ACI sécurité informatique KAA (Key Authentification Ambient)

Samuel Galice, Veronique Legrand, Frédéric Le Mouël, Marine Minier, Stéphane Ubéda, Michel Morvan, Sylvain Sené, Laurent Guihéry, Agnès Rabagny, Joël Moret-Bailly, et al.

ACI sécurité informatique KAA (Key Authentication Ambient)

Rapport final 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

Avant-propos

Le texte qui suit constitue le rapport final de l'ACI KAA. Son objectif est d'abord de présenter les résultats obtenus par les différents participants de manière succincte dans un premier temps puis ensuite de manière plus technique et plus détaillée. L'objectif est également de montrer comment cette action a facilité le développement de collaborations qui n'auraient pu voir le jour sans la motivation induite par cette ACI et son financement.

1 Rappel des objectifs de KAA et principales avancées

1.1 Résultats obtenus

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.

Nous nous sommes donc dans un premier temps intéressés aux modèles sociaux, économiques et juridiques de la confiance afin de pouvoir définir un modèle sociologique qui serait réaliste pour l'utilisateur et économiquement acceptable tout en restant bien évidemment applicable dans un cadre légal.

Une fois cette première réflexion entamée, les acteurs scientifiques du projet ont pu ainsi définir essentiellement trois architectures de gestion de la confiance, la première reposant sur la notion d'historique, la deuxième sur des échanges de services et la troisième s'apparentant à une modèle de réputation qui semble pouvoir trouver une utilisation directe dans des réseaux de type pair à pair. Pour ces deux modèles, de nombreuses simulations informatiques ont été réalisées afin de les valider. Cependant, afin de compléter cette approche dans une démarche qui permettrait de coller au plus près de la réalité, une expérience d'économie expérimentale a été proposée et un premier protocole permettant de valider le dernier modèle de confiance proposé a été définie. Il reste cependant à mener à bien l'expérience proprement dite afin de voir comment des humains vont régler les paramètres du modèle. Cette expérimentation aura lieu normalement dans le courant de l'année prochaine.

1.2 Déroulement du projet

Le projet s'est articulé en moyenne autour de réunions de tous les partenaires qui avaient lieu une fois tous les 6 mois. En plus de ces réunions, plusieurs séminaires dédiés ont été organisés afin d'inviter des personnes extérieures à nos équipes travaillant sur le thème de la confiance.

- Séminaire pluridisciplinaire du 20 janvier 2006. Deux papiers ont été particulièrement analysés : d'abord le papier de Nabila Jawadi (Paris Dauphine) qui a travaillé sur la confiance dans les équipes virtuelles (titre du papier : "Nature et développement de la confiance dans les équipes virtuelles"). Le second papier présenté par Dimitri Dubois (Université de Montpellier 1) s'est intéressé à la " confiance dans les interactions économiques et sociales " et traite plus globalement de la confiance dans la théorie économique. Il apparaît que 3 pré-requis sont indispensables à la confiance : le RISQUE : lié

au temps ou à l'incomplétude informationnelle ; l'INTERDEPENDANCE : entre celui qui fait confiance et celui qui reçoit la confiance ; la VULNERABILITE : celui qui fait confiance se rend vulnérable vis à vis de celui à qui appartient la décision d'honorer ou non la confiance.
- Séminaire du 27 juin 2006. Présentation de toutes les avancées à mi-parcours des partenaires du projet. Définition d'une vision commune de la confiance.
- Séminaire Juin 2007. Synthèse des travaux réalisés par les membres des différentes équipes au cours des 3 ans de l'ACI.

2 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.

Précisons également que au cours de ce projet, nous ont rejoint en 2006 à nous Mathieu NEVEU du laboratoire GATE - Groupe d'analyse et de théorie économique - CNRS (Lyon) et Dimitri DUBOIS du LAMETA - Laboratoire Montpelliérain d'Economie Théorique et Appliquée (Montpellier).

3 Résultats détaillés

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.

3.1 Le point de vue des sociologues : confiance et groupes sociaux

La question de la confiance dans les échanges entre individus peut porter sur quatre aspects [1] :

1) les échangistes (X échange avec Y car X a confiance en Y et réciproquement),
2) les choses échangées (X a confiance dans la qualité de ce qu'il reçoit de Y et réciproquement, sinon il n'y a plus échange !),
3) les moyens de l'échange (X a confiance dans le procédés qui permet d'échanger avec Y et réciproquement),
4) les tiers-garants institutionnels (X échange avec Y car tout deux ont confiance dans les institutions censées garantir leurs échanges).

La sociologie ne se pose jamais la question des moyens. Elle élude volontiers la question de la qualité des choses échangées en *traitant* le problème de cette incertitude qualitative via les deux autres supports de confiance que sont la confiance institutionnelle (X et Y ne doutent pas de la qualité des choses qu'ils échangent car ils font confiance aux institutions qui régulent leurs échanges) et la confiance à autrui (X et Y ne doutent pas de la qualité des choses échangées parce qu'ils se font confiance mutuellement). Ces deux notions d'institution et d'inter-connaissance sont au cœur des analyses de l'échange en sciences sociales.

L'échange est un objet aussi central que traditionnel au sein des sciences sociales, notamment en économie où il est question d' *échange économique* pour analyser toute circulation de biens et services entre agents, ainsi qu'en sociologie et en anthropologie où le concept clé est celui d'*échange social*, concept qui recouvre l'ensemble des situations d'échange non-économique entre individus. Les sciences sociales ont pour tradition d'inscrire l'échange au sein de quatre institutions idéales-typiques :

1) la *famille*, ou encore le périmètre de la socialité primaire qui permet d'ajouter les amis, voire les voisins ;
2) l'*organisation*, qui comprend toute forme d'action collective coordonnée, depuis l'entreprise jusqu'à l'hôpital en passant par un club sportif ou un ministère ;
3) le *marché*, lieu réel ou virtuel de rencontre entre une offre et une demande de biens, services ou informations ;
4) le *réseau*, qui définit toute communauté d'individus unis par le partage d'une expérience (réseau d'anciens de...), d'un intérêt (réseau de développeurs de logiciels libres...), d'un attribut (réseau de détenteurs d'un QI supérieur à 150...), etc.

Ces quatre institutions se distinguent sur deux variables fortement discriminantes. En premier lieu, la *distance sociale* qui sépare deux individus qui échangent, cette distance sociale pouvant être forte dans le cas du marché et de l'organisation (d'où la nécessité du contrat - d'achat ou de salaire - pour produire l'échange entre inconnus) ou, au contraire, faible, comme souvent dans le cas de la famille et du réseau où l'inter-connaissance, la familiarité innée (les liens du sang de la famille) ou acquise (le partage dans le réseau), permettent l'échange sans contrat, entre des individus qui se sentent d'une façon ou d'une autre proches. En second lieu, le *degré de structuration* de l'institution, qui définit les degrés de liberté dont disposent les acteurs pour échanger (notamment choix du partenaire de l'échange et choix des choses

échangées) ; ce degré peut être faible, comme dans le réseau et le marché où les individus ont toute latitude pour se choisir et échanger ce qu'ils veulent, ou fort comme dans la famille et l'organisation, institutions où l'échange est davantage contraint par une hiérarchie et des règles. Au sein de chacune de ces quatre institutions, l'échange serait, en théorie, réglé par un mécanisme dominant :

1) l'échange dans la famille est principalement réglé par le *don*, sous-entendu qu'il n'y a pas de calcul, d'équivalence, de dette... ;
2) l'échange en organisation est principalement réglé par l' *autorité*, sous-entendue que c'est la hiérarchie, ses règles de subordination et les procédures qui régulent l'échange ;
3) l'échange dans le réseau est principalement réglé par la *confiance*, sous-entendu que c'est le fait de partager quelque chose qui permet à deux inconnus d'échanger ; et
4) l'échange sur le marché est principalement réglé par le *prix*, sous-entendu qu'il y aura transaction si et seulement si offreur et demandeur trouvent un prix d'équilibre.

