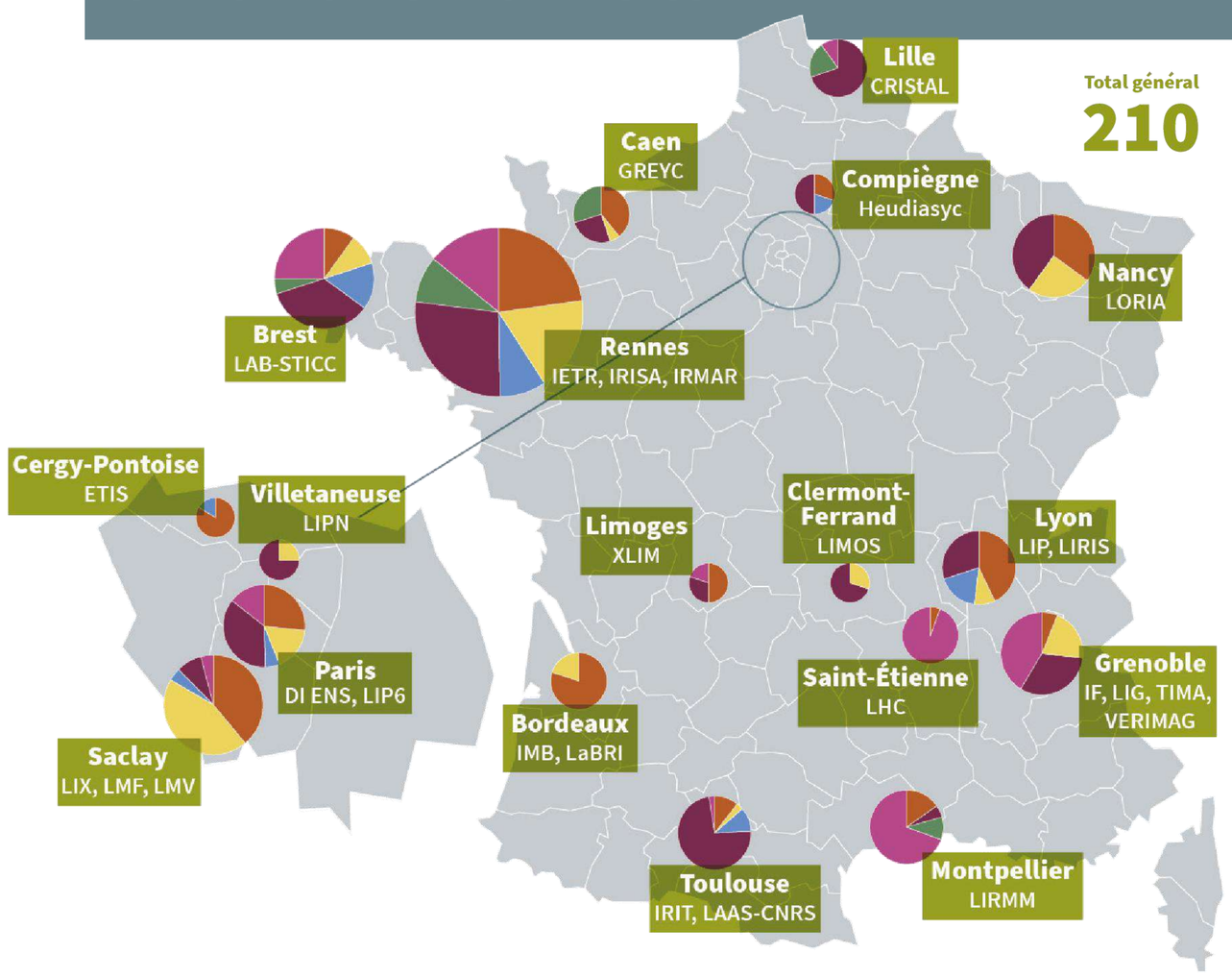
LA RECHERCHE EN CYBERSÉCURITÉ AU CNRS

Bibliothèque de stockage à bandes magnétiques du Centre de calcul de l'Institut de physique nucléaire et de physique des particules (CC-IN2P3). Cette infrastructure de recherche conçoit et opère un système de stockage de masse et de traitement de grandes quantités de données, contribuant ainsi à de nombreuses expériences d'envergure internationale, principalement dans le domaine de la physique et de l'astroparticule. Le centre participe également à des projets transdisciplinaires. Ses deux salles informatiques de 850 m² chacune hébergent plusieurs milliers de serveurs ainsi que des bibliothèques robotisées pouvant stocker près de 340 pétaoctets de données sur bandes magnétiques. © Cyril FRESILLON / CC IN2P3 / CNRS Photothèque

LES LABORATOIRES EN CYBERSÉCURITÉ



Cartographie des laboratoires en cybersécurité au CNRS

Thématiques abordées :

- Codage et cryptographie
- Méthodes formelles pour la sécurité
- Protection de la vie privée
- Sécurité des systèmes, des logiciels et des réseaux
- Sécurité et données multimédia
- Sécurité des systèmes matériels

Nombre de chercheurs et enseignants-chercheurs en cybersécurité :

- Moins de 10 personnes
- Entre 10 et 20 personnes
- Plus de 20 personnes

POLITIQUE SCIENTIFIQUE

Depuis 2015, l'Institut des sciences de l'information et de leurs interactions (INS2I) du CNRS a mené une action volontariste sur le thème de la sécurité informatique qui s'est traduite par de multiples actions.

