INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Team LICIT

Legal Issues in Communication and Information Technologies

Grenoble - Rhône-Alpes

Theme : Knowledge and Data Representation and Management

Activity Report

2009

Table of contents

1. Team

Research Scientist

Daniel Le Métayer [Team Leader, Research Director, INRIA, HdR]

PhD Student

Sophie Guicherd [with University Pierre Mendès-France]
Eduardo Mazza [with VERIMAG]

Post-Doctoral Fellow

Julien Le Clainche [since May 2009]
Manuel Maarek
Guillaume Piolle [since September 2009]
Romuald Thion

Administrative Assistant

Elisabeth Borel

2. Overall Objectives

2.1. Introduction

LICIT is an Exploratory Action created by INRIA in 2008 to undertake new research activities on the interactions between ICT and law. The motivations for this new initiative are manyfold. First and foremost, the very fast evolution of the technological landscape and the impact of ICT on the everyday life of citizens (including their private life) raise new challenges which cannot be tackled by a purely technological approach [21]. For example, the protection of privacy rights on Internet or in pervasive computing environments is by essence multidimensional and requires expertises from disciplines such as social sciences, economics, ethics, law and computer science [23]. Other examples of the ever growing intermingling of ICT and law include e-government, e-justice, electronic commerce, digital rights management (DRM), Radio Frequency Identification (RFID tags), forensics, cybercrime, Web services, virtual worlds.... As far as research is concerned however, there are still very few links between the ICT and law communities. This situation is unfortunate considering the importance of the interests (both societal and economical) at stake. In addition, at a time of growing mistrust of citizens towards technologies, more attention should be paid to the implications of research results on society.

Starting from this observation, the objective of LICIT is to contribute, in partnership with research groups in law, to the development of new approaches and methods for a better integration of technical and legal instruments.

In practice, the interactions between ICT and law take various forms and go into both directions [18]:

- The ICT “objects” are, as any other objects, “objects of law“: on one hand, there is no reason why new technologies and services should escape the realm of law; on the other hand, it may be the case that existing regulations are too specific and need to be adapted to take into account the advent of new, unforeseen technological developments (e.g. certain provisions of privacy regulations become inapplicable in a pervasive computing context, intellectual property laws are challenged by the new distribution modes of electronic contents...). Understanding precisely when this is the case and how regulations should evolve to cope with the new reality may be a tricky “techno-legal” issue with potential impacts on both disciplines.
- ICT can also provide new enforcement mechanisms and tools for the benefit of the law. For example, DRM technologies are supposed to “implement” legal provisions and contractual commitments, Privacy Enhancing Technologies (PET) help reducing privacy threats, certified tools can be provided to support electronic signature, computer logs can be used in courts... At a different level, data mining or knowledge management systems can be applied to the extraction of relevant legal cases, to the analysis of computer logs or the formalization of legal reasoning.

Generally speaking, legal and technical means should complement each other to reduce risks and to increase citizens' and consumers' trust in ICT: on one side, laws (or contracts) can provide assurances which are out of reach of technical means (or cope with situations where technical means would be defeated); on the other side, technology can help enforcing legal and contractual commitments. This synergy should not be taken for granted however, and if legal issues (and more generally, the social consequences of the technologies) are not considered from the outset, technological decisions made during the design phase may very well hamper or make impossible the enforcement of legal rights.

On the longer term, further thoughts need to be devoted to the management of requirements raised by rapidly evolving technologies which may conflict with bodies of regulations which, by essence and for the sake of "legal security", require a form of stability. This complex issue is related to the problem of finding the right level of abstraction in regulations - or strike the right balance between very general principles (which remain stable but offer little indication as far as practical application is concerned, and can thus lead to another form of legal insecurity) and precise provisions whose application may be less prone to interpretation but are bound to become quickly outdated.

The means used by LICIT to reach its objectives are twofold:

1. Research actions: to investigate specific research topics following an interdisciplinary approach in order to better integrate legal and technical instruments. This research work emphasizes the use of formal methods as a link between the ICT and legal dimensions.
2. Networking actions: to favour the emergence of an "ICT and law" research community and to enhance the interest of ICT researchers in this emerging field.

