Action Concertée Incitative
Jeunes Chercheurs

Sécurité informatique, protocoles cryptographiques et détection d'intrusions

Jean Goubault-Larrecq
LSV/CNRS UMR 8643
ENS de Cachan

18 mai 2001

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

FICHE D'IDENTIFICATION (1/3)

Projet :

Titre du projet : **Sécurité informatique, protocoles cryptographiques et détection d'intrusions**

Chef de projet : **Jean Goubault-Larrecq**

N^o d'identification : **1071**

Résumé du projet (1/2 page maximum) :

Le but de ce projet consiste à développer plusieurs approches de la sécurité informatique ainsi que des ponts entre ces approches.

Notamment, nous proposons de développer des méthodes automatiques de vérification de protocoles cryptographiques dans le but typique de vérifier la sécurité des systèmes de commerce électronique, des frontaux de sécurité, des portails Internet ou des GSM. D'autre part, la sécurité étant un problème global, il est aussi nécessaire de s'intéresser à d'autres méthodes de sécurisation de systèmes d'information. Une approche prometteuse est la détection d'intrusion en temps réel, par analyse de fichiers de logs. Une technique originale développé chez Dyade puis au LSV se fonde sur des techniques adaptées de model-checking. Ces deux approches sont complémentaires, et il est primordial de les faire collaborer. Ainsi, une vérification d'un protocole cryptographique qui ne conclut pas à la sécurité du protocole donne une description des attaques possibles contre ce protocole. Il est alors possible de décrire ces attaques sous forme de signatures qui viendront alimenter un outil d'audit de logs. Ceci résout ainsi, au moins partiellement, mais de façon rigoureuse, l'un des problèmes les plus cruciaux dans les outils d'audit à base de signatures, à savoir quelles sont les signatures pertinentes.

En général, nous souhaitons fédérer diverses approches de la sécurité, en exploitant les synergies entre approches différentes, dans le but de proposer un environnement de sécurisation globale des systèmes d'information.

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

FICHE D'IDENTIFICATION (2/3)

Chef de projet :

- Nom, prénom : **Goubault-Larrecq, Jean**
- Date de naissance : **10 avril 1965**
- Poste et date de nomination dans le poste :
  professeur des universités, associé à temps plein, 01 octobre 2000
- Établissement : **École Normale Supérieure de Cachan**
- Unité : **LSV/CNRS UMR 8643**
- Directeur de l'unité : **Michel Bidoit**
- Adresse complète :
  LSV, ENS Cachan, 61 avenue du président-Wilson, 94235 Cachan Cedex
- Téléphone : **01 47 40 24 30** – Télécopie : **01 47 40 24 64**
- Adresse électronique : **goubault@lsv.ens-cachan.fr**
- Budget global du laboratoire ou de l'unité de recherche accueillant le projet : **1.138 kF**

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

FICHE D'IDENTIFICATION (3/3)

Noyau de l'équipe :

Nom	Prénom	Labo	Poste	Date de nomination	Age	% Temps consacré
GOUBAULT-LARRECQ	Jean	LSV	Pr ENS Cachan	10/2000	35	50 %
DEMRI	Stéphane	LSV	CR CNRS	10/1995	33	30 %
BOISSEAU	Alexandre	LSV	Doctorant	09/2000	26	30 %
CORTIER	Véronique	LSV	Doctorante	09/2000	22	40%
ROGER	Muriel	LSV	Doctorante	09/1999	28	40%

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

CURRICULUM VITAE ET LISTE DE PUBLICATIONS DU CHEF DE PROJET

GOUBAULT-LARRECQ Jean Né le 10 avril 1965, à Rouen (76).
Nationalité Française
Marié, deux enfants.
Adresse : 1, rue des bateliers, 92100 Clichy
Tél : 01 47 31 62 40
Mél : goubault@lsv.ens-cachan.fr
Poste actuel : Professeur associé à temps plein,
LSV/CNRS UMR 8643, ENS Cachan,
depuis le 01 octobre 2000.

Carrière : directeur d'action, G.I.E. Dyade, avr. 1997–sep. 2000
chargé relations internationales, G.I.E. Dyade, sep. 1996–sep. 2000
chercheur invité, université de Karlsruhe, mar.–août 1996
ingénieur de recherches, Bull S.A., sep. 1989–fév. 1996

Diplômes : Habilitation à diriger les recherches (1997)
Université Paris IX Dauphine.
Docteur de l'École Polytechnique en informatique (1993)
mention très honorable avec félicitations.
D.E.A. Systèmes Informatiques de Paris VI (1988)
mention TB.
Ingénieur des Mines (1988).
Ingénieur polytechnicien (1986).
Licence de mathématiques, Université Paris VI (1984).
Baccalauréat C mention TB (1981).

Thèmes de recherche : Démonstration automatique de théorèmes.
Interprétations calculatoires des logiques modales et géométrie.
λ-calcul, calculs de substitutions explicites.
Techniques de preuve par réflexion, intégration de
méthodes de model-checking et de techniques de preuve.
Vérification de protocoles cryptographiques.
Détection d'intrusion, audit de logs par model-checking.

Points forts : Contacts industriels.
Diversification thématique.

Publications récentes (depuis 1997) :

[GM97] Jean Goubault-Larrecq et Ian Mackie. *Proof Theory and Automated Deduction*, volume 6 of *Applied Logic Series*. Kluwer, ISBN 0-7923-4593-2, 1997.

[GG00] Healfdene Goguen et Jean Goubault-Larrecq. Sequent combinators: A Hilbert system for the lambda calculus. Mathematical Structures in Computer Science 10(1):1–79, 2000.

[Gou97b] Jean Goubault-Larrecq. Ramified higher-order unification. In *Proceedings of the 12th Annual IEEE Symposium on Logics in Computer Science (LICS'97)*, pages 410–421. 1997.

[Gou98b] Jean Goubault-Larrecq. A proof of weak termination of typed $\lambda\sigma$-calculi. In *Proceedings of TYPES'96*, Springer Verlag Lecture Notes in Computer Science, volume 1512, pages 134–151. 1998.

[Gou99a] Jean Goubault-Larrecq. Conjunctive types and SKInT. In *Proceedings of TYPES'98*, Springer Verlag Lecture Notes in Computer Science, volume 1657, pages 106–120, 1999.

[Gou99c] Jean Goubault-Larrecq. A simple sequent system for first-order logic with free constructors. In *Proceedings of the International Conference on Automated Theorem Proving with Analytic Tableaux and Related Methods (TABLEAUX'99)*, Springer Verlag Lecture Notes in Artificial Intelligence, volume 1617, pages 202–216, 1999.

