Janvier 2019
Numéro 1

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Edito du directeur

Meilleurs voeux pour cette année 2019, qui s'annonce particulièrement prometteuse pour le pré-GDR Sécurité Informatique. Pré-GDR ? "GDR" devrais-je dire, car la première bonne nouvelle de l'année est le passage au statut de GDR depuis le 1er janvier 2019.

Ce changement de statut marque la maturité de cette initiative lancée en 2016 par l'INS2I, et constitue une opportunité pour lancer de nouvelles initiatives. La première est devant vos yeux, il s'agit de la "Gazette du GDR", périodique bimestriel qui permettra à notre communauté de partager des informations. Un grand merci à Patrick Bas (CNRS / UMR CRIStAL) qui a accepté de prendre la responsabilité de la Gazette, à Annelie Heuser (CNRS / UMR IRISA) qui l'appuie dans cette tâche, et Solène Bernard (École Centrale de Lille / UMR CRIStAL) qui participe à la production du document.

L'année 2019 verra également la création d'un club de partenaires industriels, d'un conseil scientifique et la mise en place d'un nouveau site web. Évolution majeure, les groupes de travail *Sécurité des systèmes logiciels* et *Sécurité des réseaux et des infrastructures* vont fusionner pour renforcer les échanges au sein de ces deux communautés. Les futurs responsables, Aurélien Francillon et Olivier Levillain, vont travailler conjointement avec Carlos Aguilar Melchor et Jean-Yves Marion pour mener à bien cette fusion.

Au nom du bureau du GDR, je vous souhaite une excellente lecture. La Gazette est un outil pour la communauté, et par la communauté, alors n'hésitez pas à nous faire part de vos commentaires, questions et informations à partager.

Gildas Avoine

Rubriques

Événements

(repris en partie du forum du GDR)

Conférence "7th ACM Workshop on Information Hiding and Multimedia Security" *Paris (FR), 3-5 juillet 2019, soumission: 20 février*

Conférence "15th International Summer School on Training And Research On Testing" *Clermont-Ferrand (FR), 1-5 juillet, 2019*

Conférence "10th IFIP International Conference on New Technologies, Mobility and Security" *Canary Islands, Spain, 24-26 juin 2019, soumission: 20 février*

Conférence "32nd IEEE Computer Security Foundations Symposium" *Hoboken, NJ, USA, 25-28 juin 2019, soumission : 22 février*

Conférence "4th IEEE European Symposium on Security and Privacy", *Stockholm, Suède, 17-19, juin 2019*

Workshop "ENabling TRust through Os Proofs ... and beYond" *Stockholm, Suède, 16 June 2019, soumission: 11 mars*

Evénement "Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information" *Erquy (FR), 15-17 mai, soumission: 3 février*

Conférence "IEEE International Conference on Blockchain and Cryptocurrency" *Seoul, Corée, 15-17 mai*

Conférence "Tokenomics, International Conference on Blockchain Economics, Security and Protocols" *Paris (FR), 6-7 mai 2019*

Conférence "IEEE Man2Block International Workshop on Managing and Managed by Blockchain" *Washington DC, 12/04/19*

Conférence "5TH IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies" *Washington D.C., USA, 8 Avril 2019,*

GDR "Journée méthodes formelles pour la sécurité" *Paris (FR), 18 mars 2019*

En direct des labos

Philippe Gaborit

Philippe Gaborit, professeur à l'Université de Limoges et longtemps responsable du Master crypto dénommé Cryptis, travaille principalement sur les codes correcteurs et leurs applications à divers domaines : la cryptographie, le tatouage, le network coding, la théorie des nombres ou encore les codes ADN. La Gazette a choisi d'interviewer cet enseignant chercheur du XLIM au sujet de son expertise en cryptographie post-quantique.

Bonjour Philippe, peux tu nous expliquer pourquoi nous devons passer à la cryptographie post quantique ? Quand les attaques quantiques risquent-elles d'être une menace sérieuse ?

Alors que la cryptographie basée sur des problèmes de théorie des nombres comme la factorisation ou le logarithme discret était bien établie, Peter Shor des Bell Labs a proposé en 1994 un algorithme quantique permettant de résoudre le problème de la factorisation en temps polynomial.

