Compte rendu du Conseil Scientifique de l'INS2I

29 Février 2016

Présentation des membres invités

- Michèle Basseville, présidente section 7, DR CNRS IRISA
- Valérie Berthe, membre CS CNRS
- Michael Blum, CID51
- Matthieu Latapy, CID53

Actualités de l'Institut – échanges avec la direction de l'INS2I

Organisation
L'équipe scientifique de l'institut s'est réorganisée récemment. Un Directeur Adjoint Scientifique (DAS) s'occupe préférentiellement des laboratoires de la section 6, un autre DAS de la ceux de la section 7. Chacun des directeurs est accompagné de 3 chargés de mission. Cette organisation est bien opérationnelle, les laboratoires étant souvent à la croisée entre ces sections. Ce découpage n'est donc pas exclusif, les frontières scientifiques étant bien évidemment considérées. Isabelle Fantoni et Matthieu Cord ont rejoint l'institut pour épauler Wilfrid Perruquetti dans la section 7. Stéphane Viallette est également entrant comme chargé de mission côté section 6.

Médailles
La médaille d'argent a été décernée en 2016 à Jean-Marc Jézéquel (IRISA), travaillant sur les sciences du logiciel. Pour les médailles de bronze ont été retenues Aida Todri-Sanial et Meghyn Bienvenu (LIRMM).
Michel Bidoit rappelle le processus pour la sélection des lauréats. La section fait des propositions, l'institut ensuite les retient ou fait d'autres propositions. Enfin, la décision est prise par le collège de direction du CNRS.

Promotions
La promotion CR2 vers CR1 est assez peu sélective. Cette année, toutes les candidatures à une promotion CR1 ont été acceptées.
Le nombre de promouvables DR2 vers DR1 est toujours plus important que le nombre de candidats. Cependant, l'institut ne connait plus la situation de goulot d'étranglement qui existait il y a quelques années, rendant désormais, selon Michel Bidoit, la compétition raisonnable. 10 DR2 ont été promus en section 6 et 7 (cf. proposition de classement des sections). Pour les promotions vers DRCE, le nombre de possibilités est faible. Cependant, 2 DR1 ont été promus cette année DRCE1. Par ailleurs, une personne a également été promue DRCE2.

Délégations
Le nombre de candidats pour une délégation est remonté cette année, mais n'a toujours pas retrouvé les niveaux d'il y a 2 ou 3 ans.

Concours
Le concours chercheurs est en cours.

Pour les ITA, la campagne NOEMI d'hiver est terminée. Cependant, le taux de succès est cette année assez faible (inférieur à 50%). Michel Bidoit rappelle qu'une NOEMI est une étape préalable à l'ouverture d'un concours. Le bilan n'a pas encore été réalisé globalement au CNRS. Il est difficile pour le moment d'interpréter ces résultats.
Le nombre de postes ouverts au concours est important cette année, mais ne permettra pas de pourvoir tous les postes NOEMI non pourvus. Les arbitrages pour la campagne de concours et de la NOEMI de printemps sont en cours.

Les priorités ITA ont été mises sur les laboratoires depuis 4 ans, souvent au détriment des moyens pour les délégations et les services communs (ce qui peut expliquer les difficultés à déployer de nouveaux outils). Michel Bidoit estime donc qu'il existe une grande tension pour les ITA au sein des délégations, les besoins étant devenus au fil des ans très importants.

