

REVUE DE PRESSE

2018

01101100

01101111

01110010

01101001

01100001

01101100

01101111

01110010

01101001

011000010111

11100100111

1000010111

11111111

Loria



Loria



UNIVERSITÉ
DE LORRAINE



Portrait d'entreprise

Cyber-detect, l'assurance tous risques

Par La rédaction de LA SEMAINE • La rédaction • 13/03/2018 à 16h00

Installé dans les locaux d'Artem, Cyber-detect s'est imposé en moins d'un an sur le marché de la cybersécurité. À sa tête : Laurent Werner, 30 ans, créateur et président de la start-up nancéienne, qui fêtera son premier anniversaire au mois d'avril.

« Si Photoshop est l'ami du graphiste, on peut dire que Cyber-Detect est l'ami du cyber-expert », résume Laurent Werner, président de Cyber-Detect. Cette jeune start-up, composée de six membres, est le fruit de dix années de recherche au laboratoire lorrain de recherche en informatique et ses applications (Loria). C'est surtout la traduction d'un réel danger présent au quotidien sur internet. Les entreprises, collectivités, universités se tournent de plus en plus vers des spécialistes de la cybersécurité pour endiguer ce fléau difficile à contrer.

En cause : ce qu'on appelle un « malware ». C'est un programme malveillant qui, dans sa structure, importe des fonctionnalités malveillantes dans le but de nuire au système informatique. « Pour entrer, il lui faut un point d'entrée comme une pièce jointe dans un mail », précise Laurent Werner.

Diplômé d'un master de sciences à ICN Business School en 2015, il décide de créer deux ans plus tard sa start-up, basée à Villers-lès-Nancy. « C'est le résultat d'une rencontre avec Jean-Yves Marion et Guillaume Bonfante en 2016 à la bourse aux technologies. Chercheurs au Loria, ils recherchaient un porteur de projet pour développer leur solution. »

À la différence d'un anti-virus qui va détecter et contrer un programme malveillant déjà connu, l'entreprise nancéienne va détecter des « codes » (parties d'un programme) malveillants jamais répertoriés dans les bases d'anti-virus, comme l'explique Laurent Werner : « On a mis au point une solution logicielle pour accompagner les experts dans l'analyse de malwares inconnus. Un programme analysé sera déclaré comme malveillant lorsque qu'on remarque des similitudes avec un malware dans l'exécution de ses fonctionnalités. »

Une réputation grandissante

Un an après sa création, Cyber-Detect rencontre un vrai succès auprès des institutions et des grandes entreprises, comme la direction générale de l'armement (DGA) ou l'Université de Lorraine, ou encore une grande société de chemin de fer français. « La DGA est notre client historique, nous avons pu passer de la recherche à la réalité. Lorsqu'elle a fait appel à nous, elle avait des problèmes pour solidifier son système mais elle voulait surtout comprendre et retrouver l'origine de ces nouvelles attaques. L'université de Lorraine cherchait plutôt un moyen de se sécuriser », souligne son président.

Une efficacité saluée par le ministre de l'Intérieur lors de son discours au Forum International de la Cybersécurité de Lille en janvier dernier. La start-up avait repéré en mai dernier l'attaque « Adylkuzz », un malware qui profitait d'une faille dans Windows. Sa renommée, presque mondiale, lui ouvre des partenariats à l'étranger : « Nous sommes en discussion avec un partenaire aux États-Unis qui s'occupe de procès d'affaires autour du plagiat informatique », confesse Laurent Werner.

La suite ? La start-up prépare une offre pour les smartphones et autres objets connectés. Elle souhaite aussi rendre accessible sa cybertechnique aux PME dans le courant de l'année : « Cette solution, actuellement destinée aux experts et appliquée par ceux-ci, on souhaite en faire un programme qui fonctionnera tout seul, pour ressembler à un anti-virus. » En attendant, Cyber-Detect souhaite étoffer son équipe pour mener à bien tous ses projets.

Benoît Soenen (clp)

Alérion ► Villers-lès-Nancy

Comment rendre un drone intelligent

La start-up nancéienne conçoit des « équipements d'intelligence embarquée » pour adapter les engins aux missions les plus difficiles.

La spin off a décollé il y a trois ans, depuis le campus de la fac de sciences. Porté par Laurent Ciarletta, enseignant chercheur à Mines Nancy, spécialiste de la gestion des réseaux dynamiques, et Anne-Sophie Didelot, Alérion « fonctionnalise » les drones, c'est-à-dire qu'elle conçoit des « équipements d'intelligence embarquée » afin d'adapter les engins à toutes sortes de missions. Elle développe aujourd'hui des solutions « qui rendent les drones plus sûrs et plus intelligents ». Car si potentiellement le marché est immense, c'est bien la sécurité qui empêche l'industrie du drone de décoller réellement.

Hydradrone

Installée dans les murs du Loria, dans la « Silicon Villers », Alérion compte aujourd'hui trois salariés et quatre associés et est engagée dans plusieurs projets de recherche collaboratifs. La start-up a ainsi été amenée à concevoir un « hydradrone », un engin dédié à la surveillance environnementale. Le premier prototype devrait voler dès ce printemps.

Drone de surveillance

Alérion développe également des drones de surveillance d'infrastructures. Ces engins ont été conçus pour surveiller de près les lignes d'Enedis, les canalisations en sortie de barrage, et même les clôtures de l'aéroport de Lyon. Cette nouvelle façon d'appréhender



Le prototype de l'hydradrone, dédié à la surveillance environnementale. Photo ER

la maintenance des grandes infrastructures ouvre de belles perspectives de développement.

La start-up nancéienne est engagée dans un programme qui permettra de vivre les grands événements sportifs comme jamais. Dans le cadre de ce projet porté par la Commission européenne, Alérion développe en effet des essais de drones pour multiplier les points de vue et les angles originaux. Bref, pour renforcer la sensation d'immersion du spectateur. Toute la difficulté est d'assurer des conditions de sécurité maximales.

« Les appareils sont en cours de montage et

les tests sont prévus au deuxième semestre de cette année », indique Anne-Sophie Didelot. Les essais d'Alérion devraient couvrir le Giro, en Italie.

S.L.

Alérion et Air Marine, numéro 1 de la filière

Alérion se rapproche d'une société bordelaise, Air marine, experte en inspection aérienne par avion et par drone, spécialisée dans l'acquisition et exploitation de données par ces mêmes moyens. Les deux entreprises ont en effet signé une lettre d'intention en vue de son rapprochement avec la société Alérion.

Pour Alérion (70 000€ de CA), cette fusion va lui permettre de renforcer ses activités à travers des projets de développement et le déploiement en Nouvelle Aquitaine de son réseau d'excellence scientifique, de se doter

de nouvelles compétences en R & D, de favoriser l'émulation positive de la nouvelle équipe créée et de bénéficier de la notoriété d'Air Marine, et ainsi devenir un leader de la filière drone.

Air Marine, 31 salariés, 2,5 M€ de CA, travaille pour les plus grands donneurs d'ordre européens. Ce rapprochement va leur permettre de renforcer leurs compétences en R & D, apporter une sensibilité et un savoir-faire managérial nouveau, associer son image à celle déjà reconnue d'Alérion.

S. L.



Bénéficiaire de la notoriété d'Air Marine. Photo ER

Informations

Alérion

- Espace Transfert, 615, rue du Jardin botanique, 54600 Villers-lès-Nancy. Tel. 03 54 95 86 00
- Chiffre d'affaires : 70 000 €
- Trois salariés et quatre associés ;

Sailendra

La « sérénité » d'être adossé à un grand groupe

Quand il a quitté « un bon poste » pour créer la start-up Sailendra, les personnes qui l'ont encouragé à « foncer » étaient bien peu nombreuses. Mais Régis Lhoste, aujourd'hui âgé de 40 ans, savait que s'il renonçait, il « le regretterait toute [sa] vie ». Il a bien fait d'y croire.

Agée de 10 ans, Sailendra est spécialiste des solutions d'analyse comportementale par l'intelligence artificielle. Elle élabore des algorithmes qui permettent d'observer les comportements d'achat d'un utilisateur, de prédire ses futurs besoins et de les lui proposer. Sailendra est devenue filiale du groupe Pharmagest à hauteur de 70% en décembre 2016. La start-up issue de l'Université de Lorraine, via le Laboratoire lorrain de recherche en informatique et ses applications (Loria), a séduit Thierry Chapusot dès l'origine du projet, tant il pressentait l'intérêt de telles technologies développées par la start-up dans le domaine de l'e-commerce pour celui de l'e-santé.

« Nous concentrer sur notre cœur de métier »

Pour Régis Lhoste, l'opération est gagnant-gagnant : « Nous avons besoin d'être adossés à un grand groupe. Cela nous permet d'avoir des capacités de développement bien



Régis Lhoste : « Pharmagest nous permet de nous concentrer sur notre cœur de métier ». Photos Cédric JACQUOT

plus faciles. Depuis un an, Pharmagest nous a apporté de la professionnalisation, de la sérénité, et nous permet de nous concentrer sur notre cœur de métier. C'est surtout l'opportunité pour nous de travailler sur de beaux projets au sein du groupe. Notre fil rouge depuis toujours, c'est le challenge ».

Sans être « pieds et poings liés », ajoute Régis Lhoste qui apprécie « la liberté

d'action » préservée de Sailendra. La start-up qui compte 7 personnes, diversifie ainsi son offre. Tout en bénéficiant au sein du groupe Pharmagest « d'une émulation sans prix qui nous permet d'avoir de nouvelles idées ».

En janvier dernier, Sailendra a accompagné Pharmagest au plus grand salon high-tech grand public du monde, à Las Vegas.

M.-H. V.

Noviatek

« Un énorme coup d'accélérateur »



Mathieu Muller et sa box santé.

Mathieu Muller est un passionné, un inventif. A 12 ans déjà, il imaginait « un détecteur d'inondations » qu'il vendait à des voisins ! Ingénieur systèmes, le jeune homme, est aujourd'hui, à 29 ans, directeur associé, avec Régis Ciré, de Noviatek. Une start-up, créée par les deux jeunes gens en 2011 alors qu'ils étaient encore étudiants à l'Université de Lorraine, et filiale à 80% de Pharmagest depuis 2016.

Noviatek a développé Noviacare, une « box santé » destinée à favoriser le maintien à domicile des personnes âgées ou fragiles. Un système intelligent autonome (nul besoin de connexion internet) qui se place dans la pièce à vivre, équipé de capteurs sans fils installés à des endroits « sensibles » du domicile : salle de bains, toilettes, porte de réfrigérateur, porte d'entrée, etc. Pendant 15 jours, le système « apprend les habitudes de la personne », explique Mathieu Muller, « ce qui nous donne un modèle de cohérence de vie ». Par la suite, la box va pouvoir, grâce à de complexes algorithmes, comparer au quotidien les scénarios de vie, et détecter les premiers signes d'une perte d'autonomie. Un repas ou un médicament non pris ? Un proche sera prévenu. Une cascade d'alertes

permet d'aller jusqu'au déclenchement des secours en cas de graves problèmes.

Dès le début de l'aventure, les deux associés se sont rapprochés de professionnels de santé pour développer ce système : « Nous avons, par exemple, bénéficié d'une formation pour comprendre les maladies neurodégénératives ».

Entrer dans le giron Pharmagest a constitué un « énorme coup d'accélérateur » pour la start-up qui depuis « a pu se consacrer à 100% » à sa box. « On a toujours su que notre travail serait moteur de quelque chose, sinon nous ne serions pas allés au boulot chaque jour de 8 à 18 h sans salaire de 2011 à 2016. En revanche, si Pharmagest n'avait pas cru en nous, nous aurions arrêté », avoue Mathieu Muller.

Cinquante boîtiers et 300 capteurs sont installés dans le Grand Est. La phase d'expérimentation se termine. « Nous allons analyser toutes les données pour performer les algorithmes », poursuit le jeune homme.

Le produit, « pour lequel grâce à Pharmagest, nous avons déposé deux brevets », rappelle Mathieu Muller, sera présenté à Paris cet été.

M.-H. V.

EN BREF



Au programme : stands d'infos sur la vivisection et les méthodes substitutives.

VANDŒUVRE

Pour les droits des animaux

A l'occasion de la Journée mondiale des animaux dans les laboratoires - JMAL -, qui a lieu le 24 avril, l'équipe bénévole d'International Campaigns Nancy organise une action de sensibilisation et de mobilisation sur le sort des animaux dans les laboratoires et les moyens de faire avancer cette cause ce dimanche. Au programme : stands d'informations sur la vivisection et les méthodes substitutives, cosmétiques non testés sur animaux ; un tractage et la présentation d'une pétition. « Certaines démarches ont été entamées à propos de l'expérimentation animale au pôle santé de Nancy Brabois », indiquent les organisateurs. « Certaines choses ont bougé... Nous avons lancé une pétition, avons rencontré élus municipaux et régionaux sensibles à la cause animale ».

