ACI «Sécurité & Informatique»

Présentation et bilan 2004

Le Ministère délégué à la Recherche et aux Nouvelles Technologies (MRNT) a créé en 2003 une Action Concertée Incitative (ACI) intitulée « *Sécurité & Informatique* », en collaboration avec le département Sciences et Technologies de l'Information et de la Communication du CNRS, avec l'INRIA et à partir de cette année avec la DGA.

Conformément à l'esprit des ACI, cette action vise essentiellement à développer une recherche amont et s'inscrit donc en complémentarité des différents réseaux de recherche et d'innovation technologique (RRIT), en particulier le RIAM, le RMNT, le RNRT, le RNTL ou le RNTS dont l'objectif principal est de développer les interactions entre recherche académique et entreprises.

Le présent document présente cette ACI, ses objectifs scientifiques, son mode de fonctionnement avec en particulier son comité de pilotage et son conseil scientifique, l'appel à propositions 2004 et les projets labellisés en 2004.

Sous l'impulsion du Conseil Scientifique, une véritable animation scientifique de l'ACI a démarré :

- Les premières journées scientifiques de l'ACI se sont déroulées les 11 et 12 décembre 2003 à Rennes, http://www.irisa.fr/manifestations/2003/ACI/.
- En 2004, ces journées sont organisées à Toulouse du 15 au 17 novembre, http://www.laas.fr/ACISI2004.
- Un site web de l'ACI, http://aciSI.loria.fr, a été mis en place pointant en particulier sur les pages de l'ensemble des projets labellisés par l'ACI en 2003 et en 2004. On peut également y trouver les brochures de description des activités de l'ACI 2003 et 2004.
- Le suivi des projets est assuré par 2 membres du conseil scientifique.

Table des matières.

Objectifs scientifiques.

L'objectif de cette ACI est de fortement dynamiser la recherche sur l'ensemble des aspects de la sécurité et de la sûreté des systèmes informatiques, des systèmes informatisés, des systèmes d'information, en prenant en compte leurs dimensions juridiques

Informatique et sécurité sont aujourd'hui indissociables et à la confluence entre des disciplines scientifiques comme les mathématiques, la physique, la logique, l'informatique, l'automatique et le traitement du signal, tout en ayant de très fortes interactions avec le droit individuel, national et international.

Les réseaux et systèmes informatiques prennent un rôle et une place chaque jour plus importants dans tous les aspects des activités humaines. Les situations multiples dans lesquelles il est indispensable de savoir définir et garantir leur sécurité concernent aussi bien les activités professionnelles qu'associatives ou personnelles. La sécurité se décline alors de nombreuses manières, par exemple dans le cadre des transactions électroniques mais également dans la protection des données, des informations, des personnes et des biens. Dans ce contexte, la sécurité comprend en particulier celle des systèmes, des logiciels, des protocoles, des architectures globales, des composants matériels, des réseaux tant filaires ou optiques que radios, des équipements d'extrémités, des moyens de stockage de l'information. Le caractère distribué, ouvert, mobile, ubiquitaire, de beaucoup de systèmes complexifie grandement le problème et la recherche de solutions.

Par ailleurs, la sécurisation des systèmes d'information repose sur de nouvelles techniques de sécurisation algorithmique d'une part, mais aussi sur des principes physiques comme la cryptographie quantique ou la cryptographie par chaos. On s'intéresse alors à l'étude et à l'élaboration de principes physiques théoriques, ou encore à la réalisation de démonstrateurs faisant appels à des principes originaux.

L'informatique a un rôle crucial dans la sûreté de fonctionnement des systèmes technologiques critiques et/ou complexes, tels que les centrales nucléaires, les avions et engins spatiaux, les systèmes industriels de production continue (électricité, pétrole, chimie, métallurgie, sidérurgie), les grands ouvrages de génie civil (barrages, ponts, plateformes pétrolières), les véhicules et les infrastructures des systèmes de transport routiers et ferroviaires. En raison de la diffusion massive de capteurs de toutes natures, ces systèmes bénéficient à l'heure actuelle d'une instrumentation conséquente, et leur sûreté de fonctionnement passe par la conception d'algorithmes de traitement in-situ des données numériques ainsi disponibles. Sur la base des informations et connaissances disponibles (instrumentation, modèles), il s'agit alors en particulier d'opérer une véritable perception (détection, localisation, diagnostic) et réaction (correction, tolérance, maintenance) par rapport aux événements imprévus ou d'évolutions ou de déviations par rapport à un état ou un comportement de référence normal, souhaitable ou nominal. Les événements et déviations en question concernent aussi bien le système proprement dit que son environnement humain et technique, en particulier les infrastructures informatiques.

La sécurité informatique peut être un moyen de pallier les difficultés de faire respecter un droit ou une obligation (e.g. dispositifs de protection de la vie privée, sécurité anti-contrefaçons, ...). Pour renforcer le dispositif, le droit intervient alors pour sanctionner les atteintes aux systèmes de sécurité. Cette approche qui consiste à superposer une couche juridique et une couche technique pose de nombreuses difficultés qui nécessitent de proposer de nouveaux modèles d'interaction entre droit et sécurité informatique. Par ailleurs, l'archivage et la pérennisation des contenus numériques font émerger des enjeux juridiques qui sont étroitement liés aux choix techniques en matière de sécurité (charge de la preuve, présomptions, tiers de confiance, ...). Les croisements entre droit et sécurité se retrouvent aussi dans les pratiques et les usages des outils assurant la sécurité; il faut alors se poser la question de la complémentarité dans les réponses juridiques et techniques.

Dans ce contexte scientifique et dans un cadre international très actif tant du point de vue académique qu'industriel, l'ACI sollicite des projets novateurs, se situant au meilleur niveau international et contribuant à faire avancer significativement la recherche dans les domaines mentionnés plus haut et à renforcer ainsi la place de la France dans cette thématique de recherche sur les scènes européenne et internationale.

Organisation et fonctionnement.

L'organisation et le fonctionnement de l'ACI Sécurité Informatique sont basés sur la coopération d'un Comité de Pilotage et d'un Conseil Scientifique. Le Comité de Pilotage, comprenant les représentants des divers partenaires de l'ACI, est la seule entité décisionnelle. Il choisit le Conseil Scientifique, valide l'appel à propositions, rédigé en collaboration avec le Conseil Scientifique, labellise les projets et définit leurs financements après expertise par le Conseil Scientifique. L'ensemble des décisions du Comité de Pilotage est soumis à l'approbation de la Directrice de la Recherche du Ministère en charge de la recherche.

Le comité scientifique analyse le contexte scientifique et propose des directions d'action. Il évalue les propositions de projets et propose au comité de pilotage les propositions à labelliser. Il suit les projets financés dans leur réalisation et leurs résultats. Il organise les journées annuelles de l'ACI.

L'articulation entre les deux structures est assurée par la présence du président du Conseil Scientifique dans le Comité de Pilotage.

Comité de pilotage 2004 :

- **Michel BIDOIT**, MRNT, président du Comité de Pilotage
  (suppléant : Michel ADIBA, MRNT)

- **Pascal CHAUVE**, DGA

- **Serge FDIDA**, CNRS-DSTIC

- **Daniel HAUDEN**, MSTP
  (suppléante : Véronique DONZEAU-GOUGE, MSTP)

- **Gilles KAHN**, INRIA
  (suppléant : Jean-Jacques LEVY, INRIA)

- **Claude KIRCHNER**, président du Conseil Scientifique

- **Antoine PETIT**, CNRS-DSTIC
  (suppléant : Luis FARINAS, CNRS-DSTIC)

- **Jean-Pierre VERJUS**, INRIA

Conseil Scientifique 2004 :

Claude KIRCHNER (Président du Conseil Scientifique)
Directeur de recherche INRIA, Nancy

Michèle BASSEVILLE
Directrice de recherche CNRS, Rennes

Pascale CHARPIN
Directrice de recherche INRIA, Rocquencourt

Jean-Marc CHASSERY
Directeur de recherche CNRS, Grenoble

Jean GOUBAULT-LARRECQ
Professeur, ENS de Cachan

Frédéric CUPPENS
Professeur ENST Bretagne, Rennes

Michel DIAZ
Directeur de recherche CNRS, Toulouse

Laurence DUCHIEN
Professeure, Université des Sciences et Technologies de Lille

Nicolas HALBWACHS
Directeur de recherche CNRS, Grenoble

Isabelle de LAMBERTERIE
Directrice de recherche CNRS, Ivry

Laurent LARGER
Maître de conférences, Université de Franche-Comté

Régis LEVEUGLE
Professeur, INP Grenoble

Alain MERLE
CEA LETI Grenoble

Refik MOLVA
Professeur, EURECOM Sophia-Antipolis

David POWELL
Directeur de recherche CNRS, LAAS Toulouse

Pascal URIEN
Professeur, ENST, Paris

Françoise SIMONOT
Professeure, Ecole des Mines de Nancy

Appel à propositions 2004.

Cet appel a encouragé et a considéré toute proposition originale.

L'appel à proposition a mis en avant qu'une attention particulière serait portée aux projets visant à développer les thèmes suivants:

• l'émergence et le suivi d'une législation garantissant à la fois le respect de la vie privée, les souverainetés nationales et les échanges internationaux basés sur une confiance réciproque démontrable,

• les recherches duales (i.e. civile et militaire),

• la vérification, la validation, le test, la mesure et l'évaluation de la sécurité et la sûreté de fonctionnement des systèmes informatiques,

• les mécanismes et algorithmes en ligne destinés à améliorer la sûreté et la sécurité des systèmes et des réseaux.

• la sécurisation des couches basses des systèmes informatiques.

Par ailleurs les communautés scientifiques en droit, électronique, optique, automatique, traitement du signal ont été également encouragées à répondre à cet appel.

Types de projets.

Les projets attendus, d'une durée maximale de 36 mois, étaient de plusieurs types :

- *Projet de recherche* : sur un domaine commun d'expertise clairement défini, basé sur la coopération active d'un nombre limité d'équipes.

- *Projet de recherche multi-thématique* : basé sur la coopération active d'équipes de recherche relevant de champs disciplinaires différents. Le projet proposera un programme de recherche commun, pluridisciplinaire, basé sur la complémentarité des équipes participantes.

- *Projet de recherche avec infrastructure* : grâce à son financement conséquent, cette ACI peut être l'occasion de monter des projets de recherche nécessitant l'acquisition d'équipements hors de portée des financements classiques. De tels projets, s'appuyant sur un programme de recherche commun, devront être particulièrement argumentés. Le problème des moyens humains indispensables à l'utilisation et la maintenance des équipements devra être abordé, en explicitant les demandes faites dans le cadre de l'ACI et, le cas échéant, les autres apports.

