Modeling Security and Trust Relationships within Organizations
MOSTRO

1. Project Title
Modeling Security and Trust Relationships within Organizations

2. Acronym: MOSTRO

3a. Principal investigator

Institution: Laboratory for Applied Ontology – Istituto di Scienze e Tecnologie della Cognizione - Consiglio Nazionale delle Ricerche (ISTC-CNR)

Name: Nicola Guarino

Address: Via Solteri, 38 – 38100 Trento

Telephone: 0461-828486

E-mail: guarino@loa-cnr.it

3b. Officer with legal responsibility

Institution: Consiglio Nazionale delle Ricerche, Istituto di Scienze e Tecnologie della Cognizione, Sezione di Padova

Name: Emanuela Magno Caldognetto

Address: Via Anghinoni, 10

Telephone: 049-8274418

E-mail: magno@csrf.pd.cnr.it

4. Co-principal investigators

Institution: Universita'' degli Studi di Trento, Dipartimento di Informatica e Telecomunicazioni (UNITN)

Name: Fabio Massacci

Address: via Sommarive, 14 – Povo - Trento

Telephone: 0461-882086

E-mail: massacci@ing.unitn.it

Institution: Institut de Recherche en Informatique de Toulouse (IRIT)

Name: Andreas Herzig

Address: 118 route de Narbonne - 31062 Toulouse cedex 04 - France

Telephone: +33 5 61 55 81 23

E-mail: Andreas.Herzig@irit.fr

5. Table of contents

1. Project Title 1
2. Acronym 1
3a. Principal investigator 1
3b. Officer with legal responsibility 1
4. Co-principal investigators 2
5. Table of contents 2
6. Abstract 3
7. Keywords 3
8. Project type 3
9. Length (in months) and beginning date of the project 3
10. Project description 4
  10a. Overall goal and specific objectives 4
  10b. State of the art and preliminary results 7
  10c. Scientific relevance and benefits 10
  10d. Methods and expected results 11
  10e. Workplan and deliverables 12
  10f. Gantt Chart 13
11. Resources available 13
12. References 14
13. Description of research units 16
  13.1. ISTC-CNR 16
  13.2. UNITN 18
  13.3. IRIT 21
14. Budget 24
  Table 14a 24
  Table 14b 25

Table 14c 25
15. Yearly budget justification 26
Table 15a - First year 26
Table 15b - Second year 26
Table 15c - Third year 26

6. Abstract

Although security concerns are central to organizations, they rarely affect the design and development of the software. This simple observation explains why nowadays software problems are mainly due to security design flaws. These kinds of flaw are hard to detect, and are often the major cause for system reorganization and adjustments, that is, for notoriously expensive processes.

Different factors concur in determining this situation: first, security is a non-functional requirement, thus it is hard to capture with standard software design techniques; second, security is mostly a social and not a technical problem, thus it is hard to capture in standard design languages; third, there is no homogeneous way to represent security concerns at different levels of software description, thus it is hard to trace security issues along the phases of software development.

The MOSTRO project aims at aims at detecting and isolating security flaws at the very early stages of software design and development, taking into account as well as the reasons for existing ineffective practices in software design. Our approach is based on an interdisciplinary view of the security problem that includes techniques from ontological analysis, security modeling, multi-agents reasoning, and systems engineering, and incorporates security concerns in a coherent and formally verifiable way at all the stages of software design and development.

For achieving this, an ontologically well-founded language for modeling organizations will be developed, paying particular attention the social interaction within organizations, as related to security requirements. The intended semantics of this language will be described by means of an axiomatic theory, the Organizations Security Ontology. Relying on such ontology, the project will develop formal reasoning techniques and algorithms allowing one to analyze organization and system models with respect to security. The methodology itself will consist of a set of guidelines to be used in the everyday practice of requirements engineering. A specific case study related to the security problems of electronic payments, proposed by Informatica Trentina SpA, will be defined in the early phase of the project. It will serve to elicit real-world information for the ontological analysis, and validate both the methodology and the reasoning algorithms.

Due to the international reputation of its partners, who have a leadership position in all the scientific areas addressed, the project plans also to have a long-term educational impact in Trentino, fostering the diffusion of high-quality technical and scientific competence in the critical sectors of information systems design and business analysis.

7. Keywords

requirements engineering, ontological analysis, security modeling and analysis, automated reasoning, agent societies

8. Project type

Mixed research

9. Length (in months) and beginning date of the project

Length: 36 months. Beginning date: 1st January 2004

10. Project description

10a. Overall goal and specific objectives

A guiding scenario

NovelTrends is a forward looking public administration (it could as well be a corporation) and it has been spurred by the European and National legislation on security and data protection (EU Directive 97/66/CE L.675/96 DPR 318/99, DPCM 16/1/2002 "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali.") to write their own security policies, their security operating procedures, and to comply with the requirements of the law.

Since NovelTrends is a complex organization and runs (in outsourcing) many ERP/HR (Enterprise Resource Planning/Human Resources) packages, they decided to write their own security policy with the (expensive) help of a top consultancy company. The result is a policy that uses a combination of bottom-up and top-down processes. This is described in a comprehensive document of 1000+ pages. Each single system, like backup procedures, permissions to access the ERP system for the administrative staff, etc. is listed and described in detail. The ERP support group has even created a small plug-in to the ERP system so that, if a person changes position in the administration, her permissions change accordingly.

The proud chairman has presented the 1000+ document to the board, which has duly approved it, and a few separated reports: one from the software administrator office (ensuring that the policy guidelines can be implemented in the existing software system), one from the executive manager office (ensuring that the policy guidelines address the security needs of the company), and one from the legal office (ensuring that the policy guidelines satisfy the existing laws on this subject).

Yet, no member of the board, including the chief technical officer, has a clue on how these 1000+ pages are actually related to the goals of the organization and to the structure of the trust relationships embedded in its hierarchy. Although they could read who has access to what, they cannot find in these guidelines the *reasons* (rationales) for deciding about these access rights. This kind of information is not included in the document nor in the reports they approved. Indeed, they read the policy without understanding what it actually does because the relationships among the different elements are hidden in the overwhelming amount of details, case lists, and procedures that constitute the policy itself.

Motivations and overall goals

As opposed to what occurs for other kinds of requirements, for security modeling there are no such things as well-assessed languages for capturing security requirements at the high organizational level, nor methodologies, tools and techniques for transforming such descriptions into progressively more detailed descriptions down to running code.

One of the fundamental reasons behind this gap is that Software Engineering has been considering security as a non-functional requirement [5]. Non-functional requirements introduce quality characteristics, but they also represent constraints under which the system must operate [31,35]. System designers have recognized the need to integrate most of the non-functional requirements into the system development processes [10], for instance reliability and performance. However, security remains an afterthought.

The usual approach towards the inclusion of security within a system is to identify security requirements *after the definition of the software.* This attitude often leads to problems, since security mechanisms have to be fitted into a pre-existing design, therefore generating serious design challenges as software vulnerabilities [32] or organizational blunders [1].

A second difficulty, pointed out by R. Needham (former head of Microsoft Research), is that security is mostly a social problem, rather than a technical problem. For instance, there is often a difference between the alleged protocols that users should follow when working with the software (those dictated by the formal organization trust relationships) and other possible protocols dictated by malice, incompetence, or short cuts. These problems arise at the interface between the software and the users, and this is one of the reasons why we prefer to use the term "system engineering" rather than "software engineering" in dealing with this problem.

Technically, there are at least three reasons for the lack of support for security [25]. Firstly, security needs are generally expressed by organizational security policies. An organization defines high-level policies about security with respect to its strategic objectives and its organizational structure. Such policies have to be mapped to the specific functionalities of the computerized information system. Without an explicit model of the organization and the trust relationships between its components, it is difficult to find a connection between organizational security policies and the system functionalities. Also, consequently, it can be particularly complex to find the motivations regarding specific functionalities. Secondly, security constraints are generally difficult to analyze and model. A major problem in analyzing non-functional constraints is the need to distinguish functional and non-functional requirements and yet, at the same time, a single non-functional requirement may relate to one or more functional requirements. On the one hand, if non-functional requirements are stated separately from functional requirements, it is sometime difficult to see the correspondence between them. On the other hand, if stated with the functional requirements, it may be difficult to keep separate functional and non-functional considerations. On top of this, developers lack expertise for secure system development. Many developers, who are not security specialists, must develop or integrate systems that require security features. Without an appropriate methodology to guide those changes, it is likely that they fail to produce effective solutions [28].

Security should be considered during the whole development process and it should be defined together with the analysis of the structure of the organization and the requirements specification. Taking security into account along with the functional requirements throughout the development stages helps to limit the cases of conflict by avoiding them from the very beginning or to isolate them very early in the development process. On the contrary, adding security concerns as an afterthought increases the chances of conflicts. A solution to this kind of problems requires a deep study of the system, its organization, and its properties. Thus, a considerable amount of money and valuable time is needed. Also, most of the times a major rebuild of the system becomes necessary.