[Gou00b] Jean Goubault-Larrecq. A method for automatic cryptographic protocol verification (extended abstract). In *Proceedings of the International Workshop on Formal Methods in Parallel Programming, Techniques and Applications*, Springer Verlag Lecture Notes in Computer Science, volume 1800, pages 977–984. 2000.

[RGL01a] Xavier Rival et Jean Goubault-Larrecq. Experiments with finite tree automata in Coq. In *Proceedings of the International Conference on Theorem Proving in Higher-Order Logics (TPHOL'01)*, Springer Verlag, 2001. À paraître.

[RGL01] Muriel Roger et Jean Goubault-Larrecq. Log auditing through model-checking. In *Proceedings of the 14th International IEEE Computer Security Foundations Workshop*, Keltic Lodge, Nova Scotia, Canada. IEEE Press, juin 2001. À paraître.

[SG97] Peter H. Schmitt et Jean Goubault-Larrecq. A tableau system for linear-TIME temporal logic. In *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'97)*, Springer Verlag Lecture Notes in Computer Science, volume 1217, pages 130–144. 1997.

[VGPA00] Kumar Neeraj Verma, Jean Goubault-Larrecq, Sanjiva Prasad, et S. Arun-Kumar. Reflecting BDDs in Coq. In *Proceedings of the ASIAN'2000 Conference*, Springer Verlag Lecture Notes in Computer Science, volume 1961, pages 162–181, 2000.

[GG99] Jean Goubault-Larrecq et Éric Goubault. Order-theoretic, geometric and combinatorial models of intuitionistic S4 proofs. In *Proceedings of the First Workshop on Intuitionistic Modal Logics and Applications (IMLA'99)*, Trente, Italie, juillet 1999.

Principales responsabilités scientifiques et administratives (incluant direction de thèse) :

- Directeur de l'action VIP (Verified Internet Protocols) au GIE Dyade, 1999–2000. Directeur de l'action VIP/recherche au GIE Dyade, 1997–1998.

- Comités de programmes : International Conference on Theorem Proving with Analytic Tableaux and Related Methods (TABLEAUX), 1997–2000. International Joint Conference on Automated Reasoning (IJCAR), 2001. International Conference on Logic, Programming, and Automated Reasoning (LPAR), 2001. International Conference on Automated Deduction (CADE), 2002. Second International Workshop on Intuitionistic Modal Logics and Applications (IMLA), 2002.
- Organisation de colloques : First International Workshop on Logical Aspects of Cryptographic Protocol Verification (LACPV), 2001.
- Édition de revues : numéro spécial sur les protocoles cryptographiques, International Journal of Telecommunications and Information Technology (JT&IT), 2001.
- Rapporteur des thèses : Alexandre Miquel (Paris VII, 2001); Guillaume Gillard (Paris VII, 2001); Dominique Larchey-Wendling (Nancy I, 2000); Olivier Pons (CNAM, 1999); Mehdi Ayadi (Paris IX, 1998).
- Examinateur aux jurys de thèse : Romain Guider (INRIA Sophia-Antipolis, 2000); Laurent Mauborgne (École Polytechnique, 1999).
- Examinateur aux jurys d'habilitation : Serena Cerrito (Paris XI, 2000).
- Direction de thèse : Nabil El Kadhi (1998-2001), université Tunis II et INRIA. Co-direction avec Mohammed Ben Ahmed (Tunis II). Effectuée à Tunis et au GIE Dyade. Sujet: vérification statique des programmes cryptographiques.
- Direction de thèse : Muriel Roger (1999-2001) en cours, université Paris VII puis ENS Cachan (depuis 2000). Sujet: comparaison de modèles de protocoles cryptographiques (anciennement: audit de logs et model-checking).
- Direction de thèse : Eva Rose (1999-2001) en cours, université Paris VII. Sujet: aspects sécuritaires des cartes à puce Java.
- Direction de thèse : Kumar Neeraj Verma (2000-2001) en cours, ENS Cachan. Sujet: intégration de méthodes de preuve et de model-checking.

Dépôts de brevets, logiciels :

- Logiciel : Moteur d'audit de logs log$\mathcal{W}$eaver 2.6 (anc. `logcheck`), GIE Dyade, 2000; LSV, 2001.
- Brevet (avec Muriel Roger) : "Procédé et dispositif de résolution de modèles, utilisation pour la détection des attaques contre les systèmes informatiques", dépôt français du 13 septembre 1999, correspondant Dyade, demandeurs : 1. INRIA 2. Bull S.A. Récépissé de dépôt no. 9911716.
- Logiciel : Outil d'analyse automatique de protocoles cryptographiques `CPV`, GIE Dyade, 1999–2000.

- Logiciel : Garbage collector de la machine virtuelle JavaTerminal de Bull/CP8, 1998 (R&D Award Bull).
- Logiciel : `HimML` versions 14 (1997), 15 (1998), 16 (2000), un compilateur de bytecode pour une extension de Standard ML avec des ensembles et mappes finis efficaces. En Open Source, disponible sur `www.lsv.ens-cachan.fr/~goubault/`.

Information scientifique, technique et vulgarisation :

- Exposé invité aux journées ASPROM sur la sécurité du logiciel, Paris, oct. 2000.
- Exposé invité aux Journées systèmes infinis, Paris, mars 2001.
- Exposé invité aux premières journées du LIX, Palaiseau, mai 2001.

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

EQUIPE IMPLIQUEE DANS LE PROJET (1/2)

Historique de la constitution de l'équipe

L'équipe, constituée de Jean Goubault-Larrecq, Alexandre Boisseau, Véronique Cortier, Stéphane Demri, et Muriel Roger, s'est formée doucement avec l'arrivée de Jean Goubault-Larrecq au LSV, ENS Cachan, en octobre 2000. À la lumière de son expérience industrielle au GIE Dyade, en contact avec les équipes de Bull et Bull/CP8, ce dernier a fait valoir l'importance de deux axes de recherche, alors indépendants, l'un sur la vérification des protocoles cryptographiques, l'autre sur la détection d'intrusion par techniques de model-checking.

Le LSV avait déjà commencé à développer une activité de recherche dans le domaine des protocoles cryptographiques, comme l'attestent les sujets de thèse d'Alexandre Boisseau (avec M. Bidoit) et de Véronique Cortier (avec H. Comon). A. Boisseau organise d'ailleurs un groupe de travail thématique « protocoles cryptographiques » hebdomadaire, qui regroupe les chercheurs du LSV intéressés par ce domaine.