ERC
Le nombre de candidatures est toujours une préoccupation de l'institut. Malgré les appels de l'institut, peu de directeurs d'unité ont fait de retours à propos de candidats potentiels à l'ERC. Les candidats suivis par la cellule de soutien connaissent un taux de succès plus élevé (25%) que la moyenne. Par ailleurs, la cellule de soutien ne censure pas les candidatures. Julien Gossa rappelle que les collègues sont sur-sollicités par les appels à projets divers et variés. Michel Bidoit répond qu'il faut choisir ses appels, se focalisant sur les projets les plus ambitieux. Julien Gossa pointe le fait que les chercheurs sont sans doute démotivés par les refus reçus de façon consécutive, et ils ne vont naturellement pas soumettre une ERC. Matthieu Latapy pointe le fait qu'une ERC refusée permet également de réfléchir aux défis scientifiques, et fait avancer (pour d'autres appels, pour ses recherches, etc.)
Michel Beaudouin-Lafon explique que d'autres pays proposent de financer nationalement des projets ERC refusés en deuxième phase. Michel Bidoit explique que l'approche actuelle consiste plutôt à encourager à resoumettre. L'institut propose notamment d'octroyer des délégations aux enseignants chercheurs souhaitant soumettre une ERC. Michel Bidoit estime qu'il n'est pas sûr par contre qu'aider avec quelques mois ingénieurs ou 15k€ pourrait réellement servir par rapport à l'ERC. A propos du soutien aux projets refusés, Christian Barillot suggère qu'en associant une aide CNRS à une aide universitaire, cela pourrait permettre d'avancer le projet. Michel Verleysen explique qu'en Belgique, des moyens sont donnés aux soumissionnaires ERC pour démarrer les recherches. Cependant, cela a tendance à "décourager" les soumissions l'année d'après. Andreas Herzig explique que l'Espagne est un cas similaire. Les panels enfin changent tous les 2 ans : une resoumission est donc plus pertinente l'année suivante pour tenir compte de l'effet de mémoire.
Guy Cogniat demande si des domaines sont surreprésentés ou pas dans les soumissions au CNRS. Michel Bidoit répond que les réponses peuvent être sur les sujets fondamentaux ou non, portant sur des domaines assez divers à première vue. Le site https://erc.europa.eu/projects-and-results contient tous les projets financés (l'informatique est essentiellement dans le panel PE-6), ainsi que les statistiques des soumissions. Tout un chacun peut donc explorer les projets portant sur sa discipline.
Cyril Gavoille pense qu'il existe une autocensure en informatique. Christian Barillot pointe le fait que soumettre des ERC permet également de faire "exister" la discipline. Une autocensure est donc dangereuse pour l'informatique.
Cyril Gavoille rappelle que le taux de sélection des ERC commence à être équivalent à celui des ANR : il faudrait donc que les chercheurs se concentrent plutôt sur ce moyen de financement. Michel Bidoit répond que le volume de travail pour la soumission d'une ERC n'est pas non plus similaire, demandant un investissement élevé du soumissionnaire. Cependant, le

financement d'une ERC est suffisamment conséquent pour justifier un tel investissement.

PEPS jeunes chercheurs/ses
L'institut a reçu de nombreuses propositions cette année. Cependant, le taux de succès doit toujours rester élevé pour ce type d'appel. 250k€ ont été alloués à cette action (davantage que ce qui avait été initialement prévu pour maintenir un taux de succès élevé). Michel Bidoit rappelle qu'un même projet ne doit pas être resoumis (en changeant juste le porteur). Il s'agit d'un problème déontologique grave.
Serge Torres rappelle que pour certains laboratoires, la mise en commun des financements fait que des projets comme les PEPS peuvent être ponctionnés localement (pour la remise en commun). Serge Torres demande à ce que le CNRS parle d'une seule voix aux universités locales. Michel Bidoit répond qu'il s'agit d'un problème lyonnais assez particulier, traité donc indépendamment.
La sélection était prévue pour fin janvier, mais le processus a pris un peu de retard. Les notifications vont bientôt arriver (probablement cette semaine). En effet, les règles comptables de gestion de budget ont changé (GBCP), obligeant à une évolution des outils, et donc impactant l'appel JCJC.

Responsabilités collectives
Le métier de DU est compliqué, et l'institut insiste auprès des sections sur la prise en compte des responsabilités collectives dans les promotions.

