LA REVUE DE PRESSE 2016 DU Loria

De nouveaux outils contre Alzheimer

30.05.2016, par Fui Lee Luk

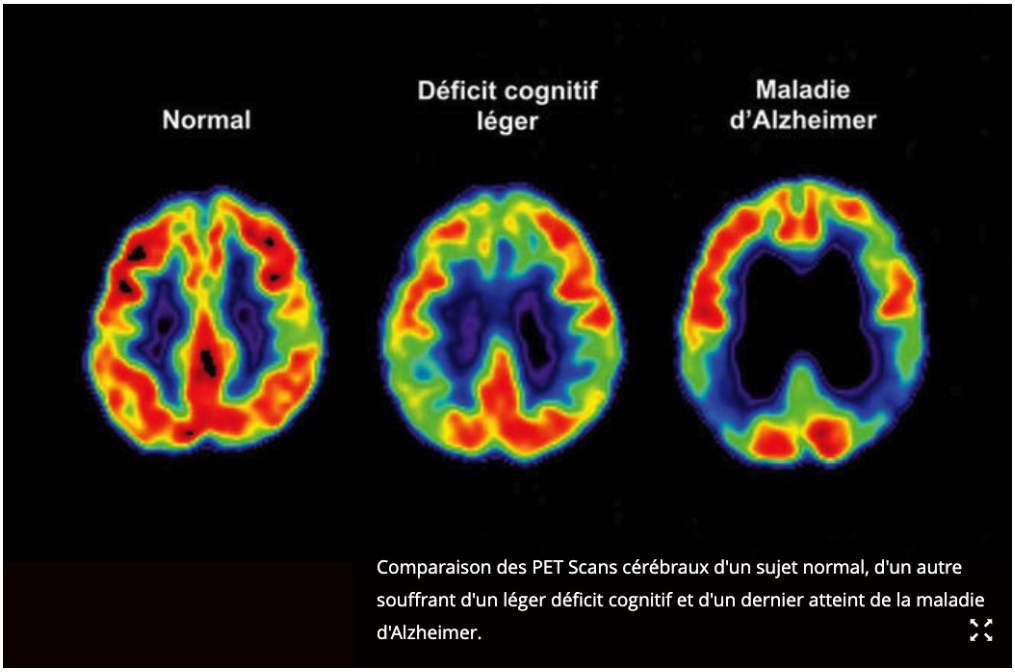
Les chercheurs ne cessent de développer des techniques toujours plus innovantes pour détecter plus tôt la maladie d'Alzheimer et aider les patients à mieux vivre avec.

C'est l'un des acquis les plus manifestes du monde moderne, et qui, du moins en théorie, profite à tous : partout dans le monde, les gens vivent plus longtemps. En un siècle, l'espérance de vie globale a plus que doublé, principalement en raison des avancées médicales et des progrès sanitaires. Cette longévité accrue fait que, dans de nombreux pays, les personnes âgées sont la classe d'âge qui connaît la plus forte croissance démographique. Cela pose de nouveaux défis à la société qui doit désormais prendre en compte les problèmes auxquels doit faire face une population vieillissante, notamment la prolifération des maladies liées à l'âge, telle la maladie d'Alzheimer. Pour en améliorer le diagnostic et la prise en charge, les chercheurs des équipes Knowledge, Information and Web Intelligence (Kiwi)1, Applied Research for (multi) Media Enrichment, Diffusion, Interaction and Analysis (Armedia)2 et Algorithmes, composants, modèles et services pour l'informatique répartie (Acmes)3, développent des outils exploitant les nouvelles technologies de l'information et de la communication.

Diagnostiquer plus tôt

La maladie d'Alzheimer est la forme la plus répandue de démence. Elle affecte principalement les personnes âgées de plus de 65 ans. Sur le plan cérébral, elle se manifeste par la formation et l'accumulation de plaques dans les fibres des cellules corticales et par une dégénérescence neurofibrillaire conduisant à la perte des connexions neuronales, et finalement à la mort des cellules du cerveau. Les patients perdent progressivement la mémoire ainsi que leurs capacités cognitives et réflexives jusqu'à tomber dans un état de dépendance totale.

L'un des premiers défis posé par Alzheimer est son diagnostic. Les techniques d'imagerie cérébrale comme l'imagerie par résonance magnétique (IRM) permettent de révéler les lésions qu'entraîne la maladie, notamment l'atrophie de certaines régions cérébrales. Il n'est toutefois pas toujours facile de déterminer le moment où un tel examen devient nécessaire, ni de faire la distinction entre une perte de mémoire liée à un Alzheimer et celle normalement observée chez toute personne âgée. Cette difficulté à détecter tôt la maladie empêche la prise en charge précoce des malades. Rien qu'aux États-Unis, alors qu'on estime qu'une personne de plus de 65 ans sur neuf souffrait d'Alzheimer en 2015, la moitié ne connaissait pas son affection4. Un diagnostic précoce est pourtant crucial pour stimuler les patients et les aider ainsi à maintenir leurs capacités cognitives le plus longtemps possible.



Comparaison des PET Scans cérébraux d'un sujet normal, d'un autre souffrant d'un léger déficit cognitif et d'un dernier atteint de la maladie d'Alzheimer.

Ce besoin en méthodes de diagnostic simples et fiables a motivé deux équipes de recherche du CNRS. Installée en Lorraine, l'équipe Kiwi s'efforce d'adapter les services offerts par des dispositifs informatiques aux besoins et aux préférences des usagers. Ce qui l'a conduite à chercher de nouveaux moyens de détecter les personnes souffrant de troubles neurodégénératifs tels Alzheimer ; sachant que la qualité de l'interaction entre l'utilisateur et ce qui apparaît à l'écran – clics, pages visitées, etc. – dépend beaucoup de l'état de sa mémoire.

Numériser les tests neuropsychologiques

Kiwi a également développé une version numérisée de tests neuropsychologiques qui n'étaient utilisés jusque-là qu'en version « papier et crayon ». Comme, le TMT (Trail Making Test), où le sujet doit relier un ensemble de points le plus rapidement possible. Concevoir des tests adaptés aux sujets visés – en l'occurrence des personnes âgées peu familiarisées avec les ordinateurs et souffrant de tares pouvant affecter tant leurs capacités perceptives que leur mobilité – s'est révélé assez complexe, note Sylvain Castagnos de Kiwi. La numérisation des tests a finalement permis aux chercheurs de disposer d'un outil de diagnostic fiable et automatisé, ce qui réduit ainsi le risque d'erreurs humaines lors du recueil des données.

La démarche de Kiwi a aussi permis d'améliorer les tests classiques en permettant l'intégration de plusieurs méthodes et outils d'exploration. Notamment en recourant à un oculomètre capable de suivre la direction du regard, rendant ainsi possible la mise en évidence des liens possibles entre des gestes ou des mouvements oculaires atypiques et la maladie d'Alzheimer. Les chercheurs ont d'ailleurs l'intention d'exploiter cet oculomètre pour stimuler les patients par des exercices cérébraux permettant de ralentir la progression de la maladie.

Modéliser pour mieux reconnaître

En collaboration avec l'unité de gériatrie du CHU de Nancy, les chercheurs de Kiwi sont en train de collecter et de comparer les données de trois populations de patients – Alzheimer, amnésiques non Alzheimer et sujets normaux – afin d'isoler les variables les plus susceptibles de révéler la pathologie du patient. L'étape suivante consistera à élaborer les modèles mathématiques qui permettront de classifier le comportement des utilisateurs en temps réel et d'aboutir à un diagnostic précoce de la maladie.

Parallèlement, à Évry, l'équipe Armedia tente elle aussi de développer une méthode de diagnostic différente des tests neuropsychologiques et de l'imagerie, basée cette fois sur l'écriture. « Spécifiquement humaine, l'écriture constitue une activité de haut niveau qui fait appel à des facultés mentales de planification, d'anticipation et de régulation », souligne la chercheuse Sonia Garcia-Salicetti. « Une maladie neurodégénérative va détériorer ces facultés, ce qui aura un effet visible sur la façon d'écrire », complète son collègue Mounîm A. El-Yacoubi.
Le dispositif d'Armedia est constitué d'une tablette tactile recouverte d'une feuille de papier sur laquelle le sujet peut écrire. Basé sur ce que l'équipe appelle une « activité naturelle », ce dispositif présente l'avantage d'être la fois simple à utiliser et non invasif.

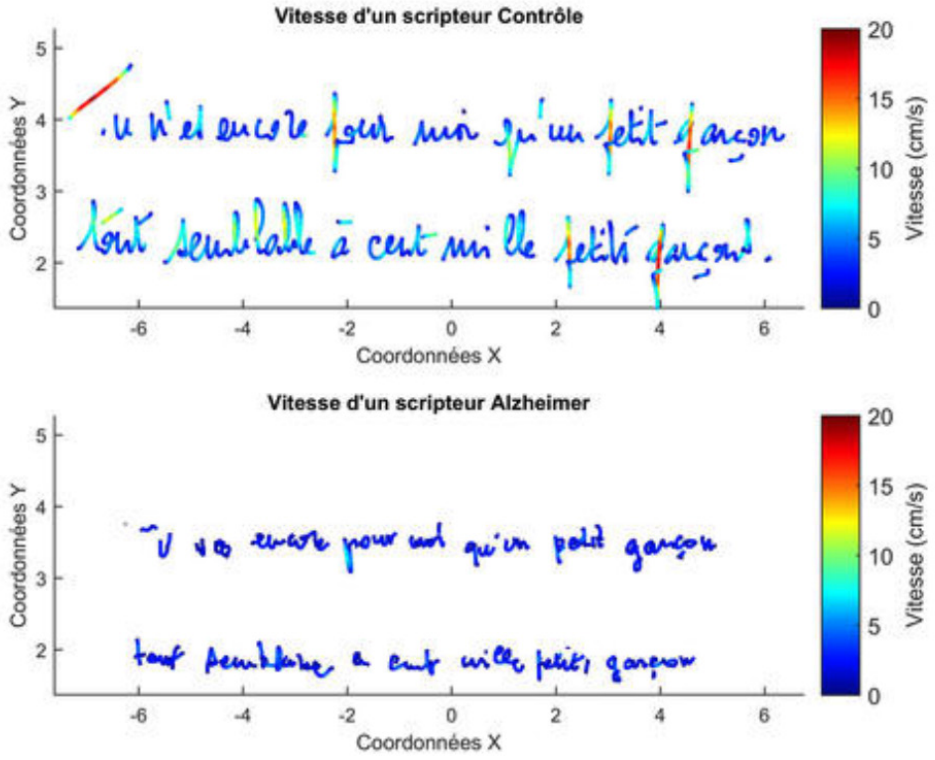
La tablette numérise et enregistre la trajectoire du stylo en temps réel ; le dispositif est ainsi en mesure d'extraire et d'analyser des informations cinématiques dont l'interprétation va permettre de détecter toute dégradation

significative des capacités d'écriture. De cette façon, le système peut reconnaître des symptômes moteurs couramment associés à Alzheimer tels qu'une lenteur, un tremblement, une raideur ou des saccades liées à une perte de la fluidité du geste d'écriture.

Accompagner les patients Alzheimer est également l'objectif que s'est fixé une autre équipe du Samovar, l'Acmes. Elle a développé pour ce faire des dispositifs d'assistance et d'accompagnement des activités routinières, tant à domicile qu'à l'extérieur. « Lorsque les patients évoluent dans un environnement peu familier (et même parfois familier), la désorientation et la déambulation sont des symptomes fréquents des troubles de mémoire et de cognition », explique l'informaticien Daqing Zhang, membre de l'équipe. Le dispositif permet de suivre en temps réel les patients, « ce qui réduit considérablement la charge de travail des soignants ou de la famille, constamment obligés de les surveiller ». Il s'agit d'un appareil équipé d'un GPS qui modélise sous forme de graphes les itinéraires réguliers. L'algorithme développé par l'équipe reconnaît en temps réel un itinéraire qui s'écarte trop du trajet habituel et envoie des alertes à l'usager pour qu'il retrouve le bon chemin.

Pour l'intérieur, l'Acmes a mis au point des « pense-bêtes intelligents » capables de remédier aux troubles mnésiques. Par exemple, grâce à des capteurs « sensibles au contexte » disposés dans la maison et capables de reconnaître l'activité du patient pour y réagir intelligemment. Un message peut être envoyé via un haut-parleur ou un téléphone à une personne qui oublie de refermer la porte du four après avoir répondu au téléphone, par exemple. Une autre méthode consiste à agir sur la planification des tâches. Si un usager oublie de fermer la porte d'entrée à clé, le système le lui rappellera en tenant compte de l'urgence, et des autres tâches en cours. Dans l'attente de leur commercialisation, les prototypes de l'Acmes sont testés in situ dans plusieurs pays européens.

Pour Daqing Zhang, l'objectif poursuivi par l'équipe de chercheurs est d'offrir « des solutions à la fois peu coûteuses et peu intrusives ». À défaut de pouvoir trouver rapidement un traitement curatif pour la maladie d'Alzheimer, elles permettront d'améliorer la vie de ceux qui en sont affectés et celle de leurs proches.



L'analyse de l'écriture sur une tablette graphique permet de diagnostiquer la maladie. Ici, une étude comparative de l'écriture d'une personne atteinte par la maladie (en bas), montre une altération.

Notes

1.Laboratoire lorrain de recherche en informatique et ses applications (CNRS/Univ. de Lorraine).
2.Services répartis, Architectures, Modélisation, Validation, Administration des Réseaux (CNRS/Institut Mines-Télécom/Télécom Sud Paris).
3.Services répartis, Architectures, Modélisation, Validation, Administration des Réseaux (CNRS/Institut Mines-Télécom/Télécom Sud Paris).
4.Alzheimer's Association, « Alzheimer's Disease Facts and figures », Alzheimer's & Dementia (2015), vol. 11 (3) : 332-384.

40 ans d'informatique en Lorraine, le Loria fête son anniversaire

Vous avez 40 ans en 2016, quels sont les éléments qui ont le plus marqué votre histoire ?

Nous sommes présents en Lorraine depuis 1976, notamment grâce aux travaux de nos chercheurs notamment sur la programmation et sur la reconnaissance de la parole. Cela nous a permis d'exister et de donner naissance au CRIN, ancêtre du Loria. À l'époque nous étions 70. Aujourd'hui 450 personnes travaillent dans nos murs. C'est grâce au Loria et aux travaux de ses chercheurs que vous pouvez taper vos courriers sans faute grâce à un logiciel de traitement de texte avec un correcteur d'orthographe, protéger votre ordinateur contre les virus, etc. Notre quotidien au laboratoire est donc marqué par de nombreuses découvertes qui ont un réel impact sur notre société.

Pouvez-vous nous dire sur quoi travaillent vos chercheurs actuellement ?

Le Loria sera très prochainement équipé d'un Creative Lab, une sorte de vitrine expérimentale qui permettra à nos chercheurs de travailler autour des systèmes physiques et robotiques. Ces systèmes sont en interactions directes avec des robots mobiles, des robots humanoïdes, des drones, des bâtiments connectés, etc. Ce Creative Lab est un bel investissement pour l'avenir.

■ **Un des plus grands laboratoires de la région lorraine fête ses 40 ans.**

Qu'avez-vous prévu pour cet anniversaire ?