The outputs of the first line of actions are research results whereas the networking actions take the form of joint events (seminars, conferences), joint projects and position papers.

2.2. Highlights of the year

The main results on privacy issues concern both the aforementioned research and networking objectives:

- Definition of a legal and formal framework for privacy agents [6].
- Co-organization of the CPDP Conference and panel on privacy by design [11].

Central to the research themes of LICIT, we have also edited a volume of collected work on "ICT and law: opportunities, challenges and limitations" [15] to be published by Bruylant.

3. Scientific Foundations

3.1. Context

As set forth in Section 2.1, LICIT is by nature not only interdisciplinary but also transversal in the sense that a wide variety of computer science areas are potentially relevant to its activities (security, formal methods, verification, automated reasoning, natural language processing, software engineering...). Encompassing this variety of competences within the action itself is obviously out of reach: the objective of LICIT is rather to establish partnerships with research groups (in ICT and law) providing complementary backgrounds in order to ensure that the highest level of expertise is available to reach the objectives of the action. As far as the legal background is concerned, the relevant domains include individual rights (privacy right, personal data protection, free speech...), contract law, legal evidence, intellectual property, legistics...

In this section, we focus on the computer science area which plays a central role in LICIT, namely formal methods, which serve as a link between ICT and law. We motivate its significance in the context of LICIT in the first subsection before outlining the relevant techniques in the second subsection.

3.2. Formal methods as a link between ICT and law

Beyond their many differences, ICT and law share a strong emphasis on formalism. This commonality is not without reason: in both cases formalism is a way to avoid ambiguity and to provide the required level of rigour, transparency and security. As an illustration, L. Fuller in his book "The morality of law" [17] puts forward the following distinctive features of a legal system: (1) set of rules (2) without contradiction (3) understandable (4) applicable (5) predictable (6) publicized and (7) legitimate. Even though they were obviously not proposed with such a comparison in mind, it is interesting to note that, among these features, the first five are also often used in computer science to characterize a good software specification.

As far as software is concerned, the fact that both disciplines refer to the word "code" is not insignificant and the explorations of the commonalities can be very fruitful (and not only from a theoretical perspective). Indeed, there are many situations where the frontier between the two notions seems to be blurring[1]. Just to take a few examples:

- Software contracts typically incorporate references to technical requirements or specifications which can be used, for example, to decide upon acceptance of the software by the customer or validity of an error correction request. In case of litigation, such specifications can also be used by the judges since they form part of the contract executed by the parties. In this perspective, the contract can thus be seen as an extension of the technical specification including further requirements such as use rights, delivery schedule, warranty, liability...
- Several languages have been proposed to express privacy policies (e.g. P3P by the W3C Consortium and EPAL by IBM); they are used by some commercial sites and can be handled by popular browsers such as Mozilla Firefox or Internet Explorer. The policies published by these sites can be used both by software code - checked by browsers or enforced by Privacy Enhancing Technologies (PET) - and by judges, possibly interpreting them as commitments on the privacy policy of the company.
- The DRM technologies are supposed to implement legal provisions and contractual commitments about the use of digital contents such as music or video.
- More and more transactions are performed on the basis of electronic contracts (SLA: Service Level Agreements for Web and grid services, electronic software licenses, e-commerce contracts...).

In fact, the convergence has developed so much that legal experts have expressed worries that "machine code" might more and more frequently replace "legal code", with detrimental effects on consumers. This topic has stirred up a series of discussions and publications in the legal community [19], [20], [22] and is bound to remain active for quite a long time. Indeed, the implementation of contractual commitments by computer code raises a number of issues such as the lack of flexibility of automated tools, the potential inconsistency between computer code and legal code, the potential errors or flaws in computer code itself or the respective roles of human beings and computers in the process.

The position taken in LICIT is that the first step for a fruitful and useful exploration of the relationships between legal and software code is the definition of a formal framework for expressing the notions at hand, understanding them without ambiguity, and eventually relating or combining them.

