Grenoble INP

Grenoble INP Press

Lettre d'information numéro 25
Mai 2016

Risque numérique, sécuriser à tous les niveaux

EDITORIAL

Jean-Louis Roch,
enseignant à Grenoble INP – Ensimag et chercheur à Verimag

La cybersécurité : un enjeu majeur

Dans un monde où le numérique intervient dans la majorité des secteurs d'activité, où l'internet des objets explose, comment garantir la confidentialité des données et la sécurité des systèmes ? Grenoble, où la sécurité a toujours été au cœur des thématiques de recherche transverses de plusieurs laboratoires, est très bien placé pour relever ces défis. Le bassin valentino-grenoblois regroupe en effet des compétences techniques fortes, rassemblées au sein de l'équipe action SCCyPhy (Security and Cryptology for CyberPhysical systems) du labex Persyval-LAB, qui regroupe une soixantaine de chercheurs issus de différents laboratoires*. Cette action affiche une ouverture sur les sciences humaines et sociales, composante indispensable de la cybersécurité en termes de protection des données privées. Ainsi, le tout nouveau réseau AMNECYS (dont fait partie le laboratoire CESICE de l'UGA) a pour ambition de rassembler des équipes pluridisciplinaires pour aborder la sécurité sous un angle global (légal, sociétal et technique), et pour apporter des réponses sur des dossiers d'expertise complexes, par exemple dans le domaine de la protection des données personnelles, ou celui de la sécurité des infrastructures d'importance vitale.

A Grenoble, la sécurité est au coeur de recherches transverses

En termes de formation, Grenoble INP- Ensimag propose un master en Cybersécurité avec l'Université Grenoble Alpes, et plusieurs écoles ont des filières spécialisées dans cette thématique. L'avenir des jeunes ingénieurs est assuré : aujourd'hui, nous avons plus d'offres d'emploi que d'étudiants. La législation prévoyant de rendre les entreprises responsables de la sécurité de leurs données, la tendance ne devrait que se confirmer !

** TIMA, CEA, GiPSA-Lab, G-Scop, Inria, Institut Fourier, LIG, LJK, TIMA, Verimag*

l'actualité de Grenoble INP
en **page 4** Brèves | Événements | Informations pratiques ...

Risque numérique, sécuriser à tous les niveaux

A L'HEURE DU TOUT NUMÉRIQUE, LA "CYBER" MENACE N'A JAMAIS ÉTÉ AUSSI FORTE. GRENOBLE INP PREND LE PROBLÈME À CŒUR ET ORGANISE LA LUTTE SUR PLUSIEURS FRONTS : SÉCURISATION DES COMPOSANTS, DES LOGICIELS ET DES SYSTÈMES…

Du téléphone à la voiture, en passant par les systèmes d'information et les systèmes industriels, tout peut aujourd'hui devenir la cible potentielle d'une cyberattaque. Qui ne se souvient de celle perpétrée contre TV5 Monde, entraînant l'arrêt de la diffusion des programmes durant deux jours en avril 2015 ?

A Grenoble INP, qui inaugurera une chaire industrielle spécifiquement dédiée (voir encadré), la résistance s'organise sur tous les fronts, de la sécurisation au niveau matériel, à la sécurisation des logiciels et des systèmes. "*Notre approche pluridisciplinaire, entre électronique et informatique, est une force*, estime David Hély, enseignant à Grenoble INP – Esisar et chercheur au LCIS. *Cela permet de répartir la sécurité sur toute la chaîne de valeur : composants, circuits, logiciels… Il ne faut laisser aucun maillon faible !*"

D'abord, au niveau du composant lui-même. Comment être sûr que les composants que l'on intègre à un système critique ne comportent pas de fonctionnalités malveillantes, ou encore des "chevaux de Troie" potentiellement insérés lors des différentes étapes du cycle de fabrication qui permettront à leurs concepteurs

Répartir la sécurité sur toute la chaîne de valeur, depuis le composant jusqu'au système complet

de prendre la main sur le système ? Comment s'assurer que le circuit n'est pas contrefait avec les risques sur la sûreté que cela encoure, ou bien encore que les circuits seront robustes aux attaques physiques de plus en plus sophistiquées ? Au LCIS, des outils sont développés pour garantir l'authenticité des composants en assurant un traçage depuis leur fabrication jusqu'à leur intégration (identification de signature RF, etc.). Enfin, des mécanismes de confiance ajoutant des "espions" qui vont s'assurer en temps réel que le circuit ne fait que ce qu'il est censé faire, sont conçus et intégrés dans les circuits.

