Enquête sur la recherche académique française en sécurité informatique

DGRI
Département A3, secteur maths STIC

Coordonnateur et rapporteur : Atilla Baskurt, Chargé de mission STIC

Février 2008

Cadre de l'étude

Le département mathématiques, physique, nanotechnologies, usages, sécurité et STIC de la Direction Générale de la Recherche et de l'Innovation (DGRI) du Ministère de l'Enseignement Supérieur et de la Recherche conduit une étude sur la recherche académique en sécurité informatique en France. Ce thème est en effet jugé stratégique. Cependant, une vision d'ensemble susceptible de porter une politique et une orientation nationale fait défaut, malgré l'existence d'éléments et travaux de qualité.

L'étude démarrée au printemps 2007 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. L'une des missions du comité a été d'établir une vision la plus complète possible des compétences scientifiques établies ou émergentes des équipes de recherche françaises sur la thématique de la sécurité informatique. Afin d'évaluer qualitativement et quantitativement les forces en présence, une enquête en ligne a été lancée. Le questionnaire composé d'une centaine de questions peut être consulté en annexe de ce document. Les laboratoires reconnus par le ministère (sections 27, 61 et 63), par le département ST2I du CNRS, les équipes de INRIA, de l'institut TELECOM, de la DGA et du CEA ont été invitées à répondre à cette enquête. Par ailleurs, la communauté des mathématiciens, également active dans une partie du domaine, a été invitée à répondre à l'enquête. Le questionnaire ciblait les équipes de recherche. 62 responsables d'équipe y ont contribué entre mai et décembre 2007.

Il convient de souligner qu'il s'agit des résultats d'une enquête qui comportent probablement certaines imprécisions ou manques engendrés par la nature même de ce type de démarche (liste de diffusion non exhaustive, réponses incomplètes,…). Par ailleurs, le comité a décidé de se limiter aux thématiques concernant la Sécurité des Systèmes d'Information et de Communication (cf. le questionnaire en annexe de ce document). Notons que les équipes travaillant sur la sûreté de fonctionnement, domaine qui partage certaines des thématiques en question (notamment preuve ou vérification formelle), n'ont pas nécessairement eu la même attitude vis-à-vis de l'enquête, certaines ont pu répondre, d'autre non.

Une analyse complète des réponses à l'enquête est proposée dans la seconde partie de ce document, la première en résume les points marquants.

Par ailleurs, le comité d'experts travaille sur d'autres actions relatives à la thématique sécurité informatique, elles sont listées ci-dessous :

- bilan des appels à projets français et européen des dernières années ;
- inventaire des études récentes françaises et internationales ;
- réflexion sur les enjeux et les priorités thématiques pour la recherche académique ;
- étude de l'opportunité de nouveaux outils d'animation de la communauté ;
- étude de faisabilité d'un défi national sur la sécurité informatique et recommandations.

La dernière action s'est achevée récemment par la production d'un document recommandant la mise en place d'un défi national sur la sécurité informatique dès 2008 et proposant quelques scénarii. Un document final présentera une synthèse de ces actions et proposera des recommandations au printemps 2008. La mise en place d'un site Web est prévue pour une large diffusion de l'ensemble des livrables.

Composition du comité

Etude menée par la DGRI, département maths – STIC
Ministère de l'Enseignement Supérieur et de la Recherche

Membres du comité
Claude Kirchner DR, INRIA **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
Alain Merle Responsable Technique du CESTI LETI, CEA
Sylvain Leroy DGE –MINEFI
Isabelle De Lamberterie DR CECOJI, CNRS, Paris
Bertrand Braunschweig Agence Nationale de Recherche, Département Matière et information
Claude Castelluccia DR, INRIA Rhône-Alpes

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

Partie I

Synthèse de l'enquête sur la recherche académique en sécurité informatique

1. Synthèse de l'enquête

1.1 Communauté de recherche académique en sécurité informatique

548 chercheurs travaillant en sécurité informatique dans ces 62 équipes, forment une communauté conséquente et bien identifiée. Parmi ces 548 chercheurs, nous trouvons :

- 293 permanents :
  - Enseignants – chercheurs : 165 dont 75 HdR (45%)
  - Chercheurs : 128 dont 52 HdR (40%)
- 217 doctorants
- 38 post-docs

D'après les équipes sondées, 11 personnels techniques permanents (soit 1 pour 50 chercheurs), accompagnent ces chercheurs. Notons également que 25 CDD techniques et 34 visiteurs académiques complètent les effectifs indiqués.

Les équipes appartiennent à différents types de structure : 32 dans des unités CNRS (dont 1 FRE et 1 UPR), 11 dans des EA (dont une associée à l'INSERM), 12 équipe-projets INRIA (dont 4 également associées au CNRS), 5 GET, 1 DGA, 1 CEA. Leur granularité est hétérogène (de 24 à 2). Leur répartition géographique met en évidence quatre grands pôles d'activités en Île-de-France (17), en Bretagne (14), en Rhône-Alpes (10) et en Lorraine (8).

La production scientifique de la communauté dans la période 2003 – 2007, est importante, notamment avec 427 publications dans des revues internationales, 88 en revues nationales, 1450 en conférences internationales et 17 ouvrages. L'innovation se traduit par 31 brevets, 28 licences de logiciel, 102 prototypes et 4 créations d'entreprise. La nature diffusante du thème sécurité informatique se traduit par une grande richesse thématique dans la liste des revues et conférences internationales citées par les équipes.

28 HdR ont été soutenues en sécurité informatique dans la même période (7 par an). La formation des jeunes chercheurs se traduit par 158 thèses soutenues, soit de l'ordre de 40 soutenances par an entre 2003-2007.

1.2 Cartographie thématique

Analyse par sous thèmes

L'enquête proposait une liste quasi exhaustive de sous thèmes dans lesquelles chaque équipe pouvait choisir plusieurs items. Le tableau 1 présente une vingtaine de sous thèmes qui ont été choisis. La palette est riche, ceci est directement lié à la nature transversale du thème sécurité qui « diffuse ».

Parmi les 62 équipes consultées, 27 (43%) reconnaissent avoir une activité significative dans le domaine de la preuve ou de la vérification formelle. C'est l'une des deux thématiques les plus étudiées en France. Une analyse plus fine montre que les compétences françaises indéniables 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. Ces thématiques figurent par voie de conséquence également parmi les thématiques les plus traitées en France à l'heure actuelle. Les

études des modèles de contrôle d'accès et celle des protocoles sécurisés mobilisent respectivement 21 et 20 équipes de recherche. L'analyse des politiques de sécurité est traitée par 17 équipes et la mise au point de méthodologies de conception d'infrastructure et de logiciels sécurisés par 17 équipes. L'analyse de code est traitée par 13 équipes.

Selon l'étude, la thématique qui mobilise le plus de chercheurs permanents en France (22 équipes de recherche, 30,3 chercheurs permanents[1]) est la cryptographie. Cette thématique est indéniablement l'une des forces de notre recherche académique. Il est à noter que la moitié des chercheurs en cryptographie est localisée au sein de la région Ile de France.

Les autres points forts sont sans nul doute 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.

Les thèmes de recherche où la communauté est moins présente (ou n'a pas répondu), sont l'analyse des signaux parasites compromettants (2 équipes, 2 chercheurs permanents), la problématique des failles physiques et de la sécurité du matériel (4 équipes, 2,9 chercheurs permanents). Les modules matériels pour la sécurité ou ayant un impact sur la sécurité (TPM, FPGA, Systèmes sur Puce, RFID) sont traités par 10 équipes et 5,6 chercheurs permanents. Cette implication semble faible si elle est confrontée aux difficultés industrielles liées à la maîtrise des composants matériels. Parmi les autres domaines qui concentrent peu de potentiel chercheur permanent, citons les systèmes d'exploitation sécurisés (8 équipes, 4,3 chercheurs permanents) et la sécurité des systèmes embarqués (11 équipes, 6,2 chercheurs permanents).

[1] Le calcul de chercheurs permanents permet d'évaluer les ressources humaines effectivement consenties sur chaque thème au niveau national. Voir la partie II section 3 pour la description du mode de calcul des chercheurs permanents.

