INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Team LICIT

Legal Issues in Communication and Information Technologies

Grenoble - Rhône-Alpes

THEME SYM

Activity Report

2008

Table of contents

1. Team

Research Scientist

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

PhD Student

Sophie Guicherd [CIBLE programme with University Pierre Mendès-France, since October 2008]
Eduardo Mazza [LISE project with VERIMAG, since November 2008]

Post-Doctoral Fellow

Manuel Maarek [LISE project, since November 2008]
Shara Monteleone [ARC PRIAM, until September 2008]
Romuald Thion [since October 2008]

Administrative Assistant

Diane Courtiol [since June 2008]
Helen Pouchot [until June 2008]

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 every day life of a majority of citizens (including their private life) raise new challenges which cannot be tackled by a purely technological approach [19]. For example the protection of privacy rights in "ambient intelligence" environments is by essence multidimensional and requires expertises from disciplines such as social sciences, economics, ethics, law and, of course, ICT [21]. 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 or interconnections 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 [8]:

- 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. part of the 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 regulation should evolve to cope with the new reality may be a tricky techno-legal issue with potential impacts on both sides.
- ICT can also provide new enforcement mechanisms and tools to the justice. 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 "legal" electronic signature, computer logs (when they meet certain requirements) 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 any 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 crucial problem of managing the conflicting requirements raised by, on one hand rapidly evolving technologies and, on the other hand, 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 (such as e.g. regulations about cookies in German law) 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 a pluridisciplinary approach in order to better integrate legal and technical instruments. This research work will emphasize 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 expected outputs of the first line of actions are research results whereas the outputs of the networking action will take the form of joint projects (coordination actions, networks, ...), joint events (seminars, conferences) and position papers.

2.2. Highlights of the year

Keywords: *ambient intelligence*, *law*, *personal data*, *pervasive computing*, *privacy*, *regulation*, *software agent*, *ubiquitous computing*.

The collaborative project PRIAM (Privacy Issues in Ambient Intelligence)[1] has gathered lawyers and computer scientists in 2007 and 2008 with the goal of putting forward a common view of privacy for pervasive computing and effective (legal and technical) instruments to protect it. PRIAM has produced two main results in 2008:

1. A formal framework for privacy management based on "Privacy Agents" in charge of managing personal data on behalf of their owners [10]. This framework has been devised consistently with the requirements and recommendations resulting from the legal study conducted in the project [9], [12].
2. The organization of the PRIAM Conference "ICT and law: opportunities, challenges and limitations" (20-21 November, Grenoble)[2].

3. Scientific Foundations

3.1. Context

Keywords: *automated reasoning*, *contract*, *formal method*, *individual right*, *intellectual property*, *knowledge management*, *legal proof*, *legistics*, *natural language*, *personal data*, *privacy*, *proof*, *semantics*, *semi-formal method*, *specification*, *validation*, *verification*.

[1] http://priam.citi.insa-lyon.fr/

[2] http://priam08.conf.citi.insa-lyon.fr/

As set forth in Section 2.1, LICIT is by nature not only pluridisciplinary but also transversal in the sense that a wide variety of computer science areas are potentially relevant to its activities (security, software engineering, program specification, validation, knowledge management, automated reasoning, natural language 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 intellectual property, individual rights (privacy right, personal data protection, free speech, ...), contract law, legal proofs, legistics, ...

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

3.2. Formal methods as a link between ICT and law

Keywords: *DRM*, *electronic contract*, *formal method*, *legal proof*, *privacy*, *specification*.

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. It is interesting to note for example that L. Fuller in his book “The morality of law” [16] 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. Among these features the first five are also often used to characterize a good 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. 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 exploited by judges since they form part of the contract executed by the parties. The contract can thus be seen in such cases 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 enterprise privacy policies (e.g. P3P by the W3C Consortium and EPAL by IBM); they are used by some of commercial sites and can be handled by popular browsers such as Mozilla Firefox or Internet Explorer. The policies published by these sites can thus 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 [17], [18], [20] 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

Keywords: *formal method*, *program analysis*, *proof*, *refinement*, *semantics*, *semi-formal method*, *specification*, *type checking*, *validation*, *verification*.