Ainsi si nous possédions un tel ordinateur quantique avec suffisamment de 'qubits' (ndlr: n qubits permettant *dans certains cas* 2^n opérations simultanées), nous serions alors capable de casser facilement la grande majorité des systèmes cryptographiques utilisés dans les applications grand public. Bien sûr les algorithmes à clé symétrique comme AES seraient moins affectés, mais la cryptographie symétrique a besoin d'algorithmes d'échanges de clé comme l'algorithme de Diffie-Hellman qui eux seraient cassés.

> "La NSA dans une annonce en 2015 a exhorté l'administration américaine à passer à la cryptographie post-quantique"

Pendant des années le nombre de qubits pour un tel ordinateur a relativement stagné (de l'ordre de la dizaine de qubits) et puis ces dernières années, de grands groupes comme Google, IBM, Microsoft, Intel aux Etats-unis ou encore ATOS en Europe, se sont intéressés au sujet avec probablement en tête les applications de l'ordinateur quantique au Big Data. Nous avons alors vu le nombre de qubits pour un tel ordinateur passer en quelques années d'une dizaine de qubits à 72 qubits pour la dernière annonce, et cela évolue très régulièrement. Nous sommes encore loin des quelques milliers de qubits nécessaires pour casser les systèmes cryptographiques, mais disons que nous constatons une progression rapide.

Il est difficile de prévoir quand exactement il pourrait y avoir des attaques, mais la perspective devient plus probable à terme. Dans la mesure où il faut du temps pour faire évoluer les systèmes industriels, la NSA dans une annonce en 2015 a exhorté l'administration américaine à passer à la cryptographie post-quantique, post-quantique dans le sens qu'elle résisterait à un putatif ordinateur quantique, on parle aussi de cryptographie quantum résistante.

Philippe Gaborit

> "Être résistant à l'ordinateur quantique signifie en pratique, être basé sur un problème difficile qui ne puisse pas être relié à l'algorithme de Shor."

A ce stade il est important de comprendre qu'il existe peu d'algorithmes quantiques, et qu'en dehors de l'algorithme de Shor pour la factorisation, les algorithmes quantiques comme celui de Grover donnent une amélioration d'un facteur racine carrée et non logarithmique. Être résistant à l'ordinateur quantique signifie en pratique, être basé sur un problème difficile qui ne puisse pas être relié directement à l'algorithme de Shor. Pour résumer, les attaques sur les systèmes cryptographiques actuels ne sont pas pour demain, plus probablement d'ici une vingtaine d'années, mais il est important de préparer la transition dès maintenant car cela va prendre du temps. C'est dans cette optique que le NIST (institut des standards américains) a lancé un appel à standardisation sur la cryptographie post-quantique. La procédure de standardisation a commencé en novembre 2017 et doit s'étaler sur 4 ou 5 ans.

Puisque tu as participé au concours NIST, que peux-tu nous dire sur la compétition ? Qui évalue les méthodes ?

L'idée de l'appel à standardisation du NIST, même si elle est basée sur le même type d'appel que les compétitions précédentes pour l'AES et SHA3, est de nature différente. Ici l'idée n'est pas d'isoler un vainqueur unique, mais plutôt de mettre en avant plusieurs types d'alternatives possibles.

En effet, le nombre de problèmes difficiles et résistants au quantique n'est pas extensible et nous ne sommes pas non plus à l'abri de progrès sur un problème spécifique. Le NIST a fait un appel sur trois grandes classes d'algorithmes : le chiffrement, l'échange de clés et la signature. Le concours a commencé en novembre 2017, il y a eu 82 soumissions, dont 69 ont été recevables. Je suis personnellement impliqué dans 8 soumissions notamment avec des collègues d'INRIA, des universités de Limoges, de Bordeaux ou encore de Rouen, ainsi qu'un partenariat avec un industriel ATOS-Worldline. Parmi ces candidatures, il y a aussi des candidatures dans lesquelles interviennent des collègues étrangers basés aux États-Unis, en Allemagne ou en Israël, et où INTEL est impliqué. Je suis également impliqué dans des systèmes basés sur les codes correcteurs d'erreurs en métrique de Hamming ou bien en métrique rang (une métrique connue en cryptographie depuis 25 ans et qui permet d'obtenir des clés de taille plus petite qu'en métrique de Hamming).

