LE 12 JUILLET 2024

JOURNÉE SCIENTIFIQUE ANNUELLE DU DÉFI CLÉ INSTITUT CYBERSÉCURITÉ OCCITANIE (ICO)

SALLE DES SÉMINAIRES DU LIRMM

BÂTIMENT 4
LIRMM UMR 5506

161 RUE ADA
34095
MONTPELLIER

9h - 17h

Inscriptions

bureau@ico-occitanie.fr

Institut Cybersécurité Occitanie

cnrs

Défis Clés OCCITANIE

La Région Occitanie Pyrénées - Méditerranée

Programme

JUILLET
12

Accueil
9h - 9h30

9h30 - 9h45

Fabien LAGUILLAUMIE (LIRMM) - Mohamed KAÂNICHE (LAAS-CNRS)

Introduction

Présentation du Défi Clé "ICO"

9h45 - 10h45

Présentations des doctorants cofinancés par l'ICO (Première Partie)

Maximos SKANDALIS (LIRMM)

Détection des désinformations et détection automatique d'inférences textuelles et de contradictions : nouveaux jeux de données pour le français et l'intérêt des approches hybrides et logiques

9h45 -10h05

Les désinformations (fake news) sur les réseaux sociaux sont un enjeu sociétal majeur. La détection automatique de désinformations peut être abordée de manières différentes, plus ou moins subjectives. La détection automatique d'énoncés contradictoires est, à notre avis, l'un des moyens les plus objectifs et les plus neutres pour faire cela. Dans cet exposé, nous présenterons d'abord l'intérêt de la tâche de détection d'énoncés contradictoires en tant que tâche de classification de paires de phrases, et son lien avec la tâche d'inférence textuelle. Nous introduirons, ensuite, certains nouveaux jeux de données pour la détection automatique d'inférences textuelles et de contradictions en français. L'évaluation que nous avons réalisée sur ces jeux de données avec des modèles récents d'apprentissage profond a montré qu'ils constituent pour ces derniers un défi plus élevé que les jeux de données existants pour le français, qui sont déjà peu nombreux. Ces résultats mettent aussi en évidence l'intérêt des approches logiques basées sur des prouveurs de théorèmes automatiques, qui peuvent constituer une solution complémentaire pour aborder cette tâche. Ce dernier point nous amènera à présenter les méthodes logiques existantes qui ont été testées sur des phrases en anglais.

Antony DALMIÈRE (LAAS-CNRS/ UT3)

Les techniques de manipulation psychologique dans les attaques d'ingénierie sociale

10h05 - 10h25

Dans l'état actuel de la recherche, il est reconnu que les vulnérabilités constituent un point commun entre les systèmes d'information et les systèmes cognitifs. Des études ont mis en évidence que 82 % des fuites de données sont causées par le facteur humain. De plus, il a été constaté que le taux de réussite pour du phishing faiblement ciblé atteint 23 %. Ces chiffres soulignent l'importance de la vulnérabilité humaine dans la sécurité des systèmes. Les travaux de cette thèse visent à quantifier les techniques de manipulation psychologique utilisées à grande échelle. Parmi ces techniques, l'émotion, la motivation, la pression temporelle et la répétition sont les plus utilisées et mesurées, avec des taux d'utilisation significatifs dans la nature. La thèse permettra d'approfondir et de mettre des métriques d'utilisation de ces méthodes exploitant la vulnérabilité humaine.

Programme

JUILLET 12

Robin THEVENIAUT (IRIT/Carleton Univ., Canada)

Développement d'un outil intégrant les facteurs humains dans les prises de décisions collaboratives dans la conception d'architectures sécurisées

10h25 - 10h45

Au cours de cet exposé, je présenterai les premiers travaux effectués par mes encadrants sur le développement de cet outil ainsi que les contributions que j'ai pu y apporter depuis mon arrivée. Ces contributions portent notamment sur la création de métamodèles permettant de représenter respectivement l'architecture logicielle, les objectifs de sécurité, les facteurs humains pris en compte, la création des profils d'équipe, la gestion de la prise de décisions, la définition des décisions d'architecture sécurisée.