Une attention particulière a été apportée aux projets susceptibles de fournir des solutions globales aux problèmes posés en favorisant les collaborations et les synergies entre chercheurs d'équipes ou de structures différentes.

Bilan de la campagne 2004.

Globalement le conseil scientifique a trouvé l'ensemble des propositions de bon à excellent. Ce sont 41 propositions qui ont été reçues. Chacune d'elle a été confiée à deux membres du Conseil Scientifique qui ont, ensemble, choisi 3 autres experts (dont au moins deux étrangers) chargés d'évaluer en détail le dossier. Ce choix s'est effectué au cours d'une réunion physique de l'ensemble du Conseil Scientifique. Il a été mis en oeuvre via l'utilisation d'un serveur web sécurisé développé spécifiquement pour l'évaluation des propositions ACI et permettant de gérer les soumissions et leurs évaluations. Les rapports des experts ont été, pour leur partie non confidentielle, transmis aux porteurs de toutes les propositions soumises.

En s'appuyant sur ces évaluations extérieures et son propre jugement, chaque membre du Conseil Scientifique a proposé une synthèse sur chacune des propositions dont il avait la charge. Une réunion physique du Conseil Scientifique lui a permis de proposer des projets à la labellisation au Comité de Pilotage ainsi qu'un premier cadrage financier.

Afin d'éviter un émiettement des engagements due au nombre important de sollicitations et, il faut le dire, à la faiblesse des financements de certains appels, le conseil scientifique souligne que les participants aux projets ACI doivent veiller à ce que leur implication soit réaliste et compatible avec leurs autres engagements effectifs ou planifiés. En particulier, il semble nécessaire que le temps de recherche effectif consacré à un projet ACI soit supérieur à 20% et donc pour un enseignant-chercheur supérieur à 40% de son temps de recherche.

L'ensemble des projets proposés à la labellisation ont été retenus par le Comité de Pilotage (aucun projet non proposé par le Conseil Scientifique n'a été labellisé par le Comité de Pilotage), parfois en adaptant les subventions proposées.
Ainsi, 19 propositions de projets ont finalement été labellisées :

- 17 relevant de la catégorie *Projet de recherche* :

  ACSION ; ALIDECS ; APRON ; BEHAVIOUR ; CADHO ; DADDI ; FIACRE ; FRAGILE ; KAA ; MARS ; MOSAIC ; POTESTA ; SATIN ; SERAC ; SR2I ; TADORNE ; VENUS

- 2 relevant de la catégorie *Projet de recherche multi-thématique* :

  ASPHALES ; METROSEC

Classification thématique des projets 2003 et 2004.

La classification par grand thème proposée ci-dessous ne doit donc pas être prise de façon stricte ou restrictive et vise à donner une première idée de la nature des projets qui ont été retenus.

(en *italique* les projets 2003 .; en MAJUSCULE les projets 2004)

Bases de données sécurisées :

CASC

Biométrie :

BIO_MUL

Construction de logiciels sûrs :

CoRSS ; DESIRS ; DISPO ; GECCOO ; MODULOGIC
ALIDECS ; FIACRE

Cryptographie :

CESAM ; CHRONOS ; OCAM ; ROSSIGNOL ; UNIHAVEGE
ACSION

Fiabilité des systèmes répartis :

FRAGILE ; MOSAIC

Intrusion :

CADHO ; DADDI

Informatique pour la sûreté et la sécurité :

CO*NSTRUCTIF ; EDEMOI*
BEHAVIOR

Matériel et sécurité :

MARS ; VENUS

Marquage :

TADORNE

Objets mobiles :

CRISS ; SPOPS
KAA

Politiques de sécurité :

POTESTA

Preuve, vérification :

CORTOS ; DYNAMO ; PERSEE ; SURE PATHS ; VERA ; VERSYDIS
APRON ; SATIN

Réseaux :

PRESTO ; Réseaux Quantiques ; SPLASH ; TRANSCHAOS
METROSEC ; SERAC ; SR2i

Sécurité et droit :

FABRIANO
ASPHALES

Financements.

Les moyens humains et financiers alloués à l'ensemble des projets sont les suivants (pour l'ensemble des 3 ans pendant lesquels ils se déroulent) :

- **4 400 K€** (dont 20 CDD et 25% qui ont été utilisés pour de l'équipement) via le FNS
- **7 allocations** de recherche du MRNT

Quelques ressources supplémentaires (post-doc, accueils d'enseignants-chercheurs, …) pourront être accordés pendant le déroulement des projets, au gré des demandes individuelles qui seront faites directement aux organismes.

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
ACSION	**PROJET DE RECHERCHE**

Titre du projet :

Nouvelles applications du codage correcteur d'erreurs à la sécurité de l'information

Description courte du projet :

Nous nous proposons dans ce projet de fédérer les connaissances complémentaires des partenaires du projet dans le domaine des codes d'erreurs et de la cryptologie, afin d'explorer des nouvelles applications du premier domaine au second. Nous nous attacherons notamment à :

1) Développer des cryptanalyses de systèmes de chiffrement en utilisant des techniques de décodage de codes correcteurs d'erreurs. Nous avons déjà commencé cette étude dans le cadre d'une ACI cryptologie précédente et proposé de telles cryptanalyses pour certains systèmes de chiffrement par flot. Nous proposons ici, à la fois d'améliorer les performances de nos cryptanalyses, mais aussi d'étendre le champ d'applications de celles-ci à certains systèmes de chiffrement par bloc et à d'autres systèmes de chiffrement par flot.
2) Développer des systèmes d'authentification de données ou d'identité utilisant des codes correcteurs d'erreurs. Nous pensons en particulier à des schémas d'identification ou de révocation de jeux de clés piratées dans le cadre de la diffusion chiffrée, ou encore de systèmes d'identification fondés sur des données biométriques, lesquelles ne peuvent s'intégrer que dans des protocoles tolérant des variations de mesure

Coordinateur du projet

Nom	Prénom	Laboratoire
TILLICH	Jean Pierre	Projet CODES, INRIA Rocquencourt

Equipes ou laboratoires partenaires

(Partenaire 2) GUILLOT Philippe	MAATICAH Université Paris 8
(Partenaire 3) ZEMOR Gilles	Laboratoire Traitement et Communication de l'information LTCI - ENST

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	12 k€	14 k€	8 k€		34 k€
Partenaire 2	9 k€	9 k€			18 k€
Partenaire 3	20 k€	25 k€			45 k€
Total	41 k€	48 k€	8 k€		97 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
				0

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
ALIDECS	**PROJET DE RECHERCHE**

Titre du projet :

Langages et Atelier Intégré pour le Développement de Composants Embarques Surs

Description courte du projet :

Ce projet s'adresse aux systèmes embarqués critiques de grande taille, pour lesquels la réutilisation devient un problème crucial. Le projet a pour objectif l'étude d'un atelier intégré pour le développement et l'utilisation de composants embarqués surs. L'usage d'un langage adéquat contribuant pour une large part à la sûreté des systèmes informatiques, nous privilégions ici une approche ``langage'' des aspects suivants: --- support au cycle de vie, depuis les phases initiales de spécification jusqu'au code embarqué efficace; --- mécanismes de composition modulaires utilisables aussi bien dans les programmes, dans leurs spécifications, dans la description des environnements; --- validation précoce des assemblages de composants; --- validation précoce du comportement dynamique des systèmes par simulation des programmes et des spécifications, tout au long des phases de développement; la possibilité d'exécuter des programmes incomplets est un des objectifs prioritaires. L'approche proposée consiste à batir un ensemble de langages, et leurs outils associés, sur un socle sémantique commun. Nous choisissons le modèle mathématique synchrone, qui fournit une sémantique simple de la concurrence et du temps. Il a été utilisé avec succès dans la définition de langages et outils industriels (e.g, Scade, Sildex, Esterel) pour la programmation de systèmes de contrôle/commande critiques. Il permet déjà, dans un cadre unifié, de décrire et composer programmes et propriétés. Il est suffisamment général pour décrire d'autres modèles de concurrence (en particulier asynchrones) et combiner des objets déterministes et non-déterministes. Nous définirons dans ce cadre commun un ensemble de langages pour: la programmation, la spécification des programmes et des environnements, la description des assemblages, les propriétés des assemblages. Par ailleurs nous étudierons l'application de méthodes de validation de manière très précoce dans le cycle de vie: validation des assemblages, validation d'un composant pour un environnement donné, etc. Nous proposons de formuler ces nouveaux problèmes de validation en termes exploitables par les techniques de vérification existantes, et de prévoir une interface de l'atelier avec les outils existants. Le projet s'appuie sur les compétences des équipes du projet dans les domaines de la programmation synchrone; de la sémantique et de l'implantation de langages pour les systèmes embarqués; des outils de validation et de simulation de systèmes.

Coordinateur du projet

Nom	Prénom	Laboratoire
M. POUZET	Marc	SPI - Laboratoire d'Informatique de Paris 6 (LIP6)

Equipes ou laboratoires partenaires

(Partenaire 2) Maraninchi Florence	VERIMAG (VERIMAG)
(Partenaire 3) Fradet Pascal	INRIA Rhone-Alpes (INRIA)
(Partenaire 4) Boussinot Frederic	INRIA Sophia-Antipolis (INRIA)
(Partenaire 5) Delosme Jean-Marc	CMOS - LaMI (LaMI)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	12 k€	34 k€			46 k€
Partenaire 2	12 k€	39 k€			51 k€
Partenaire 3	17 k€	25 k€			42 k€
Partenaire 4	4 k€	15 k€			19 k€
Partenaire 5	8 k€	11 k€			19 k€
Total	53 k€	124 k€			177 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
APRON	**PROJET DE RECHERCHE**

Titre du projet :

Analyse de PROgrammes Numériques

Description courte du projet :

Ce projet réunit cinq équipes travaillant sur l'interprétation abstraite des programmes, et se fixe pour but de faire sauter les verrous actuellement rencontrés par les techniques d'analyse statique existant pour: - vérifier statiquement des propriétés de sûreté et sécurité, - et identifier les causes d'erreur. Pour passer la barrière de la calculabilité, il est indispensable de faire appel à des analyses approchées. Mais la précision des analyses doit être améliorée pour réduire une zone d'incertitude qui peut atteindre plus de 98% d'un code avec des produits commerciaux. Les temps et les espaces d'exécution doivent être simultanément contrôlés : une analyse durant plus d'une nuit et nécessitant plus de 4GB d'espace ne peut pas être utilisée industriellement comme une analyse qui se termine en 5 minutes sur un PC. Les verrous identifiés se placent aux niveaux conceptuel (Comment traiter les nombres flottants? Comment prendre en compte les non-linéarités? Comment gérer automatiquement un compromis entre vitesse et précision en choisissant le domaine abstrait le plus adapté, en modifiant le partitionnement selon les points de contrôle, en ajoutant des variables auxiliaires pour mémoriser l'historique des calculs, et en modulant le nombre de contextes d'analyse d'une procédure?), technologique (Comment écrire un multi-analyseur indépendamment des abstractions utilisées? Comment peut-on utiliser un domaine abstrait défini par une autre équipe?) et expérimental (Comment peut-on définir des benchmarks en analyse statique ou sur des domaines abstraits?). L'accent est mis sur les programmes comportant d'important aspects numériques (calculs en flottants, compteurs, indices de tableaux) et pour lesquels les méthodes de vérification fondées sur des modèles d'états finis sont inopérantes. L'objectif est aussi d'analyser des programmes de taille réelle (100 à 500 KLOCs), composés de plusieurs milliers de procédures. Des interpréteurs abstraits adaptatifs sont indispensables pour fournir la précision et l'efficacité que de telles applications nécessitent.