Autre point intéressant : Google, qui a pris comme marqueur d'être à la pointe de l'innovation numérique, participe également au concours en proposant la solution NewHope. La procédure de standardisation a commencé en novembre 2017 et doit s'étaler sur 4 ou 5 ans.

Pour l'instant nous en sommes au premier tour, il y a eu une conférence de présentation des candidats en avril 2018. Les candidats passants au second tour devraient être connus en janvier 2019 (ndlr: à l'heure où nous publions la Gazette, les résultats ne sont toujours pas annoncés) avec une deuxième conférence pour la compétition après la conférence CRYPTO en août 2019. Nous ne savons pas encore combien il y aura de tours en tout. L'évaluation s'effectue à partir des retours d'autres cryptographes dans le monde mais comme pour les précédents concours, c'est le NIST qui décide à partir de ses propres analyses, probablement en se basant sur les retours de la communauté cryptographique.

Tout est complètement public, toutes les soumissions sont accessibles sur le site du NIST et il existe une liste publique où les personnes intéressées peuvent échanger sur chacun des candidats. Tous les détails peuvent se trouver à l'adresse : https://csrc.nist.gov/projects/post-quantum-cryptography/ .

Quelles sont les méthodes avec le plus d'avenir ?

Il y a essentiellement quatre grands types de problèmes durs utilisés en cryptographie post-quantique :

(1) les systèmes basés sur les réseaux euclidiens, (2) les systèmes basés sur les codes (métrique rang ou métrique de Hamming), (3) les systèmes basés sur la résolution de systèmes multivariés, et enfin, (4) les signatures basées sur les fonctions de hachage. Il existe aussi des approches plus récentes comme les systèmes basés sur les isogénies, mais là pour le coup il s'agit de problèmes pour lesquels il est difficile d'avoir le recul nécessaire. Chacun des grands types de problèmes a ses avantages et ses inconvénients.

Les systèmes basés sur les réseaux ont l'avantage d'avoir de très bonnes réductions de sécurité et de bons paramètres, il s'agit de candidats très sérieux, on peut citer notamment Kyber et NewHope pour le chiffrement et l'échange de clé ou encore Di-Lithium ou Falcon pour la signature. En codes correcteurs d'erreurs, il y a bien sûr le système de McEliece (Classic McEliece) mais qui utilise de très grosses clés, nous avons proposé avec BIGQUAKE une version avec des clés plus courtes à base de cyclicité. Il faut noter qu'au niveau réduction de sécurité pour les codes il y a eu récemment de très gros progrès obtenus et on arrive à avoir des systèmes à la fois très efficaces et très simples pour le décodage comme par exemple le système BIKE.

"Le concours a commencé en novembre 2017, il y a eu 82 soumissions, je suis personnellement impliqué dans 8 soumissions"

La métrique rang avec les systèmes RQC ou ROLLO (une réunion des soumissions LAKE, LOCKER et OUROBOROS-R) fait un peu figure d'outsider mais en terme de paramètres elle rivalise avec les systèmes basés sur les réseaux pour le chiffrement ou l'échange de clés.

Les systèmes multivariés sont surtout intéressants pour leur petite taille de signature, mais souvent les paramètres sont grands.

Enfin les signatures basées sur les fonctions de hachage ont l'avantage d'être uniquement basées sur la sécurité de ces fonctions. Elles donnent des signatures de grosses tailles mais ont l'avantage d'être simples et sont déjà très soutenues par les industriels américains.

Qui devrait gagner selon toi ?

Encore une fois il n'est pas prévu qu'il y ait seulement un seul gagnant mais plusieurs. Le NIST devrait probablement sortir une "short-list" de plusieurs systèmes basés sur différents types de problèmes, l'idée étant de ne pas mettre tous ses œufs dans le même panier et qu'il y ait des alternatives quoiqu'il arrive. Sachant que la phase d'industrialisation prend du temps, on parle souvent d'une dizaine d'années. Un détail intéressant, la communauté française est très présente sur la compétition avec des chercheurs fortement impliqués sur la plupart des soumissions les plus importantes notamment sur les réseaux, les codes ou le multivarié.

Merci Philippe, et bonne chance pour la suite !

