Working document for information (not yet approved)

Chaire de professeur junior

Electromagnetic cybersecurity (CYBEREM)

Université de Rennes 1 / IETR (Institut d'Electronique et des Technologies du numéRique)

Rennes, France

Project Title: Electromagnetic cybersecurity (CYBEREM)

Keywords: Electromagnetic eavesdropping /Side Channel Attacks/ Electromagnetic Aggression / Deny of Service

Duration: 4 years (tenure-track for full-professor permanent position)

Funding: Over 1 M€ (including Equipment: 600 k€, Agence National de Recherche: 200 k€, Ph.D. budget UR1: 120 k€ and other expenses) over the 4-year period

Scientific topics: Electromagnetism / Electronics

Corresponding Section (s) of the french CNU/CoNRS: CNU 63 / CNRS 08

Cybersecurity in higher education and research in Rennes

Cybersecurity in the broad sense is a cornerstone for digital sciences and technologies. This is particularly the case for the Brittany region, in particular for all higher education establishments and national research organizations (mainly CNRS and INRIA) at the local scale of Rennes area. In this context, multiple entities are located in the Rennes metropolitan area (Pole of Excellence in Cybersecurity, DGA-MI, an extremely dense and dynamic network of firms and professional organizations). Cybersecurity has been at the heart of Rennes Higher Education and Research responses to calls for projects of the Future Investment Program for several years.

While research themes relating to "software" cybersecurity are supported, the hardware component of the security of cyber-physical systems is a weak point in our skills portfolio. The major priority is therefore to address this weakness by allowing the recruitment of a junior professor with expertise in hardware cybersecurity. He or she will be assigned to the IETR, UMR CNRS 6164 and will help position the Rennes site on the challenges of material cybersecurity, at the best international level. He or she will also play a key role in the deployment of EUR CyberSchool and the establishment of dedicated learning paths (secure communications, security for IoT, etc.).

Cybersecurity at the IETR laboratory, UMR CNRS 6164

Cybersecurity has established itself as a rapidly growing discipline at IETR since 2015 on the very specific aspect of hardware cybersecurity. Electronics, which form the material medium for digital exchanges of information, indeed presents many exploitable vulnerabilities in connection with information eavesdropping (auxiliary channel attacks) or in the context of a denial of service attack. Communication systems and networks (for example of Internet of Things type), on-board systems or terminals, cyber-systems (in particular autonomous vehicles) or even automata are all examples of targets that can be attacked by other means than software intrusion. The historical specialties of the IETR in the field of electronics and telecommunications (from the elementary component to the system) give the IETR essential and major assets to meet the challenge of preserving the security associated with the hardware configurations of the various information technology systems which make the daily life of our digital society. Material cybersecurity is identified as a strategic development axis at the IETR for the next five years (2021-2026), as identified in its laboratory project and constitutes one of the transversal axes of the unit due to its multidisciplinary nature. This domain benefits from a very favorable eco-system, through the pole of excellence in cybersecurity (PEC) in Brittany, the EUR Cyberschool and the current and future presence of important players in the field on the territory or nearby (Secure IC, Thales, ANSSI, IRT b <> com, …). The IETR is also very strongly committed to the future CEPR 2021-2027 CYMOCOD program (Cyber-systems and Cyber-security, Mobility, Connectivity, Data: issues at the heart of the digital transformation of society, its sovereignty and of its transitions) which will provide significant additional material resources in the field of electromagnetic cybersecurity at the INSA Rennes site. This context is therefore very favorable to recruit a brilliant young researcher to meet the many scientific challenges in this field of research very little explored by the academic community in France and at an international scale.

Scientific projet

In the coming years, we should see a total renewal of techniques related to the electromagnetic safety of electronic systems. The means of electromagnetic eavesdropping and attack are becoming more accessible, and the number and diversity of critical systems vulnerable to electromagnetic agressions also tend to grow considerably. The electromagnetic aspect of cybersecurity must be dealt with according to two different angles: i) passive or active attack by auxiliary channels in order to compromise information ii) electromagnetic agression for the purpose of denial of service. The recruited junior professor will aim to develop activities in this field of electromagnetic cybersecurity and will rely on recent and future investments (CPER CYMOCOD project 2021-2027) of the QOSC platform of the IETR and the Security platform of Physical Systems. He will perform this activity within eWAVES team whose research portfolio concerns both EMC, wave-matter interaction (including living organisms) and the manipulation of wavefronts in complex environments. Two major issues will be addressed. The first concerns passive and active listening techniques, which can promote electromagnetic couplings and detect compromising information, even at relatively long distances. Different candidate techniques may be proposed, including advanced exploitation of the propagation channel, possibly resorting to the use of hidden components. The second concerns vulnerability analysis, aiming at denying service of equipment, systems or systems of systems through intentional electromagnetic attacks by manipulation of optimized wavefronts. This electromagnetic & cybersecurity field of investigation constitutes a major challenge for the evolution of more traditional investigation techniques for electromagnetic compatibility (EMC) in the advent of autonomous systems or vehicles managing critical processes and could partly renew the vision of EMC experts for the years to come with a view to bringing the necessary security countermeasures.

Teaching project

This chair is part of the transformation project of the Master Doctorate offer, which is part of the 2022-2027 project for Université of Rennes 1 and its partners at the Rennes site. This model aims to generalize the model inspired by the so-called Ecoles Universitaires de Recherche (EUR): development of majors / minors, learning and skills block, development of links with the socio-economic world (apprenticeship, work-study, continuous education), implementation of international Masters, and Master leading to PhD. The holder of this chair will be required to work on minors and majors in electronics and to speak in English as part of the planned international masters. The chair must therefore contribute to the on-going transformation of the offer of master's / doctorate / engineering training. The teaching project within the ISTIC UFR (Computer Science-Electronics) is part of the development of the EUR cyberschool and the demand for the creation of the Master Sciences for Engineering and Applications (SPIA) with an objective of international development. This project is divided into two parts. The first part concerns the development of a major on the electromagnetic security of electronic systems and on the security of the physical communication layer within the SPIA and IT masters in partnership with INSA Rennes, ENS Rennes, CentraleSupélec and IMT Atlantic. Projects related to this major will be proposed to students throughout the master's course as part of the training. The second part concerns the initial training of students in order to offer a minor initiation to research at the bachelor's level on topics still related to the safety of radiofrequency systems. These lessons can be given in English.

Contact: Philippe Besnier, directeur de recherche CNRS, directeur adjoint IETR, philippe.besnier@insa-rennes.fr (+33 2 23 23 86 92)