INFORMATION SOCIETY TECHNOLOGIES
(IST)
PROGRAMME

contract for:

FET Open Assessment Project

Annex 1 - Description of Work

Project acronym: AVISS
Project full title: Automated Verification of Infinite State Systems
Proposal no: IST-2000-26410
Related to other Contract no.:

Date of preparation of Annex 1: December 1, 2000

Operative commencement date of contract:

Contents

1 Project summary

1.1 Objectives

This 1 year assessment project aims at laying the foundations of a new generation of verification tools for automatic error detection for e-commerce and related security protocols. To assess the potential of this technology, we will develop a prototype verification tool incorporating inference engines based on three promising automated deduction techniques: on-the-fly model-checking based on lazy data-types, theorem-proving with constraints, and model-checking based on propositional satisfiability checking. The assessment consists of two phases: a development phase aimed at the design and implementation of a prototype verification tool, and an analysis phase, in which the tool (and the techniques) will be tested and evaluated against a corpus of 50 security protocol verification problems. This will pave the way to turning the prototype into a mature technology, whose application in the industrial setting will be ascertained in a follow-up, full RTD project with industry involvement.

1.2 Description of the work

The project consists of two main tasks.

- To define a high-level language for specifying protocols, and design and implement a translator from protocol descriptions to a standard declarative format.

- To develop and test a technology for infinite state space exploration adapted to protocol verification based on three techniques operating on the translator's output. The first technique, on-the-fly model-checking, uses lazy data-types and specialized algorithms that can automatically handle infinite state spaces. The second technique, theorem-proving with constraints, provides an efficient way of representing an infinite state space using a constraint store. Additionally, it offers advantages in checking timing and freshness properties, which are crucial for security protocols. In both these techniques, flaws are detected by efficient pattern matching on traces. Often infinite state spaces can be iteratively approximated by large finite states spaces. The third technique will employ model-checking techniques based on propositional satisfiability checking to reason about these approximations.

  Although each technique can work independently, they will be integrated into a single prototype verification tool where they will interact and benefit from each other's strengths. This will require foundational research in the scope and limitations of our symbolic reasoning techniques (completeness of simplifications, complexity, expressiveness) as well as advances in integrating cooperating semi-decision procedures.

In parallel to the above activities, collaboration with industrial partners will be initiated in order to identify a set of representative case studies coming from the industrial practice on which to apply the results of the project.

1.3 Milestones and expected results

The 1 year assessment will identify key problems and the potential of our verification techniques on e-commerce security protocols; we will also begin collaboration with industry.

1. We shall define our protocol specification language, the verifier input language, and we shall implement the translator.

2. We shall develop and tune of a set of techniques for exploring the protocol state space.

3. We shall integrate the techniques defined above in a prototype verification tool.

4. The last phase of the project will be dedicated to experimentation and evaluation on a publicly available corpus of state-of-the-art protocols.

2 Project objectives

The project aims at designing a push-button technology, based on automated deduction, for error detection for a large class of infinite state systems with particular application to e-commerce and related security protocols. If successful, the technology will pave the way to the construction of industrial-strength protocol verification tools which will reduce time-to-market and increase confidence on applications, thereby improving the competitiveness of the European e-commerce industry.

During the 1 year FET assessment project, we will assess the potential and lay the foundations of the proposed technology by developing a prototype verification tool based on three promising automated deduction techniques: on-the-fly model-checking based on lazy data-types, theorem-proving with constraints, and model-checking based on propositional satisfiability checking. Given a protocol verification problem in a high-level specification language (for instance a description of a protocol together with a security property to check), the tool will first translate the problem description into a logical formalization, which will be then processed by inference engines implementing the selected automated deduction techniques. Whenever the input protocol is flawed and when the analysis carried out by the tool completes successfully, the tool will return an execution trace witnessing an attack on the protocol.

The success criteria are the following:

Coverage: the number of protocols, security properties, and types of security threats that can be specified in the tool's input specification language.

Effectiveness: the number of insecure protocols detected as flawed and the number of different types of attacks to the insecure protocols detected.

Performance: the time spent by the tool to detect errors in the protocols.

In the industrial setting, no fully automated tool is available for error detection in security protocols. For instance, the french company Trusted Logic, one of the leading companies in the area of embedded software with high security requirements, is using the COQ proof-assistant, which is an interactive tool and therefore requires user-guidance and expertise. In the academic setting, only 2 projects can be compared to ours: Casper [36], developed at the University of Leicester (UK), and CAPSL [21], developed at SRI Palo Alto (USA).

Casper is a compiler that maps a protocol specification into a process algebra (CSP). The approach is oriented towards finite-state verification by model-checking with FDR [39], and the system has been applied successfully to a library of protocols described in [22],

which includes well-known and important real-life security protocols such as the Needham-Schroeder Public Key Protocol and the Otway-Rees Protocol. Our verification techniques, based on theorem proving methods, will however handle infinite states models, and will thus allow us to relax many of the strong assumptions for bounding information (necessary to get a finite number of states) in model checking.

CAPSL is a specification language for authentication protocols. There exists a compiler [25] from CAPSL to an intermediate formalism CIL, which may be converted to an input for automated verification tools, but only a translator into an interpreter to the rewriting logic based specification language Maude seems to be available, and compiling of goals (security properties) and intruders is not available. Up to now, CAPSL-Maude has been tested only on the Needham-Schroeder Public Key Protocol protocol.

