Séminaire thématique « Sécurité en sciences de l'information »

Conseil Scientifique d'Institut de l'INS2I

Fiche de synthèse – journée du 29 Février 2016

Rédigée par le groupe de travail « Sécurité en sciences de l'information » : Guy Gogniat (animateur), Véronique Cortier, Julien Gossa, Isabelle Queinnec

Contributions, concernant les éléments de prospective, du GDR ISIS (avec le concours de William Puech, Cédric Demonceaux et Mari Kobayashi), du GDR SoC-SiP (avec le concours des équipes du Lab-STICC, du LCIS, du LIRMM, du Laboratoire Hubert Curien, du TIMA, de l'IRISA, du LTCI et du département Systèmes et Architectures Sécurisées), du GDR MaDISC (avec le concours de Benjamin Nguyen) et du GDR MACS (avec le concours d'Isabelle Queinnec).

Executive summary

Le domaine de la sécurité en sciences de l'information est un domaine pluridisciplinaire, depuis la physique jusqu'au traitement de l'information. Cette dimension pluridisciplinaire nécessite une organisation de la recherche concertée afin de pouvoir apporter des réponses complémentaires aux enjeux de sécurité. Les questions juridiques et sociologiques sont également essentielles et doivent être prises en compte. La question de l'acceptabilité des solutions technologiques par les utilisateurs ne doit pas être oubliée. Pour appréhender ces différents points, le CSI a organisé le 29 février 2016 une journée de réflexion autour de ce thème. Suite à cette journée, le CSI recommande 8 propositions à l'INS2I :

Proposition 1 : Suivre les actions et le développement du pôle d'excellence cyber (PEC) afin de voir comment ce dernier contribue aux évolutions de ce domaine.

Proposition 2 : Promouvoir les actions visant à rapprocher les acteurs académiques et industriels autour du développement de prototypes afin d'encourager les transferts technologiques.

Proposition 3 : Recenser les plateformes d'évaluation présentes dans les laboratoires de l'INS2I et veiller, lorsque cela est pertinent, à leur mutualisation afin de permettre aux chercheurs et industriels d'avoir accès à ce type d'infrastructure.

Proposition 4 : Encourager davantage les actions du type écoles thématiques et rencontres entre les doctorants et les entreprises.

Proposition 5 : La mise en place du pré-GDR « Sécurité » par l'INS2I est une action marquante qui doit être soutenue, promue et étendue.

Proposition 6 : Mettre en place une programmation pluriannuelle d'appel à projet PEPS dans le domaine de la « sécurité » et faire une cartographie des domaines couverts par les propositions afin d'identifier les éventuels points de faiblesse.

Proposition 7 : Mettre en place un défi dans le domaine de la « sécurité » afin de promouvoir les collaborations interdisciplinaires.

Proposition 8 : Développer un document visant à faire la promotion des chercheurs de l'INS2I dans le domaine de la « sécurité ».

Le CSI propose également des éléments de prospectives basés sur des échanges avec plusieurs GDR traitant de la sécurité en sciences de l'information. Ainsi, les enjeux liés à la protection de la vie privée et des données multimédia y sont présentés. Les questions scientifiques liées à la vidéosurveillance et à la biométrie y sont également abordées. La protection de la couche physique dans le contexte des télécommunications et les défis liés à la sécurité des composants logiciels et matériels sont également présentés.

1. Introduction

Depuis près de 20 ans, on assiste à un bouleversement considérable des Sciences et Technologies de l'Information et de la Communication (STIC) avec des éléments marquants comme l'accroissement massif des systèmes embarqués et des objets communicants, la domination de l'Internet, la dématérialisation des systèmes/infrastructures de calcul et de communication, la multiplication des *smart devices*, la montée en puissance des systèmes de production de biens manufacturés et de services qui sont de plus en plus connectés[1]. Ces modifications profondes des technologies et de leurs usages ont un impact majeur sur nos sociétés qui sont chaque jour davantage consommatrices de technologie, d'information et de communication. Au-delà des progrès et du confort que ces bouleversements procurent, ils soulèvent de nombreuses questions, notamment dans le domaine de la sécurité en sciences de l'information. En effet, il devient nécessaire d'introduire la sécurité comme pivot du développement de nos technologies et de nos échanges d'information en adressant notamment les questions suivantes : Comment concevoir des systèmes numériques de confiance ? Comment garantir la confiance de leur implantation et de leur contrôle ? Comment anticiper les risques et les vulnérabilités ? Comment définir des modèles et des politiques de sécurité ? Comment avoir l'assurance de la protection des biens et des services ? Ou encore comment garantir la sécurité par conception ?