3.3. Relevant techniques

The formal methods relevant to LICIT include (1) specification methods and (2) validation methods.

1. Specifications are models or abstract representations of IT systems and their properties which can be used to define their expected behaviour without ambiguity. Specifications can also serve as a basis for various kinds of analyses and tools such as consistency analysis, validation, evaluation, certification, animation.... Specifications can play a role at different phases of the life cycle of a system : before, during or after its design and development. Different specification frameworks

[1] Up to the point that Lawrence Lessig refers to East Coast Code and West Coast Code to denote respectively law and softwre code [20]

have been proposed, which can be roughly classified into semi-formal methods and formal methods. Semi-formal methods provide a well-defined syntax for the models (or "views" of the models) while the underlying semantics itself remains informal; in contrast, formal methods rely on a mathematical framework which is used to define the semantics of the models. The benefit of semi-formal methods is the definition of a shared body of notions, presentation rules and graphical tools which improve the communication and mutual understanding between the actors involved in the life-cycle of a system (designer, architect, development teams, evaluators, etc.). However, because of their lack of mathematical semantics, they do not necessarily guarantee the absence of ambiguity and they do not support formal verification tools. A standard example of semi-formal framework is UML. In contrast, formal methods such as Coq or B come with interactive theorem provers which help users verifying critical properties of their models. In addition, they provide ways to establish a formal link between a model and its implementation (through program extraction in Coq and refinement in B). Both formal and semi-formal methods are relevant to LICIT, especially specification techniques based on "execution traces" where the expected behaviour of a system is defined in terms of properties of its sequences of operations. As far as logical frameworks are concerned, temporal logics (which make it possible to express properties on the future or the past) and deontic logics (which involve obligation and permission operators) are of prime importance to specify legal rules.

2. Validation consists in checking a system to ensure that it behaves as expected. The expected behaviour of the system, as well as the checking process, can be performed in various ways. The most ambitious validation methods involve a formal specification of the system (using one of the aforementioned formalisms) and a proof (usually interactive) that the actual implementation complies with the specification. An alternative approach is to use the formal specification to derive test suites in a systematic way based on well-defined coverage criteria. The validation can also consist in checking simpler properties (typically well-foundedness properties such as type correctness, absence of buffer overflow or implementation of specific security properties) using automatic tools: these tools are called "type checkers" when the properties to be checked are expressed as types and "program analysers" when they are defined in terms of abstract domains. The main benefit of this category of tools is their automation; their limitation is the restricted expressive power of their language of properties. For LICIT, "a posteriori" verifications are as relevant as "a priori" verifications: a posteriori checks are necessary when a priori verifications are either insufficient or not feasible, which is the case in particular for obligations which cannot be enforced by technical means.

To conclude this subsection, we stress the fact that the separations into categories (semi-formal versus formal, type inference versus program analysis, testing versus verification) have been used for the sake of the presentation (and because they originated from different research communities) but the frontiers between them tend to blur: for example certain frameworks include semi-formal and formal techniques, graphical representations such as state diagrams can be endowed with formal semantics, types can be defined in terms of abstract domains, program analysers can themselves be checked by theorem provers...

4. Application Domains

4.1. Industrial applications

The application areas which are directly concerned by LICIT are varied, including

- Internet, pervasive computing, cloud computing, profiling, location based services, smart cards...(especially w.r.t. protection of privacy and individual rights)
- Software licensing, IT contracts (especially w.r.t. liability, compatibility, intellectual property rights).

- Banking services, telecom services, e-commerce (especially w.r.t. liability and validity of electronic contracts)
- Digital content (audio, video, information...) distribution and protection, Digital Right Management (especially w.r.t. liability and intellectual property right protection).
- Forensics and cybercrime (especially w.r.t. liability and digital proofs)

4.2. Current industrial cooperations

The PERSOPOLIS project involves a collaboration with actors of the smart card industry, including OCS (Oberthur Card Systems), TRUSTED LOGIC and CEV.

5. New Results

5.1. Privacy policies

Participants: Julien Le Clainche, Daniel Le Métayer, Guillaume Piolle, Romuald Thion.