Don, autorité, confiance et prix, associés respectivement à la famille, à l'organisation, au réseau et au marché, sont des mécanismes de régulation des échanges qui peuvent, du coup, être également discriminés selon les deux paramètres que sont la distance sociale et le degré de structuration, ce qui nous donne le tableau suivant :

		Distance sociale	
		Forte	**Faible**
Degré de structuration	**Fort**	Organisation/autorité	Famille/don
	Faible	Marché/prix	Réseau/confiance

On s'aperçoit dès lors que susciter des échanges de choses incertaines entre des inconnus (marché) n'est possible qu'en présence d'un prix. Dans un autre registre, on constate que l'échange en confiance est davantage approprié aux situations faiblement structurée et au sein desquelles les individus sont plutôt proches, non pas en raison de liens familiaux ou d'amitié, mais simplement du fait de partager quelque chose en commun (le réseau). En l'absence de prix des choses échangées, la condition pour faire échanger en confiance des individus soumis à peu - pas ? - de règles est celle de la pré-existence du partage d'une chose commune. Sinon, l'échange devra reposer sur davantage de règles de structuration des rapports sociaux et des relations inter-individuelles.

Références

[1] J.-P. Neuville, "Le contrat de confiance : étude des mécanismes de coopération dans le partenariat industriel autour de deux grands constructeurs automobiles européens." Ph.D. dissertation, IEP de Paris (sous la direction de E. Friedberg), 1996.

3.2 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. 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 [1].

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 [2].

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.

Plus précisément, les juristes s'intéressent essentiellement à la manière dont le contrat va permettre de peser sur les actions des contractants, sans pour autant avoir recours, dans cette analyse, à la notion de confiance, qui ne semble donc pas constituer un ressort pertinent pour l'action, du moins contractuelle. Dans ce registre, les intérêts pécuniaires attirent plus l'attention des analystes (y compris des économistes [3]) du droit, notamment en ce qui concerne la mise en oeuvre des mécanismes de responsabilité contractuelle, subséquents à l'inexécution desdits contrats.

Une telle approche permet, en outre, d'esquisser une modalisation des types d'organisation juridique, utile en ce qui concerne le type de régulation à choisir en ce qui concerne la problématique de l'informatique ambiante.

3.2.1 Six modèles d'organisation juridique

Toutes les règles ou ensembles de règles juridiques ne pèsent pas de la même manière sur le comportement des acteurs.

On peut schématiser un certain nombre de ces interventions de la manière suivante, après, toutefois, avoir précisé deux points : 1) les modèles utilisés appartiennent à la catégorie des " types idéaux " ; il s'ensuit que ceux-ci ne se trouvent jamais à l'état " pur " dans la réalité ; mais ils représentent des simplifications utiles pour saisir la réalité. 2) la régulation réelle d'un secteur social, emprunte systématiquement à ces différents modèles même si on peut penser qu'en général, l'un d'eux est dominant. Les modèles proposés sont au nombre de six :

1. Le modèle " administratif ". Il s'agit, dans ce modèle, d'effectuer un contrôle sur les actes ou les personnes à leur entrée dans le système. Par exemple, les autorisations administratives d'exercer une profession (médecins, avocats) ou une activité (installations classées), ou encore les simples déclarations, mais qui permettent de repérer les acteurs censés appliquer les règles, par exemple les responsables " privés " de traitements automatisés d'informations nominatives. Ce système a l'avantage d'une relative efficacité, mais présente l'inconvénient d'une certaine lourdeur : la régularité de l'action dépend de l'autorisation admirative, à moins que cette lourdeur ne soit tournée par le système de la seule déclaration.
2. La responsabilité. Les différents systèmes de responsabilité ont pour point commun le fait d'organiser la compensation (pécuniaire ou symbolique, sous la forme d'une peine) d'un dommage. L'une de leurs caractéristiques est l'intervention a posteriori. Si ces règles pèsent sur les actions, ce ne peut être que dans le cadre d'une " anticipation raisonnable " (Max Weber) des acteurs quant à l'application éventuelle des règles postérieurement à leur action.
3. La déontologie. Le modèle de la régulation déontologique réside dans le fait de faire peser sur l'acteur qui détient le pouvoir dans une relation (par exemple le médecin ou l'avocat) un certain nombre de règles dont le respect semble nécessaire au bon déroulement de la relation. Nous sommes, ici, dans une logique opposée à celle de la responsabilité : il ne s'agit pas de tirer, a posteriori, les conséquences d'une situation qui a généré un dommage, mais, a priori, de l'éviter.
4. Le contrat. Le modèle du contrat réside dans la liberté reconnue aux acteurs d'organiser leurs relations (avec la limite de l'ordre public, par exemple la loi informatique et liberté, à laquelle on ne peut déroger par contrat). Soulignons, cependant, que ce modèle nécessite, pour être efficace, une autorité de régulation destinée à garantir l'exécution du contrat ou, au moins, la sanction de son irrespect. L'avantage du système réside dans sa simplicité pour l'organisateur du système (les membres s'arrangent eux-mêmes) ; sa limite réside d'une part dans la possibilité de l'absence d'accord, d'autre part dans le caractère illusoire de l'accord si le pouvoir des parties est déséquilibré (les classiques " contrats d'adhésion ").
5. La régulation par le marché. Il s'agit, ici, d'organiser la liberté de la concurrence, l'exercice de cette dernière étant censée permettre d'atteindre le but de la législation, ici le " prix du marché ". Il s'agit, par exemple, de l'organisation des marchés des télécoms ou de l'énergie.
6. L'absence de régulation. Il s'agit, ici, de considérer que la régulation juridique n'a pas sa place dans les relations concernées, et de laisser la place à la " régulation sociale ".

Le modèle le plus pertinent pour KAA semble dans ce contexte, le modèle contractuel, dans la mesure où les situations factuelles saisies dans le cadre du projet renvoient, justement, en grande partie à des relations éphémères (notamment, personnes qui se croise et dont les

objets communicants peuvent échanger des données, par exemple dans un train ou dans un campus). Encore semble-t-il nécessaire de préciser que le contrat n'est pas un écrit et qu'il ne nécessite pas de signature, puisque le contrat se définit, en droit français, comme un simple " accord de volonté ". Encore ce contrat doit-il être " non équivoque " quant à son objet, c'est-à-dire que la personne doit savoir à quoi elle s'engage en contractant ; de même l'accord ne peut-il résulter de l'inaction, en aucun cas le silence ne pouvant valoir acceptation (sauf évidemment, contrat prévoyant lui-même, par exemple une " tacite reconduction ").

Enfin, le contrat dont nous parlons ici désigne un " contenant ", qui peut contenir des règles ou des ensembles de règles qui obéissent aux différentes logiques évoquées dans le cadre des six modèles analytiques proposés. Nous avons, cependant et jusqu'à présent, indifféremment utilisé des exemples qui renvoient à des modalités temporelles d'intervention du droit relativement différentes les unes des autres.

3.2.2 Modalités temporelles d'action du droit

Ces modalités temporelles d'intervention peuvent être présentées selon qu'elles interviennent avant ou après l'action analysée.

A priori. La modalité d'intervention du droit la plus souhaitable vis-à-vis du bon fonctionnement d'un groupe est l'intervention a priori. Dans ce contexte, le groupe social considéré se dote de ses règles de fonctionnement, orientant les comportements à venir dans le sens qu'il souhaite. Par exemple, le législateur prévoit une exonération fiscale pour tel type d'investissement, guidant les investissements possibles vers l'activité choisie. De la même manière, le législateur prévoit que telle activité, si elle est avérée, fera l'objet de sanctions, espérant que les acteurs sociaux s'abstiendront d'adopter le comportement considéré. Ce dernier exemple, est cependant relativement ambigu, puisque les règles de responsabilité peuvent être considérées comme intervenant a priori comme guide de l'action d'un acteur social qui voudrait échapper à l'engagement de sa responsabilité, et comme intervenant a posteriori, pour régler les conséquences de comportements avérés.

