paperJam

Luxembourg (/liste/questions/luxembourg) | Publié aujourd'hui 5:15

Paulo Verissimo (Expert en sécurité informatique)

«Mon programme: plus de sécurité informatique»

Le Fonds national de la recherche a déboursé 5 millions d'euros pour convaincre un expert sécurité informatique de renommée mondiale de quitter l'Université de Lisbonne pour celle du Luxembourg. Trois questions au principal intéressé.

Par : Thierry Iochem / Publié par paperJam.lu
Mis à jour : 19.09.2014 9:27

Grâce à ces cinq millions d'euros, Paulo Verissimo va rassembler une équipe de recherche internationale de top niveau

(Photo: SnT / scienceRelations)

Monsieur Verissimo, bienvenue à Luxembourg. Connaissiez-vous déjà le Grand-Duché? Quand prendrez-vous vos fonctions et où précisément?

«Je suis littéralement fasciné par le Luxembourg à présent que je connais mieux ce pays que j'ai eu l'occasion de visiter à plusieurs reprises dans le cadre de la préparation de ma contribution au Programme «Excellence Award for Research in Luxembourg» (PEARL). Venant du bord de mer et ayant été marin, c'est vraiment un changement radical! Je suis ravi à l'idée d'en apprendre plus sur le pays et ses habitants.

Le 1er septembre, j'ai débuté à mon poste de Professeur affecté à la Faculté des sciences, de la technologie et de la communication à l'Université du Luxembourg, détaché au SnT, le Centre interdisciplinaire pour la sécurité, la fiabilité et la confiance. L'Université de Luxembourg et le SnT étant

des centres de recherche internationaux très réputés, j'ai hâte d'entrer en étroite collaboration avec mes nouveaux collègues.

En tant qu'expert de renommée internationale, quels sont les principaux défis auxquels le Luxembourg doit faire face dans les infrastructures d'information?

«Le Luxembourg est un pays dont le PIB est en grande partie constitué par les industries et services relatifs aux TIC. Dans le même temps, le Luxembourg s'est positionné avec succès comme le 'Data Vault de l'Europe'. Cette stratégie implique un investissement continu dans les complexes et modernes Critical Information Infrastructures (CII), spécialement celles liées au complexe internet/cloud, particulièrement présent dans les services financiers et le e-commerce.

Cependant, à côté des gains potentiels de cette stratégie, des risques plus élevés surviennent. La valeur des actifs contrôlés par ces CII devient redoutable et, en conséquence, susceptible d'attirer des attaques ciblées très sophistiquées ou des menaces récurrentes élaborées, qu'elles proviennent du crime organisé, du cyber-terrorisme, du cyber-hacktivisme, des armées ou agences d'état, qui à leur tour ont besoin de puissantes défenses. Les mesures de sécurité superficielles ne suffisent pas: nous avons besoin de plus de sécurité et de fiabilité, et ce sera l'objet de mon programme.

Dans le cadre de son programme PEARL, le FNR vous a octroyé une bourse de 5 millions d'euros. Quel usage pensez-vous en faire?

«Je vais utiliser la subvention principalement pour établir une équipe de recherche internationale de top niveau et d'une taille critique suffisante pour relever un ensemble de défis scientifiques importants. J'ai décrit ces défis comme des priorités pour s'attaquer au problème de la sécurité des infrastructures de l'information et de la fiabilité, dans le contexte d'une menace mentionnée précédemment. Ma culture est de combiner la solide théorie à la pratique pertinente des systèmes. Par conséquent, il y aura un investissement important dans les équipements destinés à construire des prototypes réalistes permettant de valider la théorie par la pratique.

Sur les cinq prochaines années, le plan se composera de trois phases qui se chevaucheront: recrutement et constitution d'une équipe d'étudiants en doctorat et de chercheurs doctorants, suivi par la montée en puissance des activités, recherche de partenaires, obtention de subventions européennes et enfin l'atteinte d'une visibilité externe, diffusion, organisation d'événements, réseautage. L'ambition étant de devenir l'un des pôles internationaux majeurs de R&D dédiés aux CII, et faire en sorte que ce sujet soit au centre des préoccupations des organisations et entreprises partenaires.»