L'activité en détection d'intrusions avait été initiée à Dyade par Muriel Roger lors de son stage de DEA (avec J. Goubault-Larrecq). Depuis, M. Roger a souhaité réorienté sa recherche sur le problème important de la question de la relation formelle entre différents modèles de protocoles cryptographiques, et participe activement au groupe de travail thématique « protocoles cryptographiques ». Elle a donc une double compétence, en protocoles cryptographiques et en détection d'intrusions. Quant à Stéphane Demri, dont une spécialité est la complexité des logiques temporelles et modales, il s'intéresse à l'efficacité des algorithmes de model-checking pour les logiques utilisés dans les travaux de M. Roger et J. Goubault-Larrecq ou des variantes adéquates, et souhaite participer par ce biais à l'activité proposée de recherche en sécurité.

Place de l'équipe dans le laboratoire

L'équipe occupe une place essentiellement transversale dans le laboratoire, empruntant des compétences tant au groupe naissant de vérification de protocoles cryptographiques qu'au petit groupe de chercheurs travaillant sur la complexité des logiques temporelles et modales. On peut d'un autre côté considérer qu'elle forme un nouveau pôle de recherche en sécurité, tranchant avec, et complétant l'activité traditionnelle du laboratoire en sûreté informatique.

Degré d'autonomie escompté :

S'il est souhaité que ce groupe soit en principe le plus autonome possible, ayant une spécialité sécuritaire propre, il est par contre aussi souhaité de conserver des ponts avec les thèmes proches de sûreté, plus traditionnels, et dans lesquels le LSV est réputé au niveau international. Ceci permettra notamment de bénéficier des forces traditionnelles du LSV dans des domaines nouveaux, et d'en enrichir la thématique en retour.

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

EQUIPE IMPLIQUEE DANS LE PROJET (2/2)
CURRICULUM VITAE ET PUBLICATIONS DES MEMBRES DE L'EQUIPE

BOISSEAU Alexandre Né le 16 mai 1975 à Niort (72)
Nationalité Française
Mél : boisseau@lsv.ens-cachan.fr
Poste actuel : Doctorant à l'EDSP (École Doctorale Sciences Pratiques, ENS Cachan), depuis septembre 2000.
Directeur de thèse M. Bidoit,
Sujet : « Vérification de propriétés de sécurité de protocoles cryptographiques »

Diplômes : Magistère de mathématiques et d'informatique, ENS Cachan, 2000, Mention Très honorable avec les félicitations du jury.
DEA Programmation, Université Paris VII, mention TB.
Agrégation de mathématiques, 1998-1999, reçu 22ème.
Maîtrise de mathématiques, Université Paris VII, 1997-1998, mention TB.
Maîtrise d'informatique, Université Paris VII, 1997-1998, mention TB.
Licence de mathématiques, ENS Cachan, 1996-1997, mention B.
Admission à l'ENS Cachan, 1996.
Baccalauréat C, 1993, mention B.

[BB01] Michel Bidoit et Alexandre Boisseau. Abstract interpretation: an algebraic approach. In *Proceedings of the 15th International Workshop on Algebraic Development Techniques (WADT'01)*, Gênes, Italie, 1-3 avril 2001.

CORTIER Véronique Née le 31 mars 1978, à Troyes (02).
Nationalité Française
Mél : cortier@lsv.ens-cachan.fr
Poste actuel : Doctorante à l'EDSP depuis septembre 2000.
Directeur de thèse H. Comon,
Sujet : « Vérification automatique des protocoles cryptographiques »

Diplômes : Agrégation de mathématiques, 2000, reçu 52ème.
DEA Logique et Fondements de l'Informatique, Université Paris VII, mention TB.
Maîtrise de mathématiques, Université Paris VII, 1999, mention TB.
Licence de mathématiques, ENS Cachan–Paris VII, 1998, mention B.
Admission à l'ENS Cachan, 1997.
DEUG de mathématiques, Université Paris VI, 1997, mention AB.
Baccalauréat S, 1995, mention TB.

[CC00] H. Comon et V. Cortier. Flatness is not a weakness. In *Proceedings of the 14th International Workshop on Computer Science Logic (CSL'2000)*. Springer Verlag Lecture Notes in Computer Science 1862, pages 262–276, 2000.

[CCM01] H. Comon, V. Cortier, et J. Mitchell. Tree automata with one memory, set constraints and ping-pong protocols. In *Proceedings of the International Conference on Algebra, Logic, and Programming (ICALP'01)*. À paraître.

[CGJV99] V. Cortier, H. Ganzinger, F. Jacquemard, et M. Veanes. Decidable fragments of simultaneous rigid reachability. In *Proceedings of the 26th International Colloquium on Automata, Languages, and Programming (ICALP'99)*. Springer Verlag Lecture Notes in Computer Science 1644, pages 250-260, 1999. Version étendue : rapport MPI I-1999-2-004.

[CMR01] V. Cortier, J. Millen, et H. Ruess. Proving secrecy is easy enough. In *Proceedings of the 14th International IEEE Computer Security Foundations Workshop*, Keltic Lodge, Nova Scotia, Canada. IEEE Press, juin 2001.

DEMRI Stéphane Pinhas	Né le 07 décembre 1967, à Paris (75).
	Nationalité Française
Mél :	demri@lsv.ens-cachan.fr
Poste actuel :	Chargé de recherche CNRS première classe, au Laboratoire LEIBNIZ, UMR 5522, depuis octobre 1995.
	En stage de recherche depuis octobre 2000 au LSV/CNRS UMR 8643, ENS de Cachan

Diplômes : Doctorat en Informatique de l'Institut National Polytechnique de Grenoble, Mention très honorable avec félicitations du jury, décembre 1994.
DEA de l'Institut National Polytechnique de Grenoble, septembre 1990, Mention B.
Ingénieur de l'Ecole Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble, Mention B, juin 1990, .

[Dem00] S. Demri. The nondeterministic information logic NIL is PSPACE-complete. Fundamenta Informaticae 42(3-4):211–234, 2000.

[Dem01a] S. Demri. Modal logics with weak forms of recursion: PSPACE specimens. In M. de Rijke, H. Wansing, F. Wolter, et M. Zakharyaschev, éditeurs, *Advances in Modal Logics, selected papers from 3rd Workshop on Advances in Modal Logics (AIML'2000), Leipzig, Germany, Oct. 2000*. CSLI, 2001. À paraître.

