ACI sécurité informatique KAA (Key Authentication Ambient)

Rapport à mi-parcours ACI sécurité informatique

Samuel Galice[1], Véronique Legrand[1], Frédéric Le Mouël[1], Marine Minier[1], Stéphane Ubéda[1], Michel Morvan[2], Sylvain Sené[3], Laurent Guihery[4], Agnès Rabagny[5], Joël Moret-Bailly[5], Jean-Philippe Neuville[6], Jérome Pousin[7],

"Je perds l'enthousiasme et la confiance en moi-même, qualité sans laquelle on ne fait rien de bon"
Flaubert - Correspondance

[1]Centre d'Innovations en Télécommunications & Intégration de services, CITI INRIA ARES, INSA de Lyon, Bâtiment Léonard de Vinci, 21 Avenue Jean Capelle, 69621 Villeurbanne Cedex, mail : prenom.nom@insa-lyon.fr

[2]SFI, EHESS, LIP-ENS Lyon, 46 allée d'Italie, 69364 Lyon Cedex 07, mail : Michel.Morvan@ens-lyon.fr

[3]LIP-ENS Lyon, TIMC-IMAG, Faculté de Médecine, 38706 La Tronche, mail : Sylvain.Sene@imag.fr

[4]Laboratoire d'Economie des Transports (LET-ISH), Institut des Sciences de l'Homme, 14 avenue Berthelot, 69007 Lyon, Laurent.guihery@let.ish-lyon.cnrs.fr

[5]CERCRID, Université Jean Monnet, 6 rue basse des Rives, 42023 Saint-Etienne cedex 2, agnes.rabagny@univ-st-etienne.fr

[6]Centre de Sociologie des Organisations,19, rue Amélie, 75007 - Paris mail : jean-philippe.neuville@insa-lyon.fr

[7]MAPLY, Centre de Mathématiques, INSA de Lyon, 21, avenue Jean Capelle, 69621 Villeurbanne Cedex, mail : Jerome.Pousin@insa-lyon.fr

Table des matières

Les équipes impliquées dans KAA

1. Pour Le CITI (Centre d'Innovations en Télécommunications & Intégration de services), Projet INRIA ARES, INSA de Lyon :
   - Samuel Galice, ingénieur de recherche sur le projet KAA (du 01/11/05 au 31/07/2007).
   - Véronique Legrand, Professeur Associé à temps partiel, informatique.
   - Frédéric Le Mouël, Maître de Conférence en informatique.
   - Marine Minier, Maître de Conférence stagiaire en informatique.
   - Stéphane Ubéda, Professeur, directeur du CITI et du projet INRIA ARES.
2. Pour le LIP (Laboratoire de l'Informatique du Parallélisme), ENS Lyon, TIMC-IMAG :
   - Michel Morvan, Professeur.
   - Sylvain Sené, doctorant au TIMC-IMAG et à l'UJF de Grenoble depuis octobre 2005 sous les directions de Jacques Demongeot (TIMC-IMAG) et de Michel Morvan (LIP-ENS Lyon). Thèse financée par la région Rhône-Alpes (cluster 2 : informatique). Sujet de thèse : "Instabilités structurelles et analyses temporo-spatiales en biologie".
3. Pour le LET-ISH (Laboratoire d'Economie des Transports - Institut des Sciences de l'Homme), Lyon : Laurent Guihery, Maître de Conférence en sciences économiques.
4. Pour le CERCRID (Centre de Recherches Critiques sur le Droit), Université Jean Monnet, Saint Étienne :
   - Agnès Rabagny, Maître de Conférence en droit.
   - Joël Moret-Bailly, Maître de Conférence en droit.
5. Pour le ICTT (Interaction Collaborative - Téléformation - Téléactivités), INSA de Lyon, École Centrale de Lyon : Jean-Philippe Neuville, Maître de Conférence en sociologie.
6. Pour le MAPLY (Centre de Mathématiques), INSA de Lyon : Jérome Pousin, Professeur en mathématiques.