Coordinateur du projet

Nom	Prénom	Laboratoire
IRIGOIN	François	Centre de recherche en Informatique, Ecole des mines de Paris (CRI/ENSMP)

Equipes ou laboratoires partenaires

(Partenaire 2) HALBWACHS Nicolas	Verimag (VERIMAG)
(Partenaire 3) JEANNET Bertrand	Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA)
(Partenaire 4) COUSOT Patrick	ENS - Département d'Informatique (DI)
(Partenaire 5) COUSOT Radhia	Ecole Polytechnique (STIX) Sciences et Technologies de l'Information et de la Communication

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	15 k€	75 k€			90 k€
Partenaire 2	10 k€	50 k€			60 k€
Partenaire 3	5 k€	25 k€	7,2 k€		37,2 k€
Partenaire 4		45 k€		46,4 k€	91,4 k€
Partenaire 5		45 k€		46,4 k€	91,4 k€
Total	30 k€	240 k€	7,2 k€	92,8 k€	370 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 3	chercheur	100 %	12 mois	46,4 k€
Partenaire 4	chercheur	100 %	12 mois	46,4 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur
Partenaire 5	1		

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
ASPHALES	**PROJET DE RECHERCHE**

Titre du projet :

Les interactions entre sécurité informatique et sécurité juridique dans les chantiers normatifs de la Société de l'information.

Description courte du projet :

Le droit est un des moyens de créer la confiance, la sécurité informatique est un des outils pour assurer cette confiance. Comment trouver un bon équilibre entre le besoin de reconnaissance de la fiabilité d'une technique de sécurisation et un encouragement à la recherche de nouveaux procédés aptes à répondre à ce besoin de sécurité indispensable au bon développement de la société de l'information? La démarche proposée se fera en 3 étapes: I - Sensibiliser, par une "mise à plat" des textes juridiques encadrant la société de l'information et des politiques qu'ils induisent, les deux communautés (juristes et informaticiens) aux différentes "lectures" des cadres normatifs actuels ou en préparation. Le résultat de cette lecture sera un " livre blanc " regroupant tous les textes étudiés avec les commentaires sur les demandes de sécurité technique II - Etudier - à travers des questions transversales dégagées (ou confirmées) à l'issu de la première étape - les problèmes posés par les interactions entre les réponses techniques et les cadres juridiques (indépendance ou interdépendance ?) III - La troisième étape aura un triple objectif: (1) tirer de l'étude des questions transversales et de la mise à plat des textes juridiques les domaines où ces questions génèrent des besoins en recherche informatique (2) au-delà de la lecture critique du droit existant, une analyse de lege ferenda, (du droit qui se construit), permettra de proposer quelques suggestions concrètes étayées par les résultats déjà obtenus (3) L'organisation d'un colloque ouvert aux deux communautés scientifiques exposant les résultats du travail réalisées au cours du projet serait l'occasion de tirer tous les enseignements (y compris épistémologiques) du travail mené ensemble. Le projet regroupe des équipes mixtes (juristes et informaticiens) ayant chacune une spécialité en droit des technologies de l'information ou en informatique: INT - LEDUTIC (réseaux de communications électroniques, biométrie) Lille - IREENAT/ LIFL(Ordre public et Protection de la vie privée) Versailles-Saint Quentin en Yvelines- Dante (sécurité de l'économique numérique : contrats et responsabilité) Paris XI- CERDI (propriété intellectuelle en lien avec les techniques numériques) Montpellier I-ERID (Les droits de la personne dans la société de l'information) CECOJI/INRIA (Valeur probatoire et archivage). Le projet sera coordonné par le CECOJI sous la responsabilité d'I.de Lamberterie

Coordinateur du projet

Nom	Prénom	Laboratoire
DE LAMBERTERIE	Isabelle	Centre d'études sur la coopération juridique internationale-CNRS

Equipes ou laboratoires partenaires

(Partenaire 2) Lavenue Jean-Jacques	Institut de REcherche sur l'Evolution Normatif des Activités Transnationales
(Partenaire 3) Strubel Xavier	Transversalité et Multidisciplinarité Appliquée aux TIC (TEMATIC) (LEDUTIC)
(Partenaire 4) Bibent Michel	Equipe de Recherche Informatique et droit EA 2997 (ERID)
(Partenaire 5) Benabou Valérie-Laure	Droit des Affaires et Nouvelles Technologies jeune équipe (DANTE)
(Partenaire 6) Latreille Antoine	Centre d'études et de recherche en droit de l'immatériel
(Partenaire 7) Canteaut Anne	INRIA projet CODES

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	3,6 k€	65 k€	9,76 k€	46,8 k€	125,16 k€
Partenaire 2	41,4 k€	30 k€	25 k€	46,8 k€	143,2 k€
Partenaire 3	4 k€	16,4 k€		33 k€	53,4 k€
Partenaire 4		6 k€	21 k€		27 k€
Partenaire 5		9 k€	22 k€		31 k€
Partenaire 6		3 k€	18 k€		21 k€
Partenaire 7	3		21,24 k€		24,24 k€
Total	52 k€	129,4 k€	117 k€	126,6 k€	425 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 1 Coordinateur	chercheur	100 %	12 mois	46,8 k€
Partenaire 2	chercheur	100 %	12 mois	46,8 k€
Partenaire 3	chercheur	100 %	12 mois	33 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur
Partenaire 2	1		
Partenaire 6	1		

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
BEHAVIOUR	**PROJET DE RECHERCHE**

Titre du projet :

Vision et apprentissage statistique pour la reconnaissance du comportement humain; application à la surveillance du conducteur pour l'amélioration de la sécurité de la conduite automobile.

Description courte du projet :

Différentes études menées récemment au niveau international en matière de sécurité routière ont montré que les états de somnolence et d'inattention du conducteur influent sensiblement sur la sécurité de la conduite automobile. On estime que les accidents mortels de la route sont liés à la somnolence du conducteur à hauteur de 10 à 20 % ainsi qu'à sa distraction due notamment à la prolifération de technologies à bord du véhicule (téléphone cellulaire, cartes de navigation GPS, etc.). L'amélioration de la sécurité routière étant un enjeu socio-économique majeur, les pouvoirs publics et les constructeurs automobiles sont ainsi amenés à évaluer l'impact réel de la somnolence et de l'inattention du conducteur sur la sécurité de la conduite automobile. Les travaux en vision par ordinateur relatifs au domaine automobile comportent deux volets qui sont l'analyse de l'environnement extérieur au véhicule d'une part et l'analyse de l'activité dans l'habitacle d'autre part. La majeure partie des travaux de vision se sont jusqu'à présent portés sur le premier volet en couvrant notamment les problématiques de suivi de trajectoire, de détection d'obstacles ou encore d'analyse du véhicule précédent. Pour ce qui concerne l'analyse de l'intérieur du véhicule, les travaux ont essentiellement consisté à détecter et mesurer les battements de paupières et la direction du regard du conducteur. Aujourd'hui, il apparaît important de pouvoir dépasser ce stade en l'enrichissant de l'analyse automatique des comportements, dans plusieurs buts : affiner l'estimation de l'état du conducteur (par la détection des bâillements, orientation de la tête, clignement des yeux et regard, expressions faciales, gestes auto-centrés, posture, mains sur le volant, etc.), et accéder à des périodes de distraction (manipulation d'objets, etc.). Le mode opératoire de ces analyses, qui est aujourd'hui manuel et peut nécessiter un traitement image par image selon le geste traqué, les rend coûteuses et sujettes à la subjectivité. L'objectif du projet est ainsi de proposer une automatisation (et objectivation) des étiquetages des comportements observés lors de séquences de conduite. Celle-ci présente un intérêt marqué, que ce soit pour la conception de systèmes de surveillance embarqués en temps réel ou pour l'analyse de l'impact de nouvelles fonctions ou nouvelles interfaces sur l'activité de conduite. En outre, tandis que les techniques existantes se concentrent sur une vue frontale rapprochée du visage du conducteur, nous exploiterons également des vues secondaires disponibles (telle qu'une vue latérale plus large). L'annotation automatique sera conçue sur des séquences vidéo de conduite réelle et en simulateur, et évaluée par rapport aux comportements déjà étiquetés par des éthologues. Nous exploiterons pour cela les avancées récentes dans les domaines de la vision par ordinateur, de la reconnaissance de formes, de l'apprentissage, de l'inférence statistique et de la fusion. Une attention particulière sera portée à l'analyse statistique du mouvement, au suivi robuste multi-objets, à l'apprentissage de modèles probabilistes à partir d'un nombre limité de données, à la gestion de l'incertain et à la fusion ainsi qu'à l'inférence dans des espaces de dimensions élevées.