[Dem01b] S. Demri. The complexity of regularity in grammar logics and related modal logics. Journal of Logic and Computation, 2001. Accepté, à paraître.

[DS98] S. Demri et Ph. Schnoebelen. The complexity of propositional linear temporal logics in simple cases (extended abstract). volume 1373, pages 61–72, 1998. Version journal en [DS01].

[DS01] S. Demri et Ph. Schnoebelen. The complexity of propositional linear temporal logics in simple cases. Information and Computation, 2001. Accepté, à paraître.

ROGER Muriel	Née le 17 août 1972, à Paris (75). Nationalité Française
Mél :	roger@lsv.ens-cachan.fr
Poste actuel :	Doctorante à l'université Paris VII depuis octobre 1999, puis à l'EDSP depuis octobre 2000. Directeur de thèse J. Goubault-Larrecq, Sujet : ≪ Comparaison formelle de modèles de protocoles cryptographiques ≫, anciennement ≪ Audit de logs et model-checking ≫.
Diplômes :	DEA Programmation, Université Paris VII, mention TB, 1999. Licence d'informatique, Université Paris VII, 1998. Maîtrise de mathématiques, Université Paris VII, 1997. Licence de mathématiques, Université Paris VII, 1995. DEUG SMV, Université Paris VII, 1994. Baccalauréat C, 1991.

[RGL01] Muriel Roger et Jean Goubault-Larrecq. Log auditing through model-checking. In *Proceedings of the 14th International IEEE Computer Security Foundations Workshop*, Keltic Lodge, Nova Scotia, Canada. IEEE Press, juin 2001.

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

PRESENTATION DU PROJET

Objectifs du projet

Le but de ce projet est ambitieux, et consiste à développer plusieurs approches de la sécurité informatique ainsi que des ponts entre ces approches. L'optique est de construire un pôle d'excellence au LSV en matière de sécurité informatique.

Notamment, nous proposons de développer des méthodes automatiques de vérification de protocoles cryptographiques dans le but typique de vérifier la sécurité des systèmes de commerce électronique, des frontaux de sécurité, des portails Internet ou GSM. D'autre part, la sécurité étant un problème global, il est aussi nécessaire de s'intéresser à d'autres méthodes de sécurisation de systèmes d'information, et une approche prometteuse est la détection d'intrusion en temps réel, par analyse de fichiers de logs. Une approche originale développé chez Dyade puis au LSV est d'effectuer une analyse des logs par des techniques suffisamment adaptées de model-checking [RGL01]. On notera que si le projet est ambitieux en terme de diversité des approches de sécurité traitées, les porteurs du présent projet en ont les moyens, et capitalisent sur leur expertise dans les domaines du model-checking (ici appliquée à la détection d'intrusions [RGL01]), de la théorie des automates pour ce qui est des protocoles cryptographiques [Gou00b], et de la vérification en général.

Les deux approches présentées ci-dessus sont en fait complémentaires, et il est primordial de les faire collaborer dans une optique de globalisation de la sécurité. Ainsi, une vérification d'un protocole cryptographique qui ne conclut pas à la sécurité du protocole donne une description des attaques possibles contre ce protocole. Il est alors possible de décrire ces attaques sous forme de signatures d'attaques qui viendront alimenter un outil d'audit de logs comme celui de [RGL01]. Ceci résout ainsi, au moins partiellement, mais de façon rigoureuse, l'un des problèmes les plus cruciaux dans les outils d'audit à base de signatures, à savoir quelles sont les signatures devant alimenter l'outil d'audit de logs. Ainsi, les deux approches apparemment sans point commun de vérification de protocoles cryptographiques et de détection d'intrusions trouvent-elles une complémentarité naturelle.

En général, nous souhaitons fédérer diverses approches de la sécurité, en exploitant les synergies entre approches différentes, dans le but de proposer un environnement de sécurisation globale des systèmes d'information.

Aspects novateurs du projet. Le thème de la vérification, de la vérification automatique en particulier, de protocoles cryptographiques est un thème porteur ayant des applications industrielles importantes. Il pose des problèmes intéressants dans la théorie des automates d'arbres (et extensions) et des contraintes ensemblistes, qui fournissent des bases logiques importantes pour la vérification de propriétés de confidentialité, d'authentification, voire de non-duplication et de non-répudiation de messages, par des méthodes d'approximation terminantes et précises que nous nous proposons d'étudier et d'approfondir.

De même, le thème de la détection d'intrusions est un thème de recherche émergent, qui mérite une approche plus rigoureuse que la collection de méthodes ad hoc existant à l'heure actuelle dans la littérature. L'approche d'audit de logs par model-checking que nous avons récemment proposée est un premier pas prometteur dans cette direction. Il reste à examiner les problèmes de complexité de cette approche, d'optimisation des algorithmes, et d'aide à l'écriture des signatures d'attaques.

Mais l'aspect le plus novateur du projet est clairement notre souci de prendre en compte l'aspect global de la sécurité, à commencer par l'interaction que nous avons décrite plus haut entre vérification de protocoles cryptographiques et détection d'intrusions. À l'avenir, nous envisageons d'intégrer d'autres approches, en particulier de modèles de droits d'accès et de flux d'informations (à la Bell-La Padula), ou par analyse statique de code sécuritaire téléchargé : le travail [EK01], dû à un ancien étudiant de thèse de J. Goubault-Larrecq, montre la voie dans ce domaine.

À notre connaissance, personne ne travaille encore sur de telles interactions, et les diverses communautés, de vérification de protocoles cryptographiques, de détection d'intrusions, d'analyse statique de code notamment, sont encore isolées les unes des autres. Il est important aujourd'hui de dégager des synergies entre les diverses approches de la sécurité.

Place du projet dans le contexte international

Thématique des protocoles cryptographiques. Le domaine de la vérification de protocoles cryptographiques est aujourd'hui un domaine de recherche actif à travers le monde. En France, outre le LSV, l'INRIA Lorraine (M. Rusinowitch), France Télécom R&D (F. Klay, T. Genet), l'université de Provence à Marseille (R. Amadio, D. Lugiez), Verimag (Y. Lakhnech), et des industriels comme Trusted Logic (D. Bolignano), travaillent sur la vérification de protocoles cryptographiques.