A posteriori. Dans ce contexte, tout ne se déroule pas forcément conformément à ce qu'un groupe social espérait. Notamment, les règles censées guider les comportements a priori peuvent ne pas être " respectées " ou, plus exactement, les acteurs sociaux peuvent prendre le risque de les voir s'appliquer d'une manière défavorable à leurs intérêts.

C'est à ce modèle qu'obéissent les règles de responsabilité. Dans ce contexte, un acteur social devra répondre des conséquences de son action. Deux grands types de responsabilité peuvent, dès lors, être opposés : les responsabilités à visée compensatrice et indemnitaire, d'une part ; les responsabilités à visée sanctionnatrice, d'autre part.

Cette conscience de l'existence des règles de responsabilité amène, en outre, deux questionnements complémentaires. Le premier a trait à la gestion des groupes organisés (ou simplement formés ?) autour de technologies à l'origine de cette recherche. Plus précisément, ces groupes peuvent-ils échapper aux règles de responsabilité de droit commun ?, ou autrement formulé, peut-on concevoir, aux yeux du droit français contemporain, un modèle technologie de confiance juridiquement clos comme échappant aux normes de droit commun ? Le second renvoie aux modalités de régulation des groupes auxquels la présente recherche cherche à appliquer un " modèle technologie de confiance " ; plus précisément, on peut se demander si l'application de règles dans un groupe ne nécessite pas obligatoirement la présence d'un " tiers

", arbitre, juge, destiné à appliquer un certain nombre de règles " de responsabilité " en cas de violation des règles " de confiance " du groupe.

3.3 Un modèle technologique de confiance peut-il se passer d'une "autorité décisionnelle" interne ?

La question à laquelle nous venons de répondre concerne essentiellement les rapports entre la régulation du groupe dans lequel des relations de confiance peuvent se développer et son l'environnement juridique. Qu'en est-il, cependant, de la régulation du groupe lui-même ? A cet égard, le juriste ne peut que se demander si l'organisation de telle relation peut se passer d'une " autorité décisionnelle " interne, sur le modèle d'un arbitre ou d'un juge ? Ce questionnement ne relève pas de l'absolu au sens où il ne s'agit pas de prétendre qu'un fonctionnement autre serait impossible (certaines sociétés se sont, historiquement, passées de " juges "), mais de l'apport possible de la science de droit à la recherche. Si, en effet, le modèle choisi est exclusif de la figure de l'arbitre ou du juge, l'analyse juridique sera limitée à ce que nous avons précédemment évoqué.

La question mérite, cependant, d'être soigneusement analysée. On peut, dans ce contexte, affirmer, d'une part, en considération des développements précédents, qu'un juge étatique pourra toujours intervenir en ce qui concerne les activités qui font l'objet de la présente analyse dans e cadre des responsabilités civile et pénale. On peut poser, d'autre part, la question de l'efficacité d'un système de règles qui ne prévoirait pas de sanction.

Dans ce contexte, il ne s'agit pas de nier l'existence d'une contrainte, même en l'absence d'une régulation juridique ; c'est d'ailleurs ainsi que E. Durkheim définissait la possibilité même d'une science sociologique (l'étude des " faits sociaux ", que le père de la sociologie française reconnaissait à leur pouvoir de " contrainte externe " [4]). Mais il s'agit, plutôt, de déterminer ce qui fait l'originalité de la régulation juridique. Or, il semble fort que l'intérêt de cette dernière réside dans l'explicitation des règles, ou, a minima, dans la désignation d'un " tiers " indépendant des intérêts contradictoires entre lesquels il a pour fonction de trancher. Si les règles ne sont pas explicitées et s'il n'est pas prévu de processus pour " trancher les différents ", la régulation dont il s'agit échappe sans doute au qualificatif de " juridique "[8]. C'est un choix qu'il est tout à fait possible d'effectuer, mais ses conséquences échappent dès lors (sauf en ce qui concerne l'application des règles de responsabilité de droit commun) à la compétence du juriste pour renvoyer à celle du sociologue.

Qu'il soit, cependant, permis de douter d'une telle possibilité. Nous appuyons ce doute sur un exemple. : les jeux de rôles massifs en ligne (MMROPG). Les enjeux liés à ces activités ludiques sont moindres que ceux qui sont impliqués par le modèle de confiance analysé, puisque de la violation des règles ne conduit, en l'occurrence, qu'à une distorsion dans l'équilibre du jeu (outre les conséquences en termes de réputation, de " confiance ? " dans l'opérateur). Ces conséquences conduisent cependant les organisateurs de ces activités à prévoir un système de sanction des comportement déviants : comportement désagréable pour les autres joueurs, comportements qui, sans être irrégulier, consiste à profiter des failles du système de jeu (attitude qui n'est pas sans rappeler la " fraude à la loi ", dans laquelle une personne obtient un avantage indu, en jouant de la technique juridique d'une manière parfaitement régulière). Or, cette activité " répressive " nécessite une appréciation des comportements des utilisateurs qualifiés ou non de frauduleux. Cette activité peut être aisément comparée à celle d'un juge.

[8] P. Fauconnet montre, dans [5], dans une approche sociologique et ethnologique, que la responsabilité nécessité d'une part des règles de responsabilité (même non explicitées), d'autre part un jugement de responsabilité

On peut estimer, dans ce contexte, et dans le cadre d'une activité technologiquement organisée et contrainte, que si l'organisation a priori du système était suffisante, la question que nous envisageons ne se poserait pas. Or, même dans ce cadre extrêmement organisé et contraint, la mise en oeuvre d'un système de responsabilité " répressive " est apparue nécessaire.

3.3.1 Conclusion

En conclusion, cinq points doivent être considérés comme acquis :

- Le droit ne peut, par lui-même, imposer la confiance, mais il peut créer des conditions de prévisibilité des comportements des acteurs et institutions, qui favorisent la confiance, dans la stricte mesure ou les actions peuvent alors être largement anticipées.
- Les règles juridiques ne sont pas que construites sur un modèle impératif, mais peuvent mettre en place des " incitations ", pour peser sur le comportement des acteurs, notamment dans le cadre de la responsabilité : un acteur violera-t-il les règles d'un groupe qu'il a choisi d'intégrer, s'il peut être exclu de ce dernier ?
- La régulation juridique obéit à différents modèles qui permettent une large gamme d'interventions, notamment temporelles.
- Il est vain, en outre, de croire que la nouveauté technique ainsi que le contexte " spontané " des communications de l'informatique ambiante feraient échapper les acteurs aux règles juridiques d'ores et déjà existantes, et notamment les règles relatives aux responsabilités civiles et pénales.
- Enfin, on peut imaginer, lorsque des groupes sont suffisamment importants, l'apparition d'un " juge " chargé de sanctionner, en interne, les comportements déviants... À moins que l'on ne laisse cette tâche au groupe lui-même dans le cadre d'une régulation " seulement " sociale.

Références

[1] 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.

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

[3] T. Kirat, "Economie du droit", La découverte, 1999.

[4] E. Durkheim, "Les règles de la méthode sociologique", 1895, PUF, Quadrige.

[5] P. Fauconnet, "La responsabilité", F. Alcan, 1920.

3.4 Le point de vue des sciences économiques : synthèse sur les apports des sciences économiques pour penser des modèles de confiance sur objets autonomes communicants

Le projet KAA a permis de fédérer une communauté très variée d'économistes - thématiques et origines géographiques - autour des questions de confiance face aux objets autonomes communicants et leurs protocoles d'échanges d'information. Au delà des participations ponctuelles d'économistes et de gestionnaires, notre groupe de recherche "Économie" se compose des chercheurs suivants :

- Laboratoire LET (Julien Eustache, Laurent Guihéry), Université Lumière Lyon 2, Lyon
- Laboratoire GATE (Mathieu Neveu), Université Lumière Lyon 2, Ecully
- Laboratoire LAMETA (Dimitri Dubois), Université de Montpellier 1, Montpellier

Ce groupe s'est bien intégré avec les autres disciplines représentées dans KAA et a permis un réel échange de point de vue et une confrontation des analyses mais aussi des méthodes, en particulier avec les informaticiens (Marine Minier, Samuel Galice). Notre participation active aux nombreux séminaires et nos productions scientifiques - l'organisation d'un séminaire de recherche, rapports, communications, articles - ont permis aussi d'entrevoir des développements prometteurs autour de l'Economie Expérimentale, qui font actuellement l'objet d'une nouvelle recherche avec l'aide de l'Institut Rhônalpin des Systèmes Complexes : cette recherche liée directement à KAA regroupe des économistes et des informaticiens et s'annonce prometteuse.

