Etude sur la recherche académique en sécurité informatique

DGRI
Département A3, secteur maths STIC

Mai 2008

PRINCIPALES RECOMMANDATIONS

Le département maths, physique, nanos, usages, sécurité et STIC de la DGRI a conduit une étude sur la recherche académique en sécurité informatique en France en 2007. Cette étude coordonnée par Atilla Baskurt, chargé de mission STIC, a été confiée à un comité composé d'experts de sensibilités complémentaires, issus d'organismes publics & privés et acteurs de l'activité R&D en sécurité informatique en France.

Comité de pilotage :

Atilla Baskurt, coordonnateur et rapporteur de l'étude, Chargé de mission STIC, DGRI

Claude Kirchner DR, INRIA Loria Président du comité
Stéphane Coulondre MCF, LIRIS, INSA Lyon
Loïc Duflot Secrétariat Général de la Défense Nationale (SGDN) Direction Centrale de la Sécurité des SI(DCSSI)
Jean-Marc Chassery DR, CNRS, GIPSA-lab, Grenoble
Yves Correc Chargé de mission prospective Sécurité des SI au Centre d'Électronique de l'Armement (CELAR), DGA
Laurent Bellefin Directeur des Opérations Sécurité, Solucom
Bernadette Dorizzi Professeur à l'INT Evry, GET
Ludovic Me Professeur, Supelec, Rennes
Sylvain Leroy DGE –MINEFI
Isabelle De Lamberterie DR CECOJI, CNRS, Paris
Alain Merle Responsable Technique du CESTI LETI, CEA
Claude Castelluccia DR, INRIA Rhône-Alpes
Bertrand Braunschweig Agence Nationale de Recherche Département Matière et information

Ce document consigne les réflexions des membres du comité et présente des recommandations en vue d'accroître la synergie entre les équipes de recherche, entre la recherche académique et l'industrie, la formation et la société. Pour chacune des recommandations, il rappelle la situation actuelle et ses conséquences, les objectifs de la recommandation et propose des mesures de mise en œuvre.

1. Rappel des études menées par le comité

Le comité d'experts a conduit les études suivantes :

- Mise en place et conduite d'une enquête en ligne destinée aux équipes de recherche académique afin d'évaluer qualitativement et quantitativement les forces en présence en France (de mars 2007 à janvier 2008) ;
- Analyse détaillée et synthèse des résultats de l'enquête (livrable produit en janvier 2008) ;
- Etat de l'art sur les documents nationaux et internationaux concernant la thématique ;
- Réflexion sur les enjeux et les priorités thématiques pour la recherche académique ;
- Proposition de recommandations (qui fait l'objet du présent document).

2. Liste des productions du comité

Tous les documents produits par le comité peuvent être consultés sur le site WEB qui a été mis en place :

http://scoulond.insa-lyon.fr/dgri

Ces documents concernent :

- Questionnaire « enquête recherche académique sur la sécurité informatique en France »
- Rapport d'analyse et de synthèse sur l'enquête « recherche académique sur la sécurité informatique en France »
- Liste et thématiques des 62 équipes ayant répondu à l'enquête
- Document « cartographies »
- Document « étude de faisabilité d'un défi national sur la sécurité des systèmes d'information et de communication »
- Document « inventaire des études récentes françaises et internationales sur la sécurité informatique »
- Document « recommandations du comité d'experts »

3. Recommandations

RECOMMANDATION 1
CONTINUER LA DYNAMIQUE CREEE PAR LES ACI ET LES AAP ANR DEPUIS 2003

Constat sur la communauté française :

Concernant les forces en présence
62 équipes de recherche académique française ont répondu à l'enquête menée par le comité. Il s'agit d'une communauté bien établie de 550 chercheurs. La formation des jeunes chercheurs se traduit par 158 thèses soutenues, soit de l'ordre de 40 soutenances par an entre 2003-2007. 28 HdR ont été soutenues en sécurité informatique dans la même période. La production scientifique de la communauté est importante, notamment avec 427 publications dans des revues internationales, 88 en revues nationales, 1450 en conférences internationales et 17 ouvrages.