Ces enjeux touchent tous les domaines de la société du fait du caractère ubiquitaire des technologies de l'information et de la communication. On peut par exemple citer les domaines du transport (automobile, aéronautique, ferroviaire...), de l'énergie (gaz, pétrole, nucléaire...), de la santé (biotechnologies...), des média (images, vidéo, musique...), de l'industrie (SCADA...), de la distribution de biens (eaux...), des objets connectés (téléphonie, internet...), de la finance (banques…). Un des enjeux est que pour plusieurs de ces domaines il n'existe pas de culture de sécurité et que les menaces évoluent très vite avec des conséquences potentiellement dramatiques du point du vue humain et financier. Il y a donc une forme d'urgence à permettre à l'ensemble des acteurs économiques et industriels de monter en compétence dans le domaine de la sécurité en sciences de l'information afin de leur permettre de répondre aux attentes et aux exigences des marchés et des utilisateurs.

On perçoit bien la complexité sous-jacente en termes de sécurité du fait de l'hétérogénéité des systèmes, des besoins et des utilisateurs. Les enjeux en sécurité sont donc très larges et les réponses à apporter nombreuses et caractérisées par une très forte interdisciplinarité. Parmi ces enjeux scientifiques, on peut citer : la cryptographie, les méthodes formelles et les propriétés de sécurité, les services de sécurité, la détection d'intrusion, la détection d'anomalie, la sécurité du matériel, la sécurité des systèmes, la sécurité des réseaux, la sécurité des données et des systèmes de sauvegardes, la sécurité des applications et des logiciels, la sécurité des systèmes d'exploitation, la sécurité applicative, le développement sécurisé, la virtualisation sécurisée, l'authentification, la traçabilité et la journalisation, la sécurité et la protection de la vie privée des humains et de la société…

L'INS2I est au cœur de ces préoccupations et rassemble de nombreuses équipes de recherche qui font référence aux niveaux national et international. Aussi, afin de mieux appréhender la masse critique et les expertises présentes en France, le CSI de l'INS2I s'était déjà emparé de cette problématique à travers l'organisation d'un séminaire thématique « Sécurité », le 9 Décembre 2013. Ce dernier, animé par Hubert Comon-Lundh (ENS Cachan), avait accueilli les intervenants suivants : Loïc Duflot (Agence Nationale de la Sécurité des Systèmes d'Information), David Pointcheval (CNRS, INRIA, ENS Paris) et Véronique Cortier (LORIA, CNRS, Nancy). Les conclusions du CSI de l'INS2I étaient les suivantes : domaine de recherche en expansion, nécessité d'une aide au mouvement thématique en soutenant en priorité des projets exploratoires, nécessité d'un GDR « Sécurité », nécessité de faire évoluer les formations initiales, et d'adresser la question difficile du transfert industriel dans ce domaine. Comme précisé dans la suite de cette fiche de synthèse, certaines de ces recommandations ont été retenues et mises en place depuis 2015 par l'INS2I.