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

1. Modelling consists in designing models of IT systems to provide support for various kinds of analyses and tools such as consistency analysis, validation, evaluation, certification, animation, ... Modelling can take place at different phases of the life cycle of a system : before, during or after its design and development. Different frameworks have been proposed for system modelling, 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 incorporate 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.
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 formalisms set forth in (1) above) and a proof (usually interactive) that the actual implementation is consistent with the specification. An alternative 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 can be 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 restriction in terms of expressive power of the language of properties. LICIT will use and extend existing validation techniques to perform "a posteriori" as well as "a priori" verifications. A posteriori checks are necessary when a priori verifications are either not practically feasible or insufficient to establish the effective behaviour of a system.

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 correspond to different research trends) but the frontiers between them are far from absolute: for example certain frameworks include semi-formal and formal techniques, graphical representations such as state diagrams can be endowed with formal semantics, type can be defined in terms of abstract domains, ...

4. Application Domains

4.1. Industrial applications

Keywords: *Ambient intelligence*, *RFID*, *banking*, *complexity management*, *cybercrime*, *digital content*, *e-administration*, *e-commerce*, *e-government*, *electronic commerce*, *forensics*, *impact analysis*, *knowledge management*, *law making process*, *legal reasoning*, *legistics*, *multimedia*, *on-line dispute resolution*, *security*, *software engineering*, *telecommunications*, *telecommunications*, *video*, *video-surveillance*.

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

- Ambient intelligence, RFID, video-surveillance, profiling, geographic information systems, electronic passports, ...(especially w.r.t. protection of privacy and individual rights)
- Software licensing, IT contracts and services, (especially w.r.t. liability, compatibility, intellectual property right).
- Telecom services (especially w.r.t. liability)
- Banking services (especially w.r.t. liability)
- Digital content (audio, video, information, ...) distribution and protection, Digital Right Management (especially w.r.t. liability and intellectual property right protection).
- Digital libraries (especially w.r.t. intellectual property right)
- E-commerce (especially w.r.t. liability and validity of electronic contracts)
- E-services, Service Level Agreements, grids, cloud computing (especially w.r.t. liability and validity of electronic contracts).
- Forensics and cybercrime (especially w.r.t. liability and digital proofs)
- Internet and Web tools (browsers, search engines, ...) and services (Web publishing, Web 2.0, ...), virtual worlds, "Internet of things" (especially w.r.t. protection of privacy and individual rights, liability, intellectual property)
- Security, dependability, quality of service (especially w.r.t. liability).
- Technical assistance to legal activities: contract management, law making process, impact analysis, on-line dispute resolution, legal reasoning, legal knowledge management, complexity management, e-government, e-administration, ...

4.2. Current industrial cooperations

The work on risk and liability analysis described in Section 5.2 is the result of an industrial collaboration in the framework of a "Research Valorisation Agreement" between INRIA and the Trusted Logic Group.

5. New Results

5.1. Privacy issues in ambient intelligence

Participants: Daniel Le Métayer [contact person], Shara Monteleone.

Privacy is a complex and multi-faceted notion, both from the social and from the legal point of view and it has been interpreted in various ways depending on times, cultures and individual perceptions. Notwithstanding such differences, it is widely agreed that the values underlying privacy pertain to fundamental human rights and many regulations, instruments and recommendations have been introduced to protect them . However, despite apparently strong legal protections, many citizens feel that technologies - especially 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" [21]. One of the most challenging privacy issue 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". Imposing that the user of ambient intelligence environments delivers his consent before each communication of personal data would largely defeat the purpose of providing these systems in the first place. This would lead to a situation where individuals would just have the choice between refusing the new services or renouncing to their privacy rights.