À l'étranger, on compte de nombreux chercheurs intéressés par l'étude de protocoles cryptographiques. En Grande-Bretagne, il faut mentionner Gavin Lowe, à Cambridge, qui est probablement la personne au monde qui a trouvé le plus d'attaques contre le plus de protocoles cryptographiques publiés, et Larry Paulson, à Cambridge aussi, auteur de l'assistant de preuve Isabelle, et qui a proposé depuis 1997 une méthode de vérification de protocoles cryptographiques proche de celle de D. Bolignano (Dyade, puis Trusted Logic).

En Amérique du Nord, Martín Abadi, aujourd'hui chez Lucent Technologies, est sans doute la personne qui a eu, et a toujours, le plus d'influence sur la conception de modèles et de méthodes de vérification de protocoles cryptographiques : il est l'auteur ou le coauteur de nombreux travaux importants fondés sur des logiques modales, des algèbres de processus, ou des systèmes de types. De nombreux systèmes automatiques ont été inventés aux États-Unis dans le but de découvrir des attaques sur des protocoles cryptographiques, dûs à Catherine Meadows (Naval Research Laboratory), ou à Jon Millen et ses collaborateurs à SRI, Palo Alto. Microsoft Research a aussi une activité dans ce domaine (Cédric Fournet et Andrew Gordon, ce dernier étant un ancien étudiant de M. Abadi). Plusieurs équipes universitaires s'intéressent aussi à la sécurité des protocoles cryptographiques, citons en particulier celle de John Mitchell (Stanford), en collaboration avec Andre Scedrov (Pennsylvania State University, Philadelphie) et Patrick Lincoln (SRI), ou bien Scott Stoller (State University of New York, Stony Brook), ou encore Mourad Debbabi et son équipe (Université Laval, Québec, Canada).

Ceci ne prétend pas être une liste exhaustive des chercheurs du domaine, mais une liste des acteurs de premier plan du domaine. Ceci s'entend hors équipes dont le thème est la cryptologie proprement dite, comme celle de Jacques Stern à l'École Normale Supérieure, de François Morain à l'École Polytechnique, de Jean-Jacques Quisquater à Louvain-la-Neuve, de Mihir Bellare à Stanford par exemple.

Les conférences du domaine sont le *Computer Security Foundations Workshop* de l'IEEE, la *Conference on Security and Privacy* de l'IEEE, et *Computer-Aided Verification*, encore que de plus en plus de conférences publient maintenant des articles dans ce domaine.

Thématique de la détection d'intrusion. La détection d'intrusions est un domaine extrêmement diversifié et sans aucun doute beaucoup plus ancien que celui de la sécurité des protocoles cryptographiques. L'équipe de Mireille Ducassé à l'IRISA (Rennes), de Ludovic Mé (SupÉlec Rennes), de Frédéric Cuppens à l'ONERA, de Baudouin Le Charlier aux FUNDP (Namur, Belgique), d'Hervé Debar (France Télécom R&D Caen), sont quelques équipes européennes travaillant dans ce domaine. On citera aussi l'équipe STAT à l'université de Californie à Santa Barbara (Phillip Porras, Koral Ilgun, Richard Kemmerer, Steven Eckmann, Giovanni Vigna), ou l'équipe de l'université de Purdue dans l'Indiana (le système IDIOT, Sandeep Kumar, Mark Crosbie, Bryn Dole, Todd Ellis, Ivan Krsul, Eugene Spafford), qui sont probablement les équipes les plus connues en détection d'intrusion par audit de logs, à base de signatures. Si d'autres équipes à travers le monde ont aussi une activité de recherche dans ce sous-domaine précis, on ne compte plus les équipes s'intéressant à la détection d'intrusion par d'autres méthodes (data-mining, immunologie, réseaux neuraux et apprentissage, etc.)

Les conférences typiques du domaine sont l'IEEE *Symposium on Security and Privacy* et l'ACM *Workshop on Intrusion Detection Systems*, ou des conférences organisée par l'association USENIX comme la *Systems Administration Conference* ou le *USENIX Security Symposium*. La conférence qui émerge comme majeure dans ce domaine est *Recent Advances in Intrusion Detection* (RAID).

Relation de l'équipe avec les acteurs mentionnés. Les acteurs du projet sont en relation avec des industriels comme Bull, ou les PME Trusted Logic et NetSecure Software, ainsi que les universitaires français mentionnés ci-dessus.

En matière de protocoles cryptographiques, le LSV entretient des collaborations avec la plupart des acteurs mentionnés plus haut. Ceci se matérialise par exemple par des publications communes entre V. Cortier, J. Millen et H. Ruess de SRI, ou entre V. Cortier, H. Comon (du LSV, en congé sabbatique à Stanford pour 2000-2001) et J. Mitchell (Stanford). J. Goubault-Larrecq est en 2001 rédacteur en chef invité d'un numéro spécial du jeune journal International Journal of Telecommunications and Information Technology (JT&IT), où ont notamment accepté de collaborer David Pointcheval (de l'équipe de J. Stern, ENS Ulm), Jon Millen (SRI), et Vitaly Shmatikov, un étudiant de J. Mitchell, Stanford (en collaboration avec H. Comon). Jon Millen et Scott Stoller (SUNY Stony Brook) sont par ailleurs membres du comité de programme du premier Workshop on Logical Aspects of Cryptographic Protocol Verification (LACPV, satellite de CAV'2001), organisé par J. Goubault-Larrecq en juillet 2001.

En matière de détection d'intrusions, J. Goubault-Larrecq et Muriel Roger ont apporté avec eux au LSV leur technique novatrice de détection d'intrusion par model-checking, ainsi que des contacts avec l'IRISA, France Télécom R&D Caen, SupÉlec Rennes, l'ONERA, et NetSecure Software (Neuilly, France). L'activité de détection d'intrusions au LSV est neuve (fin 2000), alors que les compétences du LSV en model-checking et en vérification sont aujourd'hui reconnues internationalement. De façon significative, on rappelle que c'est le LSV qui organise la conférence majeure du domaine de la vérification au niveau mondial, CAV (Computer-Aided Verification), en 2001.

Rappelons que si l'équipe offre des forces indéniables dans les deux domaines, tant celui de la sécurité des protocoles cryptographiques que celui de la détection d'intrusions par model-checking, sa véritable originalité est dans l'interaction proposée entre les deux. À notre connaissance, personne ne travaille encore sur de telles interactions, et les diverses communautés, de vérification de protocoles cryptographiques, de détection d'intrusions notamment, mais aussi d'analyse statique de code, sont encore isolées les unes des autres. Il est important aujourd'hui de dégager des synergies entre les diverses approches de la sécurité.