Unfortunately, current methodologies for software development do not meet the needs for resolving security problems [34], and fail to provide evidence of integrating successfully security concerns throughout the whole development process. A number of solutions ranging from UML extensions to novel conceptual models have been proposed for modeling security features. But we lack models that focus on high-level security requirements, i.e., models that do not force the designer to immediately get down to security mechanisms. Moreover, current methodologies do not support sufficiently the activities for detecting security problems at the organizational level when the focus is on the strategic objectives rather than on the single activities adopted for achieving them.

To overcome these limitations, we plan in this project to develop a methodology that integrates requirements engineering with ontological analysis, adopting at the same time a rigorous logical formalization that will allow expressing and reasoning about security constraints. The formal ontological analysis of interactions within organizations will allow us to isolate and define the most fundamental entities and relationships involved in the system at stake, such as actor, goal, task, resource, ownership, trust, delegation, control…. An essential aspect of this methodology will be the capability of considering security concerns since the early phases of the requirements

analysis process. Single agents in the organization with their strategic goals and intentions will be analyzed using the approach of agent theory; social organizations will be modelled as a different kind of agents, depending on their constitutive norms and the people that recognize them; security aspects will then be modelled in terms of socio-cognitive theories of interaction among agents, by addressing the related social relationships of ownership, delegation, trust, control, and accessibility. Such a methodology will make clear why security mechanisms (such as authentication, access control, back ups, or even guards on duty) are necessary, and what are their tradeoffs from the standpoint of the corporate mission.

A different conclusion

Going back to the initial scenario, our project would contribute to reach a different conclusion.
A 20+ pages policy describing the goals and the trust structure of the organization (and accessible to the non-specialized) is proposed and approved by the NovelTrends board. The policy comes together with a 100+ pages of annex for the technically inclined and a methodology (possibly tool assisted) is available for producing the 1000+ pages detailed security document. Furthermore, the methodology explains how to take into account the company's organizational structure (given by the Human Resource Department) as well as its information system structure (given by the Information & Communication Technologies department). With such a methodology, the system developer can effectively match individual requirements at any level with the high-level goals and security requirements described in the policy approved by the board.

Specific objectives

O1. Well-founded ontology of security within organizations

We shall develop an ontologically well-founded language for modeling organizations, with a specific focus on security requirements. This objective includes the semantic characterization of a set of basic primitives for modeling organizational and security concepts, by means of an axiomatic theory, the *Organizations Security Ontology*. The language will be based on the goal/actors paradigm, and will account for notions such as "actor", "role", "goal", "subgoal", as well as for various dependency relations between actors and goals. It will rely on classical approaches based on the BDI (Belief, Desire, Intention) paradigm and logics of action, extended with social notions such as ownership, delegation and trust, The general aim is to make possible to express security considerations from very early phases of requirement analysis.

O2. Security Modeling Methodology

We shall develop a methodology for security modeling and analysis that builds on the results of ontological analysis (O1) and on existing methodologies for requirements engineering such as TROPOS [18], and aims at producing a set of guidelines to be used in the everyday practice of requirements engineering, The methodology will make clear the reasons of adopting specific security mechanisms, while addressing two crucial phases of software development:

- in the early requirements phase, which focuses on the system's organizational setting (*organization analysis*), it will allow to describe the social relations between the relevant actors (both humans and software systems), and to model *implicit* security aspects in terms of such relations.
- in the late requirements phase, which addresses the relevant functions and qualities of the system-to-be (*system requirements analysis*), it will allow for analyzing the *explicit* security needs, relating them to the goals of the stakeholders and their dependencies with the system.

O3. Automated detection of security constraints and critical processes

Relying on the logical theory developed for O1, we will develop algorithms that allow one to analyze organizations and system models with respect to security. In particular, we will focus on various kinds of analysis, such as ownership analysis (e.g., deciding whether it is possible for an actor to use a specific resource without the permission of its owner) and obstacles analysis (e.g., detecting combination of events that may break some security requirements). We will also develop a demo to show how the reasoning techniques can be used in concrete cases, with specific reference to the case study described below.

O4. Assessment of a concrete case study

A specific case study, proposed by Informatica Trentina SpA[1], will be defined in the early phase of the project. It will serve to elicit real-world information for the ontological analysis, and validate both the methodology and the reasoning algorithms. The case study will focus on an application called *Mandato Informatico*, a set of electronic payment services based on the ASP (Application Service Provider) technology. Such services include: managing the payment instructions from a public administration, authorizing the electronic signature, sending the signed documents to the bank, archiving the signed documents, acquiring payment receipts from the bank, and sending them back to the public administration. Informatica Trentina plays the role of the Certification Authority, and delivers smart cards on the basis of the organization model provided by the public administration. We shall discuss with Informatica Trentina whether focusing on the electronic payment service for PAT, already activated last year, and/or similar services involving other public administrations, that will start next year.

10b. State of the art and preliminary results

Given its highly interdisciplinary nature, this project relies on a variety of scientific results that may appear very different from each other. Yet all the partners involved are motivated to approach the project's goals in a holistic way, and are looking forward to a fruitful "contamination" of techniques and ideas. We can identify several areas of scientific investigation, currently corresponding to more or less separate communities, which will be touched by this project:

- conceptual modelling and requirements engineering
- multi-agent systems and the Semantic Web
- cognitive modelling of social interaction;
- formal ontological analysis;
- reasoning techniques for multi-agent-systems

Each partner has an international leadership in at least one of these areas. Moreover, the project will build on the results of previous projects (TICCA[2], WonderWeb[3], ALFEBIITE[4], In the following, we shall briefly discuss the state of the art and the preliminary results achieved by the partners with respect to the main project's goals. Since all the partners have given a substantial contribution to the state of the art, we shall also show their capability to carry out the proposed work, anticipating the arguments summed up in Section 10d.

[1] Informatica Trentina will participate to the project as a consultant (see Section 10d)
[2] Cognitive Technologies for Interaction and Cooperation with Artificial Agents. Project coordinated by ITC-IRST and co-funded by PAT and CNR.
[3] http://wonderweb.semanticweb.org
[4] http://www.iis.ee.ic.ac.uk/~alfebiite/ab-home.htm

O1 - Ontological analysis

While so-called ontologies[5] are now a very popular topic in computer science, their use for modelling security aspects is rather limited. The need for a "security ontology" is however well recognized, especially in the Semantic Web perspective [15][6]. Very recently, the Foundation for Intelligent Physical Agents (FIPA) has launched a Technical Committee for developing a security ontology for Multi-Agent Multi-Domain systems[7].

In philosophy, an ontological analysis of security issues leads immediately to the notion of *social reality*, studied in detail – among others – by Reinach, Searle, Gilbert, and Tuomela. Social entities are things like norms and roles, whose very existence depends on a *plurality of subjects,* a "society" of intentional agents. Security issues have been however only marginally mentioned in the philosophical ontology literature.

In the multi-agent systems community, a further important contribution to the ontological analysis of security aspects comes from cognitive theories of social action, such as those developed at ISTC-CNR by Castelfranchi and his collaborators [9]. In particular, the recent work on the theory of trust and control [12,13] appears to be very relevant for this objective.

The ISTC-CNR Laboratory for Applied Ontology (LOA) is in an excellent position for integrating these previous results in a consistent axiomatic theory, building on their extensive previous work on formal ontology; in particular, they shall exploit the results of the European project WonderWeb, which aims at developing a library of *foundational ontologies*, and the project TICCA, funded by the Provincia Autonoma di Trento, which focuses on the ontology of social interaction[8]. Moreover, they will count on the experience of UNITN in the field of conceptual modelling and requirements engineering (specifically applied to security issues) in order to combine the theoretical aspects of ontological analysis with the practical needs of systems engineering.

IRIT will also contribute to this objective by bringing the contribution of semantics of discourse to the ontology of interaction, as developed within the joint project SOIA[9], involving both IRIT and LOA, with an IRIT person (Laure Vieu) on long-term leave at LOA.

O2 – Security modelling methodology

In the requirements modelling field, we rely on the UNITN experience on the Tropos methodology[10], which has been recently used to model security concerns. For example, in [26] the authors show the relevance of modelling relationships among strategic actors in order to elicit, identify and analyze security requirements. In particular, the analysis of dependency relationships helps identifying attackers and their potential threats, while the analysis of actors' goals helps to elicit security issues in the dynamic decision-making process. Goal models have also been used to model privacy concerns [35], and to evaluate the related software solutions.

A first attempt to extend the Tropos methodology to model security issues throughout the whole software development process has been proposed in a joint work between UNITN and the University of Toronto [29, 30]. Such extension adopts the notions of *security constraint* and *secure capability* as basic concepts to be used in order to integrate security concerns throughout all phases of the software development process. The notion of constraint is however not sufficient to capture the trust relationship.