3.4.1 Problématique de recherche

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 a 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. C'est d'ailleurs autour de cette méthodologie d'économie expérimentale que nous avons le plus avancé durant ces premiers mois de travail sur le projet KAA [1]. La réputation vise ainsi à canaliser spontanément l'opportunisme et contribuer à le réduire. Dans cette perspective, les relations de confiance entre les contractants sont réduites à une estimation des coûts / avantages concernant les actions à conduire pour maintenir une bonne réputation. On peut même aller plus loin, comme chez Lepage (1989), en prétendant que le marché est auto-producteur de confiance. Cette thèse du marché comme "inducteur de confiance" suppose que ce cadre d'échange produit lui-même ses propres règles de loyauté profitables à toutes les parties (Baudry, 1992).

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.

Le point central des développements les plus récents sur ces questions s'intéresse à la question des asymétries informationnelles entre les agents. En situation d'information parfaite, la confiance s'établit de facto entre les agents car il y a une parfaite connaissance informationnelle d'autrui et de son environnement. Par contre, en situation d'information imparfaite, le problème de la confiance est central car les agents ont tendance à masquer leurs préférences

et à dissimuler les risques inhérents à une transaction (l'exemple le plus évident concerne le marché des voitures d'occasion traité par G. Akerlof). En général, ces travaux partent de l'impossibilité d'application pratique du modèle d'équilibre général et de l'écart de ce modèle avec la pratique et les expériences économiques : en effet, si l'on considère que les acteurs ne sont plus omniscients et que leur rationalité est imparfaite, l'information étant considérée comme asymétrique, alors l'efficacité de la régulation par le marché pur devient délicate, sous-optimale et voire "incomplète". C'est souvent en partant de l'analyse du don que les travaux débouchent sur les questions de confiance, voir G. Akerlof (1982, 1984) La question de confiance a été particulièrement étudiée par les néo-institutionnalistes qui considèrent que la confiance constitue un élément central de réduction des coûts de transaction entre les agents (cf. O. Williamson) : pour lui, la confiance ne s'oppose pas au calcul rationnel de l'intérêt, elle en découle. Du côté de l'École des Conventions, la confiance est perçue comme réductrice d'incertitude et s'exprime dans des règles, des conventions et permettent de fixer un ordre social stable. Pour certains économistes, la confiance ne peut se comprendre uniquement par le seul jeu des intérêts et par la relation marchande. Ces auteurs soulignent que la confiance et les conventions sont en fin de compte des solutions efficaces de nombreux problèmes économiques, notamment face à l'incomplétude des marchés. Chez Coase (1937), initiateur du courant de la Nouvelle Economie Institutionnelle, la confiance se place au delà du débat marché / intégration, car elle pose la question du mode de coordination des transactions le plus efficace. Certaines transactions sont en effet retirées du marché et retirées de la régulation par les prix pour être organisées dans la firme et soumises au principe coordinateur de l'autorité afin d'économiser sur les coûts de transaction. Ainsi, la confiance est désignée comme le mode de coordination des transactions qui se déroulent au sein de réseaux.

Dans bien des travaux, en économie expérimentale par exemple, l'opportunisme est au centre du débat : ainsi certains auteurs, comme Neuville (1997, [3]), ont analysé la confiance de manière stratégique, à partir d'observations des relations de sous-traitance dans l'industrie automobile et du cas d'un fournisseur ayant une excellente réputation. Neuville montre que la confiance peut coexister avec des comportements fondamentalement opportunistes. "La confiance, dans l'optique du fournisseur, peut devenir une véritable stratégie en vue de masquer des défaillances et des réductions clandestines des coûts de production". Ces perspectives permettent de concevoir la confiance comme un acte de construction sociale dans lequel s'inscrivent les relations de marché. Granovetter (1985, 1994) a montré la capacité des réseaux sociaux à assumer un rôle économique en favorisant la diffusion de la réputation et, le cas échéant, la sanction des comportements jugés déloyaux. Certains auteurs sont, de ce fait, conduits à expliquer un nombre probablement exagéré de situations de coopération par la relation de confiance. Chez Torre, la confiance est le ciment des relations spatialisées, Torre (1995) : elle se fonde sur la forte inter-connaissance que favorise la proximité.

Comme nous pouvons le voir, les apports de la théorie économique sont nombreux pour penser la confiance dans les réseaux communicants, à partir d'objets autonomes par exemple (PDA, smartphone,...). Mais c'est du côté de l'économie expérimentale que les principaux apports sont les plus intéressants, en particulier dans le cadre d'une coopération étroite et fructueuse avec les informaticiens.

3.4.2 Développement de la recherche

L'analyse de la confiance dans le projet KAA a emprunté aussi des voies plus institutionnelles autour de trois axes :

- Une analyse autour du civisme qui part de l'idée que la confiance nécessite un certain civisme de la part des citoyens - électeurs et s'exprime par une certaine "communion" avec les institutions, comme c'est le cas globalement dans les pays scandinaves et en Suède plus particulièrement.Ce questionnement sur la relation entre confiance et civisme a permis de participer à la restitution des travaux de la Commission Pierre Cahuc / Yann Algan autour de leur rapport : "La société de défiance. Comment le modèle français s'autodétruit." (Commission Attali).
- Une réflexion sur les différences de modèles sociétaux entre l'Europe et l'Amérique du Nord, ce dernier plaçant la confiance au centre des relations politiques, économiques et sociales. L'exemple le plus parlant est précisément la rupture de la confiance qui est très sévèrement sanctionnée dans le modèle nord-américain -Justice, délit d'initié par exemple). On retrouve dans cette analyse cette intuition fondamentale du prix Nobel d'Economie K.J. Arrow qui mentionnait que la confiance est "le lubrifiant du système économique et social". Ce travail a fait l'objet d'une communication finale de Laurent Guihéry sur le thème "Confiance et action publique : quels fondements ? Quelles relations ? Enseignements pour KAA" lors du Workshop CITI-INSA (27 mars 2006). Dans ce texte, une typologie des différents mécanismes de confiance a été proposée.
- Enfin une demande réelle des chercheurs en science dure vise à investir le champ de recherche de la monnaie virtuelle. Nous avons dans le projet KAA tenter de préciser rapidement les tenants et aboutissants de cette notion de monnaie virtuelle à la lumière des sciences économiques. Des coopérations avec des spécialistes d'économie monétaire est à l'étude (J. Blanc par exemple à Lyon 2). Des premiers éléments de recherche ont été entrepris, avec Fabio Linhares et Laurent Guihéry, autour du papier de Markus Jakobsson, Jean-Pierre Hubaux, Levente Buttyan [2]. Le papier propose un arrangement de micro-paiement pour les réseaux cellulaires de multi hop qui encourage la collaboration dans l'expédition de paquets en laissant l'avantage aux utilisateurs de transmettre par relais d'autres paquets. Proposant aussi des mécanismes pour détecter et récompenser la collaboration, ce papier présente des mécanismes appropriés pour détecter et punir de diverses formes d'abus. Il apparaît que l'arrangement résultant rend la collaboration raisonnable et la fraude indésirable. Des travaux complémentaires autour de ces premiers résultats sont en cours.