Despite apparently strong legal protections, many citizens feel that information technologies have invaded so much of their lives that they no longer have suitable guarantees about their privacy. As a matter of fact, many aspects of new information technologies render privacy protection difficult to put into practice. Many data communications already take place nowadays on the Internet without the users' notice and the situation is going to get worse with the advent of "ambient intelligence" or "pervasive computing" [23]. One of the most challenging privacy issues in this context is the compliance with the "informed consent" principle, which is a cornerstone of most data protection regulations. For example, Article 7 of the EU Directive 95/46/EC states that "personal data may be processed only if the data subject has unambiguously given his consent" (unless waiver conditions are satisfied, such as the protection of the vital interests of the subject). In addition, this consent must be informed in the sense that the controller must provide sufficient information to the data subject, including "the purposes of the processing for which the data are intended". Technically speaking, the consent of the subject can be implemented via a "privacy policy" which should reflect his choices in terms of disclosure and use of personal data. However privacy is a very subtle notion and the definition, implementation and practical use of privacy policies raise a number of challenges. LICIT has tackled these issues from three complementary perspectives in 2009: legal, theoretical and practical :

Legal perspective on the implementation of privacy policies

We have studied the legal issues raised by the implementation of privacy policies through "Privacy Agents", dedicated software components acting as "surrogates" of the subjects and managing their personal data on their behalf. The subject can define his privacy requirements once and for all, with all information and assistance required, and then rely on his Privacy Agent to implement these requirements faithfully. This technical solution triggers a number of questions from the legal side: for example, to what extent should a consent delivered via a software agent be considered as legally valid? Are the current regulations flexible enough to accept such kind of delegation to an automated system? Can the Privacy Agent be "intelligent" enough to deal with all possible situations? Should subjects really rely on their Privacy Agent and what would be the consequences of any error (bug, misunderstanding...) in the process?

In order to shed some light on these legal issues, we have focused on three main aspects of consent : (1) its legal nature (unilateral versus contractual act), its essential features (qualities and defects) and its formal requirements. In a second stage, we have drawn the lessons learned from this legal analysis to put forward design choices ensuring that Privacy Agents can be used as valid means to deliver the consent of the data subject [6]. Several kinds of Privacy Agents have been proposed (Subject Agents, Controller Agents and Auditor Agents) and the roles of the different actors involved in the process have been defined precisely. Privacy policies themselves can be expressed in a restricted (pattern based) dedicated natural language. In order to avoid ambiguities in the expression of the policies, a mathematical semantics of the privacy language has been defined. This mathematical semantics characterizes precisely the expected behaviour of the Privacy Agents (based on the privacy policies defined by their users) in terms of compliant execution traces. In addition, all privacy related actions can be recorded into log files and used as evidence in case of legal dispute.

This work is an illustration of the privacy be design approach [11]. Beyond the specific application to privacy, we have studied in a systematic way the different modes of organization of regulations, the means to measure their practical results (relevance, effectiveness, efficiency, etc.) and the potential effects of the use of technologies on these results [9]. Current privacy regulations have been assessed with respect to these criteria as well as the Software Agent solution put forward here (which appears to implement three regulation modes: administrative controls, deontological rules and liability rules).

A logical framework for the expression of privacy policies

As mentioned above, privacy is quite a subtle notion and the definition of a formal framework for expressing privacy properties and reasoning about them is of prime importance. A major challenge to this respect is to find the appropriate way of integrating deontic and temporal operators. Deontic operators are required because privacy policies are typically expressed in terms of obligations and interdictions. Temporal operators are necessary because obligations and interdictions usually come with deadlines: for example, the controller must inform the data subject before forwarding his data to a third party or must delete the data within a given period of time. Our work on this topic is the follow-up of a thesis prepared in the LIG laboratory (MAGMA team), which has put forward a number of requirements for a suitable integration of deontic and logical operators to express privacy properties (e.g. propagation of obligations until the obligation is met or the deadline is reached, monotony with respect to deadlines, etc.) and has studied their implications in a new deontic logic for privacy (DLP). DLP includes past and future operators as well as an obligation operator and its semantics is defined over Kripke-like bi-dimensional structures. It has been shown, by translation into DLP, that existing proposals do not satisfy all the requirements and have proposed new ways of expressing obligations with deadlines which meet these requirements. This model has been used to express typical rules occuring in privacy regulations and to check that it conveys the intuitive meaning [7].