---

5 Briefly, an ontology – in the present context – is a logical theory that accounts for the intended interpretation of a vocabulary. See [Guarino 98].
6 See also http://www.wiwiss.fu-berlin.de/suhl/bizer/SWTSGuide/
7 See http://www2.elec.qmul.ac.uk/~stefan/fipa-security/documents/f-in-00084-security3-workplan-v0.14.pdf
8 See the recent work of Emanuele Bottazzi (University of Ferrara), who has recently got his degree in Philosophy with a thesis on the ontology of organizations, completely developed at ISTC-CNR/LOA [2].
9 http://www.loa-cnr.it/Files/SOIA.pdf
10 http://www.troposproject.org

A further extension of the Tropos methodology has been proposed in [18], and focuses on early phases of the modelling process, i.e., requirements analysis. Other methodology proposals address the subsequent phases, aiming at enhancing UML to cope with security constraints. In particular, [23, 24] propose an extension of UML where cryptographic and authentication features are explicitly modelled. This model is rich enough to allow for a detailed analysis, and has been driven by a case study on electronic payment systems [22]. In comparison to the one developed by UNITN (which focuses on a similar case study), the system is fairly low-level, and is therefore suited to a more operational analysis. The integration of the two methodologies seems to offer a promising line of research: one can start from a high-level system analysis using the security-enhanced Tropos methodology, and then continue down the line to an operational specification using UML. Another proposal for enhancing UML with security features is the SecureUML language [21, 27], which, however, is geared towards access control: the work focuses on providing concrete syntax for representing access control notions in UML, so that access control policies can be directly modelled, and formal properties derived. These modelling features are indeed essential, but from our perspective only at the end of the system modelling process.

A further enhancement of Tropos, which we plan to implement in this project, is based on the clear separation of the roles involved in a dependency relation. For example, when modelling a credit card transaction, this means making a clear distinction between who is offering a card-transaction service (the merchant processing a credit card number), who is requesting the service (the bank debiting the payment), and who owns the money (the cardholder). Such distinction makes it possible to capture the high-level security requirements of an industrial case study without being caught into considerations about cryptographic algorithms or security mechanisms (where purpose is obscured in a morass of different details). The modelling process we envision has the advantage of making clear *why and where* encryption, authentication or access controls are necessary, and which trust relationships or requirements they address; moreover, we want to be able to discover and elicit the security issues from the structure of the organizations to be modelled. To this purpose, we believe that (i) an *ontological analysis* of organizations and their internal and external relationships is necessary, and (ii) suitable reasoning techniques must be adopted.

O3 - Reasoning on multi-agent interactions

Reasoning about agents and their interaction is a traditional topic in AI and philosophy. It includes at least the following subdomains:

- logics of action and planning [4]
- epistemic logic [11]
- speech act theory and agent communication languages [19, 20]
- deontic logic [3]
- logics of goal and intention [6, 7, 20]

All of these approaches focus on particular aspects, and none of them has a comprehensive account. This can be explained by the fact that the design of a universal framework is a difficult task, and logicians have always preferred to isolate concepts such as that of knowledge, and analyze them in depth. Probably the approach that is best developed, and to which one of the partners, IRIT, has significantly contributed, is Cohen and Levesque's framework for rational agency and interaction, which combines reasoning about belief, goals, intentions, and actions, and includes (at least parts of) speech act theory. As pointed out by several authors [33, 8], what is nevertheless lacking are notions such as obligation, permission and interpersonal commitment, which will be specifically addressed by this project. Another drawback of the theory is that there is a basic semantics, but nevertheless many of its features are only described syntactically, and lack semantics. One of the aims of the present project is thus to provide a more appropriate semantics and to integrate into it deontic components. The fact that many of the participating researchers (especially from IRIT but

also from ISTC-CNR and UNITN) have contributed to the different components allows us to realistically expect that such an integrated theory can be achieved during the project.

Once we have a clear-cut semantic framework, the next step towards formal techniques for reasoning about security is the development of automated deduction tools. While by now powerful algorithms for particular modal logics exist, there is no such tool for the kind of complex logics resulting from the combination of logics above. In previous work, IRIT researchers have advocated the usefulness of a generic modal theorem prover, and have implemented the LOTREC prototype in collaboration with Fabio Massacci (now at UNITN) [14]. Further work about reasoning strategies and combinations of theorem provers will be done during the project, based on both IRIT and UNITN past experience. This will be complemented with IRST expertise, as discussed in Section 10d.

10c. Scientific relevance and benefits

Application security is typically an afterthought in the software development process. Generally speaking, only after vulnerabilities are discovered (mainly due to testing or to feedback from the final user) the designer considers possible alternatives to solve the known problems. It is publicly recognized that software products are rarely bug-free. Bugs are introduced mainly during the design and/or the development phases, with the effect that the resulting software may misbehave or may become vulnerable to external attacks. Nonetheless, many companies treat security as 'penetrate and patch' disregarding existing security practices that would produce safer applications. This explains, at least in part, why seventy percent of the defects are due to security design flaws [17] and why the most common security mistake is the lack of adequate authentication and access control. In addition to the security drawbacks, this general attitude is the main cause for recovery and design adjustments, a notoriously expensive process.

By adopting basic software engineering principles, it is easy and relatively inexpensive to fix software flaws if these are detected early in the development process. That is, the ideal scenario is a design methodology that does not allow for security drawbacks in the first place. Some studies [17] have considered the return in investments on secure software engineering practices. The return was quantified to be 12% of the investment when the security analysis was performed during testing, 15% when performed during implementation, and 21% when performed during the design phase. Indeed, these studies demonstrate convincingly that developers should take into consideration security quality at the very early stages of the process. Furthermore, it has been shown in the same studies that the cost of correcting security flaws increases when performed at later stages of the software development.

Our project aims at detecting and isolating security flaws at very early stages of software design and development, taking into account the detection of security problems as well as the reasons for existing ineffective practices in software design. Our approach is based on an interdisciplinary view of the security problem that includes considerations from ontological analysis, security modeling, and system engineering which is a novelty in the security research area. Indeed, these three disciplines provide the main tools necessary to develop a new methodology and to guarantee the uniformity and completeness of the result.

The project aims at two main improvements over the existing status of the research.
First, it provides an ontological analysis of the social interactions within organizations putting together – in a single logical framework – agent theories, ontologies of social reality, and theories of interaction. This itself is an important contribution and we expect the part of our methodology related to this issue to be applicable to other areas as well, that is, beside security applications. For instance, e-government, information technology and law, web services and e-commerce are all areas that would benefit from using these formal models.

Second, a major benefit of our methodology will be the possibility to understand and characterize the security needs specific to an organization, independently of (and beyond) the system currently used by an organization (if any). In this way, the developer can reliably:

1. translate security requirements into specifications for the software system,
2. test and evaluate a preexisting system with respect to the requirements specific to the organization, and
3. build a software system that conforms to the specific needs, if needed.

10d. Methods and expected results

We have already shown that, given their international reputation in the respective fields, the partners are perfectly capable to perform the specific work proposed to each of them. The strategy we shall adopt to blend these competencies together in a coherent project is as follows.

First of all, we rely on the case study presented in Section 10a (Objective 4) as a way to get the different scientific "souls" of the project focusing on a single practical, relevant, and visible application scenario. Under the coordination of UNITN, the case study will be defined and discussed in more detail in the early phase of the project, with the contribution of all the partners, and the crucial collaboration of an external consultant, Informatica Trentina SpA.

Then we shall start the phase of ontological analysis, with the purpose of defining the boundaries of the problem, isolating and characterizing the main properties and relationships. All the three partners (with different roles) will be involved again in this phase, under the coordination of LOA (ISTC-CNR).

The result will be a logical language whose inferential capabilities and computational properties will be studied by IRIT, with the support of another external collaborator: ITC-IRST, Automated Reasoning Systems division, formal methods group (Paolo Traverso and Marco Roveri). The algorithms and tools already developed by IRIT and ITC-IRST for reasoning about agents' beliefs and actions will be adapted to the chosen language, and their effective capabilities will be demonstrated in the final phase of the project, applied to the case study. In particular, the T-Tool, a tool for analyzing early-requirements engineering in Tropos [16], will be extended with the verification techniques and algorithms devised within this project.

At the same time, UNITN and LOA will work together on the development of a practical methodology for security modeling, strictly intertwined with the results of ontological analysis.

The project's goals will be also pursuit by exploiting various existing national and international collaborations. Concerning the formal ontology of social reality, we plan to collaborate with the Institute for Formal Ontology and Medical Information Systems (IFOMIS, Leipzig: prof. Barry Smith), the Columbia University (prof. Achille Varzi), the University of Geneva (prof. Kevin Mulligan), the University of Texas at Austin (prof. Nicolas Asher), the University of the University of Torino (prof. Leonardo Lesmo and Maurizio Ferraris), and the CNR institute for Theory and Techniques of Juridical Information (ITTIG-CNR, Firenze). In the area of security and requirements engineering, we shall collaborate with the University of Toronto (Tropos group) and the Technical University of Aachen. Concerning the reasoning techniques and the logics of interaction, important collaborations will be maintained with the University of Sofia (prof. Dimiter Vakarelov), the Rand Afrikaans University of Johannesburg (prof. Valentin Goranko), and with France Telecom (David Sadek).