Concernant les thématiques fortes
Les activités scientifiques de la communauté peuvent être regroupées en 9 grands domaines ordonnés suivant le nombre de chercheurs permanents.

Parmi les 62 équipes consultées, 27 présentent une activité significative dans le domaine de la preuve ou de la vérification formelle. Une analyse plus fine montre que les compétences dans le domaine des méthodes formelles sont utilisées principalement dans les domaines des modèles de contrôle d'accès, méthodologie de conception d'infrastructure et de logiciels sécurisés, protocoles sécurisés, analyse de code et politiques de sécurité.

Autour de la cryptologie et de son utilisation, en particulier dans la conception de protocoles, 22 équipes de recherche sont impliquées, représentant quelques 30,3 chercheurs permanents.

Les autres points forts sont les domaines de la sécurité des réseaux sans fil (16 équipes, 10 chercheurs permanents), de la détection/prévention d'intrusion (15 équipes, 15,2 chercheurs permanents) et de l'anonymisation et de la protection de la vie privée (15 équipes, 10,1 chercheurs permanents). Il est important de noter également le potentiel sur les aspects sécurité du contenu & stéganographie qui réunissent 17 équipes et 21,3 chercheurs permanents.

Thèmes et sous thèmes	Nb équipes	Chercheurs éq. temps plein
Modèles de sécurité pour les systèmes distribués / pour la grille	11	7,4
Modèles de contrôles d'accès	21	13,1
Modèles de confiance	11	5,9
Vérification formelle / Preuve formelle	27	23,6
Politiques de sécurité	17	9,9
[Regroupés dans] Modélisation de la sécurité		**59,9**
Protocoles sécurisés d'authentification, de communication, de services	20	14,9
Cryptographie symétrique, publique, certificats, architecture de gestion de clés / Cryptanalyse	22	30,3
[Regroupés dans] Cryptographie et protocoles		**45,2**
Analyse de code - failles logicielles	13	11,2
Méthodologie de conception d'infrastructure et de logiciel sécurisés	17	11,3
Analyse légale / Forensics	6	2,6
Systèmes d'exploitation sécurisés	8	4,3
Traçabilité / Maintenance de l'intégrité	12	5,9
Signaux Parasites compromettants (analyse des causes et solution)	2	2
[Regroupés dans] Sécurité (logique) locale		**37,3**
Surveillance de systèmes	11	7,9
Sécurité des réseaux sans-fil	16	10
Prévention et détection d'intrusions	15	15,2
Pots de miel	2	0,7
[Regroupés dans] Sécurité réseau		**33,8**
Biométrie (visage / rétine / iris / empreintes digitales)	5	9,2
Vote numérique	8	5,4
PETs (Privacy Enhancing Techniques)	6	3,7
Respect de la vie privée, Anonymat, Oubli	15	10,1
[Regroupés dans] Identification et protection de l'individu		**28,4**
Sécurité du contenu (tatouage images, video, etc.)	9	10,3
Stéganographie / Analyse de canaux cachés	8	11
Sécurité des données embarquées	11	6,2
DRM / Droits numériques : Image / Son / Vidéo	6	2,9
[Regroupés dans] Sécurité du contenu		**30,4**
Tests de sécurité	12	8,1
Robustesse de la sécurité : Mesure / Analyse	8	7,1
Reporting / Audit d'infrastructure / Certification	4	2
Patterns pour la sécurité	5	3,7
Mesure de la confiance	12	6,4
[Regroupés dans] Audits et tests en fonctionnement		**27,3**
Gestion des risques	8	4,5
Aspects sociétaux : Economique / Juridique / Ethique / Géostratégie / etc.	7	6,7
[Regroupés dans] Impact opérationnel de la sécurité		**11,2**
Analyse du matériel - failles physiques	4	2,9
Modules matériel pour fonctionnement sécurisé (TPM / TSS / Cartes à puce / RFID / FPGA / SOC)	10	5,6
[Regroupés dans] Sécurité matérielle		**8,5**