> RV ce dimanche 22 avril, de 10 h 30 à 12 h 30, sur la place du marché municipal.

VANDŒUVRE-LÈS-NANCY

« Si c'est gratuit, c'est toi le produit »

Un titre un peu provoquant pour dire que derrière la gratuité apparente des réseaux sociaux se cachent bien des intérêts et... des pièges.

L'UP2V (Université populaire et participative de Vandœuvre) était au lycée Callot, ce vendredi, pour proposer une journée de formation à l'attention des élèves de 1^{ère} STMG. L'objectif : prévenir les risques encourus suite à une utilisation non réfléchie des réseaux sociaux.

Intervenaient Sabeur Aridhi, enseignant à l'École TELECOM Nancy et Abdessamad Imine, enseignant à l'IUT Charlemagne tous deux chercheurs au LORIA, respectivement spécialistes de la science des données (Big Data) et de la sécurité informatique dans le domaine des réseaux sociaux.

Un moment clé dans la formation de ces élèves interpellés sur l'utilisation faite des renseignements déposés sur la toile : « Facebook se souvient de tous les endroits où vous êtes connectés et utilise vos données qui peuvent être exfiltrées en toute légalité », et de noter que le premier réseau social est une source de données exponentielle qui recueille plus de 500 teraoctets par jour utilisables pour cibler de nouveaux prospects, ajuster des campagnes publicitaires... Et l'e-commerce n'est qu'une utilisation parmi de nombreuses autres.

La « fouille des données » déposées permet de trouver nombre



Des élèves sensibilisés aux dangers d'une utilisation non réfléchie des réseaux sociaux.

d'informations publiques ou sensibles comme l'orientation sexuelle, la situation familiale, le casier judiciaire, les origines sociales, les croyances...

Le mot d'ordre était donc « prudence » et pour répondre à l'utilisation sans cesse croissante de ces jeunes aux écrans, Michaël Bisch, médecin-psychiatre, et Alice Cohn, psychologue, spécialistes de l'addiction aux objets numériques interrogeaient les élèves sur leur définition de l'addiction. Les jeunes ont évoqué le manque, l'impulsivité, l'agressivité. Et le médecin psychiatre de décrire

« le smartphone comme une pompe à dopamine », la dopamine étant l'hormone du circuit de la récompense cérébrale.

Une journée de rencontre productive, conclue par le proviseur, Sylvie-Eve Freyermuth qui remer-

ciait les différents intervenants, et incitait les adolescents à une conduite responsable : « Evitez de vous mettre en situation de vous faire grignoter vos espaces de liberté ».

Selon une enquête réalisée par les lycéens de Callot...

96 % des élèves utilisent les réseaux sociaux. 72 % les consultent de leur smartphone. 30 % y passent entre 2 et 4 heures par jour. 61 % des parents cautionnent le temps passé sur les réseaux. Et l'utilisation principale faite de ces outils est le chat et « regarder ce que font les autres ».

bloc-notes

ART-SUR-MEURTHE

Messe

> dimanche 22 avril. À 10 h 30. Église. Pour l'ensemble paroissial Art-sur-Meurthe, Bosserville, Lenoncourt.

HEILLECOURT

Stationnement interdit

> samedi 28 avril. De 9h à 17h. Le stationnement allée des Grands-Pâquis sera interdit au droit des établissements Joly et la circulation sera réglementée par un policier municipal. Les services de la Métropole y occuperont cette rue en impasse pour l'opération Compost. Tél. 03 83 55 17 20.

HEILLECOURT

Réaffirmer l'importance des langues



L'importance des langues, une nécessité dans la formation du citoyen européen.

Le collège Montaigu s'est engagé depuis deux ans dans une politique d'ouverture culturelle et linguistique et développe son offre de formation. A la rentrée de septembre 2018, les élèves de 6^e pourront candidater pour une section bilingue (anglais-allemand), et une section européenne en espagnol dès la 4^e accueillera des candidats volontaires. Réaffirmer l'importance des langues est une nécessité dans la formation du citoyen européen. En attendant, les 3^e de Montaigu ont découvert en mars ou en avril derniers soit l'Espagne, soit la Grande-Bretagne. Au retour, les élèves ont pu exploiter leur carnet de voyage afin de préparer les évaluations en langues prévues en mai prochain, mais aussi l'oral du brevet.

Ce qui nous a interpellés aujourd'hui

Nancy-Natal, un pont universitaire

La collaboration entre l'Université de Lorraine et l'Université Fédérale de Rio Grande Do Norte (Brésil) a été officialisée le vendredi 27 avril au laboratoire d'informatique Loria, à Vandoeuvre-lès Nancy, en présence du représentant de la rectrice de l'université brésilienne Fédérale de Rio Grande do Norte et de Karl Tombre, vice-président Stratégie européenne et internationale de l'Université de Lorraine, représentant le président de l'Université de Lorraine.

Cette collaboration va permettre de développer des activités et des projets spécifiques en analyse des données de l'apprentissage (learning analytics) et autour de la e-santé. Cette collaboration se matérialisera par des échanges et des collaborations entre chercheurs et enseignants-chercheurs mais aussi entre étudiants des deux universités. Des conférences et des séminaires au sein des deux universités seront également organisés. Seront prévues aussi des publications communes basées sur la recherche collaborative.

Ce protocole d'entente met en lumière les travaux de recherche du laboratoire brésilien LAIS, premier laboratoire brésilien installé au sein d'un hôpital universitaire, celui d'Onofre Lopes (HUOL) dont la vocation est l'innovation technologique dans la santé et le laboratoire d'informatique Loria, dont les thématiques de recherche sont entre autres l'intelligence artificielle, l'analyse des données de l'apprentissage « Learning Analytics », l'e-éducation et l'e-santé. Ces thèmes pourront être étendus à d'autres domaines en informatique comme la robotique, la géométrie, l'impression 3D ou à d'autres disciplines que l'informatique.

CL

03.05.2018 / L'Est Républicain

Juggle, au service des enfants autistes

Un an après sa création, l'application Juggle, qui favorise la prise en charge des enfants autistes a déjà séduit les professionnels du monde de l'autisme. Derrière cette start-up, deux jeunes Nancéiens.

C'est une équipe motivée et polyvalente. Ils ont une grande maîtrise dans le domaine de l'autisme » explique Jean-Marie Othelet, président de l'association Vivre avec l'autisme 54. Celui, qui est également père d'un enfant autiste, ne cache pas son admiration pour le travail des créateurs de l'application Juggle. Derrière ce nouveau système informatique, qui fait déjà la quasi-unanimité dans le monde des professionnels de l'autisme, il y a Henri Reydon et Corentin Karbiriou.

Éducateur spécialisé au contact de jeunes enfants autistes, Henri Reydon a vite réalisé lors de ses premières années de terrain que les moyens mis en œuvre pour encadrer les enfants étaient inadaptés. « Henri s'est rendu compte que les outils qu'il utilisait ne lui convenaient pas et qu'il avait les capacités d'en imaginer des

nouveaux pour améliorer la prise en charge de l'enfant », précise le cofondateur de Juggle, Corentin Karbiriou.

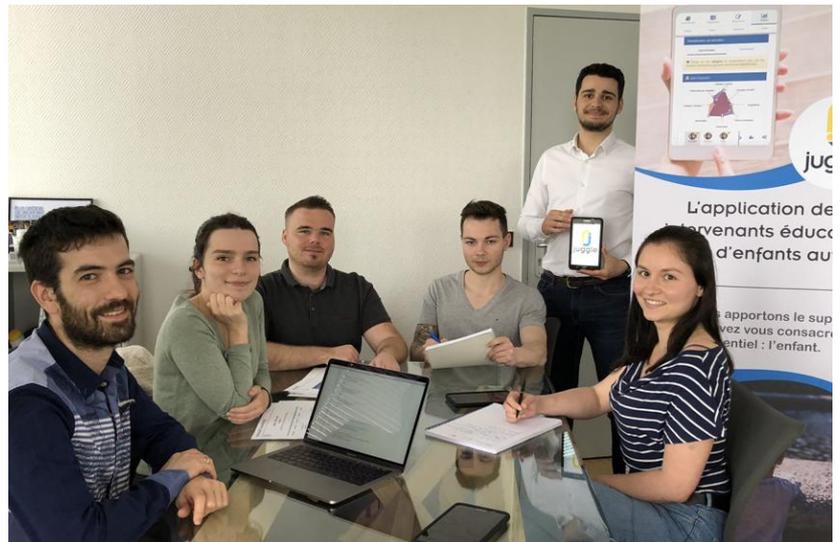
Encore en phase de tests

Toujours en phase de tests, l'objectif de l'application est simple : favoriser le lien entre les professionnels du milieu (psychologues, médecins, éducateurs) et les parents d'enfants autistes.

Pour ce faire, les deux jeunes ont créé un système informatique permettant à tous les intervenants auprès d'enfants autistes, parents inclus, d'établir un programme éducatif personnalisé pour chaque enfant.

« Notre rôle c'est d'accélérer les progrès de l'enfant en fournissant les bonnes informations aux personnes qui sont autour » observe Corentin.

Une façon d'appréhender les choses qu'apprécie Dominique BenMouffek, enseignant chercheur au Loria. « Ce que j'ai énormément aimé dans l'application, c'est l'interface. Un éducateur qui gère un groupe d'ados n'a que très peu de temps. Avec Juggle, il peut remplir les rensei-



L'équipe de Juggle, une application destinée aux intervenants éducatifs d'enfants autistes. Photo DR

gnements sur les enfants en un seul clic. C'est pratique pour apprendre des précisions sur la crise d'un ado par exemple. »

Corentin Kerbiriou et Henri Reydon ne comptent pas s'arrêter

là. « On a encore énormément de choses à faire dans ce projet, notamment concernant l'intelligence artificielle. Dans le futur, on pourrait développer ce que nous avons fait pour les enfants

autistes au profit de nouveaux bénéficiaires. Notre système pourrait être également utile pour la maladie d'Alzheimer. »

Nicolas LAURENT

Education : penser la révolution numérique

(Re) penser l'éducation à l'ère du numérique sera le thème d'un des temps forts de la prochaine édition de FestiSciences qui débute mercredi. Une plongée dans un univers en plein essor, celui des apprentissages de demain !

Moocs, serious game, plateforme France université numérique, ça vous parle ? Voilà pourtant des outils au service de nouvelles façons d'apprendre, d'échanger, de partager les savoirs qui existent déjà ! Vous aurez l'occasion d'en savoir plus grâce à l'édition 2018 de FestiSciences qui démarre mercredi prochain. En effet, l'un des temps forts programmé dans le cadre de ce rendez-vous sera consacré aux pistes pour (Re) penser l'éducation à l'ère du numérique (jeudi 24 mai à partir de 18h à Puzzle).

Autour de la table à cette occasion pour nourrir le débat : Luc Massou est maître de conférences et sciences de l'information et de la communication à l'université de Lorraine et expert mais aussi depuis l'an passé, expert auprès de la mission de la pédagogie et du numérique pour l'enseignement supé-

rieur (MiPNES), Samuel Nowakowski, chercheur au Loria (laboratoire lorrain de recherche en informatique et ses applications) et spécialiste des interactions hommes/machines, et Thierry Léger, du centre Le Lierre. L'occasion de balayer très largement le champ des expérimentations en cours et à venir en matière d'emploi du numérique dans le champ de l'éducation, au sens le plus large du terme.

Qu'il s'agisse de changement dans notre rapport au savoir ou d'emploi, d'appropriation des nouveaux outils existants, les trois spécialistes réunis autour de la table proposeront des pistes de débat à travers quelques exemples concrets.

Ressources pédagogiques libres

Ainsi Luc Massou parlera-t-il à la fois des « moocs de formation des nouveaux enseignants du supérieur développé sur la plateforme France Université Numérique (FUN) ou encore des ressources pédagogiques libres mises à disposition par les huit universités numériques thématiques françaises ».