[1] Agence Nationale pour la Recherche Sciences et Technologies de l'Information et de la Communication

Le thème de la sécurité en sciences de l'information soulevant de nombreux enjeux et les évolutions dans ce domaine étant rapides, le CSI de l'INS2I a souhaité presque 2 ans plus tard, le 29 février 2016, s'emparer de nouveau de cette question en organisant une nouvelle journée d'auditions et de réflexion autour de ce thème. Cette journée n'a pas abordé toutes les problématiques, tant le périmètre du domaine de la sécurité en sciences de l'information est large, elle a néanmoins essayé d'éclairer une initiative intéressante au niveau national à travers la mise en place du Pôle d'Excellence Cyber (PEC) et d'adresser des problématiques spécifiques dans le domaine de la virologie et de la preuve formelle. Les présentations et les réflexions ont donc porté sur ces questions à travers les interventions des invités suivants :

Jean-Marc Jézéquel, IRISA « Panorama des recherches dans le domaine de la cybersécurité notamment dans le cadre du Pôle d'Excellence Cyber »

Jean-Yves Marion, LORIA « Enjeux et avancées dans le domaine de la virologie »

David Monniaux, VERIMAG « Enjeux et avancées dans le domaine de la vérification formelle - application à la sécurité »

2. Bilan des réflexions et propositions d'actions

Le domaine de la sécurité en sciences de l'information est par essence un domaine pluridisciplinaire, depuis la physique jusqu'au traitement de l'information. En effet, la sécurité d'un système se mesure à travers son maillon le plus faible. Il est donc essentiel d'appréhender la question de la sécurité à travers la mise en place d'une chaîne de confiance (sécurité de bout en bout). Cette dimension pluridisciplinaire nécessite une organisation de la recherche concertée afin de pouvoir apporter des réponses complémentaires aux enjeux de sécurité. Les questions juridiques et sociologiques sont également essentielles et doivent être prises en compte. La question de l'acceptabilité des solutions technologiques par les utilisateurs doit également être appréhendée. La question de la formation représente également un enjeu et cela depuis les études secondaires afin de permettre aux utilisateurs d'être davantage éclairés sur ces questions jusqu'aux études supérieures afin de former les futurs experts du domaine.

Proposition 1 : Le pôle d'excellence cyber (PEC), qui adresse les dimensions recherche, formation, transfert technologique, représente une initiative intéressante qui s'inscrit dans cette démarche. Il rassemble de nombreux acteurs académiques et industriels. Le CSI recommande à l'INS2I de suivre ses actions et son développement afin de voir comment ce dernier contribue aux évolutions de ce domaine.

La complexité des systèmes est telle qu'il est important de disposer d'une masse critique suffisante afin de pouvoir explorer en profondeur les réponses scientifiques et technologiques aux enjeux de sécurité. Cette masse critique est indispensable afin de passer du concept théorique à une validation expérimentale sur des systèmes représentatifs de systèmes réels. En effet, il est essentiel de tester l'ensemble de la chaîne de protection depuis l'utilisateur jusqu'au système et cela au sein d'environnement confinés (notion de bac à sable) afin de contrôler les expérimentations. De telles approches de validation nécessitent des ressources humaines expertes qui permettent de maintenir et de développer les plateformes d'évaluation. La question du soutien en ressources humaines est un point important pour aboutir à des prototypes plus avancés et probablement plus attractifs pour les industriels. Le développement de démonstrateurs représentatifs des systèmes réels est donc un enjeu. Certains industriels français sont des acteurs économiques majeurs du domaine, aussi il est important d'établir de façon plus systématique des passerelles entre les chercheurs et les industriels. En effet, la question du transfert industriel reste complexe dans ce domaine et ce point doit être approfondi afin de créer une plus forte synergie entre recherches exploratoires et pré-compétitives.

Proposition 2 : Le CSI recommande à l'INS2I de promouvoir des actions visant à rapprocher les acteurs académiques et industriels autour du développement de prototypes afin d'encourager les transferts technologiques.

Proposition 3 : Le CSI recommande à l'INS2I de recenser les plateformes d'évaluation présentes dans ses laboratoires et veiller, lorsque cela est pertinent, à leur mutualisation afin de permettre aux chercheurs et industriels d'avoir accès à ce type d'infrastructure.