One of the results of the PRIAM project is a proposal for a technical and legal infrastructure to solve this apparent discrepancy between ambient intelligence technologies and informed consent. The solution put forward in the project is based on the notion of "Privacy Agent", a dedicated software acting as a "surrogate" of the subject and managing on his behalf his personal data. The subject can define his privacy requirements once for all, with all information and assistance required, and then rely on his Privacy Agent to implement these requirements faithfully. But this possibility also triggers a number of new 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, three main aspects of consent have been studied in PRIAM: (1) the legal nature of consent (unilateral versus contractual act), its essential features (qualities and defects) and its formal requirements. In a second stage, drawing the lessons learned from this legal analysis, a privacy architecture has been proposed to use Privacy Agents as valid means for the consent of the data subject [10]. Actually, several kinds of Privacy Agents have been proposed in PRIAM, including:

- Subject Agents which are installed on a device attached to the subjects (for example their mobile phones) and control all disclosures of their personal data (whether stored on the same device or delivered through other means such as RFID tags or sensors).
- Controller Agents which are installed on the sites of the controllers and manage the access and use of the personal data collected by the controllers. Controller Agents implement the commitments of the controllers and ensure that all requirements set by the subjects are met (retention delay, access right, modification right, ...).
- Auditor Agents which are launched by certified authorities and interact with Controller Agents to check their execution traces.

As far as the legal framework is concerned, the roles of the different actors involved in the process have been defined precisely (including the roles of the subjects, of the controllers, of the Privacy Agent providers and the personal data authority) and contract models have been proposed to formalize the commitments of the Privacy Agent provider with respect to the subjects and to the controllers. In order to minimize the risks of misunderstanding, a simple privacy language has been devised. This language is a restricted (pattern based) natural language dedicated to the expression of privacy policies (the requirements of the subject on one side and the commitments of the controller on the other side). Subjects (respectively controllers) can interact with their agents through a user-friendly interface and double-check a natural text description of their privacy requirements (respectively privacy commitments) before accepting them. In order to avoid ambiguities in the expression of privacy 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 are recorded into log files which can be audited automatically by Auditor Agents (to check that they are consistent with the authorized execution traces) and can also be used as evidence in case of legal dispute.

5.2. Risk and liability analysis

Participant: Daniel Le Métayer.

A broad variety of methods and techniques have been proposed for IT security analysis, both by the academic world and by industry, with a number of differences in terms of scope, objectives and approaches. From our experience however, one of the main challenges for the security analyst remains to get a representation of the security of the system which is both sufficiently complete and sufficiently rigorous. Rigour is especially necessary in order to establish the precise responsibilities of all actors and stakeholders. Responsibility can be understood here both in the technical sense and the legal sense (liability). Indeed, a large number of actors are usually involved in the design and operation of modern IT systems and security issues may increasingly become a matter of liability, especially when substantial valuables are at stake. Evaluating existing security analysis methods by the above yardsticks lead us to their classification into two main categories:

- In the first category, which includes most industrial methods and standards, some level of systematization is attained through the use of catalogues or checklists, which does not provide a sufficient level of rigour. In addition, these methods are appropriate only for the analysis of established (and relatively stable) categories of products such as operating systems or firewalls: they cannot be applied to the analysis of new products in emerging markets for which, typically, no data base of vulnerabilities is yet available.
- Methods in the second category provide a systematic approach based on semi-formal or formal models of the system under study. Different levels of rigour can be attained depending on the formalism used to represent the models and the tools available to analyse them. However these methods, which originate mostly from the academic world, usually focus on technical issues and leave organizational aspects out of their scope.

The ASTRA (for Asset Tracking) method has been devised precisely to fill this gap and provide a framework for the systematic security analysis of innovative products, addressing in an incremental and uniform way both organizational and technical aspects [11]. The method is iterative and relies on the systematic collection and analysis of all security relevant information to detect inconsistencies and assess residual risks. The core of the ASTRA method is the construction and analysis of functions representing different views of the system. These views include traditional notions such as locations, subjects, access rights, contexts, trust levels and sensitivity levels, but also responsability functions. For example, each constraint on the access to a location or an asset by a subject is associated with an actor in charge of ensuring this constraint.

