourd'hui systèmes cyber-physiques.
- Enfin, le chapitre 6 traite d'un domaine d'application assez original, à savoir celui des flottes de drones. Une flotte de drones en vol peut vouloir collaborer en vue de réaliser un objectif commun que cela soit dans un contexte civil ou dans un contexte militaire. Dans ses travaux, Damien Sauveron montre que ces drones sont vulnérables et sujets aux attaques et que pour résister à ces attaques, une solution serait d'embarquer un élément sécurisé au sein de chaque drone, en proposant un dispositif appelé « Active Radio Frequency Smart Secure Device » (ARFSSD), qui est actuellement en cours de développement.

Notons que la majorité des travaux de recherche décrits ici ont été le fruit de collaborations nationales et internationales que Damien Sauveron a su initier intelligemment.

Dans le cadre de ces activités de recherche décrites ci-dessus, Damien Sauveron a encadré/co-encadré 10 étudiants en Master 2 et 4 étudiants en PFE. Il a par ailleurs conseillé et orienté 4 doctorants du Royal Holloway de l'Université de Londres, ainsi qu'un doctorant du LaBRI (Université Bordeaux 1) qui a soutenu en 2008. Damien Sauveron a un bilan convenable de publications (32, dont 5 revues internationales et 18 conférences internationales et 6 participations à des ouvrages collectifs) avec une forte activité de publications depuis 2012. En termes de collaborations académiques, Damien Sauveron a participé au projet national « ANR SARAH » et au projet européen « Eliare Network Sudoe ».

L'activité la plus marquante des 10 dernières années de la carrière de Damien Sauveron reste son implication dans l'animation d'événements scientifiques. En effet, il est éditeur de 10 numéros spéciaux dans différentes revues (auxquels s'ajouteront 5 numéros spéciaux en 2015 et 2016), et de 5 actes de colloques. En 2007, il a créé le workshop WISTP qui deviendra une conférence internationale en 2015. Par ailleurs, ses responsabilités scientifiques internationales sont remarquables. Damien Sauveron a été vice-président de Décembre 2007 à Décembre 2013 de l'IFIP WG 11.2 Pervasive Systems Security, avant d'en devenir le Président en 2014. Il est directeur régional de la FTRA depuis 2010. Il est membre de l'IFIP WG 8.8 Smart Cards depuis 2006 et de ACM SIGSAC depuis 2009. En outre, il est membre du comité programme d'un nombre considérable de conférences internationales, relecteur dans plusieurs revues, etc.

Sur le plan national, il a été expert pour l'ANR et ARCSIS (Région PACA) et est membre de l'association SPECIF/SIF. Au sein de l'Université de Limoges, il est entre autres membre du conseil du laboratoire XLIM et il a été membre du conseil scientifique pendant 4 ans.

Suite à la lecture du mémoire, il apparaît clairement que Damien Sauveron a développé des activités de recherche importantes en faisant évoluer la thématique de la thèse de Doctorat d'une part et en ouvrant son activité de recherche vers des thèmes nouveaux d'autre part. Il a déjà des expériences en termes de collaborations scientifiques et de relations avec la communauté industrielle, ce qui devrait lui permettre d'amplifier ses activités d'encadrement doctoral.

En conséquence, j'estime que le travail présenté est tout à fait convenable et j'émet donc un avis favorable à la soutenance de cette HDR.

Fait à Paris, le 12 Novembre 2014



Mme Samia Bouzeffrane
Maître de Conférences/HDR
Conservatoire National des Arts et Métiers



Royal Holloway
University of London
Egham, Surrey
TW20 0EX

Professor Keith Mayes
Director ISG-Smart Card Centre
+44 (0)1784 144 08
keith.mayes@rhul.ac.uk
www.scc.rhul.ac.uk
www.isg.rhul.ac.uk

Re: Damien Sauveron, HDR review

Date: 13.11.2014

To whom it may concern,

The HDR report from Damien Sauveron summarises his research and related activities over a ten year period. The report is split into two sections starting with smart secure devices and moving on to mobile communication networks. Although the topics are separated, one can see a natural evolution in the research interest, which remains concerned about implementation security and related attacks and countermeasures; as such it appears as a coherent body of work.

As a result of these activities, Damien is a co-author on a significant number of publications covering a wide range of topics. I would expect this number to grow even further if the HDR provides Damien with greater authority and freedom to drive forward his own research programmes and projects. The publications are in general of a typical level/standard for the area of applied research, although the work on secure UAV networks has the potential to be ground breaking.

In terms of support for international academic research, Damien has accomplished a remarkable amount in the last ten years. There are relatively few researchers who can claim they were pivotal in establishing a new academic conference (WISTP) that is thriving today. He has also served on a great many programme committees as well taking the chair on numerous occasions. His recent appointment as president of IFIP WG 11.2 Pervasive Systems Security, suggests he has the support and confidence of his international peers. His international reputation can only have been enhanced by his active involvement in several European collaborative projects.

It would seem that Damien is well able to contribute to research projects and indeed appears to be a popular and reliable collaborator, with many international contacts. Therefore the main question is whether he can step up to identify and direct research, involving not only his own efforts but those of PhD students, research assistants and academic colleagues. To establish research programmes requires an appreciation of "hot topics", the standard of submission required by conferences/journals as well as opportunities and the application processes for collaborative project funding. In this respect I have no doubt to Damien's abilities and his experience on projects, conferences and programme committees, speaks for itself. To direct the research of others requires demonstration of different skills including leadership, coaching and a good deal of patience and flexibility. In this aspect I am not concerned as Damien has done a lot of teaching in France and I have also observed him offering useful guidance to Masters and PhD students when he visited Royal Holloway (UK).

In summary, I consider that the report submitted by Damien demonstrates that he has achieved a great deal to date and justifies the award of HDR, which can only enhance his future achievements.

Yours Sincerely
Professor Keith Mayes

A handwritten signature in black ink, appearing to read 'Keith Mayes', written over a horizontal line.



Discipline : Informatique

Sujet : Sécurité et Interactions des "smart secure devices" et des "réseaux mobiles"

Membres du jury :

Mme. Samia BOUZEFRANE,
Professeur - Rapporteur
M. Keith MAYES,
Professeur - Rapporteur
M. Mohamed MOSBAH,
Professeur - Rapporteur
M. Philippe GABORIT,
Professeur - Chargée de suivi
M. Serge CHAUMETTE,
Professeur - Examineur
M. Pascal URIEN,
Professeur - Examineur
Mme. Maryline LAURENT,
Professeur - Examineur

S. Bouzefrane

P. GABORIT

M. Mosbah

K. MAYES (visio)

S. CHAUMETTE (visio)

P. URIEN (visio)

N. LAURENT (visio)

RAPPORT DE SOUTENANCE

HDR de
M. Damien SAUVERON

Limoges, le 6 décembre 2014

Damien Sauveron a fait un exposé clair et synthétique.

Le jury tient à souligner la qualité et la consistance de ses travaux de recherche qui se caractérisent par un continuum allant du concept théorique jusqu'aux applications.

Damien Sauveron a répondu aux questions avec aisance, témoignant d'une connaissance approfondie du domaine de la sécurité, en particulier sur les cartes à puce et les systèmes mobiles.

Il a pu développer une vision pertinente sur des domaines à fort potentiel d'innovation.

Pour toutes ces raisons, le jury délivre à Damien Sauveron l'Habilitation à Diriger des Recherches en Informatique de l'Université de Limoges.



Collège Doctoral
e Site

ANNEE UNIVERSITAIRE 2014/2015

Etudiant : M. DAMIEN SAUVERON né le : 23/01/1977

Diplôme : HDR INFORMATIQUE

Titre des travaux : Sécurité et Interactions des "smart secure devices" et des "réseaux mobiles"

Section CNU : ~~25 - Mathématiques~~ 27 - Informatique

Unité de recherche : XLIM - Mathématiques Informatique

Directeur : M. PHILIPPE GABORIT

Lieu de soutenance : Faculté des Sciences et Techniques - XLIM salle des Conférences

La soutenance est publique.

Résultat : Favorable

Mention : Très honorable

Avis de reproduction : oui

Membres du Jury

Nom	Qualité	Etablissement	Rôle	Signature
Mme SAMIA BOUZEFRANE	MAITRE DE CONFERENCES/HDR	C.N.A.M. Paris	Rapporteur	
M. KEITH MAYES	PROFESSEUR	University of London (UK)	Rapporteur	visio
M. MOHAMED MOSBAH	PROFESSEUR DES UNIVERSITES	Institut Polytechnique de Bordeaux	Rapporteur (Président)	
M. SERGE CHAUMETTE	PROFESSEUR DES UNIVERSITES	UNIVERSITE BORDEAUX 1 SCIENCES ET TECHNO	Membre	visio
M. PHILIPPE GABORIT	PROFESSEUR DES UNIVERSITES	UNIVERSITE de LIMOGES	Membre	
Mme MARYLINE LAURENT	PROFESSEUR DES UNIVERSITES	Telecom SudPARIS	Membre	visio
M. PASCAL URIEN	PROFESSEUR DES UNIVERSITES	TELECOM ParisTech	Membre	visio

CADRE A RENSEIGNER PAR LE JURY DE SOUTENANCE

Confidentialité de la thèse :

☒ NON

☐ OUI

Corrections demandées:

☒ NON

☐ OUI

Jusqu'en (préciser obligatoirement) :

Enseignement

Responsabilités pédagogiques

- De décembre 2010 à août 2014, j'ai été **co-directeur des études du portail « Sciences de l'Ingénieur »** (entre 170 et 250 étudiants sur L1-L2). Le portail s'appelle depuis le LMD3 **« Sciences et Ingénierie (Mathématiques, Informatique, Physique, Chimie) »**.
 - À ce titre, je participais aux entretiens pédagogiques, aux manifestations de promotion de l'établissement et de la composante, à l'orientation active (Admission Post Bac), j'examinais les dossiers DAP (Demande d'Admission Préalable), etc.
 - J'organisais les réunions de pré-rentrée, les réunions de bilan pédagogique à mi-semester (S1, S2 et S3) qui regroupent tous les membres des équipes enseignantes des différents Unités d'Enseignements (UE), les différents délégués de groupe, les représentants de l'administration. Je rédigeais les procès verbaux.
 - Je gérais les discussions avec les différents responsables d'UE, les enseignants référents et les tuteurs étudiants.
 - Je préparais les bilans des résultats du contrôle continu à mi-semester afin de proposer des réorientations aux étudiants les plus faibles et je préparais aussi les jurys avec l'administration (avant – vérification des calculs Apogée, traitement des cas particuliers –, pendant et après les jurys).
 - Je traitais les différentes réclamations liées à des absences justifiées ou injustifiées aux épreuves et/ou aux cours (depuis l'instauration de l'assiduité obligatoire en première année il y a 3 ans).
 - J'organisais les réunions de présentation de poursuite d'études pour les étudiants des semestres 1 et 3.
 - Au titre de co-directeur des études je participais aussi aux réunions de l'équipe de Licence qui rassemblent les différents responsables de portails (SI, SVT, STAPS), les différents responsables des mentions de licence (Mathématiques, Informatique, etc.), les représentants étudiants et ceux de l'administration.
 - J'étais également membre de plusieurs jurys de seconde années de licence dans différentes mentions s'appuyant sur le portail Sciences et Ingénierie.
 - Je participais à la sélection des étudiants pour l'année 0, Classe Préparatoire à l'Entrée en Licence (CPEL) que nous proposons aux personnes n'ayant pas un bac scientifique ou un niveau très faible.
- Je suis **responsable de toutes les Unités d'Enseignements (UE) dans lesquelles j'interviens**. Je dois donc coordonner les différents intervenants en particulier en Informatique 1 (première année), rédiger les différents sujets, faire la collecte des notes, les transmettre à l'administration, en vérifier les saisies, assister aux jurys du portail SI et de la Licence MIASHS (Mathématiques et Informatique Appliquées aux Sciences Humaines et Sociales) dont les étudiants suivent les unités d'enseignement dont je suis responsable.
- Je suis **l'enseignant référent** en Informatique pour les étudiants de la première année de Licence du portail « Sciences de l'Ingénieur »/« Sciences et Ingénierie (Mathématiques, Informatique, Physique, Chimie) » depuis 2007 et je reçois donc tous les étudiants en difficulté qui le souhaitent. J'interagis avec le tuteur étudiant d'Informatique pour pallier les lacunes et j'organise des séances de soutiens. Je propose les sujets et corrections des devoirs blancs que le tuteur organise.
- J'ai participé aux réflexions sur les filières d'ingénierie à l'Université de Limoges et en particulier en tant que co-directeur des études, j'ai aidé à construire la prépa intégrée portée en grande partie par la Faculté des Sciences et Techniques pour l'ENSCI (École Nationale Supérieure de Céramique Industrielle) dans le cadre de son label INSA-partenaire.
- Toujours au titre de co-directeur des études, j'ai participé à la construction de la passerelles PACES (Première Année Commune aux Études de Santé) vers FST (Faculté des Sciences et Techniques) via la validation automatique de certains crédits ou semestre(s) suivant certaines conditions.
- J'ai participé à la rédaction des supports pour la plate-forme nationale « Informatique et Sciences du Numérique » dans le cadre de l'appel d'offre pour lequel l'université de Limoges a été retenue.
- J'ai formé des enseignants du secondaire de l'académie de Limoges à la spécialité « Informatique et Sciences du Numérique » lors des 2 sessions organisés par le rectorat.

Volumes d'enseignement

Même si j'ai été recruté à l'Université de Limoges en tant que MCF depuis septembre 2006, je ne vais présenter dans la suite que mes services d'enseignement effectués depuis 2007/2008.

Je tiens quand même à préciser qu'en septembre 2004 puis septembre 2005, j'ai été recruté comme ATER à l'Université de Limoges et qu'à cette époque j'avais pris la responsabilité des enseignements « Outils de l'internet », « Réseaux personnels » et que j'en avais créé le contenu (puisque 2004/2005 était la première année du LMD1 et qu'aucun de ces enseignements n'existaient avant à Limoges). J'intervenais aussi déjà en M2 dans les UEs « Sécurité informatique : Sécurité des Données, du Code et des Transferts Réseau » et « Carte à puce et applications » où j'y délivrai un contenu que j'avais créé.

Depuis 2005, en plus des heures à l'Université de Limoges, j'intervenais également en M2 à l'Université Bordeaux 1 pour délivrer des enseignements sur les cartes à puce et encadrer des projets étudiants (en 2003 et 2004, j'avais déjà encadré plusieurs projets étudiants dans cette université où j'ai obtenu mon doctorat en Informatique).

Depuis 2011, j'interviens aussi à l'ISIMA (Institut Supérieur d'Informatique, de Modélisation et de leurs Applications) à Clermont-Ferrand au niveau M2 (dernière année de l'école).

Voici une vue globale de mes volumes d'enseignement :

	Service effectué à Limoges	Cumul à Bordeaux	Cumul à Clermont-Ferrand
2007/2008	240,5	16,5	
2008/2009	353,5	16,5	
2009/2010	418,5	19,5	
2010/2011	342,5	19,5	
2011/2012	350,75	19,5	12,5
2012/2013	376,25	19,5	12,5
2013/2014	288 (réalisé avant le CRCT)	18,5	12,5
2014/2015	297,5	10	12,5

Si depuis le début de ma carrière, j'ai dû effectuer de nombreuses heures complémentaires (entre 50 et 220 par an) c'est en raison du manque d'enseignants au département Informatique de la Faculté des Sciences et Techniques de l'Université de Limoges.

Descriptif sommaire des principales unités d'enseignement

Note : pour certaines UEs les intitulés ont évolué au fil des maquettes.