10h45 - 11h15

Pause

11h15 - 12h15

Présentations des doctorants cofinancés par l'ICO (Seconde Partie)

Van Tien NGUYEN (LAAS-CNRS / IMT Atlantique)

Toward Context-aware Security for Individual Information Systems

11h15 - 11h35

For a few decades, the multiplicity of Internet services humans consume are increasing, leading people to actually manage their own Individual-oriented Information System (IIS), whose server sides are spread over the internet and operated by different service providers. The security of such systems is essentially service-centric, while the user is the focal point of all their usage. If some user-centric solutions exist to date, they are either (1) restricted to some particular services, ignoring a global user activity, (2) intrusive, by requiring a complete instrumentation of user-side terminals, or (3) too specific by requiring the cooperation between the client interface and the server side. To cope with these limitations, we propose to develop a novel approach which consists in monitoring encrypted network flows issued by a user terminal and correlating this network activity with some external contextual information related to the user activity. Due to the lack of existing comprehensive datasets, our ongoing work consists in designing a long-term measurement campaign with real users using smartphones augmented with body sensors while facing security breaches such as malware activity or smartphone theft.

Programme

JUILLET
12

Gabin NOBLET (LAAS-CNRS / Cyblex Technologies)

Génération automatique de trafic d'attaque réseau réaliste : Approches et représentation du trafic

11h35 - 11h55

Étude approfondie sur la caractérisation du trafic réseau et le choix d'un modèle de données adapté à la génération de trafic. Les résultats de cette étude ont mis en évidence l'utilisation d'un autoencodeur VQ-VAE (Vector-Quantized Variational Autoencoder) comme une solution prometteuse pour la représentation de trafic réseau. Cette approche permet de transformer la représentation de la donnée de trafic de manière à ce qu'elle soit adaptée à l'utilisation de modèles génératifs, tout en préservant les caractéristiques importantes du trafic réseau.

Ziling LIAO (LIRMM)

Susceptibilité du SRAM d'un circuit STM32 aux injections de fautes par BBI (Body Bias Injection)

11h55 - 12h15

Aujourd'hui, la mise en œuvre de protocoles de sécurité repose sur des dispositifs intégrés, lesquels sont vulnérables à diverses menaces, notamment les attaques par injections de fautes. Les mémoires embarquées, qu'elles soient volatiles ou non volatiles, montrent une grande susceptibilité à ces attaques. Nos recherches ont démontré que par impulsion de tension dans le substrat (BBI), il est aisé d'injecter des fautes dans le contenu de SRAM d'un circuit STM32 pendant une opération d'écriture. De plus, on a constaté que la méthode BBI peut dévier le fonctionnement normal du circuit, par exemple en sautant des instructions ou en modifiant la valeur du compteur de programme (PC). Ces déviations peuvent potentiellement créer des vulnérabilités exploitables dans des programmes sensibles.

12h15 - 12h30

Formation et sensibilisation

Vincent NICOMETTE (INSA Toulouse, LAAS-CNRS)

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

Dans le cadre de France 2030, des appels à projets "Compétences et Métiers d'Avenir" ont été publiés. Ces appels sont relatifs à diverses thématiques, dont la cybersécurité. Le projet OSMOSE, à l'initiative de l'ICO et porté par l'Université de Toulouse, a pour objectif de répondre à cet appel pour la région Occitanie, dans le but de pouvoir former massivement la population d'Occitanie à la cybersécurité. Le projet compte réaliser de la sensibilisation pour le plus grand nombre, augmenter le flux de spécialistes mais aussi accroître l'attractivité des métiers et des filières de la cybersécurité. Les principales ambitions de ce projet, les partenaires et les différents Work Packages seront présentés.

12h30-13h30

Cocktail déjeunatoire

JUILLET

12

Programme

13h30 - 14h15

Conférencière invitée

Katharina BOUDGOUST (LIRMM)

A gentle introduction to lattice-based cryptography

Lattice-based cryptography is a rather recent research area which attracted a lot of interest in the last years. In particular through the encryption scheme Kyber and the two signature schemes Dilithium and Falcon, all three selected by NIST for standardization and all basing their security on lattice problems. But what exactly do we mean by lattice-based cryptography? The goal of today's talk is to give a gentle introduction to this exciting research field. We will see a (small-dimensional) lattice, what the hard problems are in this domain and how we can use them to build encryption schemes. We will conclude with a personal outlook of interesting open research questions.