Privacy policies for healthcare records

Healthcare is one of the most demanding areas with respect to privacy policies and subject consent. First there is a strong pressure to implement electronic healthcare records for a variety of reasons: data availability, quality of care, cost reduction, etc. But the management of healthcare records is quite challenging because healthcare data are considered as sensitive from a legal point of view (with stronger constraints on collection and use) and such records can potentially be accessed by a large number of actors with different privileges (doctors, surgeons, physicians, nurses, etc.). Appropriate means should be provided to allow the patient to define his privacy policy with the required level of detail and confidence. In collaboration with the SMIS project team, we have defined EBAC, an event based access control model which can be used by the patient to mask healthcare records in his folder [14]. The model is based on the concepts of events, episodes and trust relations. Each healthcare record is associated with an event and each event belongs to an episode. An episode is a logically related set of events such as “abortion” or “wisdom tooth extraction”. The trust relation defines, for each episode, what each actor can do and see from the other actors’ actions. To this aim, events are qualified as “shared” or “exclusive” and read and write privileges depend on the qualification of the events. The semantics of the EBAC model has been defined in a relational framework and it has been implemented in the DBMS (Database Management System) system of the SMIS project team in the context of the DMSP (Shared Medical Social Folder) project of the Yvelines district council [5], [14].

5.2. Liability issues in software engineering

Participants: Daniel Le Métayer, Manuel Maarek, Eduardo Mazza.

Software contracts usually include strong liability limitations or even exemptions of the providers for damages caused by their products. This situation does not favour the development of high quality software because software editors don’t have sufficient economical incentives to apply stringent development and verification methods. Indeed, experience shows that products tend to be of higher quality and more secure when the actors in position to influence their development are also the actors bearing the liability for their defects. The usual argument to justify this lack of liability is the fact that software products are too complex and versatile objects whose expected features (and potential defects) cannot be characterised precisely, and which thus cannot be treated as traditional (tangible) goods. Taking up this challenge is precisely the objective of the LISE project: the project studies liability issues both from the legal and the technical points of view with the aim to put forward a formal framework to (1) define liability in a precise and unambiguous way and (2) establish such liability in case of incident.

Obviously, specifying all liabilities in a formal framework is neither possible nor desirable. Usually, the parties wish to express as precisely as possible certain aspects which are of prime importance for them and prefer to state other aspects less precisely (either because it is impossible to foresee at contracting time all the events that may occur or because they do not want to be bound by too precise commitments). Taking this requirement into account, the LISE architecture provides different levels of services which can be used by the parties depending on the economic stakes and the timing constraints for the drafting of the contract:

1. The first level is a systematic (but informal) definition of liabilities.
2. The second level is the formal definition of liabilities. This formal definition itself can be more or less detailed and encompasses only a part of the liability rules defined informally. In addition, it does not require a complete specification of the software but only the properties relevant for the targeted liability rules.
3. The third level is the implementation of a log infrastructure or the enhancement of existing logging facilities to ensure that all the information required to establish liabilities will be available if a claim is raised.
4. The fourth level is the implementation of a log analyser to assist human experts in the otherwise tedious and error-prone log inspection task.
5. A fifth level is the verification of the correctness of the log analyser with respect to the formal definition of liabilities (considering the correspondence between log files and abstract traces).

Each level contributes to reducing further the uncertainties with respect to liabilities and the parties can decide to choose the level commensurate with the risks involved with potential failures of the system. The overall approach followed in LISE has been applied to a representative case study: an electronic signature application on a mobile phone [16], [12].

6. Contracts and Grants with Industry

6.1. Risk and liability analysis

LICIT is involved in an industrial collaboration with TRUSTED LOGIC in the framework of a "Research Valorisation Agreement" on legal issues in software engineering.