In order to present our scientific results to the international community, and to stimulate further research in this field, we plan to organize an international workshop towards the end of the project, aiming at the maximal impact and visibility, both at the scientific and at the industrial level.

Finally, on the educational side, we shall involve a good number of PhD students and post-doc researchers in the project, and we plan to organize courses and seminars related to the topics we shall address. We are confident therefore that this project will have a long-term educational impact

in Trentino, and will foster the diffusion of high-quality technical and scientific competence in the critical sectors of information systems design and business analysis.

10e. Workplan and deliverables

The research activities are organized in 5 workpackages. Each workpackage has a scientific coordinator in charge of the contents and of the monitoring of the activities. The workpackages are decomposed into tasks. Deliverables represent the results of tasks.

WP0: Project Management (coordinator: ISTC-CNR)

This task will include:

- The overall coordination and overseeing of the project activities;
- The organization of periodic project meetings;
- The organization of an international scientific event towards the end of the project;
- The preparation of annual project reports;
- The coordination of dissemination activities;
- The development of a strategy for the exploitation of results and the protection of intellectual rights;
- The financial management, including the transfer of money to the partners
- The communications with the funding agency (PAT).

WP1: Ontology (coordinator: ISTC-CNR, participants: IRIT, UNITN)

T1.1 Analysis of the problem of modeling organizations and security

D1.1 *Organizations modeling roadmap*: a report on the current state of the art and a roadmap of major ontological choices in organization modeling.

D1.2 *Security modeling roadmap*: a report on the current state of the art and a roadmap of major ontological choices in security modeling.

T1.2 Definition of basic ontological primitives for modeling organizational and security concepts; characterization of their intended semantics by means of an axiomatic theory (the *Organizations Security Ontology*).

D1.3 *Ontology of organizations and security (preliminary)*: a preliminary version of the language and the axiomatic theory

D1.4 *Ontology of organizations and security (final)*: the final version of the language and the axiomatic theory

WP2: Reasoning (coordinator: IRIT, participants: ISTC-CNR)

T2.1 Analysis of the problem of reasoning about security.

D2.5 *Security reasoning roadmap*: a report on the current state of the art and a roadmap of major problems in reasoning about security.

D2.6 Logical framework for reasoning about security.

T2.2 Design and development of specific algorithms for reasoning about security.

D2.7 Specification and evaluation of the basic algorithms for security analysis.

D2.8 Final demo showing how the reasoning techniques can be used in concrete cases, with specific reference the case study defined in WP5.

WP3. Methodology (coordinator: UNITN, participants: ISTC-CNR)

T3.1 *Organization analysis:* Definition of a methodology for analyzing the security aspects of an organization in terms of the social relations between its relevant actors.

D3.9 A document with the specification of the general procedures for organization analysis.

D3.10 A document with the specification of the specific procedures for organization security analysis

T3.2 *System requirements analysis:* Definition of a methodology for specifying and analyzing the security requirements of the system-to-be, relating them to the goals of the stakeholders and their dependencies with the system.

D3.11 A document with the specification of the basic procedures for analyzing the system-to-be.

D3.12 A document with the specification of the basic procedures for system security analysis

T3.3 Definition of the whole methodology where all the processes of the different phases are combined

D3.13 A document with the specification of the whole methodology

WP4. Case study (coordinator: UNITN, participants: UNITN, ISTC-CNR)

T4.1 Further definition of a case study proposed by Informatica Trentina (secure electronic payment services)

D4.14 A document with the description of the case study.

T4.2 Application of the methodology to the case study

D4.15 Detailed application of the methodology

D4.16 Final evaluation

10f. Gantt Chart

	Month 6	Month 12	Month 18	Month 24	Month 30	Month 36
WP0	CNR					
WP1	CNR, IRIT, UNITN					
T1.1	D1.1,D.1.2					
T1.2		D1.3			D1.4	
WP2	IRIT, CNR					
T2.1	D2.5		D2.6			
T2.2				D2.7	D2.8	
WP3	UNITN, CNR					
T3.1		D3.9	D3.10			
T3.2			D3.11	D3.12		
T3.3					D3.13	
Wp4		UNITN, CNR				
T4.1			D4.14			
T4.2						D4.15, D4.16

The diagram above illustrates the main milestones, the related deadlines for the deliverables for each task.

The human effort is described in more detail in Section 14.

11. Resources available

ISTC-CNR/LOA, UNITN/DIT and IRIT laboratories are already equipped with several workstations. An adequate number of workstations (mainly Macinthoshs and Pentium-based Linux/MS-windows machines) is available to the current researchers, although new workstations are required for the additional people that will be involved in the project. The workstations are connected in a 100/1000 MBit LAN, 11 MBit WiFi, and 4 MBit WAN.

12. References

1. Anderson R., "Security Engineering: A Guide to Building Dependable Distributed Systems", Wiley Computer Publishing, 2001
2. Botazzi, E., Organizzazioni e realtà sociale: alcuni aspetti ontologici, Laurea di filosofia, Università di Ferrara, 2003.
3. Carmo, J. and Jones, A. J.I. Deontic logic and contrary-to-duties. In Gabbay, Dov M. and Günthner, Franz, Handbook of Philosophical Logic (2nd Edition), vol. 8, Handbook of Philosophical Logic, Kluwer Academic Publishers, 2002.
4. Castilho M. A., O. Gasquet, and A. Herzig. Formalizing action and change in modal logic I: the frame problem. *Journal of Logic and Computation*, 9(5):701-735, 1999.
5. Chung L., and B. Nixon, "Dealing with Non-Functional Requirements: Three Experimental Studies of a Process-Oriented Approach", Proceedings of the 17th International Conference on Software Engineering, Seattle- USA, 1995
6. Cohen, P. R. and Levesque, H. J. Intention is choice with commitment. *Artificial Intelligence* , 42:213-261, 1990a.
7. Cohen, P. R. and Levesque, H. J. Rational interaction as the basis for communication. In Cohen, P. R., Morgan, J., and Pollack, M. E., editors, *Intentions in Communication* , pages 221-256. The MIT Press: Cambridge, MA, 1990b.
8. Colombetti M. Semantic, Normative and Practical Aspects of Agent Communication. Issues in Agent Communication, pp.17-30, 2000.
9. Conte R. and Castelfranchi C. *Cognitive and social action* . Londra: London University College of London Press, 1995
10. Dardenne A., A. Van Lamsweerde and S. Fickas, "Goal-directed Requirements Acquisition. Science of Computer Programming", *Special issue on 6th Int. Workshop of Software Specification and Design*, 1991.
11. Fagin, R., Halpern, J. Y. , Moses, Y. and Vardi, M. Y. Reasoning about knowledge, MIT Press, 1995.
12. Falcone R. and Castelfranchi C. Issue of Trust and Control on Agent Autonomy. *Connection Science, Vol. 14, N°4,* pp.249-263, 2002.
13. Falcone R. and Castelfranchi C. Social Trust: A Cognitive Approach. In Castelfranchi C., Tan Y.H. (Ed.), *Trust and Deception in Virtual Societies* (pp. 55-90). Kluwer Academic Publishers, 2001.
14. Fariñas del Cerro L., D. Fauthoux, Olivier Gasquet, Andreas Herzig, Dominique Longin, and Fabio Massacci. Lotrec: the generic tableau prover for modal and description logics. In *Proc. Int. Joint Conf. on Automated Reasoning (IJCAR'01)*, number 2083 in LNAI, pages 453-458, Siena, Italie, 18-23 juin 2001. Springer Verlag.
15. Finin, T., and Anupam, J. 2002. Agents, Trust, and Information Access on the Semantic Web. ACM SIGMOD, December 2002.
16. Fuxman, L. Liu, M. Pistore, M. Roveri and J. Mylopoulos. "Specifying and Analyzing Early Requirements: Some Experimental Results" Accepted for publication in RE-2003, the 11th IEE International Requirements Engineering Conference, 8th-12th September 2003, Monterey Bay, California U.S.A.
17. Geer, D., Jr.; Hoo, K.S.; Jaquith, A.; Information security: why the future belongs to the quants, Security & Privacy Magazine, IEEE , Volume: 1 Issue: 4 , July-Aug. 2003, pp. 24 - 32.
18. Giorgini P., F. Massacci, and J. Mylopoulos. Requirement Engineering meets Security: A Case Study on Modelling Secure Electronic Transactions by VISA and Mastercard, in Proceedings of the 22nd International Conference on Conceptual Modeling, LNCS, Springer, 2003.
19. Herzig A. and D. Longin. Belief dynamics in cooperative dialogues. *J. of Semantics*, 17(2), 2000.