- **Informatique 1** : Initiation à l'algorithmique et à la programmation
- **Outils de l'Internet / Préparation au C2I** : Explications générales sur le fonctionnement de l'Internet et sur différents outils indispensables (par exemple des outils collaboratifs) afin de travailler plus efficacement. En complément de l'UE Informatique Outils qui porte sur la bureautique, cette unité prépare l'étudiant au passage du C2I.
- **Informatique 1 bis** : Reprend du départ, sur un rythme plus lent, le premier tiers du contenu de l'UE Informatique 1 pour les étudiants ayant échoué à l'issue du semestre 1 du portail SI (ceux qui ont moins de 8 de moyenne générale à la fin du S1 sont redirigés vers le second semestre de CPEL) et pour les étudiants ayant suivi le premier semestre de CPEL.
- **Informatique 2 PC** : UE destinée aux étudiants suivant le parcours Physique-Chimie du portail afin de leur apprendre comment l'informatique peut leur permettre d'interagir avec le monde physique via des capteurs, actionneurs (collecte de données sur un support mémoire puis traitement a posteriori via des outils informatiques existants comme Excel, Calc ou via des programmes qu'ils développent). J'ai développé cette UE suite à la demande des collègues physiciens et chimistes. Dans le cadre de cette UE, les étudiants utilisent une plate-forme Arduino.
- **Option Info 1 - Réseaux 1** : Apprentissage des concepts de base des réseaux aux travers des différentes couches du modèle OSI. Apprentissage du développement web (HTML, CSS, JavaScript, CGI, etc.) et mise en œuvre via le développement d'un site web.
- **Carte à puce et applications / Cartes à puce et Java Card / Cartes à puce** : Initiation à la programmation carte à puce et Java Card (technologie Java pour cartes). Initiation à la programmation sécurisée face aux attaques par canaux auxiliaires.
- **Génie logiciel et développement sécurisé / Certification et développement sécurisé** : Cours original car il apprend aux étudiants à penser la sécurité en amont de tout développement en analysant ce qu'il faut sécuriser (les biens), les menaces, les objectifs de sécurité, etc. afin de mettre en œuvre des méthodologies d'établissement de la confiance dans les mécanismes implémentés dans les produits. Ce cours est illustré au travers des méthodologies d'évaluation et de certification sécuritaires, ce qui fait des étudiants suivant cette UE (ils sont chaque année plus nombreux), des personnes courtisées par les industriels lors de la phase de recherche des stages.
- **Sécurité des systèmes embarqués** : Ce cours, prévu pour des étudiants n'ayant jamais eu de cours de sécurité, reprend les mécanismes et outils de sécurité tels que le contrôle d'accès, la cryptographie, etc. et les replace dans le contexte des systèmes embarqués. Il présente les problématiques de sécurité à tous les niveaux (logiciel, matériel) et explique comment s'en prémunir.

Détails des enseignements par année

**Année 2008-2009
(passage au LMD2)**

Université de Limoges

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
Co-responsable gestion de 7 personnes	Informatique 1	L1		60		60
Responsable UE à distance	Outils de l'internet	L1	2,5	142,5		146,25
Responsable	Option Info 1 : Réseau 1	L2	21	24		55,5
	Soutien inter-session + plan licence	L1		38		38
	Cartes à puce et Java Card	M2	9			13,5
Responsable	Génie logiciel et développement sécurisé	M2	13,5	12	12	40,25
					Total	353,5
					Heures complémentaires	161,5

Information sur les enseignements :

- Le public de tous les enseignements est « informatique » à partir du L2.
- Pour tous les enseignements j'ai réalisé la totalité des supports de cours, de TD et de TP, ainsi que les sujets des épreuves.
- **Attention les heures TP sont égales aux heures TD dans le tableau ci-dessus et dans la suite lorsqu'elles sont effectuées dans le service statutaire.**

Université de Bordeaux 1

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Cartes à puce	M2	7	6		16,5
					Total	16,5

Année 2009-2010

Université de Limoges

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
Co-responsable gestion de 8 personnes	Informatique 1	L1		60		60
Responsable UE à distance	Outils de l'internet	L1	3	199,5		204
Responsable	Option Info 1 : Réseau 1	L2	21	24	30	85,5
	Soutien inter-session + plan licence	L1		42,5		42,5
Responsable	Certification et développement sécurisé	M2	11		10	26,5
					Total	418,5
					Heures complémentaires	226,5

Information sur les enseignements :

- Le public de tous les enseignements est « informatique » à partir du L2.
- Pour tous les enseignements j'ai réalisé la totalité des supports de cours, de TD et de TP, ainsi que les sujets des épreuves.

Université de Bordeaux 1

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Cartes à puce	M2	7	9		19,5
					Total	19,5

Année 2010-2011

Université de Limoges

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
Responsable gestion de 9 personnes	Informatique 1	L1		60		60
Responsable UE à distance	Outils de l'internet	L1	3	114		118,5
Responsable	Option Info 1 : Réseau 1	L2	21	24	30	85,5
	Soutien inter-session + plan licence + colles	L1		50,5		50,5
Responsable	Certification et développement sécurisé	M2	14		7	28
Total						342,5
Heures complémentaires						160,5

Information sur les enseignements :

- Le public de tous les enseignements est « informatique » à partir du L2.
- Pour tous les enseignements j'ai réalisé la totalité des supports de cours, de TD et de TP, ainsi que les sujets des épreuves.
- Mon service dû était réduit à 182h en raison de mon congé paternité.
- Je suis devenu **co-directeur des études du portail Sciences de l'Ingénieur** (entre 170 et 250 étudiants sur L1-L2) en décembre 2010.

Université de Bordeaux 1

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Cartes à puce	M2	7	9		19,5
Total						19,5

Année 2011-2012

Université de Limoges

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
Responsable gestion de 7 personnes	Informatique 1	L1		63		63
Responsable UE à distance	Outils de l'internet	L1	3	75,5		80
Responsable	Informatique 1 bis	L1		42		42
Responsable	Option Info 1 : Réseau 1	L2	21	24	30	85,5
	Soutien inter-session + plan licence + colles	L1		46,5		46,5
Responsable	Certification et développement sécurisé	M2	16,5		9	33,75
Total						350,75
Heures complémentaires						171,75

Information sur les enseignements :

- Le public de tous les enseignements est « informatique » à partir du L2.
- Pour tous les enseignements j'ai réalisé la totalité des supports de cours, de TD et de TP, ainsi que les sujets des épreuves.
- **Rédaction des supports pour la plate-forme nationale « Informatique et Sciences du Numérique »** (43h eq TD non inclus dans le tableau ci-dessus)
- **Formation ISN des enseignants de l'académie de Limoges** (10h eq TD non inclus dans le tableau ci-dessus).
- Mon service dû était réduit à 179h en raison de différentes tâches du **référentiel national des tâches** (projet de M1, accueil lycéen).
- **L'UE Informatique 1 bis est une UE nouvelle**, créée pour les étudiants inscrits en CPEL2 (Classe Préparatoire à l'Entrée en Licence 2 – étudiants venant soit du semestre CPEL1 – semestre de remise à niveau pour les étudiants ne disposant pas de fondations scientifiques suffisantes pour un semestre 1 dans un des portails de la Faculté des Sciences et Techniques – soit du semestre 1 classique et ayant eu une moyenne inférieure à 8). **J'ai donc créé de nouveaux contenus.**

Université de Bordeaux 1

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Cartes à puce	M2	7	9		19,5
Total						19,5

Institut Supérieur d'Informatique, de Modélisation et de leurs Applications (Clermont-Ferrand)

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Sécurité des systèmes embarqués	M2	5	5		12,5
Total						12,5

**Année 2012-2013
(passage au LMD3)**

Université de Limoges

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
co-responsable gestion de 5 personnes	Informatique 1	L1		72		72
Responsable UE à distance	Outils de l'internet	L1	1,5	57		59,25
Responsable	Informatique 1 bis	L1		34,5	15	44,5
Responsable	Informatique 2 PC	L1	9	27	15	50,5
Responsable	Option Info 1 : Réseau 1	L2	21	24	15	70,5
	Soutien inter-session + plan licence + colles	L1		51,5		51,5
Responsable	Certification et développement sécurisé	M2	14	7		28
					Total	376,25
					Heures complémentaires	190,25

Information sur les enseignements :

- Le public de tous les enseignements est « informatique » à partir du L2.
- Pour tous les enseignements j'ai réalisé la totalité des supports de cours, de TD et de TP, ainsi que les sujets des épreuves.
- **Formation ISN des enseignants de l'académie de Limoges (10h eq TD non inclus dans le tableau ci-dessus).**
- Mon service dû devrait être réduit à moins de 186h en raison de différentes taches du **référentiel national des taches** (projet de M1, ...).
- Implication dans la prépa intégrée INSA.
- Création d'une **nouvelle UE** (Informatique 2 PC). **J'ai donc créé de nouveaux contenus.**

Université de Bordeaux 1

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Cartes à puce	M2	7	9		19,5
					Total	19,5

Institut Supérieur d'Informatique, de Modélisation et de leurs Applications (Clermont-Ferrand)

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Sécurité des systèmes embarqués	M2	5	5		12,5
					Total	12,5

Université de Limoges

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
co-responsable gestion de 5 personnes	Informatique 1	L1		136,5		136,5
Responsable	Option Info 1 : Réseau 1	L2	23	25,5	31,5	91,5
	Soutien inter-session + plan licence + colles	L1		28		28
Responsable	Certification et développement sécurisé	M2	16	8		32
					Total	288
					Heures complémentaires	192

Information sur les enseignements :

- Le public de tous les enseignements est « informatique » à partir du L2.
- Pour tous les enseignements j'ai réalisé la totalité des supports de cours, de TD et de TP, ainsi que les sujets des épreuves.
- Mon service dû était de 96h en raison de mon CRCT.
- Mise en place dans le cadre d'une passerelle PACES vers Faculté des Sciences et Technique de la plate-forme d'enseignement à distance et **création des supports et activités d'autoévaluation pour la discipline Informatique.**
- **Participation à une séance de formation de l'école doctorale pour présenter le CNU et le métier d'enseignant-chercheur.**

Université de Bordeaux 1

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Cartes à puce	M2	7	8		18,5
					Total	18,5

Institut Supérieur d'Informatique, de Modélisation et de leurs Applications (Clermont-Ferrand)

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Sécurité des systèmes embarqués	M2	5	5		12,5
					Total	12,5

Malgré l'obtention d'un CRCT par la voie CNU pour le second semestre, j'ai effectué de nombreuses heures complémentaires au premier semestre afin de ne pas pénaliser d'avantage mes collègues. Par exemple il a fallu que je prenne un groupe supplémentaire en L1 au pied levé !

Année 2014-2015

Université de Limoges

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
co-responsable gestion de 7 personnes	Informatique 1	L1		54		54
Responsable	Informatique 2 PC	L1	9	2*12	2*6	49,5
Responsable	Option Info 1 : Réseau 1	L2	21	24	2*9	73,5
	Soutien inter-session + plan licence + colles	L1		29		29
Responsable	Cartes à puce 1	M2	15	4,5	2*15	57
Responsable	Certification et développement sécurisé	M2	17	9		34,5
					Total	297,5
					Heures complémentaires	>100

Information sur les enseignements :

- Le public de tous les enseignements est « informatique » à partir du L2.
- Pour tous les enseignements j'ai réalisé la totalité des supports de cours, de TD et de TP, ainsi que les sujets des épreuves.
- Mise en place d'une nouvelle plate-forme d'enseignement à distance pour la passerelle PACES vers Faculté des Sciences et Technique.
- Mon service dû devrait être réduit à moins de 168h en raison de différentes tâches du **référentiel national des tâches** (projet de M1, accueil collégiens, ...).
- **Création de nouveaux supports pour le cours de « Cartes à puce 1 » de M2.**
- **Création de cours pour des collégiens** dans le cadre du programme Maths C2+ monté par l'Institut de Recherche sur l'Enseignement des Mathématiques de Limoges (5h eq TD non inclus dans le tableau ci-dessus)

Université de Bordeaux 1

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Matériels Mobiles et Systèmes Associés : Java Card	M1	4	4		10
					Total	10

Ci-dessus, il s'agit d'une intervention en M1 dans le Master Réseaux, systèmes et mobilité.

Institut Supérieur d'Informatique, de Modélisation et de leurs Applications (Clermont-Ferrand)

Commentaires	UE	Niveau	C	TD	TP	Total (heqTD)
	Sécurité des systèmes embarqués	M2	5	5		12,5
					Total	12,5

Après avoir bénéficié d'un CRCT en 2014, **je ne souhaitais plus effectuer d'heures complémentaires** car c'est une grande chance que de pouvoir se consacrer totalement aux deux facettes du métier d'enseignant-chercheur. **Néanmoins le départ soudain** (nous l'avons découvert à 1 semaine de la rentrée universitaire) **en détachement d'un collègue responsable du M2, m'a contraint d'accepter de le remplacer dans les enseignements qu'il délivrait en M2.**

Sur la base de l'expertise nationale reconnue de l'université de Limoges au travers du département TIC de la Faculté des Sciences et Techniques dans l'enseignement à distance et sur celle du master Cryptis créé il y a plus de 25 ans à Faculté des Sciences et Techniques dans le domaine de la sécurité informatique et la cryptographie, mon principal projet consiste à monter un **master francophone dans le domaine de la sécurité de l'information**. En effet, il existe des masters anglais dans la thématique, comme par exemple celui initié par mes collègues du Royal Holloway University of London, et je suis persuadé, comme d'autres collègues, qu'il existe un vivier de bons étudiants dans les pays francophones (voire même en France) qui pourrait être intéressés par une telle formation. D'ailleurs nous intervenons déjà en présentiel dans plusieurs universités d'Afrique du nord (Université Mohammed V à Rabat, Maroc, Université M'Hamed Bougara de Boumerdes, Algérie, etc.). Aussi actuellement je discute de l'opportunité d'un, tel master avec des collègues de différents établissements : Université Mouloud Mammeri de Tizi-Ouzou, Université des Sciences et de la Technologie Houari Boumediene (USTHB) à Alger, Faculté des Sciences de Monastir, Institut Supérieur des Études Technologiques en Communications de Tunis (ISET'COM), etc.

