NATIONAL PRESS RELEASE – PARIS – 21 JUIN 2022

Presentation of the national Cyber-strategy: 7 projects selected as part of the Research Priority Readiness Program

Led by the CNRS, INRIA and the CEA, the Cybersecurity Research Priority Readiness Program (PEPR) aims to strengthen the excellence of French research and support the development of the cybersecurity sector. Launched on June 21, 2022, this is part of a national acceleration strategy announced by the President of the Republic on 21 February 2021, of which it constitutes the upstream research component. With a budget of 65 million euros over 6 years, financed under the PIA 4 (now France Relance), it has just announced its initial seven targeted research projects.

In a context of constantly developing cyberthreats and major global competition aimed at developing solutions to protect citizens, corporations and institutions, France has adopted a national cybersecurity strategy, within the framework of PIA4. The goal: to triple the turnover of the sector by 2025, to train more professionals and to develop French solutions. In its latest panorama report on cyberthreats, ANSSI reported that the cybersecurity issue became even more visible during the pandemic, by amplifying teleworking and cyberattacks against vital operators and institutions.

Supporting research activities at the top global level, the Cybersecurity PEPR will strengthen national efforts in this area and its results will feed into further downstream actions related to this strategy, such as the Cyber Campus transfer program operated by INRIA and the prototyping of French solutions in calls for projects. Involving about 200 researchers and lecturers from the CNRS, CEA, INRIA, and 22 universities[1] and Grandes Écoles[2], it calls upon several disciplines: computer science, mathematics, electronics and signal processing to help secure the three layers of cyberspace (hardware, software, data).

The PEPR supports specific actions, including the implementation of targeted projects. Connection and knowledge transfer between academics and industrials will also be a focus.

A first set of seven major targeted projects covering two angles have been set up. A call for projects, launched in June and run by the ANR, will fund three additional projects.

The first 7 targeted projects

Information security

iPOP (Interdisciplinary Project on the Protection of Personal Data) will study the threats to privacy introduced by new data services and design theoretical and technical solutions for the protection of privacy, compatible with French and European regulations, that preserve quality in user experience. These solutions will be deployed and evaluated based on their technological aspects, but also on legal and societal acceptability.

SECURE COMPUTE investigates cryptographic mechanisms that ensure data security during its transfer and during the entire storage period, but also during processing, despite uncontrolled environments such as the internet for exchange and the Cloud for hosting and processing.

SVP (Security protocol verification) targets the analysis of protocols already deployed or being deployed, both in terms of the specifications for these protocols and their implementations. It will develop techniques and tools to implement solutions whose safety will no longer be cyclically challenged.

DEFMAL (Defence against Malware) studies malware (including, ransomware, botnet, etc.). It will develop new approaches to malware analysis and will help the overall understanding of the malware ecosystem in an interdisciplinary approach involving all stakeholders.

System security

SUPERVIZ (Security supervision and orchestration) targets the detection, response and remediation of computer attacks, topics grouped under the name of “Security Supervision”, which seeks to strengthen preventive protection mechanisms and to remedy their shortcomings.

SECUREVAL aims to design new tools benefiting from new digital technologies to verify the absence of hardware and software vulnerabilities, and to produce the required proof of compliance.

ARSENE aims to accelerate research and development in state and industrializable security solutions in a coordinated and structured way. In a final step, ASIC and FPGA demonstrators integrating the blocks developed will test and enhance this research work.

Notes

[1] Sorbonne Université; Université Bretagne Occidentale; Université Bretagne Sud; Université de Lille; Université de Lorraine; Université de Montpellier; Université de Rennes 1; Université de Versailles Saint-Quentin-en-Yvelines; Université Grenoble Alpes; Université Jean Monnet St Etienne; Université Paris-Saclay.

[2] ENS Rennes; ENSTA Bretagne; ENS PSL; EURECOM; Grenoble INP; INSA CVL; INSA Lyon; INSA Rennes; Institut Mines Télécom; CentraleSupélec; EDHEC.

Contacts

CNRS Press l Priscilla Dacher l **T +33 1 44 96 46 06** l priscilla.dacher@cnrs.fr
CEA Press l Tuline Laeser l **T +33 06 12 04 40 22** l tuline.laeser@cea.fr
INRIA Press l Laurence Goussu l **T +33 1 39 63 57 29** l laurence.goussu@inria.fr