L'enseignant-chercheur abordera



En matière d'usages du numérique au service de l'éducation, la révolution est en marche !
Photo d'archives Anthony PICORÉ

également les recherches en cours sur des interfaces permettant la projection d'images virtuelles dans l'environnement réel et pouvant entrer en interaction. Un type de

« dispositif qui trouverait des applications dans l'enseignement dès la maternelle », précise le spécialiste. Bienvenue au XXI^e siècle...
Le voyage vous tente ? Embar-

quement jeudi prochain à partir de 18h au Puzzle (café La Nouvelle Adresse)

H. B.

herve.boggio@republicain-lorrain.fr

24.05.2018 / France 3 Lorraine

Reportage sur Bruno Lévy, Directeur de l'Inria Nancy - Grand Est « Tout l'univers dans un ordinateur »



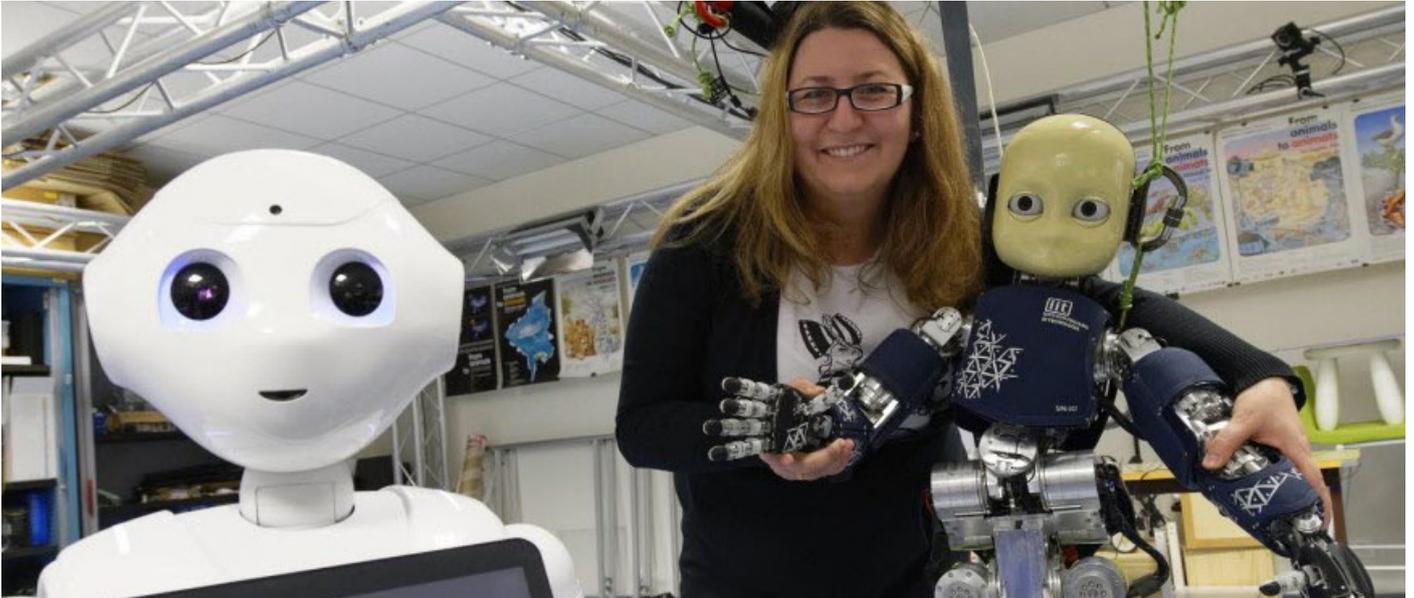
JT Lorraine France 3 Jeudi 24 Mai 2018

[Lien vers la vidéo YouTube.](#)

L'intelligence artificielle de demain

Depuis le début de la semaine, le Loria accueille la 11e Plate-forme Intelligence Artificielle, rassemblant 300 chercheurs et industriels autour de conférences et ateliers.

Par Jean-Christophe VINCENT - 06 juil. 2018 à 05:02 - Temps de lecture : 2 min



C' est un moment unique, propice aux échanges au sein d'une large communauté pluridisciplinaire intéressée par différents thèmes majeurs de l'intelligence artificielle (IA) : l'apprentissage automatique, l'ingénierie des connaissances, la représentation des connaissances et le raisonnement, les systèmes multi-agents, sur des problématiques liées à l'éthique, la santé, l'éducation, la robotique...

Depuis lundi, le Loria (Laboratoire lorrain de recherche en informatique et ses applications) organise, en partenariat avec l'AFIA (Association française de l'intelligence artificielle) et l'Université de Lorraine, la onzième Plate-forme Intelligence Artificielle (PFIA).

« L'objectif de cette manifestation, organisée pour la première fois à la Faculté des sciences et technologies à Vandœuvre-lès-Nancy, est de réunir des chercheurs, industriels et étudiants autour de conférences et ateliers consacrés à l'intelligence artificielle », expliquent Armelle Brun, maître de conférences, chercheuse au Loria, et Yves Demazeau, directeur de recherche au CNRS, présidente de l'AFIA.

Daniela Rus venue de Boston

« Ce point de rencontre unique pour la communauté de l'intelligence artificielle, dont la première édition a eu lieu à Palaiseau en 1999, permet de rapprocher les différentes disciplines qui la composent et d'établir des passerelles entre elles. Il y a 25 ans, l'intelligence artificielle était un joli rêve, elle est aujourd'hui inévitable. L'enjeu, pour la recherche française, est de s'imposer dans ce domaine, alors qu'en Chine, la politique pour développer l'intelligence artificielle est prioritaire. En tous les cas, l'IA est plus que jamais d'actualité avec la sortie du rapport Villani mettant en exergue son côté pluridisciplinaire ». Cette onzième édition rassemble en tout 300 participants dont des chercheurs de renom, tels que Daniela Rus, directrice du laboratoire de recherche en intelligence artificielle au Massachusetts Institute of Technology (MIT), à Boston, ou encore Zhongzhi Shi, directeur de recherche à l'Institute of Computing Technology, en Chine. Ce jeudi, journée dédiée à la robotique, ce sera l'occasion pour Serena Ivaldi, chercheuse du Loria, de présenter iCub, le robot européen créé pour soulager les mouvements répétitifs de l'humain.

07.2018 / La Recherche

Automates cellulaires : la complexité dans les règles de l'art

Nazim Fatès, Inria, Nancy, et Irène Marcovici université de Lorraine dans [mensuel 537](#)
daté juillet-août 2018 - 2229 mots 

Régis par des règles très simples, les automates cellulaires - une grille de cellules qui évolue - peuvent donner naissance à une riche palette de comportements et sont souvent difficiles à prévoir... De quoi inspirer et questionner les chercheurs, mais aussi certains artistes, qui les utilisent pour créer des motifs !

Des artistes se sont mis en tête de créer un tapis de 100 mètres de long tissé de sorte que la trame offre un aspect à la fois régulier et varié : certains motifs de petite taille sont observés ici et là, mais leur agencement semble désordonné (voir photo ci-dessous). Comment cette trame a-t-elle été créée ? Quelle main a pu dessiner chacun des carrés de son patron en veillant à ne pas toujours répéter la même chose ? En vérité, si ce tapis a été tissé par une machine, son patron a lui aussi été produit par une procédure automatique : c'est ce que l'on appelle un diagramme espace-temps d'automate cellulaire. Il montre l'évolution spatio-temporelle d'un système où chacun des éléments, que l'on appelle ici cellule, décide de son état en fonction de son propre état et de celui de ses deux voisins à droite et à gauche (lire l'encadré). Les automates cellulaires constituent un modèle de prédilection pour explorer la notion de système complexe dans une double perspective ...

[**Lire la suite de l'article \(en version abonné uniquement\).**](#)

07.09.2018 / Le Monde Informatique

Thales welcomes 11 new startups in the programme Cyber @Station F - Thales



[**Lien vers la vidéo YouTube.**](#)

Thales accueille 11 start-ups cybersécurité à Station F

Nicolas Certes | publié le 11 Septembre 2018



Pour la deuxième fois, Thales a sélectionné quelques start-ups spécialisée dans la cybersécurité pour les aider à développer leur solution. Toutes seront réunies dans l'accélérateur du groupe installé à Station F. Les heureux élus bénéficieront des ressources des deux entreprises pendant six mois.



Le programme Cyber de Thales offre aux start-ups lauréates un accès aux ressources du groupe, clientèle incluse, et des coaches personnalisés. (Crédit : Thales)

C'est la deuxième année que Thales accueille des start-ups à Station F pour son programme d'accélération des projets de cybersécurité. Lancée en début d'année, la sélection des sociétés participantes - françaises et étrangères - répondait à des critères précis : la start-up doit exister depuis 18 mois au minimum (trois ans au maximum), avoir réalisé une levée de fonds de série A, disposer d'un brevet ou d'un produit minimum viable, et être capable d'intégrer au moins deux de ses représentants à Station F.

Ouvert aux entreprises françaises et étrangères, cet accélérateur parisien donne accès aux marchés de Thales, à des coaches personnels et à une meilleure visibilité sur les différents salons et événements où le groupe est présent. Les start-ups sélectionnées vont

devoir relever un challenge en fonction de leur spécialité. Il y en a six, développés ci-dessous. En substance, un challenge concerne la sécurisation IoT, un autre celle du cloud public. Un troisième défi concerne l'amélioration de la prévention des attaques.

<p>CHALLENGE 1 Knowing the weakness and improving system behavior visibility</p> <p>Improve our knowledge of the cyber risks by using advance and usable threat intelligence. Improve ability to identify / or discover the current system configuration on large distributed critical infrastructure without affecting system operation.</p> <p>TYPE OF SOLUTIONS WE'RE LOOKING FOR</p> <p>Threat intelligence (and operations intelligence) capabilities and ML for content discovery. Artificial intelligence for characterization of behavior of the system. Tools to build exact system configuration for complex systems and automate vulnerability management and scoring...</p>	<p>CHALLENGE 2 Improving the ability to prevent attacks</p> <p>Improve the code quality with regard to cyber protection by assisting the developer. Reduce the likelihood of attacks by deterring the attackers while avoiding impact on productive environments.</p> <p>TYPE OF SOLUTIONS WE'RE LOOKING FOR</p> <p>Tools to allow developers to generate a code that is secured by design and to automatically assess code quality in a DEVOPS environment (and automation of security tests). Detection / discovery. Synthetic attack surface...</p>	<p>CHALLENGE 3 Improving system resilience to attacks</p> <p>React to an attack by gracefully degrading the system functions and isolating the attacker while minimizing the business impact and still being able to identify the source of the attack.</p> <p>Improve cyber detection capabilities to provide more efficient root cause analysis, more accurate predictive models to mitigate ongoing attacks, to prevent further damage and to make those detection algorithms immune to evasion & poisoning attacks. Allow cyber preventive detection to efficiently operate even in an encrypted flow without requiring up front decryption...</p> <p>TYPE OF SOLUTIONS WE'RE LOOKING FOR</p> <p>Threat detection, Behavioral analysis, Collaborative / Distributed Intrusion Detection Systems, Trustable Artificial intelligence, Security of industrial systems (such as SCADA), Adaptive security...</p>
<p>CHALLENGE 4 Impacts of quantum computing on cybersecurity</p> <p>Be prepared to the foreseen availability of quantum computation and the mathematical breakthrough it could bring.</p> <p>TYPE OF SOLUTIONS WE'RE LOOKING FOR</p> <p>"Quantum safe" cryptography & new generation of Key management systems (creation and distribution) leveraging quantum computing benefits...</p>	<p>CHALLENGE 5 Cybersecurity challenges of IoT</p> <p>Make IoT devices (and industrial IoT) and networks really secured in fast evolving market. Taking into account the huge number of devices while considering a seamless experience for the stakeholders, a measured security on such a large scale and the cost efficiency of the solution.</p> <p>Link & secure connectivity of the device. Create unique identity for secure management of devices. Ease integration of security for all the stakeholders along the value chain.</p> <p>TYPE OF SOLUTIONS WE'RE LOOKING FOR</p> <p>Objects identity creation & management (and IoT) Engineering and discovery) manages with very large scale and ensuring unique device identity. Distributed key generation / management. Light crypto compatible with embedded IoT environments. Collaborative and distributed security function.</p> <p>Facilitates initial connection of IoT devices. Universal subscription system (or supporting naturally multiple operators). Solution securing communications between devices, infrastructure & operators...</p>	<p>CHALLENGE 6 Cybersecurity of the Public Cloud</p> <p>Master the security level of public clouds and complement it to reach the expected security level. Make secure deployment of applications that don't share the same level of security. Maintain the applications in secure condition during the operations.</p> <p>TYPE OF SOLUTIONS WE'RE LOOKING FOR</p> <p>Tools efficiently supervising / managing an infrastructure that is distributed in a public cloud (cross-organizational, strengthen customer services & single point of failure avoidance). Solutions allowing application & data protection independently from public cloud operator (cloud security access broker, appliance & services for multi-tenant application management, tenant based data cryptography, Virtual ICM, VM and container security...</p>

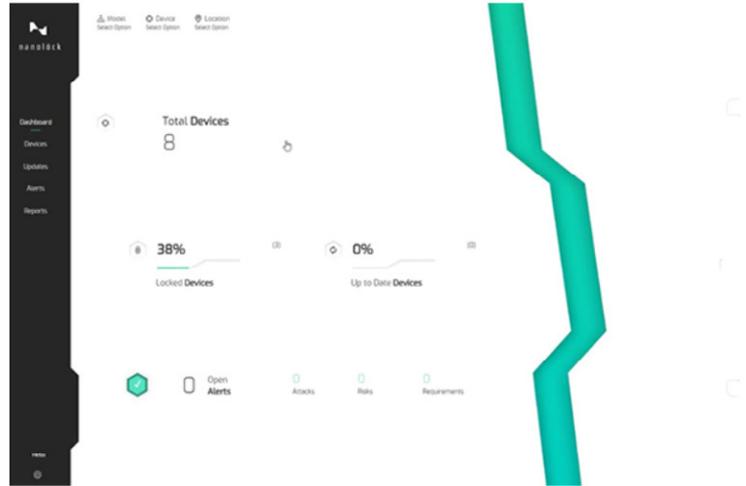
Chaque start-up sélectionnée devra relever l'un des six défis proposés par Thales (Crédit : Thales - agrandir l'image)

Akheros, la détection d'attaques inconnues

Cette société développe un composant logiciel de détection des incongruités comportementales au sein de réseaux informatiques. Elle permet de détecter des attaques avancées et persistantes (APTs) qui n'ont jamais été découvertes ou détectées au préalable. Ses algorithmes apprennent, sans supervision et sans intervention externe, le comportement d'une machine et construisent sa défense en tout point sur le réseau.