Coordinateur du projet

Nom	Prénom	Laboratoire
DAVOINE	Franck	Heuristique et Diagnostic des Systèmes Complexes (HEUDIASYC)

Equipes ou laboratoires partenaires

(Partenaire 2) PEREZ Patrick	Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA)
(Partenaire 3) MILLEMANN Sylvain	PSA Peugeot Citroën (PSA Peugeot Citroën)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	6 k€	35,5 k€	13,5 k€		55 k€
Partenaire 2	5 k€	20,5 k€	4,5		30 k€
Partenaire 3	0	0			0 k€
Total	11 k€	56 k€	18 k€		85 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur
Partenaire 1 Coordinateur	1		

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
Cadho	**PROJET DE RECHERCHE**

Titre du projet :

Collecte et Analyse de Données issues de HOneypots

Description courte du projet :

Le projet CADHo s'intéresse à la collecte, l'analyse et l'interprétation de données réelles permettant de mieux comprendre les attaques contre des systèmes informatiques et de modéliser leur impact sur la sécurité. Le projet vise un triple objectif. Premièrement, nous comptons définir et déployer un environnement distribué de collecte de données basé sur la notion de pots de miel. Cet environnement, stable et en fonctionnement 24 heures sur 24, 7 jours sur 7, sera mis à la disposition de la communauté scientifique désireuse d'analyser les processus d'attaques présents sur l'Internet. Il sera déployé dans un premier temps chez les trois membres du projet, et à terme chez le plus grand nombre de partenaires possibles en les incitant à s'intéresser à cette problématique importante, selon un principe d'échange volontaire réciproque détaillé dans la proposition. Deuxièmement, nous développerons une méthodologie d'analyse des données issues des pots de miel pour identifier des tendances et modéliser des processus d'attaques en s'appuyant sur les données collectées. En cela, nous continuerons et enrichirons les premiers résultats obtenus sur un environnement très simplifié utilisé depuis un an au sein du seul site de l'institut Eurecom. Enfin, nous définirons et utiliserons un environnement de pots de miel plus sophistiqués, dits de haute interaction, pour pousser plus avant l'étude des méthodes d'attaque en laissant les pirates prendre apparemment le contrôle de nos pots de miel et en observant leurs faits et gestes une fois ces machines compromises. Cette dernière étude, de par les problèmes techniques et légaux qu'elle nécessite de résoudre au préalable, sera menée dans la seconde phase de ce projet, sur un nombre limité de réseaux très contrôlés.

Coordinateur du projet

Nom	Prénom	Laboratoire
DACIER	Marc	Institut Eurécom (Eurecom)

Equipes ou laboratoires partenaires

(Partenaire 2) KAANICHE Mohamed	Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS-CNRS)
(Partenaire 3) Kortchinsky Kostya	GIP RENATER (CERT RENATER)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	72,4 k€	30,915 k€		44,085 k€	147,4 k€
Partenaire 2	45,6 k€	12,488 k€		36,912 k€	95 k€
Partenaire 3	27 k€	13,6 k€			40,6 k€
Total	145 k€	57,003 k€		80,997 k€	283 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 1 Coordinateur	Ingénieur	100 %	12 mois	44,085 k€
Partenaire 2	Post-doctorant	100 %	12 mois	36,912 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
DADDi	**PROJET DE RECHERCHE**

Titre du projet :

Détection sûre de fonctionnement de nouvelles formes d'intrusions

Description courte du projet :

Tous les jours, les bases recensant les vulnérabilités des systèmes d'information s'enrichissent de nouveaux cas. Ainsi, depuis plusieurs années, le nombre de vulnérabilités nouvelles découvertes chaque année est compris entre 1000 et 2000. S'offrent alors aux attaquants potentiels 3 à 6 nouvelles vulnérabilités par jour, qu'ils peuvent exploiter de diverses manières. Les administrateurs de sécurité ont donc continuellement à faire face à de nouvelles formes d'intrusion. En complément aux outils préventifs, des outils de détection d'intrusions (IDS) sont aujourd'hui couramment utilisés par les administrateurs de sécurité, pour détecter l'occurrence d'attaques contre leurs systèmes. Toute approche implantée dans un IDS et qui ne permet de détecter que des attaques déjà répertoriées se heurte aux problèmes des nouvelles formes d'attaques. Il faut donc que le répertoire d'attaques connues (la base de signatures) soit mis à jour en temps réel. Cette approche, dite par analyse de signatures d'attaque, est similaire à celle qui est utilisée dans les anti-virus, où elle montre ses limites puisqu'il y a toujours aujourd'hui des milliers de machines qui restent victimes de virus ou de vers. Ces derniers sont en outre de plus en plus rapides dans leur expansion, limitant ainsi les capacités de réactions humaines. Ainsi, le ver Slammer a atteint en quelques minutes la quasi-totalité des serveurs MsSQL du monde, infectant ainsi plus de 100000 machines. Face à ce problème, l'approche de détection qualifiée de comportementale, souvent présentée comme la seule approche permettant de détecter de nouvelles formes d'attaques, trouve tout son intérêt. Le principe de base de l'approche comportementale est de construire un modèle de référence du comportement de l'entité surveillée (utilisateur, machine, service, application) auquel on peut comparer le comportement observé. Si ce dernier s'éloigne trop de la référence, une alerte est émise pour signaler l'anomalie. Le premier objectif de cette ACI est de proposer de nouvelles approches comportementales. Les approches classiques proposent un modèle de référence explicite : suite d'appels système autorisés, valeurs statistiques acceptables pour un ensemble de variables d'observation données, etc. Cette approche explicite pose plusieurs problèmes. Tout d'abord, il n'est pas simple de définir ce qui est explicitement représentatif du comportement à modéliser. Ensuite, il faut tenir compte des évolutions normales de comportement de l'entité surveillée. Améliorer les approches explicites, notamment en traitant ces deux problèmes, est donc le premier objectif du projet. Notre second objectif est l'étude d'une approche dans laquelle le modèle de référence est implicite, contournant par là même ces deux problèmes. Cette dernière approche s'inspire d'une méthode classique en sûreté de fonctionnement, la diversification fonctionnelle. Il s'agit de confier le traitement d'une même requête à plusieurs modules implantant la même fonctionnalité de manière différente. Toute divergence dans les résultats obtenus est alors interprétée comme une possible corruption d'un ou de plusieurs modules (ou des systèmes qui les hébergent) auxquels le traitement de la requête a été confié. Un problème récurrent de la détection d'intrusions est la résistance aux attaques des mécanismes de détection. En effet, le premier objectif de l'attaquant est souvent de mettre hors service le système de détection. Dans ce projet, nous étudions la sûreté de fonctionnement de l'IDS en lui apportant des propriétés de tolérance aux intrusions. Il s'agit là de notre troisième objectif. Enfin, quel que soit leur principe de base, les approches comportementales existantes présentent un grave inconvénient : elles permettent de déterminer que quelque chose d'anormal s'est produit, mais elles ne permettent pas de diagnostiquer la cause de l'anomalie. On doit donc lui adjoindre une analyse supplémentaire des anomalies signalées, en particulier pour diagnostiquer la présence d'une nouvelle forme d'attaque, dont la signature pourra alors être réinjectée dans un IDS classique à base de signatures. Le diagnostic des anomalies est le quatrième objectif de cette ACI. À notre connaissance, très peu de travaux se sont réellement penchés sur ce sujet. Ce quatrième objectif est double. Il s'agira d'une part d'analyser les anomalies détectées pour diagnostiquer les nouveaux comportements malveillants. D'autre part, étant donné un nouveau comportement malveillant, il faudra déterminer les causes de cette malveillance et reconstruire le scénario d'attaque ayant conduit à cette malveillance.

Coordinateur du projet

Nom	Prénom	Laboratoire
MÉ	Ludovic	SSIR (Supélec)

Equipes ou laboratoires partenaires

(Partenaire 2) Hurfin Michel	Institut National de Recherche en Informatique et en Automatique (INRIA Rennes)
(Partenaire 3) Gombault Sylvain	Ecole Nationale Supérieurs des Télécoms de Bretagne (ENSTB)
(Partenaire 4) Benferhat Salem	Centre de Recherche en Informatique de Lens (CRIL)
(Partenaire 5) Debar Hervé	France Télécom R&D (FT R&D)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	11 k€	8,1 k€		59 k€	78,9 k€
Partenaire 2	7,4 k€	6,2 k€		47 k€	60,6 k€
Partenaire 3	11,9 k€	12,7 k€		63 k€	87,6 k€
Partenaire 4	11,9 k€	66 k€			77,9 k€
Total	43 k€	93 k€		169 k€	305 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 1 Coordinateur	Ingénieur	100 %	12 mois	59 k€
Partenaire 2	Ingénieur	100 %	12 mois	47 k€
Partenaire 3	Chercheur	100 %	12 mois	63 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
FIACRE	**PROJET DE RECHERCHE**

Titre du projet :

FIabilité des Assemblages de Composants REpartis: Modèles et outils pour l'analyse de propriétés de sécurité et de sûreté

Description courte du projet :

La programmation à base de composants distribués va avoir dans les années qui viennent un impact important sur les méthodes de développement de logiciels. Pour que cette approche fonctionne pleinement, à mesure que des bibliothèques de composants deviennent disponibles, il est indispensable de pouvoir assembler des composants existants en des objets plus complexes, et de garantir que cet assemblage fonctionnera correctement et remplira le rôle que l'on en attend. Le typage classique, statique, des interfaces est notoirement insuffisant pour atteindre ce but. Réunissant des équipes spécialistes des spécifications comportementales de composants, des langages et modèles pour la programmation d'applications réparties, mobiles, communicantes, et des méthodes et outils pour la vérification compositionnelle, l'objectif de FIACRE est de concevoir des méthodes et des outils pour la spécification, l'extraction de modèles et la vérification de composants répartis, hiérarchiques et communicants. Plus précisément, nous souhaitons étudier plusieurs approches complémentaires : - L'extraction de modèles comportementaux pour les composants répartis, pour laquelle il nous semble indispensable de disposer d'un langage intermédiaire adapté, qui doit permettre d'effectuer les abstractions successives nécessaires pour produire les modèles de bas niveau à vérifier. - La vérification des assemblages hiérarchiques à partir des spécifications comportementales des composants. Ceci nécessite de s'attaquer au problème de l'explosion d'états des modèles pour vérifier des systèmes de grande taille, notamment à l'aide de techniques telles que les ordres partiels ou la vérification compositionnelle. - La définition de "bibliothèques" de propriétés (formules de logique temporelle ou équivalences de comportements) adaptées à la vérification des applications distribuées, qui devront permettre une traduction aisée vers les formalismes utilisés pour la vérification d'une part, et vers des squelettes d'applications distribuées d'autre part. Notre proposition s'appuie sur un certain nombre d'approches et d'outils logiciels sérieux existants dans les équipes participantes, en particulier la bibliothèque de composants ProActive (OASIS) distribuée au sein d'Objectweb, la boîte à outils de vérification CADP (VASY), l'outil de vérification TINA (SVF), et l'approche de typage comportemental (ENST). Nous souhaitons que la collaboration débouche sur un prototype logiciel visant des applications réalistes.