20. Herzig A. and D. Longin. A logic of intention with cooperation principles and with assertive speech acts as communication primitives. In C. Castelfranchi and W. Lewis Johnson, editors, *Proc. 1st Int. Joint Conf. on Autonomous Agent and Multi-Agent System (AAMAS 2002)*, pages 920-927, Bologna, 2002. ACM Press.
21. Jézéquel J.-M., H. Hußmann, and S. Cook, editors. SecureUML: A UML-Based Modeling Language for Model-Driven Security, volume 2460 of Lecture Notes in Computer Science. Springer, 2002.
22. Jurjens J. Modelling audit security for smart-card payment schemes with UMLsec. In 16th International Conference on Information Security (IFIP/SEC 2001). Kluwer AP, 2001.
23. Jurjens J. Towards secure systems development with umlsec. In Fundamental Approaches to Software Engineering (FASE/ETAPS 2001), LNCS. Springer-Verlag, 2001.
24. Jurjens J. Using UMLsec and Goal-Trees for secure systems development. In Symposium of Applied Computing (SAC 2002). ACM Press, 2002.
25. Lampson B., "Computer Security in the real world", *Annual Computer Security Applications Conference,* 2000.
26. Liu L., E. Yu, and J. Mylopoulos. Analyzing Security Requirements as Relationships Among Strategic Actors. In Proceedings of the 2nd Symposium on Requirements Engineering for Information Security (SREIS-02), Raleigh, North Carolina, 2002.
27. Lodderstedt T., D. A. Basin, and J. Doser. Model driven security for process-oriented systems. In 8th ACM Symposium on Access Control Models and Technologies, 2003.
28. McDermott J. and C. Fox, "Using Abuse Care Models for Security Requirements Analysis", Proceedings of the 15th Annual Computer Security Applications Conference, December 1999.
29. Mouratidis H., P. Giorgini, and G. Manson. Integrating security and systems engineering: Towards the modelling of secure information systems. In Proceedings of the 15th Conference On Advanced Information Systems Engineering (CAiSE 2003), 2003.
30. Mouratidis H., P. Giorgini, and G. Manson. Modelling secure multiagent systems. In Proceedings of the 2nd International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS), 2003.
31. Sommerville I., "Software Engineering", sixth edition, Addison-Wesley, 2001
32. Stallings W., "Cryptography and Network Security: Principles and Practice", Second Edition, Prentice-Hall 1999.
33. Traum, D. R., and Allen, J. F. 1994. Discourse obligations in dialogue processing. In Proceedings of the 32 th Annual Meeting of the Association for Computational Linguistics, 1--8.
34. Tryfonas T., E. Kiountouzis and A. Poulymenakou. "Embedding security practices in contemporary information systems development approaches", Information Management & Computer Security, Vol 9 Issue 4, 2001, pp 183-197
35. Yu E. and L. Cysneiros. Designing for Privacy and Other Competing Requirements. In Proceedings of the 2nd Symposium on Requirements Engineering for Information Security (SREIS-02), Raleigh, North Carolina, 2002.

13. Description of research units

13.1. ISTC-CNR

Institution

Istituto di Scienze e Tecnologie della Cognizione del CNR (ISTC-CNR), Laboratorio di Ontologia Applicata (LOA)

Nicola Guarino (senior researcher)	8 p.m.
Claudio Masolo (researcher)	9 p.m.
Aldo Gangemi (researcher)	9 p.m.
Rino Falcone (researcher)	1 p.m.

Role

Project coordinator; expert in ontological analysis, conceptual modeling, and logical axiomatization

Description

The Institute of Cognitive Sciences and Technologies is a new institute coming from the recent restructuring of the Italian National Research Council, the major Italian network of public research. It is a highly interdisciplinary institute, with research activities on areas as diverse as natural language, cognitive development, mental models, education, cognitive simulation, emotions, knowledge engineering. The institute has three locations: Rome, Padova, and Trento. The Laboratory for Applied Ontology has been recently established in Trento (with a branch in Rome), and results from the merging of two previous groups working on ontologies in different CNR institutes: the former LADSEB-CNR and the former ITBM-CNR. The two groups have been working together in the ontology fields for more than ten years, with a strongly interdisciplinary approach that combines together Computer Science, Philosophy, and Linguistics, and relies on Logic as a unifying paradigm. They have played a leading role in promoting a well-founded ontological approach within the Computer Science community, as testified by the successful series of conferences on Formal Ontology in Information Systems (FOIS), a number of special issues on international journals, and a series of invited talks and tutorials in different communities. LOA is currently involved in various ontology-related projects, such as WonderWeb (development of a library of foundational ontologies), OntoWeb (harmonization of content standards, legal ontologies), a large EUREKA project on ontology-driven Information and Knowledge Fusion (IKF), an Italian project on the Ontology of Social Interaction (TICCA), and a FAO project on semantic interoperability of legacy systems and terminologies for food and agriculture (FOS – Fishery Ontology Service). Strong cooperation relationships exist with various research institutes, in particular with IRIT-CNRS, the University of Trento and with ITC-IRST in Trento.

Principal investigator: Nicola Guarino

Nicola Guarino (1954) is a senior research scientist at ISTC-CNR, where he leads the Laboratory for Applied Ontology. He graduated in Electrical Engineering at the University of Padova in 1978. In 1979–1984 he was responsible of the data acquisition and monitoring system of a large nuclear fusion experiment. He then joined LADSEB-CNR to work on knowledge representation issues, and recently moved to ISTC-CNR. He has been active in the ontology field since 1991, and has played a leading role in the AI community in promoting the study of ontological foundations of knowledge engineering and conceptual modelling. His current research activities regard ontology design and ontology-driven conceptual modelling. He is general chair of the conference series on “Formal

Ontology in Information Systems" (FOIS), and associate editor of the Journal of Data Semantics, the International Journal of Human-Computer Studies, and the Semantic Web area of the Electronic Transactions on Artificial Intelligence. He has published about 80 research papers, and has been guest editor of several special issues on international journals related to formal ontology and information systems.

Nicola Guarino's publications

Guarino, N. (guest ed.), *Data and Knowledge Engineering (special issue on Formal Ontology and Conceptual Modelling)*, **31**(2), 1999

Guarino, N. The Role of Identity Conditions in Ontology Design. In C. Freksa and D. M. Mark (eds.), *Spatial Information Theory - Cognitive and Computational Foundations of Geographic Information Science*. Proceedings of International Conference COSIT '99. Springer Verlag, Berlin, 1999, p. 221-234.

Guarino, N., Masolo, C., and Vetere, G. OntoSeek: Content-Based Access to the Web. *IEEE Intelligent Systems*, **14**(3), 1999, p. 70-80.

Guarino, N. 1999. Panini al prosciutto e altri trabocchetti ontologici. Commenti all'articolo di Casati e Varzi "I trabocchetti della rappresentazione spaziale". *Sistemi Intelligenti*, **11**(1): 42-53.

Guarino N., Welty, C. Towards a methodology for ontology-based model engineering. In Bezivin, J. and Ernst, J., eds, *Proceedings of the ECOOP-2000 Workshop on Model Engineering*, June, 2000.

Guarino N., Welty, C. Identity, Unity, and Individuation: Towards a Formal Toolkit for Ontological Analysis**.** In W. Horn, ed., *Proceedings of ECAI-2000: The European Conference on Artificial Intelligence*. IOS Press, Amsterdam. August, 2000.

Guarino N., Welty, C. Ontological analysis of taxonomic relationships. In *Proceedings of 19th International Conference on Conceptual Modeling (ER2000)*. October 9-12, 2000, Salt Lake City, USA

Gangemi, A., Guarino, N., and Oltramari, A. 2001. Conceptual Analysis of Lexical Taxonomies: The Case of WordNet Top-Level. In C. Welty and S. Barry (eds.), *Formal Ontology in Information Systems. Proceedings of FOIS2001*. ACM Press: 285-296.

Guarino, N. 2001. Review of John Sowa's "Knowledge Representation: Logical, Philosophical, and Computational Foundations". *AI Magazine*, **22**(3): 123-125.

Schulten, E., Akkermans, H., Guarino, N., and Doerr, M. 2001. The eCommerce Product Classification Challenge. *IEEE Intelligent Systems*(August): 86-89.

Welty, C. and Guarino, N. 2001. Supporting Ontological Analysis of Taxonomic Relationships. *Data and Knowledge Engineering*, **39**(1): 51-74.

Guarino, N. and Welty, C. 2001. Evaluating Ontological Decisions with OntoClean. *Communications of the ACM* **45**(2): 61-65

Guarino, N. and Welty, C. 2002. Identity and subsumption. In R. Green, C. Bean and S. Myaeng (eds.), *The Semantics of Relationships: an Interdisciplinary Perspective*. Kluwer:111-126.

Gangemi, A., Guarino, N., Masolo, C., and Oltramari, A. 2002. Restructuring Wordnet's top-level. *AI Magazine, fall 2003* (in press)

Guarino, N., and Welty, C. 2003. An overview of OntoClean. In R. Studer and S. Staab (eds.), *Handbook of Ontologies in Information Systems*, Springer Verlag (in press).