Thème de recherche	Nombre d'équipes concernées	Nombre de chercheurs permanents
Vérification formelle / Preuve formelle	**27**	**23,6**
Cryptographie symétrique, publique, certificats, architecture de gestion de clés / Cryptanalyse	**22**	**30,3**
Modèles de contrôles d'accès	**21**	**13,1**
Protocoles sécurisés d'authentification, de communication, de services	**20**	**14,9**
Méthodologie de conception d'infrastructure et de logiciel sécurisés	**17**	**11,3**
Politiques de sécurité	**17**	**9,9**
Sécurité des réseaux sans-fil	**16**	**10,0**
Prévention et détection d'intrusions	**15**	**15,2**
Respect de la vie privée, Anonymat, Oubli	**15**	**10,1**
Analyse de code - failles logicielles	**13**	**11,2**
Tests de sécurité	**12**	**8,1**
Mesure de la confiance	**12**	**6,4**
Traçabilité / Maintenance de l'intégrité	**12**	**5,9**
Surveillance de systèmes	**11**	**7,9**
Modèles de sécurité pour les systèmes distribués / pour la grille	**11**	**7,4**
Sécurité des données embarquées	**11**	**6,2**
Modèles de confiance	**11**	**5,9**
Modules matériel pour fonctionnement sécurisé (TPM / TSS / Cartes à puce / RFID / FPGA / SOC / etc.)	**10**	**5,6**
Modèles de confiance	**10**	**5,4**
Sécurité du contenu (tatouage images, video, etc.)	**9**	**10,3**
Stéganographie / Analyse de canaux cachés	**8**	**11,0**
Gestion des risques	**8**	**4,5**
Systèmes d'exploitation sécurisés	**8**	**4,3**
Robustesse de la sécurité : Mesure / Analyse	**8**	**7,1**
Vote numérique	**8**	**5,4**
Aspects sociétaux : Economique / Juridique / Ethique / Géostratégie / etc.	**7**	**6,7**
PETs (Privacy Enhancing Techniques)	**6**	**3,7**
DRM / Droits numériques : Image / Son / Vidéo	**6**	**2,9**
Analyse légale / Forensics	**6**	**2,6**
Biométrie (visage / rétine / iris / empreintes digitales)	**5**	**9,2**
Patterns pour la sécurité	**5**	**3,7**
Analyse du matériel – failles physiques	**4**	**2,9**
Reporting / Audit d'infrastructure / Certification	**4**	**2,0**

Tableau 1: Couverture des thématiques de recherche ordonnées par le nombre d'équipes de recherche par sous thème.

Analyse globale

A partir de cette analyse fine, une lecture plus globale fait apparaître de grands domaines de recherche. Le tableau 2 présente un regroupement possible en 9 grands domaines ordonnés par le nombre de chercheurs permanents. C'est une vision à l'échelle macroscopique qui met en évidence les thématiques fortes de la recherche académique en sécurité informatique en France (Tableau 2).

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**

Tableau 2 : Thématiques de recherche classées en 9 grands domaines classés par le nombre de chercheurs permanents.

1.3 Recherche partenariale

L'analyse de l'enquête permet d'avoir un instantané sur la recherche partenariale des 62 équipes. Tout d'abord, une participation notable aux projets des pôles de compétitivité : 33 équipes sur 62 (53%) au premier rang desquels on retrouve les pôles Images et Réseaux, Systematic, Minalogic et SCS. Concernant les nouveaux outils, l'implication des équipes est comme suit :

- 4 équipes sur 62 (6%) dans deux RTRA : Digitéo et Sciences mathématiques ;
- 15 équipes sur 62 (24%) dans 5 Instituts Carnot : LSI, GET, C3S, LAAS et LETI (rappelons que 16 instituts Carnot touchent le domaine des STIC).

L'activité en projets collaboratifs est la suivante :

- laboratoires participant à un ou plusieurs projets nationaux (ACI, ANT, réseaux RRIT, projets GET) : 48 équipes sur 62 (77%) ;
- laboratoires participant à un ou plusieurs projets régionaux : 27 équipes sur 62 (44%).
- laboratoires participant à un ou plusieurs projets industriels : 30 équipes sur 62 (48%).

Les projets partenariaux correspondent à des collaborations bilatérales entre les équipes et les partenaires industriels. Il n'y a pas de recouvrement entre les projets nationaux, régionaux et partenariaux.

Depuis 2003, l'activité collaborative a été encouragée par les actions concertées incitatives (ACI) et les appels à projets (AAP) de l'Agence Nationale de la Recherche (ANR) sur la thématique sécurité et informatique. A ce sujet, et hors enquête, notons que plus d'un 1/6e des présentations du grand colloque STIC de novembre 2007, concernent la sécurité des systèmes d'information :

- ACI 2003 : 64 projets soumis dont 28 retenus ;
- ACI 2004 : 41 projets soumis dont 19 retenus ;
- AAP ANR araSSIA 2005 : 44 projets soumis dont 20 retenus ;
- AAP ANR SetIn 2006 : 39 projets soumis dont 18 retenus ;
- AAP ANR SeSur 2007 : 40 projets soumis dont 13 retenus.

L'ensemble de ces projets a reçu une aide financière voisinant 30 M€.

1.4 Relation Recherche & Formation en sécurité informatique

L'enquête permettait à chaque équipe de lister jusqu'à 3 formations dans lesquelles elle intervenait. Ainsi, 39 équipes sur 62 ont cité au moins une formation liée à la sécurité informatique. 15 équipes déclarent être actives dans 2 formations et 5 équipes dans 3 formations. Sur les 57 formations citées, les équipes ont également en charge la gestion administrative (totale ou en partie) de 23 formations (40%). Enfin, 22 équipes sont prêtes à s'impliquer dans une nouvelle formation.

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.

Bien que l'enseignement de la sécurité informatique nécessite des prérequis 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 est 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.

Notons que 5 équipes interviennent en formation continue (112 étudiants) afin de sensibiliser les acteurs du monde industriel.

Deux écoles d'été sur cette thématique ont été organisées dans la période 2003 – 2007, réunissant 135 auditeurs.

Les équipes s'impliquent également dans des Programmes Pluri-Formation (PPF) (6).

Les types d'enseignements se répartissent en quatre catégories : des modules d'introduction (36%), de recherche (23%), de l'enseignement technique/professionnel (19%) et des travaux pratiques/plateformes (22%).

1.5 Relation européennes et internationales

Les équipes ont développé des relations internationales :

- avec l'Europe : 27 équipes sur 62 (44%) indiquent leur participation à des projets européens (dont la très grande majorité à un seul projet) ;
- avec d'autres pays : 19 équipes sur 62 (31%) citent leur appartenance à des projets internationaux.

Elles souhaitent pérenniser ces contacts avec 36 équipes sur 62 (58%) qui veulent être présents sur le plan international à l'avenir. Notons que 14 équipes sur 62 (23%) participent à des réseaux d'excellence.

Les équipes participant à l'enquête sont également très actives dans l'animation de la communauté internationale et nationale avec :

- 56 participations aux comités de rédaction de revues internationales et nationales ;
- 474 participations aux comités de sélection des conférences internationales et nationales ;
- 7 participations à des comités ou communautés comme l'IEEE ou l'AFNOR ;
- une organisation de concours international sur le thème de la sécurité du contenu.

Parmi les actions projetées pour s'ouvrir plus à l'Europe et à l'international, il faut noter la motivation à s'ouvrir à des pays comme les USA, l'Australie, le Japon, le Canada ou la Chine sous forme de collaborations bilatérales soutenues par des thèses en cotutelle et des séjours de chercheurs senior.

1.6 Relation avec la société

L'un des objectifs de la consultation des équipes était de faire le bilan des relations avec des entités (organismes, association, collectivités, autres) sur les aspects sociétaux liés à la sécurité informatique. Seules 15 équipes sur 62 (24%) ont mentionné ce type d'action : des contacts liés à l'économie des transports, aux aspects juridiques et légaux, aux aspects économiques, avec la Société des Auteurs Compositeurs et avec l'ITU/ISO.

Peu de projections ont été formulées quant à l'amorçage de nouvelles relations sur les aspects sociétaux : 12 équipes sur 62 (20%). Les actions envisagées ont pour principaux objectifs de renforcer les interactions sciences humaines / STIC et de sensibiliser les usagers à la sécurité informatique.

Par ailleurs, en analysant la cartographie thématique avec la vision sociétale, il est aisé de relever de nombreux sous thèmes de recherche développés par les équipes et qui ont une incidence sur les aspects sociétaux, notamment :

- sur des applications finalisées : le vote numérique, le contrôle d'accès, la biométrie ;
- sur des questions liées au cadre normatif organisant la protection des personnes ou des droits : la protection de la vie privée, la traçabilité, la maintenance de l'intégrité, « Digital Rights Management » (DRM).

1.7 Animation de la communauté

Participation à l'animation de la communauté française :

La principale activité d'animation concerne les Groupes de Recherche CNRS (GdR). La communauté assure un nombre important de responsabilités dans divers comités des GdR (comité de pilotage, comité scientifique, comité de direction, responsabilité d'actions thématiques, etc.). Les GdR cités sont ASR (Architecture Systèmes Réseaux), ISIS (Information, Signal, Images et ViSion) et GPL (Génie de la Programmation et du Logiciel). Des participations actives sont également soulignées dans les GdR IM (Informatique et Mathématique), I3 (Information Interaction Intelligence) et SoCSip (System On Chip - System In Package).