3.4.3 Les mécanismes de confiance dans les communautés virtuelles liées aux jeux en réseau

La dernière partie de nos travaux s'est orientée vers les mécanismes de confiance dans les communautés virtuelles liées aux jeux en réseau (papier de Julien Eustache : Mechanisms for trust in virtual communities and massively multiplayer online games, LET, 2007, 12 p.). Son observation du monde des jeux en réseaux et l'analyse concrète des communautés virtuelles lui ont permis de déterminer plusieurs critères qui déterminent la confiance chez les utilisateurs :

- **L'expérience d'utilisation.** On constate que les comportements des membres des différentes communautés citées précédemment évoluent sensiblement en fonction de leur expérience en tant qu'utilisateur. Les internautes qui participent ou appartiennent à des communautés virtuelles depuis un certain temps accepte plus facilement leur fonctionnement et les risques éventuels qui pourraient représenter un frein à l'évolution du système. Par exemple, un acheteur sur eBay sera tenté d'acheter dans un premier temps des articles qui représentent une perte potentielle peu élevée. Au fur et à mesure de

l'expérience acquise sur les sites marchands, sous réserve du bon déroulement des transactions, l'utilisateur va voir sa confiance augmenter systématiquement. De ce fait, les utilisateurs expérimentés effectuent beaucoup plus de transaction grâce à leur croyance plus élevée au bon déroulement des opérations sur Internet.

- **La prise de risque.** En plus de l'expérience acquise lors de l'utilisation et la familiarisation avec les communautés et autres sites présentés, la prise de risque est un critère qui au fil du temps améliore progressivement la confiance des utilisateurs. Celui-ci s'applique particulièrement aux réseaux Peer-To-Peer, où la peur des sanctions freine considérablement les échanges. On constate que les utilisateurs vont progressivement prendre des risques vis-à-vis de la quantité de téléchargements effectués en augmentant le nombre de fichier au fur et a mesure de l'augmentation de la confiance.
- **L'évaluation.** La qualité d'un service ou la fiabilité d'un vendeur sur Internet sont très souvent soumises à des évaluations. Ce principe fonctionne avec la plupart des sites de e-commerce, où les utilisateurs peuvent donner une notation et des appréciations sur la société ou sur l'autre utilisateur avec qui la transaction a été effectuée. On retrouve ces notations sur des sites comme eBay ou Priceminister avec des évaluations constituant le profil des utilisateurs. On remarque que les notations des utilisateurs ont une grande valeur dans l'établissement de la confiance. Il est plus facile de faire confiance à un pair qui est dans a même situation que l'utilisateur qu'a une société qui affirmerait une excellente qualité de service.
- **Les règles et sanctions.** Lorsque l'on évoque les sanctions possible auxquelles un utilisateur peut être confronté, on peut facilement imaginer que cela peut représenter un frein à l'évolution des communautés sur Internet. Pourtant, les règlements et sanctions mises en place par de nombreux sites et responsable de communautés sont un facteur de confiance non négligeable. La connaissance de sanction possible ajoute un gain de confiance important aux utilisateurs souhaitant évoluer et respecter selon les règles imposées. Sur Wikipedia par exemple, les abus et publications d'informations erronées plus ou moins volontairement sont systématiquement censurées avant de bannir les utilisateurs ne respectant pas les règles. De même World of Warcraft dispose d'un service efficace qui veille au bon déroulement du jeu et sanctionne également les joueurs qui souhaiteraient profiter des failles éventuelles du système en trichant ou en agissant de façon contraire aux règlements. On constate donc que les utilisateurs ont une confiance accrue lorsque des sanctions sont mises en place pour protéger.
- **La loi des grands nombres.** Au sein des différentes communautés, il existe toujours des litiges plus ou moins importants. On peut effectuer un rapport entre le nombre d'utilisateurs et le nombre de conflits. Lorsque l'on fait partie d'une communauté constituée de plusieurs millions d'utilisateurs, on acquiert plus facilement de la confiance qu'avec un nombre peu important de membres. La quantité d'utilisateur fait que la confiance s'installe facilement du fait de l'importance des transactions effectuées sans problème.
- **La communication.** Parmi les différents critères de confiance, la communication fait partie de ceux qui sont susceptibles d'avoir une influence très forte sur les comportements des utilisateurs. En effet, la clarté des informations disponibles sur les modalités des transactions ou encore l'annonce explicite de garanties en cas de litige ont une influence extrêmement importante sur les décisions des utilisateurs. De même, la publicité ou mauvaise publicité que l'on peut trouver à propos d'un site joue un rôle très important sur le secteur. Pour reprendre l'exemple du site perenoel.fr, on remarque qu'une mauvaise publicité va diminuer fortement la confiance des acheteurs non seulement sur le site

concerné, mais également sur tout le secteur du e-commerce. Il est donc important de détailler explicitement aux internautes, les différentes modalités des transactions.

3.4.4 Perspectives

Ce projet KAA a permis une première coopération scientifique réussie entre économistes et informaticiens. Le programme de recherches retenu pour un approfondissement de cette coopération concerne l'Économie Expérimentale en testant des protocoles de confiances entre des individus sélectionnés regroupant les équipes du GATE (Mathieu Neveu) du LAMETA (Dimitri Dubois) de l'INSA (CITI, Marine Minier, Samuel Galiste) et du LET (Laurent Guihéry, Julien Eustache). Le GATE mettra d'ailleurs à disposition sa salle d'Economie Expérimentale. La poursuite du projet de recherche devrait bénéficier d'un financement de l'Institut Rhônalpin des Systèmes Complexes.

Références

[1] 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.

[2] 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.

[3] J.-P. Neuville, "Le contrat de confiance : étude des mécanismes de coopération dans le partenariat industriel autour de deux grands constructeurs automobiles européens." Ph.D. dissertation, IEP de Paris (sous la direction de E. Friedberg), 1996.

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

During these three years, we have focused on the possible and useful methods to implant the notion of trust in networks, in their most global definition. The objective of this work is to create a global mechanism called KAA framework to handle trust in ambient networks. We assume that each device is equipped with a set of cryptographic tools in order to prove their successful past interactions with other devices. These interactions are stored in a database called History. Each entry of this History can be verified by a third party if this latter has yet interacted with both devices : this mechanism is built on Identity-Based Cryptosystems. The decision-making process relies on the following statement : when two stranger devices meet for the first time, they exchange their respective Histories. If it appears that they have a sufficient number of common trusted devices, they trust each other. In this report, we are just going to give a brief summary of the definition of trust and of our protocol that was implemented on PDAs and very carefully studied with intensive simulations. More details about the protocol can be found in [GMU07c].

3.5.1 A brief definition of trust

According to [1], trust management systems are classified into three categories : credential and policy-based trust management, reputation-based trust management, and social network-based trust management. This approach depends on the way trust relationships between devices are established and evaluated. In credential and policy-based trust management system [2, 3, 4], a device uses credential verification to establish a trust relationship with other devices. The concept of trust management is thus limited to verifying credentials and restricting access to resources according to application-defined policies : they aim to enable access control [5]. A resource-owner provides a requesting device access to a restricted resource only if it can verify the credentials of the requesting device either directly or through a web of trust [6]. This is useful by itself only for those applications that assume implicit trus t in the resource owner. Since these policy-based access control trust mechanisms do not incorporate the need of the requesting peer to establish trust in the resource-owner, they by themselves do not provide a complete generic trust management solution for all decentralized applications. Reputation-based trust management systems on the other hand provide a mechanism by which a device requesting a resource may evaluate its trust in the reliability of the resource and the device providing the resource. Trust value assigned to a trust relationship is a function of the combination of the devices global reputation and the evaluating devices perception of that device. The third kind of trust management systems, in addition, utilize social relationships between devices when computing trust and reputation values. In particular, they analyze the social network which represents the relationships existing within a community and they form conclusions about devices reputations based o n different aspects of the social network. Examples of such trust management systems include Regret [7, 8] that identifies groups using the social network, and NodeRanking [9] that identifies experts using the social network.

3.5.2 The trust model and the CHE protocol

The Knowledge Authentication Ambient project (KAA) mimics human society in order to propose trust management mechanisms for ambient networks. Our trust policy depends of the underlying social patterns [10], [LGUN05], [GLM+06b]. We also avoid trust dissemination :

each entity is viewed as an autonomous device and trust assessment is based only upon direct link between trustworthy devices. These devices may have no a priori relationship for establishing trust among them. This leads naturally to a decentralized approach that can tolerate partial information through there is an inherent piece of risk for all trusting entity. We also objects the idea of a recommendation mechanism, the trust is considered as a non transitive relation. Consequently, a device could not receive a recommendation for a device that it has never met before since there is no simple and local means to prove the semantics of such a recommendation.