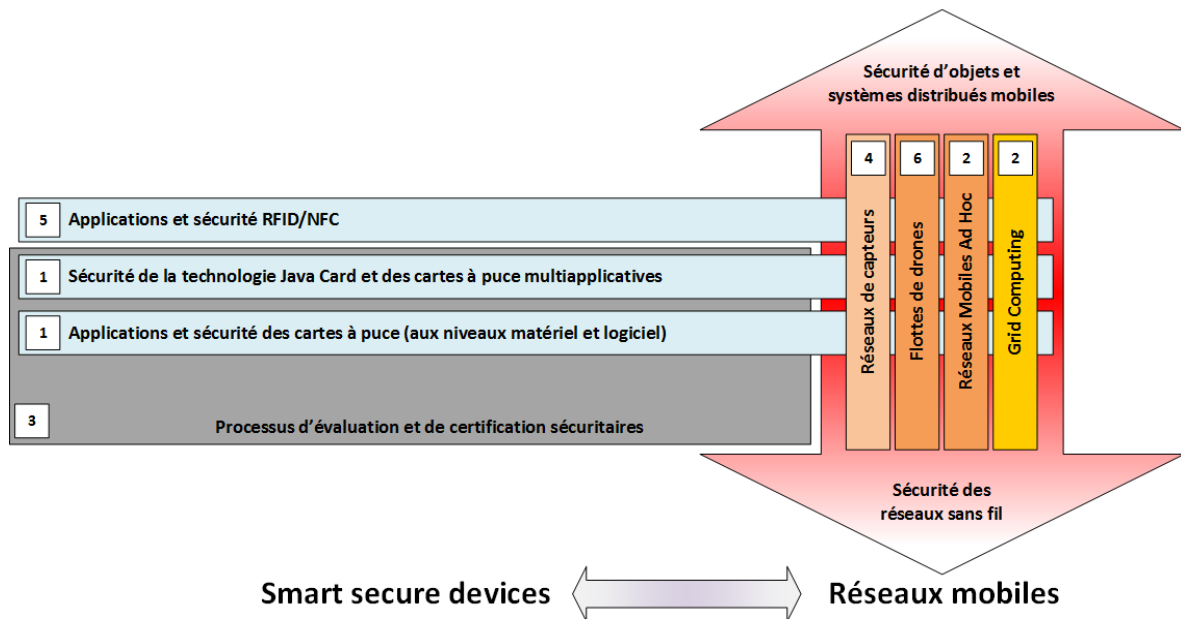
Bien évidemment à côté de ce projet ambitieux qui ne se fera pas sans une volonté politique forte (mais la tendance étant à nous inciter à développer l'enseignement à distance, j'ai bon espoir qu'il puisse aboutir), **j'entends m'investir davantage** (l'obtention de l'HDR étant un argument en faveur de cela) **au niveau du M2** afin de pouvoir former des étudiants qui pourraient poursuivre en stage recherche puis en thèse avec mes collègues et moi. Cela passe par exemple par essayer de demander la réouverture de l'UE « Initiation à la recherche » qui n'était plus assurée en raison des nombreuses heures complémentaires et du peu de candidats (je l'avais assuré bénévolement en 2007 et 2008). Je souhaiterais également renforcer la place de l'UE « Certification et développement sécurisé » car les processus de réflexion qu'elle introduit sont fondamentaux pour augmenter la confiance dans la sécurité implémentée dans les produits. À vrai dire, j'envisage même de proposer un ouvrage à visée pédagogique détaillant son contenu afin d'en faire profiter toute la communauté francophone s'intéressant à la sécurité informatique.

Recherche

Évolution et structuration de ma recherche

Lors de la rédaction de mon Habilitation à Diriger des Recherches, je me suis attaché à montrer comment et pourquoi mes travaux de recherches ont évolué, en 10 années depuis la soutenance de mon doctorat, en un projet scientifique cohérent me permettant d'acquérir mon autonomie scientifique tout en restant dans les thématiques du laboratoire XLIM.

La figure ci-dessous illustre parfaitement les évolutions tant thématiques que temporelles de mes activités de recherche pour former mon projet scientifique « *Sécurité et interactions des smart secure devices et des réseaux mobiles* » qui sera détaillé plus loin. Mais en quelques mots, celui-ci consiste à sécuriser les smart secure devices (les cartes à puce, les étiquettes radio-fréquences ou tag RFID, etc.) mais aussi à les utiliser pour sécuriser les réseaux mobiles tant au niveau des nœuds que des échanges entre eux. La numérotation sur la figure indique la chronologie de mes différentes activités de recherches. Bien sûr, celles-ci n'ont pas été réalisées dans un séquençement aussi caricatural et elles ont souvent été entremêlées. Cet ordonnancement offre toutefois une bonne vision des évolutions de ma recherche.



Ainsi après la fin de ma thèse de doctorat dans laquelle je m'étais intéressé à la sécurité et aux applications des cartes à puce (en particulier de la technologie Java Card), j'ai poursuivi mes travaux sur les cartes multiapplicatives pendant plusieurs années. Sur ce sujet, j'ai récemment obtenu de beaux résultats.

De façon parallèle, au début j'ai poursuivi mes travaux, initiés en thèse, dans le domaine de la sécurisation des grilles de calcul à l'aide de cartes à puce avant de m'en éloigner pour mettre l'accent sur l'aspect mobilité en travaillant sur les réseaux mobiles ad hoc (principalement les Mobile Ad hoc Networks – MANETs). Ces travaux ont constitué ma « conversion » au sens sacré du terme, à la « mobilité » en passant d'activités de sécurisation du « grid computing » (c'est-à-dire des systèmes fondamentalement fixes) vers des activités similaires sur le « wireless mobile computing » (c'est-à-dire des systèmes particulièrement mobiles et volatiles). Je veux toutefois souligner que les travaux fondateurs sur la sécurisation de la grille ont ouvert la piste à de nombreuses recherches fructueuses qu'a su poursuivre mon ancien directeur de thèse avec deux doctorants ayant soutenu avec succès leur thèse.

Ayant travaillé lors de ma thèse CIFRE, dans un Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI), je souhaitais faciliter l'évaluation de produits basés sur la technologie Java Card et, après avoir pris un peu de recul, montrer les limites de l'application de ces méthodologies d'établissement de la confiance, en particulier dans le cadre des cartes à puce.

Il y a 3 ans, je me suis intéressé aux réseaux de capteurs qui par bien des aspects se rapprochent des problématiques des MANETs et des cartes à puce. En un sens, ce type de réseaux est à l'interface des activités smart secure devices et réseaux mobiles ; pour leur présentation sur la figure, ces travaux pourraient se trouver indifféremment dans l'une ou l'autre des parties. J'ai choisi de les placer au sein des réseaux mobiles car même si mes contributions actuelles sont mineures, elle établissent le lien avec les travaux les plus récents sur les flottes de drones.

Plus récemment, avec plusieurs collègues, nous nous sommes intéressés à offrir des solutions innovantes utilisant la technologie RFID. Au travers de la technologie Near-Field Communication (NFC), un sous-ensemble de la technologie RFID, de nouvelles passerelles de communication entre les smart secure devices et les nœuds des réseaux mobiles sont possibles. En particulier je m'intéresse actuellement à la sécurité des tags RFID actifs pour lesquels peu de travaux ont été menés ainsi qu'à leurs utilisations pour sécuriser des réseaux mobiles. C'est dans ce contexte que je viens de débiter un coencadrement doctoral avec l'université de Tizi-Ouzou sur la thématique.

Ainsi, si mes derniers travaux sur les flottes de drones pourraient paraître complètement déconnectés du reste de mes activités, ils sont en réalité très enchevêtrés avec les points précédents puisqu'ils consistent en l'utilisation d'un smart secure device radio-fréquence actif embarqué sur chaque drone pour sécuriser tant le nœud lui-même que l'essai dans sa globalité.

Voici la totalité de ma production scientifique pour chacun de ces grands domaines. Il est bien évident que si la production est ici présentée par thématique, c'est dans la totalité que le jury d'HDR a jugé de la cohérence et de la pertinence de mon projet.

	Revue	Chapitre	SI	Actes	CI	CN	Soumis
1 – Cartes à puce		4	2+2AP	4	1		
1 – Cartes multiapplicatives	1+1RM				4	1	3
5 – RFID/NFC					1		
3 – Évaluation/Certification	1				1		
2 – Grid Computing	1			1	8	1	
2 – Réseaux Mobiles Ad Hoc	1				3		
4 – Réseaux de capteurs		2	1+3AP				
6 – Flottes de drones					1		
Autres			5			1	
Total	4+1RM	6	8+5AP	5	19	3	3

SI : Numéro spécial de revue (en anglais Special Issue) ; CI : Conférences internationales ; CN : Conférences nationales ;
RM : Révision mineure ; AP : À paraître

Tableaux récapitulatifs des publications

Nombre de publications dans de journaux internationaux avec comité de lecture	4
Nombre de publications dans de journaux internationaux avec comité de lecture (en révision mineure)	1
Nombre de publications dans des actes de colloques internationaux avec comité de lecture	18
Nombre de publications dans des colloques internationaux avec comité de lecture sans actes	1
Nombre de publications dans des actes de colloques nationaux avec comité de lecture	3
Nombre de participations à des ouvrages collectifs	6
Total	33

Nombre d'actes de colloques édités	5
Nombre de numéros spéciaux de journaux édités	8
Nombre de numéros spéciaux de journaux à paraître	5
Total	18

Nombre de participation à des œuvres de vulgarisation	6
Nombre de rapports de recherche	5
Nombre de mémoires	3
Nombre de posters	5
Total	18

Il est à noter que la pratique de publications adoptée avec quasiment tous mes co-auteurs est un classement dans l'ordre alphabétique. Le niveau de contribution de chaque auteur doit être assez similaire sur tous les travaux ci-après.

Liste complète des publications

Éditeur de

1. D. Naccache, D. Sauveron (Eds.).
[*Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices.*](#)
8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30 - July 2, 2014
Springer Lecture Notes in Computer Science Series, Vol. 8501, 2014, 201 p. ISBN: 978-3-662-43825-1
2. P. Samarati, M. Tunstall, J. Posegga, K. Markantonakis, D. Sauveron (Eds.).
[*Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices.*](#)
Fourth IFIP WG 11.2 International Workshop, WISTP 2010, Passau, Germany, April 12-14, 2010.
Springer Lecture Notes in Computer Science Series, Vol. 6033, 2010, 386 p. ISBN: 978-3-642-12367-2
3. T.-H. Kim, L.T. Yang, J.H. Park, A.C.-C. Chang, T. Vasilakos, Y. Zhang, D. Sauveron, X. Wang and Y.-S. Jeong (Eds.).
[*Advances in Computational Science and Engineering.*](#)
Second International Conference, FGCN 2008, Workshops and Symposia, Sanya, Hainan Island, China, December 13-15, 2008. Revised Selected Papers
4. J.A. Onieva, D. Sauveron, S. Chaumette, D. Gollmann, K. Markantonakis (Eds.).
[*Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks.*](#)
Second IFIP WG 11.2 International Workshop, WISTP 2008, Seville, Spain, May 13-16, 2008.
Springer Lecture Notes in Computer Science Series, Vol. 5019, 2008, 151 p. ISBN: 978-3-540-79965-8
5. D. Sauveron, K. Markantonakis, A. Bilas, A. J.-J. Quisquater (Eds.).
[*Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems.*](#)
First IFIP TC6 / WG 8.8 / WG 11.2 International Workshop, WISTP 2007, Heraklion, Crete, Greece, May 9-11, 2007.
Springer Lecture Notes in Computer Science Series, Vol. 4462, 2007, 255p. ISBN: 978-3-540-72353-0

Éditeur invité des journaux/revues

1. G. P. Hancke, A. Mitrokotsa, R. Safavi-Naini, D. Sauveron (Eds.).
[*Special Issue on Recent Advances in Physical-Layer Security*](#)
Journal of Computer Networks. Elsevier
2013 Impact Factor: 1.282 – SJR: 0.88 – Q1. À paraître en 2016.
2. R. N. Akram, H.-H. Chen, J. Lopez, D. Sauveron, L. T. Yang (Eds.).
[*Special Issue on Security, Privacy and Trust of the User-centric Solutions*](#)
Future Generation Computer Systems. Elsevier
2013 Impact Factor: 2.639 – SJR: 1.24 – Q1. À paraître en 2016.
3. N. Mentes, D. Sauveron, J.M. Sierra Cámara, S. J. Wang, I. Woungang (Eds.).
[*Special Issue on Lightweight and Energy-Efficient Security Solutions for Mobile Computing Devices*](#)
IET Information Security. IET
2013 Impact Factor: 0.631. À paraître en 2016.
4. Y-S. Jeong, H. R. Arabnia, H-C. Chao, S. D. Min, J. J. Park, D. Sauveron (Eds.).
Special Issue on Wellness Technologies and Services for Future Life Care
The Scientific World Journal. Hindawi
2012 Impact Factor: 1.730. À paraître en 2015.
5. S. S. Yeo, H. Chang, W. Chen, N K Chilamkurti, S. Rho, D. Sauveron (Eds.).
Special Issue on Advanced Service Technology and Application in Smart Sensor Networks
International Journal of Distributed Sensor Networks. Hindawi
2013 Impact Factor: 0.923. À paraître en 2015.
6. D. Sauveron, K. Markantonakis, C. Verikoukis (Eds.).
[*Special Issue on Security and Resilience for Smart Devices and Applications*](#)
EURASIP Journal on Wireless Communications and Networking, 2014. Springer.
2013 Impact Factor: 0.80.
7. S. Rho, D. Sauveron, W. Chen (Eds.).
[*Special Issue on Advanced Signal Processing and HCI Issues for Interactive Multimedia Services*](#)
Multimedia Tools and Applications, September, 2013. Springer
2013 Impact Factor: 1.058.
8. Y.S. Jeong, D. Sauveron, J.H. Park (Eds.).
[*Special Issue on Advanced Security Technologies and Services for Future Computing Environments*](#)
The Computer Journal 56 (10), 2013. British Computer Society - Oxford University Press.
2013 Impact Factor: 0.888.
9. S. Rho, D. Sauveron, K. Markantonakis (Eds.).
[*Special Issue on Advanced Semantic and Social Multimedia Technologies for Future Computing Environment*](#)
Multimedia Tools and Applications, vol 64, N°2, 2013. Springer
2013 Impact Factor: 1.058.
10. B. Preneel, J. Kim, D. Sauveron (Eds.).
[*Special Issue on Advanced theory and practice for cryptography and future security*](#)
Mathematical and Computer Modelling 55; 2012
2013 Impact Factor: 2.020.
11. J. H. Park, S.-J. Wang, Damien Sauveron (Eds.).
[*Special Issue on Security technologies and applications for convergence environments*](#)
Security and Communication Networks 5(3), 2012
12. J. H. Park, H.-C. Chao, D. Sauveron, Y. Xiang (Eds.).
Special Issue on Intelligent Internet Computing : Applications and Security Systems
JIT (Journal of Internet Technology), 2010, indexed by SCI-E (Ministry of Education – Taiwan).
2013 Impact Factor: 0.418.
13. S. S. Yeo, J. H. Park, K. P. Arnett, K. K. Lai, D. Sauveron, T. Tabata (Eds.).

Chapitres de livres

1. D. Sauveron, S. Chaumette.
[Wireless Sensor Nodes](#)
Chapter 14 in Secure Smart Embedded Devices, Platforms and Applications. Springer. 2014. ISBN: 978-1-4614-7914-7
K. Mayes, K. Markantonakis (Eds.)
2. J. Albert, L. Barrère, S. Chaumette, D. Sauveron.
[Wireless Sensor Languages and programming/Developments/Tools/Examples](#)
Chapter 24 in Secure Smart Embedded Devices, Platforms and Applications. Springer. 2014. ISBN: 978-1-4614-7914-7
K. Mayes, K. Markantonakis (Eds.)
3. S. Bouzeffrane, D. Sauveron, J. Cordry, K. Garri.
Mise en œuvre d'une application, choix de solutions, performances.
Les cartes à puce. Hermes. 2013. ISBN: 978-2-746-23913-5
S. Bouzeffrane, P. Paradinas (Eds.)
4. D. Sauveron.
[Smart Card Reader APIS.](#)
Chapter 12 and Appendice in Smart Cards, Tokens, Security and Applications. Springer. 2008. ISBN: 978-0-387-72197-2
K. Mayes, K. Markantonakis (Eds.).
5. M. Tunstall, K. Markantonakis, D. Sauveron, K. Mayes.
[Smart Cards: Communication Protocols and Applications.](#)
Chapter 151 in Handbook of Computer Networks, Wiley. 2007. H. Bidgoli (Ed.).
6. K. Markantonakis, K. Mayes, M.J. Tunstall, D. Sauveron, F. Piper.
[Smart Card Security.](#)
Computational Intelligence in Information Assurance and Security. Springer SCI Series. 2007. Vol 57, pp.201-237, ISBN: 978-3-540-71077-6. Nadia Nedjah, Ajith Abraham, Luiza de Macedo Mourelle (Eds.).

