Un master breton pour traquer les cyberpirates

A Lorient, une nouvelle formation se concentre sur la protection des objets connectés et de leurs usagers

LORIENT (MORBIHAN) - *envoyé spécial*

SIMON LANDREIN

Ils veillent sur notre santé, sécurisent nos maisons, nous assistent pour la conduite de nos automobiles, valident nos paiements... Ce sont les objets connectés. Des concentrés d'électronique et d'informatique mêlés, quasiment absents de notre quotidien au siècle dernier, qui nous accompagnent aujourd'hui dans la plupart de nos gestes. On en compterait 40 milliards en 2018, selon l'Idate DigiWorld, think tank spécialisé dans l'économie numérique, et *« à l'horizon 2020, il y en aura entre 80 et 200 milliards »,* prévoit Philippe Coussy, professeur à l'université de Bretagne-Sud (UBS).

Beaucoup de ces objets visent à optimiser la sécurité de leurs usagers, mais sont-ils sûrs eux-mêmes ? Un pacemaker, une carte de transport, une automobile, un drone... sont-ils à l'abri d'une prise de contrôle mal intentionnée ? Le garantir sera le métier de Nicolas, Samy et Eliott, étudiants du nouveau master « cybersécurité des systèmes embarqués », ouvert en 2017 à la faculté des sciences et sciences pour l'ingénieur de l'UBS à Lorient (Morbihan).

Sécuriser l'accès à ses données personnelles et professionnelles, équiper son matériel informatique d'un antivirus, d'un pare-feu, ou protéger ses connexions à distance avec un réseau privé virtuel (VPN) sont des pratiques entrées dans les usages des entreprises, puis du commun des utilisateurs. *« La sécurité s'est beaucoup développée en informatique,* reconnaît Guy Gogniat, professeur de sécurité des systèmes embarqués à l'UBS. *Mais les composants électroniques n'ont pas été créés pour se défendre contre des usages malveillants. »*

Potentiels chevaux de Troie

En clair, les logiciels qui animent les écrans de nos portables, tablettes, ordinateurs, partie immergée de nos outils numériques sont, dès la conception, pensés pour résister aux attaques des pirates informatiques. En revanche, les composants électroniques, chevilles ouvrières de notre cyberenvironnement, sont autant de potentiels chevaux de Troie. *« Le point d'entrée pour une prise de contrôle »,* explique Philippe Coussy. Une porte ouverte que les étudiants doivent apprendre à repérer, et à refermer.

Au programme des étudiants du master : de la microélectronique, de l'informatique et des mathématiques, trois matières intimement liées aux objets connectés. Parmi ses outils d'apprentissage, la faculté propose une plate-forme d'évaluation de sécurité des composants électroniques, dans un laboratoire qui semble inspiré de celui du docteur Emmett Brown dans *Retour vers le futur,* où pullulent instruments de mesure et écrans de contrôle.

C'est ici que les pionniers de cette première promotion bretonne apprennent notamment à mesurer le rayonnement électromagnétique d'un composant électronique pour en déceler les failles, les fuites, les éléments à sécuriser. *« Nous apprenons aux étudiants l'ensemble des bases théoriques et ils acquièrent ici des connaissances pratiques qu'ils pourront mettre en œuvre auprès d'un employeur »*, résume le professeur Coussy.

Justement, quelles sont ces entreprises au sein desquelles les futurs diplômés pourront mettre en pratique leurs prochaines compétences ? Les fleurons français de l'électronique et de l'aéronautique comme Thales et Safran sont les premières citées par ces étudiants, les constructeurs automobiles suivent de près. *« Nous avons besoin de ces profils »,* reconnaît Vincent Mattei, responsable recrutement et mobilité pour Thales en France.

« Le déficit entre l'offre de formation et la demande des entreprises est considérable »

VINCENT MATTEI
responsable recrutement et mobilité pour Thales en France

Pour la seule année 2018, la compagnie, qui se targue de protéger *« les systèmes d'information de dix-neuf des vingt plus grandes banques mondiales »,* prévoit de recruter 200 personnes en France dans le seul domaine de la cybersécurité.

Course technologique

La montée en puissance de l'électronique embarquée ouvre une *« multitude de possibilités dans le domaine du recrutement*, poursuit M. Mattei. *Sécuriser ces environnements ne concerne pas seulement les systèmes de défense, mais également les transports, les communications, l'aéronautique, le spatial, les banques... Cela touche le grand public, car tous les produits électroniques sont potentiellement vulnérables. Ce sont des métiers nouveaux et le déficit entre l'offre de formation et la demande des entreprises est considérable. »*

Yannick Teglia, expert sécurité chez Gemalto, multinationale spécialisée en cybersécurité, partage cette analyse sur ce secteur du marché. *« Nous avons besoin de formations spécialisées dans des domaines très larges, car nous créons de plus en plus de produits qui intègrent un composant électronique*, expose-t-il. *La croissance du numérique est exponentielle. Parallèlement, nous avons du mal à recruter, nous avons plus de besoins que de bonnes candidatures. »*

D'où l'intérêt quasiment stratégique du nouveau master de Lorient. La sûreté des objets connectés est un enjeu majeur pour toutes les entreprises qui doivent protéger leurs clients – et leur réputation. En 2015, deux hackeurs avaient fait la démonstration qu'ils pouvaient pirater à distance une Jeep Cherokee de Fiat Chrysler, prendre le contrôle de différents éléments embarqués, comme la radio, les essuie-glaces... Plus inquiétant, ils pouvaient couper le moteur, les freins et provoquer une sortie de route du véhicule ! Si ce piratage se voulait une démonstration amicale, l'avertissement a été reçu par tous les constructeurs. *« La concomitance de connectivités – smartphones, tablettes, montres – avec la voiture crée de nouvelles menaces pour la conduite automatisée »,* constate Eric Dequi, responsable des activités cybersécurité du véhicule connecté au sein du groupe PSA (Peugeot, Citroën, DS, Opel, Vauxhall).