Gestion des UMR et partage des responsabilités dans la gestion des unités
L'institut est très préoccupé par les UMR qu'il a en commun avec certaines écoles d'ingénieurs. En effet, certaines de ces écoles ne souhaitent pas s'impliquer pleinement dans les UMR, préférant financer directement les seules équipes dans lesquelles sont impliqués leurs enseignants-chercheurs. L'institut a notamment eu une discussion avec Telecom-ParisTech sur le financement des unités conjointes. Le Laboratoire Traitement et Communication de l'Information (LTCI) a en particulier été transformé en FRE en janvier 2016. Ce changement a été décidé pour plusieurs raisons, dont en particulier l'absence de dotation de la tutelle TPT à l'UMR. Michel Bidoit rappelle que 18 chercheurs CNRS travaillent notamment au sein du LTCI.
Il est difficile actuellement de faire un pronostic sur l'avenir de ce problème. Michel Bidoit rappelle qu'une UMR n'est pas un label donné à un laboratoire, et que le CNRS n'est pas une agence de moyens.
D'autres écoles que Mines-Télécom adoptent également un comportement similaire, rendant le problème aigu. Michel Bidoit rappelle néanmoins que ce comportement est très spécifique, et de nombreuses autres écoles continuent de fonctionner normalement avec les UMR. Dans ce contexte, le rapport Attali sur l'avenir de l'Ecole Polytechnique a réactivé l'acuité du problème.
Serge Torres est inquiet de ce comportement qui pourrait avoir tendance à se généraliser, les évènements récents (ministère de la défense, de l'économie, etc.) montrant que le sujet est d'actualité.
Michel Bidoit rappelle qu'il essaie de gérer ces divergences d'opinion tout en limitant le plus possible l'impact sur les personnels chercheurs, enseignants, et ingénieurs. Il est nécessaire de garder les conditions pour qu'ils puissent continuer à accomplir leurs tâches le mieux possible. Les difficultés sont bien avec la cotutelle, et ne concernent absolument pas la qualité de la recherche menée dans ces laboratoires.

Sections et Concours chercheurs

Frédérique Bassino (section 6) et Michèle Basseville feront un compte-rendu lors du prochain CSI, lorsque le concours sera terminé.

Point statutaire : avis sur la composition des jurys d'admission aux concours 2016 des chargés de recherche, pour les sections et CID

Pour la CID, chaque institut remonte des propositions, et le directoire en choisit finalement un sous-ensemble. L'institut fait une proposition, et le CSI ne donne son avis que sur une sous-proposition. Dans un souci de transparence, l'institut présente tout de même l'ensemble des propositions au CSI.
Le CSI doit voter sur la proposition : titulaire Pierre Olivier Amblard, et suppléant Michaël Blum. Il s'agit de personnes déjà présentes dans les jurys d'admissibilité.
Proposition adoptée à l'unanimité

Pour le jury CR-INS2I. IL est naturel que les présidents de section et si possible les secrétaires soient présents aux jurys d'admission.
Proposition adoptée à l'unanimité

Approbation CR du 7 décembre

https://csins2i.irisa.fr/files/2015/02/csi-cnrs-20151207.pdf
Compte-rendu adopté à l'unanimité moins 4 abstentions

Synthèse sur le journée « place des femmes »

https://csins2i.irisa.fr/files/2015/09/CS-INS2I_recommandation_Egalité-hommes-femmes.pdf
Les propositions présentées au précédent CSI ont été reprises intégralement.
Michèle Basseville pointait le fait que les chiffres présentés par Anne Pépin étaient faux. Charlotte répond qu'elle a utilisé les chiffres officiels du bilan social du CNRS (chiffres officiels). L'objectif de parité de 40% est communément acquis.
Plusieurs membres ont réagi à *"l'objectif chiffré"* à afficher. Il est nécessaire maintenant de proposer un chiffre et une échéance. Il s'agit bien d'une recommandation du CSI et non de l'institut en lui même. Michel Bidoit rappelle que la politique de l'institut et les motions du CSI sont deux choses potentiellement disjointes.
Michèle Basseville rappelle le pourcentage des lauréates féminines dans les concours de la section est faible et qu'il lui parait inopportun d'avoir des objectifs de taux de féminisation, qui pourraient créer une sorte de *"carcan"*. Isabelle Queinec répond que les objectifs correspondent à des valeurs moyennées sur une mandature par exemple. Il est également souhaitable de garder au moins le même ratio féminin dans les candidats et dans les lauréats.
Charlotte Truchet demande si la formulation d'"objectif" est pertinente. Serge Torres argumente sur le fait qu'un "objectif souhaité" est déjà peu coercitif. Et qu'il s'agit plus d'une impulsion chiffrée pour un horizon à 2026 (par exemple).
Julien Gossa propose également de chiffrer les objectifs de moyens (et non pas seulement l'objectif de parité). Il s'agit que les DU puissent y lire également des "bonnes pratiques", se sentent impliqués, et travaillent dans le sens de la parité.
Isabelle Queinec pointe le rôle du comité de suivi pour s'emparer du problème. Dans la conférence phare organisée depuis quelques années par son laboratoire (LAAS), aucune invitée n'a été présente.
Michel Verleysen propose que les objectifs chiffrés soient placés à la fin du document, afin de ne justement pas *"bloquer"* la lecture de certaines personnes.
Christian Barillot rappelle que la dynamique est également importante : le ratio de femmes n'est pas croissant, au contraire, dans nos disciplines.