Notons également la contribution au groupe de recherche en Intelligence Economique de l'IHEDN (Institut des Hautes Etudes de Défense Nationale), au groupe de travail R&D en sécurité des systèmes d'information du SGDN - DCSSI et la responsabilité du Comité d'Experts Diagnostic et Sûreté de Fonctionnement du département ST2I du CNRS.

Nous retrouvons de multiples engagements dans les Groupes d'Intérêt Scientifique (GIS), notamment les GIS SSI et ALLIANCE en Bretagne et le GIS 3SGS à Troyes. Certaines équipes sont parties prenante dans l'animation de sociétés savantes comme les branches « Sécurité des Systèmes d'Information » et « Systèmes informatiques de confiance » de la SEE (Société de l'Electricité, de l'Electronique et des Technologies de l'Information et de la Communication).

La communauté organise plusieurs colloques nationaux et journées thématiques comme le colloque Francophone sur l'Ingénierie des Protocoles (CFIP), le colloque CRiSIS - Les Risques et la Sécurité d'Internet et des Systèmes, les journées SSI du CELAR (Centre d'électronique de l'Armement) ou journées liées aux réseaux de capteurs (plate-forme RECAP) et au RFID (RFID 2006 à Lille).

Enfin, il est naturel de constater une participation active aux comités de pilotage, aux comités d'évaluation et aux expertises dans le cadre des programmes ACI et ANR et du RNRT depuis 2003.

Participation à l'animation de la communauté internationale :

Cet aspect a été analysé en grande partie dans la section 1.5 Relation européennes et internationales. Il convient d'y ajouter :

- la participation aux instances normatives comme l'AFNOR SC37 sur la biométrie ;
- l'organisation du concours international BOWS-2 en tatouage des images ;
- la participation à l'étude « Beyond the Horizon », sur la projection de la recherche sur les 15 années à venir, à l'initiative de la Commission européenne ;
- la représentation officielle de l'IEEE Computer Society auprès de l'IFIP (International Federation for Information Processing), TC-11 (Technical Committee on Security and Protection in Information Processing Systems) ;

- la représentation officielle de la SEE auprès de l'IFIP, TC-10 (Technical Committee on Computer System).

De quels types d'outils de coordination et d'animation scientifique (GdR, divers types de réseaux) pensez-vous que l'on doive disposer en France pour la sécurité informatique ?
L'ensemble des équipes participant à l'enquête souligne l'efficacité des ACI et appels à projets sur la sécurité informatique depuis 2003. Il est souligné le rôle structurant de ces programmes pour la communauté, ainsi que leur mission dynamisant la recherche partenariale. La poursuite des programmes ANR sur la sécurité informatique pour soutenir la recherche académique est sans nul doute la demande prioritaire des équipes. Notons aussi que les actions de type PARISTIC sont très appréciées afin de capitaliser les avancées scientifiques et techniques du domaine.

Excepté deux réponses isolées, la grande majorité des équipes 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. Des liens plus proches entre les pôles de compétitivité et les GdR, sont vivement souhaités afin de rapprocher d'avantage la recherche académique et les partenaires industriels.

Quant à l'expression d'autres besoins, citons ici les souhaits les plus marquants :

- la mise en place d'un centre national de collecte de vulnérabilités assurant (1) la paternité de la découverte pour les auteurs, (2) l'encadrement, en particulier juridique, de ces découvertes et (3) l'interface avec les industriels ;
- le besoin de plateformes d'expérimentation très utiles pour l'échange de données et d'expériences et pour disposer de benchmarks ;
- l'utilisation d'outils logiciels communs open source ;
- le développement de PICS (projet international de collaboration scientifique) pour une ouverture vers l'internationale ;
- la pérennisation d'une école d'été ;
- la définition d'un référentiel commun pour situer la sécurité informatique par rapport aux autres domaines de l'informatique et des télécommunications, ceci afin de distinguer la recherche en sécurité de la recherche qui utilise des résultats de sécurité ou qui comporte une coloration sécurité ;
- la nécessité d'encourager plus la mobilité des chercheurs (délégation/détachement).

Partie II

Analyse détaillée de l'enquête sur la recherche académique en sécurité informatique

2. Analyse quantitative de l'enquête

Nombre d'équipes ayant répondu à l'enquête : 62

Répartition des équipes :

équipes dans UMR CNRS	30
équipes dans EA	10
équipes INRIA	8
équipes dans UMR+INRIA	4
équipes Institut TELECOM	5
équipes dans FRE CNRS	1
équipes dans UPR CNRS	1
équipes DGA	1
équipes EA + INSERM	1
Equipe CEA	1

Répartition géographique des équipes :

Île-de-France	17
Bretagne	14
Rhône-Alpes	10
Lorraine	8
Nord-Pas-de-Calais	4
Aquitaine	2
Provence Alpes Côte d'Azur	2
Centre	1
Franche-Comté	1
Languedoc-Roussillon	1
Midi-Pyrénées	1
Poitou-Charentes	1

Effectifs des équipes :

Un total de 548 chercheurs (1.7 doctorant pour 1 HdR) :

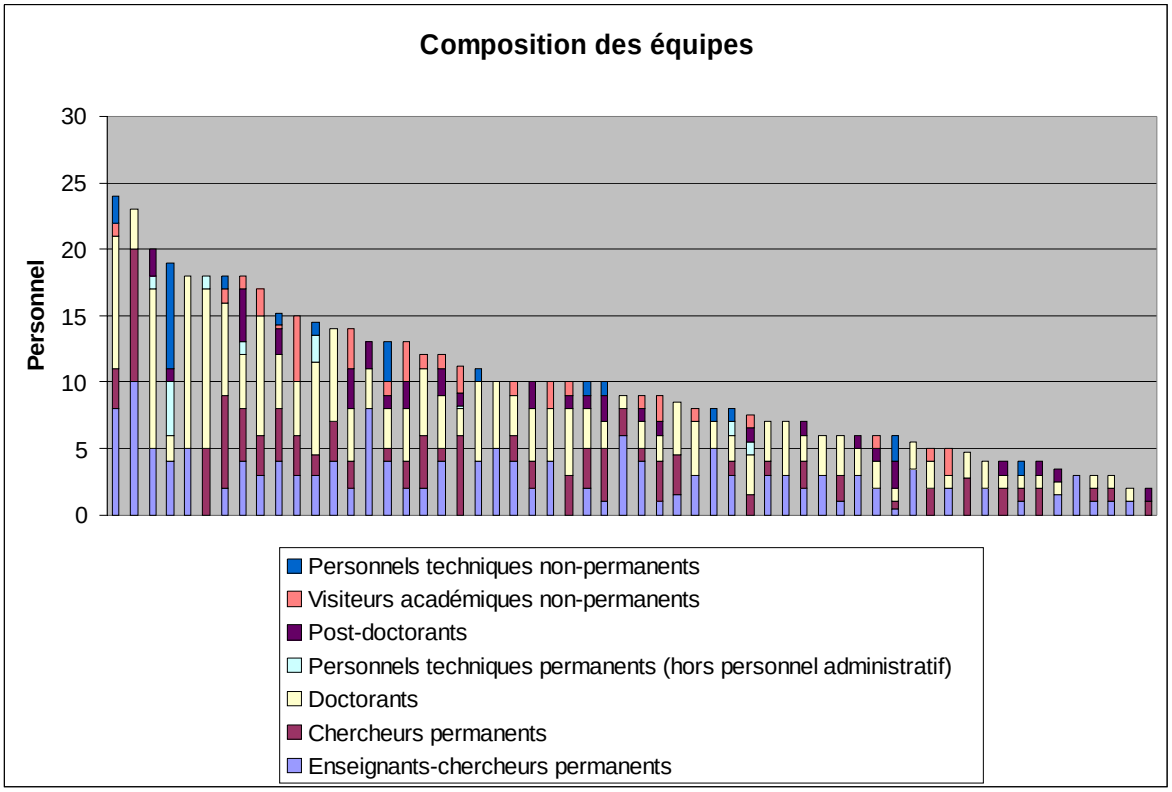
- 293 permanents :
  - Enseignants – chercheurs : 165 dont 75 HdR (45%)
  - Chercheurs : 128 dont 52 HdR (40%)
- 217 doctorants
- 38 post-docs

- Personnels techniques permanents : 11,5 (soit 1 pour 50 chercheurs)
- 25 CDD techniques
- 34 visiteurs académiques