RECRUTEMENT DE JEUNES CHERCHEUSES ET CHERCHEURS

Depuis 2016, la thématique Sécurité (cryptologie, sécurité quantique, sécurité matérielle, vie privée, sûreté et sécurité des systèmes, etc.) a été systématiquement présente sous la forme de coloriages thématiques au niveau des concours de recrutement des chargés de recherche CNRS. Depuis quatre ans, six jeunes chercheuses et chercheurs ont été recrutés sur cette thématique au sein de l'Institut de recherche en informatique et systèmes aléatoires, du Laboratoire lorrain de recherche en informatique et ses applications, du Laboratoire Hubert Curien et du Centre de Recherche en Informatique, Signal et Automatique de Lille.

ANIMATION SCIENTIFIQUE

Dans le cadre de son année thématique consacrée au thème de la sécurité en 2016, l'INS2I au CNRS a lancé plusieurs actions destinées à animer la communauté cybersécurité au sein de ses unités, avec, en particulier, la création du Groupement de recherche (GdR) Sécurité informatique. L'institut a également co-piloté avec Inria, au sein de l'alliance des sciences et technologies du numérique ALLISTENE, la réalisation en 2016-2017 de la cartographie nationale des recherches en cybersécurité.

SOUTIEN AUX THÉMATIQUES ÉMERGENTES EN SÉCURITÉ

En marge des recherches sur la sécurité informatique classique, l'INS2I-CNRS soutient également le thème émergent de la sécurité post-quantique, en particulier à travers la Fédération Paris Centre for Quantum Computing (PCQC) créée en 2014 pour coordonner les actions des équipes des unités IRIF et LIP6. PCQC présente un potentiel unique au niveau national, porté notamment par six chercheurs CNRS dont les travaux ont une très grande visibilité internationale (avec, notamment, deux projets ERC Starting Grant). PCQC est partenaire de deux projets sélectionnés en 2018 pour la phase de lancement du futur flagship européen Technologies quantiques.

START-UPS ET LABORATOIRES COMMUNS

Plus d'une vingtaine de start-ups dans le domaine de la cybersécurité sont sorties des laboratoires du CNRS ces dernières années. Cyber-Detect, fruit de dix années de recherche au LORIA, offre par exemple plusieurs produits et services, notamment en analyse de codes malveillants et de virus informatiques. Lauréate du concours i-lab 2019, la start-up Cosmian propose une plateforme pour diffuser et exploiter des données, notamment personnelles, sans les compromettre : David Pointcheval, directeur de recherche CNRS au Département d'informatique de l'École normale supérieure, s'appuiera sur cette start-up pour mener son ERC "Proof of Concept". Issue du Laboratoire d'informatique et systèmes, KeeeX développe un certificat d'authenticité numérique universel et inviolable qui protège les documents, les photos et les vidéos contre toute tentative de fraude. Enfin, la start-up rennaise Acklio, issue de l'IRISA, entend sécuriser les échanges tout en garantissant l'interopérabilité des différents réseaux de l'Internet des objets.

On compte également plusieurs laboratoires communs : Cybermallix entre le LORIA et la société Wallix, afin de développer des solutions prédictives de détection de logiciels malveillants (malwares) basées sur l'intelligence artificielle (IA). Le projet du LabCom SIBIL-Lab repose sur une collaboration entre la PME ALG (Attestation Légale) et l'organisme de recherche LIRIS-UMR CNRS 5205 qui sont implantés dans la métropole lyonnaise. La feuille de route de SIBIL-Lab est ainsi centrée sur la gestion de l'identité numérique et la détection de tentatives de fraudes dans le contexte spécifique des réseaux B2B. La chaire IA LUSIS entre l'entreprise Lusis et CentraleSupélec / Laboratoire Interdisciplinaire des Sciences du Numérique (LISN) se consacre à l'application de méthodes d'IA au domaine bancaire. Elle développe des algorithmes pour la détection de fraude par carte bancaire, soit moins de 0,5 % de ces transactions mais une perte de plusieurs milliards d'euros par an. La chaire cible également l'application d'une méthode d'apprentissage par renforcement afin de réaliser du trading automatisé consistant à acheter une action pour la revendre à meilleur prix.