Contact : *gaborit@unilim.fr*

Retour sur REDOCS

L'objectif des Rencontres Entreprises - Doctorants en Sécurité (REDOCS) est de créer des liens entre des entreprises du secteur de la sécurité informatique et des doctorants. Cette initiative s'inspire des Semaines d'Étude Maths Entreprises (SEME) créées en 2011 par l'Agence pour les Mathématiques en Interaction avec l'Entreprise et la Société (AMIES) et organisées trois à quatre fois par an dans diverses villes françaises.

Les REDOCS se déroulent en pension complète pendant une semaine afin de favoriser l'immersion dans le projet et les collaborations entre doctorants. Ainsi, les doctorants sont confrontés à des problèmes scientifiques proposés par les entreprises, problèmes issus du monde réel, aux frontières de la connaissance. Les industriels sont invités à proposer un sujet aux doctorants et ceux-ci se répartissent en groupes pour une semaine de travail.

Nuit REDOCS, 2016

Les trois premières éditions (REDOCS'16, REDOCS'17 et REDOCS'18) ont eu lieu au mois d'octobre au centre du CNRS de Gif-sur-Yvette. A chacune de ces éditions, il y a eu quinze doctorants sélectionnés pour leurs compétences et des entreprises expertes en sécurité informatique, grandes entreprises, agence gouvernementale ou PME. Les entreprises sont présentes le lundi des REDOCS pour présenter les sujets, puis le vendredi pour la restitution des résultats. Les entreprises ne sont pas présentes sur le site les mardi, mercredi et jeudi, mais elles offrent aux doctorants la possibilité de faire au moins un point téléphonique journalier. Tout au long de la semaine, les doctorants sont encadrés par le responsable des REDOCS, Pascal Lafourcade.
Comme en témoignent les enquêtes de satisfaction réalisées à la fin de chaque édition, aussi bien les doctorants que les entreprises ont apprécié cette expérience, qui constitue l'un des événements clés du GDR. A chaque fois et pour chaque problème proposé, les doctorants ont obtenu des solutions originales (voir les présentations des résultats disponibles sur les pages web de chaque édition de REDOCS). Les entreprises ont aussi apprécié découvrir de potentiels collaborateurs. Enfin d'après les fiches de satisfaction des doctorants, ils ont à l'unanimité vécu, lors de cette semaine intense, une expérience riche et unique.

"Aussi bien les doctorants que les entreprises ont apprécié cette expérience."

Pour les entreprises, les REDOCS sont un outil pour (i) établir ou renforcer des contacts avec le monde académique, (ii) obtenir des solutions originales à de vrais problèmes ouverts et (iii) identifier les candidats qui pourraient répondre positivement à une proposition d'embauche.

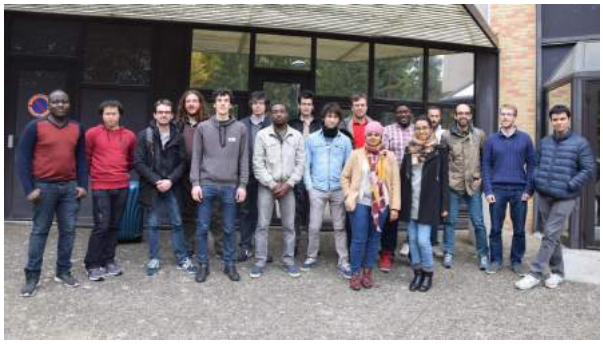
Pour les doctorants, les REDOCS constituent un moyen (i) de découvrir de manière active un sujet différent de celui de leur thèse, (ii) d'apprendre à travailler en groupe, (iii) de comprendre les contraintes d'une question scientifique lorsqu'elle est replacée dans un contexte industriel et (iv) de dialoguer avec des industriels qui ont choisi de faire de la recherche dans le monde de l'entreprise. Les REDOCS sont aussi un moyen pour les doctorants de sortir de leur routine journalière et de se surpasser car la semaine est physiquement éprouvante en raison des délais imposés.

Plusieurs doctorants ont ainsi fait remarquer qu'ils avaient apprécié la pression qu'ils ont eu aux REDOCS, qui contraste avec leur travail quotidien dans le cadre de la thèse. Enfin, les REDOCS permettent aux doctorants de valider des crédits pour leur école doctorale et les invitent à publier les résultats de leurs travaux sur HAL ou dans une conférence internationale, si les résultats obtenus le permettent.