Masolo, C., Oltramari, A., Gangemi, A., Guarino, N., Vieu, L. 2003. La prospettiva dell'ontologia applicata. To appear on *Rivista di Estetica*.

Oltramari, A., Borgo, S., Catenacci, C., Ferrario, R., Gangemi, A., Guarino, N., Masolo, C., Pisanelli, D. 2003. Negoziati di significato. To appear on *Sistemi Intelligenti*.

Further LOA Team's publications

Gangemi, A., Navigli R., Velardi P. (2003). *The OntoWordNet Project: extension and axiomatisation of conceptual relations in WordNet.* Accepted at the International Conference on Ontologies, Database and Applications of Semantics (ODBASE 2003), 3-7 November 2003, Catania, Sicily (Italy).

Gangemi, A., Mika, P. (2003). *Understanding the Semantic Web thorugh Descriptions and Situations.* Accepted at the International Conference on Ontologies, Database and Applications of

Gangemi, A., Prisco A., Sagri M.T., Steve, G., Tiscornia, D. (2003). *Some ontological tools to support legal regulatory compliance, with case study.* Accepted at the Workshop on Regulatory Ontologies and the Modeling of Complaint Regulations (WORM CoRE 2003). Part of the International Federated Conferences (OTM '03). Proceedings published by Springer LNCS, November 4, 2003, Catania, Sicily, Italy.

Gangemi, A., Navigli R., Velardi P. (2003). *Axiomatizing WordNet Glosses in the OntoWordNet Project.* Accepted at the Workshop on Human Language Technology for the Semantic Web and Web Services, 2nd International Semantic Web Conference (ISWC 2003). Sanibel Island, Florida, 20-23 October 2003.

Gangemi, A, Sagri M.T., Tiscornia, D. (2003). *Metadata for Content Description in Legal Information*. Workshop on Legal Ontologies, 9th International Conference on Artificial Intelligence and Law (ICAIL-2003), June 24-28, 2003, Edinburgh, UK.

Borgo, S., (2003). *Concurrency with Partial Information.* In Proceedings of the 2003 International Conference on Computational Intelligence For Modelling, Control & Automation (CIMCA '03), M. Mohammadian Editor.

Borgo, S. (2003). *Communicating Agents. In Proceedings of the International Conference.* CEEMAS 2003, LNAI 2691.

13.2. UNITN

Institution

Department of Information and communication Technology, University of Trento (UNITN/DIT)

Fabio Massacci (associate professor)	9 p.m.
M. Pistore (assistant professor)	4 p.m.
Paolo Giorgini (researcher)	9 p.m.
Y. Thang (PhD Student)	22 p.m.

Role

Expert in requirements engineering and conceptual modeling, with specific reference to security aspects

Description

The Department of Information and Communication Technology (DIT) was established at the University of Trento on January 1, 2002. It represents the point of aggregation of the skills on information and communication technology and intend to provide a dynamic and qualified response to the ever-increasing demand of such competences from the productive tissue at local, national or international level.

University departments are historically structures of remarkable importance for the increase of knowledge and for the technological transfer. In this context, the DIT is an innovative and promising organization in the Italian academic system. DIT is intended to be an organization:

- with a strong characterization on its core disciplines and high interdisciplinarity;
- with a leadership position in the field of services;
- of international excellence.

These targets can be achieved since people working at DIT are able to exploit the different skills of several research groups operating on various disciplines (computer science, telecommunications and electronics), traditionally connected to different scientific communities.

On the other hand, due to the wide range of knowledge provided by the different research groups, DIT can be thought as an important structure for the development and modernization of the traditional scientific disciplines. Such an interdisciplinary support is completed by a leading action in terms of services and of knowledge "management" in order to propose a national and international efficient model of technological transfer. The Department aims at being a model of integrated scientific innovation able to cope with the increasing demand of the so-called information technology society. Such a role requires excellence in both scientific research (papers) and its practical exploitation (industrial projects). In the starting phase such requirements have been reached thanks to a staff of 20 professors and researchers (affiliated to several Faculties of the University of Trento) able to collect, from a financial point of view, approximately 2.5 million Euros and to publish approximately 150 papers per year on relevant international scientific journals.

Co-Principal investigator: Fabio Massacci

Fabio Massacci received a M.Eng. in 1993 and Ph.D. in Computer Science and Engineering at University of Rome "La Sapienza" in 1998. He visited Cambridge University in 1996-1997. He joined University of Siena as Assistant Professor in 1999 and was visiting researcher at IRIT Toulouse in 2000. He won 5 CNR scholarships (three for abroad). In 2001 he received the Intelligenza Artificiale award, a young researchers career award from the Italian Association for Artificial Intelligence. In 2001 he joined the University of Trento as Associate Professor. He is member of AAAI, ACM, IEEE Computer society and a chartered engineer since 9 years.
Fabio Massacci is or has been in the Program Committee of CSFW-15, CADE-02,03, TABLEAUX-00,02,03, AAAI-02, has been conference chair for the Internat. Joint Conference on Automated Reasoning (CADE, TABLEAUX, FTP) in 2001 and is now in the steering committee of the conference. Has been invited speaker at the security session of MFPS-00 (chair Catherine Meadows NRL) on Logical Cryptanalysis of RSAand a joint invited speaker at VERIFY and FCS (Foundations of Computer Security) at FLOC-02 on Verifying Secure Electronic TRansactions by Visa and MasterCard ed has kept an invited tutorial su Automated Reasoning and the Verification of Security Protocols at TABLEAUX-99, IJCAI-03 and at the International School on Foundations of Security Analysis and Design FOSAD-2000.
His current research interests are in automated reasoning for computer security. He has worked on automated deduction for modal and dynamic logics and their application to access control. In 1999 he worked on the encoding of cryptographic algorithms (DES, RSA, etc) into satisfiability problem for verification and cryptanalysis. His interest in security protocol verification dates back to 1997 when he proposed to model protocol attacks as a planning problem.
Now he is chairman of the 10MEuro/year Computing and Telecom Services of the University of Trento (ERP, Net, phone and all the other ICT services) in whose capacity he has learned that an organizationally and financially sound solution is as important as the technical solution and that enforcing practical security may have unexpected subtle financial implications.

Fabio Massacci's publications

G. De Giacomo and F. Massacci. Combining deduction and model checking into tableaux and algorithms for Converse-PDL. Information and Computation, 162:117-137, 2000. Accepted in 1997.

F. M. Donini and F. Massacci. EXPTIME tableaux for ALC. Artificial Intelligence, 124(1):87-138, 2000.

F. Massacci. Tableaux methods for formal verification in multi-agent distributed systems. J. of Logic and Computation, 8(3):373-400, 1998.

F. Massacci. The complexity of analytic and clausal tableaux. Theoretical Computer Science, 243(1):477-487, 2000.

F. Massacci. Single step tableaux for modal logics: methodology, computations, algorithms. J. of Automated Reasoning, 24(3):319-364, 2000.

F. Massacci. Decision procedures for expressive description logics with intersection, composition, converse of roles and role identity. In B. Nebel, editor, Proc. of the 17th Int. Joint Conf. on Artificial Intelligence (IJCAI 2001), pages 193-198. Morgan Kaufmann, Los Altos, 2001.

C. Fiorini, E. Martinelli, and F. Massacci. How to fake an RSA signature by encoding modular root finding as a sat problem". Discrete Applied Mathematics, 2003. Accepted in 2001. Published in Italy as Technical Report at Dip. Ingegneria dell'Informazione, Siena and availabe on the preprint web server of the publisher.

F. Massacci and L. Marraro. Logical cryptanalysis as a SAT-problem: Encoding and analysis of the U.S. Data Encryption Standard. J. of Automated Reasoning, 24(1-2):165-203, 2000.

L. Carlucci Aiello and F. Massacci. Verifying security protocols as planning in logic programming. ACM Trans. on Computational Logic, 2(4):542-580, 2001.

L. Carlucci Aiello and F. Massacci. Planning attacks to security protocols: Case studies in logic programming. In A. C. Kakas and F. Sadri, editors, Computational Logic: Logic Programming and Beyond, volume 2407 of Lecture Notes in Artificial Intelligence. Springer, 2002.

G. Bella, F. Massacci, and L. C. Paulson. The verification of an industrial payment protocol: The SET purchase phase. In V. Atluri, editor, Proc. of the 9th ACM Conf. on Communications and Computer Security (CCS-2002), pages 12-20. ACM Press and Addison Wesley, 2002.

G. Bella, F. Massacci, and L. C. Paulson. Verifying the SET registration protocols. IEEE J. of Selected Areas in Communications, 21(1):77 -87, 2003.