Nous organisons le 2 juin, une grande célébration officielle avec nos partenaires et tous les acteurs ayant contribué au développement de la recherche informatique en Lorraine. Au mois d'octobre nous fêterons la science et notre anniversaire sur le site Artem et à la faculté des sciences et technologies et nous vous proposerons de découvrir les travaux de nos chercheurs via de nombreux ateliers.

Recherche Du Crin au Loria, quarante ans de recherche et d'innovation célébrés jeudi sur le campus Sciences

L'informatique visionnaire de Nancy

Nancy. La place de Nancy est connue mondialement pour avoir été le port d'attache d'une école de mathématiciens qui se cachaient derrière le nom imaginaire de Nicolas Bourbaki. C'était dans les années 50-60. Place forte en maths, Nancy est aujourd'hui l'un des phares de la recherche en informatique. Des mathématiciens qui ont mal tourné, qui sont devenus des artistes de l'algorithme qui fait aujourd'hui partie de notre vie quotidienne.

« Un des plus beaux fleurons informatiques du Grand Est »

Les algorithmes qui se cachent derrière le GPS de votre voiture, qui s'égaillent dans votre smartphone, qui sécurisent les sites web sur lesquels vous effectuez vos achats, qui rendent les jeux vidéos de plus en plus réalistes, les robots de plus en plus performants (notamment dans le domaine médical), ces algorithmes ont toutes les chances d'être issus des recherches menées au Loria, le Laboratoire lorrain de recherche en informatique et ses applications.

En quarante ans, on est passé de l'ordinateur de 30 kilos au tout numérique, souligne-t-on volontiers au Loria. Du refus du ministère de créer une agrégation d'informatique au prétexte qu'il venait de refuser une agrégation d'hôtellerie, à des chaires numériques.

40 ans, c'est l'anniversaire qu'a justement choisi de célébrer le laboratoire ce jeudi sur le campus en présence de ses partenaires scientifiques, institutionnels, industriels, sous l'égide de ses trois tutelles, l'Inria (Institut national de la recherche en informatique et en automatique), le CNRS et l'Université de Lorraine.

■ **Le laboratoire de recherche en informatique et ses applications.** Photo d'archives Patrice SAUCOURT

40 ans, le bel âge pour tirer un premier bilan, et pouvoir encore regarder l'avenir avec confiance ? Cet anniversaire a permis de réunir le fondateur, les anciens directeurs, l'actuel, de Claude Pair, qui a rendu hommage à Jean Legras, professeur de mécanique, véritable père de l'informatique à Nancy dès les années 60, à Jean-Yves Marion, l'actuel patron du labo, en passant par Jean-Pierre Finance, qui fut directeur du Crin (Centre de recherche en informatique de Nancy qui s'est mué en Loria au milieu des années 80), et qui souligné « la formidable aventure humaine » de ces 40 ans de recherche informatique. Il était dit que les vicissitudes institutionnelles qui ont émaillé l'histoire du labo n'allaient pas gâcher la fête. D'autant que le Loria, qui s'est fixé quatre axes de recherche (santé, sécurité, intelligence artificielle, enseignement) peut s'enorgueillir d'être, selon Pierre Mutzenhardt, le président de l'UL, « un des plus beaux fleurons informatiques du Grand Est », et « un des rares labos au monde qui travaillent sur les logiciels malveillants », glisse Eric Freyssinet, colonel et ancien doctorant du Loria, aujourd'hui conseiller contre les cybermenaces au ministère de l'Intérieur.

Bientôt une nouvelle plateforme

Le numérique étant devenu notre lot quotidien, le Loria encourt-il le risque de se banaliser, de faire l'objet d'attention dans quelques dizaines d'années d'archéologues du savoir ? Pas question de s'endormir sur les lauriers recueillis. Le Creativ'Lab CPS (Cyber-Physical-System) et Robotique, nouvelle plateforme qui sera inaugurée au début de l'année prochaine, sera un lieu unique d'innovation rassemblant tout ce concerne les drones, l'humain et la robotique. Une collaboration a été engagée entre les trois écoles d'Artem (Mines, ICN, Beaux-Arts) et le CHU de Nancy afin de développer des orthèses et prothèses de main par impression 3 D.

Ph. R.

En chiffres

▶ **Le Loria compte cinq départements, 29 équipes de recherche, 180 chercheurs et enseignants-chercheurs, 100 doctorants.**

▶ **Les contrats de recherche perçus lui rapportent annuellement 2,5 M€.**

▶ **Il a généré en quatre ans pas moins de neuf start-ups.**

▶ **Ses chercheurs produisent 600 publications internationales par an. Ils sont l'auteur de 354 communications depuis le 1er janvier 2015.**

▶ **Le Loria a fécondé ce qui allait devenir l'Ecole supérieure d'informatique appliquée de Lorraine (Esial, aujourd'hui Nancy Télécom).**

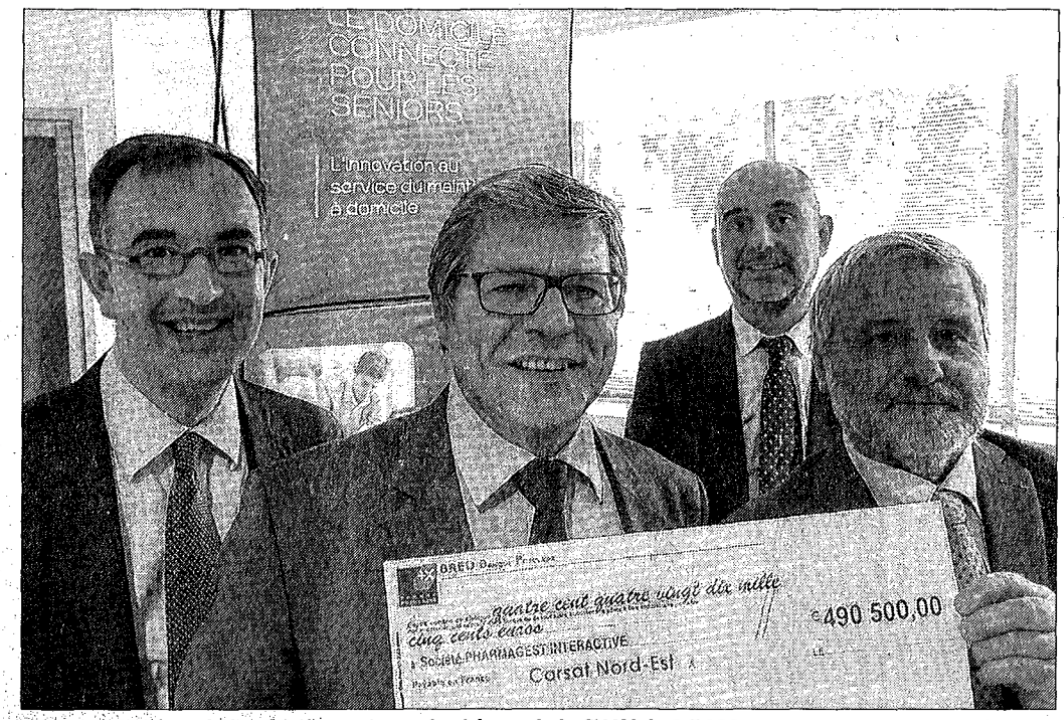
▶ **Le Loria compte 9 lauréats ERC (bourses européennes prestigieuses) et un chercheur membre du non moins prestigieux l'IUF (Institut universitaire de France).**

▶ **48 nationalités sont représentées au sein du laboratoire.**

Vieillesse Le maintien à domicile va s'améliorer grâce aux innovations de Pharmagest

Des capteurs chez les seniors

« Nous sommes en train de tester nos capteurs ». Plusieurs cadres de Pharmagest les ont en effet installés chez eux. Parfois, ils font exprès de tomber, pour voir si le système retrace fidèlement l'événement ! La filiale nouvelles technologies de Welcoop est en effet en train de développer un outil révolutionnaire dont le but affiché est de permettre aux anciens de retarder le plus longtemps possible le départ dans un Ehpad ou à l'hôpital. « Si on gagne un an ou deux de maintien à domicile, les économies seront énormes », explique le président de la Carsat, Hubert Attenont, que le projet rend enthousiaste.



■ **Les partenaires de l'opération ont reçu le chèque de la CNAV de 0,5 M€.** Photo ER

495.000 €

Pas seulement lui, d'ailleurs, puisque la CNAV, Caisse nationale d'assurance vieillesse, investit massivement dans le projet. Jeudi dernier, elle a fait un chèque de 495.000 € aux partenaires que sont Welcoop, qui investit l'essentiel d'une note qui devrait s'élever à plusieurs millions d'euros, au travers de Pharmagest, et la Carsat-Nord-Est. Les perspectives sont extraordinaires, sachant qu'en 2020, le pays comptera 27 millions de personnes âgées…

En quoi consiste techniquement le projet ? Des capteurs reliés en réseau centralisent des données sur un système d'intelligence artificielle capable d'apprendre le profil de chaque personne âgée dans son environnement. À partir de là, il fait tinter une alarme chez un opérateur médico-social (l'OHS en l'occurrence), qui mettra en train une riposte adaptée. Les capteurs 3D développés avec le Loria fonctionnent comme la « Wii ». Ils sont capables de décrypter les mouvements et certaines actions des personnes âgées. Ce qu'on appelle des « signaux faibles ». Par exemple, une chute. Si elle est lente ou brutale. Une chute lente est paradoxalement un signal plus dangereux que rapide. Ou encore la fréquence avec laquelle le tiroir à couverts est actionné. Si l'utilisation s'espace, un problème de dénutrition peut apparaître, la personne pouvant oublier de se nourrir. Ou alors le calcul du nombre de pas. Une perte d'autonomie peut passer par une phase où l'on marche de moins en moins, avec des pas de plus en plus courts…

Le dispositif est en cours de tests chez ceux qui le mettent au point, à Pharmagest. Mais en 2017, une phase expérimentale suivra chez des personnes âgées volontaires dans plusieurs foyers logements du département participant à l'opération. « Le prix de revient est de 200 € par personne », explique le président de la Carsat. « Mais plus on multipliera le dispositif, moins il sera cher ». Surtout, gagner un à deux ans avant la dépendance, c'est une économie pas seulement pour les Caisses vieillesse, mais aussi pour les intéressés, sachant que le prix moyen dans un Ehpad est de 2.500 € par mois, ce qui excède le montant de la plupart des retraites…

Guillaume MAZEAUD

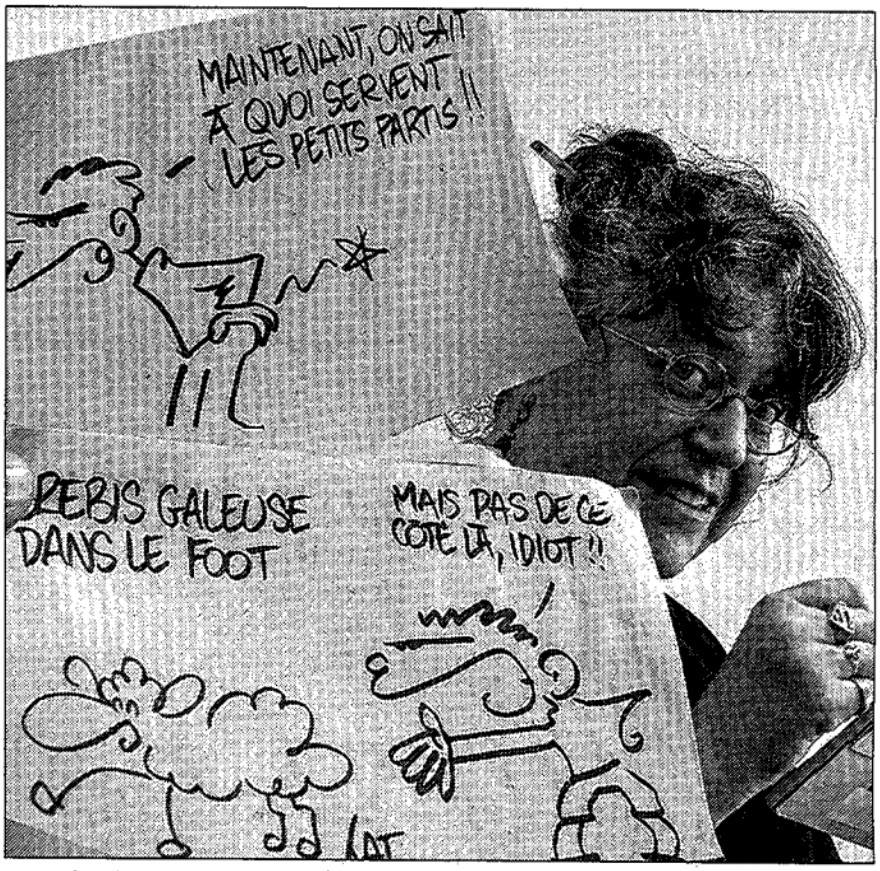
Création La dessinatrice et blogueuse Catherine Créhange a créé sa propre boîte. Enfin !

La « croqueuse » en direct

« Tous les enfants dessinent, moi, je n'ai jamais arrêté », explique la dessinatrice, caricaturiste et blogueuse nancéienne Catherine Créhange. Tout le monde la connaît parce qu'elle « sévit » sur France 3 depuis les années 80 au cours des soirées électorales, notamment. Elle a aussi mis son talent au service de la chaîne régionale « la première à avoir disposé d'une unité vidéographique » pour concevoir des génériques. Elle s'est fait remarquer en croquant en direct les joueurs de tennis pendant Roland Garros en 2010 et 2011, « la seule année où il n'a pas plu sauf le dernier jour » pour le compte de France Télévisions.

Catherine Créhange a aussi exercé son immense talent pour l'agence de communication qui l'a employée pendant des années. Avant de cesser son activité en décembre dernier.

Depuis, la croqueuse en live a créé sa propre boîte qui est actuellement en couveuse au sein de Pacelor, la pépinière d'entreprises installée à Villers, dans une aile de l'ancien bâtiment de Promotech, sur le plateau de Brabois. Son matériel est composé d'un crayon, d'un bloc de dessin et d'un ordinateur. Elle intervient ainsi en direct lors d'« événements » tel que la Fête de la Manufacture, aux deux dernières éditions d'« Osons l'économie » organisée par La Poste ou au cours de séminaires d'entreprises. Sa petite boîte a été sollicitée pour le brunch pour l'Université de Lorraine ainsi que pour les 40 ans du Loria dernièrement. La croqueuse fait également des « dessins d'humeur » au profit des boîtes de communication et de management.



