INSA DE TOULOUSE	Référence GALAXIE : 4066

Numéro dans le SI local :	0053
Référence GESUP :	0053
Corps :	Maître de conférences
Article :	26-I-1
Chaire :	Non
Section 1 :	27-Informatique
Section 2 :	
Section 3 :	
Profil :	Sécurité de systèmes informatiques Cyber Security
Job profile :	Cyber-Security, low level layers security, vulnerabilities in the system low level layers and micro-architectures, hardware based security solutions and components, security architectures and trusted execution environments.
Research fields EURAXESS :	Computer science Other
Implantation du poste :	0310152X - INSA DE TOULOUSE
Localisation :	135 avenue de Rangueil
Code postal de la localisation :	31400
Etat du poste :	Vacant
Adresse d'envoi du dossier :	Voir ci-dessous application 31077 - TOULOUSE CEDEX 4
Contact administratif : **N° de téléphone :** **N° de Fax :** **Email :**	SYLVIE REBOUL RESPONSABLE GESTION PERSONNELS ENSEIGN. 0561559519 0561559517 0561559500 sylvie.reboul@insa-toulouse.fr
Date de prise de fonction :	01/09/2018
Mots-clés :	sécurité ; informatique ;
Profil enseignement : **Composante ou UFR :** **Référence UFR :**	 Departement de Genie Electrique et Informatique GEI
Profil recherche :	
Laboratoire 1 :	UPR8001 (199517454Y) - Laboratoire d'analyse et d'architecture des systèmes du CNRS
Dossier Papier	NON
Dossier numérique physique (CD, DVD, clé USB)	NON
Dossier transmis par courrier électronique	NON e-mail gestionnaire
Application spécifique	OUI URL application https://recrutement-ec.insa-toulouse.fr

Poste ouvert également aux personnes 'Bénéficiaires de l'Obligation d'Emploi' mentionnées à l'article 27 de la loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique de l'Etat (situations de handicap).

Le poste sur lequel vous candidatez est susceptible d'être situé dans une "zone à régime restrictif" au sens de l'article R.413-5-1 du code pénal. Si tel est le cas, votre nomination et/ou votre affectation ne pourront intervenir qu'après autorisation d'accès délivrée par le chef d'établissement, conformément aux dispositions de l'article 20-4 du décret n°84-431 du 6 juin 1984.

Le profil détaillé se trouve en page 2 et suivantes

INSA TOULOUSE : FICHE DE POSTE 2018

Composante : Département de **Génie Electrique et Informatique**

Numéro de poste : MCF 0053 / GALAXIE 4066

Section CNU : 27ème section

Date de Nomination prévue : **1er septembre 2018**

Attention : le poste sur lequel vous candidatez est susceptible d'être situé dans une «zone à régime restrictif » au sens de l'article R. 413-5-1 du code pénal. Si tel est le cas, votre nomination et/ou votre affectation ne pourront intervenir qu'après autorisation d'accès délivrée par le chef d'établissement, conformément aux dispositions de l'article 20-4 du décret 84-431 du 6 juin 1984.

PROFIL : Sécurité de systèmes informatiques – Cyber-Security

Profil enseignement

Filières de formation concernées :
Informatique – Réseaux et Automatique-Electronique

Objectifs pédagogiques :
Le département Génie Electrique et Informatique (DGEI) de l'INSA de Toulouse souhaite recruter un(e) maître de conférences dans le domaine de la sécurité des systèmes informatiques. Les compétences souhaitées dans ce domaine sont plus particulièrement relatives à la sécurité des couches basses des systèmes, à l'interface entre le logiciel et le matériel (système d'exploitation, firmware, micro-architecture). Elles concernent notamment :
- les vulnérabilités dans les couches basses et la micro-architecture
- les composants et solutions pour la sécurité, assistés par le matériel
- les architectures de sécurité et les environnements d'exécution de confiance

Ces compétences pourront être mises à profit dans différents grands domaines d'applications tels que l'Internet des Objets, les systèmes embarqués critiques ou le Cloud Computing, domaines sur lesquels le Département de Génie Electrique et Informatique se positionne aujourd'hui.