Coordinateur du projet

Nom	Prénom	Laboratoire
MADELAINE	Eric	INRIA Sophia Antipolis (INRIA Sophia Antipolis)

Equipes ou laboratoires partenaires

(Partenaire 2) Lang Frederic	INRIA Rhone-Alpes (INRIA Rhone-Alpes)
(Partenaire 3) Najm Elie	Laboratoire Traitement et Communication de l'Information (LTCI)
(Partenaire 4) Vernadat Francois	Fédération de Recherche en Informatique et Automatique (FERIA)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	10 k€	23,5 k€	10,4 k€	52,6 k€	96,5 k€
Partenaire 2	10 k€	23,5 k€	10,4 k€	52,6 k€	96,5 k€
Partenaire 3	8,723 k€	19,068 k€	10,4 k€	45,609 k€	83.8 k€
Partenaire 4	18 k€	26,4 k€	20,8 k€		65,2 k€
Total	46,723 k€	92,468 k€	52 k€	150,809 k€	342 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 1 Coordinateur	Ingénieur	100 %	12 mois	52,6 k€
Partenaire 2	Ingénieur	100 %	12 mois	52,6 k€
Partenaire 3	Post-doctorant	100 %	12 mois	45,609 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
FRAGILE	**PROJET DE RECHERCHE**

Titre du projet :

Tolérance aux défaillances et intégrité garantie par les applications dans les systèmes à grande échelle

Description courte du projet :

Les systèmes à grande échelle (Réseaux de Capteurs, Grilles de Calcul, Réseaux Pair à Pair) comprennent typiquement plusieurs milliers, voire plusieurs dizaines de milliers d'éléments de base (ordinateurs, processeurs) dotés de capacités de communication (radio de faible puissance, réseau rapide spécialisé, Internet). Du fait du grand nombre de composants mis en jeu, ces systèmes sont particulièrement vulnérables à l'occurrence de défaillances (définitives, transitoires, intermittentes). Dans un réseau de capteurs, le faible coût des composants de base fait qu'il est normal qu'une proportion non négligeable d'entre eux tombe en panne après un certain temps. Dans une grille de calcul de prochaine génération (qui devrait regrouper de 50 000 à 100 000 processeurs), les études prospectives de fiabilité font état d'un temps moyen de seulement quelques minutes entre deux défaillances. Enfin, dans un réseau Pair à Pair, le comportement des utilisateurs (connexions et déconnexions) ajoute à l'entropie du réseau (congestion des routeurs, etc.). Ces défaillances peuvent avoir un impact crucial sur le fonctionnement du système : un réseau de capteurs pourrait ne pas signaler une intrusion, une grille de calcul certifier un résultat faux. L'Informatique Répartie permet de concevoir des programmes distribués sur l'ensemble des composants d'un système. Une composante importante de la recherche en Informatique répartie traite de la tolérance aux défaillances. Cependant, il est essentiel que les programmes ainsi distribués s'adaptent aux contraintes particulières (physiques, politiques, commerciales) du système sur lequel ils sont implantés. Plusieurs résultats de l'Informatique Répartie tolérante aux fautes laissent penser que de nombreux problèmes essentiels ne peuvent être résolus dans le cadre particulier des systèmes à grande échelle. Certaines problématiques particulières viennent s'y greffer en supplément. Pour les Réseaux de Capteurs, le modèle de communication inhabituel et la volonté d'effectuer des économies d'énergie font qu'un processeur a intérêt à communiquer le moins possible pour rester utile le plus longtemps possible, ce qui élimine les solutions où on cherche activement à corriger les processeurs fautifs. Pour les Grilles de Calcul et les Réseaux Pair à Pair, l'asynchronisme du système (c'est-à-dire l'absence de borne supérieure au temps de communication) fait qu'il est pratiquement impossible de distinguer un processeur en panne d'un processeur momentanément incapable de communiquer – un processeur n'étant perçu par le reste du système qu'au travers des messages qu'il émet. Le but de cette ACI est de caractériser les systèmes à grande échelle en tant que systèmes répartis, d'évaluer dans quelle mesure la tolérance aux défaillances peut être garantie dans différents contextes caractéristiques, et, dans le cas où une telle garantie est théoriquement possible, d'en proposer une implantation qui tienne compte des exigences du contexte. Une défaillance dans un système à grande échelle causera souvent un défaut de service important, et leur fiabilité est devenue un souci majeur. Les travaux actuels en liaison avec la fiabilité et la disponibilité ne sont pas adaptés aux systèmes d'information critiques parce qu'ils n'incluent pas explicitement la notion de service dégradé. Ce qui est nécessaire est une notion précise des formes de service dégradé acceptables pour l'application, des circonstances et de la proportion du temps de service dégradé pour lesquelles ces formes sont acceptables. Cette notion, la survivabilité, fait partie intégrante de cette ACI.

Coordinateur du projet

Nom	Prénom	Laboratoire
Tixeuil	Sébastien	Laboratoire de Recherche de Informatique & INRIA Futurs (LRI)

Equipes ou laboratoires partenaires

(Partenaire 2) Fleury Eric	Centre d'Innovations en Télécommunications & Intégration de services & INRIA ARES (CITI / ARES)
(Partenaire 3) Fauconnier Hugues	Laboratoire d'Informatique Algorithmique, Fondements et Applications (LIAFA)
(Partenaire 4) Guerraoui Rachid	Distributed Programming Laboratory (LPD - EPFL)
(Partenaire 5) Herman Ted	Department of Computer Science ((CS UIOWA))

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	10 k€	104 k€			114 k€
Partenaire 2	25 k€	17 k€		108 k€	150 k€
Partenaire 3	10 k€	45 k€			55 k€
Total	45 k€	166 k€		108 k€	319 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 2	Post-doc	100 %	24 mois	108 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
KAA	**PROJET DE RECHERCHE**

Titre du projet :

Système Ambiant de Sécurité basé sur les Connaissances

Description courte du projet :

Le projet KAA (Knowledge Authentication Ambient) a pour objectif de proposer un modèle de confiance pour les objets communicants autonomes. Il associe des équipes de recherche en informatique et mathématiques à des équipes de recherche en sciences sociales. En effet, les systèmes autonomes – c'est à dire les objets de la vie quotidienne dotés de capacités de communication hétérogènes, constituent un enjeu technique mais également un véritable enjeu social. Les modèles de sécurité actuels dérivent, plus ou moins, des modèles classiques où la confiance est vue comme un attribut binaire et qui nécessite encore trop souvent un « superviseur ». Beaucoup de travaux de recherche ont eu pour objectif de réduire ou de supprimer la nécessité de cette autorité de supervision. Nous proposons au sein du projet KAA de reprendre l'étude en partant des notions fondamentales de la confiance issues des systèmes sociaux et d'en déduire un modèle technologique. Nous l'étudierons mathématiquement au moyen d'outils des systèmes dynamiques (graphes d'interactions et outils stochastiques, mais également de modèle d'interactions de particules physiques) et l'implanterons dans une plate forme expérimentale. Notre premier modèle implante des mécanismes « basiques » issus de modèles sociaux. Il sera affiné durant le projet KAA, via l'étude de modèles sociaux. Nous étudierons également l'impact de nos nouveaux modèles de sécurité sur les mécanismes sociaux, notamment par rapport aux notions de respect de la vie privée et des échanges privés, de la responsabilité des acteurs et des intermédiaires, des coûts socio-économiques de l'information dans de tels dispositifs (temps d'accès, débits, coûts de traitement et de sauvegarde). Le modèle initial peut être qualifié de modèle hybride. Il suppose l'existence d'unités fonctionnelles, appelées « bornes d'imprégnation », qui sont sécurisées par des techniques « classiques » et qui permettent à un utilisateur de prendre le contrôle d'un objet. Au moment de cette imprégnation, la borne peut puiser des ressources sécurisées dans l'Internet pour personnaliser le couple objet/porteur et génère ainsi ce que l'on nomme le « germe de sécurité ». Ce germe contient des données et des algorithmes, notamment un « historique » des interactions entre le couple objet/porteur et son environnement, l'imprégnation constituant la première interaction. Lorsque deux objets de porteurs différents sont mis en présence, l'historique commun des deux couples objets/porteurs permet de dériver un niveau de confiance spontanée qui permet, en fonction des politiques de sécurité mises en œuvre sur les objets, des échanges de « services ». L'objet de l'étude que nous mènerons dans KAA se fera dans le contexte de ce modèle initial. L'idée étant de le compléter et de l'étudier en se fondant sur les mécanismes sociaux d'établissement de la confiance.

Coordinateur du projet

Nom	Prénom	Laboratoire
UBéDA	Stéphane	Centre d'Innovations en Télécommunications et Intégration de services (CITI - Projet INRIA ARES)

Equipes ou laboratoires partenaires

(Partenaire 2) Rabagny Agnès	Centre de Recherches Critiques sur le Droit (CERCRID - UMR CNRS)
(Partenaire 3) Guihery Laurent	Labortaoire d'Economie des TRansports (LET-ISH UMR CNRS 5593)
(Partenaire 4) Morvan Michel	Labortaoire de l'Informatique du Parallélisme (LIP)
(Partenaire 5) Pousin Jérome	Mathématiques Appliquées de Lyon (MAPLY CNRS UMR 5585)
(Partenaire 6) Neuville Jean Philippe	Centre de Sociologie des Organisations

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur		9 k€		90 k€	99 k€
Partenaire 2	2 k€	9 k€	9 k€		20 k€
Partenaire 3	4 k€	6 k€	9 k€		19 k€
Partenaire 4	6 k€	15 k€			21 k€
Partenaire 5	5 k€	6 k€	9 k€		20 k€
Partenaire 6	2 k€	6 k€	13 k€		21 k€
Total	19 k€	51 k€	40 k€	90 k€	200 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 1 Coordinateur	Ingénieur	100 %	24 mois	90 k€

recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
MARS	**PROJET DE RECHERCHE**

Titre du projet :

Matériel Robuste pour Systèmes Sûrs

Description courte du projet :

De plus en plus de circuits électroniques, comme les cartes à puces, sont conçus pour être automones et disséminées dans notre environnement. Ces circuits sont donc les cibles d'attaques au niveau physique. Dans ce contexte, la sécurité des couches basses devient cruciale, puisqu'un circuit conçu sans précaution particulière est vulnérable à ces attaques. Ces attaques consistent soit à altérer le circuit ou à modifier son environnement de sorte à le faire sortir de ces conditions de fonctionnement nominales, soit à espionner l'information physique révélée par son fonctionnement dynamique. Ces deux attaques sont appelées attaque par injection de faute et attaque sur les canaux cachés. Un circuit robuste doit également faire face aux fautes naturelles, provoquées par des radiations, des particules ou même par de la diaphonie interne. Ces fautes constituent une menace sur l'intégrité des calculs réalisés et compromettent donc la fonctionnalité du circuit. Les contre-mesures contre les fautes naturelles sont de même nature que celles contre les attaques par fautes. Dans le cadre du projet MARS, nous nous attachons à développer des méthodes de conception robuste, c'est-à-dire des méthodes qui garantissent aussi bien la sécurité contre les attaques que la sûreté contre les fautes naturelles. D'un point de vue théorique, les méthodes couramment employées comme parade aux fuites d'information s'appuient sur l'indiscernabilité d'événements physiques internes (comme l'encodage différentiel). La parade aux fautes est, quant à elle, souvent basée sur la redondance d'opérateurs. Ces méthodes, certes efficaces, apportent néanmoins des solutions locales à des problèmes de sécurité ou de sûreté globaux. Nous nous interrogerons dans ce projet si des solutions globales peuvent exister. La problématique scientifique, que l'ENS formalisera, peut se reformuler comme l'étude de la dissipation et de la susceptibilité aux fautes des calculs. D'un point de vue pratique, nous étudierons la possibilité de définir des contre-mesures contre les attaques sur les canaux cachés et contre les fautes (naturelles ou malveillantes) à la fois. On considérera ces contre-mesures à différents niveaux d'abstraction (du dessin des masques à la spécification du système d'exploitation). Les contre-mesures proposées pendant le projet MARS, ou d'ores et déjà publiées, seront envisagées comme des méthodes de conception automatisables. Des outils qui implémentent ces méthodes seront conçus. De plus, nous concevrons un circuit de démonstration utilisant ces outils et nous le fabriquerons. La robustesse du circuit ainsi produit sera évaluée en présence d'attaques et en environnement hostile, grâce à la plateforme d'attaques par fautes du TIMA et à celle de mesure des canaux cachés de l'ENST.