Parallèlement, les chercheurs du LCIS mais également du TIMA et du LIG, développent des méthodes pour tester la robustesse des circuits existants vis-à-vis de certains types d'attaques. "*Les cartes à puces, par exemple, peuvent être attaquées en analysant la signature de paramètres physiques tels que leur consommation énergétique, leurs émissions électromagnétiques*, explique Régis Leveugle, chercheur au TIMA. *C'est l'attaque par canaux auxiliaires. On peut également perturber volontairement le fonctionnement de cette carte afin d'analyser la différence entre les réponses normale et perturbée, et en déduire la clé de chiffrement. C'est l'attaque par faute*".

Autre laboratoire, autre approche : au LIG, des chercheurs explorent la vulnérabilité des logiciels en "boite

La sécurité au cœur des formations

Créé en 2002, le master Security, Cryptology and coding of information systems était dès l'origine une formation mixte Ensimag/UJF. A raison d'une trentaine d'étudiants par an, il a formé environ 300 ingénieurs, avant d'être restructuré cette année en master M2. Baptisé Cybersecurity, il est tout particulièrement orienté sur l'analyse des vulnérabilités et propose des contenus équilibrés en cryptologie, et sur les aspects de sécurité informatique. L'idée est de former des ingénieurs capables de faire face aux nouveaux défis posés par l'augmentation des performances des machines. De son côté, l'Esisar propose des formations au cœur desquelles la sécurité est omniprésente, et affiche la volonté de monter en compétences sur ce thème. Ainsi, la filière "Informatique et réseaux" est en cours de labellisation CyberEdu. Initié par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) à la suite de la publication du Livre blanc sur la Défense et la sécurité nationale en 2013, le projet CyberEdu a pour objectif d'introduire les notions de cybersécurité dans l'ensemble des formations en informatique de France. "*La sécurité ne peut reposer uniquement sur des experts*, estime Yves Guido, enseignant-chercheur à l'Esisar. *Chaque acteur de la chaîne des systèmes d'information doit être concerné et impliqué*". L'objectif est donc de faciliter la coopération avec les spécialistes en cybersécurité, d'améliorer la vigilance et la réaction aux incidents, et de prévenir l'apparition des vulnérabilités. L'école a pour ambition de former 50 élèves par an d'ici 5 ans. La demande en formation dans le domaine de la sécurité du numérique semble assurée. Cette démarche est fortement encouragée par l'état, qui l'a inscrite comme une priorité dans ses programmes (stratégie numérique, plan d'investissements d'avenir, loi de programmation militaire). L'école est également soutenue financièrement pour ce projet par les entreprises et collectivités du territoire, à travers plusieurs partenariats (Projet NumericLab, PIA-07).

noires". "*Nous utilisons des tests en frelatage qui consistent à soumettre le programme à des données aléatoires, mal formées, afin de prévoir son comportement s'il était confronté à un attaquant*", explique Roland Groz, professeur à Grenoble INP – Ensimag et chercheur au LIG.
Outre la mise en place de méthodes pour déterminer le niveau de robustesse des circuits aux attaques (dont certaines font l'objet de travaux de simulations), les chercheurs développent des méthodes de protection pour les rendre plus robustes. Ces protections peuvent intervenir au niveau matériel ou au niveau algorithmique, mais dans tous les cas, il est nécessaire de trouver un compromis entre le niveau de sécurité requis, le coût que cela engendre et la consommation énergétique.

Protéger les systèmes critiques sensibles

Les systèmes industriels et les systèmes d'information ne sont pas épargnés. Jusqu'à la fin des années 2000, ils étaient uniquement protégés par un ensemble de barrières, portiques, contrôles d'accès... Toute une série de mesures de protection qui restent d'actualité, mais qui ne suffisent plus. Les ordinateurs sont aujourd'hui connectés à des systèmes de contrôle commande critiques (SCADA), et "*il suffit qu'un petit malin s'introduise sur le système pour qu'il soit à même de prendre les commandes et d'envoyer des ordres malveillants dont les conséquences peuvent être dramatiques*", s'inquiète Eric Zamaï, chercheur au laboratoire G-SCOP, en mentionnant l'exemple célèbre du ver informatique Stuxnet, qui avait pénétré le réseau informatique pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium.

Pour assurer la sécurité des systèmes de contrôle commande critiques, le mot d'ordre, c'est la supervision

Pour prévenir les actes de malveillance sur les sites industriels et les infrastructures critiques, comme les réseaux électriques, les hôpitaux ou encore les centrales nucléaires, des mesures spécifiques doivent être mises en place. En plus de la sécurisation informatique du réseau de premier niveau (firewall, mots de passe), du cryptage des données et du codage des informations, les experts mettent en place des systèmes de surveillance des échanges et du pilotage des

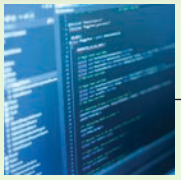
La chaire "Confiance dans les systèmes", bientôt inaugurée