Production scientifique (période 2003-07) :

- Revues internationales : 427
- Revues nationales : 88
- Conférences internationales : 1450
- Conférences nationales : 248
- Ouvrages : 17
- Editions ou co-éditions d'ouvrages collectifs : 66
- Contributions dans ouvrages collectifs : 111
- Conférences internationales et nationales organisées : 72
- Participations aux comités de rédaction de revues internationales et nationales : 58
- Participations aux comités de sélection des conférences internationales et nationales : 499
- Nombre d'HDR soutenues en sécurité informatique : 28
- Nombre de thèses soutenues en sécurité informatique : 158
- Nombre de brevet : 31
- Nombre de licences de logiciel : 28
- Nombre de prototypes : 102

Composition des équipes :



3. Analyse des thématiques de recherche actuelles et futures des équipes

Préambule
L'analyse suivante repose sur les éléments chiffrés obtenus lors de l'enquête publique pilotée par la DGRI qui visait essentiellement à recueillir des informations quantitatives sur l'activité des différentes équipes de recherche en sécurité des systèmes d'information en France. A ce titre, les réflexions présentées ici ne constituent aucunement un jugement de la valeur des travaux dans tel ou tel domaine, mais tentent de refléter au contraire les thématiques qui font l'objet d'un effort de recherche conséquent et celles qui sont au contraire délaissées par les équipes de recherche en Sécurité des Systèmes d'Information (SSI). Il est tout à fait possible qu'une équipe isolée obtienne des résultats significatifs dans un domaine précis tout en étant la seule équipe française à travailler sur le sujet. Les présentes considérations feront cependant l'analyse dans ce cas que la thématique n'est pas suffisamment couverte.

D'autre part les réflexions qui suivent peuvent potentiellement être faussées par la granularité des différents thèmes choisis pour l'enquête. Pour prendre une image grossière, la thématique « preuve ou vérification formelle » recouvre en réalité plusieurs sous domaines de compétence en fonction de l'utilisation qui est faite en pratique des connaissances théoriques (utilisation des méthodes formelles pour la preuve de protocole, méthodes formelles pour la sûreté de fonctionnement, abstraction de systèmes, « model checking » par exemple). En revanche, une thématique telle que le « vote électronique » est relativement précise et difficilement subdivisable.

Calcul du nombre de chercheurs permanents
L'évaluation du nombre de chercheurs permanents pour un thème donné et une équipe donnée est calculée en divisant le nombre de permanents de l'équipe par le nombre de thèmes traités par cette équipe. Le nombre de chercheurs permanents total est la somme, pour toutes les équipes, des chercheurs permanents pour un thème donné. Ainsi, si une équipe de 20 permanents travaille sur 10 thèmes de recherche, chacun sera crédité de 20/10=2 chercheurs permanents.

Cela ne signifie pas que seulement 2 chercheurs permanents s'intéressent au thème considéré. Le calcul permet de rendre compte au niveau macroscopique du temps passé à chaque thème, en considérant chaque équipe comme une et indivisible. En effet, il est possible qu'au sein de l'équipe, 15 permanents s'intéressent à 5 thèmes et 5 permanents s'intéressent à 5 autres thèmes. L'enquête n'est cependant pas assez précise pour tenir compte de l'organisation interne de chaque équipe.

De même, un chercheur pourrait avoir d'autres thématiques de recherche que la sécurité informatique et ne consacrer qu'un pourcentage de son temps à la thématique de l'enquête. Nous avons fait le choix de ne pas demander ces pourcentages par chercheur afin de ne pas alourdir la tâche des responsables d'équipes qui y ont contribué. La notion de chercheur permanent utilisée dans cette enquête, correspond donc à un chercheur actif dans l'une des thématiques de l'étude.

Thèmes de recherche actuels
L'enquête proposait une liste quasi exhaustive de sous thèmes dans lesquelles chaque équipe pouvait choisir plusieurs items. Le tableau 1 présente une vingtaine de sous thèmes qui ont été choisis. La palette est riche, ceci est directement lié à la nature transversale du thème sécurité qui « diffuse ».

Parmi les 62 équipes consultées, 27 (43%) reconnaissent avoir une activité significative dans le domaine de la preuve ou de la vérification formelle. C'est l'une des deux thématiques les plus étudiées en France. Une analyse plus fine montre que les compétences françaises indéniables 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. Ces thématiques figurent par voie de conséquence également parmi les thématiques les plus traitées en France à l'heure actuelle. Les études des modèles de contrôle d'accès et celle des protocoles sécurisés mobilisent respectivement 21 et 20 équipes de recherche. L'analyse des politiques de sécurité est traitée par 17 équipes et la mise au point de méthodologies de conception d'infrastructure et de logiciels sécurisés par 17 équipes. L'analyse de code est traitée par 13 équipes.

La thématique qui mobilise, selon l'étude, le plus de chercheurs permanents en France (22 équipes de recherche, 30,3 chercheurs permanents) est la cryptographie. Cette thématique est indéniablement l'une des forces de notre recherche académique. Il est à noter que la moitié des chercheurs en cryptographie est localisée au sein de la région Ile de France.

Les autres points forts sont sans nul doute 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.

Les thèmes de recherche où la communauté est moins présente (ou n'a pas répondu), sont l'analyse des signaux parasites compromettants (2 équipes, 2 chercheurs permanents), la problématique des failles physiques et de la sécurité du matériel (4 équipes, 2,9 chercheurs permanents). Les modules matériels pour la sécurité ou ayant un impact sur la sécurité (TPM, FPGA, Systèmes sur Puce, RFID) sont traités par 10 équipes et 5,6 chercheurs permanents. Cette implication semble faible si elle est confrontée aux difficultés industrielles liées à la maîtrise des composants matériels. Parmi les autres domaines qui concentrent peu de potentiel chercheur permanent, citons les systèmes d'exploitation sécurisés (8 équipes, 4,3 chercheurs permanents) et la sécurité des systèmes embarqués (11 équipes, 6,2 chercheurs permanents).

Le tableau 2 présente les mêmes thématiques en les ordonnant par le potentiel de chercheurs permanents.

Thème de recherche	Nombre d'équipes concernées	Nombre de chercheurs permanents
Vérification formelle / Preuve formelle	**27**	**23,6**
Cryptographie symétrique, publique, certificats, architecture de gestion de clés / Cryptanalyse	**22**	**30,3**
Modèles de contrôles d'accès	**21**	**13,1**
Protocoles sécurisés d'authentification, de communication, de services	**20**	**14,9**
Méthodologie de conception d'infrastructure et de logiciel sécurisés	**17**	**11,3**
Politiques de sécurité	**17**	**9,9**
Sécurité des réseaux sans-fil	**16**	**10,0**
Prévention et détection d'intrusions	**15**	**15,2**
Respect de la vie privée, Anonymat, Oubli	**15**	**10,1**
Analyse de code - failles logicielles	**13**	**11,2**
Tests de sécurité	**12**	**8,1**
Mesure de la confiance	**12**	**6,4**
Traçabilité / Maintenance de l'intégrité	**12**	**5,9**
Surveillance de systèmes	**11**	**7,9**
Modèles de sécurité pour les systèmes distribués / pour la grille	**11**	**7,4**
Sécurité des données embarquées	**11**	**6,2**
Modèles de confiance	**11**	**5,9**
Modules matériel pour fonctionnement sécurisé (TPM / TSS / Cartes à puce / RFID / FPGA / SOC / etc.)	**10**	**5,6**
Modèles de confiance	**10**	**5,4**
Sécurité du contenu (tatouage images, video, etc.)	**9**	**10,3**
Stéganographie / Analyse de canaux cachés	**8**	**11,0**
Gestion des risques	**8**	**4,5**
Systèmes d'exploitation sécurisés	**8**	**4,3**
Robustesse de la sécurité : Mesure / Analyse	**8**	**7,1**
Vote numérique	**8**	**5,4**
Aspects sociétaux : Economique / Juridique / Ethique / Géostratégie / etc.	**7**	**6,7**
PETs (Privacy Enhancing Techniques)	**6**	**3,7**
DRM / Droits numériques : Image / Son / Vidéo	**6**	**2,9**
Analyse légale / Forensics	**6**	**2,6**
Biométrie (visage / rétine / iris / empreintes digitales)	**5**	**9,2**
Patterns pour la sécurité	**5**	**3,7**
Analyse du matériel – failles physiques	**4**	**2,9**
Reporting / Audit d'infrastructure / Certification	**4**	**2,0**
Signaux parasites compromettants	**2**	**2**
Pots de miel	**2**	**0,7**

Tableau 1: Couverture des thématiques de recherche ordonnées par le nombre d'équipes de recherche par thème.