In order to measure the success of the project, the tool developed by the partners will be thoroughly tested against a corpus of security protocols which will comprise the 50 security protocols described in [22]. The choice of this corpus will allow us also to draw a detailed comparison with Casper and CAPSL-Maude.

More concretely, this assessment project will be successful if the prototype verification tool achieves the following results.

Coverage: at least 80% of the protocols in the corpus should be specifiable in the tool's input specification language.

Effectiveness: the tool should detect attacks in at least 70% of the protocols in the corpus known to be insecure.

Performance: the tool should process at least 70% of the protocols in the corpus in less than 1 hour of CPU time on standard commercially available computers.

The success will give a strong indication that the proposed techniques are ready to be turned into a mature technology whose application in the industrial setting will be ascertained via a follow-up full RTD project. Deutsche Telekom, France Télécom, and GEMPLUS have expressed their interest in partaking in such a project if the assessment phase is positive.

3　List of participants

List of Participants						
Role	Number	Part. name	Part. short name	Country	Date enter	Date exit
CO (C)	1	Albert-Ludwigs-Universität Freiburg	ALUFR	DE	Start of project	End of project
CR (P)	2	Università di Genova	UNIGE	IT	Start of project	End of project
CR (P)	3	Institut National de Recherche en Informatique et Automatique	INRIA	F	Start of project	End of project

4   Contribution to programme/key action objectives

The project fits the FET OPEN scheme, as it will contribute to the development of trust and confidence in telecommunications applications and services, which is one of the priorities of the IST 2000 Workprogramme (Research Programme 1.1.2 IST, Thematic priorities VI.1.1).

5   Innovation

Experience over the last twenty years has shown that, even assuming perfect cryptography, the design of protocols for secure electronic transactions is highly error-prone and that conventional validation techniques based on informal arguments and/or testing are not up to the task. It is now widely recognized that only verification tools based on formal methods can provide the level of assurance required. However most of the existing tools are based on either interactive verification or automatic finite-state model-checking. The interactive tools require a considerable investment of time by expert users and provide no support for error detection when the protocols are flawed. The automatic tools generally require strong assumptions that bound the information analyzed, so that an infinite-state system can be approximated by a finite-state one. Moreover, the current level of automated support scales poorly and is insufficient for the validation of realistic protocols. Finally, tuning the specification (such as building relevant approximations) and tuning the tool's parameters often requires significant expertise too.

While exploratory work has shown the potential of automated deduction techniques in this setting, most of them have never been tested on real-world problems. For this reason a FET OPEN assessment project is a necessary preliminary step before starting a wide-scale industrial involvement within a RTD project.

More concretely, the project will aim at laying the foundations of a new generation of verification tools for push-button error detection in e-commerce security protocols using a set of promising automated deduction techniques. The innovative aspects of our approach are:

- the focus on detection of errors, as opposed to certifying valid systems,

- the automatic encoding of the error-detection problem for a given protocol (for instance a description of a protocol in a standard language together with a security property to check) as the satisfiability problem in a specific logical theory,

- the proof search procedure based on appropriate advanced automated deduction techniques.

This combination has the potential to achieve a level of complete automation for the verification of important classes of infinite state protocols that is not possible with the other techniques.

6   Community added value and contribution to EU policies

The use of a multi-technology approach like ours requires a research effort with a truly European dimension: The expertise required by the AVISS project cannot be found in a

single national research group or site. Indeed, it would be very difficult to pursue the technical objectives of the proposed project without the participation of different research groups. In fact, even though the techniques to be employed in the project have a common theoretical background, their exploitation requires a considerable variety and a high degree of advanced technical and technological skills. The partners of the AVISS consortium are leading European experts in the automated deduction techniques upon which the project is based. Moreover, the partners have a common background on automated verification strengthened by a long history of international collaboration and strong bilateral relations. The AVISS consortium, therefore, collects the set of technological skills required in this assessment phase and implicitly demonstrates the need for multinational cooperation.

The presentation of the results of the project in international conferences and workshops will ensure their dissemination to the European research community and the dissemination of the results to industry will contribute to improving the competitiveness of European industry.

Moreover, the project will train young researchers in the European union on state-of-the-art techniques for reasoning about systems and protocols.

7   Contribution to Community social objectives

Electronic commerce is anticipated to revolutionize the marketplace, but its continued expansion relies on several economical and social factors that must be guaranteed by industry. One of these major enabling factors is trust: all participants must have confidence in the security of electronic transactions. Security protocols are used to ensure this: using cryptographic primitives one can exchange data in a way that should guarantee properties such as integrity of data, authentication and anonymity of participants, accountability, and non-repudiation [37, 41, 42].

The problem faced by industry is that the design and analysis of these protocols is highly error-prone. Even assuming perfect cryptography, protocols are often flawed and can potentially be exploited in ways that undermine personal privacy or are financially ruinous. Example of flaws in security or e-commerce applications are: violation of secrecy, of privacy or anonymity of participants, failure of authentication, etc. The detection of these kinds of errors is crucial from the point of view of the end-user of the services for at least two reasons:

- the users need confidence in the robustness of the services against criminal attacks,

- even under the hypothesis of a safe environment, the users desire guarantees about privacy and confidentiality concerning the information exchanged during the communications or transactions with respect to third parties involved like merchants, banks, or other authorities.