14h15 - 14h55

Présentations des Post-Doctorants

Mario LAURENT (IDETCOM)

Analyse des discours radicaux sur les réseaux sociaux numériques: tendances actuelles

14h15 - 14h35

Notre projet ICO vise à identifier et caractériser les discours propres aux groupes classés comme radicaux en ligne en associant principalement sociologie et linguistique. Nous nous intéressons plus particulièrement à la plateforme X, anciennement Twitter, sur laquelle nous avons commencé à étudier les discours de haine racistes, anti-musulmans, dès 2018 dans le cadre de deux projets. Nous expliquerons en quoi ce média est singulier et préciserons que très récemment, les règles de la plateforme ont changé, affectées à la fois par les intérêts de son propriétaire et par les nouvelles lois mises en place (DSA). En l'état actuel de notre travail, nous verrons comment les stratégies discursives sont en permanence actualisées par les groupes radicaux, qui suivent certains codes usant souvent d'une grande sophistication. En résumé, après avoir évoqué la difficulté actuelle à obtenir l'accès aux données de X, nous évoquerons les évolutions actuelles des discours de haine et de manipulation mobilisés par des groupes radicaux racistes.

Programme

JUILLET 12

Daniele CANAVESE (IRIT)

Zero-Trust Explainable Autonomous Networks

14h35 - 14h55

An autonomous network is a network that operates with minimal or no human intervention. It can self-monitor, automatically protect, and reconfigure itself to withstand abnormal events such as cyberattacks or accidental failures. For instance, if a firewall is compromised, the autonomous network can detect the attack and react autonomously by isolating the compromised security control, reconfiguring another firewall, and redirecting the traffic to the new firewall.

The project of this presentation aims to build an autonomous network based on three key technologies:
- intents: high-level non-functional requirements used to declare a network's behavior, simplifying its management;
- explainable artificial intelligence: enabling intelligent actions and reactions that are human-interpretable;
- zero-trust paradigm: a security principle stating that "no one should be trusted" considerably hardens network security.

The presentation will first focus on the general architecture and concepts behind the project. The second part will be a deep dive into how intents and AI can inject security into a network by automatically redesigning it (e.g., inserting security controls and configuring them) and considering various cybersecurity principles (emulating a human cybersecurity architect).

14h55 - 15h10

Pause

15h10 - 16h10

Présentations des porteurs de projets scientifiques

Nan MESSE (IRIT)

BridgeSec: Facilitating Effective Communication between Security Engineering and Systems Engineering

15h10 - 15h30

As we increasingly rely on systems to perform reliably and securely, it is imperative that pertinent security aspects are properly considered in systems designs. However, achieving the security-by-design ideal is challenging. Security information is typically unstructured, disperse, hard to communicate, and its assessment is somewhat subjective and tacit. Furthermore, there is a need to accommodate and harmonise two knowledge-intensive practice areas: security engineering and systems engineering. We propose a conceptual interface – BridgeSec – to communicate security information between the two practice areas. BridgeSec facilitates the collaborative capturing and management of knowledge and information by systems engineering and security engineering teams. This empowers practitioners to develop robust and secure systems from the outset, making informed security-related decisions. First, we identify a concise information-exchange interface to systematically bridge the systems engineering and the security engineering perspectives. We describe and formalise how the information-exchange interface can be effectively used, allowing to reason about the security of systems designs. Next, we provide an open-source prototype – integrated into a threat modelling tool – which rigorously implements the interface and a reasoning mechanism. Finally, we detail two diverse and prominent applications of the interface for communicating security aspects of systems designs.

Programme

JUILLET 12

Abdelhakim BAOUYA (IRIT)

Measuring the Effectiveness of Collaborative Human Responses for Architecture Security Design with Stochastic Games

15h30 - 15h50

The project proposes a formal modeling framework for architectural decision-making, specifically considering the human factors of expertise and experience. By integrating these factors, the framework aims to enhance our understanding of collaborative decision-making processes and improve the traceability of security-critical decisions. Ultimately, this will lead to increased confidence in decisions made by diverse teams.

In this presentation, we focus on the second task of the project. We model the composition of attacks, system behavior, and human expertise within concurrent stochastic games, allowing formal techniques to assess system configurations and identify optimal security mitigation strategies.

