CYBERSECURITY

Presenters: Pierre Graux / Clémentine Maurice / Pauline Puteaux

Cybersecurity

Description

Cybersecurity remains an extremely critical subject that cuts across many important disciplines. In this cross-disciplinary area, we address this subject from the angles of systems security, software, networks, content, hardware, AI, formal methods and privacy protection.

‘Emblematic’ projects

- PEPR: COMPROMIS, IPop, REDEEM, REV
- HORIZON: FLUTE, UNCOVER
- Europe: IPCEI-CIS
- ANR: ARCHI-SEC, CAPSUL, FACADES, FP-Locker, MIAOUS, PMR, PRIDE, Republic, TinyPART
- Other: 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

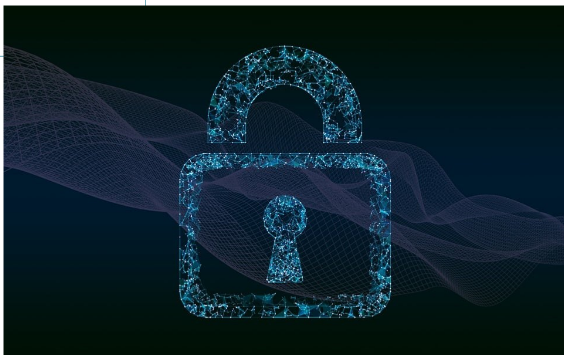
Teams concerned

♠ ***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



Cybersecurity

The cybersecurity cross-disciplinary theme is spread across eight of the thirty-one teams in the laboratory, covering four of the nine Thematic Groups.

With the exception of coding and cryptography, all the working groups identified nationally by the Security GDR are covered :

• Systems, software and network security

The 2XS team studies intrusion detection in communication networks, whether at home or in the world’s largest data centres. It is also studying how to develop methods for analysing assembler programmes to check their security properties, particularly in the context of Android applications.

The SyCoMoRES team is working on analysing the functional properties of assembler code in order, for example, to detect illegal memory access.

The EVREF team is working on language security methods based on the isolation of parts of the language and/or the use of sandboxes. Its work also covers code analysis for security. The Pharo language and its IDE, the result of this team’s work, are in the process of being certified for use by the DGA.

The Spirals team’s research focuses on tracing web browsers using browser-generated fingerprints. These highly selective methods can be used to authenticate the browser user.

• Protection of privacy

The MAGNET team develops learning methods that respect privacy. These methods are often based on the principle of distributed learning across several users, some of whom may be potentially malicious.

The MAGNET and SCOOL teams are also designing decision systems based on differential confidentiality, the principle here being to construct artificially noisy statistics in order to hide the use of personal data in the noise.

The Spirals team studies the properties of access control in a database, in order, for example, to detect from the semantics of the database whether or not it is possible to exfiltrate data.

• Formal methods for security

The 2XS team uses formal methods to design the kernel of an operating system by integrating its security properties into the design, and is studying how to facilitate the conduct of proofs by integrating them into the early stages of design.

• Security and multimedia content

The 3D SAM team offers biometric methods based on the analysis of faces and bodies with a view to recognising human behaviour. The recognition of human behaviour is studied in personal and crowd environments in relation to personal safety.

The SIGMA team works on the insertion of hidden data (steganography) and its detection (steganalysis) in innocuous content such as digital images. Another part of the team’s activities focuses on detecting the manipulation of images and protecting them using forensic analysis, watermarking or selective encryption methods.

• *Hardware systems security*

The Spirals team evaluates the security of microprocessors, particularly with regard to attacks using auxiliary channels. These methods make it possible to infer a security element (encryption key, for example) from software measurements taken directly on the system.

The 2XS team is studying how auxiliary channels can be used to characterise a system during operation, particularly as part of forensic analysis.

• *Security and AI*

This work aims to verify that a machine learning algorithm performs the task assigned to it, even in the presence of an adversary.

The SCOOL and MAGNET teams are working on fair methods to ensure that a prediction does not suffer from a bias that could be introduced by an adversary by modifying the learning base.

The SIGMA team is working on attacks that not only generate adversarial examples (examples representing a given class but classified in another class) but also detect them before the classifier is called up.

The 2XS team is working on the use of impulse neural networks (SNN) for privacy-friendly learning and their resistance to adversarial attacks.

• *Through its researchers, the cybersecurity division is involved in:*

- *Programme et équipements prioritaires de recherche (PEPR) Cybersecurity*: a strategy for accelerating cybersecurity that includes a major research programme worth €65 million, led by the CNRS, Inria and the CEA.

- *Groupement de Recherche (GdR) Sécurité Informatique (IT Security Research Group):* The GDR Sécurité Informatique (IT Security Research Group) is a tool for coordinating French, research, created by the CNRS's Institut des Sciences de l'information et de leurs interactions (INS2I) and open to the entire community. The themes covered by the GDR include coding and cryptography, formal methods for security, protection of privacy, system, software and network security, hardware system security, and multimedia data security.

- *InCyber Forum (FIC):* The InCyber Forum, held in Lille since its launch in 2007, is Europe's leading event on digital security and trust.