GDR SI - SÉCURITÉ INFORMATIQUE

OBJECTIFS

Le GDR Sécurité Informatique est une structure d'animation du CNRS créée en 2016 par le CNRS. Ouvert à toute la communauté de recherche française, académique, mais aussi industrielle et étatique, il a pour mission de favoriser les interactions entre toutes les communautés de la sécurité informatique. Le GDR fédère autour de six groupes de travail thématiques dont trois sont communs avec les GDR Informatique Mathématique (IM), Information, signal, images, vision (ISIS) et System On Chip - System In Package (SOC_2). Il organise une douzaine d'événements par an, des séminaires, publie une gazette trimestrielle et mène des actions en direction des jeunes chercheurs, notamment l'école d'été et les rencontres entreprises-doctorants en sécurité.

6 AXES THÉMATIQUES

- Codage et cryptographie (commun avec le GDR IM)
- Méthodes formelles pour la sécurité
- Protection de la vie privée
- Sécurité des systèmes, des logiciels et des réseaux
- Sécurité et données multimédia (commun avec le GDR ISIS)
- Sécurité des systèmes matériels (commun avec le GDR SOC_2)

1300 CHERCHEURS ET CHERCHEUSES IMPLIQUÉS AU SEIN DE **30** LABORATOIRES

Journées Nationales du GDR en 2018 © Marc-Olivier Killijian

PROSPECTIVES

Le GDR Sécurité Informatique mène régulièrement des réflexions prospectives, dont les éléments saillants sont présentés ci-dessous.

SÉCURITÉ DES SYSTÈMES MATÉRIELS

Avec l'avancée des technologies d'intégration, des chemins d'attaque, de l'instrumentation et du traitement de l'information, la sécurité matérielle des systèmes sur puces est un enjeu majeur de la sécurité numérique. Au-delà des moyens de contre-mesures à implanter, s'ajoute le défi de concevoir les systèmes à venir pour répondre aux exigences de sécurité mais aussi de performances.

MÉTHODES FORMELLES POUR LA SÉCURITÉ

La sécurité demande d'analyser des systèmes (protocoles comme TLS et leurs implémentations, codes...) et des propriétés sensiblement différents de ceux étudiés en sûreté, amenant de nouveaux défis aux méthodes formelles : raisonner sur des propriétés reliant des traces d'exécution entre elles, raisonner de manière quantitative, analyser du code très bas niveau (frontière logiciel / matériel), et enfin analyser des codes malveillants.

Chercheuse expliquant une proposition de protocole de vote électronique
© Cyril Frésillon / LORIA / CNRS Photothèque

SÉCURITÉ ET DONNÉES MULTIMÉDIA

Les principaux verrous scientifiques portent sur : les méthodes génératives en stéganographie et forensique, la maîtrise des taux de fausses alarmes en détection (stéganalyse, forensique) face au passage à l'échelle, la conception de méthodes de détection indépendantes du corpus d'apprentissage et l'impact des approches par *deep learning*, l'analyse et le traitement de contenus multimédia chiffrés, les systèmes biométriques multimodaux, la vidéosurveillance intelligente avec la ré-identification de personnes à des fins d'authentification.

PROTECTION DE LA VIE PRIVÉE

Une des difficultés de la thématique est d'être capable d'apporter des solutions déployables et utilisées à large échelle. Dans un monde où les applications innovantes priment sur le respect de la vie privée, l'enjeu est le développement des approches *privacy by design* ou d'anonymisation, y compris en interaction avec d'autres domaines comme le génie logiciel, les réseaux / IoT, ainsi que des collaborations pluridisciplinaires avec les disciplines juridiques et économiques notamment.

SÉCURITÉ DES SYSTÈMES, DES LOGICIELS ET DES RÉSEAUX

Dans un monde où les vulnérabilités et les logiciels malveillants sont omniprésents (par exemple les rançongiciels), de nouveaux sujets émergent autour de l'IoT et les systèmes industriels. Les défis résident dans la complexité croissante des systèmes et dans les interactions aux frontières, par exemple entre le logiciel et le matériel. De plus, le domaine tend à dépasser l'approche traditionnelle qui consiste à prévenir, pour mieux détecter les attaques et y répondre.

CRYPTOGRAPHIE ET CODAGE

Il s'effectue depuis quelques années un transfert des forces en cryptographie, allant des primitives symétriques - où les recherches très intenses des trois dernières décennies ont permis d'obtenir des primitives très abouties - vers des problèmes ouverts comme le chiffrement homomorphe et fonctionnel, la cryptographie post-quantique, la cryptanalyse et la sécurité des protocoles cryptographiques.

CONTACT

Directrice : Caroline Fontaine
caroline.fontaine@lsv.fr

http://gdr-securite.irisa.fr
Twitter : @GdrSecInfo

cnrs GDR Groupement de recherche Sécurité Informatique