Les initiatives récentes telles que l'école d'été « Cyber in Bretagne[2] » organisée conjointement par le pré-GDR « Sécurité » (présenté ci-après) et le Pôle d'Excellence Cyber (PEC) en juillet 2016 ainsi que la rencontres entreprises doctorants sécurité (REDOCS[3]) qui se tiendra en octobre 2016 où des doctorants des domaines de la sécurité informatique s'associeront sous forme de groupes afin de répondre à des problèmes posés par des entreprises sont à saluer et doivent être davantage encouragées.

Proposition 4 : Le CSI recommande à l'INS2I d'encourager davantage d'actions du type écoles thématiques et rencontres entre les doctorants et les entreprises.

La communauté adressant les questions de sécurité en sciences de l'information est relativement large et aujourd'hui présente dans différents GDR ce qui ne facilite pas toujours leurs interactions. On peut notamment citer les GDR suivants :

- GDR Informatique-Mathématique (groupe de travail Codage et Cryptographie) ;
- GDR Information, Signal, Image et ViSion, (thème Télécommunications : compression, protection, transmission, axe compression et protection) ;
- GDR System on Chip – System in Package (axe Confiance Matérielle, groupe thématique sécurité numérique) ;
- GDR Réseaux et Systèmes Distribués ;
- GDR Génie de la Programmation et du Logiciel (groupe Formalismes et Outils pour la Vérification et la Validation) ;
- GDR Modélisation Analyse et Conduite de Systèmes dynamiques ;
- GDR Masses de Données, Informations et Connaissances en Sciences.

La mise en place du pré-GDR « Sécurité[4] » par l'INS2I est donc une initiative très importante qui devrait permettre à terme de décloisonner la communauté « sécurité » française. En effet, comme indiqué dans la feuille de route du pré-GDR « Sécurité », ce dernier doit permettre de rassembler une communauté scientifique unifiée autour de tous les aspects de la sécurité informatique, tels que la cryptologie et le codage, la vérification, les questions de vie privée, l'étude des vulnérabilités et des mécanismes de protection, la sécurité matérielle, etc. Ce GDR doit permettre de mieux connaitre les acteurs académiques et industriels et rendre plus visible leurs complémentarités afin d'aboutir à une cartographie des expertises au sein de la communauté française. Il doit aussi être un outil de veille et de promotion afin de rendre plus visible à l'international l'expertise française dans ce domaine.

Proposition 5 : La mise en place du pré-GDR « Sécurité » par l'INS2I est une action marquante qui doit être soutenue, connue et étendue.

Afin de favoriser les interactions entre les chercheurs de l'INS2I, la mise en place d'appel à projet sur le thème de la « sécurité » correspond à un outil d'animation et d'accompagnement scientifique important. L'appel PEPS INS2I 2016 « Sécurité Informatique et des Systèmes Cyber-physiques » est une initiative qui va dans ce sens. Il serait également pertinent d'évaluer les domaines couverts par les propositions reçues afin de voir si certains domaines spécifiques, qui sont jugés stratégiques, n'en sont pas absents. Une programmation pluriannuelle de projets sur ce thème devrait être encouragée.

[2] https://project.inria.fr/cyberinbretagne/fr/
[3] http://confiance-numerique.clermont-universite.fr/redocs2016/
[4] http://gdr-securite.irisa.fr/

Proposition 6 : Le CSI recommande à l'INS2I de mettre en place une programmation pluriannuelle d'appel à projet PEPS dans le domaine de la « sécurité » et de faire une cartographie des domaines couverts par les propositions afin d'identifier les éventuels points de faiblesse.

La sécurité est une approche fortement interdisciplinaire, aussi il est essentiel d'associer la mission interdisciplinarité du CNRS aux actions en cours à travers par exemple la mise en place d'un défi dans ce domaine afin de mettre l'humain et la société au cœur des actions de recherche et de fédérer les différentes expertises au-delà des sciences de l'information.

Proposition 7 : Le CSI recommande à l'INS2I de mettre en place un défi dans le domaine de la « sécurité » afin de promouvoir les collaborations interdisciplinaires.