■ **Catherine Créhange dessine depuis toujours mais a lancé sa boîte depuis peu..** Photo Patrice SAUCOURT

S.L.

catherine.crehange@laposte.net

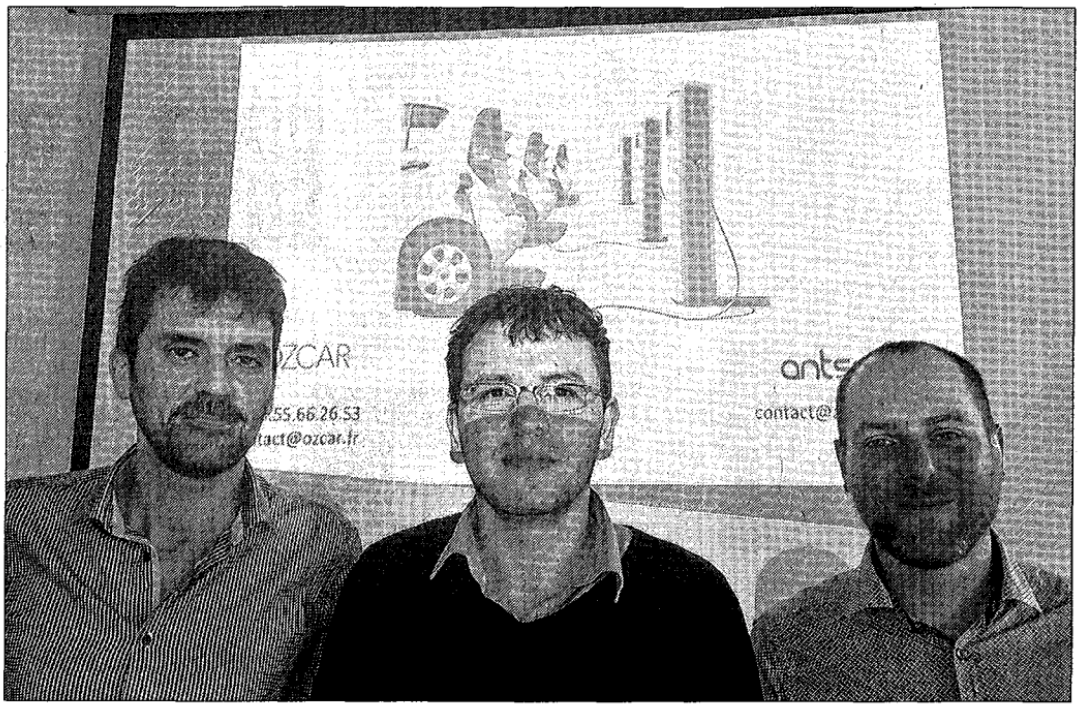
Innovation Les algorithmes du professeur des universités Ammar Oulamara ont permis la mise sur orbite de deux entreprises prometteuses

Un chercheur, deux startups

Chercheur au Loria (Laboratoire lorrain de recherche en informatique et ses applications), le professeur des universités Ammar Oulamara conçoit des modèles mathématiques et développe des algorithmes d'optimisation. Comme ceux qui font tourner nos GPS et permettent de déterminer le meilleur itinéraire en fonction de nos desiderata. Il est aussi impliqué dans l'optimisation des tournées des agents des véhicules électriques des flottes d'ERDF.

Ce sont des chercheurs comme lui qui participent à la conception du futur « smart grid », le réseau électrique intelligent qui sera de plus en plus exposé au risque du « black-out » en raison du nombre gradissant de sources d'énergie renouvelable (et donc aléatoires) et de véhicules électriques qui seront en circulation. Quand des millions de voitures électriques se rechargeront en même temps, c'est tout le système qui pourra « disjoncter ».

Grâce aux algorithmes d'Ammar Oulamara, deux startups issues de l'Incubateur lorrain ont été mises sur orbite il y a environ une année : « Ozcar » qui a investi le créneau de « l'autopartage électrique intelligent » et « Antsway » qui édite des logiciels de tournées « adaptées et optimisées » destinés aux professionnels de la logistique et de l'intervention. Le « CEO » d'Ozcar Stéphane Gonzalez



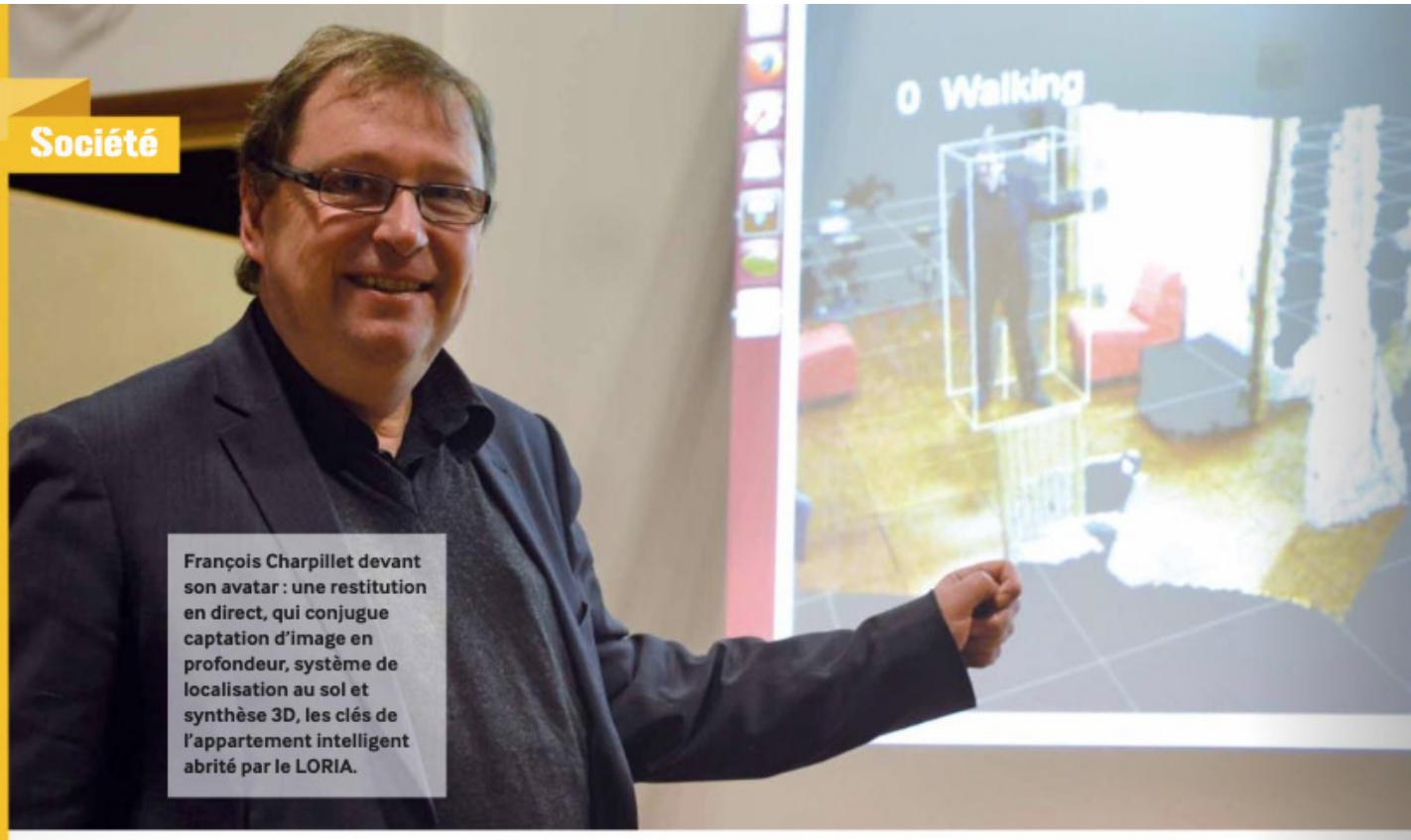
■ **Le président d'Ozcar Stéphane Gomez, le Professeur des universités Ammar Oulamara et le CEO d'Antsway Marc Grojean** Photo S.L.

affirme que sa solution permet d'atteindre un taux d'optimisation des parcs automobiles (électriques et diesel) compris entre 15 et 20 %. La start-up a entamé un partenariat avec la zone industrielle Sainte-Agathe de Florange et planche à présent sur le concept d'appart-hôtels équipés de voitures partagées.

Antsway qui emploie 6 personnes propose des outils pour « les gestionnaires de flottes, les régulateurs de tournées, les chargés d'affaires et les agents terrains » permettant « d'optimiser l'usage d'une flotte mixte thermique électrique ». Et donc de les « rentabiliser ». Antsway a participé au projet InfiniDrive piloté par la Poste et ERDF entre 2011 et 2015. La start-up travaille pour le compte de la poste luxembourgeoise (P & T Luxembourg).

Ce partenariat entre laboratoires et startups nancéiennes a bénéficié du soutien de la région lorraine. Le labo du Loria a ainsi reçu 200.000 € de subvention pour ces programmes. Ce « trio » était au menu du dernier « Créadej » organisé par l'Incubateur lorrain qui s'est déroulé à Artem vendredi 3 juin. La couveuse de l'Université de Lorraine a accompagné la création de 128 entreprises innovantes depuis 2000. Et les startups qui ont été accompagnées au cours des cinq dernières années afficheraient un taux de survie de 100 %. On leur souhaite bonne route.

S.L.



François Charpillet devant son avatar : une restitution en direct, qui conjugue captation d'image en profondeur, système de localisation au sol et synthèse 3D, les clés de l'appartement intelligent abrité par le LORIA.

DES ROBOTS À LA MAISON

Robots, capteurs en réseau, objets connectés, le défi du maintien à domicile passe plus que jamais par la technologie. Détour par Inria et le Loria(1), où les scientifiques se mobilisent pour faire reculer le mur de la dépendance.

Une bonne dose de robotique, deux doigts de domotique et le reste en objets connectés : ce cocktail à fort contenu scientifique, c'est le mix imaginé par François Charpillet, responsable de l'équipe Larsen(2) à Inria, pour répondre à tous ceux qui, malades ou très âgés, entendent poursuivre le plus longtemps possible leur existence à domicile. Un programme ambitieux qui se fixe comme premier objectif d'améliorer les mécanismes d'interaction qui doivent être mis en œuvre pendant les contacts physiques entre l'homme et la machine.

EN RECHERCHE DE NATUREL

Un robot doit être en mesure de s'exprimer " physiquement " au travers des postures qu'il prend. Et lorsqu'il entre en contact avec quelqu'un, il lui faut maîtriser sa force, ce qui nécessite des développements très fins en termes de contrôle. À l'inverse, il est essentiel qu'il puisse percevoir et interpréter les informations induites par la position du corps, l'intonation de la voix, la direction du regard, autant de signaux qui sont chez nous très intuitifs. On balaie donc un large spectre, qui va de l'informatique pure à la psychologie.

L'autre axe de recherche qui mobilise l'équipe Larsen porte sur la robustesse et la résilience. Il s'agit de concevoir des robots disponibles 24h/24 et 7j/7, c'est-à-dire capables de se reconfigurer eux-mêmes en cas de panne. Il s'agit aussi de les rendre plus robustes collectivement : d'un côté en faisant naître entre eux une forme de solidarité ; de l'autre en leur permettant d'interagir avec des environnements augmentés de capteurs, en vue d'étendre leurs capacités. Des développements qui laissent entrevoir de nouveaux services à la personne, rendus à la demande dans le cadre d'appartements dits intelligents.

L'ESPRIT DES LIEUX

Le lieu que nous propose de visiter François Charpillet en est la préfiguration. Il est pour l'heure abrité par Inria, écrin de

(1) Laboratoire lorrain de recherche en informatique et ses applications
(2) Lifelong Autonomy and interaction skills for Robots in a Sensing Environment
(3) Leader français de l'informatique officinale

PROGRAMME AGIR* : LES PROMESSES DU VIEILLISSEMENT

Soutenu par le CHRU de Nancy, l'Université de Lorraine, la Région et le Grand Nancy, et coordonné par les Prs Patrick Netter, directeur du pôle scientifique Biologie Médecine Santé (BMS), et Athanase Benetos, chef du service gériatrie du CHRU de Nancy, AGIR entend renforcer la lisibilité de la recherche lorraine sur la thématique du vieillissement.

« On considère aujourd'hui le vieillissement dans sa globalité, de sa prédiction dans les étapes initiales de la vie jusqu'aux événements tardifs liés aux facteurs d'exposition », souligne le Pr Netter : ***« Il importe donc d'étudier à la fois les phénomènes précoces, les facteurs d'exposition ultérieurs et les mécanismes dégénératifs qui contribuent à la survenue des manifestations pathologiques et à leur évolution dans des maladies ostéo-articulaires, cardio-vasculaires et métaboliques… »*** Une démarche scientifique qui associe recherches fondamentale et clinique et croise les disciplines – la biologie, la santé ainsi que l'informatique, la chimie ou encore les sciences humaines et sociales – au service d'une médecine personnalisée source d'une meilleure qualité de vie pour les patients.

HAUT NIVEAU

« En lançant un appel d'offre international dans le cadre d'AGIR – une première dans la région – nous nous sommes donné les moyens d'attirer des chercheurs d'excellence et de conforter notre leadership dans ce domaine. »
Deux d'entre eux ont d'ores et déjà été sélectionnés par le comité scientifique présidé par le Pr Pierre Corvol, professeur au Collège de France. David Meyre est professeur associé au Département d'épidémiologie clinique & biostatistiques de l'Université McMaster, à Hamilton au Canada. Ses recherches portent sur les gènes de prédisposition à l'obésité, leurs interactions avec les facteurs environnementaux et la réponse aux traitements de l'obésité. Magnus Bäck est médecin-chercheur, professeur associé en cardiologie et directeur de recherche au sein de l'institut du Karolinska à Stockholm en Suède. Il s'intéresse notamment aux processus de calcification des vaisseaux et des valves cardiaques qui accompagnent le vieillissement. Recrutés pour trois ans, ils sont appelés à développer leurs programmes scientifiques en lien avec les équipes de recherche de l'université, des établissements publics à caractère scientifique et technique, CNRS et INSERM, et du CHRU.

(*) Aging Innovation and Research

choix de ce petit bijou de technologie : *« L'appartement est truffé de 600 à 700 capteurs pour 40 m² de surface au sol : un sol technique constitué de dalles sensibles, qui ont chacune les fonctions d'une balance sophistiquée, capables de déterminer le poids d'une personne, d'identifier la position d'un meuble ou d'un robot, de savoir si quelqu'un se déplace et pour aller où… »* Aux murs, d'autres dispositifs de détection développés à l'origine pour l'industrie des jeux vidéos. Des caméras ? Pas tout à fait : *« Au lieu de saisir les couleurs, ces petits appareils discrets captent les distances et restituent en temps réel des images 3D »*. Ils permettent ainsi de suivre une activité humaine en temps réel, en se révélant à la fois moins invasifs et bien plus performants que la surveillance vidéo : *« On ne reconnaît pas les personnes, mais on peut suivre leur silhouette, les localiser avec une extrême précision, mesurer leur vitesse de marche ou visualiser une chute… »* Mieux encore, ces dispositifs peuvent être enrichis par toute une batterie d'objets connectés, centrés chacun, aux fins d'alerte, sur une facette de l'activité humaine.

LE DÉFI DE L'ACCESSIBILITÉ

Les recherches en faveur du maintien à domicile, la Région a choisi de s'y associer en lançant dès l'automne 2013 sa filière *silver* économie et en finançant notamment Satelor, projet lorrain de e-santé dans lequel, en lien avec Diatelic, filiale du groupe nancéien Pharmagest[3], on retrouve en bonne place l'équipe dirigée par François Charpillet et ses travaux sur les appartements intelligents : *« Notre premier défi consiste à imaginer des solutions techniques permettant de sécuriser les logements de personnes malades ou âgées, à coût raisonnable, de manière à les rendre accessibles au plus grand nombre. Restera dans un deuxième temps à les confronter au réel, soit au sein d'un établissement médicalisé partenaire, soit à domicile »*. Un banc d'essai qui devrait être programmé dans le cadre du prochain Contrat de Plan État-Région.