Michel Bidoit expose que les jurys d'admissibilité et d'admission sont complémentaires. Il aimerait que le jury d'admissibilité fasse des classements par paquets, et le jury d'admission ferait ensuite de la politique scientifique. Le jury d'admission respecterait bien-sûr les pré-choix du jury d'admissibilité. Par ailleurs, la parité est respectée pour les médailles d'argent. Les sections doivent maintenant remonter un couple homme/femme pour proposer des lauréats.
Serge Torres remarque que les concours avec un seul poste défavorisent en général les femmes : ce genre de situation doit être évité.
Michel Verleysen explique qu'auprès des étudiantes, il peut être opportun d'expliquer que les sciences de l'information et du vivant sont mêlées. Ainsi, être informaticien permet également de contribuer dans les sciences du vivant : c'est un message qui passe bien auprès du public féminin.
Julien Gossa s'interroge sur l'opportunité d'élargir le débat avec une phrase introductive sur toutes les discriminations. Charlotte Truchet répond que malheureusement, ce texte ne traite que de la parité (les autres discriminations sont également très importantes, mais non abordées ici). Et donc une telle phrase introductive risque d'être justement mal perçue. Christian Barillot répond que la parité est (pour lui) séparée des discriminations religieuses, d'origine, etc car cela concerne le genre et traverse les communautés. Julien Gossa fait remarquer qu'il ne s'agissait bien que d'une proposition, en notant que la composition du CSI présentait par exemple plusieurs disparités.
Andreas Herzig rappelle que les femmes devraient être sollicitées seulement pour les éléments prestigieux (i.e. pas les comités d'organisation).
Proposition adoptée à l'unanimité.

Journeé thématique « Sécurité »: (https://csins2i.irisa.fr/seminaire-thematique-securite-en-sciences-de-linformation/)

Guy Gogniat
introduction de la session et rappel des conclusions de la session du 13 décembre 2013

Cette session fait suite à la session déjà animée lors du CSI du 13 décembre 2013. Le numérique est extrêmement présent : Internet se déploie partout, les ressources deviennent de plus en plus virtualisées, etc. Nous avons des enjeux à la fois de sécurité et de sûreté. La sûreté de fonctionnement correspond à des méthodes et outils pour prévoir le bon fonctionnement et maitriser les défaillances. En sécurité, une entité intelligente peut s'adapter et contourner les défauts.
Le groupe a décidé d'avoir des présentations scientifiques très larges sur la sécurité. Michèle Basseville rajoute qu'il manque les termes de détection et de diagnostic. Par ailleurs, les systèmes peuvent également fonctionner en mode dégradé si une faute est détectée. En digression, Michèle Basseville déplore que lors du découpage des deux sections, certains domaines se trouvent à la croisée et donc non clairement identifiés dans l'une ou l'autre des sections. Michel Bidoit répond que naturellement, certains domaines se trouvent dans les deux sections, mais que cela ne leur porte pas préjudice, chaque section pouvant revendiquer un même sujet, ce qui est actuellement le cas.