Journaux

1. R. N. Akram, K. Markantonakis, D. Sauveron.
A Novel Consumer-Centric Card Management Architecture and Potential Security Issues.
Information Sciences, Elsevier.
2013 Impact Factor: 3.893 – Q1 – SJR: 2.61. En révision mineure (seule modification demandée : ordonner alphabétiquement les références – cf la notification du journal jointe à la publication)
2. D. Sauveron.
[Multiapplication Smart Card: Towards an Open Smart Card?](#)
Information Security Technical Report (ISTR), Vol. 14, No. 2, May 2009, pp70-78. Elsevier.
3. S. Chaumette, D. Sauveron.
[Smart cards and remote computing: Interaction or convergence?](#)
Information Security Technical Report (ISTR), Vol. 14, No. 2, May 2009, pp101-110. Elsevier.
4. P. Dusart, D. Sauveron, Kim Tai-Hoon.
Some limits of Common Criteria certification
International Journal of Security and Its Applications (IJSIA), Vol. 2, No. 4, October, 2008, pp11-20.
5. P-F Bonnefoi, D. Sauveron, J. H. Park.
MANETS: an exclusive choice between use and security?
Special Issue on Interactive Multimedia & Intelligent Services in Mobile and Ubiquitous Computing (MUC) of COMPUTING AND INFORMATICS, Vol. 27, No. 5, 2008.
2008 Impact Factor: 0.492

Conférences internationales avec comité de programme et actes

1. R. N. Akram, K. Markantonakis, D. Sauveron.
[*Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager*](#).
13th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (IEEE TrustCom-14) Beijing, China, 24-26 September, 2014.
Classée A dans les différentes bases de données. Taux d'acceptation < 15% ([Programme](#))
2. K. Markantonakis, K. Mayes, D. Sauveron, I. G. Askoxylakis.
[*Overview of Security Threats for Smart Cards in the Public Transport Industry*](#).
IEEE International Conference on e-Business Engineering (ICEBE) 2008. 22-24 October 2008, Xi'an, China.
Classée B dans CORE
3. I. G. Askoxylakis, D. Sauveron, K. Markantonakis, T. Tryfonas, A. Traganitis.
[*A Body-Centered Cubic Method for Key Agreement in Dynamic Mobile Ad Hoc Networks*](#).
SECURWARE 2008. 25-31 August 2008, Cap Esterel, France.
4. P. Dusart, D. Sauveron.
Which trust can be expected of the Common Criteria certification at end-user level?
First International Workshop on Information Assurance in Networks (IAN 2007). 6-7 décembre 2007, Jeju Island, Korea. **"Papier invité"**
5. S. Chaumette, S. Eonet, J. Gimenez, D. Sauveron.
Evaluation and comparison of the PRNG of different brands of Java Cards. - Framework and first results.
e-Smart 2007. 19-21 septembre 2007, Nice, France.
6. S. Chaumette, A. Karray, D. Sauveron.
Extended Secure Memory for a Java Card in the Context of the Java Card Grid project.
11th IEEE Nordic Workshop on Secure IT-systems: NordSec 2006. 19-20 octobre 2006, Linköping, Suède.
7. E. Atallah, P-F. Bonnefoi, C. Burgod, D. Sauveron.
Mobile AD hoc Network with Embedded Secure System.
Aml.d 2006. 20-22 septembre 2006, Nice, France.
8. S. Chaumette, K. Markantonakis, K. Mayes, D. Sauveron.
The Mobile Java Card Grid Project.
e-Smart 2006. 20-22 septembre 2006, Nice, France.
9. S. Chaumette, D. Sauveron.
A High Level Security Framework for the Grid: the Java Card Grid Testbed.
The 2006 High Performance Computing & Simulation (HPC&S) Conference. 28 – 31 mai 2006, Bonn, Germany. **"Papier invité"**
10. S. Chaumette, A. Karray, D. Sauveron.
The Software Infrastructure of a Java Card Based Security Platform for Distributed Applications.
4th International Workshop on Security In Information Systems: WOSIS 2006. 23 – 24 mai 2006, Phaos, Cyprus.
Classée C dans CORE. Taux d'acceptation ~ 46%
11. S. Chaumette, A. Karray, D. Sauveron.
Secure Collaborative and Distributed Services in the Java Card Grid Platform.
Workshop on Collaboration and Security (COLSEC'06). 14 – 17 mai 2006, Las Vegas, Nevada, USA.
12. S. Chaumette, D. Sauveron.
Some security problems raised by open multiapplication smart cards.
10th Nordic Workshop on Secure IT-systems: NordSec 2005. 20 – 21 octobre 2005, Tartu, Estonie.
Taux d'acceptation ~ 46%
13. E. Atallah, S. Chaumette, F. Darrigade, A. Karray, D. Sauveron.
A Grid of Java Cards to Deal with Security Demanding Application Domains.
E-Smart 2005. 21 – 23 septembre, Nice, France.
"Prix de la technologie la plus innovante" (seul prix attribué)

14. P-F. Bonnefoi, P. Poulingeas, D. Sauveron.
MADNESS: A Framework Proposal for Securing Work in Ad Hoc Networks.
International Conference on Computer, Communication and Control Technologies: CCCT'05. 24-27 juillet 2005, Austin, Texas, USA.
15. S. Chaumette, D. Sauveron.
An efficient and simple way to test the security of Java Cards.
3rd International Workshop on Security In Information Systems: WOSIS 2005. 24 – 25 mai 2005, Miami, Floride, USA.
Classée C dans CORE
16. S. Chaumette, P. Grange, A. Karray, D. Sauveron, P. Vignéras.
Secure distributed computing on a Java Card Grid.
7th International Workshop on Java for Parallel and Distributed Computing. 4–8 avril 2005, Denver, Colorado, USA.
17. S. Chaumette, P. Grange, D. Sauveron, P. Vignéras.
Computing with Java Cards.
International Conference on Computer, Communication and Control Technologies: CCCT'03. 31 juillet – 2 août 2003, Orlando, Floride, USA.
"Meilleur article de la session Computer and Systems Security"
18. S. Chaumette, I. Hatchondo, D. Sauveron.
JCAT: An environment for attack and test on Java Card.
International Conference on Computer, Communication and Control Technologies: CCCT'03. 31 juillet – 2 août 2003, Orlando, Floride, USA.

Conférences internationales avec comité de programme sans actes

1. R. N. Akram, P-F. Bonnefoi, S. Chaumette, K. Markantonakis, D. Sauveron.
Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements - A Position Paper.
2nd AETOS international conference on "Research challenges for future RPAS/UAV systems". Bordeaux, France, 9-10 September, 2014

Conférences nationales avec comité de programme et actes

1. S. Chaumette, A. Karray, D. Sauveron.
Gestion de la Sécurité pour l'Extraction Parallèle Distribuée des Connaissances.
EGC 2006 (Sixième Journées Francophones "Extraction et Gestion de Connaissances"). 17 – 20 janvier 2006, Lille, France.
2. P. Dusart, D. Sauveron.
La guerre du développement numérique. Menaces sur la confidentialité des photos numériques.
3ème Symposium sur la Sécurité des Technologies de l'Information et des Communications. 1 – 3 juin 2005, Rennes, France.
3. S. Chaumette, D. Sauveron.
Modèles de mémoire en Java Card. Introduction du concept de pré-persistance.
MAJECSTIC'04 (MAnifestation des JEunes Chercheurs STIC). 13 – 15 octobre 2004, Calais, France.

Œuvres de vulgarisation

1. Pierre Dusart, D. Sauveron.
Exploration de carte bancaire BO'.
GNU Linux Magazine/France Hors Série 39, Novembre/Décembre 2008. ISSN xxx. Édition Diamond.
2. V. Jolivet, D. Sauveron. *Sécuriser son ordinateur contre les virus.* Revue du cadre de Santé. Juillet-Août 2005, numéro 19, p28-29. ISSN 1760-2890. Édition Elviesier
3. V. Jolivet, D. Sauveron. *Sécuriser son ordinateur. Les antivirus.* Revue du cadre de Santé. Septembre-Octobre 2005, numéro 20. ISSN 1760-2890. Édition Elviesier
4. V. Jolivet, D. Sauveron. *Sécuriser son ordinateur. Les parefeux.* Revue du cadre de Santé. Novembre-Décembre 2005, numéro 21. ISSN 1760-2890. Édition Elviesier

5. V. Jolivet, D. Sauveron. *Sécuriser son ordinateur. Les parefeux II*. Revue du cadre de Santé. Janvier-Février 2006, numéro 22. ISSN 1760-2890. Édition Elviesier
6. D. Sauveron. *La carte à puce multi-applicative et sa sécurité*. Dossier de presse pour la journée Les nouveaux enjeux de la carte à puce. 19 décembre 2001, Talence, France.

Rapports de recherche

1. S. Chaumette et D. Sauveron.
New security problems raised by open multiapplication smart cards.
RR-1332-04, LaBRI, Université Bordeaux 1, 2004.
2. S. Chaumette, P. Grange, A. Karray, D. Sauveron et P. Vignéras.
Secure distributed computing on a Java Card Grid. Position paper.
RR-1331-04, LaBRI, Université Bordeaux 1, 2004.
3. S. Chaumette, J-P. Lacoustille, D. Sauveron.
Projet Sécurité Java Card, Rapport d'avancement, Phase 2, Novembre 2001 à Septembre 2002.
RR-1278-02, LaBRI, Université Bordeaux 1, 2002.
4. S. Chaumette, J-P. Lacoustille, D. Sauveron.
Projet Sécurité Java Card, Rapport d'Avancement, Phase 1, Juin 2001 à Octobre 2001.
RR-1267-01, LaBRI, Université Bordeaux 1, 2001.
5. D. Sauveron.
La technologie Java Card : Présentation de la carte à puce. La Java Card.
RR-1259-01, LaBRI, Université Bordeaux 1, 2001.

Mémoires

1. D. Sauveron.
Sécurité et interactions des « smart secure devices » et des « réseaux mobiles ».
Habilitation à Diriger des Recherches. XLIM, Université de Limoges, Décembre 2014.
2. D. Sauveron.
Étude et réalisation d'un environnement d'expérimentation et de modélisation pour la technologie Java Card. Application à la sécurité.
Thèse de doctorat. LaBRI, Université Bordeaux 1, Décembre 2004.
3. D. Sauveron.
Sécurité et vérification d'applications embarquées en environnement Java Card.
Mémoire de DEA. LaBRI, Université Bordeaux 1, Juin 2001.

Autres publications (Posters, ...)

1. E. Atallah, P-F. Bonnefoi, D. Sauveron.
MADNESS.
WISTP2007. 8-11 mai 2007, Heraklion, Greece. (Poster).
2. S. Chaumette, K. Markantonakis, K. Mayes, D. Sauveron.
The Mobile Java Card Grid Project.
The 3rd ISG Smart Card Centre Open-Day. 12 septembre 2006, Egham, UK. (Poster).
3. S. Chaumette, A. Karray, D. Sauveron.
Secure Extended Memory for Java Cards.
The 2006 International Conference on Computational Science and its Applications (ICCSA 2006). 8 – 11 mai 2006, Glasgow, UK. (Poster).
4. S. Chaumette, A. Karray et D. Sauveron.
Le projet Smart Cards Grid.
Rencontres Industriels-Chercheurs. 27 janvier 2006, Bordeaux, France. (Poster).
5. S. Chaumette et D. Sauveron.
The Smart Cards Grid Project.
Cartes 2003. 17 – 19 novembre 2003, Paris, France. (Poster).

Publications soumises

- R. N. Akram, K. Markantonakis, D. Sauveron.
Recovering from a Lost Wallet - A Smart Card's Perspective.
Journal on Pervasive and Mobile Computing, Elsevier May 2014.
2013 Impact Factor: 1.667. Soumis
- R. N. Akram, K. Markantonakis, D. Sauveron.
Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager - Extended Abstract. Electronic Commerce Research, Springer, August 2014.
2012 Impact Factor: 1.55. Soumis
- R. N. Akram, K. Markantonakis, D. Sauveron.
Feature Interaction Problems in Smart Cards with Dynamic Application Lifecycle and their Countermeasures.
11th International Conference on Information Security Practice and Experience (ISPEC 2015)
Classée B dans CORE. Soumis

Publications en cours de finalisation

- R. N. Akram, P.-F. Bonnefoi, P. Dusart, K. Markantonakis, D. Sauveron.
A Set of Efficient Privacy Protection Enforcing Lightweight Authentication Protocols for Low-cost RFID Tags.
- R. N. Akram, P.-F. Bonnefoi, S. Chaumette, K. Markantonakis, D. Sauveron.
Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements - A Position Paper – Extended Abstract.
- R. N. Akram, K. Markantonakis, D. Sauveron
A Trusted Computing Platform for Smart Cards: the TEM - Extended Version

Bref historique

Après ma thèse au LaBRI (2004) et mon post-doctorat (2006) au sein de l'Information Security Group—Smart Card Centre, Royal Holloway University of London, périodes auxquelles mes activités de recherche dans le domaine de la sécurité des cartes à puce multi-applicatives (tant d'un point de vue logiciel que matériel) et de leur utilisation pour la sécurisation de systèmes plus larges et plus complexes (réseaux ad hoc, grilles, etc.) ont donné lieu à plusieurs publications dans des conférences internationales avec comités de lecture, l'année 2007 a consisté à étendre ces travaux (en particulier vers des aspects liés à la mobilité via des propositions de solutions de sécurité pour les réseaux ad hoc mais aussi les DTN, Delay Tolerant Networks – en effet je participais au projet ANR SARAH qui s'est terminé en 2009 et dont les résultats des travaux de recherche dans lesquels j'étais impliqués ont suscité un fort intérêt de la part d'industriels du monde de la sécurité embarquée comme je le présenterai plus loin).

Parallèlement à mes travaux sur la sécurité des réseaux ad hoc et DTN (qui ont donné lieu à une publication en revue et trois publications en conférences), j'ai mené de 2007 à 2009 deux actions importantes et très prenantes qui ont porté leurs fruits dans la période qui nous concerne à savoir 2010-2014. Ainsi, j'ai participé à l'émergence d'une communauté et à la chasse aux financements. Toutefois, comme il est difficile de saucissonner des actions, pour des raisons de cohérence, je préfère vous les présenter en totalité.

L'émergence d'une communauté

Dès fin 2006, j'ai souhaité voir émerger une communauté autour des thématiques « sécurité embarquée », « réseaux mobiles » et « ubiquité ». Ainsi en 2007, j'ai été le fondateur et l'organisateur de la première édition d'un événement international, WISTP (Workshop in Information Security Theory and Practice). Cette première édition qui a eu lieu en Crète a été l'occasion de développer des collaborations avec FORTH-ICS ; elles se sont traduites par deux publications (FORTH-ICS, Royal Holloway University of London et XLIM/Université de Limoges). Cet événement, dont c'est en 2015 la 9^{ème} édition, est aujourd'hui pérennisé et reconnu. Chaque année, les actes sont publiés par Springer dans la série LNCS et WISTP reçoit le soutien de grandes sociétés savantes : ACM, IACR, IEEE, IFIP, ERCIM, etc. Toutes les personnes impliquées dans les différentes éditions reconnaissent que ce succès est le fruit de ma très forte implication tant du côté scientifique en collaborant avec les PC chairs et le Steering Committee afin de maintenir une qualité scientifique de haut niveau (dans le programme lui-même ou dans le choix des orateurs invités) que du côté organisation en collaborant avec les General Chairs et organisateurs locaux (dans l'élaboration des différents aspects de l'événement, dans la recherche de sponsors, etc.). **La reconnaissance de ces efforts s'est traduite en 2014 par ma désignation en tant que Program Chair au côté de David Naccache par les membres du Steering Committee.**

Toujours dans le désir de rassembler et dynamiser une communauté, j'ai pris des responsabilités dans le groupe de travail de l'IFIP 11.2 « Small Systems Security » en devenant vice-président en 2007 et en participant au côté du président Jaap-Henk Hoepman (TNO / Radboud University Nijmegen), du second-vice président Sjouke Mauw (University of Luxembourg) et du secrétaire Erik Poll (Radboud University Nijmegen) à la renaissance de ce groupe de travail, dont le nombre de membres se comptait alors sur les doigts d'une main. Notre première action a consisté à redéfinir le périmètre d'activité du groupe de travail vers « Pervasive Systems Security ». Notre proposition a été approuvée par l'assemblée du TC 11 « Security and Privacy Protection in Information Processing Systems », puis par l'assemblée générale de l'IFIP en 2009. En 2010, j'ai participé à l'organisation du premier séminaire du groupe de travail (localisé en parallèle de RFIDSec 2010 à Istanbul en Turquie) et j'ai trouvé la plupart des financements nécessaires à sa tenue. De la même façon en 2012, j'ai œuvré pour organiser le second séminaire qui a eu lieu en parallèle de RFIDSec 2012 à Nijmegen au Pays-Bas. **Aujourd'hui, le groupe de travail de l'IFIP 11.2 « Pervasive Systems Security » compte plus de 50 membres actifs et j'en suis le président depuis juin 2014. Afin de récompenser mes efforts et mon implication constante dans la communauté, l'assemblée générale de l'IFIP m'a décerné en décembre 2013 le IFIP Silver Core Award.**

La chasse aux financements européens...