36 MOIS DE + CHEZ SOI !

« Il existe une continuité évidente entre le projet SATELOR qui court jusqu'en 2017 et " 36 mois de plus à domicile ", autre projet porté par le groupe Pharmagest », souligne François Charpillet, directeur de recherche à Inria.
" 36 mois de plus à domicile " a pour objectif de repousser l'entrée en maison de retraite de 36 mois et de favoriser la détection précoce de la perte d'autonomie. Cela suppose de mettre au point des solutions de surveillance biométriques mesurant, par exemple, le rythme cardiaque, la tension artérielle, la respiration, la glycémie, les chutes, afin de garantir une surveillance médicale adéquate : des données qui, exploitées en temps réel, serviront à estimer un risque potentiel, voire à détecter une situation de détresse. À suivre.

Virus et malwares : les chercheurs contre-attaquent

07.03.2016, par Charline Zeitoun
Mis à jour le 22.02.2017

Grâce à leur collection de 6 millions de malwares, les chercheurs du Laboratoire de haute sécurité ont mis au point un anti-virus d'un nouveau genre, déjà utile à la gendarmerie et bientôt disponible pour les entreprises. Visite de la première plateforme de recherche française dédiée à la sécurité informatique.

Portes blindées, sas, caméra de surveillance et reconnaissance biométrique de l'œil : le Laboratoire de haute sécurité (LHS) du Loria1, à Nancy, est une forteresse où sont confinés six millions de virus informatiques. Une collection des pires « méchants » de la planète Web attrapés sur la toile par les chercheurs du LHS. Ces malwares piratent nos données, détruisent nos logiciels ou nos disques durs, voire forcent nos ordinateurs à déverser des torrents de spams pour paralyser les serveurs d'un concurrent ou un site jugé ennemi. Intérêt de collectionner ces super-vilains ? Pouvoir les analyser en profondeur. Puis concevoir des outils qui permettent d'en détecter les « mutants », des variantes issues de la même souche mais légèrement modifiées, et qui n'ont pas encore fait suffisamment de dégâts pour être répertoriés et intégrés aux anti-virus du commerce. « Ces logiciels, eux, ne détectent en général que les virus qu'ils connaissent déjà, commente Jean-Yves Marion, directeur du LHS. C'est pourquoi leurs concepteurs suivent attentivement les résultats de la recherche pour améliorer leurs programmes. » D'autant qu'il y a aujourd'hui beaucoup plus d'attaques qu'il y a dix ou vingt ans. Et que le temps des geeks des années 1980, qui craquaient les systèmes pour la beauté du geste, est bien loin…

Provoquer les attaques en exhibant des ordinateurs vulnérables

« L'amateurisme n'est plus de mise, reprend le chercheur. La plupart des attaques ont des visées lucratives ou d'espionnage et sont le fait de groupes criminels ou d'organisations gouvernementales qui mettent au point des virus dont la conception demande des mois de travail. » En novembre 2014, l'éditeur d'antivirus Symantec révélait ainsi l'existence de Regin. Depuis au moins six ans, ce malware subtilisait des mots de passe et réalisait des captures d'écran dans le réseau informatique du siège de l'Union européenne, mais aussi dans des centres de recherche, des compagnies aériennes et des réseaux de communication de plusieurs pays d'Europe, ainsi qu'en Russie, en Arabie Saoudite, au Mexique, etc., via ordinateurs et Smartphones GSM. Regin est si hors norme, si complexe (il aurait nécessité un an de travail à quatre personnes à temps plein) que, selon les experts, il ne pouvait provenir que d'une organisation gouvernementale2.

Les chercheurs du LHS utilisent un télescope virtuel, connecté à Internet via des lignes ADSL classiques, afin de simuler la présence d'ordinateurs vulnérables et de susciter des attaques qu'ils peuvent ensuite capturer.

Dans ce contexte de cyber-espionnage et de cyber-criminalité, l'attrape-virus du LHS « ramasse » tout ce qui traîne sur le Web afin d'enrichir sa collection. « C'est un télescope virtuel, développé par l'équipe Madynes 3, explique Jean-Yves Marion. Connecté à Internet via des lignes ADSL classiques, cet outil permet de simuler la présence de centaines d'ordinateurs vulnérables, de façon à susciter le maximum d'attaques que l'on va ensuite capturer : c'est la technique du "pot de miel" pour attirer l'ours et l'attraper une fois qu'il y a mis la patte », explique le chercheur. Mais comment exhiber en ligne de faux ordinateurs imprudents ? Cela revient grosso modo à envoyer des messages de signalisation. Quand, au carrefour de ses nœuds, le protocole d'Internet demande périodiquement aux machines connectées « toi en face, qui es-tu ? », le télescope virtuel produit ainsi de fausses réponses du type : « Je suis un mac et je me promène sans anti-virus » ou bien « Je suis un PC et je fonctionne avec tel système d'exploitation », système d'exploitation qu'on aura bien sûr pris le soin de choisir dans sa version la moins aboutie et la plus riche de failles…

Une fois capturés, les malwares passent à la moulinette du logiciel Gorille, l'arme secrète du laboratoire lorrain. « Comme avec les anti-virus du commerce, la méthode consiste à chercher une signature qui est propre au malware et qui permettra de l'identifier », explique Jean-Yves Marion. « Et pour nous, la signature d'un malware, c'est sa structure complète. » Bref, un portrait-robot de la « silhouette » générale du malfaiteur. Résultat : on peut le retrouver même s'il se « déguise », ou plutôt si les concepteurs du malware l'ont légèrement modifié pour en faire un mutant.

Un nouvel anti-virus adapté aux entreprises

« Pour extraire la structure d'un programme malveillant, il faut regarder la liste des instructions qui le composent, en code assembleur (c'est le langage de la machine) », explique Fabrice Sabatier, ingéneur CNRS attaché au LHS. En fonction de la nature de ces instructions (effectuer un calcul, répéter telle action, demander à l'utilisateur de rentrer une donnée, etc.), celles-ci sont représentées par une forme géométrique. Ces formes géométriques sont ensuite reliées par des nœuds qui symbolisent les « sauts conditionnels » : ce sont les fameux « if-then-else » qui donnent l'ordre d'exécuter telle action ou bien telle autre en fonction d'une condition. Ces représentations sont assez classiques en informatique. « Mais un programme est constitué de millions de nœuds ! », reprend le chercheur. Tout l'art de la méthode réside ensuite dans des règles de simplification, en supprimant tel nœud et non tel autre, ou tel paquet d'instructions jugé peu caractéristique, afin d'obtenir un dessin ou « graphe » de quelques milliers à quelques centaines de milliers de nœuds seulement (voir la vidéo plus bas).

« C'est ainsi que, grâce à nos graphes «signatures», visualisables en 3D et en couleur, nous pouvons comparer n'importe quel programme via sa structure globale, ou certains de ses "morceaux", avec les échantillons de notre collection. Et, s'il y a de gros points communs, la présomption d'avoir affaire à un malware sera d'autant plus forte », résume Jean-Yves Marion.« Notre méthode est trop complexe pour tourner sur les PC du grand public, mais nous avons aidé la gendarmerie à identifier les souches de différentes attaques virales de type Ransomware qui venaient de la même source », commente Fabrice Sabatier. La technique devrait aussi bientôt servir aux entreprises, le Loria monte une start-up pour cela4. L'intérêt pour elles est particulièrement grand car la méthode, fondée sur une analyse en profondeur des malwares, permet également de remonter jusqu'aux buts de ces derniers : en étudiant les différentes fonctionnalités de ces logiciels, on peut découvrir s'ils voulaient voler des informations, ou seulement en détruire, ou autres...

Graphe 3D d'un malware par CNRS

Dans cette vidéo : un graphe 3D est élaboré pas à pas à partir du code d'un malware.
Identifier les différentes fonctionnalités, noyées dans les milliers de lignes de code, est d'ailleurs un enjeu important où la recherche fondamentale en informatique à son mot à dire. Parce qu'il n'existe pas d'algorithme capable d'affirmer à coup sûr que deux programmes font la même chose (c'est la question de l'indécidabilité, démonstration mathématique que l'on doit à Alan Turing). « Par ailleurs, poursuit Jean-Yves Marion, analyser les virus nous amène à des questions tout aussi fondamentales du type : en fin de compte, qu'est-ce qu'un programme malveillant ? » Comment le distinguer d'un programme ordinaire qui agirait de façon pas toujours justifiable ? Qu'est-ce qui le différentie de votre application favorite de jeu en ligne, si cette dernière se met à vous géolocaliser ? Ou à transmettre vos données à un tiers, comme en a justement été accusé un fameux jeu d'oiseaux il y a trois ans5 ? Côté chercheurs, il faut au final parvenir à définir dans quels contextes certaines fonctionnalités sont suspectes et dans quels autres elles ne le sont pas…

Au cœur du code des malwares mutants

Et pour l'avenir, faut-il craindre de nouvelles générations de virus, de nature et de structure révolutionnaires ? « Les nouveautés en virologie informatique tiennent surtout dans la façon de protéger les malwares en les "déguisant" », répond Jean-Yves Marion. Il y a les mutants, évoqués plus hauts, mais aussi le fait de crypter le code du virus ou encore de le ziper et re-ziper, jusqu'à des centaines de fois, dans un autre programme, afin de le cacher et de le soustraire à l'analyse de l'anti-virus. Question dissimulation, il y a pire encore : certains malwares s'auto-modifient au fur et à mesure de leur exécution sur un PC, avec des fonctionnalités cachées qui se déclenchent par vagues, qui peuvent s'effacer en cours de route ou ne jamais s'activer !

« Depuis cinq ou six ans, il y a une véritable ingénierie de la protection des virus informatiques. Nous avions fait un test avec un de nos échantillons : nous l'avons protégé avec un logiciel du commerce (utilisé dans le cadre de la protection des fichiers pour les droits d'auteur), et il est passé à travers les mailles du filet de nombreux anti-virus qui connaissaient pourtant l'original », explique Jean-Yves Marion. Tandis qu'au LSH, on peut exécuter un virus : en l'exécutant, on le dé-zipe autant de fois que nécessaire et on observe ses vagues d'auto-modification, ce qui permet d'accéder à ses parties cachées, au plus profond de son code. Le virus est alors ré-assemblé grâce un modèle théorique développé par les chercheurs. « Nous pouvons réaliser des expériences en toute sécurité sur notre réseau, sans craindre la contagion vers d'autres machines, car c'est un cluster confiné, déconnecté du monde extérieur, qui permet de simuler des centaines de machines virtuelles », souligne l'informaticien.

Garantir la sécurité numérique des citoyens

Bien sûr, Google et les autres Gafa veillent aussi au grain. Le moteur de recherche américain possède d'ailleurs une collection de malwares encore plus impressionnante que celle du LHS avec au moins 400 millions d'échantillons, même si les doublons, mutants et autres, y foisonnent et gonflent les effectifs. « En marge de ces acteurs privés, la recherche publique joue un rôle capital, notamment dans le domaine de la virologie, trop peu développé en France et en Europe », insiste Jean-Yves Marion. « Notre approche s'appuie essentiellement sur nos connaissances en théorie de la programmation et en informatique fondamentale dont l'équipe est issue », rappelle le directeur du LHS, première plateforme de recherche académique française dédiée à la sécurité informatique.

« Parallèlement aux actions mises en place par des sociétés guidées par des intérêts commerciaux, la recherche publique doit proposer des solutions pour garantir la sécurité numérique des citoyens, chercher les failles des outils du commerce et en informer le grand public qui est ensuite libre de les utiliser ou non », souligne le chercheur.
Ce processus salutaire pousse aussi parfois les concepteurs à proposer rapidement des patchs correcteurs. Un exemple édifiant a par exemple fait trembler la toile en 2015 : une démonstration sur Logjam, réalisée par des chercheurs du Loria, avait ainsi mis en évidence une faille majeure dans le protocole https qui sécurise les connexions Internet. Sans compter que le monde tout connecté que nous nous préparons offrira de plus en plus de cibles aux hackers. « Avant d'être développés à grande échelle, le pacemaker branché sur Wi-Fi, la voiture autonome, le bracelet qui prend votre pouls ou le vote électronique devraient réclamer d'apporter un certain nombre de garanties », avertit Jean-Yves Marion. À qui choisirons-nous d'en confier la responsabilité ?

Notes
1.Laboratoire lorrain de recherche en informatique et ses applications (CNRS/Inria/Univ. de Lorraine).
2.The Intercept, magazine anglais d'investigation, pointe les États-Unis et l'Angleterre du doigt : https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/ et https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/
3.Managing dynamic networks and services/Supervision des réseaux & services dynamiques, http://www.loria.fr/la-recherche/equipes/madynes
4.Cette start-up, Cyber-Detect, devrait voir le jour fin mars 2017.
5.Selon le New York Times du 27 janvier 2014, le jeu « Angry Birds » aurait servi à la NSA, agence américaine de renseignement, et à son homologue britannique, le GCHQ, pour collecter certaines données de ses utilisateurs.

Région

blessures des sportifs

Dr Sport, l'appli médicale 100 % lorraine

Thierry Weizman a choisi Paris et le Parc des Princes hier pour présenter Dr Sport. La dernière-née des applications médicales, 100 % lorraine, capable d'évaluer les blessures sportives et donner les premiers conseils.

Thierry Weizman, médecin du sport à Metz, entouré de Camille Lacourt (natation), Jo-Wilfried Tsonga (tennis), Céline Dumerc (basket) ainsi que Muriel Hurtis (athlétisme) et Luc Abalo (handball). Photo Philippe DOBROWOLSKA

« Cinq clics pour une réponse rapide, professionnelle et rassurante. » Thierry Weizman, médecin du sport à Metz, ancien sportif de haut niveau, actuel président de Metz handball, ne vend pas de guérison miracle. Dr Sport, son application mobile téléchargeable depuis hier, cherche à répondre aux questions que ses patients lui posent depuis trente ans. Ma blessure est-elle grave ? Que dois-je faire ? Poser du chaud ou du froid ? Quels médicaments prendre ? Dois-je consulter ?

« L'application ne remplace pas une consultation », prévient le médecin. « Elle est utile en cas de douleur consécutive à une pratique sportive. » En cas de bobologie, elle rassure, prodigue ses conseils, oriente vers la médecine classique ou naturelle. Plus grave, le code couleur passe à l'orange ou au rouge. La consultation s'avère nécessaire, voire les urgences.

Unique en son genre, Dr Sport géolocalise les praticiens. « Douze spécialités en lien avec la médecine du sport ou paramédicales référencées par le ministère de la Jeunesse et des Sports sont disponibles sur toute la France. » Sans oublier les urgences et SOS mains.

Pré-diagnostic

A Paris, dans une des loges du Parc des Princes, en présence des ambassadeurs Camille Lacourt (natation), Jo-Wilfried Tsonga (tennis), Muriel Hurtis (athlétisme), Luc Abalo (handball) ou Céline Dumerc (basket), Thierry Weizman donne l'exemple d'Archibald, un quinquagénaire qui ressent un claquement au mollet en jouant au tennis. Il ne consulte que douze jours plus tard. Le diagnostic d'une rupture de talon d'Achille tombe. D'opération en ré-opération et arrêts de travail prolongés, l'homme a arrêté le sport et, plus dramatique, perdu son emploi.