La solution est commercialisée comme un composant autonome de réseau (OEM) ainsi que comme un service (SaaS) permettant d'adresser les marchés de la défense de réseaux, du transport de matériaux sensibles, la surveillance de chaîne de production ainsi que la protection des infrastructures critiques.

Nanlock Security, pour protéger les objets connectés



(Crédit : Nanolock Security)

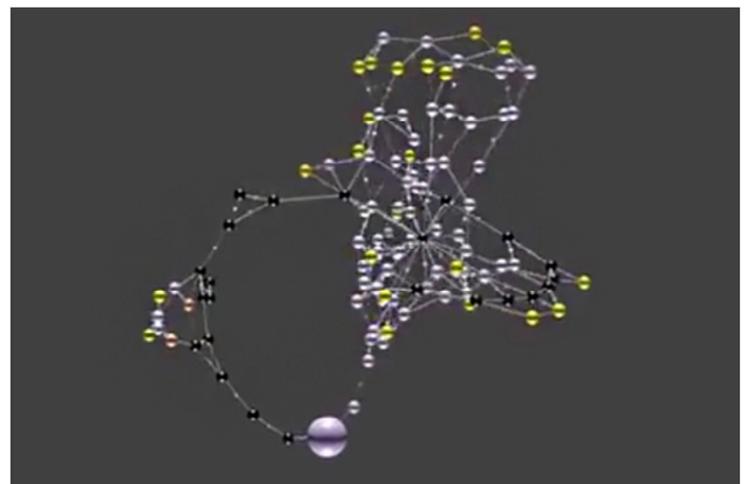
A l'origine d'une solution de sécurité et de gestion pour les périphériques connectés, Nanolock Security est une start-up américaine fondée en 2016. N'utilisant quasiment aucune ressource informatique et d'alimentation, Nanolock Security protège les microprogrammes et les informations sensibles stockées sur les périphériques IoT connectés, empêchant ainsi les attaques allant du ransomware à la manipulation malveillante du code stocké.

Grâce à une technologie embarquée et une plateforme de sécurisation des mises à jour, NanoLock empêche l'écrasement des modifications, la suppression des manipulations et les attaques sur les exécutable des applications d'image de démarrage du microprogramme et la configuration de tous les périphériques connectés et IoT.

Crypto Quantique, la puissance quantique au service de la cybersécurité

Start-up anglaise lancée en 2015, Crypto Quantique développe une plate-forme de cybersécurité à commande quantique qui exploite les processus quantiques dans les semi-conducteurs. Crypto Quantique se concentre sur la combinaison d'algorithmes cryptographiques à sécurité quantique avec les meilleurs éléments de la cryptographie moderne pour développer des produits matériels et logiciels évolutifs.

Cyber-Detect, solution d'analyse morphologique

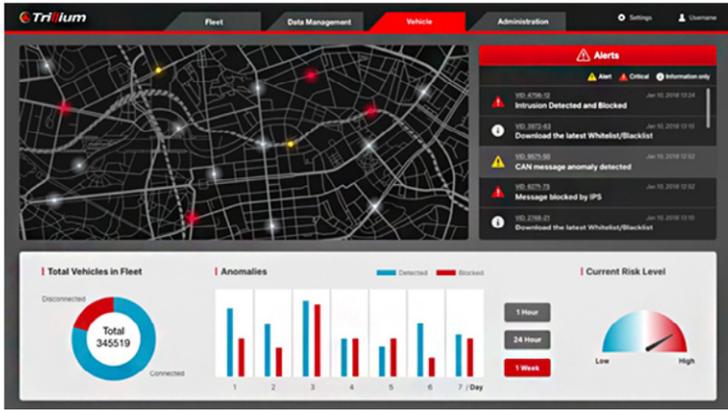


(Crédit : Cyber Detect)

Conçu à l'origine par le Laboratoire lorrain de recherche en informatique et ses applications (Loria), la solution Cyber-Detect permet de déconstruire les codes malveillants pour être capable de les analyser. Par un processus d'analyse morphologique, l'équipe de scientifiques renormalise ces codes pour contourner les processus d'obfuscations utilisés par les pirates. Une fois normalisés, les codes sont stockés dans une base de données pour être reconnus par la suite.

Trillium, protection des véhicules connectés

Trillium Secure assure particulièrement la sécurité des véhicules connectés et autonomes en plus de la confidentialité des informations privées. Via une plateforme as a service, les utilisateurs ont accès à une protection réseau embarquée, des algorithmes d'apprentissage automatique, des mises à jour en direct sécurisées et un centre d'opérations de sécurité.



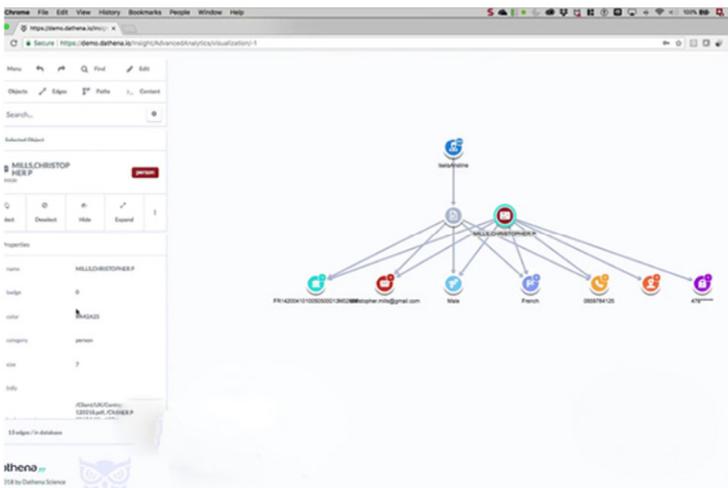
(Crédit : Trillum)

Les clients de cette compagnie japonaise sont principalement des équipementiers automobiles, des organisations d'aérospatiale et de défense, des compagnies d'assurance et des services de covoiturage pour former une défense multicouche contre les cyber-attaques. Elle dispose de centres de recherche et développement situés à Sunnyvale et Ann Arbor aux Etats-Unis, à Ho Chi Minh-Ville en Chine et à Tokyo.

Cylus, pour l'industrie ferroviaire

Toujours dans les transports, Cylus propose des solutions de protection informatique dédiée aux industries ferroviaires. Dirigée par des officiers de renseignement de l'armée israélienne, cette start-up fondée en 2017 propose d'ajouter une couche de sécurité supplémentaire aux systèmes existants pour détecter tous les terminaux connectés en bordures de voie et dans les trains.

Dathena, l'IA pour la data gouvernance



(Crédit : Dathena)

La solution de Dathena passe en revue toutes les données de l'utilisateur pour les identifier, les classer et les catégoriser grâce à des capacités d'apprentissage automatique et d'intelligence artificielle. Il peut, par exemple, regrouper des documents par sémantique, nature et sujet. La solution identifie automatiquement la valeur commerciale du contenu du référentiel de données, ainsi que les combinaisons toxiques de données, y compris les données personnelles, afin de respecter les réglementations en matière de confidentialité des données, telles que RGPD.

Quarkslab, deux solutions à la française

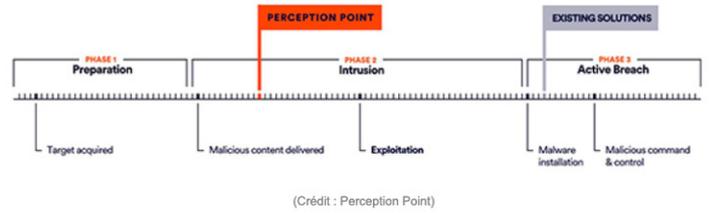
Lancée à Paris en 2011, Quarkslab propose deux solutions. Le premier, Irma, est une plateforme on premise d'analyse basée sur plusieurs moteurs pour permettre une meilleure détection des menaces. Le second, Epona, est une protection logicielle pour les applications d'entreprise. Agnostique et transparente, cet outil permet d'utiliser un processus d'obfuscation pour empêcher la compréhension de l'application par les cyberpirates. Ces derniers ne peuvent pas non plus les modifier. Avec 50 salariés, la société est basée en France, en Argentine et au Japon et développe sa clientèle dans des secteurs comme les médias, la finance, la défense, etc.

NuCypher, chiffrer les data lakes

NuCypher permet un partage transparent et sécurisé des données sensibles entre les organisations. L'utilisateur peut ainsi partager des informations avec ses partenaires, fournisseurs, clients ou régulateurs. Le propriétaire des données à des contrôles d'accès cryptographiques précis qui permettent une délégation et une révocation de l'accès à la demande, sans partage de clés privées.

La solution peut être déployée dans des blockchain autorisées ou de consortium, comme Hyperledger. Au lieu d'un réseau de nœuds entièrement décentralisé, les réseaux groupés peuvent spécifier une liste blanche de nœuds connus. Par exemple, des nœuds compatibles HIPAA ou RGPD.

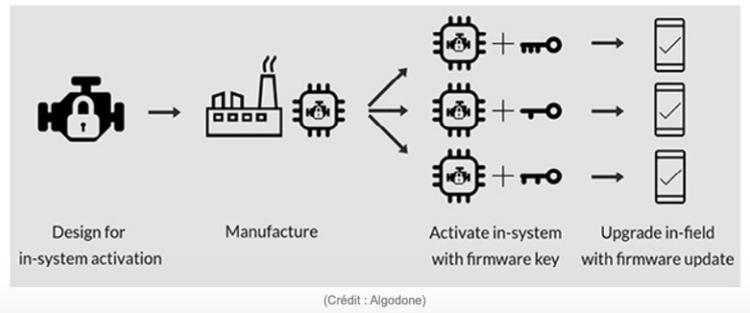
Perception Point, protéger les collaborations



(Crédit : Perception Point)

Autre société israélienne sélectionnée, Perception Point empêche les contenus malveillants d'infiltrer une entreprise via ses canaux de collaboration les plus ciblés, comme les messageries électroniques, les réseaux sociaux, les plateformes de partage de fichier ou les messageries instantanées. La technologie qu'elle développe intercepte les attaques au stade de l'exploitation pour une protection plus rapide et plus précise contre les menaces Zero-day, N-day et quotidiennes. Parmi les solutions qui intègrent Perception Point, on trouve notamment Office 365, G Suite, Dropbox, Box et Slack.

Algodone, permettre le développement du silicium as a Service



(Crédit : Algodone)

Lancé en 2015, en collaboration avec l'université de Montpellier, ce projet a pour but de créer un nouveau modèle économique pour l'industrie des semi-conducteurs, le Silicium as a Service. Grâce à une technologie brevetée de licence d'activation du silicium (SALT), les fondeurs peuvent activer ou désactiver des fonctionnalités, configurer des fonctionnalités tout au long du cycle de vie du silicium, surveiller et contrôler l'utilisation de l'appareil dans le temps, l'espace ou en fonction d'événements spéciaux et, plus important encore, de protéger les actifs de propriété intellectuelle (IP).



Article rédigé par
Nicolas Certes
Journaliste

Une erreur dans l'article?
[Proposez-nous une correction](#)

Les sciences font leur boum

La fête de la Science s'est ouverte ce vendredi. Les groupes scolaires ont pu découvrir différentes disciplines grâce à des stands et ateliers originaux. Samedi, le grand public est invité à en faire autant.

Il est un mélange savant entre le professeur Tourmesol, l'inventeur un peu loufoque des albums de Tintin et un post-ado à qui on aurait donné une multitude de jouets potentiellement explosifs ou brûlants. Sébastien Cahen, enseignant-chercheur en chimie minérale et chimie du solide, partage son métier avec le public à l'occasion de la fête des Sciences. L'événement commençait ce vendredi avec la visite des scolaires et se poursuit samedi avec le grand public. Les scientifiques de tous horizons présentent leurs disciplines. Et Sébastien s'amuse comme un petit fou. « J'ai mis des explosifs un peu partout dans le couloir d'entrée de la salle », annonce-t-il. Effectivement, lorsqu'on marche, on entend de petites déflagrations, comme celles que font les clacdoigts des enfants. Un bon moyen pour mettre les élèves de 3e dans l'ambiance avant de leur

montrer comment on fabrique une bille de chrome. Toujours le sens du spectacle : « On va avoisiner les 3.000 degrés », lance-t-il. « L'objectif, au fond, c'est de leur montrer que la chimie, c'est aussi du solide. » Et ça marche, les mêmes font des yeux ronds comme des billes de chromes. Il continue son show samedi.