Concernant la recherche partenariale

La communauté a répondu présente aux ACI et AAP de l'ANR depuis 2003 avec plus de 40 projets soumis par an (48 équipes sur 62 y participent ou y ont participé). Les équipes sont également fortement impliquées dans des projets industriels autres que les programmes nationaux (30 équipes sur 62) et dans des projets région (27 équipes sur 62). 33 équipes sur 62 émargent dans des pôles de compétitivité.

Dans la période 2003 – 07, l'innovation se traduit par 31 brevets, 28 licences de logiciel, 102 prototypes et 4 créations d'entreprise.

Concernant les relations internationales :
La communauté est active au niveau international. 14 équipes sur 62 participent à des réseaux d'excellence. 27 équipes sur 62 indiquent leur participation à des projets européens. 19 équipes sur 62 citent leur appartenance à d'autres projets internationaux. Les équipes participent à l'animation de la communauté internationale (participations aux comités de rédaction ou de sélection et aux communautés IEEE ou l'AFNOR).

Objectifs, mesures [1] **:**
Le comité souligne le rôle structurant des ACI et AAP ANR sur la sécurité informatique depuis 2003. Le bilan positif des activités scientifiques de la communauté, relevé par l'enquête, témoigne de l'intérêt de ces actions nationales mises en place dans la même période.

Alors que les besoins scientifiques, économiques et sociétaux sont profonds et clairement identifiés et que la communauté scientifique est active et de taille significative, il est important de continuer cette dynamique créée par les ACI et AAP successifs et de soutenir la recherche, tant partenariale qu'académique. Il faudrait examiner si les nouveaux programmes ANR 2008 atteignent bien cet objectif et réagir si ce n'était pas le cas.

La poursuite des actions de type PARISTIC (intégrée désormais au Grand Colloque STIC) est encouragée afin de capitaliser les avancées scientifiques et techniques du domaine.

Il paraît tout aussi souhaitable de réfléchir sur les moyens d'assurer un financement dans la durée. Le financement de projets de courte durée (3 ans ou moins) pourrait conduire à la mobilité thématique des équipes et ceci pourrait limiter la capitalisation des compétences obtenues. Des projets de durée plus longue (plus de 3 ans) devraient être envisagés.

[1] Sans obtenir un consensus, la majorité des membres du comité s'est également exprimée favorablement sur l'opportunité d'un programme spécifique ANR sur la sécurité informatique.

RECOMMANDATION 2

LABORATOIRES EN SECURITE INFORMATIQUE POUR LA RECHERCHE ACADEMIQUE

Constat : Les nombreuses équipes de recherche travaillant en sécurité informatique se trouvent devant la nécessité d'analyser les entités mettant en cause la sécurité des machines, des systèmes et des réseaux. En effet, sur tous les thèmes de travail mentionnés dans l'enquête, il faut se donner les moyens d'analyser les faiblesses potentielles mais aussi de permettre l'expérimentation de compromissions potentielles : connaître les faiblesses des systèmes permet de mieux les comprendre et apprendre à les protéger.

Dans un cadre juridique approprié, prenant en particulier en compte la loi LCEN (Loi pour la Confiance dans l'Economie Numérique), il est nécessaire de donner aux chercheurs un cadre approprié offrant les caractéristiques suivantes :

- Centre national de collecte de vulnérabilités assurant (1) la paternité de la découverte pour les auteurs, (2) l'interface avec les industriels et (3) le support juridique et informatique permettant de publier les vulnérabilités vers les acteurs appropriés (CERT, Cesti, utilisateurs, etc.)
- Encadrement physique, éthique et juridique d'expériences mettant en jeu la sécurité de systèmes d'information

On se trouve donc dans une situation très similaire aux expérimentations nécessaires en biologie pour comprendre les agents potentiels existants, les neutraliser, en créer d'autres pour mieux en comprendre les mécanismes généraux.