The key concept of our framework relies on the notion of History of past interactions : all successful interactions are represented by cryptographically provable elements and stored in the History of participant devices. Then, two unknown devices could exchange some services if they share a sufficient number of common trustworthy devices : the trust level is thus evaluated by the number of common trusted devices. Our framework includes several security protocols ensuring the robustness of the model [GLM+06a], [GMMU06], [GMU07c]. Verifying the identity of each device is realized by a particular trusted station : the imprinting station. The burden of the decision-making process, which is somehow complex and inductive in general, is also significantly reduced by the use of proved data since the decision is based on provable past behaviors.

In the KAA framework, the *Common History Extraction* protocol forms the core of the system and it is based on cryptographic methods. More precisely, it is based on the notion of cryptographic ID first introduced by A. Shamir [13], adapted to elliptic curves by D. Boneh and M. Franklin [11] for the cipher and used by Chen, Zhang and Kim [12] for a signature without a trusted PKG (Private Key Generator).

A device in the KAA framework is equipped at least with a *cryptographic package* what will make it compatible de facto with any other entity of our model, i.e. other objects which implicitly accept the model. When an object received this package and the initial parameters, it can then initiate sessions of communication by the means of the CHE protocol (detailed in [GMMU06]). If a session is accepted, the two involved devices estimate, considering their security policies, that they can trust each other during this interaction.

Starting from an empty History, a device records all the successful interactions made with other devices in order to support the future spontaneous interactions. To prove the past interactions, it creates with each met device an element of History related to their respective identities and signed by the two parts. Before any interactions, devices must build a *trust germ*, by counting the number of common devices they have in their History, or by manually forcing the relation : this is the *bootstrap* phase of our model. If the number of common interactions is sufficient (greater than a threshold p which is a function of the size n of the community and the maximum size H_{max} of the History), they can then interact.

Each device receives an initial *trust germ* from its *imprinting station* including the same following cryptographic algorithms and protocols downloaded from the imprinting station : a fingerprint algorithm, a signature algorithm, a zero-knowledge protocol, a protocol to construct secure channel and the public parameters.

The first step of our protocol supposes that both entities Alice and Bob have already interacted at least once and have built a trust bond : this is a message m signed by Bob that Alice publishes in the public part of her History $(m, sign_B(m))$ while Bob publishes $(m, sign_A(m))$ in its own History. This bond could be created by forcing by the hand the beginning interaction as in a Bluetooth like system if the number of common elements of their history were insufficient. This forms the *bootstrap* phase. Let us note that if Alice and

Bob have already met and if this new interaction is successful, they just have to modify the respective values of the intensity and to rebuild a new history element to replace the old one because it contains a timestamp. Suppose now that in the same way Bob and Charlie have built a secure channel to exchange a common message of mutual trust m'.

When Alice meets Charlie and one to each other want to prove that they have respectively met before Bob, they exchange a public part of their histories and Charlie, first, proves to Alice that Bob trust him using m'.

We have performed intensive simulations of the pertinence of our protocol concerning the size of the history, the time of the bootstrap phase, the better eviction policies of elements (for more details, see [GMMU06]). We have also implemented this protocol on PDAs using the cryptographic library MIRACL.

Références

[1] G. Suryanarayana and R. N. Taylor, "A survey of trust management and resource discovery technologies in peer-to-peer applications." [Online]. Available : citeseer.ist.psu.edu/suryanarayana04survey.html

[2] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The KeyNote Trust-Management System Version 2 - RFC 2704," RFC 2704, Available from http://www.faqs.org/rfcs/rfc2704.html, September 1999.

[3] M. Blaze, J. Feigenbaum, and A. D. Keromytis, "The role of trust management in distributed systems security." in *Secure Internet Programming*, ser. Lecture Notes in Computer Science, J. Vitek and C. D. Jensen, Eds., vol. 1603. Springer, 1999, pp. 185–210.

[4] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management." in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 1996, pp. 164–173.

[5] T. Grandison and M. Sloman, "A survey of trust in internet applications." *IEEE Communications Surveys and Tutorials*, vol. 3, no. 4, 2000.

[6] R. Khare and A. Rifkin, "Weaving a Web of trust," issue of the World Wide Web Journal (Volume 2, Number 3, Pages 77-112), Summer 1997.

[7] J. Sabater and C. Sierra, "Regret : reputation in gregarious societies." in *Agents*, 2001, pp. 194–195.

[8] J. Sabater, "Reputation and social network analysis in multi-agent systems." in *AAMAS*. ACM, 2002, pp. 475–482.

[9] J. M. Pujol, R. Sangüesa, and J. Delgado, "Extracting reputation in multi agent systems by means of social network topology." in *AAMAS*. ACM, 2002, pp. 467–474.

[10] V. Legrand, D. Hooshmand, and S. Ubéda, "Trusted ambient community for self-securing hybrid networks," INRIA, Research Report 5027, 2003.

[11] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing." in *CRYPTO*, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.

[12] 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*, ser. Lecture Notes in Computer Science, vol. 2908. Springer-Verlag, 2003, pp. 585–592.

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

3.6 Une deuxième approche technologique : Service-to-service protocols integrating service trust semantics

During the last year of the project, we have also prospected on the possible use of trust in the emerging domain of Service-Oriented Platforms (SOP). Indeed, Service-Oriented Platforms, such as the WebServices, OSGi or UPnP, are particularly adapted and more and more used for highly dynamic environments, such as ad hoc environments. We have focused on integrating trust in service-to-service protocols, especially the discovery protocol and the service negotiation protocol. Details about this integration can be found in [BL07].

3.6.1 Protocols

In ad hoc environments, different services are provided. Behavior of these services are semantically described by a service description composed of different properties. Examples of properties are the service name, the service type, the service version, the different quality of service offered. When two services communicate, they share properties to negotiate a provided service.

To integrate the trust in service-to-service protocols, we have proposed to modify a service by enriching its description and adding several policies.

First, we have enriched each property of the service description with an initial trust value. During the discovery and negotiation phases between two services, only properties that have a greater trust value than the current matching service trust value are showed. This mechanism allows a service, for instance, to show the best quality of service properties only to the services with which it has build a great level of trust. Non trusted services will only see basic quality of service properties.

These different actions are performed by several policies added to a service. For the discovery phase, we have proposed a 'Description Filter Policy' that allows only the output of properties having the right level of trust according the level of trust of the service requester. For the negotiation phase, we have defined the 'Minimum Trust Acceptation Policy' and the 'Maximum Trust Acceptation Policy' which define acceptable levels of trust that must respect a property. If the level of trust is not reached initially, it can be negotiate by the 'Temporary Trust Increase Policy' that allows to take a risk. This negotiation is limited in terms of attempts by the 'Maximum Trust Increase Policy' to prevent the deny of service and limit expedient of the protocol.

We have implemented these service-to-service discovery and negotiation protocols in an OSGi platform and have tested different scenarios (negotiation successful, different cases of aborting, etc.).

3.6.2 Perspectives

This study of integrating trust in Service-Oriented Platforms (SOP) is an early work that shows the feasibility. Several improvements can be achieved. The initial trust value for each service property is for the moment adhocly defined. Metrics and tools have to be developed to automatize and standardize these values. Cryptographic mechanisms have also to be used to ensure that these values can not be manually modified by a ill-intentioned user. Finally, we have only worked on the first phases of the communication between two services : the discovery and the negotiation. We have to integrate to the communication ending phase, the trust propagation model developed in the KAA project.