Robot qui parle

« Serre-moi la main, robot », balance un effronté collégien de 4e à l'humanoïde blanc qui bouge et parle, mais ne s'exécute pas. « T'as pas d'autorité », le chambre un camarade. Le scientifique explique : « Serrer la main est un phénomène de synchronisation très complexe, que le robot ne peut pas encore réaliser. » La technologie n'est pas encore compatible avec les bonnes manières. Il répond à des questions simples et « aime bien qu'on lui touche les cheveux ». Chloé Merger est séduite. « Il me plaît car on peut discuter avec lui alors que ce n'est pas un être humain. Mais la robotisation, ça fait un peu peur tout de même... »

Léo Dufays, quant à lui, est en 3e au lycée de Monthureux-sur-Saône. Et cette sortie, ça le bot-



Sébastien Cahen montre à une classe de troisième comment fabriquer une bille de chrome. M.B.

te : « J'aime les sciences. J'ai appris que l'eau se filtre avec du charbon actif et du sable. » Il sort de la présentation de Jean François Munoz, qui analyse l'eau pour le laboratoire national de l'ANSES, à Nancy. « C'est l'une de nos missions de communiquer sur nos actions. Nous arrivons à adapter notre discours à notre public. » La plupart des stands et interve-

nants seront toujours là ce samedi, pour recevoir et informer le grand public.

Mathieu BLARD

Le programme de ce samedi

Parmi les nombreux stands, vous pourrez découvrir les maths par le jeu, apprendre à apprivoiser un robot, ou encore vous inviter aux neurosciences. Deux conférences, sur les ondes gravitationnelles et la transition énergétique seront proposées l'après-midi.

30.10.2018 / IT Social

Des failles de sécurité sur le protocole 5G

Par Yves Grandmontagne - 30/10/2018

La 5G est la future norme de la téléphonie, mais si elle améliore la protection des données, elle n'en demeure pas moins soumise à des failles persistantes.

Dans le cadre d'une publication scientifique présentée lors de la conférence CCS 2018 (*Computer and Communications Security*), qui vient de se tenir à Toronto, une équipe de chercheurs a révélé les résultats de travaux réalisés sur la sécurité de la 5G, la cinquième génération de communications mobiles.

Un outil issu de la recherche européenne

Ces travaux ont reposé sur l'outil de vérification de protocoles de sécurité Tamarin, développé par l'ETH de Zurich, l'équipe PESTO de Nancy, commune à Inria et au Loria, et le CISPA de Sarrebruck. Et l'analyse a montré que le protocole était insuffisant pour atteindre tous les objectifs de sécurité critiques avec les hypothèses énoncées dans le standard.

Concrètement, depuis l'introduction de la norme 3G et de l'AKA (*Authentication and Key Agreement*), un protocole de communication, le périphérique et le réseau doivent pouvoir s'authentifier l'un et l'autre au moment de la connexion au réseau. Et en même temps, les échanges de données, l'identité et la localisation de l'utilisateur doivent rester confidentiels.

Un protocole encore insuffisant...

Or, Tamarin a permis d'identifier automatiquement les hypothèses de sécurité minimale requises pour atteindre les objectifs de sécurité définis par le standard proposé par le projet de partenariat de troisième génération (3GPP).

L'analyse a ainsi montré que le protocole est insuffisant pour atteindre tous les objectifs de sécurité critiques avec les hypothèses énoncées dans le standard, ont révélé les scientifiques. En particulier, une implémentation trop rapide, mais respectant la norme, pourrait aboutir à une situation où un utilisateur est facturé pour les appels d'un autre utilisateur.



Mais il n'est pas trop tard !

La publication - qui a été présentée par Jannik Dreier, maître de conférences à l'Université de Lorraine (Télécom Nancy), en collaboration avec des chercheurs de l'ETH de Zurich (Suisse) et de l'Université de Dundee (Ecosse) - intervient alors que les premières expérimentations de la 5G sont en place. Le protocole améliore considérablement la protection des données par rapport à la 2G et la 3G. Mais cela semble encore insuffisant...

Le protocole 5G AKA doit encore être amélioré, la correction d'erreur doit pouvoir être faite avant le lancement de la 5G. Sinon... L'histoire des TIC nous a appris qu'un nouveau produit, fut-il un protocole de téléphonie, n'est jamais parfait à son lancement. Il faudra seulement espérer que les pirates rencontreront suffisamment de difficultés pour que la menace ne dépasse pas une publication scientifique.

MOTS CLES 5G Sécurité



Yves Grandmontagne
Journaliste IT, IT Social

5G : les réseaux mieux sécurisés qu'en 4G mais des failles demeurent

Le samedi 27 Octobre 2018 à 20:10 par Christian D. | 1 commentaire(s)



La 5G commencera à devenir réalité à partir de 2020 et permettra d'échanger toujours plus de données. Les échanges de données seront plus sécurisés que les générations précédentes mais les chercheurs pointent déjà du doigt l'existence de faiblesses dans les protocoles.



CleanMyMac X
Un Mac comme neuf. Tous les outils pour optimiser votre Mac, dans une seule app.

EN SAVOIR PLUS



Avec la 5G, il sera possible de partager des volumes toujours plus importants d'informations à des débits très élevés. Comme pour les générations précédentes, des systèmes de sécurisation seront exploités pour éviter le pillage de ces données, qui peuvent être sensibles, des informations à caractère médical aux données personnelles en passant par les transactions bancaires.

Des chercheurs ont évalué la qualité des mesures de sécurité de la future 5G. Dans leur rapport, ils notent que le niveau de sécurité va augmenter par rapport à la 3G et la 4G mais qu'il reste des points faibles dans les protocoles.



L'étude menée par l'Université de Lorraine, avec l'aide de l'ETH de Zurich et de l'Université de Dundee a fait passer la sécurité de la 5G à la loupe du logiciel **Tamarin** de l'ETH de vérification des protocoles de sécurité apportés par **5G AKA** (*Authentication & Key Agreement*) et a trouvé des insuffisances.

"L'analyse a montré que le protocole était insuffisant pour atteindre tous les objectifs de sécurité critiques avec les hypothèses énoncées dans le standard", indique Jannik Dreier, maître de conférences à Télécom Nancy. Il note notamment qu'"une implémentation trop rapide, mais respectant la norme, pourrait aboutir à une situation où un utilisateur est facturé pour les appels d'un autre utilisateur."

Malgré tout, la sécurisation du réseau 5G sera **significativement renforcée** par rapport à la 3G et la 4G et a gommé certaines faiblesses qui pouvaient être exploitées jusqu'à présent par les **IMSI Catchers** qui peuvent se substituer aux antennes-relais et intercepter les communications.

Il reste toutefois des possibilités d'attaques permettant une identification d'un téléphone et son suivi. En l'état, l'étude relève que des cyberattaques et des violations de la protection de la vie privée peuvent être réalisées si le protocole est lancé tel quel mais des discussions sont en cours avec le 3GPP pour apporter des améliorations avant le lancement effectif de la 5G.

06.11.2018 / L'Est Républicain

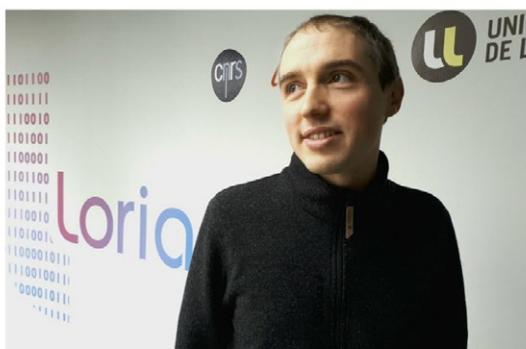
Cybersécurité

Nancy : des chercheurs pointent les failles de la 5G

Réputée plus fiable que la 4G, la 5G va se généraliser à partir de 2020. Mais son protocole de sécurité présente encore des lacunes selon une équipe de chercheurs lorrains, suisses, allemands et écossais.

Par Sarah LABIDI - 06 nov. 2018 à 05:01 | mis à jour à 07:30 - Temps de lecture : 2 min

1 | Vu 1773 fois



Jannik Dreier, enseignant chercheur au Loria et maître de conférences à Telecom Nancy. Photo S.L.



Les mobiles ne rameront plus à partir de 2020. C'est du moins la promesse de la 5G qui devrait en effet réduire considérablement la vitesse de téléchargement des contenus Internet. Seront-ils pour autant plus fiables ?



Pas vraiment selon Jannik Dreier, maître de conférences à France Telecom et chercheur au Loria (Laboratoire lorrain de recherche en informatique et ses applications), du moins si aucune modification n'est apportée au protocole de sécurité, le 5G AKA (Authentication and key agreement). Si ce nouveau protocole améliore considérablement la protection des données par rapport aux technologies 3G et 4G, il demeure vulnérable aux cyberattaques. C'est ce que démontre l'étude menée par l'Université de Lorraine, avec l'aide de l'ETH de Zurich et de l'Université de Dundee en Écosse. Ce n'est pas tout : « L'analyse a montré que le protocole était insuffisant pour atteindre tous les objectifs de sécurité critiques avec les hypothèses énoncées dans le standard », précise Jannik Dreier. « En particulier, une implémentation trop rapide, mais respectant la norme, pourrait aboutir à une situation où un utilisateur est facturé pour les appels d'un autre utilisateur. »

Pour ce faire, ils ont passé le 5G AKA à la moulinette de « Tamarin », un outil de vérification formelle développé par l'ETH de Zurich, l'équipe PESTO de Nancy, commune à Inria et au Loria, et le CISPA de Sarrebruck.

260 \$ pour tracer une puce

Et qu'est-ce qui ne tourne pas rond ? On savait déjà qu'avec un intercepteur IMSI (International mobile subscriber identity) un équipement « qui ne coûte que quelques centaines d'euros » (260 \$ sur Alibaba), n'importe qui peut localiser et « tracer » une carte de téléphone portable simplement en écoutant les transmissions entre le mobile et l'antenne du réseau. C'est d'ailleurs ainsi que procèdent les services de police et les agences de renseignements. Avec le nouveau protocole, c'est à peine plus compliqué : « Désormais, une clé sert à chiffrer les échanges entre le mobile et l'antenne, ce qui permet de se protéger de ces intrus passifs », explique le chercheur. « Mais pas des intrus actifs qui ne se contentent pas d'écouter mais qui envoient aussi des messages. » L'enjeu est énorme : « Si la nouvelle technologie de communication mobile est introduite avec ces spécifications », la protection de la vie privée n'est plus assurée et c'est la porte ouverte à de coûteuses cyberattaques. L'équipe de chercheurs, qui a présenté sa publication à la Computer and Communications Security, à Toronto, une des plus grandes conférences internationales en matière de sécurité informatique, est en contact avec la 3GPP, l'organisme de standardisation réunissant les industriels de la téléphonie.

Edition Nancy et agglomération

Meurthe-et-Moselle



Le vote électronique, une bonne idée ?

CHRONIQUE. Contrairement à une idée reçue, il n'est pas si facile de faire voter électroniquement à grande échelle et en toute confiance. Mais des solutions partielles apparaissent.

 Lire plus tard | Sciences & Prospectives |    |  Commenter

Par **Gerard Berry**

Publié le 3 nov. 2018 à 14h00

A première vue, l'informatisation du vote semble une bonne idée : simplicité, gain de temps, résultats immédiats, etc. Mais ce n'est pas si simple, à cause de contraintes incontournables : seuls les inscrits doivent pouvoir voter ; un vote doit être unique, confidentiel et non vendable ; le comptage doit être exact, vérifiable et revérifiable ; l'ajout de faux bulletins doit être impossible ; etc. La liste est longue !

**LA CHRONIQUE
DE GÉRARD BERRY**

[Lire la suite de l'article \(en version abonné uniquement\).](#)

Dans le jardin de l'IA l'arbre de décision



Quand un programme informatique répond par oui ou par non à un test, cela peut être représenté par un embranchement. Chacune des branches peut conduire à un nouveau test, donc, à un nouvel embranchement. L'arbre de décision pousse ainsi. Ses

ramifications dont d'autant plus nombreuses que les tests sont diversifiés. Pourtant, rien ne « pousserait » dans ce jardin de l'IA, si les scientifiques ne plantaient pas, dans le terreau de l'informatique, des graines sous la forme de « jeux de données ». Explications avec Marie-Dominique Devignes, chercheuse CNRS au Loria, spécialiste en bio-informatique.