Thème de recherche	Nombre d'équipes concernées	Nombre de chercheurs permanents
Cryptographie symétrique, publique, certificats, architecture de gestion de clés / Cryptanalyse	**22**	**30,3**
Vérification formelle / Preuve formelle	**27**	**23,6**
Prévention et détection d'intrusions	**15**	**15,2**
Protocoles sécurisés d'authentification, de communication, de services	**20**	**14,9**
Modèles de contrôles d'accès	**21**	**13,1**
Méthodologie de conception d'infrastructure et de logiciel sécurisés	**17**	**11,3**
Analyse de code - failles logicielles	**13**	**11,2**
Stéganographie / Analyse de canaux cachés	**8**	**11,0**
Sécurité du contenu (tatouage images, video, etc.)	**9**	**10,3**
Respect de la vie privée, Anonymat, Oubli	**15**	**10,1**
Sécurité des réseaux sans-fil	**16**	**10,0**
Politiques de sécurité	**17**	**9,9**
Biométrie (visage / rétine / iris / empreintes digitales)	**5**	**9,2**
Tests de sécurité	**12**	**8,1**
Surveillance de systèmes	**11**	**7,9**
Modèles de sécurité pour les systèmes distribués / pour la grille	**11**	**7,4**
Robustesse de la sécurité : Mesure / Analyse	**8**	**7,1**
Aspects sociétaux : Economique / Juridique / Ethique / Géostratégie / etc.	**7**	**6,7**
Mesure de la confiance	**12**	**6,4**
Sécurité des données embarquées	**11**	**6,2**
Traçabilité / Maintenance de l'intégrité	**12**	**5,9**
Modèles de confiance	**11**	**5,9**
Modules matériel pour fonctionnement sécurisé (TPM / TSS / Cartes à puce / RFID / FPGA / SOC / etc.)	**10**	**5,6**
Vote numérique	**8**	**5,4**
Gestion des risques	**8**	**4,5**
Systèmes d'exploitation sécurisés	**8**	**4,3**
PETs (Privacy Enhancing Techniques)	**6**	**3,7**
Patterns pour la sécurité	**5**	**3,7**
DRM / Droits numériques : Image / Son / Vidéo	**6**	**2,9**
Analyse du matériel – failles physiques	**4**	**2,9**
Analyse légale / Forensics	**6**	**2,6**
Reporting / Audit d'infrastructure / Certification	**4**	**2,0**
Signaux parasites compromettants	**2**	**2**

Tableau 2: Couverture des thématiques de recherche ordonnées par le nombre de chercheurs permanents.

A partir de cette analyse fine, il est important de passer à une vision plus globale en faisant apparaître des grands domaines de recherche. Le tableau 3 présente un regroupement en 9 grands thèmes ou domaines (composés d'un certain nombre de sous thèmes) avec le nombre d'équipes concernées par thèmes et sous thèmes et le nombre de chercheurs permanents.

Le tableau 4 ordonne ces 9 grands domaines suivant le coefficient (rapport nombre d'équipes pour le thème / nombre de sous thèmes regroupés au sein du thème). Ce coefficient permet en effet de minimiser l'effet du regroupement (certains thèmes comprennent 7 sous thèmes, certains uniquement deux sous thèmes, d'où l'idée de normaliser). Enfin, le tableau 5 présente les 9 grands domaines ordonnés en fonction du nombre de 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**

Tableau 3 : Thématiques de recherche classées en 9 grands domaines avec le détail dans chaque grand domaine.

Thématiques de recherche par grands domaines	Nombre d'équipes pour le thème normalisé par le nombre de sous thèmes regroupés au sein de chaque grand domaine
Cryptographie et protocoles	21
Modélisation de la sécurité	17,4
Sécurité réseau	11
Sécurité (logique) locale	9,7
Sécurité du contenu	8,5
Identification et protection de l'individu	8,5
Audits et tests en fonctionnement	8,2
Impact opérationnel de la sécurité	7,5
Sécurité matérielle	7

Tableau 4 : 9 grands domaines ordonnés suivant le coefficient (rapport nombre d'équipes pour le thème / nombre de sous thèmes regroupés au sein du thème).

Thématiques de recherche par grands domaines	Nombre de chercheurs permanents
Modélisation de la sécurité	59,9
Cryptographie et protocoles	45,2
Sécurité (logique) locale	37,3
Sécurité réseau	33,8
Sécurité du contenu	30,4
Identification et protection de l'individu	28,4
Audits et tests en fonctionnement	27,3
Impact opérationnel de la sécurité	11,2
Sécurité matérielle	8,5

Tableau 5 : 9 grands domaines ordonnés suivant le nombre de chercheurs permanents.

Analyse des sujets de recherche pour l'avenir

L'enquête demandait également aux équipes consultées quels étaient les sujets qu'elles n'abordaient pas pour l'instant mais qu'elles pourraient être tentées d'étudier dans l'avenir. Les équipes ont manifestement joué le jeu puisque 49 des 62 équipes consultées ont fourni une indication des orientations futures en matière de recherche qu'elles envisagent. Les réponses fournies sont très diverses. Cependant, parmi les thèmes considérés, nombreux sont ceux qui sont relatifs soient au domaine des méthodes formelles (vérification prouvée, sûreté, model checking) soit au domaine de la cryptographie (cryptographie prouvée, attaques par canaux auxiliaires, attaques par injection de faute, génération de nombres aléatoires …). Nombreuses sont également les équipes désireuses de s'attaquer à l'épineux problème de la récupération de données, en particulier post-mortem (Forensics). Les thématiques de vote électronique, RFID et sécurité matérielle pourraient bénéficier d'un regain d'activité dans les années à venir. Les nouvelles thématiques qui seront potentiellement abordées sont généralement proches de problématiques traitées à l'heure actuelle par les équipes, ce qui semble malgré tout relativement logique. Quelques thématiques particulièrement originales ont par ailleurs été citées telles que stéganalyse, théories équationnelles pour la sécurité, systèmes adaptatifs.

Seules 5 des équipes contactées pensent arrêter l'une des thématiques sur laquelle elles travaillent. Les raisons invoquées pour justifier l'arrêt de telle ou telle thématique sont généralement non techniques (manque de moyens humains, arrêt pour être compétitif sur d'autres domaines, manque d'intérêt pour les applications potentielles des technologies concernées).

4. Relations recherche & industrie

- Participation à des RTRA : 4 équipes sur 62 (6%)
- Participation aux pôles de compétitivité : 33 équipes sur 62 (53%) :
    - IMAGES et RESEAUX : 9
    - SYSTEMATIC : 9
    - MINALOGIC : 6
    - SCS : 5
    - AEROSPACE VALLEY : 3
    - POLE MER : 2
    - INDUSTRIES DU COMMERCE : 2
    - VEHICULE DU FUTUR : 2
    - MOV'EO : 1
    - TES : 2
- Participation aux Instituts Carnot : 15 équipes sur 62 (24%)
- Laboratoires participant à un ou plusieurs projets nationaux: 48 équipes sur 62 (77%)
- Laboratoires participant à un ou plusieurs projets régionaux: 27 équipes sur 62 (44%)
- Laboratoires participant à un ou plusieurs projets industriels : 30 équipes sur 62 (48%)
- Laboratoires participant à l'animation de la communauté : 32 équipes sur 62 (48%)

- Nombre de création d'entreprise : 4
- Nombre de brevet : 31
- Nombre de licences de logiciel : 28
- Nombre de prototypes : 102

5. Relations recherche & formation

(l'enquête permettait à chaque équipe de lister jusqu'à 3 formations)

Formation 1

- Nombre d'équipes en relation avec une formation liée à la sécurité informatique : **39 équipes** ont cité au moins une formation

Nombre d'équipes réparties par formation	Nombre d'étudiants	Nombre d'heures de face à face pédagogique	Nombre d'heures dispensées
Master : 26	663	4242	1170
Cycle ingénieur : 9	538	1305	615
Licence/DUT/BTS : 1	28	450	130
Formation continue / double compétence : 2	62	360	380
Ecole d'été : 1	50	?	20

- Répartition des formations en fonction de la nature de l'implication
  - Enseignements : 39
  - Gestion administrative : 15
- Programme Pluri-Formation (PPF) : 5
- Répartition des formations en fonction des types d'enseignements :
  - Introduction : 33
  - Recherche : 23
  - Technique/professionnel : 17
  - Travaux pratiques/plateformes : 21

Formation 2

- Nombre d'équipes en relation avec une 2e formation liée à la sécurité informatique : 15