8   Economic development and S&T prospects

The proposed approach complements other approaches based on interactive verification in that one can proceed verification by a preliminary test for errors. The results of the proposed project will allow one to find errors in the early design phases of e-commerce applications, which will lead to a dramatic speed-up of the design activity, and thus reduce one of the main

obstacles to the use of formal methods in the industrial setting. This will both reduce time-to-market and increase confidence on applications, thereby giving the European e-commerce industry a leading edge over the competitors.

9 Workplan

The workplan covers one year for assessment and experiments as a preliminary step to a wide-scale industrial involvement which will take place in a follow-up RTD project.

9.1 General description

The project is aimed at assessing three promising automated deduction techniques with respect to the long-term objective of building a new generation of verification tools for automatic error detection of e-commerce and related security protocols.

The first technique, on-the-fly model-checking, uses lazy data-types and specialized algorithms that automatically handle infinite search spaces. The second technique, theorem-proving with constraints, provides an efficient way of representing an infinite state space using a constraint store; additionally, it offers advantages in checking timing and freshness properties, which are crucial for security protocols. In both these techniques, flaws are detected by efficient pattern matching on traces. Since infinite state spaces can often be iteratively approximated by large finite state spaces, the third technique will employ model-checking techniques based on propositional satisfiability checking to reason about these approximations. Here follows a brief description of the individual techniques.

On-the-fly Model-Checking. Among the most successful approaches to model-checking are so called on-the-fly approaches, where the model to be checked is constructed incrementally, on demand, during search. On-the-fly verification techniques can be used to find flaws in very large, or even infinite, state spaces. These techniques can also be effectively combined with heuristics and other search reduction techniques.

Freiburg has developed a model-checker based on on-the-fly model-checking techniques and used it to successfully find attacks in a number of security protocols. In this approach to model-checking, a protocol and an attacker model give rise to an infinite state space that formalizes the interleaving semantics of the security protocol. Thanks to the use of specialized data structures and algorithms, it is possible to build and reason about the infinite state space of the protocol in a demand driven way. This allows for the formalization of and search in infinite state spaces, thereby simplifying the integration of powerful heuristics that accelerate search. Using these heuristics, the number of states searched is reduced dramatically in many cases.

The approach will be improved and refined in the project by (i) integrating the existing system with a declarative language common to all three techniques, (ii) investigating several promising search reduction techniques that can be integrated in the tool (in particular, the so-called "partial-order reduction" techniques), which are successfully used in other on-the-fly model-checkers, and (iii) achieving performance enhancements through careful profiling and tuning of the tool.

Theorem-Proving with Constraints. Recent advances in the theory and practice in automated deduction with constraints, built-in theories (such as associativity-commutativity), rewriting and ordering refinements have been applied to solve, automatically, a number of open mathematical problems. Preliminary experiences have shown the potential of saturation-based theorem-proving techniques for verification of hardware, protocols, telecommunication services, etc. However they have required cumbersome manual encoding and they have been unable to handle properly some features needed for protocol verification such as timeliness and freshness of messages.

The theorem-prover `daTac` developed in Nancy implements a constraint logic, which is a powerful extension of first-order logic by built-in constraints systems for which efficient decision procedures are known. It is therefore a good candidate for providing a standard format for the verifier/counter-model generator to be constructed during the project. The additional expressive power provided by exploiting the built-ins in the constraint-based theorem-provers may facilitate the translation of protocol descriptions to constraint logic and support the definition of an operational semantics for protocol executions; for instance, associativity-commutativity operators are useful for the representation of sets of messages. In this setting, the simulation of concurrent protocol executions is performed by saturation of the theory associated with a protocol by compilation, and flaws can be detected by deriving an inconsistency. Another advantage of this approach is that it makes possible a direct modeling of discrete time and fresh data generation by constraint solving. Indeed, there are no limitations on the size of messages and the number of fresh values generated over different sessions, and on the size of the state space in general.

New theorem-proving strategies will be developed that will be well-adapted to the class of problems addressed in this project and to the architecture of the verifier to be developed. Fragments of security protocols where freshness and timeliness requirements are important will be analyzed. Whenever possible, logical fragments where the theorem-proving procedure is a decision procedure (i.e. the verifier may be used not only for counter-model generation but also for certification) will be identified. Finally, efficient constraint-solving procedures in order to speed-up detection of redundancy or, dually, of inconsistency of input formulas will be developed.

SAT-based State-Exploration. Propositional satisfiability (SAT) related technology and research is one of the hottest of the current topics in Computer Science. This is due to several factors. First, there has been a dramatic speed-up for SAT procedures: since 1991 the problems solvable by SAT solvers have grown from 100 to 10,000 variables. Second, in these last few years, a variety of new algorithms, techniques, and heuristics improving on previous state-of-the-art SAT technology have been put forward. Third, on the basis of these results, researchers from various communities have started encoding real-world problems into SAT. The results have been success stories.

A SAT-based verification tool for security protocols will be built by Genova during the project, and this is expected to lead to yet another success story for two reasons. First, state-exploration tools have been able to detect flaws in a number of simple security protocols but, at the same time, they are not applicable to many interesting protocols because of the state-explosion problem. Second, SAT-based state-exploration tools have been remarkably successful in tackling previously unsolvable problems in diverse application domains such as planning and formal verification.