« L'application lui aurait permis d'obtenir un pré-diagnostic. Il aurait été dirigé vers les urgences avec interdiction de marcher. C'est pour éviter ce genre de complications que j'ai créé Dr Sport. Nous intervenons entre le problème et la consultation. » L'application a nécessité trois ans de travail intense. « J'ai écrit et ré-écrit l'algorithme. Au total, un kilomètre de long ! 300 pathologies recensées à partir de 7 000 cas cliniques. » A ses côtés, son épouse, pharmacienne, ses filles, l'une en études de médecine, l'autre en école de commerce, ont travaillé sur ce projet qui a grandi au sein de l'incubateur HEC. Le laboratoire CNRS-Inria/Loria de Nancy a développé la version informatique.

Avec son intelligence artificielle, il est le premier algorithme mondial auto-apprenant pour la prise en charge du sportif. Une société nancéienne a codé le tout. Un investisseur – aucun montant n'a été révélé – offre à Dr Sport une visibilité sur plusieurs années.

5,99 € par an

La société et sa quinzaine de salariés, domiciliée à Metz, base son modèle économique sur le paiement de l'application : 5,99 € par an. Si l'équipe ne parle guère chiffres, elle espère 100 000 téléchargements d'ici un an.

Les sportifs de haut niveau n'ont pas été trop difficiles à convaincre pour promouvoir l'application. « J'accepte les propositions qui me paraissent intelligentes », commente Camille Lacourt, « et Dr Sport répond à un besoin. C'est simple, rapide et efficace. » Jo-Wilfried Tsonga, admettant dans un sourire qu'il a « un peu d'expérience côté blessures », a été emballé. « Ce projet me collait à la peau et l'application peut se déployer dans d'autres secteurs. » Ce qui n'a pas échappé à l'équipe. Outre un déploiement étudié pour l'étranger, Dr Sport pourrait s'étendre aux blessures de la vie courante ou se développer via les objets intelligents.

Laurence SCHMITT.

Trois mille ans d'informatique

23.09.2016, par Martin Koppe

Cette photo, prise en 1962, montre quatre générations successives de circuits, de fonction comparable, sur quatre modèles d'ordinateur : Eniac (1946), Edvac (1948), Ordvac (1951) et BRLESC (1955).

L'informatique aussi a son histoire. Des premières « ablettes numériques » sumériennes aux objets connectés, un ouvrage parcourt en images les évolutions techniques de ces machines à calculer qui ont révolutionné nos sociétés.

Pierre Mounier-Kuhn, vous êtes chargé de recherche en histoire à la Sorbonne1 et au Centre Alexandre-Koyré2, et vous publiez avec Emmanuel Lazard, maître de conférences en informatique à l'université Paris-Dauphine, une Histoire illustrée de l'informatique.

Comment replacez-vous la discipline informatique dans un cadre historique ?

Pierre Mounier-Kuhn : Marginale jusqu'au milieu du XXe siècle, l'informatique est aujourd'hui devenue un phénomène historique massif : à la fois l'une des plus puissantes industries mondiales et une discipline scientifique bien établie. Notre ouvrage vise d'abord à partager la richesse de cette histoire, qui remonte à la machine d'Anticythère, voire aux premiers chiffres écrits à Sumer. L'histoire de l'informatique permet non seulement de comprendre ses origines et son développement, mais elle révèle aussi comment la société a réagi face à cette innovation. Mon premier travail de recherche portait d'ailleurs sur l'émergence de l'informatique au CNRS3.

Qu'est-ce qui a poussé les hommes à développer l'informatique ?

P. M.-K. : Trois besoins principaux : calculer, traiter des masses d'informations, automatiser des procédures. Dès le XVIIe siècle, entre Galilée et Newton, la mathématisation des sciences impose de plus en plus de calculs, motivant les machines de Schickard et de Leibniz. Simultanément, Blaise Pascal conçoit sa calculatrice en 1642 pour aider son père, receveur des impôts dans l'administration royale. Ces demandes de la science, de l'État et des grandes

organisations vont croître encore plus aux XIXe et XXe siècles. L'automation industrielle apparaît en 1801 avec les métiers à tisser Jacquard, où des cartes perforées servent de support aux « programmes » de confection des motifs. Ces cartes sont bientôt adaptées au calcul scientifique par Charles Babbage, ainsi qu'au traitement des données démographiques par Hermann Hollerith dans les années 1890, pour dépouiller le recensement américain. Dès le XIXe siècle, les techniques circulent donc entre ces trois grands domaines d'applications.

On parle parfois de machines de von Neumann et/ou de machines de Turing pour désigner les ordinateurs. Comment l'idée de l'ordinateur est-elle née ?

P. M.-K. : Une équipe de l'université de Pennsylvanie a conçu en 1943 l'énorme calculateur électronique Eniac4. Il calculait très vite, mais il fallait le reconfigurer en rebranchant les câbles pour chaque nouveau problème. D'où l'idée d'enregistrer le programme et les données sous forme électronique, directement accessible au processeur et facilement modifiable par l'opérateur. Cette idée a été formalisée en juin 1945 par John von Neumann, l'un des plus grands mathématiciens du XXe siècle. Son rapport décrit une future machine formée de quatre parties : processeur, unité de contrôle, mémoire et dispositifs d'entrée-sortie.

Si les technologies ont énormément évolué depuis, l'architecture de base est restée la même. Alan Turing, étudiant à Cambridge en 1936, cherchait à résoudre un problème de logique mathématique fondamentale. Pour sa démonstration, il a imaginé un dispositif calculant abstrait, nommé plus tard « machine de Turing », qui fournira un modèle théorique de l'ordinateur. Il joue ensuite un rôle décisif pendant la guerre en inventant des méthodes et des appareils qui permettront de décrypter les messages allemands. Fin 1945, il élaborera l'un des tout premiers projets d'ordinateurs en s'inspirant du rapport von Neumann.

Quel serait le premier « vrai » ordinateur, s'il est possible d'en choisir un ?

P. M.-K. : Tout dépend de la définition qu'on en donne ! L'Edsac5 fut le premier ordinateur à programme enregistré opérationnel, mis en service en 1949 à Cambridge sous la direction du mathématicien anglais Maurice Wilkes. L'Allemagne a aussi son héros fondateur : Konrad Zuse. Il a construit, dès la fin des années 1930, des calculateurs binaires programmables. Zuse a élaboré ensuite un système de programmation très avancé. La campagne récente de réhabilitation d'Alan Turing, condamné en 1952 pour délit d'homosexualité, permet paradoxalement à la Grande-Bretagne de rappeler qu'elle aussi a son « inventeur de l'ordinateur ». Ces distinctions attisent des controverses un brin nationalistes entre experts. Comme la France a raté le coche des premiers ordinateurs, les historiens français ont au moins la chance de ne pas participer à ces querelles de priorité !

À ce propos, comment le CNRS a-t-il géré l'apparition de l'informatique ?

P. M.-K. : Dès 1946, le CNRS a créé l'Institut Blaise-Pascal6 en fédérant un centre de calcul analogique et un laboratoire de calcul numérique. Mais ce dernier a été victime d'un calculateur électronique mal conçu et d'une mauvaise gestion de projet. Le CNRS a donné un nouveau départ à l'institut vers 1960 en changeant sa direction, en l'équipant de gros ordinateurs, puis en y fondant l'Institut de programmation avec la faculté des sciences de Paris, l'un des premiers départements d'informatique du monde ! Cet ensemble a lancé des recherches sur les applications non numériques des ordinateurs, comme la traduction ou la documentation automatique, en relation avec la linguistique computationnelle7étudiée par Marcel-Paul Schützenberger et ses disciples. Particularité notable de cette époque, j'ai été très frappé d'y voir une forte présence féminine jusqu'aux années 1980. Plusieurs femmes ont dirigé des centres de calcul scientifique, avec de grandes responsabilités techniques et financières. En 1961, la première thèse de France en informatique a été soutenue par une assistante de l'université de Nancy, Marion Créhange. Ce phénomène oublié illustre les évolutions d'une discipline dont les normes et les codes sociaux peuvent changer plusieurs fois au cours d'une génération.

Comment s'est déroulée la popularisation de l'informatique ?

P. M.-K. : Certains industriels ont compris dès les années 1950 que l'ordinateur pourrait devenir un produit commercial à destination des laboratoires, de l'armée et des États. Le marché des ordinateurs de comptabilité et gestion a fini par dépasser celui du calcul scientifique en 1962. La baisse continue des coûts et les gains en performances ont favorisé la diffusion des mini-ordinateurs, puis des micro-ordinateurs dès les années 1970. L'intégration de ces machines à des réseaux numériques, particulièrement à l'Internet à partir des années 1990, a exercé un effet réseau multiplicateur : à partir du moment où l'on pense avoir intérêt à connecter ses instruments de travail et de loisir, on est poussé à utiliser davantage d'objets informatiques.

Quelle sera selon vous l'évolution de l'informatique ? La loi de Moore, selon laquelle la densité d'intégration des composants8 double tous les 18 mois à prix constant, va-t-elle rester vraie ?

P. M.-K. : Le problème des bugs et de la vérification de programmes reste crucial. Quant à la loi de Moore, j'entends depuis 35 ans qu'elle arrive au bout du rouleau. Elle est certainement proche de ses limites physiques, et ce problème se combine avec le défi de la dissipation thermique. L'alternative se trouvera-t-elle dans les ordinateurs quantiques ? Question à poser à nos collègues physiciens !

Notes

- 1.Centre Roland-Mousnier (CNRS/Univ. Paris-Sorbonne).
- 2.Unité CNRS/EHESS/MNHN.
- 3.L'Informatique en France de la Seconde Guerre mondiale au Plan Calcul. L'Émergence d'une science, P. Mounier-Kuhn, Pups, 2010.
- 4.Electronic Numerical Integrator and Computer, ou calculateur et intégrateur électronique numérique.
- 5.Electronic Delay Storage Automatic Computer, ou calculateur électronique automatique à mémoire à retard.
- 6.« Forteresse ou carrefour : l'Institut Blaise-Pascal et la naissance de l'informatique universitaire parisienne », Revue pour l'histoire du CNRS, A. Collinot et P. Mounier-Kuhn, automne-hiver 2011, n° 27-28.
- 7.Approche où les phénomènes linguistiques sont modélisés grâce aux mathématiques.
- 8.La densité d'intégration représente la quantité de composants électroniques pouvant être intégrés sur une surface donnée.

09.2016 - L'Est Républicain

Bons plans

Le LORIA fête la science

Dans le cadre de la Fête de la Science, le Loria organise deux projections-débats sur l'Intelligence Artificielle et l'univers de la cryptographie et de la protection de la vie privée. Ces deux projections-débats seront animées par Nicolas Dupuy, docteur en physico-chimie moléculaire à l'Université de Lorraine et des chercheurs du Loria.
Le 8 octobre à 17h, faculté des Sciences et Technologies, Amphithéâtre 8 : Des machines intelligentes aux machines pensantes.
Le 15 octobre à 17h, Campus ARTEM, Amphithéâtre 200 : Cryptographie et vie privée : jusqu'ou irons-nous ?

Creative Business Days

Ce sont plus de 500 étudiants des 3 écoles qui sont réunis jusqu'à ce vendredi 30 septembre sur le campus Artem pour les Creative Business Days 2016. Cette 4e édition a pour thème les grands défis de demain et a pour objectif de familiariser les étudiants de l'Alliance Artem avec le monde de l'entreprise lors d'un projet de créativité et de stratégie. Rassemblés en groupes de 10 étudiants, ils seront ainsi sensibilisés, par un « frottement » de cultures différentes, à la remise en question des modes de pensée.

SCIENCES

Des nombres truqués pour mieux espionner

Des chercheurs franco-américains s'inquiètent du manque de transparence sur les nombres entiers choisis pour sécuriser les transactions électroniques.

Par David Larousserie • Publié le 10 octobre 2016 à 17h13 - Mis à jour le 24 octobre 2016 à 13h17

Lecture 4 min.

Tricher n'est pas jouer. Mais jouer à tricher peut être stimulant, surtout si cela met en doute la sécurité d'Internet… C'est à ce petit jeu que vient de se livrer une équipe de l'université de Pennsylvanie, du CNRS et d'Inria au sein du Laboratoire lorrain de recherche en informatique et ses applications (Loria) de Nancy.
Ces chercheurs ont, en quelque sorte, fabriqué une porte qui a toutes les apparences de la solidité, mais qui en réalité est facile à crocheter. En outre, ils sont inquiets du fait que certaines de ces portes prétendument blindées des réseaux informatiques, et qui assurent la sécurité des messages, des signatures, des paiements, des connexions chiffrées… pourraient ne valoir guère mieux !

Une clé secrète

Internet est un réseau sur lequel des machines se « parlent » en permanence pour autoriser des connexions : canal chiffré entre deux ordinateurs, transmission de messages cryptés, signature électronique… La première étape est d'échanger une clé secrète, c'est-à-dire une série de chiffres qui servira ensuite à chiffrer et déchiffrer des messages ou authentifier des transactions. La solidité de ce maillon est donc cruciale. Et elle est en fait assurée par des fonctions mathématiques.

Certaines opérations sont en effet faciles à calculer mais difficiles à inverser. Voire impossibles. Par exemple, multiplier deux nombres premiers entre eux est rapide, mais étant donné le résultat, retrouver ces deux entiers est d'autant plus ardu que des très grands nombres à plusieurs centaines de chiffres ont été utilisés. Et quand les puissances des ordinateurs progressent, il suffit d'augmenter la difficulté du calcul en accroissant la taille des nombres pour les préserver.

Des trappes dans plusieurs millions de clés de chiffrement

Ariane Beky, 13 octobre 2016, 15:45

AUTHENTIFICATION POLITIQUE DE SÉCURITÉ SÉCURITÉ

Des clés de chiffrement de 1024 bits utilisées pour sécuriser les sites Web, les VPN et les serveurs Internet peuvent inclure des « trappes » indétectables, selon des chercheurs.

Des clés de chiffrement de 1024 bits utilisées pour sécuriser les échanges et les communications sur Internet (sites Web, VPN et serveurs), peuvent utiliser des nombres premiers munis de « trappes » indétectables. L'exploit permettrait à des pirates de déchiffrer plusieurs millions de communications chiffrées, et d'identifier les propriétaires des clés. C'est ce qui ressort des travaux d'une équipe de chercheurs : Joshua Fried et Nadia Heninger, de l'Université de Pennsylvanie, Emmanuel Thomé et Pierrick Gaudry, de l'équipe projet CARAMBA (Inria-CNRS-Université de Lorraine).

« Nous démontrons dans nos travaux que la création et l'exploitation de trappes des nombres premiers (trapdoored primes) pour les standards d'échange de clés Diffie-Hellman et du DSA (Digital Signature Algorithm) est faisable pour les clés de 1024 bits avec des ressources informatiques universitaires modernes », déclarent les chercheurs dans leur article technique. Ils disent avoir « effectué un calcul de logarithmes discrets dans une trappe des nombres premiers, en deux mois sur un cluster académique ».