La personne recrutée viendra renforcer l'équipe pédagogique de la thématique sécurité. Elle sera amenée à intervenir dans la spécialité Informatique-Réseaux (IR) du DGEI (années 4 et 5) et en particulier dans les masters Toulouse Sécurité (TLS-SEC) et Innovative Smart Systems (ISS). Elle pourra également intervenir dans la spécialité Automatique-Electronique (AE) du DGEI.

La personne recrutée interviendra également au niveau licence (années 1, 2 et 3), dans le département Sciences et Technologies pour l'Ingénieur (STPI). Elle pourra notamment compléter les équipes pédagogiques relatives à l'architecture des ordinateurs, les systèmes d'exploitation, l'algorithmique et la programmation.
Elle pourra être amenée à dispenser une partie de ces enseignements en anglais et pourra aussi être sollicitée pour mettre en place des cours en ligne de type MOOC /SPOC et pour dispenser des cours de formation continue.

Profil recherche

Laboratoire d'accueil : LAAS-CNRS

Type (UMR, EA, JE, ERT) et N°	Nombre d'enseignants-chercheurs	Nombre de chercheurs
UPR	115	89

Equipe de recherche prévue : TSF- Tolérance aux fautes et Sûreté de fonctionnement informatique

L'évolution des technologies informatiques (architecture des processeurs, virtualisation des systèmes d'exploitation et des réseaux, technologies logicielles, etc.) va de pair avec une sophistication des attaques et des vulnérabilités. En particulier, l'émergence d'attaques de bas niveau, à l'interface entre le matériel et le logiciel, est un exemple de nouvelles techniques d'attaque qui commencent à proliférer. On peut citer les attaques par les contrôleurs d'entrée-sortie qui ne font pas intervenir directement le processeur principal qui exécute l'OS et les programmes d'application, ce qui rend leur détection par des logiciels (du type anti-virus ou autre) très difficile, voire impossible pour certaines d'entre elles. Les fuites d'informations par canaux cachés ou par canaux auxiliaires, par exemple via les mémoires caches, se sont aussi beaucoup développées et ont évolué avec les évolutions des architectures matérielles.
En comparaison aux attaques liées au logiciel, la connaissance actuelle des vecteurs d'attaques susceptibles d'exploiter des vulnérabilités liées aux composants matériels et à la micro-architecture des systèmes reste très limitée. Il convient donc de développer des techniques d'analyse de vulnérabilités et des moyens de protection efficaces pour prévenir, détecter ou tolérer ce type d'attaques, en prenant en compte les contraintes liées aux nouveaux contextes d'usage et les technologies associées. Le développement d'approches de protection multi-niveaux, allant des couches basses jusqu'aux applications, constitue également un défi majeur pour apporter une meilleure résilience vis-à-vis à la fois des attaques matérielles et logicielles.
Le LAAS a une expertise reconnue dans le domaine de la conception et de l'évaluation de nouveaux mécanismes pour la sécurité informatique. Les recherches couvrent un spectre allant des composants matériels jusqu'aux applications dans des domaines divers (applications web, systèmes embarqués critiques, hyperviseurs de sécurité assistés par le matériel, objets connectés, etc.). Les travaux récents se sont orientés en particulier vers l'analyse de vulnérabilités à l'interface entre le logiciel et le matériel et à la conception de plateformes sécurisées protégeant contre ce type d'attaques. Ces recherches ont besoin d'être renforcées, notamment pour élargir la surface d'attaques étudiées liées à la microarchitecture matérielle.

Discipline émergente : Sécurité de systèmes informatiques

Job profile :
Electrical Engineering and Computer Science Department opens an Associate Professor position in the field of **Cyber-Security** and more specifically oriented around **low level layers security**, at the interface between software and hardware (operating systems, firmware, micro-architecture). The main teaching domains concern:

- **the vulnerabilities in the system low level layers and micro-architectures**;
- **hardware based security** solutions and components;
- the **security architectures and trusted execution environments**.

All these knowledges / teachings will be applied to Internet of Things, Critical Embedded Systems or Cloud Computing, highly competitive fields in which the Electrical Engineering and Computer Science Department is a leader today.