The three main phases of the method are (1) the collection of information, (2) the detection of inconsistencies and (3) the risk assessment. The goal of the first and second one is to build a consistent and comprehensive view of the security of the system. The third phase is repeated, possibly with intermediate decision making steps (e.g. to decide the implementation of additional countermeasures) until a stable state is reached.

A significant advantage of the approach is to separate the issues of defining the set of responsible subjects and evaluating of the risk level. Whereas the risk level depends on the initial assumptions about trust and sensitivity of subjects and assets, the definition of responsible subjects does not rely on such assessments. This property is illustrated by the confinement theorem shown in [11]. Another important benefit of ASTRA, from the practical point of view, is that organizational rules can be handled in exactly the same way as technical rules: individual actors such as security officers or night-watchers can be represented as subjects, physical goods or authorization documents can be represented as assets, rooms or premises are represented as locations, ...

6. Contracts and Grants with Industry

6.1. Risk and liability analysis

The work on risk and liability analysis described in Section 5.2 is the result of an industrial collaboration in the framework of a "Research Valorisation Agreement" between INRIA and the Trusted Logic Group.

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. Priam (ARC Inria)

Participants: Daniel Le Métayer, Shara Monteleone.

PRIAM [3] is a two years (2007-2008) ARC (Collaborative Research Action) funded by INRIA and dedicated to the privacy issues raised by ambient intelligence technologies. PRIAM is coordinated by LICIT and involves two other INRIA teams (ACES and AMAZONES), the Law faculty of Saint-Etienne (Jean Monnet University) and the University of Twente.

One of the results of PRIAM is a proposal for a technical and legal infrastructure to solve the apparent discrepancy between ambient intelligence technologies and the informed consent of the data subject, which is the cornerstone of European regulations in terms of personal data protection. The solution put forward in PRIAM is based on the notion of "Privacy Agent", a dedicated software acting as a "surrogate" of the subject and managing on his behalf his personal data. A formal framework has been proposed for Privacy Agents and the legal issues raised have been analyzed and integrated in the solution. Further details on the results of PRIAM are presented in Section 5.1.

7.2.2. Lise (ANR)

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

The LISE [4] 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 will study 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 disageement.

[3] http://priam08.conf.citi.insa-lyon.fr/

[4] http://pop-art.inrialpes.fr/lise/

7.2.3. Fluor (ANR)

Participants: Daniel Le Métayer, Romuald Thion.

The FLUOR [5] 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 analyze the legal issues raised by the use of these documents. Emphasis will be put by LICIT on privacy issues and the design of a technical framework making it easier for organizations to handle privacy requirements and comply with privacy regulations.

7.2.4. Persopolis (Competitivity poles Systematic and TES)

Participant: Daniel Le Métayer.

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 card memory 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 will be put on the management of personal data and the associated liability issues.

7.2.5. Collaborations inside Inria

LICIT collaborates with the ACES, AMAZONES and POP ART project-teams in the context of PRIAM and LISE.

7.2.6. Cooperations with other laboratories

LICIT collaborates with the following research groups:

- 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 (LISE project).
- 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).
- 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).
- IODE (European Regulation and Human Rights) - CNRS (FLUOR project).
- LIUPPA - University of Pau (FLUOR project).
- SERES, PRATIC, LUSSI - ENSTB (FLUOR project).
- Terre-Océan - University of Polynésie Française (FLUOR project).

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

7.3. International Actions

LICIT takes part in the activities of the NESSI TSD WG FLUOR [6] ("Network European Software and Services Initiative - Trust, Security and Dependability Working Group") and has organized, in collaboration with the project-team AMAZONES, the NESSI TSD WG meeting in Lyon in November 2008.