La Fondation Partenariale de Grenoble INP, l'Esisar, le laboratoire LCIS et un consortium d'industriels s'apprêtent à inaugurer la chaire d'excellence "Confiance dans les systèmes". Celle-ci entend donner plus de visibilité et favoriser l'attractivité du pôle valentino-grenoblois dans le domaine de la sécurité et de la sûreté de fonctionnement des systèmes d'information, industriels et embarqués. "*Mise en place pour cinq ans, la chaire a pour ambition à la fois de consolider le projet pédagogique de l'Esisar sur ces thématiques, et de permettre la mise en place du programme scientifique proposé par le LCIS sur la thématique de la confiance dans les systèmes*, indique Gilles Gauthier, chargé d'affaires à Grenoble INP – Esisar. *Elle constituera le terreau favorisant le développement d'une recherche collaborative grâce au caractère pluridisciplinaire du laboratoire et permettra d'identifier de nouveaux parcours pédagogiques intéressants pour le secteur*". La Chaire financera des activités de recherche (thèses, post docs,...) et pourra s'appuyer sur la plateforme Esynov située à Valence afin de matérialiser les retombées applicatives issues de ces travaux (projets industriels de R&D, stages de fin d'études pour les étudiants des filières "Informatique et réseaux" et "Systèmes embarqués" de l'Esisar, achats de matériels pour le développement de plateaux techniques, etc.). Un volet formation continue sera également mis en place sur ces thématiques. Le consortium d'entreprises, parmi lesquelles figurent déjà InnovistaSensors / Crouzet, SKF Aerospace, GDRF,et Ansys, est appelé à s'étoffer dans les mois à venir.

Risque numérique sécuriser à tous les niveaux (suite)

systèmes. Au G-SCOP et au Gipsa-Lab, des chercheurs mettent par exemple au point des protocoles pour détecter les intrusions éventuelles en repérant les ordres anormaux. "*Une bonne connaissance du métier est nécessaire pour repérer si un ordre va à l'encontre de la physique et de la sécurité*", souligne Eric Zamaï. Le mot d'ordre, c'est la supervision. C'est-à-dire la capacité à visualiser la totalité des interactions et des échanges des composants d'un site industriel, ainsi que du contrôle-commande de tous les automates et terminaux informatiques.

Au G2E-Lab, Raphael Caire modélise quant à lui les réseaux électriques en prenant en compte leurs interdépendances avec les réseaux de communication et les systèmes d'information. "*Une plateforme a été développée au laboratoire pour simuler à l'identique l'ensemble des dispositifs matériels et logiciels mis en œuvre. Ensuite, partant du principe que le réseau a été piraté, on cherche les parades les plus efficaces*". Là encore, la force de Grenoble INP réside dans la possibilité de faire une réponse sur plusieurs axes.



Des étudiants impliqués

Très actif depuis plusieurs années, le Club Securimag regroupe des étudiants du niveau L3 au doctorat en sécurité. Il organise des séminaires réguliers sur le thème de la cybersécurité à l'Ensimag, et une conférence qui a acquis une réputation dépassant nos frontières : Grehack. Cette dernière, qui attire à Grenoble près de 200 personnes chaque année, est suivie avec intérêt par des experts de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et du Ministère de la défense. Elle se termine par l'événement CTF (Capture The Flag), une sorte de "Nuit du Hack", dans les locaux de l'Ensimag.

Par ailleurs, les étudiants de la filière Systèmes embarqués de Grenoble INP - Esisar participent régulièrement, et avec un certain succès, au concours Embedded Security Challenge lors du CSAW (Cyber Security Awarness Week) à New York. Il s'agit du plus grand événement universitaire traitant de la cyber-sécurité réunissant universitaires, organismes nationaux et industriels tels Intel, Qualcomm ou Google.

L'actualité de Grenoble INP

Grenoble INP 2ème au classement Industrie et Technologies

Industrie et Technologies vient de publier sur son site de veille technologique pour les professionnels de l'industrie son 20ème classement des écoles d'ingénieurs.

Grenoble INP est 2ème au classement général. Ce classement prend en compte le montant des contrats de recherche, le nombre de doctorants et post-doctorants, et le nombre de brevets.

Industrie et Technologies publie également le classement des écoles qui emploient le plus de doctorants. Sur ce critère, Grenoble INP obtient la meilleure note et se classe ainsi 1er.

SUIVEZ GRENOBLE INP → www.grenoble-inp.fr/**suivez-nous**

Le groupe Grenoble INP publie une lettre mensuelle "Grenoble IN'Press", accessible sur internet : www.grenoble-inp.fr
Directeur de la publication : Brigitte Plateau - Coordination : Marie-Paule Schuhl - Rédaction : Clotilde Waltz
Conception graphique et réalisation : Service communication - Crédits photos : Grenoble INP / Fotolia / Alexis Chézière
ISSN 12558-7218 • Dépôt légal en cours
Contact : communication@grenoble-inp.fr - 04 76 57 43 91 - Grenoble INP • 46 avenue Félix Viallet • 38031 Cedex 1