Marie-Dominique Devignes, marie-dominique.devignes@loria.fr

les nouveaux patients et patientes sont bien classés. Si le programme se trompe trop souvent, il faut refaire pousser un arbre en élargissant le jeu de données d'apprentissage. A l'instar des êtres humains, l'IA a ses contraintes : la machine ne peut pas apprendre correctement sur des jeux de données limités.

« En santé, l'aide à la décision ne surgit pas d'une terre vierge. Les médecins disposent déjà d'algorithmes de diagnostic basés sur leurs connaissances, leurs pratiques, leurs recherches. Cette expertise peut être représentée sous forme d'arbres de décision informatiques, ce qui permet aux machines d'exécuter ces raisonnements. Mais les machines peuvent aussi faire pousser de nouveaux arbres qu'elles « apprennent » à partir des données. Par exemple, pour comprendre pourquoi certains patients ou patientes répondent à un traitement, nous allons collecter toutes les données biomédicales disponibles sur eux, et les grouper en deux classes, selon qu'ils ou elles répondent ou non. La machine va analyser ce jeu de données et en extraire ce qui est prédominant dans chaque classe, sous forme de tests constituant les embranchements d'un arbre de décision. Cet arbre est optimal pour le jeu de données fourni, mais il n'est cependant qu'un modèle qu'il faut ensuite valider en vérifiant si

Quel rapport entre l'IA et le « web sémantique » ?

Un endroit où l'on trouve des masses de données, c'est le web. Les technologies du web sémantique permettent de faire de l'IA sur les données du web. En effet, elles donnent du sens à ces données pour que les machines puissent en apprendre quelque chose comme le feraient les êtres humains. Ainsi, la classification des pathologies doit d'abord être représentée selon les standards du web sémantique - c'est ce qu'on appelle alors une « ontologie » biomédicale - pour pouvoir être ensuite utilisée par un programme capable de calculer des similitudes entre des individus malades. Depuis longtemps, la recherche en IA essaye « d'apprendre » les ontologies biomédicales de façon automatique à partir des publications scientifiques sur le web. C'est très difficile car le langage écrit est complexe de même que les concepts médicaux.

Qu'appelle-t-on une « boîte noire » dans le monde de l'IA ?

C'est par exemple le résultat de l'apprentissage par les réseaux de neurones, profonds (« deep learning ») ou non. On rentre dans la boîte, en posant une question précise sur un cas particulier, avec toutes les données nécessaires, on en sort avec la réponse fournie par le réseau de neurones (par exemple « Oui, ce patient va répondre au traitement »). La boîte est noire car le réseau ne sait pas dire pourquoi il donne cette réponse. Il utilise seulement le résultat d'un entraînement à partir de milliers de questions du même type dont on connaissait déjà la réponse. C'est le contraire de l'arbre de décision ou des ontologies, qui se veulent intelligibles. Le défi est maintenant de combiner les performances de l'IA « boîte noire » avec les qualités de l'IA intelligible.»

Humain et logiciel : le complément d'intelligences

Les performances spectaculaires de l'IA dans le domaine de la santé, entre autre, en font un filon prometteur pour les GAFAs et autres BATX (concurrents chinois). Au milieu des annonces médiatiques des uns et des promesses mirifiques des autres, la nécessité de clarté et de pédagogie s'impose. Dans ce cadre, une rencontre avec Erwan Kerrien, chercheur en informatique dans l'équipe Magrit, commune au centre Inria Nancy - Grand Est et au Loria, est tout indiquée. Lui, sa préoccupation, c'est la quête de l'image artificielle intelligente !

« Inria collabore depuis longtemps avec le CHRU de Nancy et GE Healthcare (ex General Electric Medical Systems). Les médecins ont une bonne vision à long terme de leur discipline mais pas forcément conscience des voies d'améliorations technologiques possibles pour l'atteindre progressivement. Il faut être présent à leur côté, assister à des examens et « vivre » la difficulté au moment où elle se présente. C'est là, précisément, que nous pouvons mettre en commun nos diverses spécialités pour progresser.

Où est l'IA dans tout cela ? Je vois plutôt une collaboration de l'intelligence humaine...

Il y a effectivement une tendance à réduire l'IA au Machine Learning et, à sa sous-catégorie, le Deep Learning. Moi, je m'intéresse à l'image et à la compréhension automatique de ce qu'il y a dedans.

Une image représente un monde tri dimensionnel avec des objets, en l'occurrence, pour le médical, l'anatomie du patient. Mon objectif, c'est de pouvoir avoir une représentation intelligible de ce monde tri dimensionnel, à partir des images réelles.

Là-dessus, l'œil et l'intelligence humaine sont d'emblée plus performants : le médecin sait lire une image et distinguer les os, les organes, une éventuelle pathologie. L'ordinateur, lui, ne voit d'abord que des points de mesure dans l'espace : les pixels. Comment passer de ces points à quelque chose qui est proche de la compréhension du médecin ?

Je m'intéresse également beaucoup à la simulation par l'image en temps réel. Elle pourrait nous donner accès à des informations invisibles sur l'image

comme, par exemple, la pression artérielle mesurable in vivo. Faire de la simulation de fluide permettrait de voir le trajet du sang notamment en cas d'anévrisme. Aujourd'hui, le traitement s'arrête lorsque l'image montre qu'il n'y a plus de sang à l'intérieur de cet anévrisme.

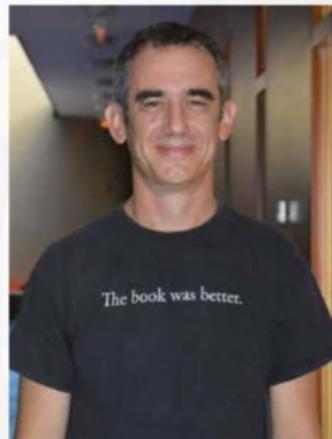
Avec un système plus intelligent, qui inclurait une simulation fiable par rapport à l'image, c'est-à-dire reproduisant la réalité dans l'espace et le temps par l'informatique, nous aurions d'autres arguments pour planifier et réaliser le traitement.

Qu'apporte la réalité augmentée ?

Une des manières d'améliorer l'interprétation de l'image, c'est d'ajouter des informations tri dimensionnelles sur l'image bidimensionnelle que regarde le médecin. Elle offre ainsi une synthèse intuitive de diverses informations complexes qui aide le médecin dans ses décisions, sans les prendre à sa place. Par exemple, il a été envisagé, à un moment d'automatiser le diagnostic de la mammographie grâce au Diagnostic Assisté par Ordinateur. Ce n'est pas arrivé. En revanche, les systèmes mis au point actuellement indiquent au médecin où il doit regarder précisément. Il suit ce conseil ou pas, mais il peut gagner du temps sur chaque examen. En résumé, j'essaie de faire en sorte que l'image complexe, pas toujours très informative et multimodale, puisse être synthétisée et facilement interprétable.

Une image 100% artificielle et donc 100% efficace ?

Non. Mais nous pouvons témoigner, nous informaticiens, après plusieurs années de travail avec les médecins, de



Erwan Kerrien,
erwan.kerrien@inria.fr

leur reconnaissance des apports de l'informatique et de leur volonté de les intégrer en routine.

Il est clair, pour chacun d'entre nous, que chaque innovation intelligente en santé restera soumise à une validation médicale humaine.»

KIWI la team de l'interaction homme / machine

Ne vous fiez pas à son allure juvénile : Sylvain Castagnos n'a rien d'un adolescent qui cherche sa voie. « Informatique / IA / Interaction Homme/Machine » semble répéter ce maître de conférences en montrant l'écran d'un ordinateur du Loria pour affirmer sa conviction : l'IA en santé est un outil qui aidera le médecin à repousser les limites de son art. Elle est, ni plus ni moins, aussi miraculeuse que la pénicilline en son temps.



Sylvain Castagnos, sylvain.castagnos@loria.fr

« Au Loria, je fais partie du département « Intelligence Artificielle, système complexe et robotique » et au sein de ce département, je suis membre de l'équipe KIWI (Knowledge Information and Web Intelligence). Nous concevons des services personnalisés sur Internet.

C'est à dire ?

Sur le web aujourd'hui, la quantité de données disponibles, correspondrait à une pile de bouquins (NDRL : la petite histoire ne dit pas le nombre de pages de chacun) qui ferait deux fois la distance de la Terre à Alpha du centaure, soit plus de 8,5 années-lumière. Pas facile de s'y retrouver ! Il a donc fallu construire l'accès à des informations personnalisées. C'est pourquoi, les moteurs de recherche actuels captent vos traces et modélisent vos préférences lorsque vous interagissez avec eux pour vous fournir ce contenu adapté.

Quel lien avec la santé ?

De la même manière, nous essayons de personnaliser les interactions entre des utilisateurs et des outils informatiques dans ce cadre. A titre d'exemple, nous avons travaillé avec le département « Maladies du vieillissement - Gériologie - Soins

palliatifs » du CHRU de Nancy, sur la mise au point d'une application pour faciliter le diagnostic précoce de la maladie d'Alzheimer et sur l'accompagnement des malades. Les médecins de la spécialité nous ont expliqué que les tests neuropsychologiques actuels ne disposent pas d'indicateurs très fiables.

Quelle a été votre contribution pour améliorer ces dispositifs ?

Un de ces tests par exemple consiste à demander de relier dans le bon ordre des chiffres figurant dans des cercles. L'âge des personnes testées et leur fragilité peut être handicapante et susceptible de fausser les résultats. Pour constituer une base de données plus fiable, nous avons d'abord numérisé ce test et réfléchi à de nouveaux modes d'interaction entre la personne et la machine. Ainsi, un dispositif de reconnaissance du geste (système kinesthésique) ou du regard, avec une caméra infrarouge détectant les positions de la main ou des pupilles du sujet, la durée de son regard et son insistance. Tout cela repose sur de l'IA à partir d'une base d'apprentissage rassemblant les données récupérées grâce aux tests effectués par divers groupes de

populations : personnes âgées sans trouble, ou avec des troubles moteur ou cognitifs. Nous obtenons alors des « données étiquetées » croisant les performances des utilisateurs avec le diagnostic du médecin : il a une maladie ou pas. C'est à partir de là que les algorithmes essayent de trouver les liens statistiques qui font que telle ou telle métrique (des unités identiques qui se répètent dans la durée) a une incidence sur le résultat.

Ces travaux avec l'IA pourraient-ils encore aller plus loin ?

L'IA pourrait être à visée diagnostique : est-ce que le sujet a, ou pas, un trouble cognitif ? Si oui, est-il plus ou moins probable qu'il soit symptomatique d'une maladie d'Alzheimer ?

Mais nous avons encore beaucoup de travail à faire et des fonds à trouver : les outils ont été développés mais nous manquons de données. Nous ne pouvons pas nous permettre la moindre marge d'erreur car les conséquences seraient dramatiques.

Le malade n'est pas un humain en panne !

On parle beaucoup d'intelligences artificielles au pluriel, comme si c'était des «créatures savantes», sans savoir ce que cela recouvre effectivement dans la réalité, il faudrait être plus circonspect. Amedeo Napoli, informaticien, travaille sur l'intelligence artificielle, la fouille de données et l'apprentissage machine. Sa spécialité est la « découverte de connaissances dans les données ». Directeur de recherche CNRS et responsable de l'équipe de recherche Orpailleur, commune au centre Inria Nancy Grand Est et au Loria, ses travaux s'appliquent en biologie, chimie et médecine, entre autres.

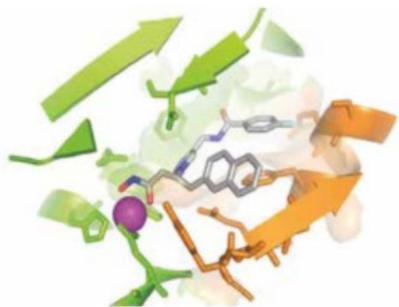


Amedeo Napoli, amedeo.napoli@loria.fr

« Dans les années 80, au temps des «systèmes experts», on a cru que le diagnostic médical ne serait plus qu'une formalité. En fait, cela a échoué car, si les systèmes de diagnostic de panne fonctionnent assez bien, l'humain n'est pas une machine et son diagnostic de dysfonctionnement est nettement plus complexe !

Quelles études mène l'équipe de recherche Orpailleur ?

Nous faisons de la fouille de données. Par exemple : prenons une table à deux entrées qui met en relation des individus et des caractéristiques. Nous cherchons à mettre en évidence les caractères qui discriminent les individus atteints ou non d'une maladie en cours d'étude. Ensuite, une fois identifiés, nous cherchons à savoir si certains caractères ou marqueurs discriminants sont prédictifs de la maladie. Ces deux tâches sont souvent très difficiles à mener.



Quels sont les objectifs de vos travaux ?

