Journée Scientifique annuelle

Défi Clé

Institut Cybersécurité Occitanie

(ICO)

Vendredi

5 décembre

2025

9H – 17H30

AMPHI BELLONTE
ENAC
7, AVENUE EDOUARD BELIN
31400 TOULOUSE FRANCE

PROGRAMME

9h - 9h30 **ACCUEIL**

9h30 - 9h45
INTRODUCTION

9h30 - 9h45 — *Mohamed KAÂNICHE (LAAS-CNRS)*

Introduction - Présentation du Défi Clé « ICO »

9h45 - 10h45
PRÉSENTATIONS DES DOCTORANTS COFINANCÉS PAR L'ICO (PREMIÈRE PARTIE)

9h45 - 10h05 — *Gabin NOBLET (LAAS -CNRS / Custocy)*

Génération de données d'intrusion réseau par apprentissage profond de représentations

La génération de données synthétiques de trafic réseau, labellisées et réalistes, est un enjeu majeur pour l'entraînement des systèmes de détection d'intrusions. Nous proposons une solution hybride permettant une génération contrôlée de trafic synthétique, reproduisant fidèlement les propriétés structurelles et temporelles des flux réels. L'approche s'appuie sur une représentation discrète du trafic et un modèle génératif conditionnel, assurant compatibilité avec les outils standards et adaptabilité à des scénarios ciblés.

PROGRAMME

10h05 - 10h25

Antony DALMIÈRE
(LAAS-CNRS / UT)

Ingénierie Sociale : Application des théories de psychologie sociale à la cybersécurité

Cette présentation est une analyse empirique du phishing en tant que vecteur d'ingénierie sociale. Une taxonomie comprenant quarante techniques de manipulation psychologique et mesurant leur fréquence d'occurrence dans des jeux de données réels de phishing sera présentée. Ainsi que les résultats d'ICL des LLM pour classifier les schémas de manipulation psychologique, atteignant une précision de 0,76.
La présentation aborde également la manière dont ces techniques de manipulation contournent les filtres antispam. Sur un échantillon de 386 messages de phishing confirmés, la majorité emploie des techniques de spoofing du texte intégré dans des images. Les résultats indiquent que l'encodage Base64 et le texte inclus dans les images permettent de contourner certains filtres antispam.

10h25 - 10h45

Robin THEVENIAUT
(IRIT / Carleton Univ., Canada)

Un framework pour la prise en compte des facteurs humains dans la prise de décision collaborative pour la conception d'architectures sécurisées

La prise de décision lors du développement d'architectures et de logiciels est un enjeu important. Ne pas prendre les bonnes décisions ou avec des conflits importants entre les différents partis peut être lourd en conséquences. Afin d'y faire face, nous proposons une approche au support à la prise de décision au travers d'un méta-modèle apportant une flexibilité suffisante de par ses concepts permettant de créer de nouvelles méthodes de prise de décision mais également d'intégrer des méthodes de prise de décision existante (Brainstorming, Voting, AHP, ...) afin qu'elles soient ensuite utilisées par les équipes de développement.

PROGRAMME

Nous y intégrons les travaux précédents sur les facteurs humains en sécurité afin de mettre en valeur cette évaluation des facteurs humains dans le cadre de la prise de décision.

Nous présenterons les contributions apportées par ces recherches au travers d'un scénario.

10h45 - 11h15 **PAUSE CAFÉ**

11h15 - 12h15

PRÉSENTATIONS DES DOCTORANTS COFINANCÉS PAR L'ICO (SECONDE PARTIE)

11h15 - 11h35 *Marie-Eve SAMSON (UT CAPITOLE)*

L'équilibre des pouvoirs dans le complexe militaro-industriel spatial en France

Le traitement des données d'origine spatiale est un socle de l'industrie spatiale de défense. La donnée spatiale, et plus encore la donnée spatiale militaire est stratégique et peut bouleverser l'équilibre des pouvoirs. Or, la législation nationale n'est pas suffisamment précise pour garantir une sécurité juridique de ces données. Les définitions ne sont pas complètes et les régimes juridiques ne sont pas adaptés pour la chaîne de responsabilité en matière de cyberspatial. De plus, certains pays autorisent l'exploitation de ressources spatiales telles que les données spatiales par les personnes de droit privé. D'autres législations s'immiscent dans les procédés de fabrication de nos appareils spatiaux et numériques. L'objectif de ces recherches est de sécuriser la donnée spatiale au sein de l'industrie française et de veiller à leur protection face aux législations étrangères invasives.