Il est donc nécessaire de permettre aux acteurs de la recherche en sécurité informatique de réaliser des expériences mettant en œuvre des mécanismes compromettant la sécurité des systèmes d'information dans un cadre physique et juridique approprié à cette fonction de recherche : des laboratoires académiques de haute sécurité informatique. De tels laboratoires existent déjà à la DGA et commencent à se mettre en place dans le milieu académique.

Objectifs, mesures :
Le comité souligne le rôle fondamental de l'expérimentation en sécurité informatique et de la nécessité de la permettre via la

Création de laboratoires académique de haute sécurité informatique (Lahsi).

Ces laboratoires, étroitement encadrés tant juridiquement que techniquement, permettraient aux chercheurs de mener à bien et de publier des résultats tant sur les faiblesses potentielles que sur les attaques informatiques. La création de ces laboratoires serait accompagnée par la mise en place d'un règlement intérieur très précis, la mise en place d'un comité d'éthique national et par un conseil scientifique associé à chaque laboratoire. Ces laboratoires seraient amenés à coopérer avec les laboratoires non académiques et les Cesti.

RECOMMANDATION 3

PLATEFORMES COMMUNES POUR LA SYNERGIE RECHERCHE & FORMATION & INDUSTRIE

Constat :

La sécurité est une problématique abordée de manière assez hétérogène. Si les grands établissements de recherche possèdent un service spécifiquement dédié, les laboratoires universitaires n'ont que peu ou pas du tout conscience des risques encourus et sous-estiment largement, voire ignorent totalement, les impacts d'une sécurité défaillante. Outre le fait que de nombreux financements imposent en contrepartie des conditions de sécurité contraignantes (physiques, organisationnelles, informatique), leur manque de prise en compte peut de plus constituer un frein à la participation des laboratoires aux pôles de compétitivité, dont les enjeux nécessitent un minimum de rigueur pour éviter les fuites d'information. Cette remarque est bien entendu valable également pour les autres types d'acteurs publics et les entreprises.

En effet, l'intelligence économique, à destination de concurrents et/ou de puissances étatiques étrangères, est maintenant un mode répandu de renseignement, passant par des pratiques qui tirent souvent partie d'un manque de sensibilisation, d'organisation et de moyens techniques. Or, sécuriser l'information, n'impose pas forcément un investissement prohibitif, si l'on raisonne par rapport à la valeur du contenu. Le volume de informations critiques n'est en effet pas énorme (estimé à 15%).

Pour atteindre un public hétérogène et important, il serait nécessaire d'appliquer une démarche par l'exemple, permettant de sensibiliser les utilisateurs, enseignants, chercheurs et ingénieurs, via des scénarios réels et simples d'attaques informatiques, aux effets d'une mauvaise prise en compte des risques liés à l'intelligence économique, et plus généralement aux menaces techniques. Cette sensibilisation devrait conduire par la suite à identifier ce qui est critique, en attachant des niveaux de sécurité spécifiques en fonction de la valeur des données, pour permettre d'obtenir des résultats satisfaisants en terme d'impact d'un problème de sécurité.

Objectifs, mesures proposées :

Le comité souligne l'importance d'un **niveau minimal de sécurité de tous les acteurs scientifiques**. Le traitement de l'information devrait être raisonné. Pour augmenter sensiblement le niveau global de la sécurité, une sensibilisation et quelques règles simples de démarche technique et organisationnelle devraient faire partie de la culture, voire du règlement, d'un laboratoire de recherche.