Afin de renforcer la visibilité des chercheurs dans le domaine de la « sécurité » il serait intéressant de recenser les chercheurs présents dans les laboratoires de l'INS2I ayant obtenu un ERC ou étant membre de l'IUF.

Proposition 8 : Le CSI recommande à l'INS2I de développer un document visant à faire la promotion de ses chercheurs dans le domaine de la « sécurité ».

3. Eléments de prospective

Sans avoir la prétention d'être exhaustive, cette dernière partie de la fiche de synthèse met en évidence plusieurs thématiques de recherche présentant des verrous scientifiques à lever.

La protection de la vie privée (PVP) est un thème central à de nombreuses discussions sur la société de nos jours, comme avec la récente loi sur le renseignement en France, les négociations sur le TAFTA (partenariat transatlantique de commerce et d'investissement), le projet de loi pour une République numérique, le règlement européen sur les données personnelles, etc. En effet, dans le monde connecté où nous vivons désormais, des données personnelles toujours plus nombreuses sont générées, souvent à l'insu des personnes concernées. Le traitement de ces données massives conduit à un profilage important des individus.

De nombreux problèmes éthiques, philosophiques et bien entendu juridiques se posent sur le concept de la protection de la vie privée. Il est donc nécessaire d'étudier (i) comment ces problèmes se traduisent en termes de problèmes théoriques fondamentaux, (ii) s'ils peuvent donner lieu à des réalisations informatiques (logiciels de type « Privacy Enhancing Technology » ou PET), (iii) les interactions avec les autres disciplines comme le droit et la sociologie sur les problèmes de PVP. Ce travail doit être mené avec les GDR des disciplines de droit et de sociologie (par exemple le GDR Normes Sciences et Techniques).

Ces problèmes incluent par exemple le contrôle de l'individu sur ces données, à la fois dans leur partage, leur exploitation, ou leur vente, son anonymat, au cours des nombreux traitements que subissent ses données, ou lors de son interaction avec des services numériques, la transparence dans le traitement, l'acquisition ou le transfert des données, la responsabilité (ou « accountability »), ou encore l'équité de la relation entre l'individu et les fournisseurs de services.

En ce qui concerne les traitements, il s'agit bien souvent de techniques d'analyse de données. On parle alors de « Privacy-Preserving Publishing » ou de « Privacy-Preserving Data Mining » (PPDM) lorsqu'on souhaite étudier la prise en compte de la PVP dans ce domaine.

Il est important de renforcer les actions de recherche sur la protection de la vie privée au sein des laboratoires de recherche de l'INS2I en partenariat avec les disciplines de droit et de sociologie.

Les pistes explorées par les équipes travaillant sur la PVP en France sont assez diverses. Elles incluent des approches cryptographiques ou des approches formelles (logique, graphes, preuve) pour proposer des protocoles ou des architectures permettant de garantir des propriétés de PVP, des techniques

d'interrogation de données protégeant la VP, des techniques de calcul sécurisées (cryptographie homomorphe, réseau de confiance ou matériel sécurisé comme présenté dans la suite).

La protection des données multimédia ; notamment comment sécuriser des données visuelles pendant leur transmission, leur archivage et leur visualisation est également une problématique importante. En effet, d'après CISCO, les données visuelles (images, vidéos, objets et scènes 3D) représenteront 80% du trafic Internet mondial en 2019. Avec le tout numérique, il devient de plus en plus facile de copier des données, de les visualiser sans droit, de se les approprier mais aussi de les falsifier. La sécurité des données visuelles peut être abordée par des aspects insertion de données cachées (tatouage, stéganographie, ...) ou par des aspects cryptographie (chiffrement sélectif, signature perceptuelle, ...). Cela concerne principalement la confidentialité, l'authentification et l'intégrité. Tous ces aspects de sécurisation doivent bien sûr respecter les standards internationaux de compression tels que JPEG ou H264. Il faut aussi adapter les techniques aux nouveaux formats multimédia (HdR, multi-composantes, stéréo, ...). De nouvelles questions voient également le jour comme l'identification et l'authentification d'une image afin de pouvoir être utilisée comme preuve juridique recevable.