Il n'y a pas de frais d'inscription aux REDOCS pour les doctorants et la pension complète leur est

"Les REDOCS sont aussi un moyen pour les doctorants de sortir de leur routine journalière."

offerte du dimanche soir au vendredi. Les équipes de recherche doivent toutefois participer en prenant en charge les frais de déplacement des doctorants. Depuis la seconde édition, les entreprises participent financièrement sous forme de sponsoring pour faire en sorte que l'événement reste gratuit pour les doctorants.



Edition 2016

Edition 2018

Edition 2017

Pour l'édition 2019 qui aura lieu à l'automne nous sommes dès à présent à la recherche d'entreprises partenaires (contact pour REDOCS)

Pascal Lafourcade, contact pascal.lafourcade@uca.fr

Sponsors des éditions 2017 et 2018

Le petit coin prospectif

Lucca Hirschi

Nous interviewons Lucca Hirschi, nouveau chercheur à INRIA Nancy Grand Est, qui a reçu le prix de thèse du GdR Sécurité en 2018. Les travaux de ce jeune chercheur portent sur le développement et l'application de méthodes formelles pour la vérification de protocoles cryptographiques ou encore la modélisation mathématique de la protection de la vie privée.

Bonjour Lucca, félicitations pour ton prix de thèse, peux tu nous dire quelles contributions ont été à l'origine de ce prix ? Peux-tu nous les présenter rapidement ?

Merci beaucoup ! Je vais tenter de résumer en quelques lignes les contributions de ma thèse qui m'ont valu ce prix. Il faut tout d'abord savoir que, malgré une apparente simplicité, les protocoles cryptographiques, qui utilisent des primitives cryptographiques (e.g., chiffrement, signature) pour sécuriser des communications (e.g., assurer la confidentialité ou l'anonymat), sont surprenamment difficiles à concevoir et constituent une source récurrente de vecteurs d'attaques. Pour s'assurer que ces protocoles remplissent leurs objectifs de sécurité, il est conseillé de faire appel à des techniques mécanisées de vérification formelle, si possible avant leur déploiement.

Ces techniques sont relativement bien développées dans le cadre des propriétés d'accessibilité telles que la confidentialité ou l'authentification.

Dans ma thèse, je me suis intéressé aux propriétés liées à la vie privée comme l'anonymat ou la non-traçabilité, exprimées comme des équivalences comportementales. J'ai développé des algorithmes et des outils pour vérifier ce type de propriétés de façon précise et efficace. Je les ai également mis en application sur des cas d'études industriels tels que le passeport électronique.

Lucca Hirschi

"J'ai beaucoup aimé combiner des travaux théoriques avec des applications très pratiques. Je trouve ça très motivant. "

Est-ce facile de concilier modèles formels théoriques et attaques pratiques ? Quelles sont les principales difficultés dans cet exercice ?

C'est compliqué. On a d'un côté un modèle mathématique avec une sémantique et un modèle d'attaquant formel, et de l'autre une spécification informelle sujette à interprétation, qui reste très souvent floue sur ses objectifs de sécurité, sur l'attaquant, et sur les cas limites du protocole. L'objectif est de formaliser une telle spécification en essayant de considérer toutes les interprétations valables de ceux qui implémenteront le protocole.
Ensuite, la plupart des outils que j'utilise ont le bon goût d'être corrects vis-à-vis de la falsification. C'est-à-dire qu'une attaque trouvée par un de ces outils est une attaque réelle contre la propriété spécifiée. Le vrai problème concerne l'autre sens : si un outil me dit que tout va bien, est-ce vraiment le cas ? La réponse est non. Ces techniques modélisent mathématiquement le protocole, l'environnement et l'attaquant : elles doivent donc faire des hypothèses qui ne sont pas forcément valides en pratique. C'est un problème insoluble. Notre objectif est d'apporter un niveau suffisant de garantie pour augmenter la confiance que l'on peut placer en ces protocoles.

"Comment modéliser mathématiquement la protection de la vie privée ? "

Que fais tu maintenant, sur quoi travailles-tu ? et quels sont tes prochains challenges ?

Je m'intéresse notamment aux protocoles de la téléphonie mobile (e.g., 5G) et à leurs impacts sur la vie privée, mais aussi aux protocoles de vote électronique et aux protocoles quantiques. Je travaille toujours sur la question de la modélisation mathématique de la protection de la vie privée et sur les méthodes pour la vérifier en pratique.