The plan of the activities consists of two major tasks:

1. Definition of the encodings: as it happened in planning and formal verification, several encodings into SAT are possible, each leading to a different computational behavior of the solver. Emphasis will be put on the definition of "parallel encodings": as in planning, they are expected to lead to the best computational results. The use of techniques for the automatic symmetry reduction of models will be also considered.

2. Experimentation with fine tuning of the SAT solver and specialization of the encoding: as recently shown, great speed-ups can be obtained by a fine tuning of the search mechanism implemented by the SAT solver; these speed-ups will make it possible to find solutions to problems that are unsolvable by other means.

Although each of these three techniques can work independently, they will be integrated into a single verifier where they will interact and benefit from each other's strengths. The expertise of the partners on the scope and limitations of the respective symbolic reasoning techniques (completeness of simplifications, complexity, expressiveness, etc.) as well as on the techniques for the integration of semi-decision procedures will be fundamental here.

Prototype verification tool. The assessment will be carried out by developing a prototype verification tool incorporating inference engines based on the three chosen automated reasoning techniques, and by thoroughly testing it against a corpus of 50 security protocols. The architecture of the prototype will be as depicted in Figure 1. Given a protocol verifica-

Figure 1: Architecture of the prototype verification tool
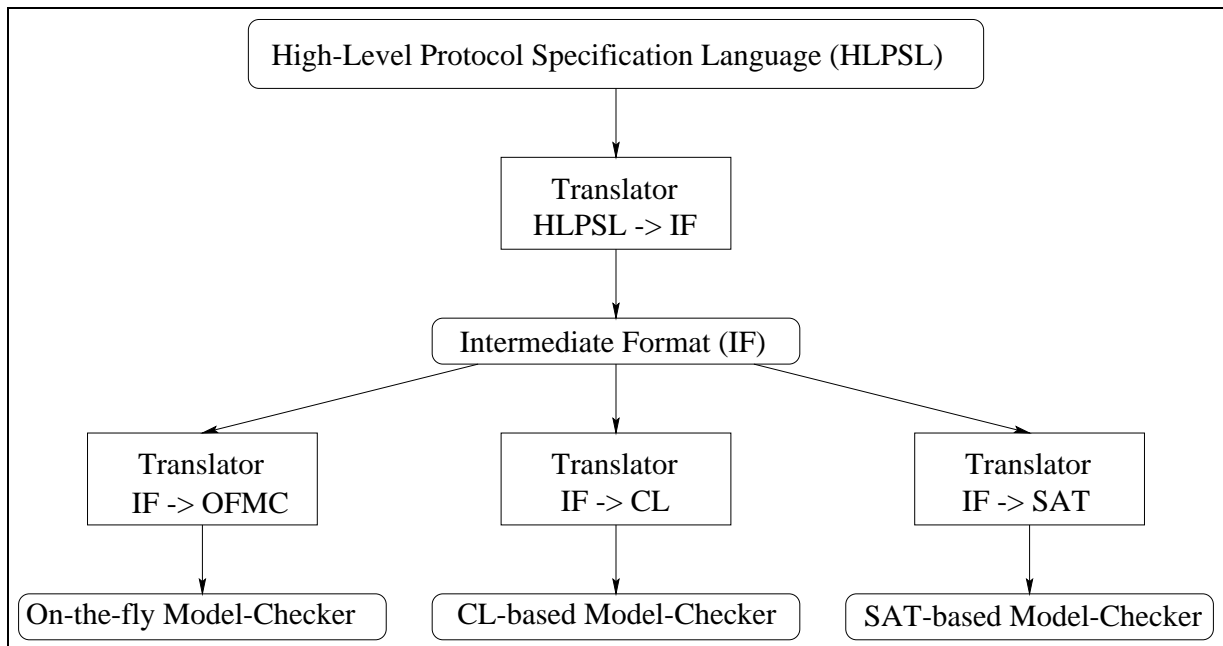
tion problem in a high-level specification language close to the language used in text-books and by engineers, the tool will first compile the problem into a standard declarative format, called *Intermediate Format* (IF), suitable for automated deduction (e.g. a subset of equational logic). While the choice of a language for protocol specification is not a difficult task

(examples of such languages already exist) the design of the translator raises non trivial issues closely related to the formal definition of semantics for protocol execution. Indeed, building a translator is important for many reasons. Firstly, it simplifies code writing since otherwise we would need 3 complete translators. Secondly, it enables the systematic comparison of competing verification techniques and heuristics. Thirdly, it makes feasible the automation of large scale examples. Finally, it opens the possibility of validating the translation process itself.

Protocol specifications expressed in the IF will then be mapped into "equivalent" deduction problems belonging to the domain of the three chosen automated deduction techniques. This activity will be carried out by specialized translators. The resulting deduction problems will be finally fed into the respective inference engine and counterexamples found by the inference engines will be mapped back into execution traces to be displayed to the user.