7. Other Grants and Activities

7.1. Regional actions

Participants: Daniel Le Métayer, Sophie Guicherd.

The CIBLE programme of Région Rhône-Alpes funds a collaborative project involving LICIT, the Valorisation Service of the INRIA Grenoble Rhône-Alpes and the research group GRDS ("Research Group in Law and Science") of the Law Faculty of Grenoble (University Pierre Mendès-France). The main objective of this project is to study, from a dual - academic and industrial - perspective the legal issues pursuant to software license agreements, especially liability issues. This project funds a doctoral position (Sophie Guicherd).

7.2. National actions

7.2.1. Lise (ANR)

Participants: Daniel Le Métayer, Eduardo Mazza, Manuel Maarek.

The LISE [2] project started in 2008 and is funded by the ANR SESUR programme. LISE is coordinated by LICIT and invloves the AMAZONES and POP ART INRIA project-teams, the Law Faculty of Versailles Saint-Quentin, the Law Faculty of Caen, VERIMAG and SUPELEC.

One of the motivations of the LISE project is the fact that, as observed by several authors, software quality and patterns of security frauds are directly related to legal liability patterns. But the precise definition of the expected functionalities of software systems is quite a challenge, not to mention the use of such definition as a basis for a liability agreement. Taking up this challenge is precisely the objective of LISE. To achieve this goal, the project studies liability issues both from the legal and the technical points of view with the aim to put forward methods (1) to define liability in a precise and unambiguous way and (2) to establish liability in case of disagreement.

7.2.2. Fluor (ANR)

Participants: Daniel Le Métayer, Guillaume Piolle.

The FLUOR [3] project started in 2008 and is funded by the ANR SESUR programme. FLUOR is coordinated by ENSTB and involves the CNRS (IODE), INRIA (LICIT), the LIUPPA (University of Pau), SWID and the University of Polynésie Française.

The FLUOR project aims at protecting corporate documents circulating within companies. More precisely, the objective of the project is to unify information flow models and usage control models and to analyse the legal issues raised by the use of these documents. Emphasis will be put by LICIT on the specification of obligations within organizations and the associated risk analysis.

7.2.3. Persopolis (Competitivity poles Systematic and TES)

Participants: Daniel Le Métayer, Julien Le Clainche.

PERSOPOLIS (2008-2010) is a project funded by the Competitivity poles SYSTEMATIC and TES. The coordinator is OCS (Oberthur Card Systems) and the other partners of the project are CEV, ENSI Caen, IAE Caen, the Law Faculty of Caen, INRIA (LICIT), NBSTECH and TRUSTED LOGIC.

The smart card life cycle includes, before delivery to the end-user, a personalization phase which consists in loading on the memory of the card data which is specific to the user (typically name, credentials, cetificates...). This personalization phase, which is highly critical, is generally conducted in the secured premises of the card manufacturer or subcontracted to a third party (“personalizer”) offering high security guarantees. In order to favour the deployment of service cards managed by local authorities (e.g. city council, social services, employment agencies...) it is necessary to reconsider this centralized personalization process while maintaining the required security guarantees. The objective of the PERSOPOLIS project is to define the technical and legal requirements for the personalization of smart cards in such “open” contexts. Emphasis is put on the management of personal data and the associated liability issues.

7.2.4. Collaborations inside Inria

LICIT collaborates with the AMAZONES and POP ART project-teams in the context of LISE and with the SMIS project-team on the design of privacy policies for healthcare folders.

7.2.5. Cooperations with other laboratories

LICIT collaborates with the following laboratories:

[2] http://licit.inrialpes.fr/lise/

[3] http://fluor.no-ip.fr/

Research groups in computer science:

- SSIR ("Security of Information Systems and Networks") - SUPELEC (LISE project).
- VERIMAG- INPG Grenoble (LISE project).
- SISTEM- ENSI Caen (PERSOPOLIS project).
- CIME - IAE Caen (PERSOPOLIS project).
- LIUPPA - University of Pau (FLUOR project).
- SERES, PRATIC, LUSSI - ENSTB (FLUOR project).
- Terre-Océan - University of Polynésie Française (FLUOR project).