Traffic HTTPS et VPN déchiffrés

Les standards internationaux de cryptographie reposent sur des nombres premiers dont l'origine devrait être vérifiable. Mais, aujourd'hui, trop de serveurs communiquent en s'appuyant sur des nombres premiers dont l'origine est invérifiable : 37% des sites en HTTPS (parmi le million de sites les plus visités du top Alexa) et 13% des VPN IPsec, rappelle Inria.

Pour son propriétaire, une clé de chiffrement dotée d'une trappe ressemble à toute autre clé fiable. Pour les attaquants qui exploiteraient la trappe, en revanche, la sécurité de la clé peut être brisée à travers la résolution plus rapide du problème du logarithme discret. Selon les chercheurs, l'échelle de difficulté pour un pirate deviendrait « très facile » pour une clé de 768 bits, « facile » pour une clé de 1024 bits, mais hors de portée pour du 2048 bits…. pour le moment.

Chaque échange sécurisé par le standard Diffie-Hellman, qui utiliserait le nombre premier p, par exemple, pourrait être déchiffré par un attaquant ayant résolu le logarithme discret pour p. Des documents exfiltrés par Edward Snowden ont montré que la NSA américaine a utilisé cette approche.

Security

Crypto needs more transparency, researchers warn

Publish primes with seeds, so we know there are no backdoors

By Richard Chirgwin 9 Oct 2016 at 22:04 6 SHARE ▼

Researchers with at the French Institute for Research in Computer Science and Automation (INRIA) and the University of Pennsylvania have called for security standards-setters to publish the seeds for the prime numbers on which their standards rely.

The boffins also demonstrated again that 1,024-bit primes can no longer be considered secure, by publishing an attack using "special number field sieve" (SNFS) mathematics to show that an attacker could create a prime that looks secure, but isn't. Since the research is bound to get conspiracists over-excited, it's worth noting: their paper doesn't claim that any of the cryptographic primes it mentions have been back-doored, only that they can no longer be considered secure.

"There are opaque, standardised 1024-bit and 2048-bit primes in wide use today that cannot be properly verified", the paper states. Joshua Fried and Nadia Heninger (University of Pennsylvania) worked with Pierrick Gaudry and Emmanuel Thomé (INRIA at the University of Lorraine on the paper, here. They call for 2,048-bit keys to be based on "standardised primes" using published seeds, because too many crypto schemes don't provide any way to verify that the seeds aren't somehow back-doored.

Examples of re-used primes in the paper include :
- Many TLS implementations use some form of default, and as a result, "in May 2015, 56 per cent of HTTPS hosts selected one of the 10 most common 1024-bit groups when negotiating ephemeral Diffie-Hellman key exchange";
- In IPSec, "66 per cent of IKE responder hosts preferred the 1024-bit Oakley Group 2 over other choices" for their Diffie-Hellman exchange; and
- OpenSSH implementations favour "a pre-generated list that is generally shipped with the software package".
If any of the "hard-coded" primes were maliciously produced – something that's happened before, for those who remember RSA's NSA-funded Dual EC Deterministic Random Bit Generator – it would be hard to spot by looking at the numbers, but factorisation would be feasible.

It might not necessarily be easy, however: the paper describing the SNFS computation notes it needed "a little over two months of calendar time on an academic cluster" (using between 500 and 3,000 cores in different phases in the operation – a total of around 400 core-years). Their experiments ran on France's Grid'5000 testbed, the University of Pennsylvania's Cisco UCS cluster, the University of Waterloo's CrySIP RIPPLE facility, and Technische Universiteit Eindhoven's Saber cluster.

Earlier this year, INRIA researchers turned up the Sweet32 birthday attack against old Blowfish and Triple DES ciphers, and in January the group warned the world that the zombie MD5 and SHA1 hash protocols live on in too many TLS, IKE and SSH implementations.

Innovation Artem fête la science vendredi avec une conférence sur notre futur quotidien multidimensionnel et évolutif

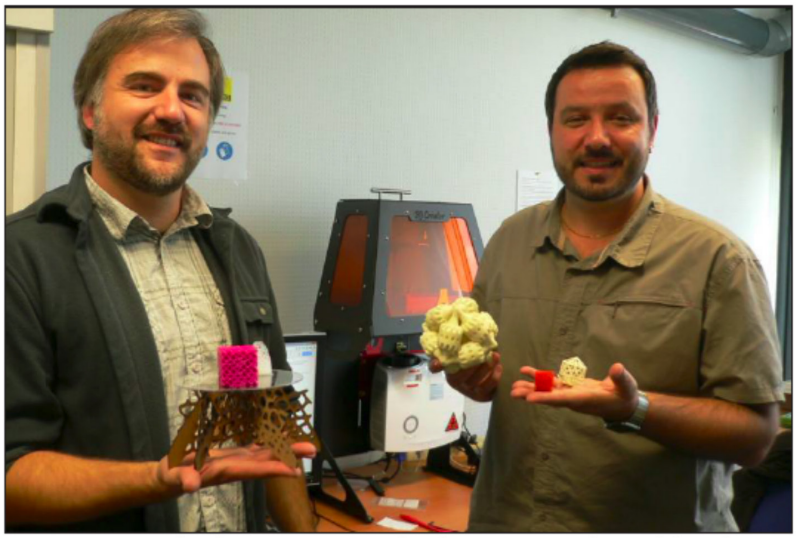
Quand la 4D fait... impression

Nancy. Souvenez-vous : c'était en juillet 1984. Le premier procédé breveté de l'impression 3D (largeur, hauteur, profondeur) venait d'être conçu à Nancy sous la conduite du professeur Jean-Claude André. Mais les Américains dégainent plus vite que le CNRS français et commercialisent la même innovation un... mois plus tard.

Mais les pionniers lorrains ont ouvert la voie à des héritiers, aujourd'hui à la pointe de l'évolution technologique qui nous transporte dans la 4D, la 4e dimension étant la dimension temporelle qui caractérise ces nouveaux objets programmables et modulables issus des imprimantes dites 3D.

Avec des applications dans les domaines du luxe (bijouterie), de l'industrie (aéronautique, automobile), de la médecine (prothèses dentaires, médicaments) de la construction (maisons, meubles), de l'habillement, de l'alimentation. Notre futur quotidien.

Ce sera précisément le thème d'une conférence grand public qui sera donnée vendredi à 17 h sur le campus Artem (quartier Blandan à Nancy) par deux spécialistes nancéiens de haut vol de l'impression 4D.



■ Les chercheurs Sylvain Lefebvre et Samuel Kenzari expliqueront que le mariage de l'informatique et des matériaux nous plonge dans le futur dès... aujourd'hui. Photo ER

Tous deux Prix du chercheur de la Région Lorraine en 2013, Sylvain Lefebvre, chercheur à l'Inria (Institut national de recherche en informatique et en automatique) et membre du Loria (Laboratoire lorrain de recherche en informatique et ses applications), et Samuel Kenzari, ingénieur de recherche au CNRS et chercheur à l'Institut Jean Lamour (IJL) expliqueront que le mariage de l'informatique et des matériaux nous plonge dans le futur dès... aujourd'hui.

Un éléphant, un meuble, du chocolat...

« L'impression 3D permet la fabrication d'un objet que ne peut réaliser la technologie classique. L'usinage est une technologie soustractive, l'impression 3D une technologie additive, on ajoute de la matière couche par couche, les possibilités géométriques sont plus vastes », synthétise Samuel Kenzari.

Les matériaux utilisés peuvent être en polymère, céramique, béton, métal. La 4D consiste à faire en sorte que les propriétés des matériaux, une fois issus de l'impression 3D puissent évoluer dans le temps en intégrant dans leur conception les paramètres de dilatation et de rétraction, de flexibilité, de résistance, d'adaptabilité », précise Sylvain Lefebvre. « Un éléphant aplati, humidifié après sa sortie de l'imprimante, peut prendre forme, un textile peut se gaufrer tout seul, on va sans doute vers des meubles programmables qui s'auto-assembleraient ». Ce qui ferait la joie de plus d'un bricoleur du dimanche. Qui aurait alors le temps de déguster ses chocolats sortis de son imprimante 3D obtenu à partir d'une buse injectant poudre et sirop sourit Samuel Kenzari. Avant de se marrer carrément : « La 4e dimension, c'est que le chocolat est mangeable. Attention de ne pas en abuser, sinon c'est vous qui changerez de forme ».

Philippe RIVET

Voir aussi notre vidéo consacrée à l'interview de Samuel Kenzari sur notre site estrepublicain.fr

Une vague de cyberattaques

L'enjeu n'est pas de savoir si un incident aura lieu mais quand. Depuis fin août, la France est tout particulièrement visée. La Lorraine n'échappe pas à cette vague de cyberattaques. Les entreprises doivent se protéger.

La première grosse vague d'attaques a eu lieu fin août piégeant de nombreuses structures. Parmi elles, La maison de l'entreprise à Maxéville près de Nancy, là où est hébergé le Medef 54. Depuis un mois, les attaques se sont encore renforcées. Ce qui fait de la France un des pays actuellement les plus attaqués d'Europe. Locky, ce malware demandeur de rançons est souvent cité. Un hôpital à Lyon, et d'autres en France, auraient perdu des données. « Nos services informatiques sont sur les dents. De nouveaux virus circulent », témoigne Géraldine Bucci-Scholler de chez SOS Seniors, un groupe qui gère une quarantaine de maisons de retraite en Lorraine, dont le siège est à Metz. Une cyberattaque, Géraldine l'a vécu en direct en mars dernier. « J'ai cliqué sur une facture adressée à l'entreprise. Rien que du très normal. » Un leurre. « D'abord, un grand blanc, puis, tous les fichiers de mon bureau disparaissaient les uns derrière les autres. J'en avais les larmes aux yeux. » Un message, en anglais, demandait une rançon de 500 $ à verser dans les trois jours pour tout récupérer.

Payer la rançon pour récupérer les fichiers

Dans ce cas, ne surtout pas tenter de camoufler. Chez SOS Seniors, le service informatique est conséquent compte tenu des données médicales à protéger. « Comme j'interviens quotidiennement sur Facebook, YouTube, etc, j'ai désormais droit à un serveur indépendant. » Mais les fichiers non sauvegardés sur le serveur ont été perdus.

Un exemple parmi combien ? Impossible de chiffrer. Les entreprises qui acceptent de témoigner – comme Rhin-Meuse la semaine dernière – sont celles qui se protègent. Celles qui payent la rançon pour récupérer leurs fichiers – les cybercriminels conservent un certain sens de l'honnêteté – camouflent la chose comme une maladie honteuse. Ce n'est qu'après la catastrophe ou en plein incendie qu'elles font appel à des sociétés spécialisées pour se protéger.

La France est le premier pays au monde à avoir inscrit la cybersécurité dans sa loi et créé une norme (ITEC 62443) garantissant une sécurité certaine. « Une norme intéressante si on exporte », commente Jean-Pierre Hauet, président ISA-France, qui a participé à sa mise au point. Par « intéressant », entendez « indispensable » même si elle ne sera jamais imparable. Bizarrement, les chefs d'entreprise ne semblent pas très concernés par le problème. Presque inconscients.

Pourtant, dans les cercles très fermés, il se dit qu'énormément de start-up françaises se font piller leurs données par des multinationales. Car, si la plupart des attaques sont purement criminelles, les offensives économiques doivent être prises au sérieux. L'usine du futur et donc connectée, nos maisons et voitures connectées sont autant de portes ouvertes à toutes les attaques informatiques. « L'internet connecté est notre cauchemar », assène Philippe Wolf, de l'IRT-SystemX à Saclay, lors d'un séminaire cybersécurité au salon I-Novia à Strasbourg. L'homme fustige ces objets connectés bon marchés non sécurisés. « Un robot cible la vulnérabilité des caméras. Dès qu'il en regroupe 300 ou 500.000, il peut viser une adresse et tirer. C'est ce qui s'est passé avec le serveur OVH le mois dernier. »

Laurence SCHMITT

L'agence de l'eau Rhin-Meuse victime d'une demande de rançon fin septembre

▶ Fin septembre, l'agence de l'eau Rhin-Meuse, installée à Rozerieulles près de Metz, a été la cible d'une cyberattaque, avec demande de rançon. Baptisé Locky, un cryptovirus, qui s'est répandu à travers le mail d'un des agents, a paralysé pendant plusieurs heures le dispositif informatique. Les services de l'agence ont donc prudemment pris les mesures nécessaires, pour annoncer un « retour à la normale » après plusieurs jours. Les quatre postes victimes de l'infection du virus informatique ont été localisés et isolés, telle une mise en quarantaine, mais leurs données ont été perdues. En 2014, deux plateformes internet de la SFEN (société française d'énergie nucléaire) et du commissariat à l'énergie atomique (CEA) avaient été victimes de cyberattaques.

■ **Bon à savoir, la DGSI sensibilise et prodigue des tas de conseils, en matière de sécurité informatique, pour protéger les entreprises au mieux contre les menaces extérieures.** Photo Alexandre MARCHI

Questions à Jean-Yves Marion

Directeur du LORIA à Nancy

« Tout ce qui est connecté et numérique est potentiellement menacé. »

Jean-Yves Marion, professeur à l'université de Lorraine dirige le laboratoire lorrain de recherche en informatique et ses applications (LORIA) à Nancy.

Le Loria a travaillé sur une nouvelle génération d'antivirus, destiné aux entreprises. De quoi s'agit-il ?

Cette recherche a été initiée avec la création au Loria du laboratoire de haute sécurité (LHS), autour de la détection des comportements malveillants. Les malwares ou virus. On a une liste de programmes malveillants. Mais face à cela il y a une catégorie de logiciels dont le comportement peut être suspect. Ou des attaques ciblées qui visent un petit groupe de personnes ou une seule personne pour acquérir des données. Le logiciel d'attaque n'est pas connu, il faut donc détecter quelque chose dont on n'a pas encore la connaissance. D'où la nécessité d'une recherche scientifique pour vérifier le comportement d'un logiciel. Les antivirus actuels sont inopérants là-dessus. Nous menons des travaux pour avoir une nouvelle génération d'antivirus qui va pouvoir détecter à la fois les virus connus mais aussi des menaces ou variations de menaces que l'on connaît. Le logiciel - Simorfo - existe et fonctionne désormais, une entreprise devrait être créée en décembre.

Peut-on dire que les cyberattaques sont fréquentes aujourd'hui ?

Complètement. La menace en termes de sécurité et l'économie souterraine criminelle induite par les attaques, est réelle. Les attaques ne se font pas uniquement sur les systèmes informatiques, mais aussi sur les téléphones et tous les objets connectés (caméras, systèmes industriels...). Et ce n'est que le début. Tout ce qui est connecté et numérique est potentiellement menacé. Avec le "smart grid" un réseau de distribution d'électricité dit « intelligent », on imagine par exemple des attaques sur la gestion de l'électricité.

Peut-on garantir aujourd'hui ou demain à des entreprises une cybersécurité qui pare toutes les attaques ?

C'est une course qui emprunte aux métaphores guerrières. Une course d'armement. Vous construisez un château fort, l'ennemi invente le canon, vous inventez le bunker...

C'est une guerre perpétuelle dont on augmente le niveau à chaque difficulté supplémentaire pour réussir une attaque.