L'objectif affiché au travers de ce désir de structuration d'une communauté était et est toujours de pouvoir développer des collaborations internationales dans le cadre de projets européens. En effet, dans le même temps en 2007, j'ai obtenu, après un avis favorable du Conseil Scientifique de l'Université de Limoges, une aide financière de 18000€ du Conseil Régional du Limousin pour m'accompagner dans le montage de projets européens.

Ainsi dès 2007, j'ai participé à la soumission du projet SEE-ERA (initié avant l'obtention du support financier régional), en réponse à l'appel ERA.NET (collaboration avec la Grèce, TEI Athènes, et divers pays des balkans), mais celui-ci n'a été retenu.

En 2008, au sein du consortium constitué de Université de Malaga (ES – porteur du projet), de l'Institut Fraunhofer (DE), de University City de Londres (UK), du Conseil de la Science et de la Technologie (UK), de l'Université Technique de Dresde (DE) et de l'Université de Milan (IT), l'Université de Limoges (FR) a participé au travers de ma personne au montage d'une proposition de projet en réponse à l'appel FET (Future Emerging Technologies) Open. Notre proposition n'a malheureusement pas été retenue car jugée pas assez "futuriste".

En 2008 toujours, j'ai participé aux InfoDays à Bruxelles sur l'appel 3 ICT FET PROACTIVE et j'ai présenté pour avis à deux « scientific officers » à huit clos puis aux scientifiques présents une proposition de projet de l'équipe, mais totalement rédigée par moi : SASSASFET (Security Assurance and Smart Secure ApplicationS of Future Emerging Technologies). Toutefois, à l'époque, ce projet n'a pas finalement pas été jugé prioritaire dans les thématiques du laboratoire.

En 2009, j'ai participé à la soumission de la proposition de projet SMOOTH SPRINT, projet de type « Collaborative Project – Large Scale Integrated Project » en réponse à l'appel « ICT-2009.1.4: Trustworthy ICT ». Ce projet comprenait 15 participants : Oberthur Technologies (FR), Université de Limoges (FR), Xerox Research Center (FR), Sagem Orga (DE), PayPal (LU), Sun Microsystems (DE), Ruhr-Universität Bochum (DE), Escrypt (DE), Institut National de Recherche en Informatique et Automatique (FR), Intercede (UK), University of Applied Sciences of Western Switzerland (CH), Grande Armée Conseil (FR), University of Namur (Facultés Universitaires Notre-Dame de la Paix) (BE), Genigraph (FR). L'intérêt de nos partenaires dans ce projet portait sur les résultats des travaux issus de l'ANR SARAH et les développements qui pouvaient en découler mais aussi sur notre expertise dans le domaine de la sécurité des systèmes embarqués. Hélas, une nouvelle fois, ce projet n'a pas été retenu.

Enfin, en 2009, j'ai participé pour le compte du laboratoire XLIM (au titre de la thématique TIC – sécurité) au montage d'une proposition de projets européens Interreg IV B, le projet « ELIARE Network Sudoe » (ENS) porté par le Conseil Régional du Limousin et dans lequel l'Université de Limoges, l'Université de Poitiers et des Universités espagnoles et portugaises sont impliquées (University of Castilla - La Mancha, Technical University of Madrid, University of Navarra, University of Elche, University of Minho, the Research Association of the Ceramics Industry – AICE, University Carlos III of Madrid). **Ce projet a été accepté pour financement.** C'est par mon intermédiaire que l'Université Carlos III de Madrid, un des membres les plus actifs, a été impliqué suite à des rencontres réalisées au sein de différentes éditions de WISTP. Le projet a démarré fin 2009. Il s'est déroulé conformément au planning et des collaborations scientifiques se sont mises en place. Pour ma part, en 2011, j'ai participé à une proposition de projet financé en Espagne (avec les collègues de l'Université Carlos III de Madrid) et dont le sujet portait sur l'évaluation de l'interopérabilité de protocoles sécurisés. Celui-ci n'a malheureusement pas non plus été retenu.

... mais aussi nationaux

En plus de ces activités autour des financements européens, en 2007, j'ai également été le coordonnateur d'une proposition de projet soumise en réponse à l'appel ANR SeSur ("Sécurité et Sûreté Informatique") entre XLIM (CNRS/Université de Limoges), le CNAM, le LaBRI (CNRS/Université Bordeaux 1), l'École Nationale Supérieure des Mines de St Etienne et l'Information Security Group—Smart Card Centre, Royal Holloway University of London (comme partenaire associé). Ce projet n'a pas été retenu pour financement.

Toujours en 2007, j'ai grandement contribué au montage d'une proposition de projet pour l'appel ANR « Jeunes chercheuses et jeunes chercheurs » afin qu'un collègue puisse piloter un projet financé qui rassemblerait les différents membres de l'équipe, alors sans professeur pour la diriger. Ce projet n'a toutefois pas été retenu.

De l'importance des financements !

Si j'ai pu conduire toutes ces activités pendant le début de cette période 2007-2010, c'est qu'à l'occasion de mon recrutement à Limoges en septembre 2006, j'ai bénéficié d'un dispositif consacré à quelques enseignants-chercheurs (sélectionnés sur la base de la qualité de leur projet scientifique), le Contrat Renforcé Recherche qui comprenait une aide de 15000€/an en crédit de fonctionnement sur deux ans et une décharge partielle de service (40h) sur la première année pour mener mon projet : « Sécurité des cartes à puce multi-applicatives et des réseaux ad hoc ». Mon projet a d'ailleurs fortement contribué à définir le contenu scientifique du programme transversal SeFSI (Sécurité et Fiabilité des Systèmes d'Information) du laboratoire XLIM qui s'est terminé en 2009.

Cette relative autonomie de moyens m'a permis de faire avancer mon projet de recherche, de renforcer mes collaborations et mes contacts (au plan national mais aussi et surtout à l'international) tout en m'inscrivant totalement dans le projet du groupe et en faisant bénéficier mes collègues des lignes comptables auxquelles j'abondais.

Une période transitoire pour s'orienter vers ...

En terme de production scientifique, l'année 2010 et une partie de 2011 ont été des périodes plus compliquées en raison du grand nombres d'heures d'enseignements que j'ai dû assurer en plus des responsabilités locales (Comité Technique, Comité Hygiène et Sécurité, direction des études). Aussi durant cette période je me suis investi dans beaucoup de comités de programme, dans l'édition de plusieurs numéros spéciaux de journaux, et aussi dans un projet DIL (Détection Innovation Laboratoire) avec deux collègues de l'équipe (dont l'un d'eux était le porteur). Ce projet intitulé « Limousin Autonomie & Médiation Sécurisée » portait sur la thématique du maintien à domicile (le projet reposait sur l'utilisation d'éléments de sécurité utilisant la technologie RFID NFC). Je devrais participer à un autre projet DIL en cours de montage qui là encore repose sur l'utilisation d'éléments de sécurité dans le domaine des communications sans contact. À cette même période j'ai également été très sollicité par l'AVRUL (Agence pour la Valorisation de la Recherche Universitaire du Limousin) pour aider à la sécurisation de données confidentielles (par exemple données médicales) de jeunes entreprises en création dans le tissu économique local (issues du Centre Hospitalier Universitaire ou start-up purement industrielles).

L'ensemble des activités scientifiques que je viens de rappeler m'ont permis d'obtenir à partir de 2012 la Prime d'Excellence Scientifique.

... de nouvelles expertises : la sécurité des capteurs communicants et RFIDs

Malgré une charge d'enseignement toujours aussi élevée et l'ajout de nouvelles missions (membre titulaire élu de la section 27 du CNU depuis 2012 – tâche passionnante mais ô combien prenante –, ajout du volet « Conditions de Travail » au CHS), depuis fin 2011, mes recherches ont porté sur deux thèmes connexes à mon expertise historique sur la sécurité des cartes à puce :

- la sécurité des capteurs communicants
- la sécurité des RFID

La prise en compte des problématiques sécuritaires sur ces « smart devices » s'est inscrit dans le cadre de mes activités au sein de l'IFIP WG11.2 « Pervasive Systems Security » mais aussi et surtout dans le cadre de nouvelles orientations scientifiques au sein de l'université de Limoges. En effet, la thématique de la « sécurité autour des capteurs » est de plus en plus présente à Limoges : tant au sein de la fédération de recherche MIRES (Mathématiques & leurs Interactions, Images & information numérique, Réseaux et Sécurité – fédération labellisée FR 3423 par le CNRS de laboratoires du PRES Limousin-Poitou-Charentes) qu'au sein du laboratoire d'excellence Σ -lim (laboratoire commun entre XLIM et le SPCTS – Science des Procédés Céramiques et de Traitements de Surface).

Ces nouveaux travaux, qui s'inscrivent dans le thème général de la « sécurité des réseaux sans fil » (domaine d'intérêt pour XLIM), ont permis de conforter les débuts de collaborations établies avec des collègues physiciens des départements OSA (Ondes et Systèmes Associés) et C2S2 (Circuits Signaux et Systèmes Hautes Fréquences).

Premiers résultats sur la sécurité des RFID

J'ai déposé en 2013 en collaboration avec les collègues d'OSA et C2S2, le projet SoRFID, « Security of RFID » qui a été financé à hauteur de 2500 euros par la fédération MIRES. Ce projet pluridisciplinaire s'inscrivait dans l'axe 3 "réseaux et sécurité" de la fédération et il adressait un aspect du précédent SNRI (Schéma National de Recherche et d'Innovation) portant sur les systèmes d'authentification RFID.

Ainsi, le projet se proposait dans une première phase d'étudier les attaques, et en particulier les attaques par relais, sur différents systèmes RFID passifs fonctionnant à des fréquences différentes (125KHz, 13,56MHz, etc.) comme par exemple : badge d'accès à des locaux, carte sans contact. L'attaque par relais (relay attack) est un type d'attaque informatique dans lequel un attaquant placé entre deux interlocuteurs ne fait que relayer un message d'un expéditeur vers un récepteur valide. Un but de l'attaque par relais est de pouvoir usurper l'identité (ou les droits) d'un utilisateur alors même que celui-ci est hors de portée du système RFID chargé de vérifier son identité (ou de lui octroyer ses droits). La force de cette attaque est de passer outre les mécanismes cryptographiques employés puisqu'elle travaille au niveau de la couche physique.

Une seconde phase du projet consistait à étudier des mécanismes de sécurité proposés contre les attaques par relais et de proposer des méthodes de contournement ou d'attaques de celles-ci : par exemple les « distance bounding protocols » (même si à notre connaissance ils ne sont pas implémentés en pratique dans des systèmes déployés). De façon parallèle, le projet devait essayer de proposer des méthodes ou des préconisations permettant de se prémunir contre les attaques par relais.

À l'issue, d'une année de travail, durant laquelle j'ai encadré pour ce projet 2 étudiants ingénieurs de l'ISITCom dans le cadre de leur projet de fin d'étude (stage cofinancé par le projet et des bourses tunisiennes) nous sommes capable de réaliser plusieurs attaques sur des tags passifs (snooping, clonage, « brute-force » et attaque relais). **Nous avons construit différents démonstrateurs low-cost et nous disposons maintenant d'une plate-forme d'expérimentation RFID pour tags passifs (125 kHz, 134 kHz et 13,56 MHz). Nous avons également réalisées des attaques sur des produits commerciaux et dans le cadre du « responsable disclosure », des contacts sont en train d'être pris avec différentes sociétés pour les sensibiliser à la faible sécurité de leurs systèmes.**

Toutefois le projet étant fini, nous cherchons des possibilités de financement et nous étudions actuellement également la possibilité de déposer un projet FUI afin de travailler sur divers aspects tels que le snooping à distance. Nous venons de recevoir des RFID actifs et nous allons commencer nos premiers travaux. Il est à noter que par bien des côtés, les RFID actifs s'apparentent actuellement dans la forme bien plus à des capteurs communicants qu'à des RFID passifs et que mes premiers travaux sur la sécurité des capteurs devrait nourrir cette activité de recherche. Je viens de débiter un coencadrement d'une doctorante sur cette thématique avec l'université de Tizi-Ouzou.

Premiers résultats sur la sécurité des capteurs communicants

Sur cette thématique j'ai contribué à deux chapitres d'ouvrages internationaux s'intéressant tant à la dimension sécuritaire intrinsèque des capteurs qu'aux problématiques de sécurité lorsqu'ils sont en réseau. J'ai également encadré en 2013, un doctorant tunisien de l'Université de Sfax à Limoges pour un stage de 2 mois sur l'implémentation d'algorithmes légers de chiffrement pour des systèmes embarqués tels que les réseaux de capteurs.

Mobilité et CRCT

En 2009, j'avais publié l'article « *Multiapplication Smart Card: Towards an Open Smart Card?* » qui a servi de cadre de référence pour les travaux de Raja Naeem Akram du Royal Holloway University of London lors de sa thèse « *User Centric Security Model for Tamper-Resistant Devices* » pour laquelle j'ai été désigné rapporteur extérieur en 2012. Grâce au temps libéré par mon CRCT, au second semestre 2014 nous avons pu mettre en œuvre plusieurs idées communes. Cela se traduit par plusieurs publications communes acceptées, soumises, ou en cours de rédaction.

Une nouvelle thématique : la sécurisation des flottes de drones

J'ai également profité du CRCT pour me déplacer au LaBRI (Bordeaux) et à l'Institut de « IT Security and Security Law » de l'Université de Passau (Allemagne) pour travailler avec les professeurs Serge Chaumette et Joachim Posegga. Dans les deux cas nous avons abordé des problématiques de sécurité informatique en lien avec l'aéronautique (drones et communications avioniques) et en lien avec les systèmes distribués.

Ces rencontres avec leurs équipes respectives ont permis d'envisager les premières bases de projets communs.

Suite à la présentation de nos premiers travaux à la conférence « Research challenges for future RPAS/UAV systems » en septembre 2014, le professeur Kamesh Namuduri (University of North Texas) souhaite que nous collaborions sur la sécurisation des Unmanned Aerial Vehiculars (drones).

Sur la thématique des drones, le Professeur Serge Chaumette, une équipe de Thales et moi-même venons de déposer en décembre 2014 un projet sur l'utilisation du network coding dans ce contexte en réponse à un appel interne de Thales.