Originalité du projet par rapport au projet du laboratoire

Le projet du laboratoire est centré sur le thème de la spécification et la vérification de logiciels, dans l'optique d'amener de nouvelles méthodes permettant la conception de logiciels sûrs. Les axes de recherche peuvent être regroupés en cinq domaines : systèmes de transitions infinis, systèmes temporisés, complexité du model-checking, compositionnalité et modularité, preuve et réécriture. Les outils scientifiques utilisés dans ces domaines ressortissent de la logique, notamment de la réécriture et du domaine des logiques temporelles, ainsi que de la théorie des automates et des réseaux de Petri.

En termes de moyens scientifiques, le projet proposé ne se démarque pas fondamentalement du laboratoire. Les outils se nomment ici aussi automates d'arbres, ou logiques temporelles, notamment. La véritable originalité du projet par rapport à celui du laboratoire tient davantage aux applications envisagées : si le LSV est aujourd'hui surtout spécialisé en *sûreté* de fonctionnement, le projet proposé s'intéresse à divers aspects de *sécurité* informatique. La différence essentielle entre les deux est qu'en sûreté, le système informatique à étudier est entièrement spécifié, et il s'agit de s'assurer que ce système n'autorise aucun comportement non souhaité; alors qu'en sécurité, le système informatique étudié contient, outre une part bien spécifiée, un ou plusieurs *intrus* dont les actions sont arbitraires, et limitées uniquement par l'imagination ou les capacités technologiques des attaquants. Un des premiers points à définir est l'ensemble des limitations plausibles des intrus — le *modèle de sécurité* —, avec comme conséquences l'étude des moyens de conception ou de certification d'une architecture de sécurité.

Les différences dans la nature des applications visées mènent à de nouveaux problèmes à traiter. Un cas symptomatique, étudié dans [RGL01], est l'inadéquation de la logique temporelle pourtant la plus adaptée a priori au problème de l'audit de logs, la logique du temps linéaire, et la nécessité en conséquence de concevoir une logique temporelle spécifique — ce qui a été fait dans op.cit. La complexité exacte du model-checking de cette dernière est encore un problème ouvert, qu'il serait intéressant d'étudier (l'efficacité est primordiale en détection d'intrusions). Un autre cas symptomatique est celui des protocoles cryptographiques [Gou00b], où l'on a été amené à étudier des approximations de systèmes de transitions infinis (incluant un intrus modélisé par un système de déduction, et un nombre potentiellement non borné de processus exécutant le même programme) par un système de transitions à contrôle fini, chaque état étant composé d'un point de contrôle et d'un n-uplet d'automates d'arbres. Dans les systèmes de transitions infinis traditionnels en sûreté, la partie infinie consiste usuellement en ensembles d'entiers définissables en arithmétique de Presburger, ou en ensembles de mots semi-linéaires approximant des contenus de files ou de piles. Si les moyens utilisés sont de même nature que ceux qui forment le fonds de commerce du laboratoire, ils en diffèrent donc néanmoins beaucoup dans les détails.

Aspects pluridisciplinaires

Le projet, qui mêle étude de protocoles cryptographiques et détection d'intrusion, avec des extensions possibles dans le domaine de l'analyse statique de programmes, est déjà de ce fait un projet pluridisciplinaire.

L'étude de la sécurité des protocoles cryptographiques implique d'autre part plusieurs outils logiques : automates d'arbres [Gou00b], contraintes ensemblistes [CCM01], théorie de la preuve [EK01], interprétation abstraite [EK01, Gou00b]. Les liens avec les algèbres de processus sont aussi forts, et Muriel Roger étudie dans son travail de thèse les liens entre modèles à base d'algèbres de processus (le spi-calcul d'Abadi et Gordon notamment, dont la sémantique est précise, mais dont l'automatisation est délicate) et modèles à la Dolev-Yao-Bolignano-Paulson [EK01, Gou00b, CCM01] (qui se prêtent bien à l'automatisation, mais dont la sémantique reste encore relativement abstraite).

La détection d'intrusions est par nature un domaine extrêmement pluridisciplinaire : automates, statistiques (data-mining), immunologie, réseaux neuronaux, théorie de l'apprentissage, ..., de nombreuses technologies ont été employées dans ce domaine jusqu'ici. Cependant la plupart de ces approches sont relativement ad hoc, et l'optique des travaux de l'équipe, illustrée dans [RGL01], est d'imposer une véritable sémantique formelle au langage de description des scénarios d'attaques. On fait ici appel au domaine des logiques temporelles, en particulier aux méthodes de model-checking des logiques temporelles.

Méthodologie envisagée

Ce projet inclut différents problèmes à traiter, dans différents domaines participant tous de la sécurité informatique. Ces problèmes incluent des volets théoriques (complexité, algorithmique, sémantique) ainsi que des volets pratiques (réalisation informatique d'outils). Chacun des aspects théoriques voyant sa justification dans l'application pratique correspondante, nous chercherons en particulier des études de cas réalistes permettant de valider les approches proposées, ou au contraire de les corriger et les adapter.

Plus concrètement, les thèmes d'activité proposés sont :

Thème 1. Étude théorique de **nouvelles méthodes de vérification approchée de protocoles cryptographiques** par automates d'arbres et contraintes ensemblistes, à la suite de [CCM01, Gou00b]. Si la confidentialité est une propriété que la plupart des méthodes automatiques actuelles savent traiter, il en est autrement de l'authentification (précisément, des différentes propriétés prétendant chacune au nom d'authentification), ainsi que de propriétés plus subtiles mais aussi importantes dans le domaine du commerce électronique, comme la non-duplication ou la non-répudiation de messages. Une forme faible d'authentification ("le message reçu par B n'a pu être créé que par A") semble pouvoir être traitable par des méthodes proches de celles utilisées en confidentialité.

En ce qui concerne la forme des protocoles cryptographiques analysés, tous les auteurs qui se fondent sur un modèle à la Dolev-Yao supposent que le système à analyser est une composition parallèle d'un intrus et d'un nombre *fini* de processus en parallèle. Ceci n'est pas réaliste, ne serait-ce que parce que les serveurs de clés fonctionnent à tous points de vue comme une composition parallèle d'un nombre *infini* (en tout cas non borné) de processus ayant le même contrôle fini — le mode *multi-sessions parallèles*. Seuls quelques auteurs considèrent les multi-sessions parallèles [DMTY97, Gou00b]. Aucun n'est encore capable de gérer les multi-sessions séquentielles, à savoir le cas où les processus mis en parallèle contiennent des boucles. (L'approximation d'une boucle par une mise en parallèle du corps de la boucle avec elle-même un nombre infini de fois est correcte, mais insuffisamment précise.) Des techniques d'*élargissements*, aussi connues sous le terme d'*accélérations*, sont notamment à développer, en l'occurrence dans le domaine des automates d'arbres pour ce qui est de la méthode de [Gou00b].