Introduction

Le but premier de cette ACI sécurité informatique pluridisciplinaire est la construction d'un modèle de confiance pour les réseaux dits opportunistes. Dans cette approche, l'hypothèse d'un réseau connecté au sens multi-saut n'est plus du tout prise en compte, les terminaux pouvant s'échanger des messages de façon opportuniste lorsqu'ils se trouvent à portée radio les uns des autres. Avant de pouvoir construire une architecture viable sur ces réseaux, il a tout d'abord fallu définir ce qu'était la confiance au sens de tous les acteurs présents. Dans ce cadre, nous avons décidé de rédiger les parties concernant les sciences humaines en français afin de ne pas dénaturer leurs contenus et les parties concernant les sciences dites dures en anglais.

1 Le point de vue des juristes : régulation juridique et confiance

La confiance semble avant tout relever de l'ordre des sentiments. Or, les recherches relatives aux rapports entre le droit et les sentiments sont peu développées. Le droit constitue, en effet, une modalité d'organisation des rapports sociaux. Or, si l'organisation de tels rapports produits indubitablement des effets renvoyant à la psyché ou au sentiment, tel n'est pas l'objet premier des analyses tant des juristes que des spécialistes de la sociologie du droit. Les deux éléments ne sont, cependant, pas totalement étrangers l'un à l'autre. On peut estimer, en effet, que le sentiment de confiance n'est pas totalement indépendant du contexte dans lequel l'individu va l'éprouver. Or, le droit à un effet sur l'organisation des rapports sociaux, donc sur le contexte dans lequel les actions humaines vont se dérouler. Dans cette perspective, la confiance peut, comme le suggèrent les analyses de M. Morvan, être déclinée en fonction de sa " cible ", par ordre ascendant, la confiance dans l'individu, la confiance dans le groupe, la confiance dans l'institution dans laquelle se déroule l'activité, et enfin la confiance dans la régulation " supra institutionnelle " éventuellement juridique, qui permettra l'application des règles quand bien même l'institution s'en serait affranchie. On conçoit, dans ce modèle, que le droit constitue une " méta régulation sociale ", en ce que, si elle ne peut provoquer, en tant que telle, la confiance des individus, elle permet, cependant, le développement d'activités dans le cadre d'une certaine anticipation.

Une telle approche n'est, évidemment, pas sans rappeler celle de M. Weber [1]. Dans ce modèle, la confiance ne renvoie pas à une qualité que l'on reconnaît à autrui, mais à une prévisibilité de son comportement, du fait du contexte institutionnel dans lequel se déroule l'activité [2]. Dans cette perspective théorique, un mémoire de Mastère 2 Droit et Justice a été soutenu, en septembre 2006, dans le cadre du CERCRID à l'Université Jean Monnet de Saint-Étienne ; celui-ci avait pour objet l'étude des rapports entre le droit des contrats et la confiance [3].

Celui-ci a mis en évidence les résultats suivants : la référence à la confiance est très importante, voire quasi systématique dans les discours des juristes à l'occasion de la présentation générale de la notion de contrat. Ainsi, ces derniers sont présentés comme fondés sur la confiance, puisque nécessitant l'accord des contractant pour exister. Cependant, l'analyse des différentes techniques contractuelles (conclusion du contrat, inexécution contractuelle etc.) laisse, quant à elle, systématiquement de côté la notion de confiance, qui ne permet pas, semble-t-il, de les expliquer.

L'exemple du contrat est particulièrement pertinent pour comprendre les rapports, ainsi que la distance, que le droit entretien avec la confiance. Ainsi, s'il semble acquis que le droit

ne peut, à lui seul, provoquer la confiance dans les individus, dans les groupes, ou dans les institutions, celui-ci peut, cependant, être considéré comme un instrument de réduction des incertitudes et des risques. L'avantage de la règle de droit ou de la prévision contractuelle, en effet, consiste dans la capacité d'anticipation des actions d'autrui que celle-ci permet. En effet, la contemplation des conséquences des choix des acteurs en considération des règles juridiques permet, dans une certaine mesure, d'anticiper leur comportement. On conçoit, ainsi, que le droit permette de réduire les incertitudes quant au comportement à venir des acteurs sociaux. Or, si l'un des comportements possibles est considéré, par l'un des acteurs, comme risqué par rapport à ses intérêts, le droit est alors un facteur de réduction des risques. Une telle présentation permet, en outre, un certain nombre de rapprochements avec l'approche économique de la confiance.

Ainsi, on peut dire que les règles données par le droit permettent de donner confiance dans le "système" plus que confiance en un individu particulier.