Jean-Marc Jézéquel (IRISA)
Jean-Marc Jézéquel présente un panorama des recherches dans le domaine de la cyber sécurité réalisée dans le cadre du Pôle d'Excellence Cyber. La DGA possède un centre de recherche important à Rennes : il s'agit de travailler en commun sur les points qui intéressent à la fois les applications civiles et militaires. La multidisciplinarité est la loi dans la recherche en sécurité

(SHS, mathématiques, physique, réseau, informatique, etc.) Un chercheur est donc plutôt spécialiste d'un domaine, appliqué au domaine de la sécurité.
Le pôle d'excellence comprend :

- 5 laboratoires (électronique, informatique, automatique, mathématiques, télécoms)
- le ministère de la défense (Saint Cyr, école des transmissions, DGA, etc.)

Les activités actuellement développées au sein du pôle sont :

- la cryptanalyse par canal auxiliaire
- la potection des couches basses (OS, etc.)
- la détection d'intrusion réseau
- le raisonnement par automatisme
- la vérification de code
- la visualisation de la sécurité
- le cloud, le web tracking and fingerprinting
- la protection de la vie privée et la protection des données
- la conception et le pilotage de drones de surveillance
- l'Internet des Objets

L'IODE (laboratoire de SHS spécialisé en droit) se focalise par exemple sur les aspects législatifs en sécurité, montrant si besoin est l'interdisciplinarité nécessaire dans ce domaine. Des outils permettent de financer les équipes dans le domaine. Ainsi, un financement spécifique (région Bretagne et ministère de la défense) permet au LHS-PEC de fonctionner. Le club recherche organise par ailleurs un certain nombre de séminaires pour fédérer les équipes. Une masse critique régionale existe, permettant d'être un acteur clé dans le domaine. Andreas Herzig demande si l'économie rentre dans le domaine et si des acteurs sont identifiés. Jean-Marc Jézéquel répond que le CREM est notamment identifié, et que l'économie fait bien partie du spectre scientifique visé (au moins civil). Philippe Lamarre demande quelles interfaces existent entre le droit et la sécurité. Jean-Marc Jézéquel répond que par exemple pour le pistage sur la vie privée, des juristes et des informaticiens discutent pour contribuer au domaine. Dans un autre domaine, les drones peuvent être utilisés pour de la cyber-surveillance : comment gérer les autorisations et sévir si les lois ne sont pas respectées.
Michel Beaudouin Lafon explique que la durée de 20 à 30 ans entre l'idée et le produit est commune en informatique.
Christian Barillot demande si un acteur en France (ex: renater) s'occupe de la gestion centralisée des mots de passe (et non pas sur un cloud à l'étranger). Jean-Marc Jézéquel répond que c'est une préoccupation de l'Etat français de proposer de tels services hébergés en France. Charlotte Truchet demande comment on teste de façon globale toute la chaine (du matériel à l'utilisateur). Jean-Marc Jézéquel répond que c'est un thème de recherche encore en cours. A sa connaissance, il n'existe pas encore d'approche holistique regardant l'ensemble des points. Jean-Marc Jézéquel cite un résultat d'une conférence récente : des dispositifs physiques non reproductibles sont produits par l'industrie (le constructeur n'est pas capable de reproduire le même équipement pour garantir leur unicité). Puisqu'on ne peut pas reproduire le modèle physique, il *suffit* de le simuler : en apprenant les réponses du vrai système (machine learning), on est capable avec une certaine probabilité de bien répondre en se faisant passer pour le système étudié. Souvent, exposer les hypothèses de départ permet aux hackers de trouver quelles hypothèses violer pour rendre le système défaillant.

Jean-Yves Marion (LORIA)

Enjeux et avancées dans le domaine de la virologie
Pourquoi la virologie constitue-elle un domaine à part ? Qu'y a-t-il derrière ? Fred Cohen a le premier défini la notion de virus dans sa thèse encadrée par Leonard Adleman, en utilisant des machines de Turing.
Un logiciel malveillant est un logiciel inséré dans un système compromettant son comportement (disponibilité, confidentialité, intégrité). La thèse de Eric Freyssinet fournit une thèse non technique définissant bien les cas d'usage.
La cybercriminalité est massive (rançon, etc.) et rentable (emails, cartes de crédit, passeports, etc.) Elle touche l'union européenne, mais également les banquiers. Il existe cependant actuellement peu de vulnérabilités zéro-day.
Actuellement, quels sont les domaines étudiés ?