9.2   Workpackage list

The workplan is organized in 4 workpackages. WP1 is devoted to project management and assessment and is aimed to keep the project on target. The technical objectives will be achieved through workpackages WP2 and WP3. WP2 is devoted to the definition of the High-Level Protocol Specification Language HLPSL, of the Intermediate Format IF, and of the translation from HLPSL to IF. In WP3 we will develop the interfaces between IF and the chosen automated deduction engines. These interfaces, together with the translation mechanism of WP2, will allow us to run the available automated deduction engines against the verification problems of the corpus. The feedback received from the experiments will give us insight on the advantages and limitations of the different automated deduction techniques as well as on the performance bottlenecks. This will naturally lead to an improvement of the encodings and of the inference procedures implemented in the automated deduction engines. In WP4 we will disseminate the results and initiate industrial contacts in order to identify a set of representative case studies.

Workpackage list							
Workpack-age No	Workpackage title	Lead Contractor	Person-months	Start month	End month	Phase	Deliverable No
WP1	Management and Assessment	1	3 (1+1+1)	1	12		D1.1-2
WP2	Translation from High-Level to Intermediate Format	3	9.3 (2+1.3+6)	1	4		D2.1-3
WP3	Encoding, Experiments and Tuning	2	13 (2+8+3)	3	11		D3.1-6
WP4	Dissemination	1	3.4 (1.4+1+1)	9	12		D4.1-3
	TOTAL		28.7 (6.4+11.3+11)				

Note: in the Workpackage list, and in the single Workpackages and in the Deliverables list below, the person-months for ALUFR (coordinating site, participants no. 1, AC cost model) do not include the hours of permament staff working on the project (832 hours, as stated in Form A8.2).

9.3   Workpackage descriptions

WP1 – Management and Assessment

Workpackage number:	1	Starting date or event:	month 1		
Participant number:			1	2	3
Person-months per participant:			1	1	1

Objectives
Project management, co-ordination, assessment and evaluation of the results.

Description of work
The project management plan includes guidelines for deliverables, presentation standards, deadlines, information flow, dissemination and reporting. The coordinator will assemble and control the deliverables (see Section 9.4), supervise the evolving project results at each milestone as well as the assessment and evaluation results.

Tasks

T1.1: Management, including

- management and co-ordination of the communication between the project contractors and the European Commission;
- management of a project web-site and of a common on-line repository of the project code and documentation (using a version-management tool such as CVS).

T1.2: Assessment and evaluation.

Deliverables

D1.1: Report describing the project progress.

D1.2: Dissemination and Use plan.

D1.3: Final report describing the results of the assessment and evaluation activities.

Milestones and expected results

The project management is expected to keep the project on target, so that each task objective separately and, as a consequence, the objectives of the whole project can best be achieved. Given the small size of the consortium, it is expected that the project management will be flexible, effective and unproblematic,

We anticipate the following four meetings attended by all partners:

- Month 1: Kick-off meeting.

- Month 4: Assessment of the preliminary results and plan for future work (including a first draft of the Dissemination and Use plan, to be delivered in final form by month 6).

- Month 8: Summary and synchronization meeting. Assessment of the results.

- Month 12: Presentation of the final results and dissemination (we will invite industrial contacts to attend this meeting).

Additional meetings and bilateral visits will be arranged as required.

WP2 – Translation from High-Level to Intermediate Format

Workpackage number:	2	Starting date or event:		month 1
Participant number:			1	2	3
Person-months per participant:			2	1.3	6

Objectives
Translation from the High-Level Protocol Specification Language HLPSL to the Intermediate Format IF.

Description of work
We will define syntactical constructs for expressing security protocol verification problems: principals, key-tables, encryption, decryption, hashing, signatures, nonces, pairing, and the like. We will study how to introduce parameterization mechanisms in order to be able to describe several instances of the protocols running sequentially or concurrently. We will introduce constructs to model intruder behaviors (e.g. passive or active) and security goals (e.g. secrecy and authentication). We will define a target language for translating protocols, based on a rewrite system formalism. We will design and implement a translator prototype.

Tasks

T2.1: Define the high-level language HLPSL for specifying protocols that is close to the languages used in text-books and by engineers.

T2.2: Design and develop a prototype translator from HLPSL to a declarative format suitable for automated deduction (e.g. a subset of equational logic), namely the Intermediate Format IF.

Deliverables

D2.1: Specification of the HLPSL and prototype parser for the language.

D2.2: Specification of the IF.

D2.3: Development of a prototype translator from HLPSL to IF.

Milestones and expected results
Preliminary version of the semantics of the HLPSL. (A formal definition of the semantics of the HLPSL will be part of the follow-up RTD project.)

WP3 – Encoding, Experiments, and Tuning

Workpackage number:	3	Starting date or event:	month 2		
Participant number:			1	2	3
Person-months per participant:			2	8	3

Objectives

The objective of the workpackage is to experiment the chosen automated deduction techniques implemented in the prototype verification tool against the verification problems of the corpus.

Description of work

The first step (*encoding*) will be the definition of encodings that will translate the protocol verification problems, obtained by applying the translator of WP2 to the corpus, into deduction problems falling into the scope of application of the chosen automated deduction techniques. These encodings, together with the translation mechanism set up in WP2, will allow us to run the available automated deduction engines against the verification problems of the corpus (*experiments*). The experiments will indicate ways to improve the encodings as well as the inference strategies implemented in the available automated deduction engines (*tuning*).

Tasks

Each of the following tasks consists of several activities which are mutually dependent (all of them are closely related to the development of the prototype verification tool) and are therefore grouped in single tasks.

