Institut Mines-Télécom

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

cyber-cni.fr/

We are hiring!

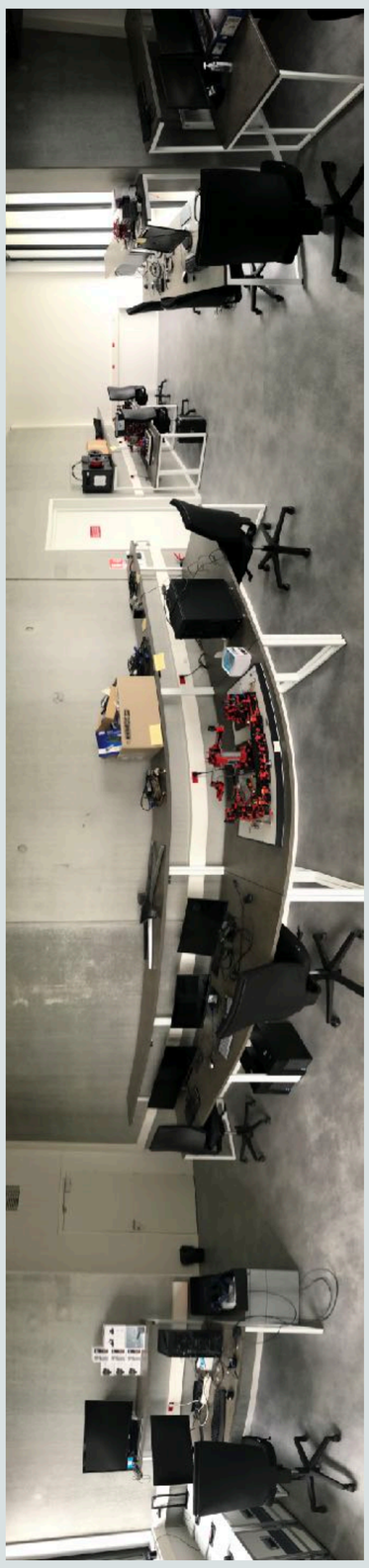
Jeune Docteur (<2ans après doctorat)

(24 months/ full time 35h/w)

IPSec + TLS

We are looking for an outstanding candidate to strengthen our research team. We offer challenging research in a rich environment with excellent research perspectives. This position is to be filled from Oct 15, 2021.

IPSec et TLS sont deux technologies de protection des protocoles réseau.
De manière générale, IPSec sert plus à sécuriser un lien statique entre deux sites, tandis que TLS permet de sécuriser des connexions ad hoc.
Le protocole IPSec travaille sur la couche OSI 4 et est donc typiquement géré par le système d'exploitation avec les privilèges "kernelland".
Quant à TLS, il intervient au niveau de la couche OSI 7, et est donc implémenté en mode "utilisateur".
Pour autant, les deux protocoles s'appuient sur un échange de clés et une authentification des paquets.
Ainsi, une accélération des algorithmes cryptographiques sous-jacents est souhaitable, car autrement, ceux-ci pourraient bien constituer le goulet d'étranglement de la solution en terme de débit.
Ainsi, il est souhaitable de disposer d'une ressource cryptographique à même de pouvoir décharger le processeur applicatif des tâches de calcul d'algorithmes symétriques.
En effet, la cryptographie asymétrique concerne l'établissement de clé, réalisée une fois et qui n'est donc pas critique en temps de calcul.
En revanche, les calculs symétriques opèrent sur la charge utile et doivent donc être réalisés en flux tendu.



Job description

Les missions de ce post-doc sont de définir une interface unique et pratique, qui permette d'aller adresser des accélérateurs de cryptographie symétrique.
Les défis sont les suivants :
- possibilité de cohabitation d'IPSec et de TLS sur une partie hôte, et gestion de la ségrégation des deux protocoles ;
- démonstration de la sécurité des clés : il s'agit de vérifier qu'une même clé ne peut pas être utilisée pour les deux protocoles,
  ni par des traitements de frames différentes sur un protocole donné ;
- gestion de la charge moyenne pour IPSec et TLS.