Visibilité nationale et internationale

- Orateur invité par le Professeur Abdelkader Belkhir à l'occasion des Septièmes Journées Scientifiques du Laboratoire des Systèmes Informatiques (JLSI'14) de l'Université des Sciences et de la Technologie Houari Boumediene (USTHB) à Alger (Algérie)
« *Cartes à puce et sécurité* »
10/12/2014 – Présentation orientée Recherche
- Orateur invité par l'IREM de Limoges dans le cadre des Journées MathC2+, Limoges (France)
« *Les cartes à puce* »
21/10/2014 – Présentation orientée Vulgarisation
- Séminaire au sein de IT-Security Group de l'Université de Passau à Passau (Allemagne)
« *Security and Interactions of Smart Secure Devices and Mobile Networks* »
29/07/2014 – Présentation orientée Recherche
- Séminaire du LIMOS (Laboratoire d'Informatique, de Modélisation et d'Optimisation des Systèmes), Clermont-Ferrand (France)
« *Sécurité des Smart Secure Devices et des réseaux mobiles* »
30/05/2013 – Présentation orientée Recherche
- Orateur invité par la Faculté des Sciences et Techniques dans le cadre des Journées Lycée à la FST, Limoges (France)
« *Les cartes à puce pour le lycée* »
13/12/2011 et le 29/05/2012 – Présentation orientée Vulgarisation
- Orateur invité par Elopsys à ICTF (International Contactless Technologies Forum), Lille (France)
« *Sécurité des réseaux et solutions. État des lieux des solutions existantes et à venir.* »
12/06/2008 – Présentation orientée Recherche/Vulgarisation
- Orateur invité par le WIF (Webdesign International Festival), Limoges (France)
« *Sécurité des usages du WEB actuel et futur* »
18/04/2008 – Présentation orientée Vulgarisation
- Orateur invité à Mathématiques pour tous (organisé par l'IREM, le CIJM, le TML, l'APMEP), Limoges (France)
« *La carte à puce pour tous !* »
30/01/2008 – Présentation orientée Vulgarisation
- Orateur invité par la Faculté des Sciences et Techniques dans le cadre du Colloque Franco-Algérien "Applications de l'arithmétique aux télécommunications", Limoges (France)
« *Présentation de la cartes à puce et son utilisation dans les réseaux informatiques* »
14/12/2007 – Présentation orientée Recherche/Vulgarisation
- Orateur invité par le projet européen InspireD avec le Professeur Serge Chaumette au workshop « The future of Smart Cards » rassemblant les personnes ayant le plus contribué au monde de la cartes à puce, Paris (France)
« *The Mobile Java Card Grid Project* »
13/12/2006 – Présentation orientée Recherche
- Orateur invité par la Région Limousin à l'inauguration de la Maison du Limousin, Paris (France)
« *Carte à puce : SALS et SRAD* »
25/10/2006 – Présentation orientée Recherche/Vulgarisation

Des activités de direction de la recherche

Parmi les activités de direction de la recherche et d'animation scientifique que j'ai accomplies, il y a tout d'abord le travail effectué en tant que vice-président du groupe de travail de l'IFIP¹ Pervasive Systems Security (2007-2013) puis en tant que président depuis 2014. En décembre 2013, en reconnaissance du travail accompli, l'assemblée générale de l'IFIP m'a décerné le « Silver Core Award » qu'aucun chercheur français n'a reçu depuis 2010. De membres se comptant sur le doigt d'une main avant mon arrivée, nous sommes aujourd'hui plus de 50 membres actifs dans le groupe de travail. Je suis actuellement en train de structurer encore davantage ce groupe afin de former des sous-groupes (task forces) collaborant sur des sujets spécifiques (par exemple pour faire un état de l'art, ou produire une proposition). En tout cas, notre groupe est l'un des plus actifs du Comité Technique 11 Security and Privacy Protection in Information Processing Systems.

Mes activités de direction de la recherche et d'animation scientifique se sont aussi traduites et renforcées par la publication de plusieurs numéros spéciaux sur des thématiques scientifiques importantes dans différents journaux ayant de bons facteurs d'impact. Par exemple j'ai rédigé l'an dernier en quasi-totalité des propositions de numéros spéciaux acceptés dans Computer Networks (Impact Factor 1.282), Future Generation Computer Systems (Impact Factor 2.639) et IET Information Security (Impact Factor 0.631). Ceci révèle ma capacité à identifier les sujets importants (confirmé la présence d'éditeurs invités prestigieux à mes côtés et par l'accord des éditeurs en chef de ces journaux) et à conduire un processus rigoureux dans la sélection des articles pour obtenir un ouvrage cohérent et de qualité.

Enfin, si je ne devais citer qu'un seul événement majeur auquel j'ai pu apporter ma vision scientifique parmi les dizaines dans lesquels j'ai été impliqués (conférences, workshops, séminaires), il s'agirait sans conteste de WISTP (Workshop in Information Security Theory and Practice).

Alors que j'ai créé WISTP en 2007 et que je me suis toujours fortement impliqué dans sa réussite, sa 8^{ème} édition vient de se terminer avec un taux d'acceptation de 24%. Face aux différents indicateurs positifs que recueille ce workshop (le taux d'acceptation moyen sur 8 ans est inférieur à 30%, il va devenir une conférence en 2015).

Tous ces éléments sont des indicateurs tendant à montrer ma capacité de direction de la recherche.

Encadrement de niveau doctoral

Lors de mon post-doctorat au Royal Holloway, University of London, **j'ai conseillé et orienté plusieurs thésards locaux dans leurs travaux de recherche (Lishoy Francis, Xuefei Leng, William Sirett et Michael Tunstall)**. J'ai également **conseillé et orienté Achraf Karray** dont la thèse s'est déroulée au LaBRI et **Ève Atallah lors de sa thèse en co-encadrement** qui s'est déroulée dans une collaboration que j'avais initiée entre l'Université de Limoges et le LaBRI sur une thématique visant à sécuriser les réseaux ad hoc en s'appuyant sur la carte à puce (thèse soutenue en 2008).

Un passé un peu grisâtre :

Jusqu'à présent, malgré une demande répétée chaque année depuis plus de 5 ans, aucun financement ne m'a été attribué et l'opportunité de co-encadrer une thèse officiellement ne s'est jusque là pas présentée. Il faut dire que le collègue Professeur qui dirigeait l'équipe à laquelle j'appartenais alors, octroyait tous les moyens à son profit et à celui de 2 autres collègues, laissant deux autres collègues et moi-même dépérir. Suite à ses agissements, depuis 2 ans, il ne fait plus partie du laboratoire et il est parti en détachement à la rentrée 2014 pour 2 ans.

Un avenir plus rose :

Avec la soutenance de mon Habilitation à Diriger des Recherches, cette page s'est tournée et **je commence à encadrer puisqu'en décembre 2014 un co-encadrement à 60% avec Malika Belkadi de l'Université Mouloud Mammeri de Tizi-Ouzou de Amina Cherif, étudiante avec financement, titulaire d'un master en « Réseaux, Mobilité et Systèmes Embarqués », vient de débiter sur le sujet de thèse « Sécurité des RFID actifs et applications » que j'ai proposé et rédigé.**

Un financement industriel par NXP sur la « conception des mécanismes de protection pour un module de sécurité pour les matériels mobiles » est aujourd'hui également ouvert pour un candidat que j'encadrerai à la rentrée 2015.

¹ L'IFIP (International Federation for Information Processing) créée en 1960 sous les auspices de l'UNESCO est la société savante pour l'informatique (elle peut être comparée à IEEE). Elle est reconnue par l'ONU et rassemble plus de 56 sociétés savantes du domaine du traitement de l'information réparties sur les 5 continents et représentant plus d'un demi million de membres. Elle comprend plus de 3500 scientifiques venant du monde académique et de l'industrie. Elle est organisée en 13 comités techniques, eux-même divisés en 101 groupes de travail.

En 2013/2014, j'ai participé à une séance de formation de l'école doctorale pour présenter le CNU et le métier d'enseignant-chercheur.

Encadrement de niveau M2

2004	Co-encadrant du stage de DEA de Achraf Karray « <i>Calcul sécurisé sur grille de cartes à puce</i> »
2005	Co-encadrant à 50% des stages de Master Recherche ISIC de l'Université de Limoges : • Eleonore Nicolas, « Parallélisation de l'algorithme pour le Differential Power Analysis » • Céline Burgod, « Algorithmes de routage sur TMCs (Terminaux Mobiles Communicants) dans un réseau ad hoc »
2006	Aucun encadrement en France en raison de mon post-doctorat.
2007	Co-encadrant des stages de Master Recherche ISIC de l'Université de Limoges : • Adolf Abdallah, « Conception d'un protocole de routage réactif sécurisé à l'aide de processeurs sécurisés embarqués » • Didier Ribiere, « Mise en œuvre de la "Certificateless Public Key Cryptography" en combinaison avec des environnements d'exécution sécurisés » • Winbir Hien, « Élaboration d'un simulateur pour réseau ad hoc mobile (MANet) » • Kassim Youssouf, « Protocole de Routage pour les réseaux Ad hoc de faible densité et à connectivité erratique » • Khalid Rafaa, « Étude et implémentation de protocoles de dérivation de clés de session pour un environnement contraint » Co-encadrant des projets de Master Professionnel CSI (Cryptologie et Sécurité Informatique) de l'Université Bordeaux 1 • Stéphanie Eonet et Jonathan Gimenez, « Statistical Testing of Random Number Generators on Java Cards »
2008	Co-encadrant à 80% des stages de projet de fin d'étude d'élèves ingénieurs de l'EniSo (Tunisie) • Manel Ben Kilani et Noura Ben Hadj Youssef sur un sujet relatif à la « Simple Power Analysis en mode sans contact », 5 mois (mars-juillet 2008) Faute de candidats dans le Master recherche sur les sujets que j'avais proposés, je n'ai pas eu l'occasion de co-encadrer d'étudiants locaux en 2008. En revanche, j'ai co-encadré à 33% le stage de Master Pro de : • Kassim Youssouf, « Analyse des Risques et Préconisations des Mesures Sécuritaires pour la Plateforme SANTESSIME » ; stage effectué dans la société SANTESSIME (localisée à Limoges)
2009	Depuis que notre master est devenu indifférencié, de moins en moins d'étudiants souhaitent s'orienter vers la recherche et je n'ai plus encadré que des étudiants de Master Pro : • Caroline Siu, « Side Channel Cryptanalysis » ; stage effectué dans la société RFI Global Services (Basingstoke, UK)
2010	De la même façon, j'ai encadré deux étudiants lors de leur stage de Master Pro (l'institution d'accueil, n'ayant aucune compétence en sécurité) : • Nadhem Boulifa, « Conseils et sécurisation de la plate-forme ABIS de l'unité INSERM U850 » ; stage effectué au CHU de Limoges dans l'unité INSERM U850 • Faycal Necer, « Utilisation spécifique de la méthode EBIOS® pour élaborer une PSSI pour l'unité INSERM U850 » ; stage effectué au CHU de Limoges dans l'unité INSERM U850
2013	Encadrement à 100% du stage de deux mois de Jalel Hajji, doctorant à l'Université de Sfax (Tunisie) « l'implémentation d'algorithmes légers de chiffrement pour des systèmes embarqués »
	Co-encadrement à 80% des stages de projet de fin d'étude d'élèves ingénieurs de l'ISITCom (Tunisie) à Limoges : • Khalil Mighri, « RFID et attaque par relais : réalisation d'un faux lecteur » • Ghanem Kerfahi, « RFID et attaque par relais : réalisation d'un faux tag » Co-encadrement à 80% du stage de Master Professionnel de Mohamed Ghachem de la Faculté des Sciences de Monastir (Tunisie) « Développement d'un application de contrôle de l'assiduité des étudiants reposant sur la carte étudiant » à Limoges

Rapporteur de thèse

- **Rapporteur extérieur** pour le Royal Holloway, University of London sur la thèse de **Raja Naeem Akram** en 2012

Jury de thèse

- **Examineur** dans le jury de thèse d'**Achraf Karray**, pour les travaux qu'il a menés en co-tutelle entre le LaBRI (Université Bordeaux 1) et l'Université de Sfax (Tunisie), soutenue en décembre 2008.

Encadrements de niveau M1

- J'encadre chaque année environ 8 projets de M1 (par exemple en 2014/2015 : 12 étudiants à Limoges à 100% et 7 à Bordeaux à 50%).

Responsabilités scientifiques 2010-2014 et rayonnement

Responsabilités scientifiques internationales

- [Président de IFIP WG 11.2 Pervasive Systems Security](#) (depuis 2014 ; vice-président de Décembre 2007 à Décembre 2013)
- Directeur régional de la FTRA (depuis 2010)
- Membre de IFIP WG 8.8 Smart Cards (depuis 2006) et de ACM SIGSAC (depuis 2009)

General Chair :

- [FutureTech 2011](#) (Loutraki, Greece)

Program Chair :

- [STA2014](#) (Ostrava, Czech Republic)
- [WISTP2014](#) (Heraklion, Greece)
- [FutureTech 2010](#) (Busan, Korea)

Workshop Chair :

- [ST Com2011](#) (Jeju, Korea)
- [CSA 2011](#) (Jeju, Korea)

Workshop/Panel/Tutorial Chair :

- [WISTP2013](#) (Heraklion, Greece)
- [WISTP2012](#) (Egham, UK)
- [WISTP2011](#) (Heraklion, Greece)
- [WISTP2010](#) (Passau, Germany)

Publications Chair :

- [HPCS 2010](#) (Caen, France)

Member of Steering Committee :

- [WISTP](#) (2008 - ...)

Publicity Chair :

- [ACSA-14](#) (Busan, Korea)
- [SMPE-2013](#) (Barcelona, Spain)
- [HPCC-2011](#) (Alberta, Canada)
- [UIC-2011](#) (Alberta, Canada)
- [ATC-2011](#) (Alberta, Canada)

Éditeur associé :

- [Springer Human-centric Computing and Information Sciences \(HCIS\)](#)
Section "Privacy, Security and trust management"
- [The FTRA Journal of Convergence](#)
Section "Security and Trust"

Membre des Comités de Programme de :

- [HSA 2015](#) (Los Angeles, California, USA)
- [SECITC 2015](#) (Bucharest, Romania)
- [IUPIT 2015](#) (London, UK)
- [PAIT 2015](#) (London, UK)
- [SEC 2015](#) (Hamburg, Germany)
- [MobiSecServ 2015](#) (Gainesville, Florida, USA)
- [CSS 2014](#) (Paris, France)
- [SMART 2014](#) (Paris, France)
- [ECCWS 2014](#) (Piraeus, Greece)
- [HAS 2014](#) (Heraklion, Greece)
- [CUTE 2013](#) (Danang, Vietnam)
- [CSS2013](#) (Zhangjiajie, China)
- [MobiCASE 2013](#) (Paris, France)
- [HCI 2013](#) (Las Vegas, Nevada, USA)
- [ECIW-2013](#) (Jyväskylä, Finland)
- [AIM 2013](#) (Seoul, Korea)
- [CUTE 2012](#) (Hong Kong, China)
- [3SL 2012](#) (Besançon, France)
- [AIM Summer 2012](#) (Jeju, Korea)
- [ECIW 2012](#) (Laval, France)
- [HPGC2011](#) (Jeju, Korea)

