RECRUTEMENT ENSEIGNANTS-CHERCHEURS
RENTREE 2018

Institut d'ingénierie, Grenoble INP, grand établissement de statut public, ses 6 écoles et sa Prépa intégrée, propose des formations d'ingénieurs avec un contenu scientifique de base solide et une haute spécialisation technologique. L'établissement compte plus de 5 500 étudiants et 1 300 personnels enseignants-chercheurs, enseignants, administratifs et techniques. Ces enseignements sont appuyés sur une recherche de très haut niveau menée au sein des laboratoires communs avec les membres et partenaires de la communauté du site Univ. Grenoble Alpes. Grenoble INP se positionne au cœur des défis technologiques d'avenir (Energie, Société du numérique, Micro nanotechnologie, Industrie du futur). Grenoble INP est reconnu dans les classements nationaux et internationaux, il est membre de réseaux internationaux d'ingénierie et propose plus de 350 programmes d'échanges aux étudiants.

Profil court : **Cybersécurité, réseaux et systèmes répartis**

Corps : **MCF** **N° poste :** **0403**

Discipline : Section 1 : **27**

Localisation : **Saint Martin d'Hères**

Date de recrutement : **01/09/2018**

ENSEIGNEMENT

Ecole de rattachement : **ENSIMAG**

Site web de l'école : **http://ensimag.grenoble-inp.fr/**

Contact de l'école : Christophe Rippert <Christophe.Rippert@grenoble-inp.fr>, Jean-Louis Roch <jean-louis.roch@grenoble-inp.fr>

Profil d'enseignement :

La personne recrutée devra enseigner prioritairement dans les domaines de la cybersécurité au sens large aussi bien en tronc commun qu'en enseignement de spécialité afin de former des ingénieurs pour sécuriser l'exploitation des infrastructures de calcul et de communication : de la prévention à la protection en passant par les protocoles de sécurité, les primitives de chiffrement (cryptologie), leurs implémentations, les analyses de sécurité. Elle devra s'investir dans les enseignements du tronc commun Ensimag (1ere année et environ 75% des filières de la 2ème année) qui constitue le socle de nos élèves ingénieurs, reconnu par nos partenaires

industriels et en recherche, qui leur permet à la fois de se spécialiser et aussi de rester généralistes et adaptables. Elle sera ainsi amenée à s'impliquer dans des enseignements comme en système, réseau et applications réparties (clouds). Elle sera amenée à s'investir dans l'équipe pédagogique cybersécurité et prendre des responsabilités dans le Master Sciences, Technologies, Santé : Télécommunications et Réseaux spécialité Réseaux d'Entreprise, co-habilité par le CNAM et Grenoble INP – Ensimag. En collaboration avec les équipes pédagogiques concernées, elle devra s'impliquer dans le montage d'enseignements par projets et la formation par le Numérique.

RECHERCHE

Laboratoire d'accueil : LIG

Site web du laboratoire : https://www.liglab.fr/

Contact du laboratoire : Eric Gaussier <eric.gaussier@imag.fr>

Profil de recherche :

Equipe d'accueil : CONVECS, CTRL-A, DRAKKAR, ERODS, POLARIS, SPADES, VASCO

La problématique de la sécurité dans le cyberespace devient cruciale au vu des risques, menaces et vulnérabilités liés à notre dépendance aux technologies numériques et systèmes interconnectées. L'ouverture des réseaux à un nombre important d'objets, la dépendance de presque tous les domaines de notre vie de la communication continue et fiable et un nombre grandissant de possibilité des attaques par des maliciels amplifient les problèmes de sécurité et de vulnérabilité. Le développement de l'Internet des Objets (IoT) ajoute encore une nouvelle dimension à ces problèmes. On peut noter la création d'un groupe de travail d'Allistene pour répondre aux différents enjeux relatifs à la cybersécurité – le poste proposé s'insère dans cette démarche.