Thème 2. **Réalisation d'un ou plusieurs prototypes de vérificateur de protocoles cryptographiques**, sur les principes développés dans le thème 1. Il devra permettre de valider l'effectivité et l'efficacité des techniques précédentes, et si possible fournir en sortie une description des attaques possibles. Le prototype `CPV` développé par J. Goubault-Larrecq à Dyade en 2000 peut être considéré comme l'ancêtre de ce prototype à venir. (`CPV` ne traite que de la confidentialité, pas des multi-sessions séquentielles, traite en partie des multi-sessions parallèles, et ne fournit pas de description des attaques possibles.)

Thème 3. Étude de la **complexité du model-checking pour les logiques temporelles utilisées en détection d'intrusions**, à commencer par celles proposées dans [RGL01]. Ceci devrait mener à des raffinements de ces logiques, dans le double but de préserver le pouvoir d'expression nécessaire à la description des attaques qui se présentent en pratique, tout en améliorant les performances de l'outil de détection d'intrusions par model-checking. L'outil actuel, log$\mathcal{W}$eaver version 2.6, développé à Dyade en 2000 puis au LSV en 2001, se fonde sur la deuxième logique de [RGL01] et un algorithme qui, s'il semble efficace sur quelques exemples, est néanmoins exponentiel. On ne sait pas aujourd'hui si le problème du model-checking de cette logique est NP-complet ou s'il peut être effectué en temps polynomial. (Le problème est dans NP.) Dans le premier cas, il sera nécessaire de comprendre les constructions forçant la NP-complétude et si possible de les éliminer; dans le second cas, la preuve fournira des idées d'optimisations de l'algorithme de log$\mathcal{W}$eaver.

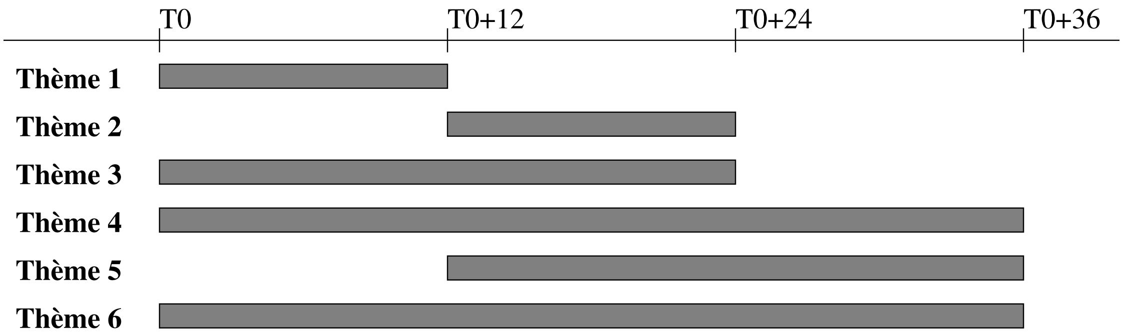
Thème 4. **Évolution de l'outil** log$\mathcal{W}$eaver d'audit de logs (détection d'intrusions) par model-checking, à la lumière du point précédent. Ceci inclut les améliorations algorithmiques suggérées ci-dessus. Ceci inclut aussi des enrichissements de la logique dont log$\mathcal{W}$eaver effectue le model-checking, qui pourront être suggérés par l'étude de la complexité, dans la mesure où ces enrichissements sont potentiellement utiles, et ne coûtent pas en complexité temporelle ni spatiale.

Thème 5. **Études de cas**. L'équipe entretient de bonnes relations avec les industriels de la carte à puce (qui sont français : Gemplus, Schlumberger/CP8, Oberthur Card Systems), avec Trusted Logic, et avec Bull (le GIE Dyade où travaillait J. Goubault-Larrecq jusqu'en 2000 était un GIE commun entre Bull et l'INRIA). Il serait souhaitable de nouer des liens avec un ou plusieurs de ces acteurs, qui permettraient à l'équipe de disposer d'études de cas réalistes sur lesquelles tester ses techniques de vérification de protocoles cryptographiques, et/ou de détection d'intrusion. En l'absence de telles collaborations, des protocoles publiés comme SSL (Netscape) fourniront déjà des études de cas suffisamment réalistes.

Ces études de cas devraient permettre notamment de guider l'évolution du prototype de vérificateur de protocoles cryptographiques, ainsi que de l'outil log$\mathcal{W}$eaver, et de cerner les besoins d'une plateforme de sécurisation globale comprenant sécurité statique (vérification de protocoles cryptographiques) et dynamique (détection d'intrusions).

Thème 6. Étude de formalisme d'**analyses statiques de code** permettant d'aider à l'extraction d'une spécification de protocole cryptographique à partir d'une implémentation (partant de travaux comme [EK01], par exemple). L'expérience montre que les besoins industriels portent en effet rarement sur un algorithme ou une spécification, et beaucoup plus souvent sur du code existant. La difficulté qu'il y a à analyser un protocole cryptographique sont démultipliées si ce protocole n'est disponible que sous forme d'un gros programme, mélangeant aspects de protocoles, d'architecture, d'interface homme-machine, de bases de données, etc. À l'heure actuelle, aucune solution n'est disponible. En principe, l'interprétation abstraite fournit un cadre à ce domaine, mais des domaines d'interprétation abstraite spécifiques demandent à être développés. En attendant, toute analyse d'un protocole cryptographique sous-jacent à un programme dont le texte source est donné doit passer d'abord par une relecture attentive, par un expert, du texte source, activité donnant lieu à toutes sortes d'erreurs. L'utilisation de l'interprétation abstraite serait une solution à ce problème. Il s'agit là d'un travail plus prospectif, qui devra si possible être guidé par des études de cas, et qui recèlent probablement de nombreuses chausses-trappes. (On notera que le langage analysé dans [EK01] n'est pas directement le langage Java, comme le souhaite l'auteur, mais un langage intermédiaire qui mentionne explicitement des primitives de cryptographie. Beaucoup de travail est donc encore nécessaire.)