Les tâches à effectuer sont les suivantes :
- étude des protocoles IPSec et TLS sous l'angle de la cryptographie et identification des synergies envisageables ;
- dimensionnement des performances de blocs de cryptographie symétrique optimisée ;
- analyse de la gestion des priorités (arbitration, "load balancing") pour l'usage concurrent de deux protocoles TLS et IPSec ;
- définition des interfaces et du contrôle d'une architecture matérielle (AES-GCM) convenant à la fois pour TLS et IPSec.

Cette période de post-doc sera propice à la rédaction de publications scientifiques à fort impact, notamment :
- un état de l'art des implémentations matérielles de protocoles cryptographiques tournées vers Internet, et leur compatibilité / interopérabilité (étude des synergies entre couches OSI) ;
- une étude qui démontre formellement l'isolation entre les flots de données indépendents (propriété nécessaire pour des applications traitant de la donnée classifiée) ;
- une comparaison empirique entre les performances des protocoles de sécurité implémentés à différents niveaux ;
- une proposition d'évolution des algorithmes canoniques des ciphersuites vers des algorithmes régionaux (par exemple le remplacement de l'AES par ARIA, CIPHERUNICORN-A, CLEFIA, Hierocrypt-3, SC2000, voire SM4), voire AEAD (Authenticated Encryption with Associated Data, comme https://competitions.cr.yp.to/caesar.html), en faisant effet de levier sur le caractère partiellement reconfigurable des FPGA.

Ce travail permettra à l'étudiant post-doc d'interagir avec les doctorants de la Chaire Cyber CNI, et aussi partager ses résultats avec l'entreprise Secure-IC.

CHAIR OF CYBER CNI
Critical National Infrastructures

Requirements - what you should bring

Recent PhD (<2 years) in a related field, extraordinary research skills. Curiosity and motivation to work in a dynamic research environment.

Languages: French, English (ability to read and write research papers in English)

Application process

Application deadline: 30.9.2021, 3pm CEST

Please send an email with one (1) PDF including:
- a motivational letter (covering the points “requirements”)
- your CV
- your certificates
- a research statement (containing your research methodologies and possible research directions you would be interested to develop including references)
- contact addresses (mail and phone) of 1-3 people we can contact to inquire information about you

to **recruit-secure-ic-2021-3@cybercni.fr**.

Institut Mines-Télécom
IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom
TELECOM Paris
TELECOM SudParis
AIRBUS AMOSSYS BNP PARIBAS La banque d'un monde qui change
EDF NOKIA Bell Labs SNCF PÔLE D'EXCELLENCE CYBER

Your future hosting environment: Excellence in Cybersecurity research and education in France