T3.1 (Freiburg): Define the encoding from the IF to the input format for the on-the-fly model-checker based on lazy data-types. Develop a prototype translator implementing the encoding, experiments with problems from the corpus, tuning of the encoding and/or of the on-the-fly model-checker.

T3.2 (Nancy): Define the encoding from the IF to the input format for the constraint-based theorem-prover. Develop a prototype translator implementing the encoding, experiments with problems from the corpus, tuning of the encoding and/or of the constraint-based theorem-prover.

T3.3 (Genova): Define of the encoding from the IF to the input format for the model-checker based on propositional satisfiability checking. Develop a prototype translator implementing the encoding, experiments with problems from the corpus, tuning of the encoding and/or of the model-checker based on propositional satisfiability checking.

Deliverables

D3.1-3: (by month 3) Preliminary definition, implementation, and experimentation with the encodings from IF to the input formats for the on-the-fly model-checker based on lazy data-types (D3.1), for the constraint-based theorem-prover (D3.2), and for the model-checker based on propositional satisfiability checking (D3.3).

D3.4-6: (by month 7) Final definition, implementation, and experimentation with the encodings from IF to the input formats for the on-the-fly model-checker based on lazy data-types (D3.4), for the constraint-based theorem-prover (D3.5), and for the model-checker based on propositional satisfiability checking (D3.6).

Milestones and expected results
We expect a classification of the advantages and limitations of the chosen automated deduction techniques as well as of the different encodings. We also expect to identify the performance bottlenecks obtained by profiling.
Milestones are due at the meeting at month 4 and at the meeting at month 8. The former will enable us to compare and assess the preliminary version of the encodings. The latter will enable us to compare and assess the final version of the encodings.

WP4 – Dissemination of Results

Workpackage number:	4	Starting date or event:	month 8

Participant number:		1	2	3
Person-months per participant:		1.4	1	1

Objectives
Dissemination of results to academia and industry.

Description of work
The final phase of the project will focus on the dissemination of results to academia (by presenting the project at international conferences and workshops that the project members will attend)and to industrial contacts (by organizing a meeting between project and industry representatives).

Tasks

T4.1: Produce the final version of the project web-site including the evaluation of all the project results and an on-line demo of the verification tool.

T4.2: Dissemine the results to scientific events and industrial partners.

Deliverables

D4.1: Project web-site, including results, evaluation and on-line demo.

D4.2: Joint paper(s) on the project at international conference(s).

D4.3: Report on industrial case studies identified with industrial contacts.

Milestones and expected results
This workpackage will disseminate the result of the assessment project to the international scientific community and to the industrial contacts.

9.4   Deliverable list

Deliverable list							
Del. No	Del. name	WP no.	Lead participant	Estimated person-months	Del. type	Security	Delivery (proj. month)
D1.1	Project presentation	1	1	1	Report	Pub	2
D1.2	Dissemination and Use plan	1	1	1	Report	Pub	6
D1.3	Final report	1	1	1	Report	Pub	12
D2.1	HLPSL spec. & parser	2	3	3	Report, Spec. & Impl.	Pub	3
D2.2	IF spec. & parser	2	3	3	Report, Spec. & Impl.	Pub	4
D2.3	Translator from HLPSL to IF	2	3	3.3	Report & Impl.	Pub	4
D3.1	Prelim. Def., Impl. & Exp. with on-the-fly m.c.	3	1	1	Report & Impl.	Pub	4
D3.2	Prelim. Def., Impl. & Exp. with C.L.	3	3	1	Report & Impl.	Pub	4
D3.3	Prelim. Def., Impl. & Exp. with SAT m.c.	3	2	4	Report & Impl.	Pub	4
D3.4	Final Def., Impl. & Exp. with on-the-fly m.c.	3	1	1	Report & Impl.	Pub	8
D3.5	Final Def., Impl. & Exp. with C.L.	3	3	2	Report & Impl.	Pub	8
D3.6	Final Def., Impl. & Exp. with SAT m.c.	3	2	4	Report & Impl.	Pub	8
D4.1	Final project web-site	4	1	0.4	Web-site	Pub	12
D4.2	Paper (at intl. meetings)	4	2	2	Conf. Paper & Talk	Pub	10
D4.3	Case Studies	4	1	1	Report	Pub	11