Nombre d'équipes réparties par formation	Nombre d'étudiants	Nombre d'heures de face à face pédagogique	Nombre d'heures dispensées
Master : 7	173	1460	448
Cycle ingénieur : 5	210	1400	262
Formation continue / double compétence : 1	10	4	4
Ecole d'été : 2	85	52	12
Site Web pédagogique:	200	50	1

- Répartition des formations en fonction de la nature de l'implication
  - Enseignements : 14
  - Gestion administrative : 6
- Programme Pluri-Formation (PPF) : 1
- Répartition des formations en fonction des types d'enseignements :
  - Introduction : 7
  - Recherche : 5
  - Technique/professionnel : 4
  - Travaux pratiques/plateformes : 3

Formation 3

- Nombre d'équipes en relation avec une troisième formation liée à la sécurité informatique : 5

Nombre d'équipes réparties par formation	Nombre d'étudiants	Nombre d'heures de face à face pédagogique	Nombre d'heures dispensées
Master : 1	12	500	120
Cycle ingénieur : 2	290	1100	120
Formation continue / double compétence : 2	40	310	58

- Répartition des formations en fonction de la nature de l'implication
    - Enseignements : 4
    - Gestion administrative : 2
- Programme Pluri-Formation (PPF) : 0
- Répartition des formations en fonction des types d'enseignements :
    - Introduction : 4
    - Recherche : 0
    - Technique/professionnel : 3
    - Travaux pratiques/plateformes : 3

Résultats cumulés

Nombre d'équipes réparties par formation	Nombre d'étudiants	Nombre d'heures de face à face pédagogique	Nombre d'heures dispensées
Master : 34	848	6202	1738
Cycle ingénieur : 16	1038	3805	997
Licence/DUT/BTS : 1	28	450	130
Formation continue / double compétence : 5	112	674	442
Ecole d'été : 2	135	52	32
Site Web pédagogique : 1	200	50	1

- Répartition des formations en fonction de la nature de l'implication
    - Enseignements : 57
    - Gestion administrative : 23
- Programme Pluri-Formation (PPF) : 6
- Répartition des formations en fonction des types d'enseignements :
    - Introduction : 44
    - Recherche : 28
    - Technique/professionnel : 24
    - Travaux pratiques/plateformes : 27
- 22 équipes sont prêtes à s'impliquer dans une nouvelle formation.

6. Relations avec l'Europe

- Participation à des projets européens : 27 équipes sur 62 (44%)
    - 24 équipes participant à 1 seul projet
    - 1 équipe participant à 2 projets
    - 1 équipe participant à 5 projets
- Participation à des projets internationaux (autres que européens) : 19 équipes sur 62 (31%)
- Equipes voulant être présents sur un plan international à l'avenir : 36 équipes sur 62 (58%)
- Participation à des réseaux d'excellence : 14 équipes sur 62 (23%)
- Animation de la communauté internationale en sécurité : 23 équipes sur 62 (37%) :
- Participation à la programmation des conférences internationales : 13
- Participation à des comités ou communautés comme l'IEEE ou l'AFNOR : 7
- Participation à l'édition de journaux spécialisés : 4
- Participation à des comités de lecture de revues internationales : 3
- Programmer et participer à des projets européens et internationaux : 2
- Organiser des concours sur le thème de la sécurité
- Actions projetées pour s'ouvrir plus à l'Europe et à l'international :
    - Participer à des projets européens : 12
    - Mener des projets avec des universités étrangères, comme des thèses en cotutelle : 5
    - Organiser des conférences internationales : 4
    - Poursuivre les projets en cours : avec les USA, l'Australie, le Japon, la Colombie, le Canada, la Chine : 4
    - Répondre à l'appel à proposition FP7 de la Commission Européenne : 3
    - Participer au working group IFIP IETF
    - Organiser des sessions spéciales / colloques / workshops
    - Encourager la mobilité des enseignants chercheurs et des étudiants
    - Développer des plateformes d'expérimentation communes

7. Relations avec la société

- Relation avec des entités (organismes, association, collectivités, autres) sur les aspects sociétaux liés à la sécurité informatique : 15 équipes sur 62 (24%)
- Les actions entreprises sont les suivantes :
    - Contacts liés à l'économie des transports
    - Contacts liés aux aspects juridiques et légaux
    - Contacts liés aux aspects économiques
    - Contact avec la Société des Auteurs Compositeurs
    - Contact avec les entreprises liées à la défense
    - Contact avec l'ITU/ISO
    - Contact avec le SGDN DCSSI
- Projections sur de nouvelles relations sur les aspects sociétaux : 12 équipes sur 62 (19%)
- Les actions projetées sont les suivantes :
    - Organiser des réunions de vulgarisation
    - Traiter les aspects juridiques de l'entreprise
    - Organiser des actions avec les collectivités locales
    - Renforcer les interactions sciences humaines / STIC

8. Outils de coordination, d'animation présents et futurs

Participation à l'animation de la communauté française :

Membres des comités de pilotage, des comités d'évaluation ou experts dans le cadre des programmes :

- ACI Sécurité&informatique (SI 2004)
- ARA Sécurité, Systèmes embarqués et Intelligence Ambiante (SSIA 2005),
- ANR SETIN (2006)
- ANR SESUR (2007)
- ANR "Sécurité Globale" 2007
- RNRT pour les aspects sécurité

Animation des GdR, autres :

- Membres du comité de pilotage ou comité scientifique ou responsabilité :
    - Comité scientifique du GdR ASR (Architecture Systèmes Réseaux)
    - Comité de pilotage du pôle RésCom du GDR ASR
    - Comité de direction du GdR ISIS (Information, Signal, Images et ViSion)
    - Comité scientifique du GDR GPL (Génie de la Programmation et du Logiciel)
    - Responsable du GDR GLP et responsable du groupe de travail MFDL
    - Responsable Action tatouage, thème D, GdR ISIS
- Participations :
    - GDR IM (Informatique et Mathématique)
    - GDR I3 (Information Interaction Intelligence)
    - Groupe de recherche en Intelligence Economique de l'IHEDN (Institut des Hautes Etudes de Défense Nationale)
    - GdR SoCSip

Organisations de conférences nationales, de journées :

- Participation au comité de pilotage du Colloque Francophone sur l'Ingénierie des Protocoles (CFIP)
- Organisation d'événements liés aux réseaux de capteurs (plate-forme RECAP) et au RFID (RFID 2006 à Lille)
- Participation à la commission d'évaluation des journées SSI du CELAR (Centre d'électronique de l'Armement) depuis 1997
- Participation au comité de programme de Conference on Security in Network Architectures (SAR) et Conference on Security in Information Systems (SSI)
- Participation au comité de programme du colloque CRiSIS - Les Risques et la Sécurité d'Internet et des Systèmes
- Participation à la commission sur la formation nationale « Sécurité informatique pour les administrés »

Animation dans sociétés savantes, associations scientifique :

- Animation du cercle SSI du club 63 de la SEE

- Participation au GIS SSI Diwall (GIS créé par ENST Bretagne, IRISA, INSA Rennes, Supélec Rennes, Université Rennes 1)
- Création et présidence du Club 63 "Systèmes informatiques de confiance" de la SEE
- Participation au groupe SSI de SEE
- Participation au GIS STIC Alliance
- Participation au GIS 3SGS à Troyes

Au CNRS :
- Responsable du Comité d'Experts Diagnostic et Sûreté de Fonctionnement du département ST2I du CNRS

Participation à l'animation de la communauté internationale :

Note : pour faciliter la lecture, nous ne mentionnons pas ici toutes les participations en tant qu'éditeurs associés aux revues internationales, les organisations et les participations aux comités de programmes des conférences internationales.

- Vice-chair du Technical Committee on Fault Detection, Supervision and Safety of Technical Processes SAFEPROCESS
- Un des leaders du réseau ECRYPT
- Présidence du comité stratégique de ECRYPT
- Participation à AFNOR SC37
- Co-responsable du laboratoire virtuel "Theorie en tatouage" du REX Ecrypt
- Co-organisateur du concours BOWS-2 (bows2.gipsa-lab.inpg.fr)
- Participation à 'Beyond the Horizon' à l'initiative de la Commission européenne.
- Représentant officiel de l'IEEE Computer Society auprès de l'IFIP TC-11 (Technical Committee on Security and Protection in Information Processing Systems), depuis août 1999.
- IFIP : Vice présidence Représentant de la SEE à l'IFIP TC-10 Computer System
- Participation active à l'IETF Projets européens

De quels types d'outils de coordination et d'animation scientifique (GdR, divers types de réseaux) pensez-vous que l'on doive disposer en France pour la sécurité informatique ?