3.7 Une approche mathématique de la confiance

3.7.1 definition of the goals

The objective of our work was to study the diffusion of trust in a population, and to find the asymptotic states. The very simple mathematical model we used was characterized by the following :

- the population is represented by a probability density function f depending on a x variable and on time t. The variable x measures the length of the list of "individuals in which we can trust".
- The evolution of the function f is mainly due to : a diffusion process which accounts for the possible interactions between all individuals, the diffusion constant is d, and a competitive process localized in x which accounts for the following "a priori" : individuals preferentially have interactions with similar individuals. The competitive process between different individuals is modelized by the term : $af(t,x)(K - Cf(t,x))$ where a is a constant growing coefficient and K is a constant limitation coefficient.

The equation we dealt with was :

$$\frac{\partial}{\partial t} f(t,x) - d\Delta f(t,x) = af(t,x)(K - Cf(t,x)). \tag{1}$$

A complete description of the model can be found in [1].

3.7.2 The main obtained results

Starting from an homogeneous population with numerical simulations we have checked that the population is clustered in two subgroups, on the left a group of individuals where trust indices are very low, and on the right a group of individuals where trust indices are very hight. An other approach was tested with a mathematical model consisting of ordinary differential equations connected through the adjacency matrix of a graph. With a least square criteria, the best graph were searched. Unfortunately, a such approach did not give relevant results see for example [2].

Références

[1] **Picq M. Pousin J.,** Adaptation d'une équation différentielle modélisant le principe de divergence de Darwin dans le cadre du modele de confiance. Stage INSA de Lyon 2006.

[2] **Pousin J.,** Images Transportation for Identifying the dynamic of some Compartmental Models in Biology. submitted to ISBI 2008.

[3] **M. Picq J. Pousin and Y. Rouchdy,** A Linear 3D Elastic Segmentation Model for Vector Fields. Application to the Heart Segmentation in MRI, Jour. of Mathematical Imaging and Vision, n. 4, p. 227-241 2007.

3.8 une troisième approche technologique : A distributed protocol for trust diffusion

During these three years, we have focused on the possible and useful methods to implant the notion of trust in networks, in their most global definition. The objective of this work was to create a trust diffusion protocol for ad hoc networks efficient to find dishonest nodes and capable to be used in other more general networks. And such a protocol could not be modeled and developed without a good understanding of what was the real sense of trust. Indeed, the trust notion is not a mathematical notion and does not really get a sense in computer science too. This notion is definitely a social and human notion. Our research in this context directly came from the remark that lots of network protocols did not integrate trust diffusion or used a trust notion whose definitions was not close enough to the social reality (cf. [1, 2]) or whose weight or influence seemed to be not sufficient. So, our objective was to implant trust diffusion in networks by basing on the human and social definition of trust. In this report, we are just going to give a brief summary of these researches whose details can be found in [3] and present the interesting perspectives of this work.

3.8.1 Protocol

As we have just introduced, the constructed protocol was created by basing on the social notion of trust that can be defined by : "Firm reliance on the integrity [...] of a person or a thing" and "Certainty based on past experience". Moreover, like in numerous works, the fact that the trust we have in someone is the fruit of the personal experience and the reputation was integrated. Another essential point according to us was that there exist different kinds of trust. Indeed, a researcher can trust the scientific opinion of one of his colleagues without forcedly trusting the opinion of the latter on his other colleagues. That second important point was also integrated. The protocol uses consequently the two following trust notions, trust in actions and in opinions, and computes trust marks to evaluate them. Furthermore, it uses also a double-level of trust by giving trust indices to trust marks that it computes. This second level of trust allows to evaluate the reliability of the computed trust marks and represents our main contribution in the context of trust modeling in networks. All the details about the dynamics of the protocol can be found in [3].

Furthermore, this protocol was tested and validated by simulations in different kinds of networks (more precisely in their underlying graph model). Indeed, it seemed to be relevant to analyse the behaviour of the protocol in complete graphs and social graphs, *i.e.*, power-law fixed degree distribution graphs whose clustering coefficient is important.

Finally, we also focused on the robustness of this trust diffusion protocol by analysing its behaviour against different possible kinds of attacks and by comparing the latter to an other protocol (γ-protocol) which uses the trust diffusion but not the double level of trust (N.B. in [3], we compared it to a protocol which did not use the diffusion principle). Simple attacks were thus simulated and we highlighted that a network implementing such a protocol had to be composed by more than sixty percent of dishonest nodes to be perturbated. Moreover, we focus on more intelligent attacks such as coalitions of nodes called *Trojan attacks* and *detonator attacks*. A Trojan attack consists in the creation of a little group of nodes honest in their action and dishonest in their opinion because they protect a real dishonest node (in action and opinion) that wants to perturbate the network. A detonator attack allows the real dishonest node to launch its dishonesty process after a certain number of interactions. In these

two cases, the protocol showed a great efficiency in comparison to the γ-protocol.

3.8.2 Perspectives

The efficient results obtained thanks to the studied distributed trust diffusion protocol showed that the latter could be of great interest in ad hoc networks and more generally in every kind of networks. Besides, one of the main perspectives would be to implement plugins in order to be able to use it in file-sharing networks such as Emule or BitTorrent. That could allow us to validate it on real networks. Let us note that this protocol could also be used in Internet in order to measure trust users give to web sites and broadcast sites "dishonesty".

However, before thinking to that, some improvements have to be realized. Future researches will focus on the reduction of the size of the transmitted information. The protocols lightness is crucial to avoid the networks surcharge. The challenge here is to find the good equilibrium between its reduction and its relevance.

It would be of interest to increase the robustness of the protocol by thinking to new and more and more intelligent attacks such as, fro instance, a coalition of nodes which wants the others to believe that a certain node is dishonest whereas it is not the case.

Finally, another perspective on which we particularly focus on is the conception and the realisation of an experience in the framework of experimental economy that consists in the creation of a game played by a significant number of remunerated students allowing to obtain some indications about the protocol and target the weak points of the protocol. More details about this perspective are given elsewhere in the report.

Références

[1] S. Buchegger and J.-Y. Le Boudec. A Robust Reputation System for P2P and Mobile Ad Hoc Networks. In *Proceedings of the Workshop on the Economics of Peer-to-Peer Systems*, 2004.

[2] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The EigenTrust Algorithm for Reputation Management in P2P Networks. In *Proceedings of the International World Wide Web Conference*, pages 640–651, 2003.

[3] M. Morvan and S. Sené. A Distributed Trust Diffusion Protocol for Ad Hoc Networks. In *Proceedings of the International Conference on Wireless and Mobile Communications 2006*, page 87 (6 pages). IEEE Computer Society Press, 2006.

3.9 Proposition de validation par l'économie expérimentale

3.9.1 Contexte

Afin d'évaluer de manière réaliste le dernier protocole proposé, M. Neveu (du laboratoire GATE) et D. Dubois (du LAMETA) ont mis en place un jeu de la confiance qui a pour objet la confrontation d'un modèle de confiance/réputation à la réalité des décisions prises par les agents. Pour capturer ces décisions nous prévoyons de recourir à l'économie expérimentale. L'objectif est double : (i) évaluer le modèle dans différents contextes, spécialement les communautés ouvertes et virtuelles, et (ii) contribuer à la paramétrisation du modèle.

Les premiers résultats, issus de simulations du dernier modèle présenté, montrent qu'il peut s'appliquer aux réseaux pairs à pairs et aux réseaux ambiants. Une expérimentation contrôlée en laboratoire, avec des utilisateurs réels, est une étape indispensable pour l'appréciation de la pertinence et de la robustesse du modèle. Deux points feront l'objet d'une attention particulière : (i) la détermination des facteurs qui favorisent l'émergence de communautés, groupes ou sous-groupes, leur pérennité au cours du temps mais aussi leur échec ou mort, et (ii) l'étude des comportements des utilisateurs dans le réseau ou face au réseau. Cette dernière s'appuiera sur l'analyse des décisions prises par les individus : la fixation du seuil de confiance au delà duquel l'individu refuse les interactions avec les membres du réseau et la fixation du seuil de croyance/confiance en les informations circulant sur le réseau au sujet de l'indice de confiance propre à chacun des autres membres du réseau. Cette analyse " empirique " permettra d'ajuster les paramètres du modèle théorique et d'apprécier l'acceptabilité sociale du modèle.