L'univers de la cybersécurité est innovant et en perpétuel mouvement. Les entreprises, les universités et les écoles se livrent avec les hackeurs à une course sans fin. Les premiers inventent des solutions, les seconds cherchent et trouvent des failles que les premiers s'empressent de combler.

Une véritable course technologique contre la montre, qui réclame des compétences de plus en plus pointues, car *« les attaques sont de plus en plus performantes »,* affirme Arnaud Tisserand, directeur de recherche au CNRS au laboratoire des Sciences et techniques de l'information, de la communication et de la connaissance.

Comme un officier instructeur qui formerait des corsaires, ce chercheur rappelle aux étudiants les différents niveaux de menaces qu'ils auront à contrer : *« Les bidouilleurs, parfois talentueux mais dépourvus de moyens »*, puis *« les hackeurs chevronnés »*, les professionnels de la cybersécurité de *« sociétés concurrentes »,* et, peut-être un jour, *« les mafias et les Etats »,* aux moyens quasi illimités. Bienvenue dans votre futur métier, déclinaison « cyber » des *« gendarmes et des voleurs »,* encourage, confiant, le scientifique. ■

ÉRIC NUNÈS

Pendant les concours, la chasse aux cybertricheurs est ouverte

« NOUS SOMMES PLUSIEURS *à nous balader avec nos détecteurs de communication »*, raconte Marc Bonnet, président de Concours communs polytechniques (CCP) – qui changeront de nom pour devenir CCINP pour la session 2019 –, qui fédère plusieurs dizaines d'écoles et rassemble jusqu'à 4 000 candidats sur un même site. Entre les montres numériques et les lunettes connectées, les antisèches ont pris le tournant de la modernité, et la surveillance des concours aussi.

Toutes les étapes du concours sont largement sécurisées. En raison du décalage horaire, quand les épreuves ont lieu à l'étranger, les élèves sont isolés dans un hôtel dès l'ouverture des sujets en France. Coffre, contrôle d'accès aux bâtiments, systèmes anti-intrusion : avec le développement des objets connectés, la vigilance s'aiguise pour déjouer les astuces parfois sophistiquées des cybertricheurs. Lors de la préparation des sujets, les échanges entre les rédacteurs ne peuvent transiter que quatre heures sur une plate-forme cryptée. Ensuite, ils s'autodétruisent. *« Une fois l'épreuve corrigée, si des réclamations se font jour, il faut au moins trois personnes dont deux informaticiens pour accéder aux notes et les modifier »*, relève Jean-Marc Le Lann, le directeur du concours CCP.

De son côté, face aux demandes de vérification de notes pour les épreuves d'admissibilité *« qui ont augmenté de manière exponentielle »,* le concours Centrale-Supélec (qui rassemble chaque année plus de 23 000 candidats pour 15 000 places dans une dizaine d'écoles) a engagé une nouvelle procédure plus contraignante depuis 2016. Les réclamations sont désormais limitées à une seule épreuve par candidat.

« Manque de respect » des institutions

Les comportements de certains candidats troublent les organisateurs. *« L'un des élèves a filmé son oral. Il remettait en cause certaines questions et a envoyé sa vidéo au directeur de l'école »,* se souvient Catherine Gautier de La Plaine, déléguée générale de Passerelle, un concours réservé à des étudiants pour entrer dans de grandes écoles de management par des voies parallèles. Un comportement contestataire qui révèle, selon elle, *« un manque de respect »* des institutions. Une autre fois, un candidat s'est fait pincer avec des antisèches sur sa calculatrice : *« Il avait beau être dans son tort, il a aussitôt demandé à appeler son avocat, avec un aplomb et une arrogance étonnante ! »*

Assumer sa triche : c'est le libre-arbitre de chacun face au concours que défend Marie Glinel, en doctorat de droit, lorsqu'elle prend la parole au sein de la juridiction administrative qui statue en dernier ressort sur les décisions des commissions disciplinaires des universités. Elle fait partie des 11 étudiants, sur les 60 membres du Conseil national de l'enseignement supérieur et de la recherche (Cneser) qui fixent le sort des fraudeurs.

« Je refuse la vision déterministe qui consisterait à chercher des excuses. La confiance va de pair avec la responsabilité », tranche cette adhérente de l'Union nationale interuniversitaire (UNI), qui rappelle la palette large de sanctions (privation d'examen, amendes, prison).

A Ecricome, une banque de concours mandaté par les écoles de commerce, sur cinq incidents relevés en 2017, trois ont donné lieu à un rapport. *« Une fois, un élève est sorti en emportant par erreur sa copie. Il s'en est aperçu, l'a rapportée aussitôt, mais c'était trop tard »*, explique Stéphane Civelli, son délégué général. De quoi devenir responsable. ■

MADELEINE VATEL