Les réseaux sont devenus omniprésents et au cœur de la Société Numérique. Ils évoluent en permanence pour offrir des débits de plus en plus élevés et s'adapter aux nouveaux usages. En même temps que la complexité des réseaux s'accroît, il faut qu'ils fonctionnent de manière optimale et fiable, en supportant une large diversité des services pour des utilisateurs de plus plus en plus exigeants. Dans ce contexte de la complexité accrue et de la pénétration de la programmabilité dans les équipements réseau, la problématique de la sécurité de communication et de données devient également importante. Les mesures et l'observation du trafic réseau pourront permettre aux opérateurs de réseau de mieux comprendre les menaces à la cybersécurité et utiliser ces connaissances pour développer de nouveaux moyens pour les atténuer.
Au delà de la couche réseau, il importe de construire des systèmes capables d'exploiter efficacement ces grandes infrastructures distribuées (cloud, fog, IoT, …) sans que la défaillance ou la compromission d'une sous-partie ne remette en cause la fonctionnalité du reste de la plate-forme. Pour cela, il est indispensable de concevoir ces systèmes en s'appuyant sur des paradigmes intrinsèquement tolérants aux pannes, passant naturellement à l'échelle, et capable de contenir des utilisateurs ou des programmes cherchant à s'approprier trop de

ressources. Dans un tel contexte, la capacité à caractériser le comportement des utilisateurs, à comprendre, évaluer et correctement mesurer les performances de chacun des composants ainsi que de l'ensemble de l'infrastructure s'avère essentiel.

Description des axes de recherche associés au poste :

Aspects Cybersécurité :

- méthodes de détection d'anomalies, d'intrusion et d'attaques, sécurité du DNS
- sécurité et la protection de la vie privée des objets connectés IoT
- modèles pour la sécurité IoT
- métriques de réputation
- sécurité appliquée à l'architecture des machines et des systèmes, à la gestion de l'information (protection des données, vie privée), à l'analyse et conception de logiciels sûrs
- automatisation des mécanismes d'auto-protection : gestion dynamique des compromis entre sécurité/vie privée, performances, et utilité des données partagées
- programmation certifiée par assistants de preuve
- méthodes de détection d'anomalies, d'intrusion et d'attaques, sécurité du DNS
- sécurité et la protection de la vie privée des objets connectés IoT
- modèles pour la sécurité IoT
- métriques de réputation
- sécurité appliquée à l'architecture des machines et des systèmes, à la gestion de l'information (protection des données, vie privée), à l'analyse et conception de logiciels sûrs
- automatisation des mécanismes d'auto-protection : gestion dynamique des compromis entre sécurité/vie privée, performances, et utilité des données partagées
- programmation certifiée par assistants de preuve

Aspects Réseaux et Systèmes Répartis :

- conception et développement de protocoles et de mécanismes de communication à contraintes d'énergie pour l'Internet des Objets, protocoles pour des communications avec des objets contraints dans la 5G
- méthodes de mesures, d'analyse et de classification du trafic réseau, méthodes d'analyse du trafic chiffré
- conception et développement de protocoles de transport et d'algorithmes de Contrôle de Congestion et de Qualité de Service
- orchestration, déploiement et reconfiguration de services et d'applications dans des environnement cloud/fog/IoT
- méthodes formelles pour la conception et la programmation des systèmes répartis et applications IoT (calculs de processus, langages flots de données)
- gestion de fautes et analyse causale des dysfonctionnements

ACTIVITES ADMINISTRATIVES

Spécificités du poste ou contraintes particulières :

Cliquez ici pour taper du texte.

Compétences attendues :

Savoir :	Cliquez ici pour taper du texte.
Savoir-faire :	Cliquez ici pour taper du texte.
Savoir-être :	Cliquez ici pour taper du texte.

Mots clés : Cliquez ici pour taper du texte.

Mots clés : https://www.galaxie.enseignementsup-recherche.gouv.fr/ensup/pdf/Mots_cles/mots-cles.pdf