Expressions sur le besoin de nouveaux GdR :
- Besoin d'un nouveau GdR dans le domaine biométrique
- Besoin d'un GdR dédié à la sécurité sous toutes ses facettes pour permettre les échanges entre les diverses communautés : modélisation, cryptographie, système, réseaux, ...
- Besoin d'inter GdR solutions hard et soft et des liens plus proche entre pôles de compétitivité et GdR
- Un GdR sur la sécurité logicielle serait intéressant (inexistant aujourd'hui)
- L'outil GdR s'est avéré fructueux dans nombre de thématiques. Un GdR spécialisé "Sécurité Informatique" serait le bienvenu.
- Il faudra réfléchir sur le rapprochement de la communauté par un GdR spécifique ou un nouveau type d'animation qui permet aux diverses communautés touchant à la sécurité informatique de se retrouver et de découvrir ce que font les uns et les autres

Les GdR existants ou les outils existants sont suffisants :
- Non, l'existant est suffisant (GDR GPL et journées PARISTIC)
- Compte tenu des effectifs dans le domaine qui nous concerne (tatouage, data hiding, fingerprinting), les outils déjà présents (GdR, ANR) suffisent.

Expressions sur le besoin d'autres structures :
- Centre national de collecte de vulnérabilités assurant (1) la paternité de la découverte pour les auteurs et (2) l'interface avec les industriels
- Tout moyen permettant de décloisonner, sur le thème sécurité et sûreté, l'informatique et le reste des STIC !
- PICS (projet international de collaboration scientifique) pour une ouverture vers l'internationale
- Sujet trop vaste et varié pour qu'un GDR soit productif, il faudrait privilégier l'aspect formation de type école d'été et échanges avec les industriels.
- Les GdR sont des outils d'animation très pertinents mais il faudrait être prudent quant au recouvrement trop important d'un nouveau GdR sécurité avec les GdR existants.
- Assurer plus de coordinations entre les équipes travaillant sur des "thèmes sécurité" et celles travaillant sur des sujets parfois perçus à tort comme ne faisant pas partie de la "bulle" sécurité : la disponibilité, la tolérance aux défaillances ...
- Création d'une revue dans ce domaine en France
- Un référentiel commun pour situer la sécurité par rapport aux autres domaines de l'informatique et des télécommunications, ceci afin de distinguer la recherche en sécurité de la recherche qui utilise des résultats de sécurité ou qui comporte une coloration sécurité.

Autres remarques :
- Les ACI et appels à projets sur la sécurité, ont été particulièrement efficaces.
- Les petites structures sont plus efficaces qu'un GDR ou un réseau
- Un nouvel appel ANR commun pour la sécurité, similaire à SeSur ?
- Réseau de sécurité et santé
- Il faudra favoriser l'analyse critique des solutions proposées

Quelles éventuelles actions futures pour mieux capitaliser les compétences des équipes françaises (projets collaboratifs, plateforme d'expérimentation, outils de développement commun,…) pensez-vous nécessaires ou prometteuses, ou au contraire inutiles ?

Pour une plateforme :
- Projets collaboratifs recherche & industrie
- Plateformes d'expérimentation très utiles surtout pour échange de données et expériences et pour disposer de benchmarks
- Plateforme d'évaluations comparatives de systèmes biométriques
- PICS (projet international de collaboration scientifique) pour une ouverture vers l'internationale
- Outils logiciels communs open source
- Laboratoire Haute sécurité

Contre une plateforme :
- Les plateformes sont inutiles car en général des usines a gaz. Pareil pour les outils communs. Les projets ACI sont très utiles.

Autres remarques :

- Assurer un financement plus récurrent des efforts de recherche et investissements intellectuels des équipes au-delà de la durée d'un seul projet. Le financement actuel de la recherche par projets encourage trop la mobilité thématique des équipes et ne permet pas la capitalisation des compétences obtenues
- La communauté est très vaste. Aussi, il nous semble plus prometteur de capitaliser sur des actions de type PARISTIC
- La sécurité étant souvent vue comme une thématique transversale dans beaucoup de laboratoire, de nombreux projets se trouvent "partiellement et faiblement" impliqués dans cette thématique. En conséquence, un effort important doit être fait pour assurer une mise en relation de ces petits groupes de chercheurs (recensement des activités, projets fédérateurs,...)
- Au-delà des aspects (coordination et animation), le soutien à la recherche académique en sécurité informatique doit être soutenu et accru. Il faut veiller à ne pas trop orienter ce soutien sur une voie trop axée sur exigences des grandes entreprises
- La poursuite des programmes ANR (ACI-SI, SeSur, Setin) est très importante
- Trouver des outils facilitant la mobilité d'enseignant chercheurs (délégation/détachement) par le biais de projets Sécurité serait bénéfique
- Les principales équipes françaises du domaine (tatouage, data hiding, fingerprinting) collaborent déjà via les structures existantes
- Certaines études sur la sécurité incluent des contraintes fortes de confidentialité limitant la diffusion des résultats, d'où le très faible nombre de publications et de brevets. Elles devraient être encadrées et respecter des contraintes fortes de confidentialité. Certaines sont difficilement compatibles avec les modes de financement existants (ANR, etc).

Eléments complémentaires que vous jugez utiles pour cette enquête

- Bénéficier d'une synthèse de l'enquête en retour
- De nombreuses remarques sur la nature jeune des équipes sur la sécurité informatique
- Il serait bon que l'évaluation des projets soumis à l'ANR s'appuie sur la qualité des résultats obtenus pendant les projets précédents soumis par le même consortium, et permette ainsi la continuité d'efforts de recherche
- Peut-être au sein des projets nationaux autorises la présence (même très limité) des équipe de recherche étrangères
- La biométrie se situe à la frontière entre sécurité des systèmes et reconnaissance des formes.
- Le thème de la virologie nécessite de faire des expériences, d'où la volonté de mise en place d'un laboratoire de haute sécurité au Loria, qui est inscrit dans le cadre du CPER et du GIS 3SGS

9. Questionnaire de l'enquête

Recherche académique en sécurité informatique

DGRI, département Maths, nanos, physique, usages, sécurité, STIC
(Mai 2007 ➔ Septembre 2007)

Informations administratives

Acronyme de votre laboratoire ou unité de recherche
Intitulé complet de votre laboratoire ou unité de recherche
Type de laboratoire ou d'unité de recherche

Par exemple : UMR, EA, etc. suivi du numéro associé

- Nom et prénom du directeur
- Nom de l'équipe de recherche au sein du laboratoire où s'effectue la recherche en sécurité informatique
- Nom et prénom du responsable de l'équipe
- Email du responsable de l'équipe
- Coordonnées de l'équipe
- Code postal du laboratoire
- Site web de l'équipe

Effectifs détaillés de l'équipe

- Effectif total de l'équipe

Toutes les questions suivantes concernent exclusivement la partie du personnel de l'équipe concernée par les travaux liés à la sécurité informatique.

- Nombre d'enseignants-chercheurs permanents de l'équipe concernés par la sécurité informatique
- Nombre d'HDR parmi ces enseignants-chercheurs
- Nombre de chercheurs permanents de l'équipe concernés par la sécurité informatique
- Nombre d'HDR parmi ces chercheurs
- Nombre de personnels techniques permanents (hors personnel administratif) de l'équipe concernés par la sécurité informatique
- Nombre de doctorants de l'équipe concernés par la sécurité informatique
- Nombre de post-doctorants de l'équipe concernés par la sécurité informatique
- Nombre de visiteurs académiques non-permanents de l'équipe concernés par la sécurité informatique
- Nombre de personnels techniques non-permanents de l'équipe concernés par la sécurité informatique

Production scientifique

Toutes les questions ci-dessous concernent la partie de la production scientifique de l'équipe exclusivement relatives à la sécurité informatique, pendant la période de référence 2003-2007

- Nombre d'articles dans des revues internationales a comité de rédaction
- Nombre d'articles dans des revues nationales a comité de rédaction
- Quelles sont les revues internationales et nationales qui intéressent votre thématique sécurité ?

Ce ne sont pas forcément les revues dans lesquelles vous avez publié, mais celles qui caractérisent bien votre communauté et/ou celles dans lesquelles vous avez l'objectif de publier

- Nombre d'articles dans des conférences internationales à comité de sélection
- Nombre d'articles dans des conférences nationales à comité de sélection
- Quelles sont les conférences internationales et nationales qui intéressent votre thématique sécurité ?