Research groups in law:

- GRDS ("Research Group in Law and Science") - Law faculty of Grenoble, University Pierre Mendès-France (CIBLE project).
- CERCRID ("Research Group in Law") - Law Faculty of Saint-Etienne, University Jean Monnet.
- DANTE ("Business and New Technologies Law") - Law Faculty of Versailles Saint-Quentin (LISE project).
- PRINT("Intellectual Property") - Law Faculty of Caen (LISE and PERSOPOLIS projects).
- IODE (European Regulation and Human Rights) - CNRS (FLUOR project).

7.3. International Actions

LICIT takes part in the activities of the NESSI TSD WG ("Network European Software and Services Initiative - Trust, Security and Dependability Working Group").

8. Dissemination

8.1. Scientific community

As part of the networking activities put forward in Section 2.1, LICIT has organized the following events:

- Organization of the second and third editions of the seminar "DIAGONALES Information Technologies and Society" in partnership with the Law Faculty of Grenoble (Pierre Mendès-France University).
- Co-organization of the Annual Conference on Computers, Privacy and Data Protection CPDP 2009 (Brussels, 16-17 January 2009)[4]. Other organizers are the Free University of Brussels (VUB), the University of Tilburg, the University of Namur and the Fraunhaufer Institute.

Daniel Le Métayer has been a member of the scientific committees of :

- The Annual Conference on Computers, Privacy and Data Protection CPDP 2009.
- The Annual Conference on Security in Network Architectures and Information Systems SAR-SSI 2009.

and has given the following invited talks:

- IRISA, Rennes: *Informatique et libertés : contradiction dans les termes ou nouvelle alliance ?*
- Lille, INRIA-Industries Forum: *Quand le droit se mêle de technologies, et vice versa.*
- Copenhagen, conference "The net will not forget": *Privacy by design: a matter of choice.*
- Paris, Atelier sur le droit à l'oubli (Secrétariat d'Etat chargé de la prospective et du développement de l'économie numérique): *Protection de la vie privée: moyens techniques*.
- Rennes, Conférence C&ESAR (Computer & Electronics Security Applications Rendez-vous), *Quand le droit se mêle de technologies, et vice versa.*

[4] http://www.cpdpconferences.org/program.html

8.2. Teaching

8.2.1. Courses

Daniel Le Métayer has given a tutorial on information technologies and law at ENS CACHAN (Rennes).

8.2.2. Advising

- Eduardo Mazza, co-advised by Daniel Le Métayer (with Marie-Laure Potet, VERIMAG), PhD in computer science, INPG.
- Sophie Guicherd, co-advised by Daniel Le Métayer (with Etienne Vergès, GRDS Law Faculty of Grenoble), PhD in law, Pierre Mendès-France University.

9. Bibliography

Major publications by the team in recent years

[1] F. BESSON, T. JENSEN, D. LE MÉTAYER, T. THORN. *Model checking security properties of control flow graphs*, in "Journal of Computer Security", vol. 9, 2001.

[2] P. FRADET, D. LE MÉTAYER. *Shape types*, in "ACM Symposium on Principles of Programming Languages (POPL'97)", ACM, 1997.

[3] T. JENSEN, D. LE MÉTAYER, T. THORN. *Verification of control-flow based security properties*, in "IEEE Symposium on Security and Privacy", IEEE, 1999.

[4] D. LE MÉTAYER. *Describing software architecture styles using graph grammars*, in "IEEE Transactions on Software Engineering", vol. 24, n^{o} 7, 1998.

Year Publications

Articles in International Peer-Reviewed Journal

[5] T. ALLARD, N. ANCIAUX, L. BOUGANIM, P. PUCHERAL, R. THION. *Seamless Access to Healthcare Folders with Strong Privacy Guarantees*, in "Journal of Healthcare Delivery Reform Initiatives", 2009, to appear.

