RAPPORT D'ACTIVITÉ DIGITRUST

Citizen Trust in a Digital World

ÉDITO

Marine Minier
Professeure Université de Lorraine au Loria
Responsable scientifique du projet

2020 a été l'année du Covid-19 avec son lot de télétravail et de réunion à distance. Malgré cela, la belle cohésion que DigiTrust a su instiguer dans le domaine de la cybersécurité sur le site lorrain a réussi à se poursuivre !

2020 a été aussi l'année de l'explosion du vote électronique où nos chercheurs ont su s'illustrer. On peut citer ici notamment les résultats d'Enka Blanchard dont le système de vote co-réalisé avec le MIT est actuellement utilisé sur les campus américains.

Durant cette année, deux thèses DigiTrust ont également été soutenues. D'une part, la thèse de Margaux Duroeulx a renforcé les liens existants entre le CRAN et le LORIA en s'intéressant à des techniques informatiques issues du SAT pour modéliser et analyser les problèmes de fiabilité lorsque ceux-ci sont représentés par des arbres de fautes. D'autre part, la thèse de Béatrice Linot a renforcé les liens entre le LORIA et le 2LPN en étudiant la confiance dans les situations de travail collaboratifs médiatisés par des environnements numériques.

2020 a également été l'année de la signature du centre virtuel franco-allemand permettant de renforcer en matière de cybersécurité les liens entre le LORIA et le CISPA (Saarbrücken, Allemagne). Ainsi, quatre chaires ont été définies autour des problématiques de cybersécurité. Elles mettent en avant un chercheur côté français et un chercheur côté allemand. D'ailleurs, deux workshops ont déjà eu lieu depuis et ont bien su démontrer l'intérêt d'une telle démarche autour de thèmes de recherche prédéfinis.

Cet accord montre l'importance que LUE accorde à la coopération transfrontalière de la Grande Région. Localement, DigiTrust a été également impliqué dans l'Incubateur Lorrain et le club des partenaires IT ainsi que dans le conseil pour la création de deux start-ups. Nous n'oublions pas notre double mission enseignement/recherche car DigiTrust a également labellisé la nouvelle licence professionnelle de cybersécurité de l'IUT Nancy-Brabois.

DigiTrust a démarré en septembre 2018 et ce pour une durée de quatre ans. Ainsi, à mi-parcours, DigiTrust a permis de renforcer les liens des laboratoires impliqués notamment à travers les thèses en co-tutelles où plusieurs laboratoires sont impliqués.

Jean-Yves Marion
Directeur du LORIA

La révolution numérique concerne la science, s'invite dans nos vies privées et s'applique globalement à toute la société. Or ce colosse a des pieds faits d'argile à cause de la cyber-insécurité et son lot de cyber-attaques incessantes et en augmentation. Au-delà des délits, les risques cyber menacent notre vie privée par un traçage abusif de nos actions, les entreprises en exfiltrant des informations ou en les bloquant, et surtout nos démocraties.

Il faut dès lors avoir la capacité de concevoir des systèmes numériques sûrs, et de protéger nos systèmes et leurs applications des cyber-attaques. Pour cela, il faut une ingénierie solide, de l'innovation et une recherche libre de pouvoir explorer toutes les directions possibles. Le projet DigiTrust permet de mettre en œuvre ces trois facettes avec des équipes qui proviennent de plusieurs disciplines scientifiques.

Dans ce dispositif, le LORIA joue un rôle central avec des chercheurs reconnus tant au niveau national qu'au niveau international. Le projet DigiTrust sort de nos frontières avec des liens forts et privilégiés avec le Luxembourg et l'Allemagne (CISPA) et avec des projets structurants au niveau européen comme CONCORDIA.

SOMMAIRE

CHIFFRES-CLÉS / *KEY FIGURES*

6 LABORATOIRES DU SITE LORRAIN / 6 LABORATORIES

2LPN · Bureau d'économie théorique et appliquée (BETA) UMR 7522 · CRAN · Institut Élie Cartan · IRENEE · Loria

PARTENAIRES PUBLICS / PUBLIC PARTNERS

cnrs · Inria · Université de Lorraine · Universität des Saarlandes · uni.lu Université du Luxembourg

BUDGET

2,5 millions €

FORMATION

Création d'une licence pro
Cybersécurité et Cyberdéfense

IMPACT ÉCONOMIQUE ET SOCIAL

Cartographie de la cybersécurité /
Cybersecurity regional map
2 start-ups soutenues /
2 supported startups

PERSONNEL / *STAFF*

45 Membres permanents /
Permanent Members

13 groupes de recherche
research groups

11 doctorants
(thèses financées et en cours)
on-going and financed theses

4 jeunes chercheurs
et ingénieurs recrutés
young researchers as post-doc
and engineers

1 chaire d'excellence en
collaboration avec CISPA
chair of excellence in collaboration
with CISPA

PUBLICATIONS

70 productions scientifiques
scientific papers

>300 publications scientifiques en cybersécurité
(2019-2020)

hal.archives-ouvertes.fr/IMPACT-DIGITRUST

10 événements d'ampleur locale,
nationale et internationale

Parmi eux, la signature d'un accord entre le LORIA et notre partenaire allemand CISPA. Une lettre d'accord à l'appui de cette construction a été signée par Michael Backes, directeur scientifique du CISPA, et par Karl Tombre, directeur exécutif de LUE.

LE PROJET

DIGITRUST AU SEIN DE L'INITIATIVE LORRAINE UNIVERSITÉ D'EXCELLENCE (LUE)

Le projet ***Citizen Trust in the Digital World*** (acronyme DigiTrust) fait partie de la dernière vague des projets IMPACT au sein de l'initiative Lorraine Université d'Excellence (LUE) proposée dans le cadre de l'appel d'offres PIA2 IDEX/I-SITE. Il été lancé en avril 2019 et son ambition est de construire la confiance des citoyens dans le monde numérique autour de quatre axes de recherche.

CONTEXTE

La révolution numérique a un impact fondamental sur la vie quotidienne, notamment sur la façon dont les citoyens s'informent, communiquent et s'organisent. Cette révolution a également modifié la fabrication et l'approvisionnement en biens et en énergie, la conception des villes, les infrastructures de transport, et même l'administration et la vie politique. De nouveaux paradigmes tels que les villes intelligentes, la fabrication ou l'utilisation des objets connectés (IoT) reposent sur une communication connectée en permanence à toutes les échelles, ce qui accroît encore la dépendance de la société moderne à l'égard des technologies numériques.

En 2020, on s'attendait à ce que 30 milliards d'objets intelligents soient utilisés. Le potentiel économique, sociétal et culturel apporté par cette révolution numérique est, toutefois, accompagné de menaces dues à des cyber-attaques et à la divulgation de données privées. Néanmoins, pour de telles utilisations, il est nécessaire que le citoyen ou le consommateur aient un fort niveau de confiance vis-à-vis de ces technologies.