Propos recueillis par Stéphanie SCHMITT

Aperotech#2 La pépite medtech Harmonic Pharma invitée ce jeudi sur l'Embarcadère

La PME qui dope la recherche

Harmonic Pharma est l'invitée du prochain Aperotech, le rendez-vous mensuel des startups et des acteurs du numérique que nous organisons en partenariat avec France 3 Lorraine et Lorraine Inside, l'association des entreprises de croissance.

Polypharmacologie. Cette PME innovante compte parmi les rares entreprises à tenter l'aventure de la « polypharmacologie » qui consiste à découvrir de nouvelles applications aux médicaments existants déjà bien tolérés. « C'est ce qu'on appelle le « Drug Re-discovery » ou la « Re-découverte pharmacologique », explique Stéphane Gegout directeur général et co-fondateur avec Michel Souchet de cette entreprise créée en 2009.

Parmi les exemples célèbres de « repositionnement », on peut citer le Zyban, un antidépresseur qui s'est avéré efficace pour le sevrage tabagique ou le Viagra conçu à l'origine pour réduire la tension artérielle et améliorer la circulation sanguine. Des découvertes fortuites qui ont fait la fortune de certains labos.

Innovation. Cette PME, hébergée dans les murs du Loria, a trouvé un moyen innovant qui ne doit plus rien au hasard de déterminer de nouvelles applications : la bio-informatique, et plus précisément les harmoniques sphériques qui permettent à la fois de décrire la forme et les propriétés physico-chimiques des molécules et de les comparer entre elles.

■ **Une partie de l'équipe d'Harmonic Pharma.** Photo D.R.

Anticancéreux prometteur Harmonic Pharma a centré ses recherches dans le domaine de la cancérologie et a découvert HPH112, une nouvelle application anticancéreuse d'un médicament bien toléré et utilisé jusqu'alors en infectiologie. La PME a atteint aujourd'hui un stade déterminant de son développement.

Lazar Christitch, directeur du Bussiness Développement, d'Harmonic Pharma répondra aux questions de Francine Dubail, rédactrice en chef adjointe de France 3 Lorraine et notre confrère de l'Est Républicain Saïd Labidi ce jeudi à partir de 19 h sur l'Embarcadère, une péniche du port Sainte-Catherine

Pour participer, s'inscrire à said.labidi@estrepublicain.fr

Education 400 personnes participent depuis hier à Maxéville à une formation sur les usages du numérique en classe

Un drone pour apprendre ses leçons

Maxéville. L'imagination n'a pas de limite dans l'Éducation. On croyait qu'un seul petit stylo, un ordinateur, voire une tablette suffisait à apprendre sa leçon en classe. On se trompait. On peut désormais se servir d'un drone…C'est qu'on a découvert hier à l'École supérieure du professorat et de l'éducation (Espé) de Lorraine, à Maxéville, près de Nancy.

Jusqu'à ce mercredi soir, s'y déroule un séminaire de formation sur les usages du numérique éducatif. En clair, il s'agit pour les 400 profs présents de réfléchir à la place du numérique dans l'amélioration de la qualité des cours et de l'apprentissage.

« Excellent support »

Pour Laurent Ciarletta, enseignant - chercheur à l'université de Lorraine, et cofondateur de la start-up Alerion, le drone constitue un excellent support d'enseignement. « Quand vous utilisez un drone, les élèves font à la fois de la mécanique, de l'informatique, de la robotique et de l'électronique », explique le maître de conférences. Le professeur se sert du drone avec ses étudiants de l'École des Mines de Nancy au moins depuis 2008 : « On fait des choses incroyables avec ces objets. Mes étudiants s'éclatent, je le vois bien. Ils y passent du temps car ils veulent que ça marche. Avec la machine, ils ne peuvent pas tricher au final. Cela fonctionne ou cela ne fonctionne pas. »

Deux freins

Michel Pesta est également enseignant. Au lycée Louis-Vincent de Metz. Il y transmet les secrets des sciences de l'ingénierie.

Le drone est pratiquement devenu un objet familier de son quotidien professionnel. Cela fait cinq ans qu'il l'a inclus dans sa pédagogie. Depuis une réforme scolaire du bac STI (sciences et technologies industrielles). « Pour les jeunes, indique-t-il, c'est plus concret que des cours magistraux. C'est plus attrayant. »

Pour les deux profs, la présence du drone dans les classes pourrait se développer. Mais à les écouter, on sent deux freins à cette évolution.

■ **Laurent Ciarletta, chercheur, travaille sur des drones avec ses étudiants de Nancy.** Photo ER

Le premier est financier. Un drone « de base » correct, c'est 300 € en moyenne. « L'an dernier, j'ai présenté un kit à 100 € pour les collégiens et lycéens, mais cela n'a pas été accepté », raconte Laurent Ciarletta.

Le second frein est réglementaire. La récente affaire du survol de Nancy, en 2014, le prouve, on ne fait pas voler un drone où l'on veut. Il faut avoir des autorisations et respecter la sécurité.

Le bon vieux stylo a donc encore un peu de temps devant lui.

Mickaël DEMEAUX

Retour sur le brunch - défi LUE « ingénerie au service de la santé et du vieillissement »

A l'occasion de la journée de lancement Lorraine Université d'excellence, le 29 septembre à la Faculté des Sciences et Technologies de Nancy, le brunch - défi «santé» a permis d'aborder l'étude H2020 «FrailSafe» (détection fragilité grâce à des outils connectés), la FHU CARTAGE, la recherche en imagerie, la question des plateformes numériques de services intégrés (ONPA) ainsi que l'appartement intelligent (LORIA).

Animé par Athanase Bénétos, professeur de médecine interne et de gériatrie et Laurence Verger, directrice de la communication recherche du CHRU de Nancy, ce brunch a mobilisé de nombreux acteurs (INRIA - ORANGE - Weelcoop - Human Shape - Human Games, URAFPA, URIOPSS, HARMONIC PHARMA, INSERM, SANOFI, MGEN, ONPA, RSV Concept, CRAN, PERSEUS, IJL...). La question centrale dans le contexte de l'essor de la « silver économie » a été « La conciliation technologie/robotique et facteur humain : est-elle une utopie ? » Ce fil rouge qui anime les échanges montre qu'il s'agit de conserver une pratique éthique au quotidien et de faire avec les patient(e)s/citoyen(ne)s.

Athanase Bénétos coordonne une étude européenne innovante pour mesurer chez les plus de 70 ans les signes avant-coureurs de l'apparition de la fragilité liée à l'âge. Les citoyens volontaires pour cette étude vont être équipés d'objets connectés (vêtement, tablette, téléphone, bracelet,…) pour enregistrer des données sur leurs comportements. Ces mesures sont essentielles à une meilleure compréhension de cette étape de l'avancée en âge, parallèle à l'apparition de pathologies, afin de pouvoir anticiper cette fragilité voire de la prévenir.

Freddy Odille, chercheur en imagerie médicale au sein du laboratoire Inserm IADI (Imagerie Adaptative Diagnostique et Interventionnelle), a présenté les nouvelles techniques d'imagerie cardiaque et mammaire. Ces technologies au carrefour de plusieurs disciplines de recherche, mettant à contribution des start-up et des industriels, se focalisent sur les dispositifs médicaux d'imagerie en particulier concernant les organes en mouvement et ce dans un but à la fois diagnostique et curatif.

François Charpillet, directeur de recherche à l'INRIA et responsable de l'équipe de recherche LARSEN commune INRIA /LORIA a témoigné des avancées exponentielles en e-santé et assistance à la personne, notamment l'intelligence artificielle et la robotique. L'objectif est de développer les connaissances et l'apprentissage des robots « tout en gardant les pieds sur terre », c'est-à-dire leur permettre de s'adapter à des environnements complexes prédominés par les signaux humains. Les partenariats avec les professionnels de santé et le monde économique permettent de valider la recherche pour construire et conserver une expertise des systèmes d'analyse.

Céline Bourguignon, directrice de l'URIOPSS a évoqué le projet de plateforme numérique d'assistance aux personnes en perte d'autonomie. Il s'agit de créer des nouveaux environnements pour les personnes en perte d'autonomie en connectant leur chez elles à différents réseaux : cercle social, services publics, commerces de proximité, services à domicile. La plus-value serait d'en faire également un outil de sécurité en offrant à l'entourage la possibilité d'être prévenu en cas de « point de rupture » dans le quotidien de l'usager. Un projet issu des réflexions et des constats de la dynamique SAILOR (Santé, Autonomie, Innovation en Lorraine), qui est un espace partenarial multi thématique.

Les communications sur ces progrès ont suscité de nombreuses interrogations et débats notamment sur « La connexion des timings Industrie – Recherche ». Diverses idées ont été avancées :

- développer une culture commune et pragmatique entre des acteurs aux objectifs et aux langages différents pour concrétiser les projets ;

- valoriser les partenariats et favoriser la mixité entre les univers médical, industriel et de recherche en santé pour permettre un enrichissement mutuel : confiance, lisibilité et simplicité ;

- harmoniser les demandes initiales des acteurs via l'expression de leurs besoins, puis impliquer tous les partenaires nécessaires (y compris les utilisateurs) pour co-construire ensemble.

Il s'agit de développer une spirale dynamique vertueuse sur le territoire pour entrer dans la « modernité du grand âge », mieux grandir et vieillir ensemble ! Les échanges entre participants se sont poursuivis et de nombreux rendez-vous ont été pris : objectif atteint pour ce brunch - défi «santé».

Science Deux chercheurs Nancéiens du CNRS et de l'INRIA ont mis au jour une faille dans la sécurité d'Internet qui pourrait se révéler intentionnelle. La question de l'espionnage des entreprises est posée

Une faille dans la sécurité d'Internet

Nancy. À qui pourrait profiter une faille dans la sécurité du Net ? « À la NSA par exemple ». Vigie d'Internet au niveau mondial, l'agence de sécurité nationale américaine est citée par Pierrick Gaudry. Chercheur au CNRS, il a mis au jour au sein du laboratoire lorrain de recherche en informatique (Loria), avec Emmanuel Thomé chercheur à l'INRIA et une équipe de chercheurs de l'université de Pennsylvanie, « une faille dans la sécurité d'Internet. Avec l'idée qu'on ne peut pas exclure que la faille que nous avons mise en évidence, ait été créée intentionnellement… ».

De quoi parle-t-on ? Pour communiquer de façon sécurisée, deux ordinateurs mettent en œuvre des protocoles cryptographiques. Une communication chiffrée et totalement invisible pour l'usager lambda. Des algorithmes qui utilisent des nombres premiers (seulement divisibles par un et eux-mêmes). « Ces nombres sont très grands en taille. On parle de 1 024 bits, soit 309 chiffres, au minimum pour pouvoir créer ce que l'on appelle une "clé" de sécurisation des échanges entre deux ordinateurs », explique Pierrick Gaudry.

« Dans un monde normal, ces nombres n'ont pas de propriétés particulières. Ils sont pris au hasard. Nous avons travaillé à créer un nombre premier qui ait l'air aléatoire. Mais dont la structure arithmétique intérieure cache une porte dérobée ». Porte d'entrée dans la fameuse « clé » de sécurisation d'un échange entre deux ordinateurs. En clair un mouchard, capable de pirater une communication chiffrée en 80 minutes.

■ **Des nombres truqués pour pirater les communications chiffrées entre deux ordinateurs.** Illustration Alexandre MARCHI

Espionnage de réseaux sécurisés d'entreprises

« Si nous avons pu créer cette faille, quelqu'un d'autre a pu le faire. » Car le coup de la porte dérobée n'est pas nouveau. « Nous avons remis au goût du jour une technique créée par un Américain dans les années 90. Ce même chercheur qui a aussitôt été embauché… par la NSA. »

Si l'idée de cette faille avait été jugée « peu crédible » en regard des moyens de l'époque, elle prend une tout autre résonance aujourd'hui. Et pose question.

« On imagine que l'intérêt majeur de ce type de faille intentionnelle n'est pas la surveillance de masse. Mais bien l'espionnage de réseaux sécurisés d'entreprises. On sait qu'aujourd'hui 13 % des réseaux d'entreprise utilisent le même nombre premier "louche". Qui n'a aucune traçabilité. Et on le retrouve pourtant dans les standards (normes) de sécurisation sur Internet. »

Qui émet des recommandations sur les normes de fabrication des standards de sécurité du Net ? Des instances américaines proches de la NSA. De là à faire le lien avec les révélations du lanceur d'alerte Edward Snowden sur les opérations de surveillance des communications sur Internet par l'agence de sécurité américaine, le pas est franchi.

Et pour monsieur tout le monde ? Cette découverte aura des conséquences positives. « Cette faille fait déjà l'objet de discussions publiques pour faire évoluer les standards de sécurité sur Internet ».

Stéphanie SCHMITT

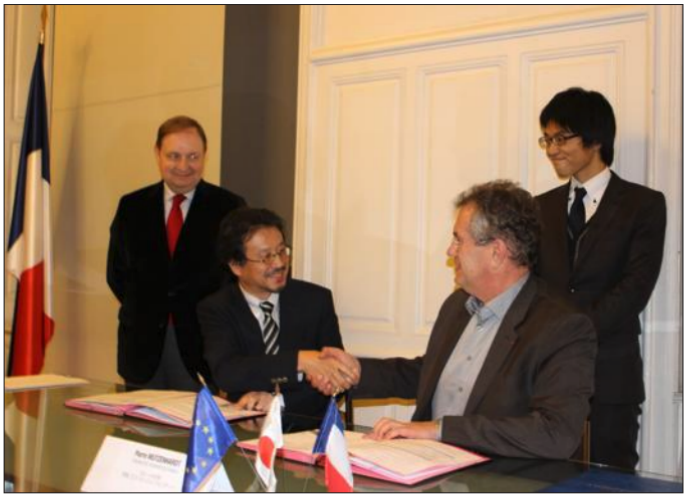
11.2016 - L'Est Républicain

Loria

Un partenariat avec le Japon

Dans le cadre du jumelage de Kanazawa et de Nancy, le LORIA et le JAIST (Japan Advanced Insitute of Science and Technology) a officialisé sa collaboration en présence des élus de la Ville de Nancy, Pierre Mutzenhard, président de l'Université de Lorraine et Satoshi Tojon, doyen du JAIST.

Les deux laboratoires sont connus et reconnus au niveau international en informatique pour leur excellence scientifique. La signature de cette collaboration, officialisée internationalement sous le nom de Memorandum Of Understanding, a pour but de concrétiser des projets scientifiques communs, de renforcer les relations universitaires par le biais notamment de reconnaissance de diplômes, d'encadrement de doctorants et de programmes d'échanges entre étudiants, ainsi que pour les enseignants-chercheurs et les chercheurs. Les travaux de ces deux laboratoires couvrent un grand nombre de thèmes communs comme le calcul à haute performance, la sûreté et sécurité en informatique, la robotique, les réseaux informatiques, l'analyse d'image ou le traitement automatique des langues naturelles et la musique.



■ **La convention signée.**

La création de ces nouvelles synergies internationales au profit de la recherche en informatique repose sur un noyau d'enseignants-chercheurs actifs qui coopèrent déjà dans les domaines de la robotique et de la sécurité.