cyber-cni.fr/

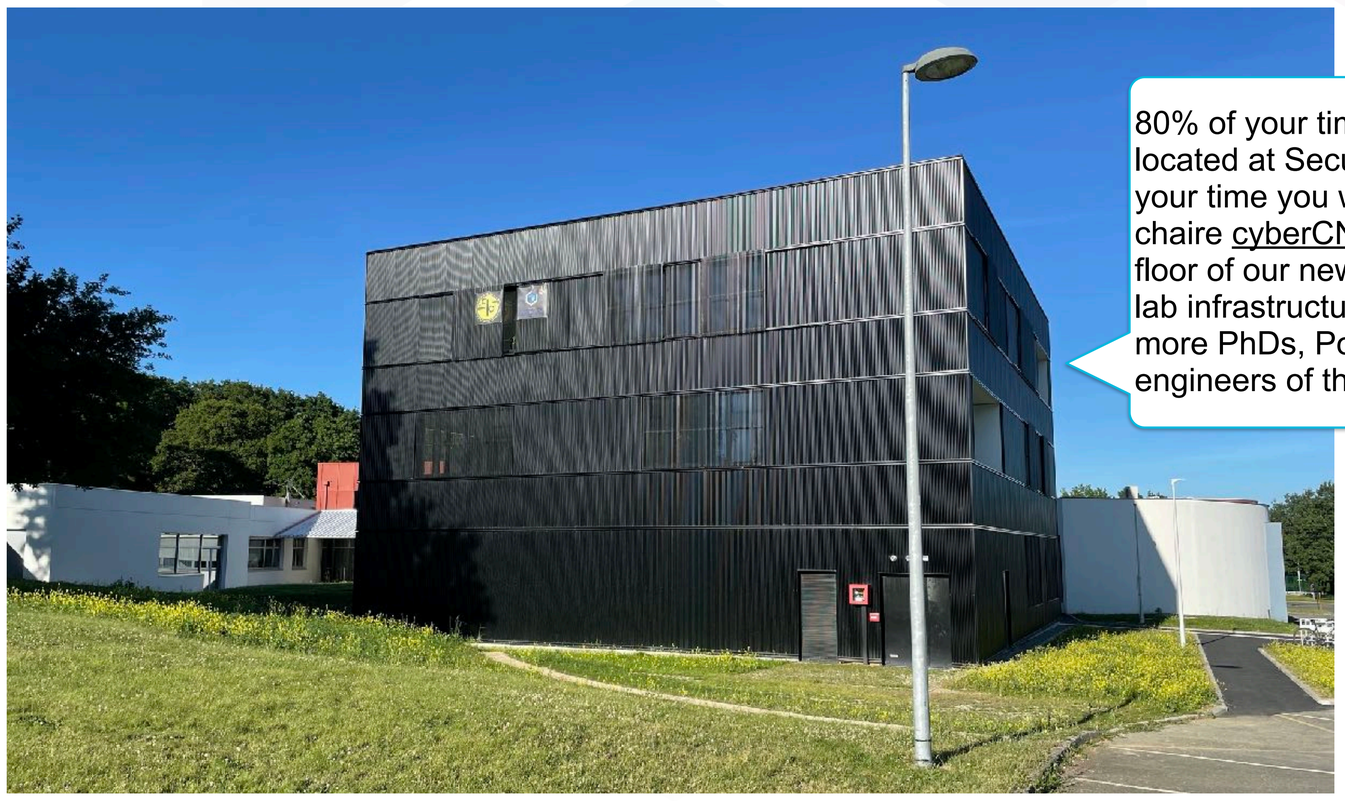
The hosting environment

The offered position is within one of France's finest addresses for research at a chair that is well-known for its excellence in cybersecurity. This offer is together with Secure-IC (https://www.secure-ic.com/), the security science company, where you will spend 80% of your time. 20% of your time you will be at the chair.

The position is located within the IMT's school IMT Atlantique at the Rennes campus within the SRCD department at the chair Cyber CNI. Relocation to Rennes is required.

IMT: The Institut Mines Télécom (IMT) is France's biggest engineering school. It is comparable to an elite university in Germany for instance. IMT is a public institution dedicated to higher education and research for innovation.
It is a key player in the fusion of science, engineering and digital technology, and takes its schools' skills into the major fields of transformation in digital technology, industry, energy and the environment as well as their impact on the industry of the future, cities, health, and autonomy. For more info: https://www.imt.fr/en/imt/presentation-of-imt/

IMT Atlantique: Internationally recognized, IMT Atlantique's research positions it as one of the world's Top 400 Technological Universities. This research, conducted in the fields of digital sciences, engineering sciences, physics and management, fosters the conditions for inter-disciplinary research that is a source of innovation in response to the major challenges facing companies and society. For more info: https://www.imt-atlantique.fr/en/research-innovation



Chair Cyber CNI: Cybersecurity for Critical Networked Infrastructures (Cyber CNI) is an industrial research chair. The Cyber CNI Chair at IMT Atlantique is devoted to research, innovation, and teaching in the field of the cybersecurity of critical infrastructures, including industrial processes, financial systems, building automation, energy networks, water treatment plants, transportation.

The chair covers the full stack from sensors and actuators and their signals over industrial control systems, distributed services at the edge or cloud, to user interfaces with collaborative Mixed Reality, and security policies.

The chair currently hosts 6+3 PhD students, 1+3 PostDocs, 11 Professors, 1+1 engineers, and 1 internship student. The chair runs a large testbed that enables applied research together with the industry partners. The industry partners of the second funding round are Airbus, Amossys, BNP Paribas, EDF, Nokia Bell Labs, and SNCF.

Brittany is the cybersecurity region number 1 in France. The chair Cyber CNI is strongly embedded in the cybersecurity ecosystem through its partnerships with the Pôle d'Excellence Cyber (PEC) and the Brittany Region. The chair provides a unique environment for cybersecurity research with lots of development possibilities. For more info : https://cybercni.fr

This poster was made at the chaire Cybersecurity for Critical Networked Infrastructures (Cyber CNI) | https://cyber-cni.fr/ | Our monthly cybersecurity speaker series https://talk.cybercni.fr/ | Our science blog https://future-iot.org/