Florent GALTIER (LAAS-CNRS)

Plateforme d'expérimentation pour la sécurité des objets connectés

15h50 -16h10

Dans le cadre du PEPR cybersécurité, le LAAS participe au projet Superviz. Superviz est un projet de recherche sur la thématique de la supervision de la sécurité. Les principaux axes de recherche sont traités dans 6 work packages : 1) identifier et gérer le risque, 2) détecter les attaques, 3) résister et répondre aux attaques, 4) rendre la supervision sûre, 5) concevoir des méthodes de validation des mécanismes de détection et 6) développer des plates-formes d'expérimentation. Une plateforme d'expérimentation est mise en place au LAAS dans le cadre de ce projet et elle concerne plus spécifiquement la sécurité des objets connectés. Elle intègre un ensemble d'objets connectés permettant de générique du traffic légitime, des équipements permettant d'exécuter des scenarios d'attaque et des sondes de collecte du traffic. Elle permet à un utilisateur de capturer des traces de traffic légitime et malveillant et de les soumettre à des algorithmes de détection d'intrusion. L'exposé décrira cette plateforme, ces objectifs et les expérimentations qu'il est possible de réaliser. Elle est partiellement financée par l'ICO.

16h10 – 16h50

Présentation du financement des ingénieurs pour des démonstrateurs et prototypes de recherche

JUILLET
12

Programme

Nathalie AUSSENAC-GILLES (IRIT)	***SEM4Trust : Améliorer la confiance dans les réseaux sociaux par des analyses sémantiques***	16h10 - 16h30

Les réseaux sociaux sont aujourd'hui les supports d'attaques envers les particuliers et les institutions, que ce soit en diffamant des personnes, en diffusant des rumeurs ou des contenus faux et négatifs, ou encore en utilisant les comptes des contributeurs pour s'introduire dans des machines ou des réseaux. Dans SEM4Trust, et suite à notre participation au projet européen Starlight, nous nous intéressons à la propagation de contenus malveillants. Plus précisément, nous souhaitons assister des tâches utiles dans le cadre d'enquêtes policières : l'analyse de conversations multiples, le repérage de certains types de discours (haineux, sexistes, violents, etc), ou l'identification/ caractérisation des auteurs. Pour cela, nous proposons une plateforme permettant de réaliser et croiser plusieurs types d'analyses de données de réseaux sociaux pour (i) représenter le contenu et les caractéristiques des conversations codées par des graphes de connaissances ; (ii) analyser le langage contenu dans les échanges présents sur ces réseaux mais aussi la structure et les paramètres caractérisant le contexte de ces échanges (membres des réseaux concernés, heures et dates des échanges, nature des données échangées, etc) ; (iii) choisir la ou les analyses à prendre en compte et visualiser leurs résultats pour en faciliter l'interprétation par les utilisateurs. Ces défis relèvent de la recherche en IA, plus précisément en traitement automatique des langues (TAL), analyse sémantique de contenus, ingénierie et représentation des connaissances sous forme de graphes.

Gwenaëlle DONADIEU (LIRMM, UM)	***NumDiag, un score de confiance de la protection des données***	16h30 - 16h50

Le Projet NumDiag vise à développer un logiciel d'analyse des risques d'atteinte aux données à destination des fabricants d'objets connectés et dont le résultat est un score de confiance à destination des utilisateurs. Fruit d'un projet de recherche interdisciplinaire au croisement entre l'informatique, le droit et les sciences comportementales, le logiciel NumDiag est actuellement en phase de prototypage et a bénéficié du soutien financier de l'ICO à double titre : pour l'organisation d'une manifestation scientifique ainsi que pour le recrutement d'un ingénieur.

16h50 – 17h

Conclusions

https://www.ico-occitanie.fr

bureau@ico-occitanie.fr

https://www.linkedin.com/company/institut-cybersécurité-occitanie/

@ICO_Occitanie

HAL https://hal.science/ICO-OCCITANIE/

Liste de diffusion: diffusion@ico-occitanie.fr

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

LIRMM

IRIT

LAAS CNRS

ICO Institut Cybersécurité Occitanie

cnrs

Défis Clés OCCITANIE

La Région Occitanie Pyrénées - Méditerranée