Coordinateur du projet

Nom	Prénom	Laboratoire
GUILLEY	Sylvain	Laboratoire Traitement et Communication de l'Information (LTCI)

Equipes ou laboratoires partenaires

(Partenaire 2 LEVEUGLE Régis	Qualification of Circuits (QLF) TIMA

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	15 k€	50 k€	9 k€		74 k€
Partenaire 2	20 k€	65 k€	9 k€	38 k€	132 k€
Total	35 k€	115 k€	18 k€	38 k€	206 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 2	Post-doc	100 %	12 mois	38 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur
Coordinateur	1		

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
MetroSec	**PROJET DE RECHERCHE**

Titre du projet :

Métrologie pour la Sécurité et la Qualité de Service

Description courte du projet :

Le grand dessein de l'Internet est de devenir un réseau multi-services garantissant des qualités de services (QdS), et ceci en toutes circonstances, y compris les plus difficiles. Parmi celles-ci se trouvent notamment les moments où une attaque de déni de service, simple ou distribuée, est perpétrée, et pendant lesquels le réseau devient incapable de fournir les services demandés. Cette extrême fragilité de l'Internet souligne le lien étroit qui existe entre sécurité informatique et QdS. Plus généralement, l'Internet présente cette même sensibilité face à tous types de ruptures des caractéristiques de son trafic, qu'elles soient liées à des pannes, des comportements byzanthins de certains éléments du réseau, ou plus simplement à des augmentations fortes mais légitimes du trafic liées par exemple à la diffusion sur le réseau d'un événement populaire. L'objectif ultime de ce projet est donc d'augmenter la robustesse et l'insensibilité du réseau vis-à-vis des ruptures dans le trafic et la topologie, afin qu'il puisse continuer de fournir un service acceptable et de garantir la QdS demandée (réduisant ainsi à néant l'effet de possibles attaques). Le projet MétroSec se propose donc d'abord de développer et mettre en œuvre des outils de métrologie – actif et passif – et de supervision et de surveillance des caractéristiques du réseau et de son trafic. L'analyse des traces et mesures doit permettre de mettre en évidence la nature et l'importance de l'impact de ces ruptures sur la QdS du réseau, ainsi que sur la propagation en temps et en espace (à travers la topologie du réseau) d'éventuelles altérations de celle-ci. L'un des axes de recherche de ce projet se fonde sur les premiers résultats de caractérisation et de modélisation du trafic issus des travaux de métrologie engagés depuis quelques années, notamment par les équipes de recherche impliquées dans MétroSec. Ces travaux ont montré que les phénomènes d'invariance d'échelle constituaient l'une des caractéristiques majeures qui décoraient les statistiques du trafic Internet moderne. Ces travaux menés par certains partenaires de MétroSec, et quelques rares autres groupes dans le monde, ont, de plus, établi que les attaques perpétrées sur un réseau induisent des variations fortes dans les paramètres caractérisant les invariances d'échelle. Ces approches ayant donné d'encourageants premiers résultats, l'objectif de cet axe de recherche est donc de construire des outils de traitement du signal permettant de détecter, mettre en évidence et caractériser des ruptures, des variations « anormales » des caractéristiques du trafic. Ces variations seront, dans un premier temps, recherchées, par analyses en ondelettes, décomposition modale empirique ainsi que par des méthodes de type filtre de Kalman multi-échelle. De façon complémentaire, le projet propose d'utiliser des outils de théorie des graphes pour détecter les ruptures dans le comportement du réseau. Il s'agit ici de surveiller les variations dans la topologie observée du réseau ou des échanges. Les outils statistiques d'analyse des graphes et de leur dynamique permettent d'espérer une description fine de ces topologies et de l'impact des ruptures de comportements du réseau sur leurs propriétés. Il s'agit donc de mesurer cet impact, de l'analyser et de développer des méthodes de détection et de réaction appropriées. A partir des analyses précédentes, MétroSec proposera des améliorations architecturales, protocolaires et topologiques pour le maintien du réseau à un niveau élevé de QdS, malgré l'occurrence de ruptures. La robustesse vis-à-vis des ruptures donnera aux outils de métrologie et d'analyse (traitement du signal et graphe) le temps de classer la rupture en temps réel et de mettre en place ldes réactions appropriées. En cas d'attaque, par exemple, des outils d'identification et d'élimination des paquets incriminés seront développés et mis en œuvre, ainsi que des mécanismes d'identification des attaquants. A terme, MétroSec doit fournir un ensemble cohérent d'outils de métrologie et d'analyse de trafics et de topologies, qui permettront le développement de méthodes efficaces de surveillance, de supervision et de réaction aux anomalies. Ces méthodes combinées aux nouvelles solutions architecturales et protocolaires de communication augmenteront significativement la qualité des services réseaux, même face à une attaque. Assurer l'intégration et la complémentarité des quatre champs disciplinaires (réseau, traitement du signal, théorie des graphes et systèmes répartis), constitue un enjeu et un défi essentiel de ce projet. Cette synergie multidisciplinaire a déjà été ébauchée au travers du travail de l'Action Spécifique 88 du département STIC du CNRS, « métrologie des réseaux de l'Internet », et éprouvée à travers ses conclusions.

Coordinateur du projet

Nom	Prénom	Laboratoire
OWEZARSKI	Philippe	Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS)

Equipes ou laboratoires partenaires

(Partenaire 2) Salamatian Kavé	Laboratoire d'Informatique de Paris 6 (LIP6)
(Partenaire 3) Abry Patrice	Ecole Normale Supérieure de Lyon (ENS Lyon)
(Partenaire 4) Latapy Matthieu	Laboratoire d'Informatique Algorithmique, Fondements et Applications (LIAFA)
(Partenaire 5) Riveill Michel	Informatique, Signaux et Systèmes (I3S)
(Partenaire 6) Gallon Laurent	Laboratoire Informatique de l'Université de Pau et des Pays de l'Adour (CSySEC)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	82,4 k€	58,587 k€	9,3 k€		150,287 k€
Partenaire 2	55 k€	47,145 k€	15,5 k€		117,645 k€
Partenaire 3	32 k€	32,679 k€			64,679 k€
Partenaire 4	9 k€	26,584 k€	25 k€		60,584 k€
Partenaire 5	3,6 k€	16,205 k€	20 k€		39,805 k€
Partenaire 6	13 k€	18,3 k€	3,7 k€		35 k€
Total	195 k€	199,5 k€	73,5 k€		468 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
MOSAIC	**PROJET DE RECHERCHE**

Titre du projet :

Mobile System Availability, Integrity and Confidentiality.

Description courte du projet :

Le projet proposé vise l'étude de nouveaux mécanismes de tolérance aux fautes et de sécurité pour les dispositifs mobiles sans-fil dans des applications d'intelligence ambiante (l'informatique ubiquitaire, le support tactique pour les champs de bataille ou la sécurité civile, la domotique, etc.). Nous nous focaliserons sur les réseaux épars auto organisés, utilisant de façon prédominante des communications sans-fil à un seul saut, c'est à dire des réseaux composés d'un faible sous-ensemble d'une population importante de mobiles, réseaux qui se créent spontanément par le fait d'une certaine proximité et la découverte mutuelle, et qui cessent d'exister dès que la communication n'est plus possible. Nous explorerons le problème peu étudié jusqu'à présent de la tolérance aux fautes dans ces réseaux. Le premier objectif consiste à définir un service de sauvegarde et de restauration automatique de données, basé sur la coopération entre mobiles n'ayant aucune relation de confiance pré-établie. Un tel service vise à assurer la disponibilité des données critiques gérées par des mobiles qui sont particulièrement vulnérables à l'épuisement des batteries, aux dommages physiques, au vol, … L'idée principale est de permettre à un mobile d'exploiter des pairs accessibles afin de gérer la sauvegarde de ses données critiques. L'implémentation d'un tel service par coopération entre mobiles n'ayant aucune relation de confiance préalable est loin d'être triviale du fait des nouvelles menaces introduites : (a) des mobiles « égoïstes » peuvent refuser de collaborer, (b) les mobiles qui servent de sauvegarde peuvent également défaillir ou attaquer l'intégrité ou la confidentialité des données, (c) des mobiles malveillants peuvent chercher à provoquer un déni de service par l'inondation des pairs avec de fausses requêtes de sauvegarde, etc. Traiter ces menaces est le second objectif du projet. Nous avons l'intention d'étudier des mécanismes de gestion de la confiance dans les services collaboratifs entre mobiles mutuellement suspicieux. Dans ce contexte, des mécanismes basés sur la notion de réputation (pour une évaluation de la confiance a priori et une imputabilité a posteriori) et de récompense (pour l'incitation à collaborer) sont d'un grand intérêt. Dans les réseaux épars et éphémères que nous considérons, les mécanismes ne peuvent se baser ni sur l'accès à des tiers de confiance ni sur la présence d'une majorité des mobiles considérés, la réputation et la récompense autoportées semblent par conséquent particulièrement bien adaptées.