Pour cela, le projet LUE DigiTrust vise à mener des recherches autour de la sécurité informatique telles que sur les usines et villes intelligentes, capteurs, caméras, téléphones mobiles, montres, équipements de maison, de voiture, de santé. Afin de répondre à ces défis et de contribuer à préserver la confiance des citoyens peuvent avoir dans le numérique, DigiTrust encourage la recherche interdisciplinaire basée sur la complémentarité des expertises présentes dans les entités de l'Université de Lorraine et de ses partenaires. La conception d'approches globales vise à assurer un degré élevé de sécurité contre la malveillance et vers des garanties certifiables de respect de la vie privée. L'objectif scientifique global est la conception, l'analyse et la mise en œuvre des systèmes numériques auxquels la société civile peut faire confiance pour résister aux attaques et pour protéger les biens contenus dans ces systèmes.

BACKGROUND

DigiTrust is a funded LUE project at the heart of the ongoing digital revolution. This digital revolution impacts everyday life, including the ways citizens inform and entertain themselves, communicate and organize, stay healthy. However, due to the increase in the utilization of smart objects, attacks on computer networks have been mounted. In order to respond to the challenges and help preserve the trust citizens can place in their digital environment, DigiTrust is to foster interdisciplinary research based on the complementary expertise present in different entities of the Université de Lorraine and its partners. This interaction contributes to the design of comprehensive approaches towards demonstrably high degrees of safety against malicious attacks and towards certifiable guarantees of privacy.

ORGANISATION / *ORGANIZATION*

COMITÉ OPÉRATIONNEL

Le comité opérationnel du projet est composé de Marine Minier, directrice scientifique et d'un chercheur correspondant à chaque volet scientifique et/ou chaque laboratoire partenaire. Au total, treize chercheurs associés au **LORIA, CRAN, 2LPN, BETA, IRENEE** et **IECL** composent ce comité. De plus, un chef de projet est en charge de l'animation opérationnelle et assure la communication de manière étroite avec le comité de pilotage et la cellule LUE. Ce comité coordonne les actions menées au sein des différents axes de recherche de DigiTrust, décide l'allocation des ressources en tenant compte de l'intérêt scientifique, de l'impact socio-économique, des aspects multidisciplinaires et de la compétitivité internationale et assiste le responsable scientifique et le chef de projet dans la prise de décision sur l'orientation du projet.

COMITÉ SCIENTIFIQUE

Le comité scientifique est composé de la directrice scientifique, un représentant de chaque institution (CNRS, Inria, Université de Lorraine), les directeurs des laboratoires partenaires de DigiTrust et quatre autres chercheurs renommés dans le domaine scientifique et/ou représentant des partenaires socio-économiques de DigiTrust. Son rôle est d'assister la directice scientifique dans la définition des priorités et suggérer des interactions inédites, en tenant compte des orientations des institutions participantes et du contexte international de la recherche. Le conseil scientifique se réunit une ou deux fois par an. Des chercheurs renommés dans le domaine de la cybersécurité comme Gildas Avoine (INSA Rennes), Hervé Debar (Institute polytechinique de Paris), Ludovic Mé (Centrale Supélec), Olivier Bettan (Thales) et Radu State (Université de Luxembourg) ont déjà participé au comité scientifique.

OPERATIONAL COMMITTEE AND A SCIENTIFIC COMMITTEE

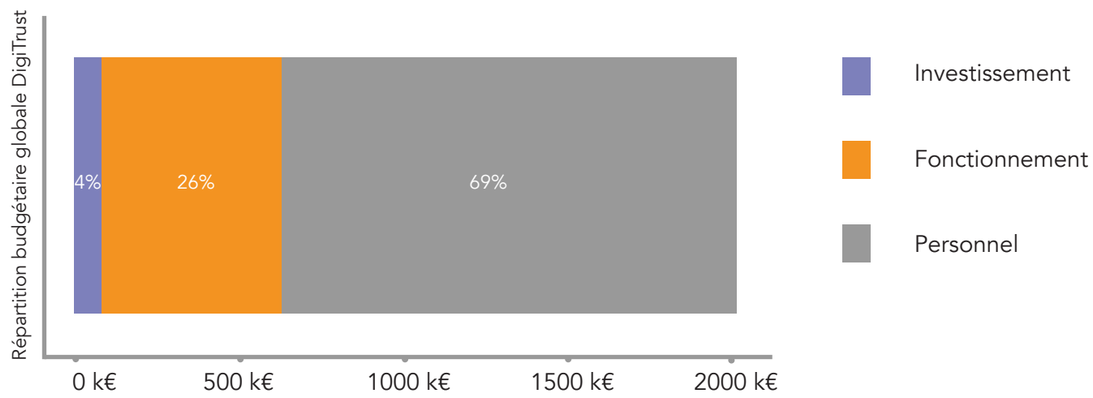
DigiTrust is organized as follows: an **operational committee** formed by Marine Minier, scientific leader for the project and at least one representative of each laboratory in the consortium. A project manager is in charge of planning, organizing, and directing the project for a time, budget and scientific organization. The operational committee coordinates the actions carried out within the different research axes of DigiTrust, decides on the allocation of resources taking into account the scientific interest, the socio-economic impact, the multidisciplinary aspects and the international competitiveness, and assists the scientific manager and the project leader in making decisions on the orientation of the project.

The role of the **scientific committee** is to assist the scientific leader in setting priorities for research subjects and suggesting novel interactions, taking into account the orientations of the participant institutions and the international research context. It is composed by the scientific leader, the project manager, a representative of each participating institution, the directors of the partner laboratories of DigiTrust, two members external to the site of University of Lorraine, chosen for their international recognition in the scientic field, and/or two members representing the socio-economic partners of DigiTrust.

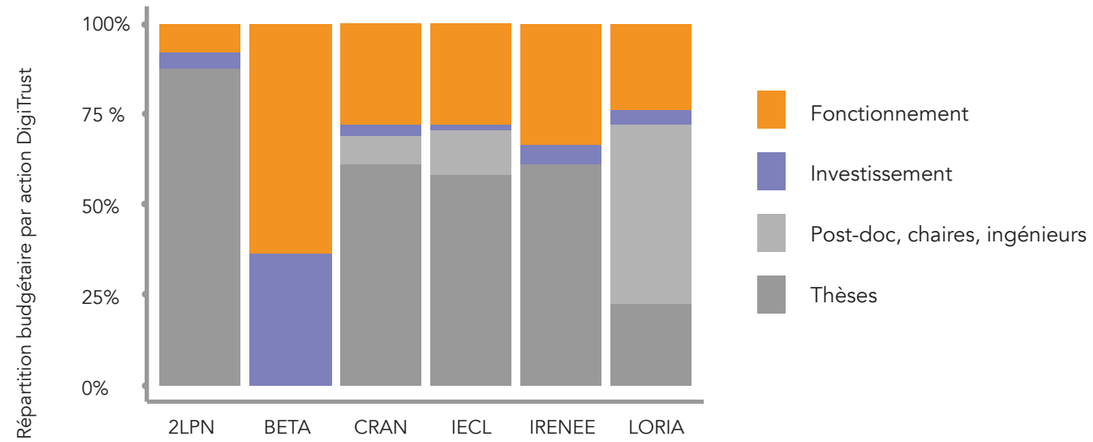
Journée de lancement du projet, avril 2019

BUDGET

La répartition budgétaire DigiTrust peut être visualisée avec les diagrammes ci-dessous. Au total, Lorraine Université d'excellence (LUE) a affecté environ 2442 K€ à DigiTrust pour une durée de 48 mois. La masse salariale correspond à environ 70% des dépenses suivie par 26% du budget destiné au fonctionnement (recherche, missions, participations aux évènements) et 4% à l'investissement (matériel et équipement). Chaque laboratoire membre a réparti son budget alloué en accord avec ses actions.