Outre l'outil expérimental, la science économique apporte des connaissances dans le domaine de la confiance. En particulier, de nombreux résultats expérimentaux montrent qu'en matière de confiance et de réciprocité la théorie a des pouvoirs prédictifs limités. En effet la théorie des jeux, qui représente une situation de confiance par le " jeu de la confiance " (trust game), est sans appel : l'équilibre (parfait en sous-jeu) est l'absence de confiance. Les expérimentations en laboratoire montrent au contraire que les individus ont tendance naturellement à faire confiance et à réciproquer. Pour autant la confiance et la réciprocité sont sensibles à différents aspects de l'environnement, comme la possibilité de communiquer avec l'autre, l'existence d'un mécanisme de réputation ou la circulation d'informations sur les comportements des autres membres de la population. Des facteurs psychologiques et sociologiques, encore peu abordés dans les modèles de décisions, affectent également la confiance et la réciprocité des individus.

3.9.2 Le protocole proposé

Lors de la réalisation du jeu en lui-même afin de pouvoir exploiter les données, il faut au minimum des données indépendantes provenant de 6 groupes de joueurs, chaque groupe étant composé au minimum de 6 sujets. De même, le nombre de période de jeu devra être de au minimum 30 pour permettre un phase d'apprentissage, une phase d'essai avant le début de l'expérience est également prévue pour que les sujets se familiarisent avec le jeu.

Les joueurs devront prendre trois types de décisions : un niveau de sécurité (rho) pour déterminer les membres du réseau auxquels le sujet accorde sa confiance, une pondération (lambda) entre le trust mark individuel (lié à l'historique personnel) et le trust mark récupéré sur le réseau (historique des membres du réseau), et un choix binaire de retour en réponse à la confiance accordée par les membres du réseau au sujet : X (ne pas honorer la confiance) et

Y (honorer la confiance).

En première période rho et lambda sont initialisés à 0.5 afin que des interactions puissent avoir lieu. Les sujets ne peuvent modifier ces valeurs. Il s'en suit que chaque sujet interagit durant cette période avec chacun des autres membres du réseau.

Pour modéliser l'acte de confiance d'un sujet à l'égard d'un autre, nous proposons d'utiliser le jeu de la confiance (plus de détails de ce jeu peuvent être trouvé dans [1]).

3.9.3 Conclusion

Nous ne donnons pas ici les principaux détails du protocole en lui-même mais celui-ci est déjà prêt et débattu. Il reste donc à développer le logiciel (ce qui est prévu pour début 2008), à organiser les sessions expérimentales et à analyser les données recueillies à l'aide de modèles économétriques spécifiques. La finalité est d'améliorer le modèle informatique existant et d'en proposer de nouveaux, compte tenu des observations, tout en gardant à l'esprit les deux contraintes que sont la viabilité économique et l'acceptabilité sociale.

Références

[1] D. Dubois, "la confiance dans les interactions économiques et sociales", papier de recherche, LAMETA, Université de Montpellier 1.

3.10 Prestation de l'ingénieur de recherche du projet

Un ingénieur expert, Samuel Galice, a été recruté dans le cadre de cette ACI pour renforcer les moyens de développement logiciel relatifs au projet. La période de sont contrat s'est situé entre novembre 2005 et juillet 2007.

Durant cette période, Samuel Galice s'est attaché à réaliser des simulations concernant le premier protocole proposé sur des graphes particuliers. Dans un deuxième temps, Mr Galice a réalisé une implémentation sur PDAs du premier protocole proposé afin de mesurer les différents temps d'exécution de ce protocole et de proposer un prototype réaliste de celui-ci.

4 Bilan et perspectives

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 sociologues, la confiance est une donnée inhérente à la société qui permet de classifier les différentes interactions à l'intérieur d'un groupe social. 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 des outils qui permettent 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 dernière 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.

Afin de valider socialement l'une de nos approches, nous avons développé un protocole du jeu de la confiance en économie expérimentale qui se veut une représentation du dernier modèle proposé. En effet, nous pensons que dans le cas d'une volonté de description informatique de la confiance, l'utilisation de simulation n'est pas suffisante pour juger si le modèle est pertinent et pourra être facilement utilisé par des personnes ou des groupes sociaux. Ainsi, une validation passant par les sciences humaines et sociales nous semble beaucoup plus réaliste. C'est pourquoi nous pensons que l'économie expérimentale peut nous aider à parvenir à nos fins à défaut de pouvoir tester en grandeur réelle nos modèles.

Publications du projet

Références

[GMU07b] Samuel Galice, Marine Minier et Stéphane Ubéda : the kaa framework : A history-based trust establishment in ambient networks. *Int. J. Intell. Cont. and Syst.*, 12(4):331–340, 2007.

[GMU07c] Samuel Galice, Marine Minier et Stéphane Ubéda : A trust protocol for community collaboration. *In IFIPTM - Trust Management*, volume 236 de *IFIP*, pages 169–184. Springer, 2007.

[BL07] Cédric Lévy-Bencheton et Frédéric Le Mouël : Trust protocol integrating services' semantics. In *4th Workshop for Ubiquitous Networking and Enablers to Context-Aware Services (Ubiq NW) in conjunction with the 4th International Symposium on Ubiquitous Computing Systems (UCS 2007)*, Tokyo, Japan, November 2007.

[GLM+06a] Samuel Galice, Véronique Legrand, Marine Minier, John Mullins et Stéphane Ubéda : A history-based framework to build trust management systems. *In Second International IEEE SECURECOMM Workshop on the Value of Security through Collaboration (SECOVAL 2006)*, page to appear, august 2006.

[GMMU06] Samuel Galice, Marine Minier, John Mullins et Stéphane Ubéda : Cryptographic protocol to establish trusted history of interactions. *In* Levente Buttyán, Virgil D. Gligor et Dirk Westhoff, éditeurs : *ESAS*, volume 4357 de *Lecture Notes in Computer Science*, pages 136–149. Springer, 2006.

[MS06] Michel Morvan et Sylvain Sene : A distributed trust diffusion protocol for ad hoc networks. *In* Petre Dini, Christer Åhlund, Cosmin Dini et Eugen Borcoci, éditeurs : *ICWMC*, page 87. IEEE Computer Society, 2006.

[GLMM06] Samuel Galice, Véronique Legrand et Stéphane Ubéda Marine Minier, John Mullins : Modelization and trust establishment in ambient networks. International Symposium on Intelligent Environment, Cambridge, April 2006. poster, 5 pages.

[GMU07a] Samuel Galice, Marine Minier et Stéphane Ubéda : Gestion de la confiance dans les communautés ouvertes. 2007.

[LGUN05] V. Legrand, S. Galice, S. Ubéda et J.-P. Neuville : Identification pour les réseaux spontanés. *In 4ème rencontre francophone sur Sécurité et Architecture Réseaux*, France, 2005.

[LUMB+04] Véronique LeGrand, Stéphane Ubéda, Joël Morêt-Bailly, Agnes Rabagny, Laurent Guihéry et Jean-Philippe Neuville : Vers un modèle de confiance pour les objets communicants : une approche sociale. *In 3ème rencontre francophone sur Sécurité et Architecture Réseaux*, France, 2004.

[LNAU03] V. Legrand, F. Nait-Abdesselam et S. Ubéda : Etablissement de la confiance et réseaux adhoc : un état de l'art. *In 2ème rencontre francophone sur Sécurité et Architecture Réseaux*, Nancy, France, 2003.

[GLM+06b] Samuel Galice, Véronique Legrand, Marine Minier, John Mullins et Stéphane Ubéda : The kaa project : a trust policy point of view. Research Report RR-5959, INRIA, 2006.

[Gui06] Laurent Guihéry : Internet, réseaux et confiance : les apports de la sciences économique pour une nouvelle économie des réseaux. papier de recherche en cours, projet KAA, 2006.

[Eus07] Julien Eustache : Mechanisms for trust in virtual communities and massively multiplayer online games. LET, Université Lumière Lyon 2, 12 pages, 2007.