PROGRAMME

11h35 - 11h55

Van Tien NGUYEN
(LAAS-CNRS / IMT Atlantique)

Towards Context-aware Intrusion Detection in Individual-oriented Information Systems: An Empirical Study on Android Malware

In recent years, the range and volume of Internet services utilized by an individual have significantly expanded. This growing relationship between an individual user and diverse digital services has led to the emergence of Individual-oriented Information System (IIS) that encompasses the user, their physical devices, and the information systems they interact with. Current security approaches within an IIS suffer from three main limitations: (1) they are restricted to specific services, (2) they require intrusive instrumentation of each user single device, or (3) they rely on specific integration between client and server components. As a result, they fail to globally protect against attackers who possess enough information to bypass standalone security schemes. To overcome these constraints, we propose to (1) consider a network-oriented approach to detect intrusions which may occur within an IIS and (2) to make sensors taking part of the IIS contribute to the intrusion detection by providing user-related contextual data. In the absence of any suitable dataset that mixes network and physical contextual data, we construct a new integrated dataset comprising benign data captured through an in-situ experiment and intrusion traces extracted from CIC-AndMal2017—a widely referenced dataset in the literature. Our evaluation confirms that considering both user physical context and network features improves the performance of intrusion detection, thereby making IIS more resilient to attackers.

PROGRAMME

11h55 -12h15

Maximos SKANDALIS
(LIRMM)

Apprentissage profond et méthodes formelles pour la détection automatique d'énoncés contradictoires - application a la détection de désinformations

En traitement automatique des langues et en IA, les tâches de détection automatique de contradictions et d'inférence textuelle sont des tâches de classification de paires de phrases, avec deux (contradiction / pas de contradiction) ou trois (inférence, contradiction, ni l'un ni l'autre) étiquettes possibles lors de la prédiction. Dans cet exposé, nous présentons d'abord les jeux de données introduits pour les deux tâches pour le français, couvrant des thématiques également pertinentes pour la tâche de détection de désinformation, puis décrivons le premier pipeline neurosymbolique complet pour la tâche d'inférence textuelle pour le français. Le pipeline comporte deux étapes : (1) le parsing sémantique, qui consiste à obtenir la représentation logique des phrases, en utilisant des LLMs pour les étiquetages grammaticale et morphosyntaxique et le prouveur GrailLight pour la génération de preuves et de lambda termes, et (2) le raisonnement automatique à partir de ces représentations logiques, en adaptant au français le démonstrateur automatique LangPro, qui est basé sur la méthode des tableaux pour la logique naturelle. Sur le jeu de données SICK-FR, les résultats obtenus sont comparables à ceux de LangPro sur les versions anglaise et néerlandaise de SICK, et surpassent ceux de modèles Transformeurs récents entraînés sur XNLI. Enfin, nous discutons des sources d'erreurs potentielles dans le pipeline ainsi que des moyens d'améliorer davantage les résultats obtenus, par exemple en donnant accès au démonstrateur de théorèmes à des connaissances lexicales via une base de connaissances pour le français.

12h15 - 13h30

COCKTAIL DÉJEUNATOIRE

PROGRAMME

13h30 – 15h00

PRÉSENTATIONS DES POST-DOCTORANTS ET DES GROUPES DE TRAVAIL

13h30-13h50

Gabrielle BECK
(LIRMM)

Threshold Cryptography

Fully Homomorphic Encryption (FHE) is a powerful cryptographic primitive that enables a device with limited resources to securely outsource computation of a function to a third party with the guarantee that they will learn nothing about sensitive inputs. When multiple devices desire to securely compute a function over their joint input, they can instead utilize a Threshold FHE (ThFHE) scheme, which captures the same functionality of an FHE scheme except in a multiparty setting where the output of functions are only recoverable if enough devices in the group authorize it and private inputs remain hidden from other devices. ThFHE and FHE have seen a wide variety of potential applications in the construction of blockchains, privacy-preserving machine learning, healthcare, and other cryptographic primitives. We explore the current landscape of ThFHE schemes: how they are normally constructed, where those constructions currently stand in relation to closely related primitives like threshold public key encryption, and some open areas where we are trying to make progress in improving the state of the art. Discussion will include attempts to bring down the size of the decryption key shares via the use of better linear secret sharing schemes, attempts to use Reyni arguments for decreasing the size of the ciphertext, and the role that another cryptographic primitive, circuit privacy, plays in these attempts.