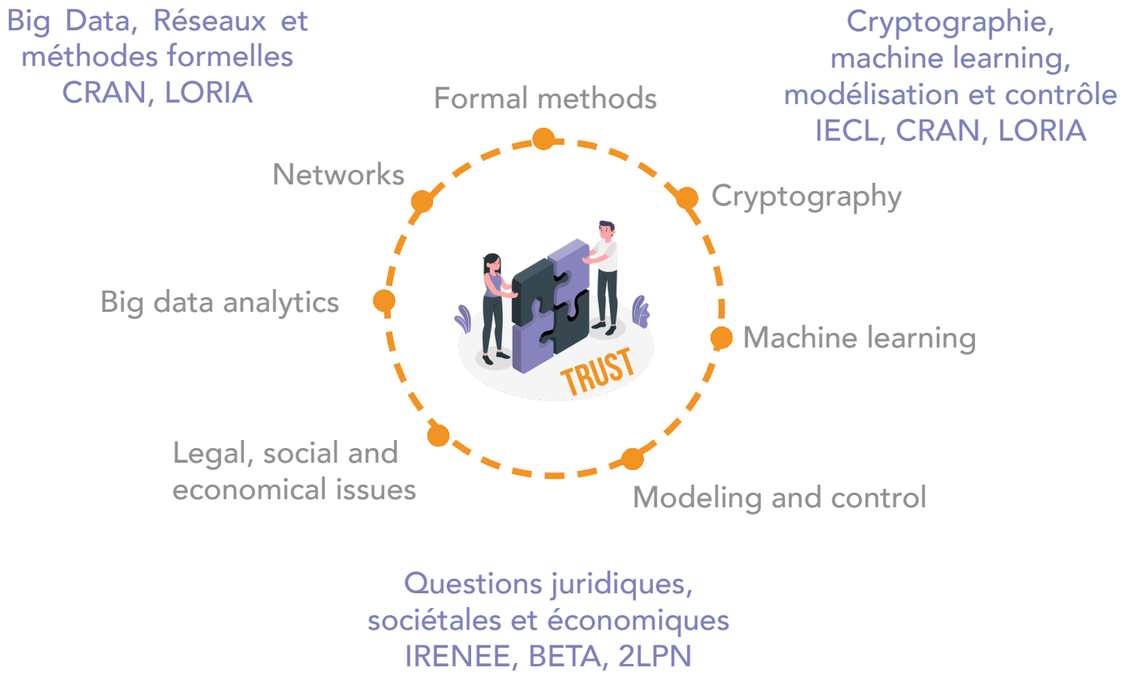
Répartition budgétaire quantitative du projet DigiTrust en fonction des actions (ordonnée) x le financement destiné en euros (abscisse) / *DigiTrust budget distribution according to the actions (ordinate) x the intended funding in euros (abscissa).*



Répartition proportionnelle du budget total attribué à chaque laboratoire partenaire en fonction des actions / *Proportional distribution of the total budget allocation to each partner laboratory according to their actions.*

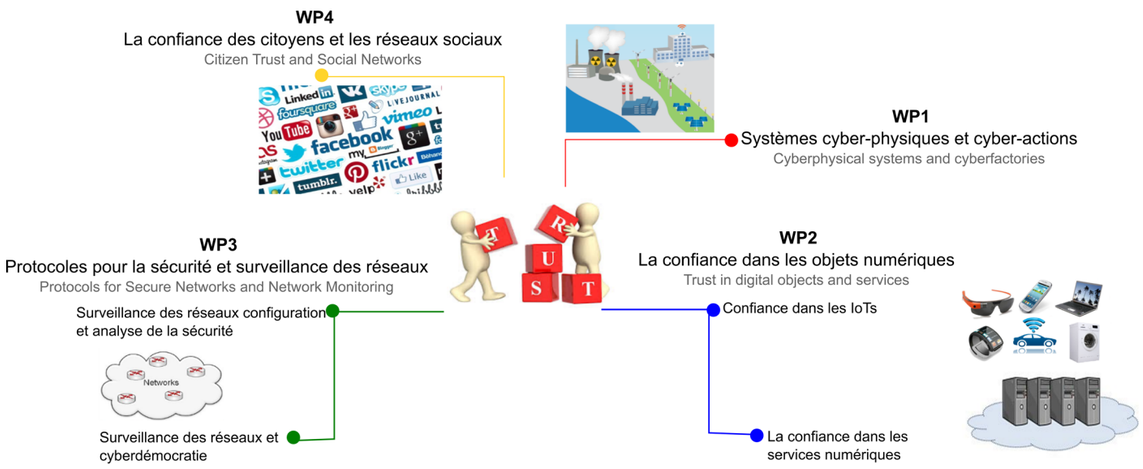
The DigiTrust budget can be visualized with the diagrams above. In total, LUE has allocated approximately 2442 K to DigiTrust for a period of 48 months. The payroll corresponds to about 70% followed by 26% of the budget for operations (research actions, professional meetingsas conferences and workshops) and 4% for investment (material and equipment). Each member laboratory has allocated its budget in accordance with its actions.

CONSORTIUM



THÉMATIQUES DE RECHERCHE / *RESEARCH AXES*

Concernant la recherche, le projet DigiTrust comporte quatre axes (WP). Ces axes ont été définis par les défis applicatifs dans le vaste domaine des systèmes numériques. Chaque membre du consortium apporte son expertise pour répondre aux problèmes spécifiques posés dans chacun de ces axes.



The DigiTrust project consists of four axes, illustrated on page 8. These axes are defined by applicative challenges in the broad area of digital systems. Participants from the different laboratories bring their respective expertise to respond to the specific problems raised within each of these axes.

WP1: CYBERPHYSICAL SYSTEMS AND CYBERFACTORIES

To encompass systems ranging from IoT contexts to manufacturing and organisms of vital importance including transportation, supplies of energy, gas and water, hospitals, banks or services of public safety. The security of those systems is critical, and attacks on the distributed equipments that communicate through public networks can have disastrous consequences on the economy and the life and well-being of persons. In order to assess and increase the resilience of these systems, DigiTrust participants develop and apply formal methods and control engineering techniques for testing, verifying, and certifying systems against security threats.

WP2: TRUST IN DIGITAL OBJECTS AND DIGITAL SERVICES

In this axis of DigiTrust, we focus on trust in small, smart objects for use in everyday life (IoT) that interact with services provided remotely, in the cloud.

By digital objects, we refer to everyday connected smart objects that users carry with them or install in their personal environment (e.g., homes or cars), whereas digital systems designate servers that objects connect to and that provide always-on services. The ubiquity of these objects and systems, and their vulnerability to technological and socially engineered attacks, provide an attractive attack surface that can lead to denial of service or loss of private data.

Challenges in this context are the design of digital investigation, the use of big-data methods such as machine learning for detecting and diagnosing attacks from system logs, as well as reverse code analysis for detecting malware.

WP3: PROTOCOLS FOR SECURE NETWORKS AND NETWORK MONITORING

Networks form the backbone of the connected digital world: they support the communications among users and devices that interact with each other and with servers. They both enable the services that citizens and businesses rely on, and they are the vectors of attacks. The DigiTrust project works on two complementary topics: the design and analysis of protocols for secure networks, and the monitoring and security management of communication networks.