9.5 Project planning and timetable

A GANTT chart depicting the scheduling of the workpackages is given in Figure 3.
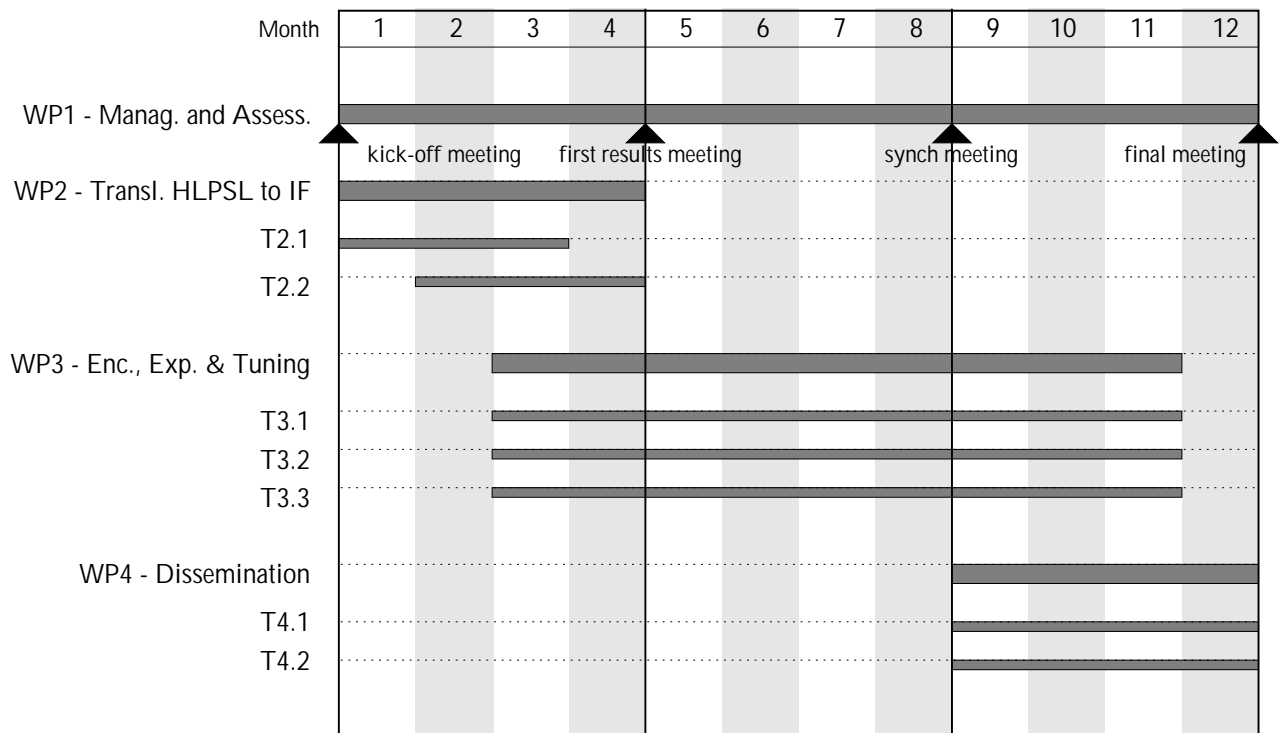
Figure 2: GANTT Chart of the AVISS Assessment Project

9.6 Graphical presentation of project components

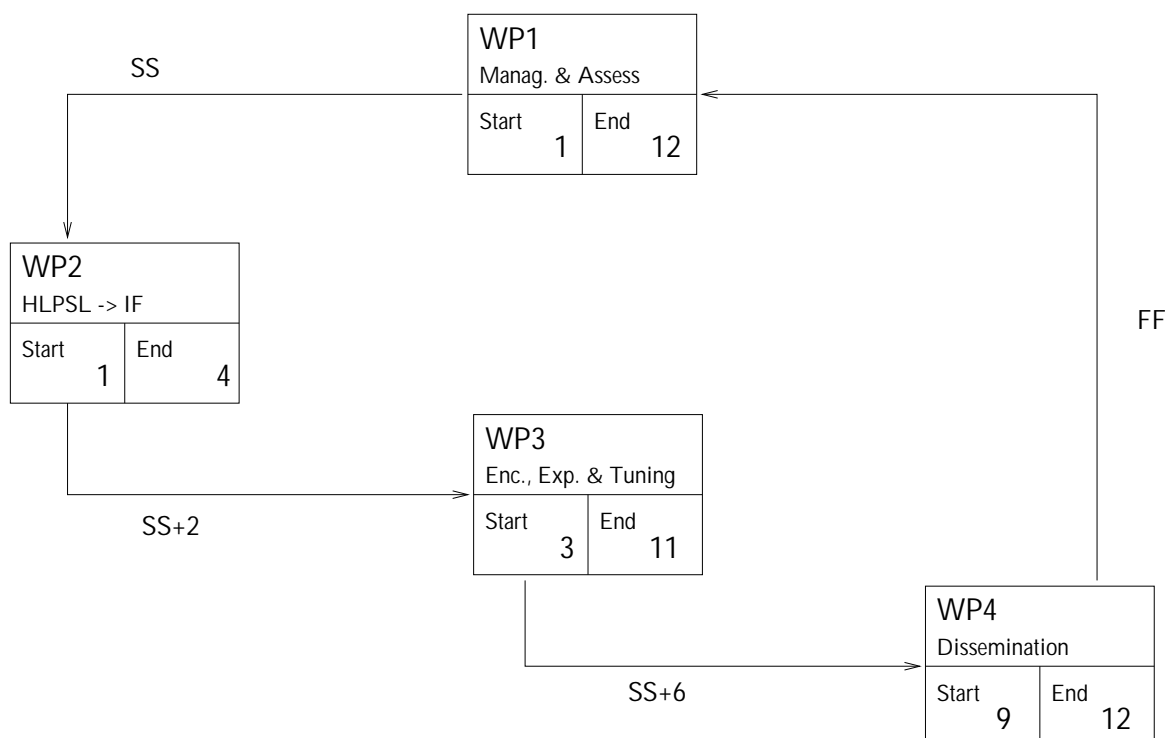A PERT chart representing the logical dependencies between the workpackages is given in Figure 3.