[6] D. LE MÉTAYER, S. MONTELEONE. *Automated consent through privacy agents : legal requirements and technical architecture*, in "The Computer Law and Security Review, Elsevier", vol. 25(2), 2009.

[7] G. PIOLLE, Y. DEMAZEAU. *Representing privacy regulations with deontico-temporal operators*, in "Web Intelligence and Agent Systems: an International Journal (WIAS)", 2009, to appear.

Articles in National Peer-Reviewed Journal

[8] J. LE CLAINCHE. *Chronique du droit de l'internet*, in "JCP, Semaine juridique", 2009.

[9] D. LE MÉTAYER, S. MONTELEONE, J. MORET-BAILLY. *Les ressources du droit alliées aux moyens de la technologie : application à la protection des données personnelles*, in "Revue Lamy Droit de l'Immatériel (RLDI)", vol. 51, 2009.

Invited Conferences

[10] T. ALLARD, N. ANCIAUX, L. BOUGANIM, P. PUCHERAL, R. THION. *Concilier ubiquité et sécurité des données médicales*, in "Les technologies au service des droits, opportunités, défis, limites", Bruylant, 2009, to appear.

[11] D. LE MÉTAYER. *Privacy by design: a matter of choice*, in "Conference on Computers, Privacy and Data Protection (CPDP)", Springer Verlag, 2009, to appear.

International Peer-Reviewed Conference/Proceedings

[12] C. ALLEAUME, C. BIDAN, V.-L. BENABOU, D. BERAS, N. CREPEAU, S. FRENOT, G. GOESSLER, R. HARDOUIN, L. MÉ, J. LE CLAINCHE, D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. STEER, V. VIET TRIEM TONG. *Liability in software engineering: overview of the LISE approach and application on a case study*, in "International Conference on Software Engineering, ICSE'2010 (conference version of the research report with same title)", ACM/IEEE, 2009, to appear.

[13] R. THION, S. COULONDRE. *Data Dependencies for Access Control Policies*, in "International Workshop on Logic in Databases (LID'09), RR 127", Roskilde University, 2009.

Scientific Books (or Scientific Book chapters)

[14] T. ALLARD, N. ANCIAUX, L. BOUGANIM, P. PUCHERAL, R. THION. *Trustworthiness of Pervasive Healthcare Folders*, in "Pervasive and Smart Technologies for Healthcare: Ubiquitous Methodologies and Tools", IGI Global Publishing, 2009, to appear.

Books or Proceedings Editing

[15] D. LE MÉTAYER (editor). *Les technologies au service des droits, opportunités, défis, limites*, Bruylant, 2009, to appear.

Research Reports

[16] C. ALLEAUME, C. BIDAN, V.-L. BENABOU, D. BERAS, N. CREPEAU, S. FRENOT, G. GOESSLER, R. HARDOUIN, L. MÉ, J. LE CLAINCHE, D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. STEER, V. VIET TRIEM TONG. *Liability in software engineering: overview of the LISE approach and application on a case study*, n^o RR-7148, INRIA, 2009, http://hal.inria.fr/inria-00440437/en/, Research Report.

References in notes

[17] L. L. FULLER. *The morality of law*, Yale University Press, 1964.

[18] D. LE MÉTAYER, A. ROUVROY. *STIC et droit : défis, conflits et complémentarités*, in "Interstices", November 2008, http://interstices.info/jcms/c_34521/stic-et-droit-defis-conflits-et-complementarites.

[19] L. LESSIG. *The future of ideas: the fate of the commons in a connected world*, Random House, 2001.

[20] L. LESSIG. *Code and other laws of cyberspace, Version 2.0*, Basic Books, 2007.

[21] Y. POULLET. *The Directive 95/46/EC: ten years after*, in "Computer Law and Security Report", vol. 22, 2006, p. 206–217.

[22] J. REIDENBERG. *Lex informatica: the formulation of information policy rules through technology*, in "Texas Law Review", vol. 76, n^{o} 3, 1998.

[23] A. ROUVROY. *Privacy, data protection and the unprecedented challenges of ambient intelligence*, in "Studies in Ethics, Law and Technology, Berkley Electronic Press", 2008.