CYBERSECURITE

Animateurs : Pierre Graux / Clémentine Maurice / Pauline Puteaux

Cybersécurité

Description

La cybersécurité demeure un sujet extrêmement critique, transverse à de nombreuses disciplines importantes. Dans cet axe transversal, nous adressons ce sujet sous les angles de la sécurité des systèmes, des logiciels, des réseaux, des contenus, du matériel, de l'IA, des méthodes formelles, et de la production de la vie privée.

Projets « emblématiques »

• PEPR : COMPROMIS, IPop, REDEEM, REV
• HORIZON : FLUTE, UNCOVER
• Europe : IPCEI-CIS
• ANR : ARCHI-SEC, CAPSUL, FACADES, FP-Locker, MIAOUS, PMR, PRIDE, Republic, TinyPART
• Autre : FedMalin, ICAR2, « Identification des interactions dans une architecture Internet des Objets » LoRa-R, Partenariat OVHCloud « DDoS », STaRS ASCOT, « Gérer vos données sans fuite d'information », SWHSec, TRUMPET

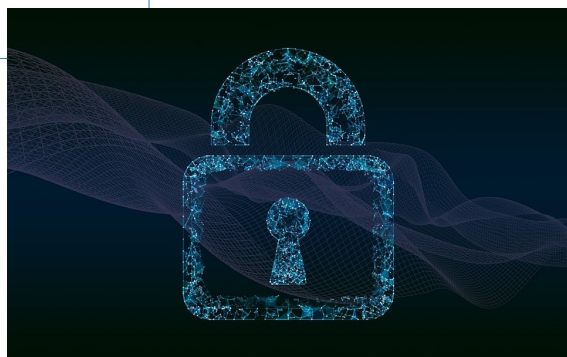
Equipes concernées

♠ ***GT DatInG (Data Intelligence Group) :*** MAGNET, SCOOL, SIGMA

♠ ***GT GL (Génie logiciel) :*** EVREF, Spirals

♠ ***GT Image :*** 3D SAM

♠ ***GT SISE (Systèmes Informatiques Sûrs et Efficaces) :*** 2XS, SyCoMoRES



Cybersécurité

L'axe transversal cybersécurité est réparti au sein du laboratoire dans huit équipes sur trente et une couvrant ainsi quatre Groupes Thématiques sur neuf.

Ainsi, à l'exception de celui sur le codage et la cryptographie, la totalité des groupes de travail identifiés nationalement par le GDR Sécurité sont abordés :

• *Sécurité des systèmes, des logiciels et des réseaux*

L'équipe 2XS étudie la détection d'intrusion dans les réseaux de communication qu'ils soient domestiques ou au sein des plus grands datacenters du monde. Elle étudie également comment développer des méthodes d'analyse de programmes assembleurs pour vérifier leurs propriétés de sécurité, en particulier dans le cadre des applications Android.

L'équipe SyCoMoRES cherche elle à analyser les propriétés fonctionnelles des codes assembleurs afin par exemple de détecter des accès mémoire illégaux.

L'équipe EVREF travaille sur des méthodes de sécurisation des langages basées sur l'isolement de parties du langages ou/et l'utilisation de bacs à sable. Ses travaux portent également sur l'analyse de code pour la sécurité. Le langage Pharo et son IDE, résultat de cette équipe, sont en voie de certification pour une utilisation par la DGA.

L'équipe Spirals a un axe de recherche porté sur le traçage de navigateurs web à partir d'empreintes générées par les navigateurs. Ces méthodes très sélectives peuvent être utilisées de manière à authentifier l'utilisateur du navigateur.

• *Protection de la vie privée*

L'équipe MAGNET développe des méthodes d'apprentissage respectueuses de la vie privée. Ces méthodes sont souvent basées sur le principe d'un apprentissage distribué sur plusieurs utilisateurs dont certains peuvent potentiellement être malicieux.

Les équipes MAGNET et SCOOL conçoivent également des systèmes de décisions reposant sur la confidentialité différentielle, le principe, ici, est de construire des statistiques artificiellement bruitées afin de cacher l'utilisation de données personnelles dans un bruit.

L'équipe Spirals étudie les propriétés de contrôle d'accès dans une base de données, afin, par exemple, de détecter à partir de la sémantique de la base s'il est possible ou non d'exfiltrer des données.

• *Méthodes formelles pour la sécurité*

L'équipe 2XS utilise les méthodes formelles pour concevoir le noyau d'un système d'exploitation en intégrant ses propriétés de sécurité by-design et étudie comment faciliter la conduite de la preuve en l'intégrant dès les premières étapes de la conception.

• *Sécurité et contenus multimédia*

L'équipes 3D SAM propose des méthodes de biométrie à partir de l'analyse des visages, des corps en vue de la reconnaissance des comportements humains. La reconnaissance des comportements humains est étudiée dans un environnement personnel et de foule en relation avec la sécurité des personnes.

L'équipe SIGMA travaille sur l'insertion de données cachées (la stéganographie) et leur détection (la stéganalyse) dans des contenus anodins tels que les images numériques. Une autre partie des activités de cette équipe se focalise sur la détection de manipulation des images et leur protection par des méthodes d'analyse forensique, de tatouage, ou de chiffrement sélectif.

• *Sécurité des systèmes matériels*

L'équipe Spirals évalue la sécurité des micro-processeurs notamment vis-à-vis d'attaques par canaux auxiliaires. Ces méthodes permettent possiblement d'inférer un élément de sécurité (clé de chiffrement par exemple) à partir de mesures logicielles directement prises sur le système.

L'équipe 2XS étudie comment les canaux auxiliaires peuvent être utilisés pour caractériser un système en cours de fonctionnement notamment dans le cadre d'analyses forensiques.

• *Sécurité et IA*

Ces travaux visent à vérifier qu'un algorithme d'apprentissage automatique effectue bien la tâche qui lui est demandée et ce même en présence d'un adversaire.

Les équipes SCOOL et MAGNET travaillent ainsi sur des méthodes équitables qui permettent de garantir qu'une prédiction ne souffre pas d'un biais qui pourrait être introduit par l'adversaire en modifiant la base d'apprentissage.

L'équipe SIGMA travaille sur des attaques qui permettent de générer les exemples adverses (exemples représentant une classe donnée mais classés en une autre classe) mais aussi de les détecter avant l'appel au classifieur.

L'équipe 2XS travaille sur l'utilisation des réseaux de neurones impulsionnels (SNN) pour un apprentissage respectueux de la vie privée et leur résistance aux attaques adverses.

• *L'axe cybersécurité, à travers ses chercheurs et chercheuses, est impliqué dans :*

- Programme et équipements prioritaires de recherche (PEPR) Cybersécurité : stratégie d'accélération de la cybersécurité qui comporte un important programme de recherche, d'un montant de 65 millions d'euros, qui est piloté par le CNRS, Inria et le CEA.

- Groupement de Recherche (GdR) Sécurité Informatique : Le GDR Sécurité Informatique est un outil d'animation de la recherche française créé par l'Institut des sciences de l'information et de leurs interactions (INS2I) du CNRS, et ouvert à toute la communauté. Les thématiques couvertes par le GDR incluent le codage et la cryptographie, les méthodes formelles pour la sécurité, la protection de la vie privée, la sécurité des systèmes, des logiciels et des réseaux, la sécurité des systèmes matériels, la sécurité et les données multimédia.

- Forum InCyber (FIC) : Le Forum InCyber, qui se tient à Lille depuis son lancement en 2007, est le principal événement européen sur les questions de la sécurité et de confiance numérique.