Une idée reçue voudrait que le droit soit régulièrement dépassé par l'évolution technologique. Le droit serait constitué de normes prises à un instant T, en fonction de l'état du monde de ce moment, et serait dépassé dès lors que le monde évoluerait, cette évolution entraînant l'existence, voire la béance de " vides juridiques " [4]. Or, s'il est exact que le droit ne peut prévoir l'évolution des techniques, non plus qu'il ne peut prévoir des règles spécifiques à chaque technique nouvelle, cet état de fait ne signifie pas que l'évolution ne pourrait faire face qu'à des " vides ". C'est oublier, en effet, que le droit comprend un certain nombre de règles générales, dont la " texture ouverte " permet leur application à des réalités non envisagées par le législateur au moment de leur édiction [5].

Dans ce contexte, il faut comprendre, d'une part que ce n'est pas parce qu'il n'existe pas de règles spécifiques aux relations qui font l'objet de la présente recherche, qu'il n'existe pas de règles du tout ; les règles générales, notamment les règles de responsabilité, continuent à s'appliquer ; il n'existe pas de vide juridique. Il faut comprendre, d'autre part, que les relations dont il s'agit, pour nouvelles qu'elles soient, ne peuvent échapper aux règles de droit commun.

On peut donc affirmer qu'un modèle technologique de confiance ne saurait échapper aux règles de droit commun, quand bien même il serait techniquement innovant.

Références

[1] M. Weber, "Sociologie du droit", PUF. 1986, trad. J. Grosclaude. Volume composé à partir d'un manuscrit composé entre 1911 et 1913.

[2] P. Lascoumes et E. Serverin, "Le droit comme activité sociale : pour une approche wébérienne des activités juridiques", Droit et société numéro 9, 1988, p. 165-187.

[3] S. Comello, "Droit et confiance", 2006.

[4] M.-C. Rivier, "L'alibi du vide juridique", Économie et humanisme 1991, 22-26.

[5] H.L.A. Hart, "Le concept de droit", trad. M. van de Kerchove, 1976, Publications des facultés universitaires Saint-Louis.

2 Le point de vue des sciences économiques : Premier éléments sur les apports des sciences économiques pour penser des modèles de confiance sur objets autonomes communicants

La question de la confiance a été globalement bien traitée par les sciences économiques, dans différents champs d'analyse (économie monétaire et rôle de la " confiance " dans la monnaie, économie de l'information et nouvelle micro-économie,...). L'économie des contrats et des conventions ont aussi contribué à l'analyse de la confiance, de même que la nouvelle sociologie économique. Plus récemment des apports intéressants viennent de l'économie expérimentale et de la théorie des jeux où la confiance est traitée par un modèle de réputation.

De manière synthétique, on peut dire que la confiance joue plusieurs rôles positifs : réduire l'incertitude (qui s'exerce sur la concurrence et sur l'évolution des marchés en réduisant les coûts de transactions) et atténuer l'asymétrie d'information entre les individus, par exemple entre les fournisseurs et les clients. Elle est donc fondamentale dans le système économique et social. On peut également la percevoir comme un mode de coordination des transactions qui se déroulent au sein de réseaux.

Un séminaire pluridisciplinaire de recherches a été organisé pour mettre en valeur les travaux du volet économique du projet KAA. Il s'est tenu à l'ISH le vendredi 20 janvier 2006 et a regroupé une dizaine de chercheurs. Deux papiers ont été particulièrement analysés : d'abord le papier de Nabila Jawadi [3] qui a travaillé sur la confiance dans les équipes virtuelles. Ce texte place la confiance au centre de la constitution et de l'émergence d'équipes virtuelles. Trois types d'équipes virtuelles ont été proposés : les équipes virtuelles pures, les équipes virtuelles plus classiques, les équipes virtuelles hybrides où une confiance instantanée apparaît " ex ante ". Ces équipes se positionnent sur un espace caractérisé par divers critères : la durée de vie du groupe (courte ou longue), l'expérience antérieure partagée (forte ou faible), la dispersion géographique (forte ou faible), l'interdépendance (forte ou faible). La critique la plus radicale qui a été avancée concerne le pure opportunisme qui peut aussi animer les équipes virtuelles... sans qu'il soit fait référence à une certaine notion de confiance, chaque membre du club en tirant un certain bénéfice propre. Ce papier appelle des recherches complémentaires qui sont en cours. Sur cette question des équipes virtuelles et des mécanismes de confiance dans le monde virtuel, Fabio Linhares et Laurent Guihéry du LET ont travaillé sur l'article de Edward Castronova [6]. Il a été mis en valeur les règles particulières de ces mondes virtuels dédiés aux joueurs qui connaissent aujourd'hui un franc succès. Les liens entre ces mondes virtuels et le concept de confiance sont en cours d'analyse. Il semble néanmoins que, là encore comme dans la vie " réelle " et l'environnement économique et social, les mécanismes de confiance dans ce monde appelé Norrath joue un rôle fondamental.