The Associate Professor will join the pedagogical team on cyber-security. He/she will teach in the Computer Science and Networking Diploma at the master level (4th and 5th year at INSA Toulouse), in the Toulouse Security Master (TLS-SEC) and Innovative Smart Systems (ISS) Master. He/she will also give some teachings in Control and Electronics Diploma in our Department.

The Associate Professor will also teach at bachelor level (1st, 2nd and 3rd year). He/she will join the pedagogical teams on computer architecture, operating systems, algorithms and programming.
The future Associate Professor will be asked to teach some classes in English. He/she can be asked to set-up new online classes like MOOC /SPOC and participate to ongoing professional education. He/she will be also asked to participate to the administrative tasks, as all the other colleagues in the department.

Research Fields :

The evolution of computer technologies (processor architecture, virtualization of operating systems and networks, software technologies, etc.) have also lead to the emergence of more sophisticated attacks and vulnerabilities. A particular example is the proliferation of **low-level attacks** at the **interface between hardware and software**. We can mention for instance I/O attacks that bypass the main processor hosting the OS and application programs. This stealthiness makes their detection by traditional software techniques (anti-virus or other type) very difficult, if not impossible for some of them. Another example is **Information leakage attacks by side channels or by covert channels**, for example via the memory cache that have also increased recently and evolved along with the hardware microarchitecture evolutions.

Compared to software-related attacks, the current knowledge of attack vectors that can exploit vulnerabilities related to hardware components and system microarchitecture remains very limited. Therefore, it is necessary to design efficient vulnerability analysis techniques and protection mechanisms to prevent, detect or tolerate such attacks, taking into account the constraints related to new usage scenarios of information systems and related technologies. The development of **multi-level protection approaches**, ranging from low-level layers to applications, is also a major challenge for providing better resilience to both hardware and software attacks.

LAAS has a recognized expertise in the field of **designing and evaluating new mechanisms for computer security**. Research activities cover a wide area from hardware components to applications in various application areas (connected objects, critical embedded systems, hardware-assisted security hypervisors, web applications, etc.). Recent work focus mainly on the **analysis of vulnerabilities at the interface between software and hardware** and the **design of secure platforms** protecting against this new type of attack. These researches need to be strengthened, especially to be able to cover the new types of attacks related to the microarchitecture.

Autres activités

La personne recrutée sera sollicitée comme tous les autres enseignants-chercheurs pour assumer des responsabilités collectives et/ou administratives (par exemple : responsabilité d'une unité d'enseignement, d'une année d'étude, etc.), participer aux salons/forums de promotion de nos formations, aux jurys de recrutement d'étudiants et autres activités du département.

Contacts :

Enseignement : Prof. Daniela Dragomirescu, Directrice du Département de Génie Electrique et Informatique
daniela.dragomirescu@insa-toulouse.fr gei-secretariat-direction@insa-toulouse.fr Tel : 05 61 55 98 11

Recherche : Pierre Lopez, Directeur-adjoint du LAAS-CNRS pierre.lopez@laas.fr Tel : 05 61 33 62 98

IMPORTANT

Lorsque vous aurez enregistré votre candidature dans **GALAXIE**, vous recevrez dans la soirée ou le lendemain sur votre boîte mail un identifiant et un mot de passe qui vous permettront de déposer votre dossier dans l'application spécifique prévue à cet effet : https://recrutement-ec.insa-toulouse.fr

Le guide du candidat relatif à cette application est disponible sur le site web de l'INSA à l'adresse suivante : http://www.insa-toulouse.fr/fr/personnel/enseignant.html à la rubrique : Recrutement des enseignants-chercheurs pour 2018-2019

Date limite de dépôt des dossiers : Jeudi 29 mars 2018 à minuit

Pièces justificatives à fournir :

Consulter l'arrêté du 13 février 2015 relatif aux modalités générales des opérations de mutation, de détachement et de recrutement par concours des maîtres de conférences.

Tout dossier ou document déposé hors délai
Tout dossier incomplet à la date limite susmentionnée
SERA DECLARE IRRECEVABLE