Une des idées est de faire des analyses plus complètes pour mettre en place du dépistage de pathologie à grande échelle. Le problème, c'est que nous ne savons pas pendant combien de temps un marqueur va être discriminant et / ou prédictif. Le monde évolue dans des environnements fluctuants et, à un moment donné, tel facteur va prendre de l'importance dans la pathologie en s'associant avec certains autres marqueurs qui n'ont pas d'effets isolément. C'est très complexe de travailler sur la combinaison des marqueurs et leurs interactions avec l'environnement.

Sur quoi travaillez-vous actuellement ?

Beaucoup de choses... Avec des nutritionnistes de Clermont-Ferrand (INRA), nous cherchons des marqueurs prédictifs du diabète de type 2 dans une cohorte où sont enregistrées des données sur des personnes depuis plus de 20 ans. Cette étude est globale et tient compte de caractéristiques liées à la biologie, la génétique, les habitudes et les lieux de vie, etc.

Nous menons également des recherches sur les antibiotiques dont on sait que l'efficacité est remise en question par la résistance bactérienne. À tel point que l'Organisation Mondiale de la Santé en a fait une priorité. Nous disposons de bases de données d'antibiotiques existants et des bases de molécules candidates pour devenir éventuellement des antibiotiques. S'y ajoutent d'autres molécules dont on aimerait savoir si elles ont des caractéristiques

propres aux antibiotiques. Il faut alors tester des assemblages innovants qui peuvent donner des antibiotiques nouveaux à valider ensuite à la paillasse. Trouver de nouvelles stratégies informatiques pour combiner ces structures moléculaires devrait faire avancer l'état de l'art.

Grâce à un système qui s'appuie sur des principes d'intelligence artificielle ?

Ces recherches relèvent de la découverte de connaissances et sont, de fait, liées à l'IA. Longtemps les données ont été « opposées » aux connaissances. Clairement, l'aller-retour entre elles est permanent et naturel. D'un côté, les données peuvent être analysées pour révéler des éléments de connaissance. De l'autre, les connaissances peuvent intervenir en fouille de données et aussi être gérées et analysées comme des données. Aujourd'hui, il est bon de gommer certains clivages et de travailler de concert pour traiter des problèmes médicaux difficiles mais importants pour toute la société. »

L'IA pour que l'humain fasse de vieux os

A lors que le Grand Est se mobilise pour créer un Gérontopôle avec l'aide de la Région Grand-Est, de l'Agence Régionale de Santé et de la CARSAT, depuis quelques années déjà, un groupe multidisciplinaire de scientifiques (gériatres, psychologues, sociologues, mathématiciens, informaticiens) accompagné d'industriels et d'associations d'usagers (Welcoop, Pharmagest, ONPA,...) travaille sur l'amélioration de la vie des personnes âgées à travers leur cadre de vie. Ce qui se dessine, c'est que le domicile de demain concentrera des technologies issues de l'Intelligence Artificielle pour permettre l'autonomie à long terme. En témoignent Christine Perret-Guillaume, gériatre au CHRU de Nancy et François Charpillet, directeur de recherche Inria et coordonnateur de « l'Habitat Intelligent en Santé ».



François Charpillet,
francois.charpillet@inria.fr

Christine Perret-Guillaume,
c.perret-guillaume@chru-nancy.fr

François Charpillet : « C'est le principe de l'habitat augmenté par des technologies multiples : robotique, capteurs intelligents, domotique, etc. Nous avons mis au point un dispositif qui devrait être commercialisé fin 2018, CARELIB, incluant un capteur qui détecte les chutes et évalue la capacité de la personne à se déplacer. Derrière cette technologie, il y a de l'IA et de l'apprentissage automatique.

Comment choisissez-vous vos sujets d'étude ?

Christine Perret Guillaume : Nous listons les besoins par des regards croisés entre les usagers, les professionnels de santé, les industriels et les structures associatives sur la technologie, le numérique et l'IA. Il faut préserver ces échanges entre scientifiques et personnes de terrain car ces innovations seront intégrées à des environnements qui doivent rester humains.

FC : Avec cet appartement intelligent, nous évaluons les solutions proposées, ce qui est faisable ou pas, avec un objectif d'industrialisation. Nous devons être capables de produire des équipements abordables, sachant qu'ils seront diffusés au plus grand nombre. Cette contrainte très forte nous impose des choix techniques pertinents.

Aujourd'hui, un robot humanoïde, au stade de la recherche fondamentale, vaut plus de 250 000 €. Nous réfléchissons à des outils moins sophistiqués comme, par exemple, une solution conçue sur la base du modèle de robot-aspirateur qui permettrait d'observer les situations à risque, voire d'appeler les secours.

Toutes ces technologies s'inscrivent donc dans une logique de surveillance de l'individu même

si c'est pour la bonne cause... ?

CP-G : C'est bien pour cela qu'il faut un encadrement éthique. En tant que professionnels de gériatrie, nous préférons parler de sécurité. Ce sont bien ces innovations qui rendent possibles la prévention primaire et secondaire et la réadaptation. Nous commençons à travailler sur le repérage de la fragilité de la personne âgée pour déterminer à quel moment sa façon de bouger et de se comporter change dans son environnement et comment un habitat augmenté pourrait permettre une stimulation intelligente pour maintenir son autonomie.

FC : Il y a un rapport direct entre ces outils et les bénéfices que le public pourra en tirer. Si l'on met au point des technologies qui ne font que du « flicage », elles ne seront pas acceptées. En revanche, si le service est là, l'usager acceptera de perdre une partie de son intimité.

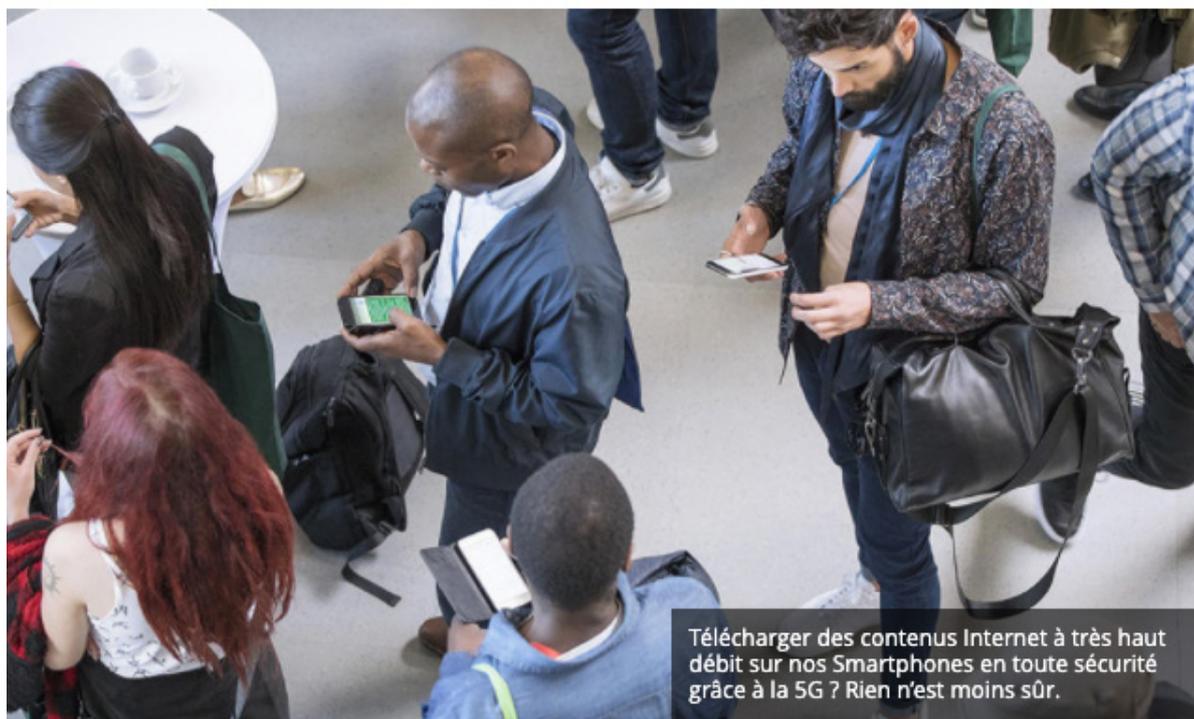
Est-ce que vous vous projetez vous-même en future personne âgée quand vous créez ces innovations ?

CP-G : Nous sommes influencés par les personnes âgées que nous rencontrons, mais, de là, à se projeter nous-mêmes...

FC : La vraie question c'est : pourquoi mettre cette recherche technologique au service de la santé ? Justement parce que ces travaux ont un impact immédiat à plus court terme. Surtout, cela me permet d'avoir des contacts avec des personnes d'autres spécialités et d'autres milieux. Je sors la tête du labo ! »

La 5G en mal de sécurité

23.11.2018, par [Martin Koppe](#)



© Caiaimage/TomMerton/GETTY IMAGES

[Partager](#)

Avec un débit dix fois supérieur à celui de la 4G, la 5G fait rêver. Mais avant que ce bolide ne débarque dans nos mobiles en 2020, il reste un point crucial à améliorer : la sécurité. Explication.

Avec des pointes prévues à 20 gigabits par seconde, la tempête 5G devrait atteindre nos téléphones en 2020. Les utilisateurs se réjouissent de l'approche de cette cinquième génération de standard de télécommunication mobile qui, avec des débits jusqu'à dix fois plus rapides que la 4G, promet de s'adapter à des usages nomades toujours plus gourmands en données.

Alors que ce standard est encore en cours de conception au 3GPP^[1], organisme qui regroupe des représentants d'industriels et d'opérateurs téléphoniques, différentes équipes de recherche profitent de cette phase d'élaboration pour tester et renforcer la future norme.

Ainsi, au [Laboratoire lorrain de recherche en informatique et ses applications](#) (LORIA)^[2], Jannik Dreier et ses collègues proposent différentes pistes d'amélioration. « *Le 3GPP met surtout en avant la hausse du débit, explique ce maître de conférences à Télécom Nancy, mais les protocoles changent aussi à chaque nouvelle génération, notamment en matière de sécurité.* »

Des failles anciennes

En collaboration avec les chercheurs de [l'école polytechnique fédérale de Zurich](#) et de l'université de Dundee en Écosse, Jannik Dreier a souligné la survivance de failles de sécurité dans la nouvelle norme 5G, lors de la conférence CCS^[3] de Toronto, en octobre 2018. « *La téléphonie mobile a hérité de points faibles qui remontent à son tout premier protocole d'identification, déplore-t-il. Toute la sécurité repose sur les cartes SIM, où sont stockées les clés d'identifications partagées avec les réseaux.* » Les problèmes de sécurité sont inhérents aux technologies sans fil car, contrairement à un transport de données confiné dans un câble, rien ne protège les informations quand elles transitent par la voie des airs.

« Contrairement à un transport de données confiné dans un câble, rien ne protège les informations quand elles transitent par la voie des airs. »

La sécurité passe donc par la capacité du téléphone et du réseau à s'identifier et à s'authentifier lors de la connexion. Dans le même temps, toutes les informations personnelles et les données du détenteur de la ligne téléphonique doivent être préservées. Mais le système n'est pas parfait. Jannik Dreier pointe ainsi les risques de traçabilité de l'utilisateur lorsqu'on peut identifier puis suivre le téléphone. Une opération encore aujourd'hui aisément réalisable avec la 4G, grâce à des appareils comme les intercepteurs IMSI^[4] qui scrutent les échanges entre le téléphone mobile et les antennes-relais du réseau pour pister leur cible.

« *La 5G va régler le problème face à un intercepteur passif, qui ne fait qu'écouter, détaille Jannik Dreier. Mais si quelqu'un injecte des messages dans la communication entre téléphone et antenne du réseau, ce qui est relativement facile, alors il peut à nouveau tracer le mobile et son utilisateur.* »



Des antennes relais permettent de tester la 5G en conditions réelles, comme ici en Allemagne.

© OLIVER BERG / DPA / dpa Picture-Alliance/AFP

[Partager](#)

Le problème du compteur

Là encore, c'est l'architecture historique des téléphones mobiles qui est en cause. Comme les premières cartes SIM ne pouvaient pas générer de valeurs aléatoires, tout reposait et repose toujours sur un système de compteur. Conçu pour ne pas recevoir plusieurs fois un même message, celui-ci réagit quand il est sollicité.

« Pourtant, les cartes d'aujourd'hui pourraient s'en passer, car elles peuvent générer des valeurs aléatoires, déplore le chercheur, mais apparemment les décideurs n'ont pas voulu changer le standard aussi profondément. Les outils exploitant la traçabilité sont notamment utilisés par la police et les services de renseignement. Ils leur permettent de savoir qui était à proximité d'une scène de crime, mais aussi d'une manifestation. C'est très pratique pour eux, mais engendre un risque de surveillance de masse », poursuit-il. Difficile en effet de ne pas craindre de dérives, sans même compter le détournement par des criminels, quand les deux tiers de la population mondiale utilisent un téléphone portable.