- équipements mobiles et IoT
    - pour Airbus, de nombreuses informations arrivent (plan de vol, etc.) Chaque objet offre une surface d'attaque.
    - healthcare : pompes à insuline, etc.
    - réseaux (routeurs de coeur)
- les menaces web
- médias sociaux
- attaques ciblées
    - Regin qui exploite l'architecture SOA : 8 mois ont été requis pour l'analyser. Les modules sont chargés au fur et à mesure des besoins du logiciel.
    - Dragon Fly : espionnage sur les systèmes électriques (en visant de petits fournisseurs)
- vol de données et vie privée
- cyber-criminalité

Prendre le contrôle d'un système consiste à exploiter une vulnérabilité (buffer overflow, injection SQL/code). Le social engineering peut également permetttre d'entrer dans un système. Une attaque peut s'appliquer à n'importe laquelle des *surfaces* du système.
Les directions actuelles de recherche peuvent comprendre :

- Défense (IDS) : comment surveiller / détecter / classifier ?
    - Qu'est ce qu'un code malveillant ? Que fait un logiciel donné (géo-localisation, envoi d'emails, etc.) ?
- Les attaques posent des problèmes légaux : les botnets sont difficiles à désactiver. Cependant, comment les attaquer sans violer la loi ?
- Prévention : audit des équipements présents et des vulnérabilités logicielles (i.e. détecter un bug, exploitable pour une attaque).
    - Système de test pour détecter une faute
- Protéger le système : virtualisation, cloisonnement
- Aspects juridique et législatifs, éducationnels

Actuellement, pour détecter un code malveillant, on collecte des signatures et on inspecte un système pour les chercher. Eventuellement, le model-checking permet également de rechercher les vulnérabilités. Cependant, actuellement, l'auto-modification est très compliquée à déchiffrer. Les fonctions sont déchiffrées à la volée quand le programme en a besoin. Une analyse dynamique est donc nécessaire afin de pouvoir le détecter. On construit une vue abstraite à partir de traces d'exécution (une signature), et à travers une analyse statique, on essaie de le classifier en attaque ou non.

3 grands défis :

- Offuscation : comment enlever les protections et comprendre ce qu'ils font réellement ?
- Passage à l'échelle : analyse de logs, de traces d'exécution, etc.
    - 6M de malware au LHS (400M détenus par google)
- Extraction automatique de l'information utile : étude des dégâts, des origines d'un logiciel
    - des logiciels peuvent avoir des visuels différents, mais partageant le même code : peut-être que des groupes différents exploitent la même plateforme ?

La communauté est très diverse :

- quelques chercheurs académiques
- beaucoup d'entreprises (grands groupes et petites entreprises répondant à des incidents)
- conférences académiques, ou de hackers
- séminaires Dagstuhl
- ANR Défi 9 sécurité globale, H2020
- Les LHS de Rennes et Nancy

Matthieu Latapy demande si des hackers guidés par le ludique sont toujours présents parmi les hackers. Jean-Yves Marion explique que les hackers passionnés sont très peu nombreux, et que le critère financier est prépondérant. Véronique Cortier cite aussi les activistes, et Michel Bidoit complète avec les services de l'Etat. Jean-Yves Marion insiste sur la complexité des logiciels d'espionnage. Il est très difficile de les détecter. Il cite une attaque sur les dissidents tibétains, suivie par des arrestations. La variabilité des attaques (nature, cible) est très large. Les erreurs de la part des hackers sont par ailleurs maintenant peu fréquentes.
Serge Torres demande si des questions scientifiques particulières, propres au domaine, ont émergé. Jean-Yves Marion explique que les questions levées existent déjà : il est par contre nécessaire de les adapter au domaine. Concernant les systèmes d'exploitation, isoler les applications est un domaine créé par le besoin en termes de sécurisation. Les programmes auto-modifiant sont maintenant utilisés également par des éditeurs logiciels pour protéger leur propriété intellectuelle. Cependant, le domaine des codes auto-modifiant est encore vierge : il n'existe pas d'ouvrage de référence par exemple.
Jean-Yves Marion rappelle que désassembler du code n'est pas un problème décidable (le saut dépend de la valeur d'un registre). Or, il n'est pas possible de regarder les valeurs d'une pile de façon statique.
Philippe Lamarre demande si l'isolation est bien garantie dans les navigateurs modernes. Jean-Yves Marion répond que le nombre d'attaques pour les navigateurs est un chiffre parlant. Jean-Yves Marion cite un article de Ken Thompson (prix Turing) expliquant comment concevoir un code malveillant attaquant le compilateur de C afin d'infecter n'importe quel programme compilé par ce biais.