Internet : des clés plus fragiles qu'il n'y paraît

Des chercheurs ont démontré qu'il serait aisé de compromettre la sécurité des communications sur Internet en utilisant des nombres «truqués».

Internet est-il sûr ? Plus précisément, les protocoles qui permettent à deux ordinateurs distants de communiquer sont-ils immunisés contre le piratage ? La question est d'importance tant ces protocoles font partie de notre quotidien numérique. Une connexion sur le site de votre banque ? Celle-ci commence par la mise en place d'un canal sécurisé. Un achat en ligne ? Idem. Le paiement dématérialisé de vos impôts ? Rebelote. Or une équipe franco-américaine impliquant des chercheurs du Laboratoire lorrain de recherche en informatique et ses applications1 (Loria), vient de démontrer qu'il est possible de compromettre une clé de chiffrement pour la rendre quasi inopérante… sans que personne ne s'en aperçoive.

Partager ses clés sans les compromettre

Pour le comprendre, il faut revenir à la base de la sécurité sur Internet. À savoir, l'échange d'une série de chiffres – la clé – entre deux ordinateurs, grâce à laquelle sont ensuite chiffrées les informations ou authentifiées les connexions. Le principe ? Camoufler cette clé par de complexes opérations mathématiques qui sont à la fois faciles à calculer dans un sens, mais difficiles à craquer par un tiers malveillant qui tenterait d'utiliser le résultat de ces opérations pour retrouver la clé.Concrètement, les échanges de clés sur Internet sont fondés sur l'algorithme de Diffie-Hellman, du nom de ses inventeurs en 1976. Explications : imaginons qu'à chaque extrémité d'une ligne de communication, Alice et Bob se mettent d'accord sur un nombre premier – c'est-à-dire qui ne soit divisible que par lui-même et par un – choisi parmi une liste standard préétablie.
Alice et Bob choisissent ensuite chacun de leur côté un nombre secret qui, combiné avec le nombre premier précédent selon l'algorithme Diffie-Hellman, permet à chacun de calculer un troisième nombre qu'ils vont pouvoir échanger en ligne. À ce stade, la magie de l'algorithme permet à Alice et Bob de calculer un ultime nombre commun (la clé) calculé à partir du nombre reçu de l'autre et de leur propre nombre secret – nombre qui, lui, n'a jamais été échangé.

Gare aux nombres premiers piégés

Ainsi, n'ayant pas la possibilité d'accéder à ces nombres secrets, un pirate, même s'il a intercepté les nombres échangés, sera dans l'incapacité de retrouver la clé. Du moins en théorie… En effet, un pirate ayant eu connaissance du nombre premier échangé au départ et disposant d'une puissance de calcul suffisante pourrait « craquer » cette clé.

Un écueil dont on peut se prémunir en utilisant des nombres premiers suffisamment grands, de telle sorte que le nombre d'opérations mathématiques à réaliser pour déterminer la clé soit hors de portée d'un malfaiteur commun. De nos jours, une clé construite à partir d'un nombre premier de 768 bits n'offre plus qu'une protection illusoire. En effet, en juin, une équipe de l'université de Leipzig et de l'École polytechnique fédérale de Lausanne est parvenue à casser une telle clé. Il est vrai qu'en pratique, les nombres utilisés sont de 1 024 bits, soit environ 300 chiffres. Mais là où le bât blesse, c'est que certains nombres premiers génèrent des clés totalement perméables aux algorithmes casseurs de clés.

La chose est évidemment technique, mais grosso modo si ce nombre est la valeur d'une certaine fonction – d'un polynôme – en un point, et que le pirate le sait, les clés associées sont compromises. Cette faille vient d'être démontrée par les informaticiens du Loria qui ont craqué une clé fondée sur un nombre premier de 1024 bits savamment choisi. « Nous y sommes parvenus 10 000 fois plus rapidement que le temps nécessaire pour une « vraie » clé, et ce avec 10 fois moins de puissance de calcul que celle utilisée par nos collègues de Leipzig et de Lausanne dans le cas à 768 bits », précise Emmanuel Thomé, du Loria.

Des listes de nombres à surveiller

Pour que cette faille soit exploitée, il faut donc que les listes standard, qui recensent les nombres utilisés en cryptographie, aient été préalablement truquées par ceux-là même qui veulent se livrer à des activités d'espionnage. Or, souligne le cryptologue, « personne ne sait très bien comment ces nombres ont été sélectionnés ». On note toutefois qu'une des listes couramment utilisées a été établie par un sous-traitant de la NSA. Et que le scientifique à l'origine de la méthode utilisée par le groupe franco-américain, Daniel Gordon, travaille également pour une entreprise proche de cette même agence.

Si l'on ajoute à cela que les documents rendus publics par le lanceur d'alerte Edward Snowden montrent que la NSA a essayé d'influencer les standards et les spécifications pour les techniques commerciales de clés publiques, tous les ingrédients sont réunis pour un roman d'espionnage moderne à succès.
« Notre objectif n'est pas d'alimenter la théorie du complot, prévient Emmanuel Thomé. Mais de montrer que la sécurité d'Internet est très largement perfectible. » Comment ? En commençant par piocher des nombres premiers dans des listes labellisées, en augmentant la taille des clés ou bien encore en affinant les algorithmes de cryptographie. Histoire que l'ombre de « big brother » ne plane pas au-dessus de votre prochain achat sur Internet !

INDUSTRIE DU FUTUR

Afin d'aider la lutte contre les cybermenaces, le LORIA[1] de Nancy a créé Gorille. Ce logiciel repère les similitudes entre les codes binaires pour mieux identifier les nouveaux malware. Avec cette technologie, les entreprises bénéficient d'un processus automatisé qui optimise la protection de leur réseau. Cette technologie est présentée lors de la Bourse aux Technologies organisée par l'IMT le 15 novembre 2016.

Vous vous sentez ralenti, comme paralysé ? Vous êtes probablement contaminé… par un virus informatique ! Malheureusement ceux-ci ne sévissent pas en fonction des saisons. Au contraire, il ne nous laisse aucun répit. D'autant qu'à eux s'ajoutent les maliciels (ou malware) et autres cybermenaces qui infestent les réseaux et affectent les entreprises, les médias ou encore les Etats sans distinction. En 2015, Panda Security dénombrait 230 000 nouveaux malware découverts chaque jour. Pour lutter contre cette contagion grandissante, les analystes disposent de peu d'armes. Afin d'aider ces experts virologues dans leur traitement des infections, une équipe de chercheurs du LORIA de Nancy a mis en place le logiciel Gorille. Celui-ci offre un processus automatisé dans le but d'augmenter la productivité des rétro-analystes face à des menaces en perpétuelle évolution.

Une analyse par similarités

Détecteur de maliciels, recherche de plagiat, cybersécurité… les fonctionnalités de Gorille sont vastes. Ce logiciel multi-facette a été conçu pour comparer des codes binaires. « L'analyse de ces codes vise à comprendre ce que fait un logiciel : est-ce qu'il lit les touches du clavier ? Est-ce qu'il transmet des informations sur le web ? etc. Actuellement, cette tâche est particulièrement difficile car elle est faite à la main par des rétro-analystes », explique Guillaume Bonfante, l'un des chercheurs à l'origine du logiciel.

Là où d'autres techniques cherchent les différences dans les codes de deux logiciels, Gorille s'appuie sur l'identification de similitudes. Une approche qui permet de gagner en efficacité car les points communs entre les codes sont généralement plus rares que leurs différences. La technique utilisée par le LORIA répond à un autre constat : l'écriture des virus peut être dépourvue d'imagination. En effet, il est assez facile de construire de nouveaux virus en se basant sur d'autres déjà existants.

Alors pourquoi vouloir s'embêter à en réinventer un entièrement si l'on peut en plagier un autre ? Parce que Gorille vient bouleverser le cours des choses et met fin à la fainéantise des écrivains de virus !
« Nous sommes capables de reconnaitre des programmes différents dès lors qu'ils emploient quelques briques logicielles communes. C'est ainsi que nous avons découvert les liens entre les trois célèbres malwares : Stuxnet, Duqu et Gauss. Gorille reconnait chacun d'eux à partir d'une souche d'un des autres », développe Guillaume Bonfante.

Une combinaison de techniques

Regardons plus en détail comment Gorille a permis d'en arriver là. Dans son analyse, le logiciel étudie les graphes de flot de contrôle. Ces derniers sont des outils d'observation du fonctionnement d'un code. Ils permettent de suivre l'enchainement d'instructions lorsque ceux-ci sont exécutés. Gorille ajoute à cela une étape d'abstraction de ces graphes. « Celle-ci est nécessaire pour accéder à la robustesse de notre technique aux transformations des logiciels et la reconnaissance de ceux qui partagent des sources », détaille le chercheur. Autrement dit, cette méthode permet de reconnaître la forme d'un logiciel malveillant. Guillaume Bonfante parle alors d'analyse morphologique et Gorille est le seul logiciel à fonctionner ainsi.

« Notre méthode est globale, elle porte sur la totalité du code et elle est structurelle (graphe de flot de contrôle). Donc avec l'analyse par similarités, l'écrivain d'un virus ne peut plus réutiliser simplement des lignes de code déjà existantes mais doit « repartir de zéro » pour construire un nouveau virus ». En complément, les chercheurs utilisent une analyse dynamique de codes binaires. En effet, les logiciels ont la fâcheuse capacité à pouvoir s'auto-modifier ce qui rend leur traitement difficile. « Ce procédé permet de révéler des parties cachées de code que nous étudions par la suite avec Gorille. Ces parties cachées sont très communes pour les malware (> 92%) et suffisent en général à tromper les logiciels antivirus usuels », explique Guillaume Bonfante.

Un logiciel dédié aux entreprises

Avec sa robustesse et son adaptabilité, l'innovation Gorille est un logiciel de qualité dédié à la cyberdéfense. Son autonomie permet d'évaluer le rapprochement entre des codes binaires qui serait difficile à mettre en œuvre humainement parlant. Les résultats des analyses ainsi optimisées sont ensuite transmis à l'utilisateur sous diverses formes : document texte, pages html… Toutefois, ces résultats demandent un certain niveau d'expertise pour être analysés. D'autre part, c'est à l'entreprise que revient le choix d'utilisation de Gorille. Elle peut l'exécuter par collectes journalières ou horaires, par anticipation à l'entrée du réseau, après un pare-feu, etc.

En somme, le logiciel fonctionne sous Windows, Linux et MacOS. En plus, les chercheurs ont la possibilité d'analyser les codes que l'on trouve généralement sur les téléphones portables. « Le logiciel a été conçu pour être intégré à des solutions globales d'analyse de code », ajoute Guillaume Bonfante.

Une démocratisation à venir

L'équipe de recherche à l'origine de Gorille a décidé de créer une spinoff appelée Simorfo (en cours d'élaboration). Celle-ci permettra la valorisation de Gorille et de l'analyse morphologique directement sur le marché européen de la cybersécurité. Les chercheurs veulent ainsi proposer leur solution innovante que Guillaume Bonfante résume en trois idées : « La découverte de nouveaux malware, la robustesse aux transformations des logiciels et la simplicité, car notre technologie s'adapte à de nombreux contextes et emplois ».

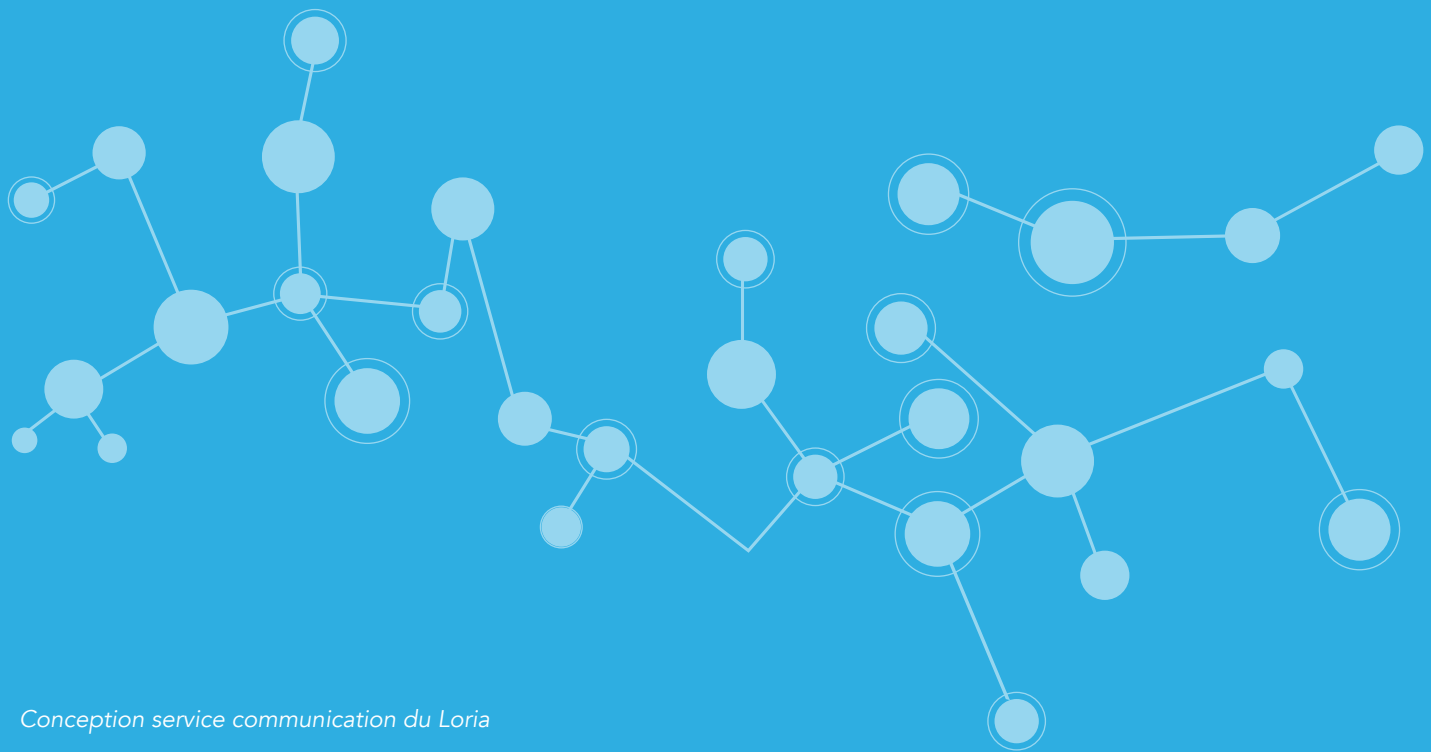
[1]LORIA : Laboratoire lorrain de recherche en informatique et ses applications, est une UMR commune au CNRS, l'Université de Lorraine et l'Inria.

Le +

Gorille sera présenté à la Bourse aux technologies

Mardi 15 novembre 2016, l'Institut Mines-Télécom (doublement labellisé Carnot pour la qualité de sa recherche partenariale) organise avec Mines Nancy et en lien avec Télécom Nancy, l'École nationale supérieure de Géologie et Télécom Physique Strasbourg, une nouvelle Bourse aux technologies autour du thème « Big Data pour l'optimisation industrielle ». Le LORIA y présentera son logiciel pour la cybersécurité.

Loria



Conception service communication du Loria