La 5G était à l'honneur lors du Congrès mondial du mobile, qui s'est tenu à Barcelone en février.

© Miquel Benitez / GETTY IMAGES EUROPE / Getty Images/AFP

Partager

Des appels facturés à autrui

Conçu en partenariat avec l'école polytechnique de Zurich, le LORIA et le CISPA [5] de Sarrebruck, l'outil de modélisation Tamarin permet d'analyser la fiabilité d'un protocole donné. Jannik Dreier et ses collègues ont ainsi testé la version adaptée à la 5G d'AKA [6], le protocole de sécurité implémenté depuis la 3G que le 3GPP veut continuer d'améliorer. « On ne fait pas que dénicher des failles et nous ne cherchons pas qu'à casser, souligne Jannik Dreier. Nous procédons à des vérifications formelles afin d'améliorer la sécurité. »

Si le protocole ne contient pas de faille, Tamarin établit alors une preuve mathématique de sa sécurité. En revanche, en cas de problème, l'outil génère une description de l'attaque identifiée. Les chercheurs ont ainsi découvert un défaut pouvant amener à une situation où les appels sont facturés à quelqu'un d'autre, si deux téléphones sont utilisés en même temps et à proximité.

“Malgré l'approche de l'échéance de 2020 et l'arrivée officielle de la 5G, de nombreuses améliorations peuvent encore être apportées, surtout au niveau logiciel.”

« Même si cette faille est probablement difficile à exploiter en pratique, elle n'est pas exclue par le standard. Nous avons envoyé ces résultats au 3GPP et ils nous ont fait un premier retour assez bref, précise le chercheur. Le processus prend en effet du temps, car il passe par des réunions physiques, des propositions, puis, enfin, un vote. Nous ne faisons pas partie de ces instances, cela reste leur choix de modifier ou non le protocole. »

Malgré l'approche de l'échéance de 2020 et l'arrivée officielle de la 5G, de nombreuses améliorations peuvent encore être apportées, surtout au niveau logiciel. Les chercheurs du LORIA travaillent d'ailleurs à adapter des outils tels que Tamarin, afin que les ingénieurs puissent s'en servir dès la conception.

La partie matériel et équipement est en revanche très difficile à changer une fois celui-ci produit et déployé. « Les problèmes de traçabilité ne vont malheureusement pas être réglés uniquement avec ce genre de petits changements, insiste Jannik Dreier. Il faudrait tout simplement arrêter d'utiliser un compteur dans les cartes SIM, mais cela exigerait une refonte totale du protocole... » ♦

Notes

1. Pour 3rd Generation Partnership Project, « Projet de partenariat de troisième génération ».
2. CNRS/Université de Lorraine/INRIA.
3. Pour Computer and Communications Security, « Sécurité des ordinateurs et des communications ».
4. Pour International Mobile Subscriber Identity, « Identifiant international de client mobile ».
5. Pour Center for IT-Security, Privacy & Accountability, « Centre pour la sécurité, la vie privée et la responsabilité informatiques ».
6. Pour Authentication and Key Agreement, « Accord sur les clés d'authentification. »

Des failles de sécurité dans la future norme de communication mobile 5G

7 décembre 2018, 00:50 CET



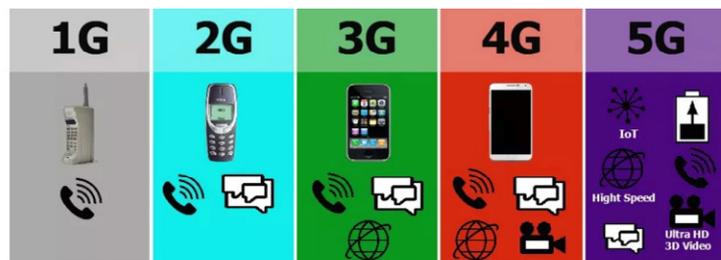
Réseaux mobiles, Geralt/PhotoBay

Les deux tiers de la population mondiale, soit environ cinq milliards de personnes, utilisent quotidiennement un téléphone mobile. Ils se connectent au réseau via leurs cartes SIM, passent des appels, envoient des SMS, échangent des images ou effectuent des achats. Le réseau est, bien entendu, vulnérable aux attaques. À maintes reprises, des délinquants ont pu accéder à des communications lors de la connexion de l'appareil au réseau afin d'intercepter des conversations ou de voler des données.

Comment progresser en matière de sécurité ? La cinquième et dernière génération de communications mobiles (5G) prévue pour un déploiement d'ici 2020 devrait offrir plus de garanties aux utilisateurs. Afin de soutenir la sécurité, le périphérique et le réseau doivent pouvoir s'authentifier l'un et l'autre au moment de la connexion. En même temps, les échanges de données, l'identité et la localisation de l'utilisateur doivent rester confidentiels. Pour cela un protocole de communication appelé Authentification and Key Agreement (AKA) est mis en œuvre depuis l'introduction de la norme 3G.

Protocole 5G AKA

La norme de communication mobile 5G s'appuie donc sur le protocole 5G AKA. Le nouveau protocole améliorera considérablement la protection des données par rapport aux technologies 3G et 4G. Notamment, grâce à lui, un problème a été résolu concernant une faille auparavant exploitée par les intercepteurs IMSI (International Mobile Subscriber Identity). Avec ces appareils, l'identité internationale d'abonné mobile d'une carte de téléphone portable pouvait être lue pour déterminer l'emplacement d'un appareil mobile et suivre un utilisateur. Pour ce faire, l'appareil avait seulement besoin d'écouter les transmissions entre le téléphone mobile et l'antenne du réseau mobile. Cela n'est plus possible désormais avec le 5G AKA.



Les possibilités des différents réseaux, TheDuran.com, CC BY-NC

Comment évaluer globalement la sécurité offerte par le protocole 5G AKA ? Pour le vérifier, notre équipe du laboratoire d'informatique Loria, en collaboration avec des chercheurs de l'École Polytechnique Fédérale de Zurich, l'Université de Dundee et le Centre National sur la Cybersécurité de Sarrebruck a utilisé l'outil de vérification de protocoles de sécurité Tamarin. Il a permis d'identifier automatiquement les hypothèses de sécurité minimale requises pour atteindre les objectifs de sécurité définis par le standard proposé par l'organisme de standardisation 3GPP. L'analyse a montré que le protocole était insuffisant pour atteindre tous les objectifs de sécurité critiques avec les hypothèses énoncées dans le standard. En particulier, une mise en œuvre trop rapide, mais respectant la norme, pourrait aboutir à une situation où un utilisateur est facturé pour les appels d'un autre utilisateur.

Nous avons montré que le protocole permettait également d'autres types d'attaques, notamment des attaques de traçabilité. Lors de ces attaques, le téléphone mobile n'envoie pas l'identité complète de l'utilisateur, mais un attaquant peut identifier un téléphone, et le tracer. Vu les faiblesses identifiées, si la nouvelle technologie de communication mobile est introduite avec ces spécifications, cela peut entraîner de nombreuses cyberattaques avec des conséquences sur la protection de la vie privée.

Vérification formelle

Pour aboutir à ce résultat, nous nous sommes appuyés sur la vérification formelle. Il s'agit de vérifier que tout standard assure des propriétés de sécurité suffisantes pour être commercialisé. Tout système ou programme grand public possède un document de spécification technique que nous appelons un standard. Ce document est en général public et décrit avec précision le contenu et fonctionnement du système. C'est à partir de ce document de spécification que nos chercheurs ont pu faire ces vérifications.

L'avantage de l'approche permet de tester différentes propriétés comme l'authentification, la confidentialité, la traçabilité avant la commercialisation du système. Le logiciel « Tamarin » permet de bâtir des modèles mathématiques précis du système à partir du standard et d'y insérer des scénarios d'intrusion pour ainsi construire des preuves de ce qui est garanti ou non. Comme par exemple l'authentification afin d'être sûr qu'on s'adresse à la bonne personne. Tamarin est également un outil d'aide à la décision car il permet d'évaluer rapidement des solutions alternatives pour parer aux failles détectées.

La vérification formelle est utilisée en particulier pour la sécurité dans l'automobile et l'aéronautique. Il est évidemment crucial que les standards utilisés dans les avions ne contiennent pas de bugs. L'objectif de la vérification n'est donc pas seulement de trouver des failles mais au contraire d'assurer leur absence, donc d'améliorer le système en proposant des alternatives et des corrections.

Il faut toujours se préoccuper des brèches pour éviter des conséquences graves. Dans les protocoles de communication 3G et 4G, il y a une faille permettant à une personne malveillante de suivre un autre individu, et cette faille est effectivement exploitée en pratique par les intercepteurs d'IMSI. Nous sommes en contact avec le 3GPP pour résoudre les problèmes identifiés dans la norme 5G, mais le problème de la traçabilité est complexe et nécessite une importante remise à niveau.

☞ téléphonie mobile informatique piratage cybersécurité normes

NOTRE ETABLISSEMENT |

« Permettre à l'Homme de vivre dans de meilleures conditions » : l'intelligence artificielle selon Sylvain Castagnos



Publié le 17/12/2018



Présents lors du Salon « Osez l'économie de demain » le 13 décembre dernier, Sylvain Castagnos et le LORIA présentaient notamment le projet d'application mobile de la « National Gallery » de Londres. Une application intégrant une intelligence artificielle permettant au visiteur d'obtenir un parcours de visite personnalisé. Maître de conférences en intelligence artificielle à l'IDMC – LORIA, le travail de recherche de Sylvain Castagnos consiste à concevoir des assistants intelligents capables d'améliorer les interactions entre le grand public et les services en ligne. Il s'agit en particulier de les aider à trouver la

meilleure information, à répondre à leurs besoins ou à leur faire gagner du temps. Ses travaux se déclinent dans plusieurs domaines applicatifs tels que l'e-éducation, la e-santé, l'héritage culturel, la musique en ligne... Ces systèmes reposent sur la modélisation du comportement des utilisateurs et sur des algorithmes d'intelligence artificielle et collective.

“ C'est la machine qui doit proposer des interactions adaptées pour être le plus utile possible. ”

Quelle est votre définition de l'intelligence artificielle & collective ?

L'intelligence artificielle permet, entre autres, de mieux comprendre le comportement humain et de s'adapter automatiquement aux exigences et attentes des utilisateurs. Ce n'est pas à l'Humain de s'adapter à la machine. C'est la machine qui doit proposer des interactions adaptées pour être le plus utile possible. La modélisation des phénomènes collectifs permet ensuite de rapprocher un utilisateur à une communauté et d'exploiter automatiquement la connaissance acquise par cette communauté (sur la base des expériences passées) pour lui fournir des recommandations adaptées.

“ Aider les utilisateurs à faire le tri. ”

Comment s'est imposée l'intelligence artificielle dans votre activité ?

Mes premiers travaux de recherche s'inscrivaient dans le domaine des systèmes de recherche et d'accès à l'information (moteurs de recherche, intranets documentaires). La quantité d'information disponible sur Internet et le nombre d'internautes ont crû de manière exponentielle ces 20 dernières années, au point qu'il devient difficile de trouver l'information pertinente dans un temps raisonnable sans avoir recours à ces algorithmes. Une problématique plus récente est venue s'ajouter au problème de passage à l'échelle : la véracité des informations présentes sur Internet. Il s'agit donc d'aider les utilisateurs à faire le tri pour identifier les ressources utiles et importantes qu'ils n'auraient pas nécessairement consultées spontanément, tout en écartant les fausses informations et les informations non pertinentes. Il ne s'agit en revanche pas de censurer l'accès à l'information ou d'aller à l'encontre des principes de respect de la vie privée. Les modèles d'Intelligence Artificielle s'inscrivent donc dans un contexte multi-objectif (temps de calcul, précision, vie privée...). Ces mêmes modèles se sont par la suite avérés pertinents dans d'autres domaines applicatifs pour l'aide à la personne (e-éducation, e-santé, héritage culturel...).

“ L'Europe et la France prennent la pleine mesure de ces risques. ”

Selon votre point de vue quels seront les conséquences de l'immersion de l'intelligence artificielle dans le futur ?

L'intelligence artificielle est un outil puissant permettant d'assister l'Homme dans ses tâches quotidiennes ou lui permettre de vivre dans de meilleures conditions. Mais comme toute technologie, elle comprend des risques qu'il faut veiller à maîtriser. Nous entendons beaucoup parler ces derniers temps de grandes entreprises ayant collectées des informations personnelles à l'insu des utilisateurs à des fins commerciales, voire à des fins de manipulations politiques. Fort heureusement, l'Europe et la France prennent la pleine mesure de ces risques en promulguant des lois pour protéger les usagers. Il est tout à fait possible de fournir la même qualité de service aux usagers tout en étant respectueux de leur vie privée et en ayant une démarche éthique. C'est ce à quoi nous nous employons.

01101100
01101111
01110010
01101001
01100001
01101100
01101111
01110010
01101001
011000010111
111001001111
1000010111
11111111

Loria