Le second papier présenté par Dimitri Dubois [2] s'est intéressé à la " confiance dans les interactions économiques et sociales " et traite plus globalement de la confiance dans la théorie économique. Il rappelle que la confiance est fondamentale est peut être considérée comme un " capital social ". De manière globale, la confiance affecte positivement de nombreux indicateurs de performance économique [5] : elle est donc fondamentale dans le système économique et social.

A partir de cette introduction, il apparaît que 3 pré requis sont indispensables : *le risque*, lié au temps ou à l'incomplétude informationnelle, *l'interdépendance* entre celui qui fait confiance et celui qui reçoit la confiance, *la vulnérabilité* (celui qui fait confiance se rend vulnérable vis à vis de celui à qui appartient la décision d'honorer ou non la confiance).

Cette présentation a suscité de nombreux débats car la méthodologie avancée emprunte la voie de l'économie expérimentale, ce qui a permis à un collègue de Lyon 2 de se joindre au groupe pour participer au débat. La plupart des développements s'appuie ainsi sur " the investment game " [1].

Les perspectives futures de recherche s'inscriront dans plusieurs axes :

- économie expérimentale avec une coopération avec des chercheurs du GATE qui a été initiée avec succès. Les protocoles de " confiance " sont ainsi nombreux a être testés avec cette méthodologie [2].
- l'économie institutionnelle autour des liens confiance - civisme - institutions ce qui permet de caractériser certains fondements comparés de nos sociétés et donc d'éclairer les modèles de confiance plus ou moins opératoires.
- Enfin une demande réelle des chercheurs en science dure vise à investir le champ de recherche de la monnaie virtuelle. Nous tenterons donc de préciser rapidement les tenants et aboutissants de cette notion de monnaie virtuelle à la lumière des sciences économiques [4].

Références

[1] J. Berg, J. Dickhaut et K. McCabe, "Trust, Reciprocity and Social History", In *Games and Economic Behavior 10*, p. 122-142, 1995.

[2] D. Dubois, " Confiance et population : doubles rôles et information dans le jeu de l'investissement répété ", LAMETA, Université de Montpellier 1. working paper, juin 2005, version préliminaire.

[3] N. Jawadi, " Nature et développement de la confiance dans les équipes virtuelles ". Université de Paris Dauphine, Dauphine Recherche en Management, Laboratoire CREPA, 2005.

[4] M. Jakobsson, J.-P. Hubaux, and L. Buttyán, "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks". 7th International Financial Cryptography Conference (FC), 2003.

[5] S. Knack, " Confiance, vie associative et performance économique ". papier de recherche, 1997.

[6] E. Castronova, "Virtual worlds : a first-hand account of market and society on the cyberian frontier". CESifo Working Paper No. 618, December 2001.

3 Une première approche technologique : A cryptographic protocol to establish trust history interactions

Nowadays, wireless communications are a critical aspect of computing devices, and offer open solutions for providing mobility and autonomous actions : A smart device as the center of a Personal Area Network is only one major device in an environment where every object will soon be able to communicate and devices in radio range can potentially establish self-organized networks of two or more objects. In such a context, the peer-to-peer communication capabilities of smart objects will not be restricted simply to access fixed networks and mobility during the use of more complex services, addressed by means of ad hoc communication capabilities, will necessarily receive more attention.

However without centralized trusted agents, we are facing a risk management problem requiring a specific security model and associated cryptographic techniques. Also, we propose a trust decision based on the use of informations cryptographically proved, to reduce this risk. Roughly, smart devices record past interactions between autonomous nodes in an *History* (after a bootstrap phase) ; to interact, nodes first search common interactions in their history ; then, they mutually authenticate ; and finally, they prove, using a security protocol, called *Common History Extraction* (CHE) protocol (implementing a trust management framework), that these common interactions really took place. If the number of such common interactions is sufficient that is, upper a certain threshold, then the interaction may occur [4].