David Monniaux (VERIMAG)
Enjeux et avancée dans le domaine de la vérification formelle - application à la sécurité

David Monniaux s'intéresse à la vérification formelle. Etudier un code d'Airbus (par exemple) permet d'étudier le comportement d'un code dans un environnement précis et connu. Dans la cryptographie, il est possible de faire des erreurs dans l'algorithme, mais également

dans le protocole (ex : l'attaquant contrôle le réseau, l'attaque de l'homme du milieu, etc.) Il s'agit donc de raisonner sur les protocoles pour éviter de tels problèmes. On fait abstraction des fonctions cryptographiques grâce à des modélisations mathématiques (hachage, etc.). D'autres méthodes tentent donc de prouver que casser le protocole revient presque (à epsilon près) à casser les primitives cryptographiques. Des outils comme Cryptoverif sont apparus. Par contre, la preuve assistée en utilisant par exemple Coq reste compliquée.

La fuite d'information consiste à ce qu'une donnée secrète soit divulguée par le programme. Une approche simpliste consiste à pister les dépendances et vérifier si une information va vers l'extérieur, dépendant des données secrètes. On peut également s'intéresser à l'attaque aux canaux cachés (ex : inférer des informations sur la clé secrète en fonction de l'énergie consommée). Les caches étant partagés par plusieurs applications, peut-on en tant qu'attaquant apprendre des informations supplémentaires ? On peut exploiter une application tierce pouvant communiquer avec une application théoriquement isolée, permettant à cette application isolée d'envoyer des informations. David Monniaux cite le problème du buffer overflow dans un code C.

Il existe trois approches face à ces problèmes de sécurité : langages à mémoire sûre, JIT, et approches formelles. Certains éditeurs n'utilisent pas de système d'exploitation et s'interdisent d'utiliser certaines fonctions pour simplifier la détection de bugs. Clairement, un équipement personnel (smartphone) représente un défi très différent. Comment sécuriser un navigateur qui s'adapte à la volée au code ?
Patrice Godefroid (Microsoft) a proposé de désassembler du code, et de regarder à l'exécution les instructions dépendant de données externes. La programmation sous contrainte permet ensuite d'étudier le comportement du code.

Isabelle Queinec demande si une collaboration plus étroite entre les différentes étapes ne serait pas pertinente. David Monniaux explique que chaque domaine travaille séparément (commande d'automatisme versus conception du système l'intégrant). Par ailleurs, les personnes en charge des tests ne devraient pas être en contact trop étroit avec les concepteurs. Cependant, il est effectivement compliqué d'analyser un code non compris.

Discussion
Christian Barillot demande quels sont les grands sujets à explorer dans le domaine de la sécurité, et quels sont les points forts actuels en France : sur quels points le CNRS peut-il jouer un rôle ? Guy Cogniat complète en disant que de nombreux GDR s'intéressent à la sécurité. Jean-Marc Jézéquel pointe le fait que les intérêts sont divergents entre académiques et industriels. Andreas Herzig complète en pointant le fait que l'interdisciplinarité est un sujet peu étudié par les industriels. La confiance en SHS est plus large qu'en informatique : l'humain doit également avoir confiance dans le système, les preuves ne sont sans doute pas suffisantes. David Monniaux pointe le fait que les industriels ont aussi peu confiance dans la recherche académique : ils cherchent souvent des solutions clé en main.
Valérie Berthe demande s'il existe des actions de la part de la mission interdisciplinarité sur la sécurité. Michel Bidoit répond que le focus a été donné sur l'appel à projet en sécurité, mais que ce n'est pas encore au programme de la mission. L'INS2I souhaiterait également développer les interactions avec les SHS. Cependant, l'institut a besoin d'identifier au préalable les initiatives existantes dans le domaine et les structurer.