  Ce ne sont pas forcément les conférences dans lesquelles vous avez publié, mais celles qui caractérisent bien votre communauté et/ou celles dans lesquelles vous avez l'objectif de publier
- Nombre d'ouvrages écrits
- Nombre d'éditions ou de co-éditions d'ouvrages
- Nombre de contributions à des ouvrages
- Nombre de conférences internationales et nationales organisées par l'équipe
- Nombre de participations aux comités de rédaction de revues internationales et nationales

  Ne compter que les participations en tant que membre officiel des comités. Ne compter qu'une seule fois les participations au même comité reconduites d'une année sur l'autre.
- Nombre de participations aux comités de sélection des conférences internationales et nationales

  Ne compter que les participations en tant que membre officiel des comités. Ne compter qu'une seule fois les participations au même comité reconduites d'une année sur l'autre.
- Nombre d'HDR en sécurité informatique soutenues dans l'équipe
- Nombre de thèses en sécurité informatique soutenues dans l'équipe

Aspects thématiques

Au sein de chaque groupe de thèmes suivants, cochez ceux concernés par vos travaux

- Sécurité logique / Modèles de sécurité
  - Cryptographie symétrique, publique, certificats, architecture de gestion de clés / Cryptanalyse
  - Modèles de confiance
  - Modèles de contrôles d'accès
  - Modèles de sécurité pour les systèmes distribués / pour la grille
  - Protocoles sécurisés d'authentification, de communication, de services
  - Respect de la vie privée, Anonymat, Oubli
  - Sécurité du contenu (tatouage images, video, etc.)
  - Stéganographie / Analyse de canaux cachés
  - Systèmes d'exploitation sécurisés
  - Traçabilité / Maintenance de l'intégrité
- Sécurité des télécommunications / des systèmes
  - Analyse légale / Forensics
  - Prévention et détection d'intrusions
  - Pots de miel
  - Sécurité des réseaux sans-fil
  - Surveillance de systèmes
  - Signaux Parasites compromettants (analyse des causes et solution)
- Analyse / Conception / Specification / Validation / Tests
  - Analyse de code - failles logicielles
  - Analyse du matériel - failles physiques
  - Aspects sociétaux : Economique / Juridique / Ethique / Géostratégie / etc.
  - Patterns pour la sécurité
  - Gestion des risques
  - Mesure de la confiance
  - Méthodologie de conception d'infrastructure et de logiciel sécurisés

Politiques de sécurité
Reporting / Audit d'infrastructure / Certification
Robustesse de la sécurité : Mesure / Analyse
Tests de sécurité
Vérification formelle / Preuve formelle

- Dispositifs de sécurité et application des modèles de sécurité
  Biométrie (visage / rétine / iris / empreintes digitales)
  DRM / Droits numériques : Image / Son / Vidéo
  Modules matériel pour fonctionnement sécurisé (TPM / TSS / Cartes à puce / RFID / FPGA / SOC / etc.)
  PETs (Privacy Enhancing Techniques)
  Sécurité des données embarquées
  Vote numérique

- Si vos thématiques n'apparaissent pas dans la liste ci-dessus, vous pouvez les préciser
  Thématique 1:
  Thématique 2:
  Thématique 3:
  Thématique 4:

Liens recherche / entreprises et recherche / recherche

Toutes les questions ci-dessous concernent exclusivement la thématique sécurité informatique, pendant la période de référence 2003-2007

- Votre équipe participe-t-elle à un ou plusieurs RTRA (Réseaux Thématiques de Recherche Avancée) ?
- Nom des partenaires, type de relation, le type de résultats communs
- Votre équipe participe-t-elle aux pôles de compétitivité ?
- Nom des pôles de compétitivité concernés
- Votre équipe participe-t-elle aux instituts Carnot ?
- Nom des instituts concernés
- Votre équipe participe-t-elle à un ou plusieurs projets nationaux ?
  Par exemple : ANR, RNTL, etc.
- Nom du projet, année de début / fin
- Votre équipe participe-t-elle à un ou plusieurs projets régionaux ?
- Nom du projet, année de début / fin
- Votre équipe participe-t-elle à un ou plusieurs projets industriel ?
- Nom de/des entreprise(s), nom du projet, année de début / fin
- Si vous participez à l'animation de la communauté française en sécurité informatique, précisez sous quelle forme
  (GdR, collaborations régionales, divers comités de pilotage, et.)

Valorisation / Développement

Toutes les questions ci-dessous concernent exclusivement la thématique sécurité informatique, pendant la période de référence 2003-2007

- Nombre de brevets
- Nombres de licences de logiciels
- Nombre de prototypes
- Le cas échéant, site(s) web de(s) prototype(s)
- Votre équipe a-t-elle participé à la création d'une ou plusieurs entreprises ?

- Nom de/des entreprise(s), Date de création, Site web, Nombre d'employés (si toujours en activité)

Lien Recherche / Formation

Toutes les questions ci-dessous concernent exclusivement la thématique sécurité informatique, pendant la période de référence 2003-2007

- Votre équipe est-elle en relation avec une formation liée à la sécurité informatique ?
- Vous pouvez mentionner dans cette page deux formations maximum auxquelles votre équipe participe
- Niveau de la formation
  - Licence / DUT / BTS
  - Master
  - Formation continue / Double compétence
  - Cycle Ingenieur
  - Autre
- Nombre d'étudiants concernés par cette formation
- Volume de la formation en nombre d'heures de face à face pédagogique

  Cela correspond au volume total de la formation en sécurité, indépendamment des enseignements dispensés par votre équipe. Le nombre d'heures éventuellement enseignées est demandé ci-dessous.
- Quel est le type de relation avec cette formation ?
  - Intervention sour forme d'enseignements
  - Gestion administrative
  - Programme Pluri-Formation (PPF)
  - Autre:
- Quel est le type d'enseignement dispensé ?
  - Introduction / Fondamentaux
  - Recherche
  - Technique / Professionnel
  - Travaux pratiques / Plate-formes
- Nombre d'heures dispensées

  En heures équivalent TD

(possibilité de 2 formations)

Liens Société / International

Toutes les questions ci-dessous concernent exclusivement la thématique sécurité informatique, pendant la période de référence 2003-2007

- Etes-vous en relation avec des entités (organismes, association, collectivités, autres) sur les aspects sociétaux liés à la sécurité informatique ?

  (ex. Economique, Juridique, Ethique, Géostratégie, Ergonomie, Responsabilité, Gestion de crises)
- Nom des entités, nature et objectifs de la relation, type de résultats communes (s'il y a lieu)
- Votre équipe participe-t-elle aux réseaux d'excellence ?
- Nom du réseau
- Votre équipe participe-t-elle à un ou plusieurs projets européens ?
- Nom du projet, année de début / fin
- Avez-vous des projets internationaux (autre que projets européens) ?
- Type et nom des projets, nom des partenaires, années de début / fin

- Si vous participez à l'animation de la communauté internationale en sécurité informatique, précisez sous quelle forme

  (Comités de normalisation, comités de programme des conférences ou revues internationales, participation à la programmation projets européens,…)

Prospectives

Parties "Prospectives" sur les 3 à 5 années à venir

Toutes les questions ci-dessous concernent exclusivement la thématique sécurité informatique

- Quelles nouvelles thématiques (par ordre de priorité) souhaitez-vous explorer ?

  Cette question a pour but de déceler les nouvelles tendances afin de les faire émerger et de les encourager

  Thématique 1:
  Thématique 2:
  Thématique 3:
  Thématique 4:
- Quelles sont les thématiques actuelles que vous souhaitez abandonner ? Pour chacune, merci de préciser pourquoi

  Les raisons de l'abandon d'une thématique peuvent sont fondamentales pour cette enquête qui a pour ambition de comprendre la dynamique de la communauté.

  Thématique 1:
  Thématique 2:
  Thématique 3:
  Thématique 4:
- Quelles sont, selon vous, les pistes à explorer pour améliorer l'échange recherche – entreprises ?
- S'il y a lieu, est-ce que vous projetez de participer à la mise en place de formations liées à la sécurité informatique ?
- Pouvez-vous préciser la nature et un échéancier de ces actions
- Projetez-vous de mettre en place des relations fortes avec des entités sur les aspects sociétaux liés à la sécurité informatique ?
- Pouvez-vous préciser la nature et un échéancier de ces actions
- Projetez-vous d'être plus présents dans les actions internationales ?
- Pouvez-vous préciser la nature et un échéancier de ces actions
- De quels types d'outils de coordination et d'animation scientifique (GdR, divers types de réseaux) pensez-vous que l'on doive disposer en France pour la sécurité informatique ? Merci de préciser en quoi ces nouveaux outils vont améliorer l'existant.
- Quels éventuelles actions futures pour mieux capitaliser les compétences des équipes françaises (projets collaboratifs, plateforme d'expérimentation, outils de développement commun,…) pensez-vous nécessaires ou prometteuses, ou au contraire inutiles ?

Compléments

- Vous pouvez mentionner ci-dessous des éléments complémentaires que vous jugez utiles pour cette enquête.