- [IAS 2011](#) (Malacca, Malaysia)
- [NSS 2011](#) (Milan, Italy)
- [ECIW 2011](#) (Tallinn, Estonia)
- [IWCS 2011](#) (Loutraki, Greece)
- [DICTAP2011](#) (Dijon, France)
- [3SL 2011](#) (Saint-Malo, France)
- [PDCAT-10](#) (Wuhan, China)
- [RISC'10](#) (London, UK)
- [eForensics 2010](#) (Shanghai, China)
- [CRiSIS'2010](#) (Montreal, Canada)
- [HPCC 2010](#) (Melbourne, Australia)
- [NSS 2010](#) (Melbourne, Australia)
- [STM'10](#) (Athens, Greece)
- [IAS 2010](#) (Atlanta, Georgia, USA)
- [HumanCom 2010](#) (Cebu, Philippines)
- [SEC2010](#) (Brisbane, Australia)
- [ANT 2010](#) (Paris, France)
- [SECRYPT 2010](#) (Athens, Greece)
- [SHPCS2010](#) (Caen, France)
- [ECIW2010](#) (Thessaloniki, Greece)
- [ICEIS 2010](#) (IWRIT -- Funchal, Madeira, Portugal)
- [SH2010](#) (Busan, Korea)
- [CTS 2010](#) ([COLSEC'10](#) -- Baltimore, Maryland, USA)
- [AICCSA' 2010](#) (Hammamet, Tunisia)
- [MOBILIGHT2010](#) (SECURE -- Barcelona, Spain)
- [WISTP2010](#) (Passau, Germany)

Membre du Bureau Éditorial de :

- [SCN](#) (Security and Communication Networks)
- [JPT](#) (Journal of Platform Technology)
- [IJITCC](#) (International Journal of Information Technology, Communications and Convergence)
- [JIPS](#) (Journal of Information Processing Systems)
- [IJSH](#) (International Journal of Smart Home)
- [IJSIA](#) (International Journal of Security and Its Applications)
- the Special Issue on "[MUE2007](#)" of the [IAHUC](#) (International Journal of Ad Hoc and Ubiquitous Computing)
- the Special Issue on "[Application and Security Service in Web and Pervasive Environments](#)" of the [AutoSoft](#) (Intelligent Automation & Soft Computing)

Membre du Bureau de relecture de :

- the [Special Issue on "RFID: Technology, Systems, Applications"](#) of the [JNCA](#) (Journal of Network and Computer Applications)
- [IJCS](#) (International Journal of Computational Science)

Relecteur pour :

- [Information Sciences](#) (2014 -- ISSN: 0020-0255 / Elsevier)
- [IEEE Transactions on Industrial Informatics](#) (2014 -- ISSN: 1551-3203 / IEEE Computer Society & IEEE Industrial Applications Society & IEEE Industrial Electronics Society & IEEE Robotics and Automation Society & IEEE Systems, Man, and Cybernetics Society)
- [IEEE Communications Letters](#) (2014 -- ISSN 1089-7798 / IEEE Communications Society)
- [International Journal of Information Security](#) (2013 -- ISSN 1615-5262 / Springer)
- [JIPS](#) (2009, 2012 -- ISSN 1976-913X / Korean Information Processing Society)
- [UAIS](#) (2012 -- ISSN 1615-5289 / Springer)
- [Computers & Security](#) (2011, 2014 -- ISSN 0167-4048 / Elsevier)
- [IJSIA](#) (2010 -- ISSN 1738-9976 / SERSC)
- [JNCA](#) (2010 -- ISSN 1084-8045 / Elsevier)
- [Computer Standards & Interfaces Journal](#) (2009 -- ISSN 0920-5489 / Elsevier)
- [ISA2009](#) (Seoul, Korea)
- [Springer Telecommunications System Journal](#) (2009 -- ISSN 1018-4864 & 1572-9451 / Springer)
- [IEEE Transactions on Parallel and Distributed Systems](#)
- [The Computer Journal](#) (ISSN 0010-4620 / British Computer Society)

La liste complète de mes activités depuis 2006 est disponible à l'adresse : <http://damien.sauveron.fr/professional-activities/>

Responsabilités scientifiques locales

- **Membre élu au Conseil du Laboratoire d'XLIM par le collège des MCF (2012-...)**
- **Membre élu du Conseil Scientifique de l'Université de Limoges (2008-2012)**
- **Point de contact** (pour la thématique TIC – sécurité) pour le laboratoire XLIM lors du montage d'un **projet européen Interreg** entre l'Université de Limoges, la région Limousin, des Universités Espagnoles et Portugaises : **Projet accepté pour financement** et terminé en septembre 2012.
- **Membre de l'association SPECIF/SIF et correspondant pour l'académie de LIMOGES** (depuis 2007)
- Membre du Comité de Sélection (sections 27-61) pour le recrutement d'un Maître de conférences en 2014 à Limoges
- Membre du Comité de Sélection (section 27) pour le recrutement d'un Maître de conférences en 2009 à Limoges

Expertises

- **Expert pour le 7^{ème} PCRD, l'ANR et ARCSIS (Région PACA). Évaluations de plusieurs dossiers pour ces deux derniers organismes**

Autres responsabilités et activités locales sur la période considérée

- Pendant plusieurs années après la création des pôles de compétitivité, j'ai rencontré régulièrement les responsables du pôle ELOPSYS (implanté en Limousin) et la dizaine d'acteurs industriels régionaux sur la thématique « Réseaux haut-débit sécurisés » pour élaborer des projets de recherche communs.
- J'ai géré la plupart des relations avec les industriels dans l'équipe avant 2009 et j'en gère encore beaucoup en raison de contact privilégié : Atos Origin, EADS, Feitian Technologies, gemalto, Giesecke&Devrient, Fujitsu, Identive Infrastructure, Oberthur Card Systems, Pro-Active, UL (ex-RFI Global Services Ltd), Technicolor, Trusted Logic, etc.

Sécurité et interactions des « smart secure devices » et des « réseaux mobiles »

Ayant soutenu mon Habilitation à Diriger des Recherches en décembre 2014 sur le projet Sécurité et interactions des « smart secure devices » (RFID, carte à puce, capteur, etc.) et des « réseaux mobiles » (réseaux ad hoc, réseaux de capteurs, réseaux véhiculaires, etc.), je souhaite poursuivre mes efforts sur celui-ci. En particulier, je souhaite étudier les possibilités d'utilisation de RFID actifs pour la sécurisation des flottes de drones autonomes (Autonomous Unmanned Aerial Vehicle Swarm). Ces travaux commencés lors de mon CRCT en 2014 ont donné lieu à une publication à la conférence « Research challenges for future RPAS/UAV systems » en septembre 2014, et ont suscité l'intérêt de chercheurs américains. En particulier, le professeur Kamesh Namuduri (University of North Texas) souhaite que nous collaborions sur cette thématique.

Bref état de l'art sur cette thématique de mon projet

1) sur l'utilisation de RFID dans les flottes de drones

Dans la littérature sur les flottes de drones, rares sont les travaux s'intéressant à la sécurisation de l'identité (ou des éléments pouvant la représenter, e.g. la clé privée d'une paire de clés en cryptographie asymétrique). C'est pourtant sur la sécurité des données impliquées dans les mécanismes d'authentification que repose toute la confiance permettant les opérations futures entre drones (échanges de données, routage dans l'hypothèse où il est utilisé, etc.). Dans les architectures de sécurité pour les flottes de drones permettant des communications de groupe (e.g. [1]) ou des travaux collaboratifs (e.g. [2]), la possibilité d'un attaquant ayant un haut potentiel d'attaque (c'est à dire pouvant par exemple accéder physiquement à un drone suite à sa capture) n'est quasiment jamais envisagée. C'est pourtant un modèle réaliste comme nous l'avons montré dans notre article de positionnement [0]. Dans les rares travaux qui envisagent ce modèle d'attaquant, la sécurisation physique des éléments d'identification, cœur de la sécurité, est reléguée au rang d'hypothèse sur le matériel utilisé ou sur des contres-mesures supplémentaires comme l'autodestruction du drone [3]. Les seuls travaux qui envisagent réellement de protéger les éléments d'identification sont ceux initiés au LaBRI via l'utilisation de Java Card [4,5]. Puisque je me propose d'étendre ces travaux via l'utilisation de RFID actifs, il est intéressant de voir l'utilisation des RFID dans des contextes proches. Dans les travaux sur les flottes de robots, on trouve l'utilisation de RFID passifs pour faire communiquer des robots soit pour de l'affectation de tâches [6], soit pour de la synchronisation [7]. En revanche, en aucun cas dans ces travaux, il n'est question de sécurité. Les autres travaux en lien avec l'utilisation de RFID pour les drones consistent à faire l'inventaire de marchandises avec un drone embarquant un lecteur [8] ou à injecter des RFID sous la peau de personnes à l'aide de cyber insectes [9] ce qui est loin de nos préoccupations.

2) sur la sécurité des RFID actifs

Actuellement, les seuls produits basés sur les RFID ayant été évalués en considérant un potentiel d'attaque élevé et certifiés par des organismes nationaux tels que l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) sont les puces intégrées dans les passeports « dit biométriques ». Mais il s'agit là de solutions à base de RFID passifs et ils ne peuvent convenir à nos besoins du fait de distance de communication plus que limitée (une dizaine de centimètres). De plus, les solutions utilisant les RFID passifs, en particulier dans le domaine du contrôle d'accès, sont sujettes à des attaques mises en œuvre par les équipes de Radboud Universiteit Nijmegen [10-16], du Royal Holloway University of London [17-20], de Ruhr-Universität Bochum [21-24] et de University College London [25,26] remettant en cause les choix de conception des industriels (sécurité par l'obscurité, algorithmes propriétaires, etc.).

S'il existe bien des RFID actifs, les premières études sur leur sécurité [27] semblent montrer quelques vulnérabilités. Toutefois, il faut prendre en compte que les RFID actifs étudiés dans [28] sont forcément vulnérables puisque pas conçus pour résister à un potentiel d'attaque si élevé. **Beaucoup de travail restant à faire dans ce domaine, j'ai proposé un sujet de thèse sur la sécurité des RFID actifs pour une doctorante que je coencadre et qui débute à l'Université Mouloud Mammeri de Tizi-Ouzou.**

Impact potentiel de cette thématique de mon projet

Il ressort de ces deux états de l'art que peu de laboratoires s'intéressent à la sécurisation des éléments d'identification mis en jeu dans les processus d'authentification dans le contexte des flottes de drones. Il s'agit donc d'un sujet original pouvant avoir un impact intéressant pour la défense nationale française dans le cadre du développement de ses propres drones.

Il ressort également que face aux enjeux financiers liés aux récentes attaques contre RFID passifs déployés presque partout dans le monde et aux coûts de remplacement de ces systèmes, la sécurité physique et logique des RFID passifs mais aussi actifs va être un sujet majeur auquel les laboratoires français doivent s'intéresser.

Ce projet peut contribuer à adresser pour partie le défi 7 de l'« Agenda stratégique France Europe 2020 » [29], les axes 3 et 4 du rapport « Défense et sécurité des systèmes d'information - Stratégie de la France » [30] ainsi que divers aspects du « Livre blanc sur la défense et la sécurité nationale » [31].

Organisation de cette thématique

Cette thématique comprend plusieurs volets complémentaires :

- 1) L'intégration d'une couche de sécurisation des éléments d'identité en utilisant des RFID actifs dans une flotte de drones. Bien évidemment, il ne s'agit pas simplement de reproduire le système IFF (Identification, Friend or Foe) existant depuis la seconde guerre dans l'aviation militaire et civile ou des solutions plus récentes comme l'Automatic Dependent Surveillance-Broadcast (ADS-B – système dont la sécurité est fortement discutable) mais de disposer d'une plate-forme d'identification sécurisée permettant de mettre en œuvre les mécanismes de sécurité nécessaires à la protection des échanges et des données. Idéalement, de par les collaborations existantes, nous étudierons aussi l'impact des solutions proposées sur les aspects algorithmiques des missions mises en œuvre au LaBRI dans les essais de drones (au sens large : robots terrestres et aériens).
- 2) En parallèle du renforcement des compétences sur les RFID passifs développées au sein du projet SoRFID (Security of RFID) de la fédération MIREs que j'ai piloté et dans lequel des enseignants-chercheurs du DMI (Département Mathématiques et Informatique) ont collaboré avec ceux des départements OSA (Ondes et Systèmes Associés) et C2S2 (Circuits Signaux et Systèmes Hautes Fréquences), les travaux consisteront avant tout à développer un système RFID actif sécurisé sur la base de notre bonne connaissance du monde de la carte à puce. Il sera envisager la conception et la mise en œuvre de nouveaux protocoles cryptographiques low-cost basés sur les codes.

Enfin, comme je pensais que les flottes de drones pourraient être un contexte applicatif idéal aux travaux que mènent des collègues de DMI et C2S2 sur le « network coding with rank metric », j'ai déposé, en décembre 2014, avec eux, une équipe de Thales et une équipe du LaBRI un projet sur l'utilisation du network coding dans ce contexte en réponse à un appel interne de Thales. Une collaboration avec l'équipe émergente Mécatronique du laboratoire XLIM est également envisageable sachant qu'ils utilisent aussi des drones dans leur recherche.

Si, j'ai décidé de développer ci-dessus, une thématique particulière de mon projet, j'entends tout de même continuer à travailler sur les cartes multi-applicatives ouverte et les mécanismes de sécurité et infrastructures nécessaires pour favoriser leur déploiement. En effet, ces cartes trouvent leur place dans les systèmes RFID actifs envisagés.

Il est également à noter que nous sommes actuellement en cours de redéfinition du périmètre des équipes au sein du laboratoire XLIM pour le prochain contrat (2018) et que dans ce contexte **je viens de définir un projet intitulé « Sécurité des Systèmes et Réseaux » qui regroupera 3 maîtres de conférences dans la future équipe CRYPTIS.**

Bibliographie

- [0] R. N. Akram, P.-F. Bonnefoi, S. Chaumette, K. Markantonakis, D. Sauveron.
Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements - A Position Paper.
2nd AETOS international conference on "Research challenges for future RPAS/UAV systems". Bordeaux, France, 9-10 September, 2014
- [1] Adrian N. Phillips.
A Secure Group Communication Architecture for a Swarm of Autonomous Unmanned Aerial Vehicles
Air Force Institute of Technology., 2008 - 128 pages
- [2] Sbeiti, M., Wolff, A., Wietfeld, C.
PASER: Position Aware Secure and Efficient Route Discovery for Wireless Mesh Networks
International Conference on Emerging Security Information, Systems and Technologies - SECURWARE, Nice/Saint Laurent du Var, France, Aug 2011.
- [3] J Kong, H Luo, K Xu, D.L Gu, M Gerla, S Lu
Adaptive security for multilayer ad-hoc networks
Wireless Communications and Mobile Computing, 2 (5) (2002), pp. 533–547
- [4] Serge Chaumette, Rémi Laplace, Christophe Mazel, Aurélien Godin.
Secure cooperative ad hoc applications within UAV fleets -- Position paper
28th IEEE Military Communications Conference (MILCOM 2009), Oct 2009, Boston, United States. Proceedings of The 28th IEEE Military Communications Conference (MILCOM 2009), pp. 1-7
- [5] S. Chaumette, R. Laplace.
Embedding Java Cards to secure communications and manage identities in a UAVnet (network of drones)
In Proceedings of e-Smart'11, Sophia-Antopolis, Nice - France, 2011
- [6] Tanel Tammet, Jüri Vain, Andres Puusepp, Enar Reilent, Alar Kuusik
RFID-based Communications for a Self-Organising Robot Swarm
Second IEEE International Conference on Self-Adaptive and Self-Organizing Systems, SASO 2008, 20-24 October 2008, Venice, Italy; 01/2008
- [7] Giulio Zecca, Paul Couderc, Michel Banâtre, Roberto Beraldi
Swarm robot synchronization using RFID tags
International Journal of Intelligent Computing and Cybernetics 2, 4 (2009) 846-849
- [8] <http://marblar.com/idea/kWpA7>
- [9] <http://www.networkworld.com/community/blog/future-drone-surveillance-swarms-cyborg-insect-drones>