The security protocol CHE is based on the notion of cryptographic ID first introduced by A. Shamir [5], adapted to elliptic curves by D. Boneh and M. Franklin [1] for the cipher and used by Chen, Zhang and Kim [2] for a signature without a trusted PKG (Private Key Generator). The main advantages to use elliptic curve ID based cryptography is the gain in size and in computational time in adequacy with small devices used in ambient networks such as PDAs or smart phones. Moreover, user's public key being or being derived from his identity, there is no requirement of public key directories. Also, key distribution being far simplified, this make ID-based cryptosystems advantageous over the traditional Public Key Cryptosystems (PKCs).

We also have described a second security protocol called the CHEWA (Common History Extraction With Authentication) protocol that includes a strong off-line authentification provided by a two-level off-line certification using the Gentry's Certificate-based encryption [3] instead of the encryption version proposed in [1].

We have computed the potential size of the history and the threshold number of common nodes contained in the history computing the corresponding probability of success inspired from the birthday paradox. For example, if the number of nodes present in the network is 100 and the size of history is 22 (using a least-recently-used (LRU) eviction policy), the success probability to share at least 5 common nodes is about $56,6\%$ and for 3 common nodes this probability reachs 92%. In this case, we could see that the size of the history is reasonable and could be easily carried by each node.

Moreover, to initiate an interaction, the node that provides a service to an other sends it the concatenation of all the public keys Q_{ID} that it has in its history. Each public key is 160 bits length, so in the most popular case with an history containing 30 elements, it must send a chain of 600 bytes, that is very reasonable.

In addition, with a threshold equal to 3, the number of verifications that must be done is very low. We have tested our protocol on a PC powered by a 3 Ghz Pentium IV and have

found that the duration for ciphering and signing using our protocol is about 0.78 and 0.9 ms. This is also the duration for the verification of an element.

In a near future, we want to provide a formal proof of security for this protocol.

Acknowledgment The professor John Mullins from the Ecole Polytechnique de Montréal joins the research while visiting the CITI Lab and the INRIA ARES project during his sabbatical.

Références

[1] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In *Advances in Cryptology - Crypto'2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[2] X. Chen, F. Zhang, and K. Kim. A new ID-based group signature scheme from bilinear pairings. In *Information Security Applications, 4th International Workshop - WISA'03*, volume 2908 of *Lecture Notes in Computer Science*, pages 585–592. Springer-Verlag, 2003.

[3] Craig Gentry. Certificate-based encryption and the certificate revocation problem. In *AIC - EUROCRYPT'03*, LNCS 2656, p. 272-293. Springer, 2003.

[4] Véronique Legrand, Dana Hooshmand, and Stéphane Ubéda. Trusted ambient community for self-securing hybrid networks. Research Report 5027, INRIA, 2003.

[5] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology - Crypto'84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1984.

4 une seconde approche technologique : A Distributed Trust Diffusion Protocol for Ad Hoc Networks

Ad hoc networks can be defined as collections of mobile nodes, distributed and independent, being able to communicate by radio transmission and to self-organize. They constitute networks with unstable infrastructure. Since the neighborhood of every node changes over time, it is important to develop protocols that will help each node to identify reliable other nodes with which it can interact safely.

Let us present two definitions of the concept of *trust* given by the Webster's classic 1913 : *"Firm reliance on the integrity, ability, or character of a person or thing"* and *"Certainty based on past experience"*. Trust is therefore a natural notion acquired and systematically used by anyone to decide if an exchange with somebody else is conceivable or not. Let us remark that the trust we can have in somebody usually depends on the personal knowledges we have about the person and also on his/her reputation according to other people we have already met. This is usually the way that trust diffuses in human groups. For example, a researcher can trust the scientific opinion of a colleague while not trusting the opinion of the same colleague about the work of other scientists. The idea is to transfer this human trust diffusion protocol to ad hoc networks. Literature about trust management in P2P systems [1, 2] presents some solutions using both personal and external opinions. However, these protocols do not offer protection against attacks made by a set of nodes working in coalition, for example diffusing wrong positive opinions about a dishonest node (called Trojan attack further in the paper). That is why we propose in this paper to study a management policy that also measures the trust quality by introducing a *new level of trust* that adds weights both on a node own experiences and on external knowledges this node has received from the others.