Sans préconiser le recours à une forme académique, le comité propose l'emploi de **plates-formes de sensibilisation** par l'exemple. Ces plates-formes, relativement génériques et adaptables, dont le coût rapporté aux pertes macroscopiques liées à une mauvaise sécurité devrait rester négligeable, auraient pour double avantage d'être utilisables également dans le contexte de la formation initiale et de la formation continue des utilisateurs, voire des entreprises.

RECOMMANDATION 4
ENCOURAGER L'ENSEIGNEMENT DE LA SECURITE INFORMATIQUE EN LICENCE

Constat :

L'enquête a montré que les équipes de recherche entretenaient des relations étroites avec la formation. Plus de la moitié d'entre elles sont liées à une formation sur la sécurité.

En analysant les résultats cumulés sur toutes les formations indiquées, il est aisé de constater que la grande majorité des formations sont en master (34 formations avec 848 étudiants) ou en cycle d'ingénieur (16 formations avec 1038 étudiants). L'enquête ne permet pas de distinguer les niveaux M1 ou M2. Cependant, il est probable que la majorité des formations Master se situe plutôt au niveau master recherche. Il est important de faire en sorte que la sécurité ne soit pas qu'une affaire de spécialistes. Or, de manière générale, les étudiants, même au niveau ingénieur, n'ont pas toujours de compétences sécurité. Les formations professionnalisantes (master ou ingénieur) doivent ainsi intégrer un minimum de sécurité.

Cependant, la sécurité est une pyramide qui passe à la fois par de la technique et par de l'organisation, à tous les niveaux. Bien que l'enseignement de la sécurité informatique nécessite des pré requis importants, notamment en informatique, systèmes d'exploitation, réseaux, il faut souligner que les équipes sondées n'interviennent quasiment pas dans les formations licence, DUT ou BTS.

Il paraît pourtant indispensable de sensibiliser les étudiants plus tôt, idéalement en L1 et au plus tard au niveau L3, à des notions mettant en œuvre la sécurité comme l'identification des menaces, la programmation sécurisée ou les réseaux sécurisés. D'autre part, une sensibilisation aux méthodes d'analyse des risques, aux normes autour de la sécurité, et à l'intelligence économique serait aujourd'hui de mise.

Objectifs, mesures proposées :
Le comité souligne l'importance d'une **sensibilisation à la sécurité à tous les niveaux de la formation, et le plus tôt possible dans le cursus, par exemple en Licence 3.**

De façon complémentaire, cela pourrait passer par une sensibilisation sous la forme de scénarios réels, par l'intermédiaire de plates-formes dédiées de démonstration et d'expérimentation.

Parallèlement, une sensibilisation des acteurs socio-économiques (utilisateurs, entreprises, etc.) serait importante et pourrait être réalisée via la formation continue.

RECOMMANDATION 5
PROPOSITIONS DE PISTES D'AMÉLIORATION DE L'ANIMATION DE LA COMMUNAUTÉ

Constat :
La principale activité d'animation de la communauté concerne les Groupes de Recherche CNRS (GdR ASR, ISIS, GPL, IM, I3, SoCSip). Des engagements peuvent être cités dans des Groupes d'Intérêt Scientifique (GIS SSI, ALLIANCE et 3SGS), dans des sociétés savantes (SEE). Des colloques nationaux et journées thématiques sont régulièrement organisés. Il convient d'y ajouter des actions de type « défi », comme l'organisation du concours international BOWS-2 en tatouage des images.

Excepté des réponses isolées, la grande majorité des équipes sondées expriment l'intérêt d'un nouveau GdR dédié à la sécurité sous toutes ses facettes pour permettre les échanges entre les diverses communautés : modélisation, cryptographie, système, réseaux, biométrie, sécurité des contenus, sécurité des logiciels, solutions hardware et software, etc. A ce sujet, il faudrait être prudent quant au recouvrement trop important d'un nouveau GdR sécurité avec les GdR existants.