WP4: CITIZEN TRUST AND SOCIAL NETWORKS

This axis of DigiTrust focuses on technological and societal measures that contribute to improve the trust that citizens place in connected systems and services. We intended to develop two complementary aspects. The first one focuses on the transparency of algorithms that helps explain how resources are allocated and how results and recommendations are obtained. The second aspect concerns the problems of identifying and remedying vulnerabilities of privacy in social networks

WP1 - SYSTÈMES CYBER-PHYSIQUES ET CYBER-ACTIONS

Malgré des collaborations régulières entre le CRAN et le LORIA, jamais à ce jour le thème de la sécurité n'avait été abordé de manière conjointe et significative. L'initiative LUE a eu indéniablement un effet structurant à ce titre. DigiTrust a permis d'élargir les domaines d'interactions entre ces deux laboratoires. En particulier, DigiTrust a favorisé le croisement original de l'automatique, de la théorie du contrôle et de la cryptographie.

Gilles MILLERIOUX, CRAN

Les systèmes cyber-physiques (CPS) associent le monde physique et numérique. On dénomme sous cette terminologie tout système physique piloté par des équipements informatiques. Présents dans les domaines des transports, de la santé, de l'énergie, les CPS occupent une place centrale dans notre vie quotidienne. Les opérateurs d'importance vitale comme les hôpitaux, les fournisseurs d'énergie, acteurs majeurs dans ces secteurs, leur accordent une attention privilégiée. Les CPS sont tout aussi présents dans le domaine de la production et sont des éléments caractéristiques de l'Usine du Futur. Les interactions au sein d'un ou plusieurs CPS requièrent des échanges de données qui s'opèrent majoritairement au travers de réseaux publics. Ils sont donc exposés à des attaques aux conséquences économiques potentiellement désastreuses et pouvant mettre en danger des vies humaines. On mentionnera à ce titre la cyber-attaque paralysant la centrale nucléaire de Bouchehr en Iran via le virus Stuxnet.

Pour faire face à la vulnérabilité des CPS et renforcer la confiance dans ces systèmes, les échanges et interactions doivent être sûrs, privés et sécurisés. Ce sont précisément les objectifs de cet axe du projet DigiTrust. Cet axe s'appuie sur des expertises complémentaires, tout particulièrement celles du LORIA pour les méthodes formelles et celles du CRAN pour la théorie du contrôle et le diagnostic. Il bénéficie également des avancées issues des autres axes de Digitrust, en matière de cryptographie, d'analyse des journaux et des logiciels malveillants, ou encore de vérification des protocoles.

THÈSE

SYNTHÈSE DE NOUVEAUX AUTOMATES À ÉTATS FINIS DÉCRITS PAR UNE REPRÉSENTATION MATRICIELLE : APPLICATION À LA CRYPTOGRAPHIE (2019-2022) - HAMID BOUKERROU

SOUS LA DIRECTION DE MARINE MINIER (LORIA- ÉQUIPE CARAMBA) ET GILLES MILLERIOUX (CRAN - DÉPARTEMENT CID, CONTRÔLE IDENTIFICATION DIAGNOSTIC)

Depuis le mois d'octobre 2019, j'ai entrepris la préparation d'une thèse dans le domaine de la cryptographie. L'essor considérable des technologies de l'information et de la communication, dans le contexte actuel de la révolution numérique et de l'Internet des Objets, nécessite de renforcer la sécurité des échanges. Tous les secteurs sont concernés, les systèmes embarqués et les équipements mobiles, les véhicules autonomes mais aussi les grands systèmes comme les villes intelligentes ou les systèmes de distribution de l'énergie électrique dénommés « smart-grids ». Cette transformation numérique touche également les équipements de contrôle industriel. Ces derniers intègrent des réseaux où capteurs, actionneurs et superviseurs sont connectés, constituant les systèmes SCADA, doivent faire face à présent à de multiples menaces de piratage informatique. Dans ce contexte, la cryptographie joue un rôle majeur. Mes travaux portent sur la cryptographie symétrique. L'objectif est d'élaborer de nouvelles architectures de chiffreurs dans la classe particulière des chiffreurs symétriques à flot appelés auto-synchronisants. Le travail repose sur des concepts issus de la théorie du contrôle et des systèmes dynamiques. Les systèmes dynamiques admettent des modèles décrits par des automates à nombre d'états finis. L'analyse de la sécurité des architectures proposées est également menée.

ZOOM SUR LES ALUMNI

Alumni

THÈSE SOUTENUE : ÉVALUATION DE LA FIABILITÉ DES SYSTÈMES MODÉLISÉS PAR ARBRES DE DÉFAILLANCES GRÂCE AUX TECHNIQUES DE SATISFIABILITÉ - MARGAUX DUROEULX

SOUS LA DIRECTION DE NICOLAE BRÎNZEI (CRAN, ÉQUIPE ISET) ET STEPHAN MERZ (LORIA, ÉQUIPE MOSEL-VERIDIS)

L'étude de la fiabilité des systèmes vise à établir la probabilité de la défaillance d'un système pendant un intervalle de temps donné. Elle prend en compte l'architecture du système et détermine quelles combinaisons de défaillances de composants de base (souvent redondés pour augmenter le niveau de fiabilité) conduisent à ce que le système ne puisse plus fonctionner. La thèse de Margaux Durœulx propose d'utiliser des techniques issues des méthodes formelles et plus précisément de satisfiabilité propositionnelle pour gérer cette combinatoire qui peut être statique ou dynamique, dans le sens que l'ordre de défaillance de composants influe sur la défaillance du système. C'est grâce à ce mélange de méthodes provenant de l'automatique et de l'informatique symbolique qu'il est possible d'entrevoir l'analyse de grands systèmes industriels avec de multiples causes de défaillance.

WP2- LA CONFIANCE DANS LES OBJETS ET SERVICES NUMÉRIQUES

En permettant le financement et l'accompagnement d'une thèse de doctorat conjointe, le dispositif LUE a fourni une très belle opportunité de mise en commun des compétences et connaissances, tant théoriques que méthodologiques, relevant de la psychologie-ergonomie (CNU 16) et de l'informatique (CNU 27). La complémentarité a été un atout indéniable pour la réalisation de la thèse de Béatrice Linot et a reposé sur un dialogue permanent, non seulement entre les encadrants, mais également entre les disciplines. »

Jérôme DINET (2LPN)

Les objets numériques sont soit des objets intelligents connectés transportés ou installés par exemple en maison ou en voiture, alors que les systèmes numériques désignent les serveurs qui leur fournissent des services. L'ubiquité de ces objets et systèmes, ainsi que leur vulnérabilité aux attaques technologiques et sociales, offrent une surface d'attaque attrayante qui peut conduire à un déni de service ou à la perte ou au vol de données privées. Il faut s'assurer de la sécurité de chaque équipement, de chaque serveur, et de leurs liaisons.