Let us call *efficient* a protocol that leads to prevent bad interaction and *reliable* a protocol that aims at favoring good interactions. This work consists in creating, studying and validating by simulations a new efficient distributed trust diffusion protocol for ad hoc networks using the double level of trust described above.

We have proposed and evaluated a distributed protocol to manage trust diffusion in ad hoc networks. In this protocol, each node i maintains a "trust value" about an other node j which is computed both as a result of the exchanges with node j itself and as a function of the opinion that other nodes have about j. These two aspects are respectively weighted by a trust index that measures the trust quality the node has in its own experiences and by a trust index representing the trust the node has in the opinions of the other nodes. Simulations have been realized to validate the robustness of this protocol against three kinds of attacks : simple coalitions, Trojan attacks and detonator attacks.

Références

[1] Sonja Buchegger and Jean-Yves Le Boudec. A Robust Reputation System for P2P and Mobile Ad-hoc Networks. *P2P and Mobile Ad-hoc Networks, Second Workshop on the Economics of Peer-to-Peer Systems*, 2004.

[2] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The EigenTrust Algorithm for Reputation Management in P2P networks. *The Twelfth International World Wide Web Conference*, 2003.

Conclusion

Nous venons de confronter dans ce rapport les différents points de vue que les acteurs de l'ACI peuvent avoir de la confiance. Pour les juristes, cette dernière reste une modalité de construction de la vie sociale. Le but de la législation pénale est alors de gérer les trahisons de confiance en garantissant que la sanction tombe bien en cas de fraude. C'est cette transparence qui permet de lutter contre l'arbitraire et qui permet également, dans nos sociétés modernes, d'anticiper les sanctions car le droit est un médiateur. Pour le juriste ou l'économiste, la confiance n'existe pas. Elle est le résultat de l'évaluation d'un risque qui se traduit par l'établissement d'un contrat. Dans un cadre économique, la confiance permet cependant de faire diminuer les coûts généraux entraînés par l'absence de confiance.

Le point de vue scientifique cherche à développer un outil qui permet de rendre opérable les points de vue précédents. Le premier modèle développé s'appuie sur une définition sociale des différentes formes de confiance présentes dans la société et cherche à mettre en place un schéma de gestion de confiance. Cette approche essaye de définir, via une politique de confiance, une confiance locale qui ne serait pas fondée sur une réputation ou une recommandation diffusable à toutes les entités présentes. Quant à la deuxième vue scientifique, elle s'inspire essentiellement des définitions juridique et sociale de la confiance. Elle met en place et elle teste un modèle de réputation qui permet de diffuser la confiance à des pairs.

Au fil des différentes discussions menées au sein de cette ACI, nous nous sommes rendu compte que même si chaque discipline avait une bonne vision de comment était définie la confiance dans son domaine, il était très dur de faire émerger une vision globale et commune. Dans ce but et après cette première partie de l'ACI, nous allons chercher à dégager une vision commune. Notre premier objectif est une journée de discussion et de Workshop interne à l'ACI qui aura lieu le 27 juin afin de tenter de dégager une vue plus cohérente.

Publications

French conference with lecture committee

– "Vers un modèle de confiance pour les objets communicants : une approche sociale", Véronique LeGrand, Stéphane Ubéda, Joël Morêt-Bailly, Agnes Rabagny, Laurent Guihéry, Jean-Philippe Neuville. Conférence SAR (Sécurité et Architecture Réseaux), 2004.

International conference with lecture committee

– "Modelization and trust establishment in ambient networks", poster, Samuel Galice, Véronique Legrand, Marine Minier, John Mullins, Stéphane Ubéda, International Symposium on Intelligent Environment, 2006.

– "A Distributed Trust Diffusion Protocol for Ad Hoc Networks", Michel Morvan, Sylvain Sené. In International Conference on Wireless and Mobile Communication 2006, to appear.

Research Report

– "Trusted Ambient community for self-securing hybrid networks", Véronique Legrand, Daniel Hooshmand, Stéphane Ubéda, INRIA Rhône-Alpes, ARES project, reseach report number 5027, 21 pages, 2003.

– " The KAA project : a trust policy point of view", Samuel Galice, Véronique Legrand, Marine Minier, John Mullins, Stéphane Ubéda, INRIA Rhône-Alpes, ARES project, reseach report to appear, 24 pages, 2006.