PROGRAMME

13h50-14h10

Cyrius NUGIER
(ENAC)

Adaptation d'Outils Cryptographiques pour un Contexte Post-Quantique

En prévision du moment où des ordinateurs quantiques pourraient effectuer des attaques sur nos cryptosystèmes actuels, le NIST a décidé de standardiser deux nouveaux cryptosystèmes : Kyber, basé sur les réseaux euclidiens, et HQC, basé sur les codes correcteurs d'erreurs. Afin de permettre une intégration rapide et facilitée dans nos protocoles de communication, il est crucial que leurs empreintes et leurs performances (taille et temps de génération des clefs, taille des chiffrés, temps de chiffrement et déchiffrement) soient aussi optimisés que possible. En parallèle, en avançant vers la standardisation des implémentations, l'évaluation de la sécurité de celles-ci vis-a-vis des fuites par canaux auxiliaires est nécessaire.

Les travaux présentés se concentrent sur HQC. Ils mettent en avant les dernières limites de la théorie des codes correcteurs qui bloquent l'optimisation des performances. Une technique est proposée pour contourner une de ces limites en choisissant judicieusement la répartition des erreurs, ce qui permet de réduire la taille des clefs et chiffrés. Ce changement permet aussi d'intégrer une version alternative de la multiplication polynomiale de HQC, améliorant ainsi les temps de chiffrement et déchiffrement. Finalement, nous illustrerons que certaines parties du déchiffrement sont actuellement vulnérables à des attaques par analyse de la consommation électrique, et que des contre-mesures logicielles ou matérielles doivent être mises en place.

PROGRAMME

14h10-14h30

Pierre AYOUB
(LAAS-CNRS)

Analyse des menaces émergentes à l'interface logiciel/matériel pour les technologies sans fil de l'Internet des Objets

L'Internet des Objets connaît un développement exponentiel depuis plusieurs années, entraînant un déploiement massif d'objets connectés reposant sur des protocoles de communication hétérogènes. La sécurité de ces objets connectés relève d'un caractère critique, dans la mesure où ils peuvent être exploités à des fins malveillantes : intrusion dans un réseau, diffusion de logiciels malveillants, ou encore impact direct sur la sécurité des personnes dépendant de ces capteurs. Cette présentation vise à mettre en évidence les nouvelles surfaces d'attaque émergentes au cours de ces dernières années, lesquelles demeurent à ce jour relativement peu étudiées. Dans un premier temps, nous analyserons comment l'hétérogénéité des protocoles employés, tels que Bluetooth Low Energy, Zigbee ou Matter, peut conduire à des attaques dites inter-protocolaires, notamment dans des scénarios d'attaque par pivot. Dans un second temps, nous étudierons la manière dont les attaques par canaux auxiliaires électromagnétiques — longtemps considérées comme peu pertinentes dans le contexte des objets connectés — se révèlent en réalité constituer une menace crédible. Enfin, nous proposerons une méthodologie permettant d'analyser systématiquement ces vecteurs d'attaque, en vue d'améliorer à la fois leur compréhension, leur exploitation et les mécanismes permettant de s'en prémunir.

PROGRAMME

14h30-15h

Caroline BARDINI
(CNRS)
et
Nicolas SABY
(Université de Montpellier)

Post-Doc: ACCES – Apprentissages en Cryptographie et CybersÉcurité au Secondaire
Groupe de Travail : CyCLyC – Cybersécurité et Cryptographie au Lycée et Collège

En France, les questions de cybersécurité sont peu présentes dans les curricula, et la cryptographie ne fait pas directement partie des contenus de mathématiques ou d'informatique à enseigner au secondaire.

Nous nous proposons d'amorcer ce questionnement sous deux angles différents mais complémentaires : l'un (ACCES) repose sur un ancrage théorique autour de la sémiologie, sémiotique et didactique, l'autre (CyCLyC) vise à développer et accompagner un groupe de travail rassemblant des enseignants du secondaire, en informatique et mathématiques, et des chercheurs. Les deux projets s'articulent autour de l'élaboration d'activités interdisciplinaires ancrées dans des questions d'actualité, et l'exploration de potentiels d'apprentissage en mathématiques et informatique autour de la cryptographie. Le travail s'appuie sur une compréhension des concepts en jeu dans la cryptographie afin d'identifier les obstacles épistémologiques, didactiques et sémiotiques.