L'expertise des laboratoires impliqués dans DigiTrust en matière de cryptographie et de logiciels malveillants est donc essentielle pour mener à bien cette tâche qui recoupe de multiples aspects : mise en place de chiffrements avec des contraintes d'énergie et de mémoire, de la sécurité des transmissions, analyse des données pour détecter des attaques en temps-réel, travailler l'ergonomie des systèmes et les interactions avec l'utilisateur pour que les enjeux de sécurité soient bien compris. De plus, DigiTrust vise également à renforcer la confiance dans le cloud et les environnements collaboratifs. Le projet s'intéresse à la manière dont la technologie de stockage et de transmission d'informations doit rester transparente, sécurisée, privée voire décentralisée.

POST-DOC

KÜBRA BENLI - IECL, ÉQUIPE D'ANALYSE ET THÉORIE DES NOMBRES (05/2021-09/2021)

I obtained my PhD in Mathematics at the University of Georgia in August 2020. My main research interest is Analytic Number Theory and my PhD thesis was based on distribution of special types of prime numbers in certain ranges. Since May 2021 (until September 2022), I have been a postdoctoral fellow at IECL, working under the ARITHRAND project. My objective during my time at the University of Lorraine is extend my earlier results and get a new perspective on the problems worked by the members of the community. In particular, I have been working on bounding different types of exponential sums in order to obtain the uniform distribution results on certain sequences.

THÈSE

ANALYSE DU FLOT DE DONNÉES DANS LES MALWARES. CARTOGRAPHIE DES FONCTIONNALITÉS ET LEURS CORRÉLATIONS. (2019-2022) - TRISTAN BENOIT

SOUS LA DIRECTION DE JEAN-YVES MARION (LORIA, ÉQUIPE CARBONE) ET GUILLAUME BONFANTE (LORIA, ÉQUIPE CARBONE)

Des méthodes d'apprentissage automatique sur les graphes de flots dans le but de classifier un exécutable ont été établies. Premièrement, l'apprentissage sur les graphes se fait par la convolution sur les graphes qui est un analogue de la convolution sur les images. Secondement, les graphes de flots étant trop volumineux, ils sont réduits d'abord en conservant uniquement les instructions liées au flot puis par la sélection d'un nombre fixe de petits graphes. Ces méthodes sont utilisées pour prédire les outils ayant servi à produire un exécutable. Afin d'évaluer la prédiction, des dizaines de milliers d'exécutables ont été compilés avec différents outils. Afin d'affiner l'analyse, le langage assembleur est étudié par apprentissage automatique. De plus, de nouvelles méthodes d'apprentissage, via la prédiction de lien, sont étudiées pour comprendre un graphe de flot. En combinant toutes ces méthodes d'apprentissage et en relation à des méthodes classiques d'analyse, une cartographie des programmes malveillants sera établie.

THÈSE

SUITES AUTOMATIQUES ET MORPHIQUES DE GRANDE COMPLEXITÉ LE LONG DES SOUS-SUITES (2019-2022) - PIERRE POPOLI

SOUS LA DIRECTION DE DAMIEN JAMET (LORIA, ÉQUIPE ADAGIO) ET THOMAS STOLL (IECL, ÉQUIPE D'ANALYSE ET THÉORIE DES NOMBRES)

Les suites automatiques sont des suites déterministes et ne sont pas de bonnes suites pseudo-aléatoires. En effet, il existe plusieurs mesures pour déterminer si une suite peut être qualifiée de pseudo-aléatoire ou non. Pour les suites automatiques, il est connu que leur complexité en sous-mots est linéaire et cela ne peut pas correspondre au profil d'une suite pseudo-aléatoire. Cependant cette suite possède une mesure de complexité d'ordre maximal large et nous informe que cette mesure n'est donc pas suffisante en pratique pour construire des suites pseudo-aléatoires. De récents résultats montrent cependant que si la suite de Thue-Morse est étudiée le long des carrés les mesures peuvent changer radicalement. Les objectifs de la thèse sont donc d'étudier ce phénomène de raréfaction des suites automatiques et morphiques pour améliorer leurs applications en cryptographie.

- Popoli, On The Maximum Order Complexity Of Thue-Morse And Rudin-Shapiro Sequences Along Polynomial Values, Uniform Distribution Theory 15(2), 2020

- Damien Jamet, Pierre Popoli, Thomas Stoll. Maximum order complexity of the sum of digits function in Zeckendorf base and polynomial subsequences. Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences , Springer, 2021

ZOOM SUR LES ALUMNI

Alumni

THÈSE SOUTENUE : CONFIANCE DANS LES SITUATIONS DE TRAVAIL COLLABORATIFS MÉDIATISÉS PAR DES ENVIRONNEMENTS NUMÉRIQUES, BÉATRICE LINOT

SOUS LA DIRECTION DE JÉRÔME DINET (LABORATOIRE 2LPN) ET FRANÇOIS CHAROY (ÉQUIPE COAST, LORIA)

Quelle que soit l'origine d'une catastrophe (catastrophe naturelle, explosion industrielle, attaque terroriste, etc.), la rapidité avec laquelle les différents services de secours et d'aide interviennent est déterminante pour limiter le nombre de victimes. Aujourd'hui, la coordination de ces différents services passe par des outils numériques dont les utilisations ne sont pas sans poser problème (conscience partagée de la situation, confiance dans les données échangées, confidentialité et rapidité des transmissions, interopérabilité entre systèmes et procédures). En se basant sur un grand nombre d'entretiens menés auprès de différents experts et d'observations de simulations, ce sont ces facteurs humains qui étaient au centre de la thèse réalisée par Béatrice Linot, conjointement encadrée par Jérôme Dinet (laboratoire 2LPN) et François Charoy (Coast Team INRIA/Loria, Télécom Nancy), avec un double objectif : mieux comprendre les comportements et processus psycho-ergonomiques au cœur des communications entre les services intervenant lors de gestion de crises majeures, en particulier concernant la confiance dans les données, les outils et les partenaires ; proposer des préconisations pour l'aide à la conception de dispositifs numériques plus efficients, plus efficaces et renforçant cette confiance.

WP3 - PROTOCOLES POUR LA SÉCURITÉ ET SURVEILLANCE DES RÉSEAUX

Les réseaux sont le premier vecteur d'attaques informatiques. Il est primordial de les sécuriser via la conception en amont de protocoles dont les propriétés sont prouvées, et en aval via la supervision des communications visant à détecter les attaques en cours et à les contrecarrer par des actions défensives. Ces deux approches complémentaires sont au cœur du WP3. Nos chercheurs utilisent des concepts et techniques empruntant aussi bien aux domaines des mathématiques, de l'informatique ou de l'automatique pour ainsi garantir ou renforcer la sécurité des différents réseaux (5G, industriel, etc.)

Thibault CHOLEZ, LORIA

Une fois la confiance assurée dans chaque équipement, il faut s'intéresser à la sécurité des réseaux interconnectant ces objets notamment en surveillant ces réseaux et aux protocoles de sécurité associés notamment les protocoles cryptographiques. La vérification des protocoles cryptographiques peut se faire en utilisant des méthodes formelles notamment pour des protocoles complexes comme le vote électronique. La surveillance des réseaux concerne les menaces dites persistantes avancées qui sont en fait des attaques récurrentes. Pour cela, le projet DigiTrust utilise notamment les outils du Big Data ou de l'intelligence artificielle tout en tenant compte des nouveaux paradigmes des réseaux comme les SDN (Software Defined Networks pour l'acronyme anglais) qui permettent la virtualisation des ressources réseaux en les dissociant des éléments physiques du réseau.