- [10] Roel Verdult, Flavio D. Garcia and Josep Balasch.
Gone in 360 Seconds: Hijacking with Hitag2
In 21st USENIX Security Symposium (USENIX Security 2012).
USENIX Association, pages 237-252, 2012.
- [11] Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult and Milosch Meriac.
Dismantling iClass and iClass Elite
In S. Foresti and M. Yung , editors,
17th European Symposium on Research in Computer Security (ESORICS 2012).
Lecture Notes in Computer Science, Vol. 7459, 2012. Springer Verlag.
- [12] Flavio D. Garcia, Gerhard de Koning Gans and Roel Verdult.
Exposing iClass Key Diversification. (Best Paper Award)
In 5th USENIX Workshop on Offensive Technologies (WOOT 2011)
USENIX Association, pages 128-136. 2011.
- [13] Flavio D. Garcia, Peter van Rossum, Roel Verdult and Ronny Wichers Schreur.
Dismantling SecureMemory, CryptoMemory and CryptoRF
In 17th ACM Conference on Computer and Communications Security (CCS 2010).
ACM Press, pages 250-259. 2010. ACM.
- [14] Flavio D. Garcia, Peter van Rossum, Roel Verdult and Ronny Wichers Schreur.
Wirelessly Pickpocketing a Mifare Classic Card. (Outstanding Paper Award)
In 30th IEEE Symposium on Security and Privacy (S&P 2009), pages 3-15. 2009. IEEE.
- [15] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur and Bart Jacobs.
Dismantling MIFARE Classic
In S. Jajodia, and J. Lopez, editors,
13th European Symposium on Research in Computer Security (ESORICS 2008).
Lecture Notes in Computer Science, Vol. 5283, pages 97-114, 2008. Springer Verlag.
- [16] Gerhard de Koning Gans, Jaap-Henk Hoepman and Flavio D. Garcia.
A Practical Attack on the MIFARE Classic
In G. Grimaud and F.-X. Standaert, editors,
8th Smart Card Research and Advanced Application Conference (CARDIS 2008).
Lecture Notes in Computer Science, Vol. 5189, pages 267-282, 2008. Springer Verlag.
- [17] G. P. Hancke.
Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens
Journal of Computer Security. Vol 19, Issue 2, pp. 259-288, March 2011.
- [18] G.P. Hancke, K.E. Mayes and K.Markantonakis.
Confidence in Smart Token Proximity: Relay Attacks Revisited
Elsevier Computers & Security, Vol. 28, Issue 7, pp 615-627. October 2009.
- [19] G.P. Hancke.
Eavesdropping Attacks on High-Frequency RFID Tokens
Presented the 4th Workshop on RFID Security (RFIDSec), July 2008.
- [20] G.P. Hancke
Practical Attacks on Proximity Identification Systems (Short Paper)
Proceedings of IEEE Symposium on Security and Privacy, pp 328-333, May 2006.
- [21] Timo Kasper, Ingo von Maurich, David Oswald, Christof Paar
Cloning Cryptographic RFID Cards for 25\$
Presented at the 5th Benelux Workshop on Information and System Security, WisSec 2010, November 29-30, 2010, Nijmegen, the Netherlands.
- [22] Timo Kasper, Ingo von Maurich, David Oswald, Christof Paar
Chameleon: A Versatile Emulator for Contactless Smartcards
13th International Conference on Information Security and Cryptology - ICISC 2010, Seoul, Korea, December 1-3, 2010, volume 6829 of LNCS, pages 189-206, Springer.
- [23] Timo Kasper, Michael Silbermann, Christof Paar
All You Can Eat or Breaking a Real-World Contactless Payment System
Financial Cryptography and Data Security, 10 January 25-28, 2010, Springer LNCS.
- [24] Markus Kasper, Timo Kasper, Amir Moradi, Christof Paar
Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed
2nd International Conference on Cryptology in Africa, Progress in Cryptology - AFRICACRYPT 2009, Gammarth, Tunisia, 21-25 Juni, 2009.
- [25] Nicolas T. Courtois, Sean O'Neil and Jean-Jacques Quisquater.
Practical Algebraic Attacks on the Hitag2 Stream Cipher in RFID Transponders
In eSmart 2009, European Smart Card Security Conference, 22-25 September 2009, Sophia Antipolis, French Riviera
- [26] Nicolas T. Courtois
The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime
SECRYPT 2009 - International Conference on Security and Cryptography: 7-10 July 2009, Milan, Italy
- [27] Timo Kasper, David Oswald, Christof Paar
Wireless security threats: Eavesdropping and detecting of active RFIDs and remote controls in the wild
19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2011

[28] Jae Hoon Park, HoonJae Lee, ManKi Ahn
Side-Channel Attacks against ARIA on Active RFID Device
Convergence Information Technology, International Conference 2007

[29] Ministère de l'Enseignement Supérieur et de la Recherche
Agenda stratégique France Europe 2020
2013
http://cache.media.enseignementsup-recherche.gouv.fr/file/France-Europe_2020/21/7/AgendaStrategique_252217.pdf

[30] Agence Nationale de la Sécurité des Systèmes d'Information
Défense et sécurité des systèmes d'information - Stratégie de la France
2011
http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

[31] Ministère de la Défense / SGA / SPAC
Livre blanc sur la défense et la sécurité nationale
2013
http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf

Charges collectives

Responsabilités locales

- **Membre du CTP (Comité Technique Paritaire) puis du CT (Comité Technique) de l'Université de Limoges depuis juillet 2009**
J'ai participé à différents groupes de travail issus de ces comités (« Action Sociale », « réorganisation de la recherche », etc.). Je suis inscrit sur d'autres groupes de travail qui ne se sont pour l'instant pas réunis : « Parité », « Évolution du métier d'enseignant-chercheur ». **J'ai décidé de ne pas me représenter en position éligible aux dernières élections professionnelles (4/12/2014). Je ne siégerai donc plus.**
- **Membre du CHS (Comité Hygiène et Sécurité) puis du CHSCT (Comité Hygiène et Sécurité – Conditions de Travail) de l'Université de Limoges depuis 2011.** Je pense là aussi ne plus siéger et laisser la place à d'autres collègues désignés par mon organisation syndicale afin que les responsabilités tournent et que tout le monde se forme sur ce sujet ô combien important.
- **Membre du bureau du Snesup Limousin depuis 2010**
- **Participation aux réunions de « Dialogue Social » entre la présidence de l'Université de Limoges et les organisations syndicales**
- **Forte implication lors des élections universitaires de 2008 et 2012**

Responsabilités nationales

- **Membre titulaire élu de la section 27 du Conseil National des Universités (mandature 2012-2015)**
- **Pilotage pour la section 27 du CNU du groupe de réflexion sur les PEDR qui a établi les critères de classification des dossiers.**

Autres activités

- **Activité de conseil, bénévole, auprès d'une société de communication pour l'utilisation de la carte à puce sans contact dans une application innovante. L'application a été utilisée lors de l'organisation d'un workshop de projet européen.**
- **Organisation de la session de qualification de la section 27 du CNU en janvier 2012 à Limoges.**

Descriptions et avis de responsables Recommandations

Philippe Gaborit
Professeur en Informatique
Directeur du Département Informatique
Université de Limoges

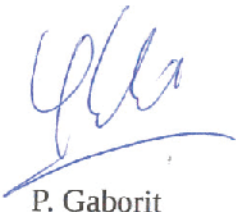
Limoges le 14/12/2014

**Lettre d'attestation et d'appréciation
pour l'enseignement de M. Damien Sauveron**

Je suis responsable du département d'informatique de l'université de Limoges depuis 2009. J'atteste par la présente lettre depuis 2009 M. Damien Sauveron a bien donné les cours décrits dans son dossier. Je n'ai que des bons retours de la part des étudiants à son sujet, il est un enseignant apprécié, sérieux et compétent dans son travail. En particulier, il s'est fortement impliqué dans la pédagogie en étant co-directeur du portail Sciences et Ingénierie en plus d'assurer la création de nouveaux cours.

L'équipe pédagogique du département a toujours pu compter sur lui pour assurer de nombreuses heures complémentaires (en raison du déficit d'encadrement du département informatique – l'équivalent de 10 postes de permanent) ou quand il a fallu l'an dernier prendre un groupe de L1 supplémentaire ou même encore quand cette année il a accepté d'assurer les cours laissés vacants en M2 par un collègue qui nous a informé de son départ en détachement à quelques jours de la rentrée.

Cordialement



P. Gaborit

Philippe Gaborit
Professeur en Informatique
Université de Limoges
gaborit@unilim.fr

Limoges le 14/12/2014

Lettre de soutien à la qualification aux fonctions de Professeur

par P. Gaborit (PR en Informatique), chargé de suivi de M. Damien SAUVERON pour l'HDR

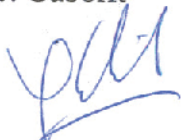
Par la présente, en qualité de chargé de suivi (garant), je soutiens la demande de qualification aux fonctions de Professeur de Monsieur Damien SAUVERON. Damien SAUVERON a soutenu avec succès son HDR le 6 décembre 2014 et il a su répondre avec aisance aux différentes questions.

Il a 4 articles de revues internationales et 19 papiers en conférences internationales, il a récemment obtenu une publication dans une conférence de rang A (*TrustCom*) et a un papier en cours d'acceptation (minor revision) dans la très bonne revue internationale *Information Sciences*, il a de plus plusieurs autres articles de revue en cours de soumission. Ses résultats récents montrent sa capacité à mener une recherche originale et cohérente de bonne qualité en parallèle d'une forte implication dans la communauté universitaire (CNU, CS, CT, CHSCT, Conseil du laboratoire XLIM, etc.). Si depuis son recrutement en 2006, Damien SAUVERON n'a pas eu l'opportunité de pouvoir co-encadrer de doctorant, il a toujours enseigné en Master 2 à Limoges ainsi que dans d'autres établissements (Bordeaux et Clermont-Ferrand) tout en encadrant régulièrement des stages de master 1 et 2. Il a également participé aux pilotages d'activités de recherches internationales comme la création de conférences et le pilotage d'un groupe de travail international sur la sécurité des systèmes pervasifs. En reconnaissance de ces dernières activités, l'assemblée générale de l'« International Federation for Information Processing » (IFIP) lui a attribué le IFIP Silver Core Award fin 2013. En 2014, Damien a su mettre à profit son CRCT en faisant preuve de mobilité géographique et thématiques vers des domaines tels que les RFIDs et la sécurité des flottes de drones. Ces domaines d'applications pourraient se révéler d'intérêt dans le cadre de collaborations transverses au laboratoire XLIM, voire internationales. Depuis la soutenance de son HDR, il a pu établir un coencadrement avec l'Université de Tizi-Ouzou sur la sécurité des RFID actifs (qu'il entend utiliser dans les flottes de drones) et il a déposé, en partenariat avec des équipes du LaBRI et de Thales, un projet de recherche que je pense prometteur sur l'utilisation du codage réseau dans les flottes de drones.

Sur la base de ces éléments, et même si par certains aspects le dossier peut sembler un peu jeune notamment sur l'aspect purement revues internationales, je pense que dans son ensemble, et notamment en raison de l'aspect investissement dans les comités de conférences internationales, et aussi pour son investissement dans l'enseignement, le dossier de M. Damien SAUVERON est tout à fait satisfaisant, et donc je soutiens son dossier pour la demande de qualification aux fonctions de Professeur.

Cordialement,

P. Gaborit





*College of Engineering
Department of Electrical Engineering*

Nov. 12th, 2014

Damien Sauveron
D'épartement Mathématiques Informatique,
Limoges, France

Dear Dr. Sauveron,

It is my pleasure to meet you in person during the AETOS conference that was held during September 9-10, 2014 in Bordeaux. I enjoyed listening to your presentation titled "Improving Security of Autonomous UAV fleets by using New Specific Embedded Secure Elements". I also read the paper as well with great interest.

You have highlighted the requirements for securing UAVs in the face of attacks from a strong adversary. You presented an accurate threat model and analyzed the threat model diligently to come up with the functional requirements and security requirements.

As a researcher with background in information security and working with UAVs, I enjoyed listening to your ideas. I believe that you captured the security requirements very accurately.

Obviously, there is lot of work to be done in this emerging area of research. I will be very happy to collaborate with you. I believe your project is very well planned and our collaboration will lead to fruitful outcomes.

I wish you the best in your research pursuits.

Sincerely

Kamesh Namuduri

Kamesh Namuduri
Associate Professor
940-369-8960

Prof. Dr. Joachim Posegga

Chair of IT-Security



Universität Passau · 94030 Passau

To whom it may concern

Phone	+49 851 509-3211 (Secretary)
Telefax	+49 851 509-3212
E-Mail	itsec-office@uni-passau.de
Sign	JP/re
Date	13.11.2014

Dear Sir or Madam,

I have known Dr. Damien Sauveron for many years, and have always been impressed by his scientific work and his engagement in the scientific community.

Dr. Sauveron visited my research group, the Chair of IT-Security within the Faculty of Mathematics and Informatics, in July 2014. We took this opportunity and continued our fruitful cooperation and decided to initiate work in the area of IT-Security, in particular smart devices and the Internet of Things. The research proposal that he proposes to secure fleets of Unmanned Vehicles with active RFIDs is a very interesting use case for us. Indeed, in the FP7 project RERUM (REliable, Resilient and secUre IoT for sMart city applications), which is currently running, my team is developing an architectural framework for the interconnectivity of a large number of heterogeneous smart objects based on the concept of "security, privacy and reliability by design" that could be used in this context. There are also strong links to the FP7 project COMPOSE, and a nationally funded project within the Bavarian FORSEC research network.

In addition, we have discussed security issues in airborne communication and systems during his visit, and we are interested in this topic on which members of my team are working.

I strongly support his proposal which also shares other exciting aspects like embedding security and reliability on hardware smart objects (here active RFIDs), providing reliable, self-managed, robust and context-aware communications minimizing energy consumption.

Yours sincerely,

Prof. Dr. Joachim Posegga

TELECOM SudParis
Département RST
Prof. Maryline LAURENT
9, rue Charles Fourier
91 011 Evry Cedex
Tél : 01 60 76 44 42

Evry, LE 17 décembre 2014

Objet : Lettre de recommandation de Mr Damien SAUVERON en vue des qualifications aux fonctions de professeur

Madame, Monsieur,

J'ai participé à la soutenance de HDR de Damien Sauveron le 6 décembre 2014. Elle portait sur la sécurité et les interactions des « smart secure devices » et des « réseaux mobiles ».

Au travers de sa présentation, de son mémoire et des discussions attenantes, j'ai pu apprécier les qualités de Mr Sauveron, en particulier son grand dynamisme, sa capacité d'animateur scientifique et l'originalité de ses idées (le modèle UCOM, l'application du network coding aux flottes de drones). Au-delà de ses contributions scientifiques, il a démontré au cours de ces dernières années d'excellentes capacités à fédérer la recherche et à initier et conduire des collaborations scientifiques nationales et internationales. Soulignons par exemple sa forte implication dans le groupe de travail IFIP 11.2 « Pervasive Systems Security », ce qui l'a amené à en devenir le président en 2014. Il est aussi le fondateur du workshop WISTP en 2007 qui connaît actuellement un vif succès et prendra le statut de conférence en 2015. Il est éditeur invité de numéros spéciaux dans des journaux de bon, voire d'excellent niveau, comme « Journal of Computer Networks ».

Pour toutes ces raisons, je soutiens la candidature de Dr Damien Sauveron à la qualification aux fonctions de professeur.

A faire valoir ce que de droit,



9 rue Charles Fourier
91011 Evry Cedex
France

Maryline LAURENT

Professeur à l'Institut Mines-Télécom, Télécom SudParis

Responsable de l'équipe R3S du laboratoire CNRS UMR5157 SAMOVAR

Tél : + 33 (0)1 60 76 44 40

Fax : + 33 (0)1 60 76 43 37

Siret : 180 092 025 00048

APE : 8542Z

www.telecom-sudparis.eu