Quels conseils pourrais-tu donner aux étudiants de thèse travaillant en sécurité informatique ?

Ce domaine est très vaste, donc je trouve délicat de donner des conseils génériques. Personnellement, j'ai beaucoup aimé combiner des travaux théoriques avec des applications très pratiques. Je trouve ça très motivant. Idéalement, les deux extrêmes se stimulent l'un l'autre : les analyses pratiques révèlent des limitations et des imprécisions dans les techniques de vérification existantes et les développements théoriques apportent d'une part une meilleure compréhension des risques et des contre-mesures, et d'autre part des techniques systématiques et génériques pour analyser des protocoles.

Merci Lucca, bonne continuation !

Contact: *lucca.hirschi@inria.fr*

Jobs

(repris en partie du forum du GDR)

Rédacteur Latex pour la Gazette
La gazette recherche un doctorant "latex-gourou" pour aider l'équipe de rédaction à réaliser un modèle latex pour la gazette. Le doctorant retenu devrait pouvoir avoir une compensation en crédits auprès de son école doctorale.
Contact : Patrick Bas patrick.bas@centralelille.fr

Chercheur, *CEA Grenoble* *topic: design of tools for the vulnerability analysis of fault injection attacks, and tools for the automated application of countermeasures.*
Contact : Damien Couroussé damien.courousse@cea.fr

Stage Ingénieur, Master 2, Orange Labs Lannion, équipe PROF (Profiling et Data Mining) *titre: Génération de CRA synthétiques à l'aide de modèles en grilles et de chaînes de Markov, (5 mois: mars-juillet 2019).*
Contact : Françoise Fessant francoise.fessant@orange.com

Maître de Conférence, EURECOM *sur le thème de la sécurité et de la protection de la vie privée, une préférence sera donnée aux candidatures liées aux technologies suivantes:*
- Registres distribués,
- Preuves sans apport de connaissance,
- Anonymisation, confidentialité différenciée,
- Protocoles réseaux sécurisés,
Contact : Aurélien Francillon aurelien.francillon@eurecom.fr

Doctorant, Surrey Centre for Cyber Security & Surrey's 5G Innovation Center *5GTech-Sec: Security analysis of systems using emerging 5G Technologies, project: development of formal models, verification mechanisms and tools that are particularly suited for the verification of 5G systems,*
Contact : Dr Ioana Boureanu i.boureanu@surrey.ac.uk

Stagiaire de Master 2 ou en fin d'école d'ingénieurs *sujet : Détection d'intrusion à l'aide des techniques de machines learning, 6 mois, au plus tôt février 2019,*
Contacts : Gregory Blanc, Houda JMILA Gregory.blanc@telecom-sudparis.eu, Houda.jmila@telecom-sudparis.eu

Stagiaire de Master 2 ou en fin d'école d'ingénieurs, LIMOS, Université d'Auvergne
Sujet : l'Etude et analyse de risques d'attaques liées à la modification de données envoyées/reçues par des capteurs, 4 - 6 mois, adébut mars/avril suivant possibilités
Contacts : Laurençot Patrice , Salva Sébastien sebastien.salva@ucal.fr,laurencot@isima.fr

Stagiaire de Master 2 ou en fin d'école d'ingénieurs, laboratoire LIFO, INSA Centre Val de Loire *Sujet : Utilité et respect de la vie privée dans les données liées,, démarrant février/mars, Stage de M2 et bourse de thèse.*
Contact : Cédric Eichler cedric.eichler@insa-cvl.fr

Stagiaire de Master 2 ou en fin d'école d'ingénieurs, Télécom SudParis (Évry), Laboratoire SAMOVAR, Université Paris-Saclay *Sujet : Context-aware privacy protection in the Internet of Things, 5 - 6 mois, adébut mars/avril suivant possibilités.*
Contact : Sophie Chabridon Sophie.Chabridon@telecom-sudparis.eu

Doctorant, Surrey Centre for Cyber Security & Surrey's 5G Innovation Center *Objective: verify how human-machine teaming can help human users to make more informed decisions regarding security of cyber-physical systems (Only UK or French nationals are eligible).*
Contacts : Prof. Shujun Li , Prof Joaquin Garcia-Alfaro jgalfaro@ieee.org, S.J.Li@kent.ac.uk