THÈSE

AUTOMATISATION SDN SÛRE DE RÉSEAUX À TEMPS ET FIABILITÉ CRITIQUES (2019-2022) - LOÏC DESGEORGES

SOUS LA DIRECTION DE THIERRY DIVOUX (CRAN, DÉPARTEMENT INGÉNIERIE DES SYSTÈMES ECO-TECHNIQUES - ISET) ET JEAN-PHILIPPE GEORGES (CRAN, DÉPARTEMENT INGÉNIERIE DES SYSTÈMES ECO-TECHNIQUES - ISET)

Mes travaux portent sur la sécurisation d'architectures réseau dites « Software Defined Networking ». Leur originalité est de centraliser le contrôle des nœuds d'interconnexion à qui on retire toute « intelligence et autonomie locale ». Cette vision globale permet une commande du réseau plus fine et plus réactive. Cependant, cette centralisation rend l'architecture sensible à une défaillance ou à une attaque du contrôleur. C'est pourquoi je travaille à la définition d'un observateur du contrôleur, qui va analyser son activité, et identifier des dérives comportementales symptomatiques de dysfonctionnements ou d'agressions extérieures. À cette fin, je développe des algorithmes par apprentissage dont je vérifie la pertinence et l'efficacité par simulation. N'intervenant pas sur le réseau, l'observateur reste discret et donc protégé. En cas de problème, il pourra proposer une bascule sur un contrôleur de secours.

POST-DOC

JEUNE CHERCHEUR DIGITRUST DÉDIÉ AUX ÉTUDES DE L'UTILISABILITÉ DE LA SÉCURITÉ. (2020-2021) ENKA BLANCHARD (LORIA).

Après mes études de mathématiques et informatique à l'ENS Paris et à l'Université de Paris, j'ai soutenu en 2019 une thèse sur les aspects humains de l'authentification et des systèmes de vote, lauréate du prix PSL Interfaces Humanités/Sciences Sociales. Au sein du projet DigiTrust, je poursuis des travaux de recherche transdisciplinaire, sur des sujets tels que l'utilisabilité de la sécurité, le vote en basse technologie et les interactions entre théorie queer et théorie crip. En parallèle à ces travaux, j'ai poursuivi aussi une deuxième thèse au sein de la chaire d'intelligence spatiale de l'Université Polytechnique Hauts-de-France, avec une dimension théorique centrée sur l'utilisation de mathématiques discrètes pour formaliser des modèles de mobilités urbaines, et une application au cas d'étude privilégié des spatialités du handicap.

- Enka Blanchard. Crip spatialities and temporalities I: discreet crips in a discrete world. EspacesTemps.net, Association Espaces Temps.net, 2020.

- Enka Blanchard. Crip spatialities and temporalities 2 : a systematic typology of temporal taxes. EspacesTemps.net, Association Espaces Temps.net, 2020.

- Nikola Blanchard, Siargey Kachanovich, Ted Selker, Florentin Waligorski. Reflexive Memory Authenticator: A Proposal for Effortless Renewable Biometrics. Emerging Technologies for Authorization and Authentication, 11967, pp.104-121, 2019.

MEMBRES ALUMNI /ALUMNI MEMBERS

- Lama SLEEM : Post-doctoral fellow dedicated to implementations of the NIST lightweight analyst into the IoT-Lab. (Axis 3). 2020.
- Soline BLANC : 1-year DigiTrust engineer dedicated to implementations of the NIST lightweight analysts into the IoT-Lab. (Axis 3). 2020.

WP 4 - LA CONFIANCE DES CITOYENS ET LES RÉSEAUX SOCIAUX

« Les réseaux sociaux offrent une opportunité unique de profilage des citoyens susceptible d'être exploitée à des fins commerciales ou politiques. Nous étudions comment les données privées d'un usager peuvent être inférées uniquement à partir des images qu'il publie. Nous proposons des contre-mesures fondées sur l'apprentissage automatique afin de bloquer ces fuites d'information. »

Michael RUSINOWITCH, LORIA

DigiTrust s'intéresse aussi à la confiance et aux systèmes de réputation dans les réseaux et notamment les réseaux sociaux. Il s'appuie sur des travaux de recherche portant sur la transparence des algorithmes, sur les systèmes de recommandation, sur la protection des données personnelles dans les réseaux sociaux via les méthodes formelles mais aussi grâce à l'apprentissage automatique ou machine learning ou au Big Data. Les sciences humaines et sociales sont également sollicitées en s'intéressant d'un point de vue juridique et économique aux notions de contrats, ceux portant par exemple sur les données personnelles et également d'un point de vue psychologique sur la confiance en des organisations virtuelles.

THÈSE

PRIVACY PROTECTION AGAINST INFERENCE ATTACKS IN SOCIAL NETWORKS (2018-2021) - BIZHAN ALIPOUR PIJANI

SOUS LA DIRECTION DE ABDESSAMAD IMINE (LORIA, ÉQUIPE PESTO) ET MICHAËL RUSINOWITCH (LORIA, ÉQUIPE PESTO)

The thesis objective is to provide **social network** users with an application to audit their profile and prevent them from publishing data that may endanger their **privacy**. To that end, we investigate potential **privacy attacks**, study their feasibilities and analyze their impacts. Therefore, the following issues have to be addressed:

- **Detection of privacy vulnerabilities**. Each user has a profile containing personal attributes (such as gender, age) and describing relationships and interactions with other users. Among these attributes, some are considered to be sensitive according to General Data Protection Regulation and national regulations. In this stage, the goal is to propose a methodology for characterizing and building attacks.

- **Countermeasures design and implementation**. When a sensitive attribute is vulnerable to an inference attack, the proposed inference algorithm will provide explanations (such as posts, pictures, friends' comments) that have probably led to the leak. This can be exploited to investigate effective countermeasures.

Bizhan Alipour Pijani, Abdessamad Imine, Michaël Rusinowitch. Inferring attributes with picture metadata embeddings. ACM SIGAPP applied computing review : a publication of the Special Interest Group on Applied Computing, Association for Computing Machinery (ACM), 2020, 20 (2), pp.36-45.

THÈSE

L'ACTE ADMINISTRATIF NUMÉRIQUE (2019-2022) - ALEKSANDR STEPANOV

SOUS LA DIRECTION DE PIERRE TIFINE (IRENEE) ET PHILIPPE COSSALTER (IRENEE, UNIVERSITÄT DES SAARLANDES)

Mon étude se focalise sur l'élaboration d'une théorie complète de l'implication des algorithmes dans le processus décisionnel des autorités administratives. Il s'agit d'une recherche sur les technologies et les méthodes optimales de l'algorithmisation de l'Administration et leur encadrement légal et doctrinal afin de rendre la procédure administrative plus vite, plus efficace et plus juste. La prise d'un acte administratif numérique oblige de bien définir le degré juridiquement possible de la participation algorithmique ainsi que les garanties de respect des droits humains et des principes fondamentaux du droit administratif.