Further UNITN Team's publications

P. Bresciani, P. Giorgini, F. Giunchiglia, J. Mylopoulos, A. Perini. TROPOS: An Agent-Oriented Software Development Methodology. Journal of Autonomous Agents and Multi-Agent Systems. 2003. Kluwer Academic Publishers, 2004.

A.F. Dragoni and P. Giorgini. Distributed Belief Revision. In Journal of Autonomous Agents and Multi-Agent Systems. Kluwer Academic Publishers, Volume 6, Number 2, pp.115-143, March 2003.

A.F. Dragoni, P. Giorgini, and L. Serafini. Mental States Recognition from Communication. In Journal of Logic and Computation, Oxford university Press, Vol 12 No. 1, 119-136, 2002.

A. Fuxman, L. Liu, J. Mylopoulos, M. Pistore, M. Roveri and P.Traverso. "Specifying and Analyzing Early Requirements" Accepted for publication in the Requirements Engineering Journal. To appear.

A. Cimatti, M. Pistore, M. Roveri and P. Traverso "Weak, Strong, and Strong Cyclic Planning via Symbolic Model Checking". In Artificial Intelligence (AIJ). 147(1,2)2003, 35--84. Elsevier.

13.3. IRIT

Institution

Institut de recherche en informatique de Toulouse

Andreas Herzig (CNRS researcher)	6 p.m.
Laure Vieu (CNRS researcher)	9 p.m.
Olivier Gasquet (UPS Associate Professor)	3 p.m.
Dominique Longin (CNRS researcher)	3 p.m.
Marc Pauly (CNRS researcher)	1 p.m.
Mohammad Sahade (PhD student)	12 p.m.

Role

Expert in ontology, logics of interaction and reasoning.

Description

IRIT is one of the biggest computer science research institutes in France (about 300 researchers), affiliated with the National Research Council (CNRS), the Paul Sabatier University in Toulouse (UPS), and the National Polytechnics Institute (INP). There are two research groups working in knowledge representation and reasoning : Plausible Reasoning, Decision, and Proof Methods (RPDMP, lead by Didier Dubois, Henri Prade and Claudette Cayrol) and Logic, Interaction, Language, and Computation (LILaC, lead by Andreas Herzig). While the former mainly investigates theories of uncertainty, the latter focusses on formalization of reasoning in logic.
LILaC investigates logical models of interaction following two lines of research.
The first line focuses on logics for reasoning about knowledge, belief, time, actions and obligations (A. Herzig, Ph. Balbiani, O. Gasquet, D. Longin, M. Pauly). There, the integration of logics of belief with speech act theory and theories of action is currently investigated, together with its application to the formalization of services on the web. LILaC has expertise concerning the development of automated theorem proving methods for the resulting logics (in particular modal and description logics), and has implemented a generic theorem prover (Lotrec).
A second line focusses on modelling the structure of interaction (F. Evrard, P. Muller, L. Vieu). Here, LILaC has expertise on discourse representation theory (DRT), its segmented version (S-DRT), as well as on the theory of dialogue games. In particular it is currently investigated how S-DRT and dialogue game theory can be combined in a fruitful way.
LILaC is involved in several national projects, in particular those of the "Cognitique" program and the CNRS program "knowledge, learning and new technologies of information and communication" (TCAN).

Co-Principal investigator: Andreas Herzig

Andreas Herzig (1960) studied computer science in Darmstadt and Toulouse. In 1989 he obtained a Ph.D. in Computer Science at Paul Sabatier University in Toulouse on Automated Deduction in Modal Logics. Since 1990 he is a CNRS researcher.
He is Executive Editor of the Journal Applied non Classical Logics, and member of the Editorial Board of the Electronic Transactions on Artificial Intelligence.
He has participated in several Esprit project (ALPES, Basic Research Actions MEDLAR1, MEDLAR2, and DRUMS2). He co-edited a book on Conditional Logics, and co-authored a chapter in the Handbook of Logic in Artificial Intelligence and Logic Programming. He has published about 60 scientific papers in journals (Artificial Intelligence, J. of Semantics, J. of Logic

and Computation, Int. Journal of Intelligent Systems and others) and conferences (IJCAI, ECAI, CADE, KR, UAI and others).
His main research topic is the investigation of logical models of interaction, with a focus on logics for reasoning about knowledge, belief, time, actions and obligations and the development of theorem proving methods for them. He currently investigates the integration of logics of belief with speech act theory and theories of action.

Andreas Herzig's publications

Samir Chopra and Andreas Herzig, editors. Belief Change: Theory and Practice. J. of Applied Non-Classical Logics (JANCL), 11(1/2), 2001.

Andreas Herzig, Brahim Chaib-Draa, and Philippe Mathieu. Modèles formels de l'interaction - actes des secondes journées francophones (MFI'03), Cépaduès-Editions, Toulouse, may 2003.

Marcos A. Castilho, Olivier Gasquet, and Andreas Herzig. Formalizing action and change in modal logic I: the frame problem. Journal of Logic and Computation, 9(5):701-735, 1999.

Andreas Herzig and Omar Rifi. Propositional belief base update and minimal change. Artificial Intelligence, 115(1):107-138, November 1999.

Andreas Herzig and Dominique Longin. Belief dynamics in cooperative dialogues. J. of Semantics, 17(2), 2000. (vol. published in 2002.)

Maud Champagne, Andreas Herzig, Dominique Longin, Jean-Luc Nespoulous, and Jacques Virbel. Formalisation pluridisciplinaire de l'inférence d'actes de langage non littéraux. Revue i3, 2002. 1er hors série, eds. B. Chaib-draa, B. and R. Demolombe, 2002 (selected papers of MFI'01).

Andreas Herzig. Logics for belief base updating. In Didier Dubois and Henri Prade, editors, Handbook of defeasible reasoning and uncertainty management, volume `Belief change'. Kluwer Academic Publishers, 1998.

Didier Dubois, Luis Fariñas del Cerro, Andreas Herzig, and Henri Prade. A roadmap of qualitative independence. In Didier Dubois, Henri Prade, and Erich P. Klement, editors, Fuzzy Sets, Logics and Reasoning About Knowledge, volume 15 of Applied Logic Series, pages 325-350. Kluwer Academic Publishers, 1999.

Marcos Castilho, Andreas Herzig, and Camilla Schwind. Raisonnement sur les actions: les approches basées sur la causalité et la dépendance. In Le temps, l'espace et l'évolutif en Sciences du Traitement de l'information. Cépaduès-Editions, September 2000.

Andreas Herzig and Gabriella Crocco. Les opérations de changement basées sur le test de Ramsey. In Pierre Livet, editor, Révision des croyances, pages 21-41. Hermès, 2002.

Andreas Herzig and Omar Rifi. Update operations: a review. In Henri Prade, editor, Proc. Eur. Conf. on Artificial Intelligence (ECAI'98), pages 13-17. John Wiley & Sons, Ltd., August 1998.

Luis Fariñas del Cerro, Andreas Herzig, Dominique Longin, and Omar Rifi. Belief reconstruction in cooperative dialogues. In Fausto Giunchiglia, editor, Proc. 8th Int. Conf. on Artificial Intelligence: Methods, Systems, Applications (AIMSA'98), LNAI. Springer-Verlag, September 1998.

Andreas Herzig and Dominique Longin. Belief dynamics in cooperative dialogues. In Jan van Kuppevelt, Noor van Leusen, Robert van Rooy, and Henk Zeevat, editors, Proc. Amsterdam Workshop on the Semantics and Pragmatics of Dialogue (Amstelogue'99), 2000. 20 pages.

Andreas Herzig and Dominique Longin. A topic-based framework for rational interaction. In Actes TALN'2000, June 2000. Poster Session.

Andreas Herzig, Jérôme Lang, Dominique Longin, and Thomas Polacsek. A logic for planning under partial observability. In Proc. Nat. (US) Conf. on Artificial Intelligence (AAAI'2000), Austin, Texas, August 2000.

Andreas Herzig, Jérôme Lang, and Thomas Polacsek. A modal logic for epistemic tests. In Proc. Eur. Conf. on Artificial Intelligence (ECAI'2000), Berlin, August 2000.

Andreas Herzig, Jérôme Lang, Pierre Marquis, and Thomas Polacsek. Updates, actions, and planning. In Proc. Int. Joint Conf. on Artificial Intelligence (IJCAI'01), page 8. Morgan Kaufmann, August 2001.

Luis Fariñas del Cerro, David Fauthoux, Olivier Gasquet, Andreas Herzig, Dominique Longin, and Fabio Massacci. Lotrec: the generic tableau prover for modal and description logics. In Proc. Int. Joint Conf. on Automated Reasoning (IJCAR'01), page 453-458, Siena, Italie, 18-23 june 2001. Springer Verlag, LNCS 2083.

Laszlo Aszalos and Andreas Herzig. Reasoning about failure. In Andrea Omicini, editor, Engineering Societies in the Agents' World, 2nd Int. Workshop (ESAW'01), number 2203 in LNAI, pages 74-86. Springer Verlag, 2001.