Coordinateur du projet

Nom	Prénom	Laboratoire
Killijian	Marc-Olivier	Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS)

Equipes ou laboratoires partenaires

(Partenaire 2) Roudier Yves	Institut Eurécom (Eurecom)
(Partenaire 3) Banâtre Michel	Institut de Recherche en Informatique et Systemes Aleatoires (IRISA)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	17,5 k€	37,8 k€	9 k€		64,3 k€
Partenaire 2	28,7 k€	23 k€	6 k€		57,7 k€
Partenaire 3	15,8 k€	21,2 k€	18 k€		55 k€
Total	62 k€	82 k€	33 k€		177 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur
Coordinateur	1		

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
Potestat	**PROJET DE RECHERCHE**

Titre du projet :

Politiques de sécurité : test et analyse par le test de systèmes en réseau ouvert

Description courte du projet :

Dans le cadre de la réalisation de services de plus en plus ouverts, s'appuyant sur la mise en réseau de parties de systèmes informatiques, avec des solutions hétérogènes, les responsables de la sécurité manquent souvent d'éléments d'analyse bien formalisés. La sécurité de ces systèmes est donc organisée en fonction de connaissances pragmatiques, en s'appuyant sur des failles connues et les mesures de protections associées. Il reste alors à vérifier que la politique de sécurité ainsi définie est bien celle qui est effectivement mise en oeuvre dans le système. Pour cela, on procède généralement à des audits, qui portent sur les procédures administratives et sur la configuration du systèmes. Des tests sont ensuites menés, correspondant à des sondages du système, pour vérifier si certaines vulnérabilités connues ne resteraient pas présentes. S'il existe des outils pour certains tests spécifiques (comme les craqueurs de mots de passe), il n'y a pas de solution analysant la conformité globale d'un système par rapport à une politique de sécurité. Plusieurs raisons peuvent expliquer ces déficiences. D'abord, il y a peu d'études actuellement sur la modélisation formelle complète de politiques de sécurité, même si certains aspects, comme le contrôle d'accès, ont fait l'objet d'études plus poussées. Ensuite, les travaux d'analyse par vérification menés en sécurité ont plus souvent porté sur la vérification d'éléments ponctuels, comme les protocoles cryptographiques ou l'analyse de code. Enfin, la plupart des travaux menés concernent la vérification a priori de la cohérence de politiques de sécurité, avant leur mise en oeuvre. Nous nous intéressons ici au test de la conformité de la configuration de systèmes par rapport à une politique définie. Dans le cadre du projet POTESTAT nous envisageons d'aborder le problème du test de politique de sécurité sur un réseau ouvert selon les points suivants : - Modélisation formelle adéquate pour les politiques de sécurité, permettant une analyse par le test. - Définition d'une notion de conformité de la configuration de systèmes par rapport à ces éléments d'une politique de sécurité. L'objectif est de parvenir à une théorie du test analogue à ce qui peut exister dans le domaine des tests de protocoles (Z.500). - Méthodes de test de la conformité à une politique, avec en particulier les problèmes de testabilité, d'environnement d'exécution, d'analyse de code et de sélection de tests pertinents. L'objectif ultime (à plus long terme que le travail théorique de l'ACI) est que les responsables de sécurité des outils d'analyse puissent disposer d'outils, permettant : * de modéliser les flux d'informations, les éléments du réseau (protocoles utilisés, types de noeuds et type de sécurité associée etc.), afin de pouvoir décrire plus formellement la politique de sécurité dans l'optique d'un test de conformité * d'outiller cette modélisation afin de pouvoir mener des vérifications de cohérence ou des recherches de point faible * d'étudier plus particulièrement une automatisation des procédures de test des systèmes pour vérifier si la politique de sécurité effectivement mise en oeuvre correspond bien à celle déclarée.

Coordinateur du projet

Nom	Prénom	Laboratoire
GROZ	Roland	Laboratoire Logiciels Systemes et Reseaux (LSR-IMAG)

Equipes ou laboratoires partenaires

(Partenaire 2) MOUNIER Laurent	Verimag (verimag/imag)
(Partenaire 3) Jeron Thierry	Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	5 k€	31 k€	13 k€		49 k€
Partenaire 2	5 k€	26 k€	13 k€		44 k€
Partenaire 3	10 k€	25,8 k€		37,2 k€	73 k€
Total	20 k€	82,8 k€	26 k€	37,2 k€	166 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 3	Post-doc	100 %	12 mois	37,2 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
SATIN	**PROJET DE RECHERCHE**

Titre du projet :

Analyse de la Sécurité pour des Protocoles et Infrastructures de Confiance

Description courte du projet :

La conception de systèmes de communications sûrs est un défi. Il est possible de monter de véritables attaques en exploitant uniquement les faiblesses des protocoles. Ces attaques échappent souvent aux concepteurs à cause de la difficulté à prévoir a priori les différentes manières possibles pour un environnement malicieux d'interférer avec les différents agents. Ceci montre l'importance de disposer d'outils puissants capable d'analyser le flot d'information distribué entre les différents agents communicants. Les algèbres de processus et les techniques de réécritures associées offrent des modèles adaptés pour de telles analyses. Par exemple, elles peuvent exploiter des critères d'observation adéquats pour vérifier la confidentialité ou l'authentification pour les protocoles cryptographiques; mais elles conviennent également à d'autres applications telles que la répartition à grande échelle de politiques de contrôle d'accès dynamiques sur des OS sécurisés. D'intéressants résultats ont été obtenus récemment par ces approches, cependant leur application effective à des problèmes de type industriel nécessite de résoudre des questions fondamentales telles que: procédures de décision plus efficaces et approximations plus précises, prise en compte de l'incidence du temps, modélisation adéquate des primitives cryptographiques imparfaites, de la notion du déni de service et étude formelle des attaques associées. Les équipes du projet SATIN dispose de compétences complémentaires en sécurité et méthodes formelles; notre objectif est de relever le défi de l'analyse et de la conception de systèmes distribués surs. Nous nous appuierons sur des avancées récentes en modélisation formelle, résolution de contraintes, automates d'arbre et critères d'observation pour systèmes concurrents. L'interaction avec nos partenaires industriels CEA-DAM et France Telecom sera naturellement importante pour valider les résultats obtenus à chaque étape du projet.

Coordinateur du projet

Nom	Prénom	Laboratoire
RUSINOWITCH	Michael	Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

Equipes ou laboratoires partenaires

(Partenaire 2) HAINS Gaétan	Laboratoire d'Informatique Fondamentale d'Orléans (LIFO)
(Partenaire 3) GENET Thomas	Institut de Recherche en INformatique et Systemes Aleatoires (IRISA)
(Partenaire 4) KLAY Francis	France Telecom R&D (DTL)
(Partenaire 5) OUDOT Laurent	Commissariat à l'Energie Atomique. (CEA) DAM

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur		42 k€	12 k€		54 k€
Partenaire 2		54 k€			54 k€
Partenaire 3		12 k€		37 k€	49 k€
Total		108 k€	12 k€	37 k€	157 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 3	Post-doc	100 %	12 mois	37 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur
Coordinateur	1		

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
SERAC	**PROJET DE RECHERCHE**

Titre du projet :

Modèles et protocoles de SEcuRité pour les réseaux Ad-hoC

Description courte du projet :

Un réseau ad hoc est un réseau sans fil dynamique et spontané, à plusieurs sauts. Chaque mobile/noeud du réseau doit envoyer des messages par "broadcast", afin d'informer ses voisins de son existence. Ainsi, chaque noeud est potentiellement amené à router les messages de ses voisins (au sens large). Historiquement, ces réseaux ont été proposés dans un contexte militaire, mais leur intérêt dans le monde civil s'est considérablement développé depuis. Dans tous ces contextes, la sécurité est primordiale, tant pour préserver la confidentialité que pour assurer l'authentification des parties lors des échanges. Mais la sécurité des réseaux ad hoc n'a encore pas été entièrement explorée, et nous sommes loin de pouvoir assurer dans ces réseaux les mêmes services d'authentification, confidentialité, ... que dans les réseaux filaires, ou encore les réseaux possédant une infrastructure. Nous nous plaçons ici dans un cas extreme, qui requiert des mécanismes plus sophistiqués, efficaces, mieux adaptés. Nous avons ainsi choisi de porter notre attention sur deux aspects essentiels. 1) La définition de modèles de confiance adaptés aux réseaux ad hoc, prenant en compte la dynamique du réseau (liaisons éphémères) et le manque d'infrastructure. Aucun noeud ne doit a priori être privilégié par rapport à un autre, puisqu'il n'existe pas, a priori, de hiérarchie entre eux. 2) Sécuriser le routage des messages traversant le réseau, afin de faire face aux difficultés rencontrées, telles que l'égoïsme d'un noeud, la rupture d'une liaison, l'usurpation d'identité, ... Ce travail s'appuiera sur la définition des modèles de confiance et permettra d'améliorer les protocoles de routage existants. Ces modèles de confiances et protocoles de routage sécurisés seront implémentés dans une plate-forme "open source", afin d'illustrer leur efficacité et leur passage à l'échelle.

Coordinateur du projet

Nom	Prénom	Laboratoire
FONTAINE	Caroline	Laboratoire d'Informatique Fondamentale de Lille - UMR 8022 (LIFL)

Equipes ou laboratoires partenaires

(Partenaire 2) LENEUTRE Jean	Laboratoire Traitement et Communication de l'Information - UMR 5141 (LTCI)
(Partenaire 3) AUGOT Daniel	INRIA Rocquencourt projet CODES

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	6 k€	44 k€			50 k€
Partenaire 2	6 k€	44 k€			50 k€
Partenaire 3	6 k€	44 k€			50 k€
Total	18 k€	132 k€			150 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
SR2I	**PROJET DE RECHERCHE**

Titre du projet :

Sécurité du Routage Interdomaine dans Internet

Description courte du projet :

Internet est divisé en des milliers de régions autonomes nommées AS (autonomous systems). Un AS a ses propres routeurs et est connecté aux autres AS pour échanger des données. Chaque AS emploie ses propres règles pour sélectionner des routes. BGP est le protocole de routage entre AS dans Internet. A ce titre, il est responsable des délais à cause du choix des chemins. Le point fondamental pour un algorithme de routage sur un réseau de grande taille est le caractère nécessairement dynamique de la topologie, des liens disponibles et des machines connectées. Les routeurs BGP doivent donc avertir leurs voisins lorsque les chemins doivent être modifiés à cause d'une panne ou d'une correction. Et ils propagent cette information si elle leur arrive. Depuis longtemps, on a constaté que BGP a un problème d'instabilité. Des états logiques de routes physiquement correctes peuvent osciller pendant de très longues périodes. On constate aussi qu'une panne réelle provoque une avalanche de messages de mises à jour. BGP souffre donc typiquement d'un problème de fiabilité puisqu'une panne élémentaire de routeur provoque des problèmes transitoires graves. Mais BGP et les routeurs montrent également des problèmes de sûreté qui menacent la connectivité d'Internet. Les attaques de vers se propageant par envoi à des adresses IP aléatoires ont provoqués récemment d'importantes pannes de routeurs BGP. BGP souffre donc de multiples problèmes de sécurité : fiabilité tout d'abord par ses réactions aux pannes de liens, fiabilité également lorsque des politiques incohérentes gênent la convergence du routage ou provoque une surcharge du réseau par inondation d'information de mises à jour obsolètes, et aussi sûreté lorsque des attaques sur d'autres composantes du réseau stressent le routeur et provoque une panne. Le projet a pour but d'améliorer la fiabilité du réseau grâce à des améliorations des algorithmes, le design de politiques locales correctes, un monitoring du réseau et des contrôles statistiques. Ces techniques peuvent aussi aider à limiter la propagation de vers et plus difficilement le déni de Service. Les différentes équipes du consortium vont mettre en commun leur compétences pour, l'analyse des propriétés d'autostabilisation, la tomographie active et passive en récupérant toutes les informations du réseau, des modèles statistiques permettant de détecter des variations de trafic, la construction d'une image "plus réaliste" du graphe de la topologie logique du réseau, permettant de limiter les échanges de messages, d'accélérer la convergence et d'améliorer la sécurité du routage inter-domaine.