THÈSE

PRIVACY PRESERVING BIG DATA MANAGEMENT AND ANALYTICS IN DISTRIBUTED ENVIRONMENTS (2021-2024) ALA EDDINE LAOUIR

SOUS LA DIRECTION D'ABDESSAMAD IMINE (LORIA, ÉQUIPE PESTO) ET ALFREDO CUZZOCREA (LORIA-CISPA)

Nowadays, big data management and analytics, based often on distributed environments, is gaining momentum within the research community. Basically, the main issue with big data management concerns with effectively and efficiently managing massive big data repositories for a wide variety of typical data management tasks, such as representation, querying, indexing, partitioning, and so forth. On the other hand, big data analytics concerns with extracting useful, actionable knowledge from big data repositories for decision making purposes, by extending classical approaches inherited from decades of data mining and machine learning research. In this so-delineated context, the issue of supporting privacy-preserving big data management and analytics plays a first-class role, especially with respect to the wide class of emerging big data application scenarios, which range from social networks to bio-informatics, from sensors networks to web recommendation tools, from e-science systems to e-government systems, and so forth. In all these applicative settings, protecting the privacy of sensitive information can be clearly intended as an enabling technology.

The main objectives of this PhD thesis consist in devising innovative models, methods and techniques for effectively and efficiently supporting privacy-preserving big data management and analytics in distributed environments, by also providing significant realizations in reference case studies.

ALFREDO CUZZOCREA . CHAIRE D'EXCELLENCE LUE - DIGITRUST LORIA ET CISPA (2020-2021)

The research activities by Alfredo Cuzzocrea in the context of the DigiTrust project are focused on the issue of supporting privacy-preserving big data management and analytics in distributed environments. The main paradigm pursued by this conceptual setting is represented by the so-called big-data-driven cybersecurity, i.e. a paradigm that predicates achieving cybersecurity of complex systems via making secure and privacy-preserving big data repositories that populate those systems. Particularly, while this topic is general enough to house various lines of research, the main challenge considered is the case of OLAP-based big data analytics over Clouds, where the main challenge consists in making (massive) OLAP (Online Analytical Processing) data cubes privacy-preserving under several distributed security protocols (e.g., SMC). This problem is relevant in several application scenarios, ranging from IoT systems to bio-informatics frameworks, from sensors networks to social networks, from smart cities to intelligent transportation systems, and so forth.

MEMBRE ALUMNI / ALUMNI MEMBER

- Anne Claire MANSION : « Impacts juridiques et politiques de l'utilisation des technologies de confiance décentralisées : le cas de la technologie Blockchain »

ENSEIGNEMENT ET FORMATION / *LEARNING AND TRAINING*

En 2019, le projet DigiTrust a soutenu :
- la création de la Licence Professionnelle Cybersécurité et Cyberdéfense ;
- les actions de communication et de promotion de la cybersécurité ;
- le financement d'écoles thématiques reconnues comme formation par les écoles doctorales ;
- la création de la « réserve opérationnelle et citoyenne » en relation avec l'armée et le Comcyber par l'utilisation de la plateforme de formation dédiée CyberRange à Telecom Nancy et à Mines Nancy.

La Licence Professionnelle Cybersécurité et Cyberdéfense, labellisée SecNumEdu par l'ANSSI, est une formation technique préparant aux métiers de la sécurité du numérique pour des étudiants visant une insertion professionnelle immédiate à Bac+3. Elle se déroule en alternance sous contrat d'apprentissage ou de professionnalisation. Elle comprend 450H de formation et 150H de projet tuteuré, répartis sur 22 semaines de l'année, les 30 semaines restantes se faisant dans l'entreprise d'accueil.

En sortie de formation, les étudiants diplômés auront les compétences pour pouvoir directement viser des métiers comme administrateur de solutions de sécurité et analyste SOC (security operation center). Ils auront aussi été sensibilisés aux métiers de coordinateur sécurité, d'auditeur technique en sécurité, de pentesteur et d'analyste forensic, et seront donc capables d'accomplir des tâches simples liées à ces métiers.

Les débouchés sont les entreprises et les startups spécialisées dans la cybersécurité, les opérateurs d'importance vitale (OIV) et de services essentiels (OSE), les services de l'état, et finalement toutes les organisations dont les menaces qui pèsent sur leur système d'information peuvent perturber leur activité et engendrer de lourdes pertes financières.

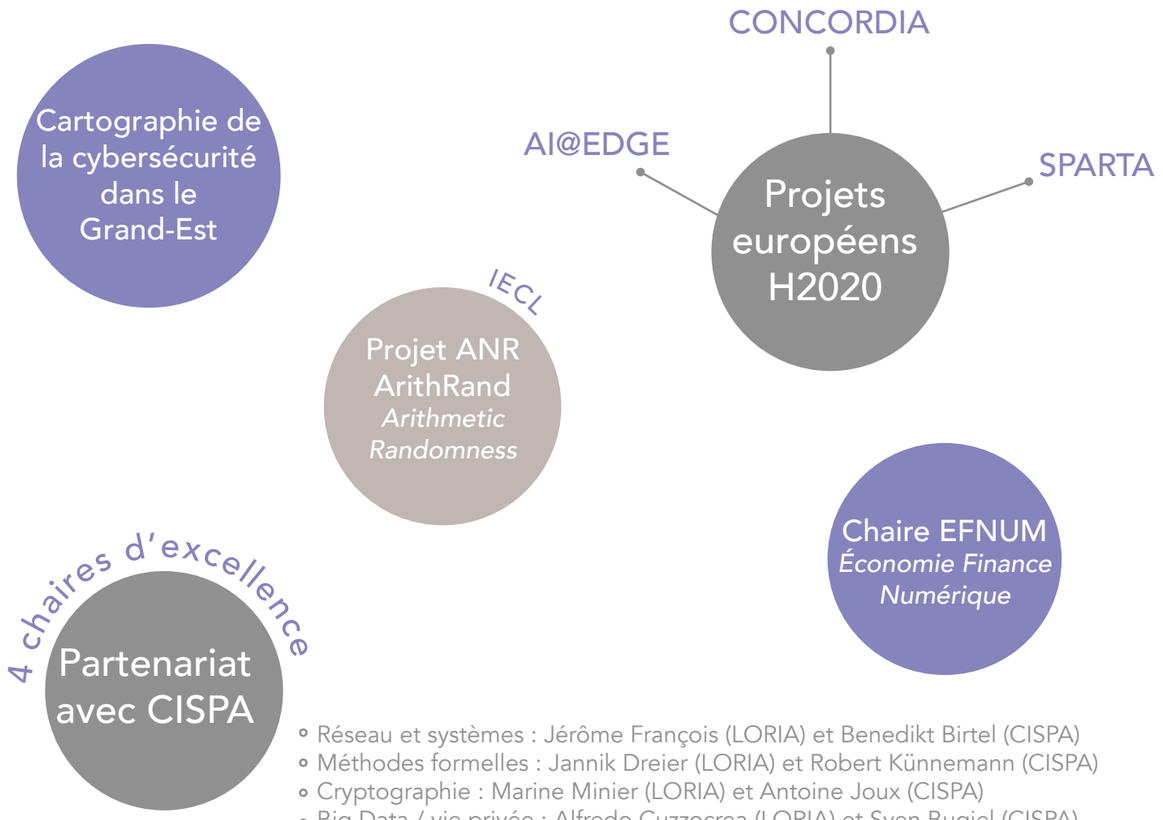
Capacité d'accueil : 12 étudiants
1ère année (2020-21) : 9 étudiants recrutés (choix lié à la situation sanitaire)