Andreas Herzig and Dominique Longin. A logic of intention with cooperation principles and with assertive speech acts as communication primitives. In C. Castelfranchi and W. Lewis Johnson, editors, Proc. 1st Int. Joint Conf. on Autonomous Agent and Multi-Agent System (AAMAS 2002), pages 920-927, Bologna, 15-19 july 2002. ACM Press.

Andreas Herzig and Dominique Longin. Sensing and revision in a modal logic of belief and action. In Frank van Harmelen, editor, Proc. ECAI2002, pages 307-311. IOS Press, 2002.

Andreas Herzig and Dominique Longin. Intention et principes de cooperation pour le traitement des requetes et des questions fermees au travers des assertifs. In Proc. 13eme Congres Francophone AFRIF-AIFA de Reconnaissance des Formes et Intelligence Artificielle (RFIA'02), Angers, pages 221-230. AFRIF-AIFA, 8-10 january 2002.

Andreas Herzig and Dominique Longin. On modal probability and belief. In Nevin L. Zhang and Thomas D. Nielsen, editors, Proc. ECSQARU2003, pages 62-73, volume 2711 of LNAI. Springer Verlag, 2003.

Andreas Herzig, Sébastien Konieczny, and Laurent Perrussel. On iterated revision in the AGM framework. In Nevin L. Zhang and Thomas D. Nielsen, editors, Proc. ECSQARU2003, pages 477-488, volume 2711 of LNAI. Springer Verlag, 2003.

Andreas Herzig, Jérôme Lang, and Pierre Marquis. Action representation and partially observable planning using epistemic logic. In Proc. Int. Joint Conf. on Artificial Intelligence (IJCAI'03), pages 1067-1072. Morgan Kaufmann, August 2003.

Further IRIT's team publications

Marcos A. Castilho, Olivier Gasquet, and Andreas Herzig. Formalizing action and change in modal logic I: the frame problem. *Journal of Logic and Computation*, 9(5):701-735, 1999

Andreas Herzig and Omar Rifi. Propositional belief base update and minimal change. *Artificial Intelligence*, 115(1):107-138, November 1999

Luis Fariñas Del Cerro, Olivier Gasquet. *Tableaux Based Decision Procedures for Modal Logics of Confluence and Density*. In : *Fundamenta Informaticae* , V. 40 N. 4, p. 317-333, december 1999

Masolo, C. & L. Vieu (1999). Atomicity vs. Infinite Divisibility of Space. In: C. Freksa & D. Mark (eds.), *Spatial Information theory. Proc. of COSIT'99*. Berlin: Springer Verlag, LNCS n° 1661, pp. 235-250.

Andreas Herzig and Dominique Longin. Belief dynamics in cooperative dialogues. *J. of Semantics*, 17(2), 2000.

Andreas Herzig, Jérôme Lang, Pierre Marquis, and Thomas Polacsek. Updates, actions, and planning. In *Proc. Int. Joint Conf. on Artificial Intelligence (IJCAI'01)*, page 8. Morgan Kaufmann, August 2001.

Bras, M. & L. Vieu, eds. (2001). *Semantic and Pragmatic Issues in Discourse and Dialogue. Experimenting with Current Dynamic Theories* Oxford: Elsevier, Current Research in the Semantics/Pragmatics Interface (CRiSPI) n° 9.

Luis Fariñas del Cerro, David Fauthoux, Olivier Gasquet, Andreas Herzig, Dominique Longin, and Fabio Massacci. Lotrec: the generic tableau prover for modal and description logics. In: *Proc. Int. Joint Conf. on Automated Reasoning (IJCAR'01)*, page 453-458, Siena, Italy, 18-23 june 2001. Springer Verlag, LNCS 2083.

Andreas Herzig and Dominique Longin. A logic of intention with cooperation principles and with assertive speech acts as communication primitives. In C. Castelfranchi and W. Lewis Johnson, editors, *Proc. 1st Int. Joint Conf. on Autonomous Agent and Multi-Agent System (AAMAS 2002)*, pages 920-927, Bologna, 15-19 july 2002. ACM Press.

Asher, N. & L. Vieu (2003). Subordinating and Coordinating Discourse Relations. *Lingua,* to appear.

14. Budget

Due to the nature of the project, the foreseen budget is largely bound to personnel expenses. The estimate of additional person months required for each workpackage is reported in the additional table 14c below. For certain workpackages, we have also reported the name of the foreseen consultant, as discussed in Section 10d.

Table 14a

Global costs of the project in EURO, by participant institution

Expense category	ISTC-CNR	IRIT	UNITN
Personnel (1)	**300,900 + 80,000**	**84,000 + 90,000**	**166,300 + 40,000**
Equipment	**21,000**	**3,500**	**10,500**
Consumables	**15,045**	**4,200**	**8,315**
Travel subsistence	**25,000**	**19,500**	**13,000**
Specific costs (consultants, etc.)	**136,000**	**26,000**	**0**
Publications (2)	**30,500**	**7,500**	**6,000**
Personnel Training	**19,000**	**10,000**	**6,000**
Result Exploitation (3)	**20,000**	**0**	**0**
General Expenses (4)	**76,180**	**34,800**	**41,260**
Miscellaneous	**0**	**0**	**0**
Total	**643,625 + 80,000**	**189,500 + 90,000**	**251,375 + 40,000**

(1) The figures for the Personnel expense category are split into Additional Personnel expenses and Available Personnel expenses.
(2) The Publications expense category includes the organisation of a final workshop (charged to the coordinator).
(3) Result Exploitation expenses correspond to a pre-competitive study to be carried out at the end of the project (charged to the coordinator).
(4) General expenses are calculated as 20% of the sum of all personnel expenses (including available personnel expenses, charged to participant institutions).

Table 14b

Global costs of the project in EURO

Expense category	Charged to "Fondo unico"	Charged to participant institutions
Personnel	**551,200**	**210,000**
Equipment	**35,000**	
Consumables	**27,560**	
Travel and subsistence	**57,500**	
Specific costs (consultants, etc.)	**162,000**	
Publications	**44,000**	
Personnel Training	**35,000**	
Result Exploitation	**20,000**	
General Expenses	**152,240**	
Miscellaneous	**0**	
Total	**1,084,500**	**210,000**

Table 14c

Distribution of human effort (in person-months) across partners and workpackages

	Additional person-months			*Available p.m.*	*Total*	*Consultants*
	PhD students	*Post-docs*	*Analists/ assistants*			
WP0					***42***	
ISTC-CNR			*36*	*6*	*42*	
WP1					***115***	
ISTC-CNR	*36*	*36*		*12*	*84*	
IRIT	*18*			*9*	*27*	
UNITN				*6*	*6*	
WP2					***79***	***ITC-IRST*** *(ca. 15 p.m.)*
ISTC-CNR	*36*				*36*	
IRIT	*18*			*25*	*43*	
UNITN						
WP3					***111***	
ISTC-CNR	*36*			*6*	*42*	
IRIT						
UNITN	*36*	*24*		*9*	*69*	
WP4					***39***	***Informatica Trentina*** *(ca. 10 p.m.)*
ISTC-CNR		*18*		*3*	*21*	
IRIT						
UNITN			*18*		*18*	
TOTAL					***386***	

15. Yearly budget justification in EURO

Table 15a - First year (36% of human effort, all Equipment expenses)

Expense category	Charged to "Fondo unico"	Charged to participant institutions
Personnel	**198,432**	**75,600**
Equipment	**35,000**	
Consumables	**9,922**	
Travel and subsistence	**20,700**	
Specific costs (consultants, etc.)	**58,320**	
Publications	**8,640**	
Personnel Training	**12,600**	
Result Exploitation	**0**	
General Expenses (*)	**54,806**	
Miscellaneous	**0**	
Total	**398,420**	**75,600**

(*) Note: general expenses are calculated as 20% of the sum of all personnel expenses (including those charged to participant institutions)

Table 15b - Second year (38% of human effort)

Expense category	Charged to "Fondo unico"	Charged to participant institutions
Personnel	**209,456**	**79,800**
Equipment	**0**	
Consumables	**10,473**	
Travel and subsistence	**21,850**	
Specific costs (consultants, etc.)	**61,560**	
Publications	**9,120**	
Personnel Training	**13,300**	
Result Exploitation	**0**	
General Expenses	**57,851**	
Miscellaneous	**0**	
Total	**383,610**	**79,800**

Table 15c - Third year (26% of human effort, all Result Exploitation expenses, special Publication expenses for the organisation of a final workshop)

Expense category	Charged to "Fondo unico"	Charged to participant institutions
Personnel	**143,312**	**54,600**
Equipment	**0**	
Consumables	**7,166**	
Travel and subsistence	**14,950**	
Specific costs (consultants, etc.)	**42,120**	
Publications	**26,240**	
Personnel Training	**9,100**	
Result Exploitation	**20,000**	
General Expenses	**39,582**	
Miscellaneous	**0**	
Total	**302,470**	**54,600**