8. Dissemination

8.1. Scientific community

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

- PRIAM Conference "ICT and law: opportunities, challenges and limitations" (20-21 November Grenoble)[7].
- First edition of the seminar "DIAGONALES Information Technologies and Society"[8] which is expected to become a regular event and is organized in partnership with the Law Faculty of Grenoble (Pierre Mendès-France University).

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

- The Annual Conference on Privacy Protection CPDP (to be held in Brussels, 16-17 January 2009)[9].
- The first International Workshop on Advances in Policy Enforcement (APE'08)[10].

8.2. Teaching

8.2.1. Courses

Daniel Le Métayer and Shara Monteleone have given a course on privacy at INSA Lyon.

8.2.2. Advising

- Eduardo Mazza, co-advised by Daniel Le Métayer (with Marie-Laure Potet, VERIMAG), since November 2008. PhD in computer science, INPG.
- Sophie Guicherd, co-advised by Daniel Le Métayer (with Etienne Vergès, GRDS Law Faculty of Grenoble), since October 2008. 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.

[6] http://www.nessi-europe.com/Nessi/

[7] http://priam08.conf.citi.insa-lyon.fr/

[8] http://www.inrialpes.fr/35632740/0/fiche___actualite/RH=1143806338978

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

[10] http://www.ieee-security.org/Calendar/cfps/cfp-APE2008.html

[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.

[5] D. Le Métayer, V.-A. Nicolas, O. Ridoux. *Exploring the software development trilogy*, in "IEEE Software", vol. 15, n^{o} 6, 1998.

[6] L. van Aertryck, M. Benveniste, D. Le Métayer. *Casting: a formally based software test generation method*, in "IEEE Int. Conference on Formal Engineering Methods (ICFEM 1997)", IEEE, 1997.

Year Publications

Articles in International Peer-Reviewed Journal

[7] D. Le Métayer, S. Monteleone. *Automated consent through privacy agents : legal requirements and technical architecture*, in "The Computer Law and Security Report, Elsevier", 2009.

Articles in National Peer-Reviewed Journal

[8] 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.

Invited Conferences

[9] S. Monteleone. *Data protection e comunicazioni: necessita di un approccio tecnico-giuridico*, in "La disciplina delle varie forme della comunicazione", Jovene editore s.p.a., 2008.

International Peer-Reviewed Conference/Proceedings

[10] D. Le Métayer. *A formal privacy management framework*, in "Formal Aspects of Security and Trust (FAST'2008)", LNCS, 2008, http://pop-art.inrialpes.fr/~lemetayer/fast2008.pdf.

[11] D. Le Métayer, C. Loiseaux. *ASTRA: a security analysis method based on asset tracking*, in "Proceedings of the IFIP TC 11 23rd International Information Security Conference", vol. 278, 2008, p. 541-555, http://pop-art.inrialpes.fr/~lemetayer/ifipsec2008.pdf.

[12] D. Le Métayer, S. Monteleone. *Computer assisted consent for personal data processing*, in "3d LSPI Conference on Legal, Security and Privacy Issues in IT", 2008, http://pop-art.inrialpes.fr/~lemetayer/lspi2008.pdf.

[13] R. Thion. *Conception de modèles de contrôle d'accès dédiés pour les systèmes d'information de santé*, in "9th International Conference on System Science in Health Care (ICSSHC'08)", 2008.

National Peer-Reviewed Conference/Proceedings

[14] M. Maarek, Y. Naudet, P. Plichart, T. Latour. *Ontologies, règles et services: vers une connaissance actionnable*, in "2d Francophone Conference on Ontologies (JFO'08)", ACM Digital Library, December 2008.

[15] M. MAAREK, D. LE MÉTAYER. *Deriving legal arguments from software traces*, in "Natural Language Engineering and Legal Argumentation Workshop (NaLELA 2008)", ACM Digital Library, 2008.

References in notes

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

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

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

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

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

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