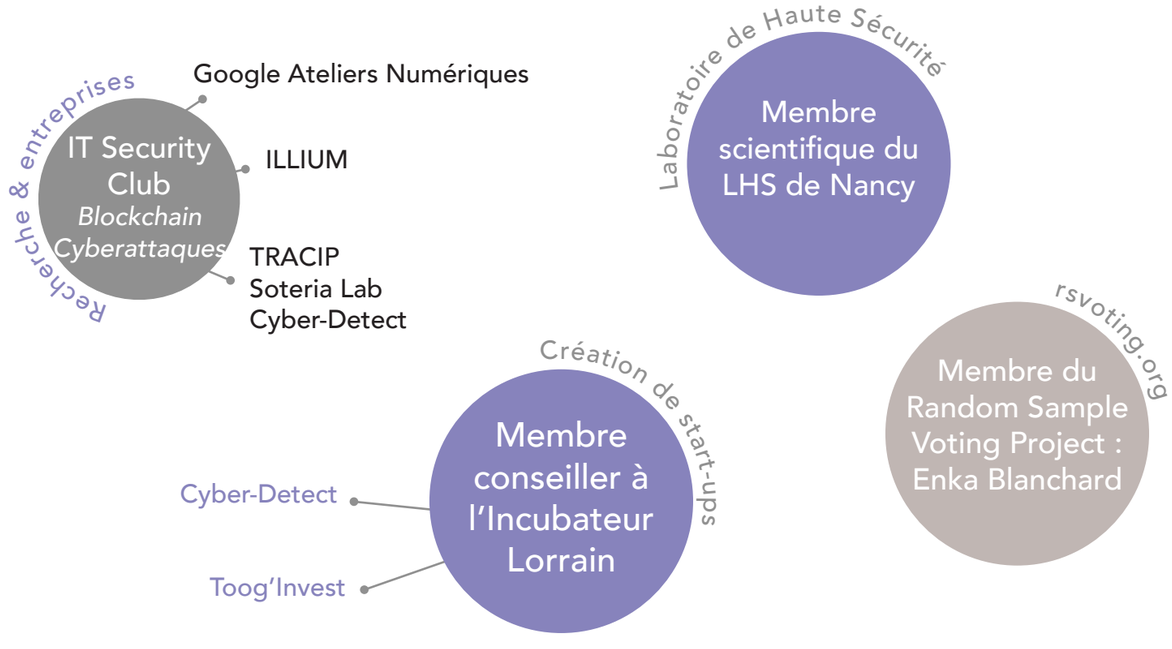
Contacts :
Vincent Lecuire
vincent.lecuire@univ-lorraine.fr
Nicolas Krommenacker
nicolas.krommenacker@univ-lorraine.fr

From an education point of view, DigiTrust is a partner of a « Licence Pro Cybersécurité » at IUT Nancy-Brabois. DigiTrust also partly funds some thematic schools recognized as training by doctoral schools. DigiTrust also participates in the creation of the « operational and citizen reserve » in relation with the army and the Comcyber through the use of the dedicated training platform CyberRange at Télécom Nancy and at Mines Nancy.

En juin 2021, la licence a organisé un exercice de gestion de crise cyber pendant deux jours >

DIGITRUST DANS SON ENVIRONNEMENT





FAITS MARQUANTS / *HIGHLIGHTS*

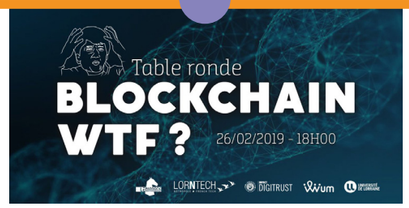
SEPTEMBRE 2018
Démarrage du projet
Deux thèses déjà en cours sur la thématique

OCTOBRE 2018
Démarrage d'une thèse de doctorat

JANVIER 2019
Google BlockChain 2019
«Déconstruire les idées reçues»
Google Ateliers Numériques

FÉVRIER 2019
Participation au Club de la Sécurité de l'Information Régional
CLUSIR
La cybersécurité dans tous ses états

FÉVRIER 2019
Lor'n'Tech BlockChain



AVRIL 2019
Kick-off meeting
Journée de lancement officiel du projet

OCTOBRE 2019
1° Conseil scientifique DigiTrust

OCTOBRE 2019
Démarrage de 6 thèses

NOVEMBRE 2019
Journée Fédération Charles Hermite : « Sécurité et confiance dans les échanges des données de santé »

JANVIER 2020
1° workshop Franco-Allemand sur la Cybersécurité suivi de l'accord avec le CISPA

JANVIER 2020
Recrutement d'Alfredo Cuzzocrea comme Chaire d'excellence LUE - DigiTrust - CISPA

2020
35 millions de malwares au LHS !

DÉCEMBRE 2020
Point mi-parcours LUE-DigiTrust

FÉVRIER 2021
First virtual workshop day of the Franco-German Center for Cybersecurity from Nancy and Saarbrücken

FÉVRIER 2021
Exercice CyberRange avec la base de défense de Nancy, Lorraine INP, Mines Nancy et TelecomNancy

AVRIL 2021
Participation à la 3° session Capteur de territoire (Fédération des EPL)
La transition numérique et le citoyen

MAI 2021
Second virtual workshop day of the Franco-German Center for Cybersecurity from Nancy and Saarbrücken

2021
DigiTrust Webinaire

JUIN 2021
Workshop DigiTrust - OLKi

CONTACTS

COMITÉ OPÉRATIONNEL

Marine Minier, Responsable scientifique DigiTrust, LORIA
Anne Boyer, Professeure, Université de Lorraine, LORIA
Anne Gégout-Petit, Professeure, Directrice de l'IECL
Antoine Lejay, Directeur de recherche Inria, IECL
Armelle Brun, Professeure, Université de Lorraine, LORIA
Didier Wolf, Directeur du CRAN
Gilles Millerioux, Directeur adjoint du CRAN
Jean-Yves Marion, Directeur du LORIA
Jérome Dinet, Directeur du 2LPN
Michaël Rusinowitch, Directeur de recherche Inria, LORIA
Philippe Cossalter, Professeur agrégé des facultés de droit, membre IRENEE, Universität des Saarlandes
Samuel Ferey, Directeur de la Maison des Sciences de l'Homme (MSH Lorraine), BETA : Bureau d'Économie Théorique et Appliquée
Stephan Merz, Directeur de recherche Inria, LORIA
Thibault Cholez, Maître de conférences, Télécom Nancy, LORIA

PROJET IMPACT DIGITRUST

Laboratoire lorrain de recherche en informatique et ses applications
Campus scientifique
BP 239
54506 Vandoeuvre-lès-Nancy Cedex
Tél : +33 3 83 59 20 00

https://www.lue.univ-lorraine.fr/fr/article/digitrust

@LUE_Digitrust

CONTACT
PROJECT MANAGER DIGITRUST
MAIRA NASSAU
MAIRA.NASSAU@LORIA.FR

PARTENAIRES

UN PROJET LORRAINE UNIVERSITÉ D'EXCELLENCE

6 LABORATOIRES

Publication : Juin 2021
Conception - réalisation : service communication LORIA

Crédit photos : DigiTrust, membres et partenaires du projet DigiTrust, Freepik, Undraw, Flaticon