Coordinateur du projet

Nom	Prénom	Laboratoire
Konig	Jean Claude	Laboratoire d'Informatique et de Microélectronique de Montpellier (LIRMM)

Equipes ou laboratoires partenaires

(Partenaire 2) Tixeuil Sébastien	Laboratoire de Recherche de Informatique & INRIA Futurs (LRI)
(Partenaire 3) Fourneau Jean-Michel	Parallélisme Réseaux Systèmes Modélisation (PRiSM)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	9,5 k€	27 k€			36,5 k€
Partenaire 2	6 k€	24 k€			30 k€
Partenaire 3	9,5 k€	61,915 k€		44,085 k€	115,5 k€
Total	25 k€	112,915 k€		44,085 k€	182 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC
Partenaire 3	ingénieur	100 %	12 mois	44,085 k€

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
Tadorne	**PROJET DE RECHERCHE**

Titre du projet :

Tatouage de données contraintes

Description courte du projet :

Garantir la protection de la propriété intellectuelle ou industrielle d'un document électronique est un enjeu important pour le développement d'une économie de l'information. Le tatouage (watermarking) est une technique participant à cette protection, en permettant l'insertion robuste et discrète d'information dans un document, comme par exemple l'identité de son propriétaire. De nombreuses techniques de tatouage existent pour les données multimédia comme le son, l'image ou la vidéo, mais ces dernières ne constituent qu'une part des échanges effectués sur les réseaux. Une grande partie de ces échanges est constituée de données extrêmement structurées et contraintes, ayant également une forte valeur marchande ou intellectuelle. On peut citer : les bases de données relationnelles et les documents Xml, les données géométriques, les mesures de senseurs physiques distribués et les résultats de calculs intensifs. Un point central reliant ces différentes applications est l'existence de forte contraintes d'utilisabilité : le tatouage (i.e. l'altération) de tels documents doit se faire en respectant un grand nombre de contraintes formellement exprimées. Pour dissimuler de l'information, on cherchera par exemple à perturber : - le contenu d'une base de données relationnelle tout en laissant invariant un ensemble de requêtes SQL ; - la géométrie d'une région géographique tout en préservant ses relations topologiques avec les autres régions et certaines propriétés métriques ; - la solution d'un problème d'optimisation tout en garantissant la presque optimalité de la solution ; - le comportement d'un service web, en préservant son utilisabilité et sa composabilité avec d'autres services. Il est très important de prendre en compte une vaste gamme de contraintes, en particulier lorsque les documents en questions sont à l'origine de décisions humaines importantes (sanitaires, économiques, etc.) La variété de ces contraintes et la taille des documents considérés donne à la découverte de tatouages valides un aspect combinatoire difficile. L'objectif de l'ACI Tadorne est 1) de produire des algorithmes de tatouage efficaces pour ces types d'applications, en s'appuyant sur une description logique de leur contraintes d'utilisabilité 2) de fournir une analyse de ces méthodes spécifiques en utilisant la théorie de la complexité (au pire ou en moyenne) et la logique, dans le but d'optimiser leur temps de calcul et leur robustesse 3) de valider cette approche par un prototype, avec un accent particulier sur le tatouage de données géographiques. Cet effort de recherche sera conduit par quatre laboratoires : le Cedric (CNAM Paris EA 1395), menant une activité "Tatouage de données structurées" et possédant une forte expérience en bases de données géométriques et en services web, le Lamsade (Université Paris Dauphine UMR 7024) et le GREYC (Université de Caen UMR 6072), spécialisés dans la théorie de la complexité des problèmes d'optimisation et des algorithmes probabilistes, et enfin le laboratoire COGIT (IGN Paris), spécialisé dans le traitement informatique des données géographiques. L'aspect juridique sera également pris en compte par la participation d'un avocat spécialisé en droit d'auteurs et protection de l'information. Ce projet favorise une approche théorique en amont, sur des données complexes, tout en restant en relation avec une application concrete. Il complètera l'expertise française en tatouage (déjà forte pour les données multimédia) sur le thème récent des données fortement structurées, thème en expansion dans le champ international.

Coordinateur du projet

Nom	Prénom	Laboratoire
GROSS-AMBLARD	David	Centre d'étude en Informatique du Cnam (CEDRIC)

Equipes ou laboratoires partenaires

(Partenaire 2) Bazgan Cristina	Laboratoire d'Analyse et Modélisation de Systèmes pour l'Aide à la Décision (LAMSADE)
(Partenaire 3) Le Bars Jean-Marie	Groupe de Recherche en Informatique, Image, Automatique et Instrumentation de Caen (GREYC)
(Partenaire 4) Ruas Anne	Information géographique et cartographie (COGIT)
(Partenaire 5) Nédélec Yves Henri	avocat à la cour, chargé d'enseignement à l'université de Dauphine

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	4 k€	14,55 k€	3,1 k€		21,6 k€5
Partenaire 2	3 k€	14,1 k€			17,1 k€
Partenaire 3	6,6 k€	12,6 k€			19,2 k€
Partenaire 4	2 k€	2,05 k€			4,05 k€
Total	15,6 k€	43,3 k€	3,1 k€		62 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur

I - FICHE D'IDENTITE DU PROJET

Numéro du projet :

ACI SI 2004

Nom du projet :	**Type de projet :**
VENUS	**PROJET DE RECHERCHE**

Titre du projet :

EValuation des Effets Nuisibles pour les Usagers d'un Système intégré (VENUS)

Description courte du projet :

Le projet VENUS concerne le développement des nouvelles méthodes et des outils consacrés à l'analyse prédictive, à la validation et à la qualification des systèmes électroniques intégrés sécuritaires en utilisant l'injection de fautes logicielle et matérielle. Le projet résulte d'une collaboration entre deux laboratoires de recherche : le laboratoire TIMA de Grenoble et le laboratoire IXL de Bordeaux. Le laboratoire TIMA a une expérience très importante dans le développement des méthodologies et des outils d'injection de fautes logicielles et matérielles dans les systèmes électroniques. En utilisant différentes approches d'injection, il est possible d'obtenir pendant la conception d'un circuit une évaluation de la sensibilité de différentes architectures complexes face aux perturbations, et aussi de valider des procédures de protection mises en place par les concepteurs au niveau matériel ou logiciel. Un autre domaine d'expertise du laboratoire TIMA concerne l'évaluation de la sensibilité de circuits intégrés par des campagnes de test sous radiations. Le laboratoire IXL développe des techniques d'injection de fautes matérielles basées sur les impulsions laser afin de stimuler électriquement, dynamiquement et localement les circuits intégrés par l'intermédiaire de l'effet photoélectrique. La première direction de recherche développée à IXL consiste en la modélisation expérimentale de l'environnement radiatif par le biais d'impulsions laser ultra courtes. La deuxième direction de recherche concerne l'analyse de défaillances dans les circuits intégrés en étudiant le comportement électrique global d'un module soumis à une simulation photoélectrique. Les nouvelles méthodologies et les outils qui seront développés dans le cadre du projet VENUS concernent deux directions de base. En premier, nous nous intéresserons à l'analyse prédictive de la sensibilité des architectures matérielles complexes. La plateforme de prédiction de la sensibilité comportera le développement de méthodes et d'outils d'injection de fautes multi niveaux, qui pourront être utilisés depuis la description RTL jusqu'au niveau portes logiques. Cette plateforme s'appuiera sur l'environnement déjà développé à TIMA, qui sera étendu pour pallier différentes limitations des approches existantes, notamment sur les axes suivant : - extension des modèles de fautes disponibles et prise en compte des fautes multiples, - modélisation fine de l'environnement du circuit afin de mieux mettre en évidence les défaillances réelles du point de vue de l'application, - prise en compte de blocs analogiques dans le circuit, - exploitation de la hiérarchie structurelle dans l'analyse des propagations d'erreurs, - exploitation des approches de preuve formelle pour réduire la durée des expérimentations. Un deuxième ensemble de méthodologies et d'outils visera à développer une plateforme d'évaluation de la sensibilité des architectures matérielles complexes émulées dans un composant FPGA, ou implémentées en ASIC. L'évaluation de la sensibilité sera obtenue par plusieurs méthodes : injection de fautes au niveau logiciel, et injection de fautes matérielles à l'aide du laser et par des campagnes de test sous radiations. Les méthodologies et les outils seront validés sur plusieurs architectures et applications. Les résultats obtenus d'après les deux types d'approches seront comparés afin d'affiner la modélisation de fautes et la méthodologie pour garantir une très bonne corrélation.

Coordinateur du projet

Nom	Prénom	Laboratoire
ANGHEL	Lorena	Techniques of Informatics and Microelectronics for Computer Architectures (TIMA)

Equipes ou laboratoires partenaires

(Partenaire 2) Lewis Dean	Laboratoire d'étude de l'intégration des composants et systèmes électroniques (IXL UMR CNRS 5818)

II - Récapitulatif global des moyens attribués au projet :

Financements via le Fonds National de la Science :
Toutes les sommes sont indiquées TTC.

	Equipement	Fonctionnement (Hors vacations, Hors CDD)	Vacations	CDD	Total
Partenaire 1 Coordinateur	25 k€	98,5 k€	16,2 k€		139,7 k€
Partenaire 2	20 k€	60 k€	9,3 k€		89,3 k€
Total	45 k€	158,5 k€	25,5 k€		229 k€

Détails des dépenses de personnels (CDD) :

Nom du partenaire bénéficiaire	Type d'emploi (Ingénieur, post-doc,…)	Quotité de temps de travail	Durée du contrat	Montant total TTC

Allocations de recherche et apports des organismes de recherche :

	Allocation de recherche	Post-doc	Accueil d'enseignant-chercheur