Objectifs, mesures proposées :
Le comité indique ici quelques pistes d'actions pour améliorer l'animation de la communauté maintenant bien identifiée :

- Favoriser les journées thématiques transversales inter-GdR
- Mettre en place d'une école d'été inter-GdR
- Tisser des liens plus proches entre les pôles de compétitivité et les GdR afin de rapprocher d'avantage la recherche académique et les partenaires industriels
- Mettre en place des procédures simples de mobilité de chercheurs entre les équipes (délégation / détachement / séjours courte durée)

RECOMMANDATION 6
MISE EN PLACE D'UN DEFI NATIONAL EN SECURITE INFORMATIQUE

Constat :
Le contexte national semble favorable pour la mise en place d'un défi national en sécurité informatique, comme le montrent certains indicateurs :

- La synthèse de l'enquête DGRI[2], qui atteste de l'existence d'une communauté structurée et importante tant au niveau qualitatif que quantitatif ;
- Le nombre de projets déposés aux différents appels ANR depuis plusieurs années, preuve du dynamisme de cette communauté ;
- L'existence de nombreux acteurs publics et privés (institutions, organismes, associations, groupes de travail,…) qui connaissent la sécurité informatique, réfléchissent, et prospectent ;
- Les documents nationaux et internationaux qui convergent sur l'importance stratégique de cette thématique.

Pour l'ANR, il pourrait s'agir d'une première expérience pilote qui permettrait d'affiner la notion de défi et évaluer son efficacité.

Objectifs :
- Il s'agit de définir des enjeux ambitieux dont l'atteinte préfigure une rupture forte en termes de nouveau produit ou d'avancée des connaissances, puis de soutenir des travaux qui permettent d'atteindre ces enjeux ;
- Il est important que le défi préconise une approche système : un Système d'Information (SI) avec son architecture, son système d'exploitation, ses protocoles, ses données et ses utilisateurs, le tout fonctionnant dans un contexte utilisateur et interagissant avec l'extérieur : un SI Contextualisé "SIC" qui sécurise l'organisation et la diffusion de l'information (qui doit utiliser quel type de données et pourquoi faire ?) ;
- Le défi doit réussir le savant mélange entre la recherche amont et la recherche à retombées industrielles (ou comment éliminer le gap entre la recherche amont et celle à finalité « usages » ?) ;
- Le défi doit créer une synergie recherche & formation & industrie (vers une plateforme qui pourrait servir à sensibiliser les usagers et à former des spécialistes) ;
- Le défi doit servir à construire une base pour un éventuel futur projet national fédérateur.

Points sur lesquels il faudrait veiller :
- Les fonctionnalités visées devraient nécessiter la collaboration de plusieurs compétences afin d'avoir un maximum de consortium qui répondent à l'appel ;
- Il serait important de tenir compte des résultats thématiques de l'enquête réalisée par la DGRI : **trouver un bon compromis entre une problématique terrain (besoin**

- [2] Rapport d'analyse et de synthèse sur l'enquête « recherche académique sur la sécurité informatique en France »

« **enduser** ») **et les forces en présence en France**. Le défi ne pourrait pas être une réussite si les compétences visées ne sont pas celles en présence forte en France. En effet, un défi demande une réponse rapide, cela ne serait possible que si de nombreuses équipes ont déjà les compétences visées ;

- Il faudrait certainement prévoir deux phases indépendantes : une phase de développement et une phase d'attaque ;
- Il faudrait un soutien financier à toutes les équipes qui tentent le défi afin d'encourager les équipes à répondre ;
- Il serait important de garantir la gestion de la confidentialité dans le cadre d'un tel défi. Outre les éventuels risques liés à une diffusion de techniques d'attaques sur des produits de sécurité, la gestion des résultats et la confidentialité de l'étude paraissent indispensables pour motiver les développeurs et disposer de propositions au niveau de l'état de l'art.