Un autre versant consiste à détecter si un message est caché dans une image (stéganalyse) ou si le chiffrement est suffisant (cryptanalyse). Il s'agit de la « sécurité à partir de données visuelles ». Dans ce domaine sont abordées également les problématiques de traçabilité de données visuelles et de détection de falsification tels que des copier-déplacer dans une image ou des copier-coller d'une image vers une autre. Dernièrement il est apparu des aspects phylogénie des images qui consistent à partir d'un ensemble d'images très similaires (récupérées sur des réseaux sociaux par exemple) de retrouver qui est le parent de qui afin de remonter à l'image source. Il existe aussi des méthodes d'identification d'appareil photo numérique à partir d'analyse de bruit et de distorsion contenus dans une image.

La vidéosurveillance et la biométrie correspondent également à des problématiques importantes. Il s'agit d'identifier des personnes pour des accès sécurisés ou analyser des comportements afin de détecter des comportements malveillants. Il s'agit ici de « sécurité des personnes », et non de sécurité des données. La vidéosurveillance amène aux problèmes de reconnaissance de personnes, reconnaissance de gestes, analyse de foules. La reconnaissance de visage basée vision est un sujet très étudié, considéré comme mature et pour lequel on annonce désormais un taux de reconnaissance supérieur à 99%[5]. En revanche, l'analyse de geste et de comportement reste un problème ouvert même si l'arrivée des caméras 3D a permis d'améliorer fortement les résultats. Cette problématique rencontre un grand succès aux niveaux national et international.

A l'échelle plus macroscopique, l'analyse de foule est également un sujet d'étude qui rassemble un nombre important d'acteurs. Dans le cas d'une foule peu dense, les méthodes de détection et de suivi de personnes ont atteint des performances très satisfaisantes même en présence de fortes occultations. Par contre, l'analyse de foule dense reste un problème difficile à résoudre et encore ouvert.

La sécurité de la couche physique est une autre des grandes thématiques actuelles en théorie de l'information. Le principe de la sécurité pour la couche physique est d'exploiter le bruit présent naturellement dans tous les canaux de transmission pour garantir la sécurité inconditionnelle des communications. L'idée repose sur le fait que les signaux interceptés par des écouteurs indésirables subissent généralement une dégradation différente de ceux reçus par les récepteurs légitimes (par exemple, une atténuation différente qui induit un rapport signal-à-bruit différent). Afin d'adresser cette problématique il est nécessaire d'étudier la capacité maximale d'un canal sous contrainte de sécurité. En effet, la théorie de l'information donne une limite fondamentale (théorique) de la capacité maximale d'un système de transmission. L'ajout de l'aspect sécurité (garantir que l'on ne peut rien obtenir comme information à partir d'une séquence d'observation sur un canal) rajoute des contraintes sur la transmission. Sur ces aspects sécurité de la couche physique, la France a des bonnes productions sur

[5] Spreeuwers, L.J. (2015). "Breaking the 99% barrier: optimisation of 3D face recognition". IET Biometrics 4 (3): 169–177

les aspects théoriques, moins sur les aspects pratiques de mise en œuvre sur lesquels beaucoup d'actions doivent encore être menées.

La composante matérielle de la sécurité en sciences de l'information est passée depuis quelques années au premier plan en raison du développement et de l'utilisation intensive des systèmes électroniques embarqués et aujourd'hui du développement de la cybersécurité, de l'internet des objets et des objets connectés. Outre les attaques par analyse de fuites apparues dans les années 90, de nouvelles menaces sur les systèmes électroniques sont apparues récemment du fait d'une filière de conception et de fabrication globalisées au niveau mondial. Les risques associés comprennent l'insertion de matériel malveillant (chevaux de Troie matériels, portes dérobées…), la contrefaçon de circuits intégrés et le vol d'IP (Intellectual Property). D'autre part, les attaques sur le matériel cryptographique évoluent aussi en efficacité, par exemple en couplant l'analyse sur canaux cachés à l'injection de fautes (notamment sur le canal électromagnétique), ou en visant plusieurs points simultanément lors des attaques en fautes. De nombreux verrous scientifiques et technologiques doivent encore être levés dans les prochaines années pour relever le défi de la sécurité matérielle de l'information.