15h00 - 15h30 **PAUSE CAFÉ**

PROGRAMME

15h30 – 16h50

PRÉSENTATION DU FINANCEMENT DES INGÉNIEURS ET DES PORTEURS DES PROJETS SCIENTIFIQUES

15h30-15h50

Pascale ZARATÉ
(IRIT)

SEM4Trust : Améliorer la confiance dans les réseaux sociaux par des analyses sémantiques

L'objectif de SEM4Trust est de proposer une plateforme permettant de réaliser et croiser plusieurs types d'analyses de données de réseaux sociaux à des fins d'enquête, comme l'analyse de conversations multiples, le repérage de certains types de discours (haineux, sexistes, violents, etc), ou l'identification des auteurs.

15h50-16h10

Quentin PEYRAS
(IRIT)

Vers la vérification de politiques de sécurités pour les systèmes distribués à états infinis

La non-interférence garantit l'absence de fuites de données non autorisées durant l'exécution du système. La vérification des politiques de sécurité est complexe et nécessite l'analyse de multiples chemins d'exécution. Les hyperpropriétés offrent un cadre permettant de décrire des politiques de sécurité comme la non-interférence. Toutefois, les méthodes existantes telles que HyperLTL se limitent aux modèles à états finis. Nous nous intéressons à une étude de cas illustrant l'utilisation de HyperFOLTL, conçue pour les systèmes distribués à états infinis, et proposons une approche formelle pour vérifier des politiques de sécurité dans de tels systèmes.

PROGRAMME

16h10-16h30

Florent GALTIER
(LAAS-CNRS)
et
Radhouene AZZABI
(CEA Tech Occitanie)

Plateforme PEPR SuperviZ

Dans le cadre du projet SuperviZ du PEPR Cybersécurité, le LAAS-CNRS et le CEA Tech Occitanie travaillent sur des plateformes d'expérimentation pour l'évaluation de méthodes de supervision en sécurité informatique.
Avec le soutien de l'ICO, nous avons notamment mis en place au LAAS une plateforme dédiée à la sécurité des objets connectés. Elle permet d'évaluer les performances d'approches de détection d'intrusion sans-fil de façon reproductible dans un environnement contrôlé, et de générer des datasets de communications entre ces objets contenant ou non du trafic malveillant. Le CEA Tech Occitanie est en train de développer un portail d'expérimentations multi-plateformes, ainsi que de nouveaux modules de visualisation et d'interaction. Actuellement, la plateforme LAAS-CNRS est en cours d'intégration à ce portail, permettant ainsi de gérer les expérimentations et d'explorer les résultats via des interfaces de visualisation 3D.

Nous présenterons l'avancement et les capacités actuels de la plateforme, son architecture et les nouvelles interfaces de visualisation, ainsi que les perspectives d'évolution.

PROGRAMME

16h30 - 16h50

Abdelhakim BAOUYA
(IRIT)

HERMES-Design: Human-CEntric CollaboRative Architectural Decision-Making for SEcure System Design

We developed a formal modeling framework that integrates human factors; expertise, constraints, and collaborative behavior into architectural decision-making for dependable cyber-physical systems. Using GPS satellite maintenance as a use case, we formally combined system design knowledge with team expertise through concurrent stochastic games. The resulting models, analyzed via PRISM-games, quantify reliability, availability, maintainability, and collaborative trade-offs between ground and orbital teams. Overall, the project produced two papers demonstrating how formal and human-centric modeling improves decision traceability, system security, and confidence in collaborative maintenance strategies.

16h50 – 17h00
FORMATION

16h50 -17h

Vincent NICOMETTE
(INSA Toulouse/ LAAS-CNRS)

PROGRAMME

Projet OSMOSE : Présentation de la réponse à l'AMI CMA « Cybersécurité »

Le projet OSMOSE (Occitanie – Sensibilisation et montée en compétence en sécurité), porté par l'Université de Toulouse, fort de 21 partenaires de toute l'Occitanie, est lauréat de l'AMI CMA Cybersécurité.
Ce projet, doté d'un budget de 10M d'Euros, dont 6M de subvention, est financé pour une durée de 5 ans. Cette présentation, faisant suite à son récent lancement, introduira les partenaires, explicitera l'organisation et définira les ambitions principales du projet.

17h00 - 17h30

DISCUSSION GÉNÉRALE - CONCLUSIONS

CONTACT

bureau@ico-occitanie.fr

https://www.ico-occitanie.fr

Liste de diffusion: diffusion@ico-occitanie.fr
Email : sympa@laas.fr - Objet : subscribe diffusion-ico-occitanie

https://www.linkedin.com/company/institut-cybers%C3%A9curit%C3%A9-occitanie/

Défis Clés OCCITANIE

La Région Occitanie Pyrénées - Méditerranée

ICO Institut Cybersécurité Occitanie