Calendrier du programme



Collaborations prévues

Sur le domaine des protocoles cryptographiques, il existe des collaborations naturelles entre l'équipe du projet et John Mitchell à Stanford (où H. Comon a passé une année sabbatique en 2000-2001, et où V. Cortier a passé quelques mois en 2001), et avec Jon Millen chez SRI (V. Cortier y a aussi passé quelques mois en 2000-2001). D'autres collaborations sont envisageables avec M. Debbabi (que J. Goubault-Larrecq connaît depuis l'époque où il était doctorant avec D. Bolignano chez Bull) à l'Université Laval, ou avec Trusted Logic (dont le PDG est D. Bolignano, et où Alexandre Boisseau a effectué son stage de DEA en 2000). Sur le plan scientifique, les collaborations avec Stanford et le SRI, qui ont déjà porté des fruits, semblent importantes. Au plan national, l'équipe pense travailler en proche collaboration avec les équipes de R. Amadio et D. Lugiez au LIM à Marseille, et de M. Rusinowitch à Nancy (projet Prothéo, INRIA Lorraine).

À propos de la détection d'intrusion, J. Goubault-Larrecq a des liens avec l'équipe de M. Ducassé à l'IRISA, et les systèmes logWeaver [RGL01] du premier et SuTekh de J.-P. Pouzol, étudiant de la seconde [DP00] ont une origine commune dans le souci de construire un outil meilleur que ASAX [Mou97]. L'équipe espère d'autre part collaborer avec d'autres équipes comme celle de France Télécom R&D Caen (Hervé Debar), de l'ONERA (Frédéric Cuppens), et de SupÉlec Rennes (Ludovic Mé).

Le projet touchant à d'autres disciplines, il est naturel de chercher des collaborations avec des équipes de recherche dans ces disciplines. En matière de model-checking, les collaborations qu'entretient déjà le LSV, avec le LIAFA ou Verimag par exemple seront exploitées et poursuivies. En matière d'analyse statique de code, une collaboration naturelle envisageable est avec l'équipe de Patrick Cousot à l'ENS de la rue d'Ulm. Le thème s'y prête. De plus, J. Goubault-Larrecq et P. Cousot se connaissent depuis longtemps, plus précisément depuis que le premier a effectué sa thèse (en 1990-1993) sous la direction du second.

Références

[CCM01] H. Comon, V. Cortier, et J. Mitchell. Tree automata with one memory, set constraints and ping-pong protocols. In *Proceedings of the International Conference on Algebra, Logic, and Programming (ICALP'01)*. À paraître.

[DMTY97] Mourad Debbabi, Mohamed Mejri, Nadia Tawbi et I. Yahmadi. Formal Automatic Verification of Authentication Cryptographic Protocols. In *Proceedings of the 1st IEEE International Conference on Formal Engineering Methods (ICFEM'97)*. IEEE Press, 1997.

[DP00] Mireille Ducassé et Jean-Philippe Pouzol. Handling Generic Intrusion Signatures is not Trivial. Recent Advances in Intrusion Detection (RAID) Workshop, 2000.

[EK01] Nabil El Kadhi. Automatic verification of confidentiality properties of cryptographic programs. *Networking and Information Systems*, 2001. Accepté.

[Gou00b] Jean Goubault-Larrecq. A method for automatic cryptographic protocol verification (extended abstract). In *Proceedings of the International Workshop on Formal Methods in Parallel Programming, Techniques and Applications*, Springer Verlag Lecture Notes in Computer Science, volume 1800, pages 977–984. 2000.

[Mou97] Abdelaziz Mounji. Languages And Tools for Rule-Based Distributed Intrusion Detection. Thèse de doctorat, Facultés Universitaires Notre-Dame de la Paix, Namur, Belgique. 1997.

[RGL01] Muriel Roger et Jean Goubault-Larrecq. Log auditing through model-checking. In *Proceedings of the 14th International IEEE Computer Security Foundations Workshop*, Keltic Lodge, Nova Scotia, Canada. IEEE Press, juin 2001.

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

JUSTIFICATION FINANCIERE (1/2)

A - Moyens financiers demandés dans le cadre de l'ACI (en kF TTC) : 640 kF

- Justification scientifique des moyens demandés :

On estime les besoins en fonctionnement à un voyage en Amérique du Nord (12 kF), ou un en Europe (9 kF) plus un en France (3 kF), par an et par chercheur en moyenne, pour 5 chercheurs dans l'équipe, soit un total de 60 kF par an.

En équipement, on compte l'achat d'un PC à 20 kF par an, plus 10 kF en petit matériel, entretien et documentation, ce qui fournit une base de 30 kF par an.

L'effort de réalisation informatique se concentre dans le thème 2 et le thème 4. Le thème 4 sera pris en charge par J. Goubault-Larrecq, qui est le créateur de l'outil log$\mathcal{W}$eaver, avec des collaborations possibles d'autres membres de l'équipe. Pour le thème 2, ainsi que le thème 5 (études de cas, du moins la première année du thème 5, $T_0 + 12$–$T_0 + 24$), il est prévu d'embaucher un ingénieur expert, pour un coût de 300 kF la deuxième année. L'effort d'implémentation nécessitera aussi cette même année l'achat d'un serveur, au prix estimé de 50 kF, et d'un PC suppémentaire à 20 kF, pour un coût d'équipement supplémentaire de 70 kF. Le coût d'équipement monte ainsi à 100 kF la deuxième année, contre 30 kF pour les deux autres.

- Récapitulatif global (en kF TTC) :

	Année 1	Année 2	Année 3	Total
Équipement	30	100	30	160
Fonctionnement	60	60	60	180
Personnel temporaire	–	300	–	300
Total/année	90	460	90	640

- Organisme ou établissement qui assurera la gestion financière du projet :
LSV/CNRS UMR 8643, ENS Cachan, 61 av. du président-Wilson, 94235 Cachan Cedex.

PROPOSITION ACI « JEUNES CHERCHEURS » 2001

JUSTIFICATION FINANCIERE (2/2)

B - Autres moyens dont pourra bénéficier le projet :

- Soutien financier provenant du laboratoire ou de l'unité de recherche à laquelle appartient le porteur de projet :

- Demandes de contrats et/ou subventions en cours et contrats et/ou subventions déjà obtenus par le demandeur ou un autre membre de son équipe :

- Proposition RNTL 2 DICO (détection d'intrusions coopérative), déposée.

- Équipements dont pourra bénéficier le projet :