Si les algorithmes standards de chiffrement à clé symétrique ou à clé publique sont toujours au cœur des efforts de recherche et de développement, de nouveaux schémas de chiffrement sont de plus en plus étudiés. C'est notamment le cas du chiffrement authentifié, du chiffrement post-quantique et du chiffrement homomorphe. Ce dernier type de chiffrement est particulièrement intéressant, cependant les réalisations actuellement disponibles ne sont pas utilisables en pratique. Des réalisations efficaces doivent être proposées rapidement par la communauté pour augmenter l'acceptabilité de ces nouveaux schémas. C'est pourquoi, les liens entre les algorithmes, les représentations des données, les architectures matérielles et logicielles et la résistance aux attaques physiques seront aux cœurs des travaux scientifiques en sécurité dans les années à venir.

La complexité et l'hétérogénéité des Systems-On-Chip (SoC) grandissants, des méthodes efficaces pour leur conception et pour l'évaluation de la sécurité des moyens de protection logiciels et matériels doivent être étudiées. Pour cela, il faut disposer d'outils de conception conjointe logicielle-matérielle et de synthèse de haut niveau prenant en compte la sécurité comme une contrainte de conception, ces outils n'existent pas encore. Durant les phases de conception, des outils de vérification holistique formelle de la sécurité portant à la fois sur le logiciel et le matériel sont aussi nécessaires. Le développement de la sécurité par conception reste un objectif fort dans les années à venir avec de nouveaux enjeux comme par exemple la gestion des droits de propriété des IP et des circuits, la surveillance comportementale des systèmes, la résilience des systèmes matériels sensibles, la garantie des fonctions de test, de diagnostic et de débogage sans préjudice sur la sécurité et la proposition de mécanismes sophistiqués d'authentification et d'identification. Le développement de chaines de confiance allant du système au composant est un enjeu fort de la sécurité aujourd'hui. La vérification formelle (multi-niveaux et multi-technologies) de l'ensemble de la chaine de confiance est à développer dans un futur proche (notion de « sécurité prouvée »).

Pour de nombreuses applications il existe un besoin fort en réalisations matérielles légères et même ultralégères d'algorithmes de chiffrement devant apporter des garanties élevées de sécurité vis-à-vis des attaques physiques. Il faut aussi pouvoir coupler des systèmes cryptographiques sûrs et légers avec des éléments de traçabilité et d'identification intrinsèque des composants matériels. Les fonctions physiques non clonables qui bénéficient aujourd'hui d'une attention très forte de la communauté, ne sont qu'une réponse partiellement satisfaisante. Il convient donc d'étudier précisément leur modélisation afin d'apporter les garanties de sécurité inhérentes au processus de certification de la sécurité.

Enfin, de façon connexe à la sécurité en sciences de l'information, il est également nécessaire d'élaborer des méthodes pour assurer un fonctionnement robuste et stable du système dynamique global lors de catastrophes naturelles, de pannes accidentelles (pannes d'équipement, erreur humaine, bug de logiciels), ou à la suite d'attaques malveillantes. Ceci se fait au travers de certificats (garanties a priori)

de bon fonctionnement, de mécanismes de détection de défauts et de diagnostic de pannes, de gestion des risques et de reconfiguration dynamique. Ces dimensions doivent également être appréhendées afin de garantir la disponibilité des systèmes quelles que soient les conditions de fonctionnement.

On comprend à travers ces enjeux la complexité et les interactions entre les problématiques liées à la sécurité. Il est donc essentiel de permettre aux différentes communautés scientifiques de se rencontrer pour développer des solutions allant de la théorie de l'information jusqu'à la mise en œuvre de solution logicielle et matérielle tout en intégrant la problématique des usages et de l'acceptabilité.