Charlotte Truchet demande comment identifier les chercheurs travaillant en sécurité. Michel Bidoit explique qu'il existe plusieurs initiatives, avec notamment des chercheurs dont les

applications *peuvent* toucher le domaine. La phase actuelle de construction d'un GDR en sécurité demande du temps, mais permettra à terme de structurer la communauté. La sécurité attire l'attention, et représente un domaine porteur.

Christian Barillot expose sa compréhension du domaine, avec une démarche de type parade : identification des problèmes, et résolution. Un travail de prospection est-il possible ? La nature du risque évolue : comment s'y préparer ? Jean-Yves Marion répond qu'il avait tenté de présenter cette approche : comment rendre les solutions sûres ? Côté défense, il s'agit d'augmenter la robustesse des mécanismes existant. Il faut complexifier les attaques, les rendre plus coûteuses. Jean-Marc Jézéquel confirme que fondamentalement, il est impossible de prévoir ce que fera la machine en face. La majorité des attaques sont simples (exploitant des erreurs majeures). Il est nécessaire de solutionner déjà ces problèmes. Dans l'Internet des Objets, l'accès doit être sécurisé.

Matthieu Latapy demande si les aspects relatifs aux forces de l'ordre sont également regardés : Jean-Yves Marion et Jean-Marc Jézéquel répondent que oui.

Préparation des futures journées thématiques

- Journée Ethique du 9 mai, coordonnée par Isabelle Tellier
    - Intervenants ayant accepté : Max Dauchet (responsable du comité d'éthique d'Allistène, CERNA), Raja Chatila (membre du Cerna, robotique), Karen Fort (MdC Paris IV), Herve Chneiweiss (président du comité d'éthique Inserm)
    - Isabelle Queinnec demande si une introduction peut aborder les différences entre éthique / morale / juridique. Isabelle Tellier répond qu'elle demandera aux orateurs d'aborder ce sujet.
    - Valérie Berthe cite la relation entre chercheurs et maisons d'édition comme facette du problème de l'éthique.
    - Julien Gossa pointe le lien entre pression d'évaluation et éthique. Michel Bidoit rappelle que les chercheurs sont évalués chaque année. Michèle Basseville comprend l'inquiétude des enseignants-chercheurs sur le lien entre évaluation et modulation de service. Mais une évaluation doit être faite par les pairs, en terme de conseil et non de sanction.
- Autres idées de journées :
    - Arts et sciences de l'information (liens objets technologiques et art)
    - Internet des objets & réseaux de capteurs (touchant aux domaines de l'INS2I)
        - Inbar Fijalkow, Fabrice Théoleyre
- Discussion concernant les propositions d'*années thématiques prioritaires* :
    - Relations avec l'économie (théorie des jeux)
    - Sur les interfaces avec les autres sciences
        - Matthieu Latapy cite les philosophes et historiens de l'informatique, présents dans la CID
    - Cyber, Physical and Human Systems : symbiose hommes/machines (prothèses, exo-squelettes), humains comme opérateurs (aéronautique, chirurgie), agents dans les systèmes multi-agents (trafic, Usine 4.0), humains comme éléments dans les systèmes contrôlés (bâtiments intelligents) : sûreté, sécurité, politique publique

USAGE INTERNE AU CSI - NON PUBLIC

Concours Chercheurs

Au concours DR2, la section 6 a un peu moins de candidats que les années précédentes (une quarantaine en 2015). L'autocensure est élevée dans la section, un faible ratio de promouvables déposant un dossier.

Le concours CR1 (2 postes) a attiré de nombreuses candidatures (comme chaque année). Le nombre de candidats CR2 a de nouveau baissé cette année.