Figure 3: PERT Chart of the AVISS Assessment Project

9.7 Project management

The project management plan includes guidelines for deliverables, presentation standards, deadlines, information flow, and reporting. The Project Coordinator (PC), Prof. Dr. David Basin, the leader of the coordinating site (Freiburg), will act as the central node in the project, chairing and moderating the project meetings, assembling and controlling the deliverables, and supervising the evolving project results at each milestone as well as the assessment results.

The project management and co-ordination tasks include the following sub-tasks:

- Management and co-ordination of the communication between the project contractors and the European Commission.

- Management of a project web-site and of a common on-line repository of the project code and documentation (using a version-management tool such as CVS).

The project management is expected to keep the project on target, so that each task objective separately and, as a consequence, the objectives of the whole project can best be achieved. Given the small size of the consortium, it is expected the the project management

will be flexible, effective and unproblematic. The small size will also allow for the use of e-mail and telephone (as well as the above mentioned common on-line repository) as a means for the communication flow within the consortium. Furthermore, apart from the kick-off meeting in month 1, three other meetings are scheduled to take place in the months 4, 8 and 12 in order to assess the accomplished work.

A Project Coordination Committee (PCC) will be built, consisting of the PC and the other Site Leaders (appointed by their sites, and responsible for the local activities). The PCC will be responsible for the overall progress of the project towards the achievement of its goals, and for controlling the direction the project takes and resolving difficulties. In particular, the PCC will decide possible changes in the project programme such as stopping certain activities or re-distributing resources.

The PCC will also appoint Work Package Coordinators (WPCs). Each WPC will be responsible for maintaining a coherent activity within the corresponding workpackage, for monitoring progress and deliverables, and for reporting to the PCC, with recommendations for decisions whenever necessary.

Each site in the project has the responsibility to carry out its planned contribution within its budget, to contribute to the deliverables, to provide full documentation of project activities as requested by other partners, the PCC, or WPC to provide documentation on the financial situation of the project to the PCC as requested, and to provide any information deemed necessary by the PC for reports to European Commission authorities.

10   Clustering

Not applicable.

11   Other contractual conditions

Not applicable.

12   (Optional) Supplementary reports and concertation activity: Other action-specific conditions

Not applicable.

13   (Optional) Other considerations

Not applicable.

References

1. A. Armando, C. Castellini, and E. Giunchiglia. SAT-Based Procedures for Temporal Reasoning . In *Proceedings of 5th European Conference on Planning (ECP-99)*, LNAI, pages 98–109. Springer Verlag, Berlin, 1999.

2. A. Armando, J. Gallagher, A. Smaill, and A. Bundy. Automating the Synthesis of Decision Procedures in a Constructive Metatheory. *Annals of Mathematics and Artificial Intelligence*, 22(3,4):259–279, 1998.

3. A. Armando and E. Giunchiglia. Embedding Complex Decision Procedures inside an Interactive Theorem Prover. *Annals of Mathematics and Artificial Intelligence*, 8:475–502, 1993.

4. A. Armando and S. Ranise. Constraint Contextual Rewriting. In *Proceedings of the International Workshop on First order Theorem Proving (FTP'98)*, pages 65–75. Vienna, Austria, November, 23-25 1998.

5. A. Armando and S. Ranise. Constraint Solving in Logic Programming and in Automated Deduction: a Comparison. In F. Giunchiglia, editor, *Proceedings of 8th International Conference on Artificial Intelligence: Methodology, Systems, Applications (AIMSA98)*, LNAI 1480, pages 28–38. Springer-Verlag, Berlin, 1998.

6. A. Armando and S. Ranise. From Integrated Reasoning Specialists to "Plug-and-Play" Reasoning Components. In J. Calmet and J. Plaza, editors, *Proceedings of the Fourth International Conference Artificial Intelligence and Symbolic Computation (AISC98)*, LNCS 1476, pages 42–54. Springer-Verlag, Berlin, 1998.

7. A. Armando and S. Ranise. A practical extension mechanism for decision procedures. In *4th Workshop on Tools for System Design and Verification (FM-TOOLS 2000)*, pages 53–57. Reisenburg Castle near Ulm, Germany, July 10-13 2000. Extended version to appear on the Journal of Universal Computer Science.

8. A. Armando and S. Ranise. Termination of Constraint Contextual Rewriting. In C. Kirchner, H. et Ringeissen, editor, *3rd International Workshop on Frontiers of Combining Systems (FroCoS'2000)*, LNCS 1794, pages 47–61. Springer-Verlag, Berlin, 2000.

9. A. Armando, A. Smaill, and I. Green. Automatic Synthesis of Recursive Programs: The Proof-Planning Paradigm. *Automated Software Engineering*, 6(4):329–356, 1999.

10. L. Bachmair, I. V. Ramakrishnan, A. Tiwari, and L. Vigneron. Congruence closure modulo associativity-commutativity. In C. Kirchner, H. et Ringeissen, editor, *3rd International Workshop on Frontiers of Combining Systems (FroCoS'2000)*, LNCS 1794, pages 242–256. Springer Verlag, Berlin, 2000.

11. D. Basin. Logical framework based program development. *ACM Computing Surveys*, 30(3):1–4, 1998.

12. D. Basin. Lazy infinite-state analysis of security protocols. In *Secure Networking — CQRE [Secure] '99*, LNCS 1740, pages 30–42. Springer-Verlag, Berlin, 1999.

13. D. Basin and S. Friedrich. Modeling a hardware synthesis methodology in Isabelle. *Formal Methods in Systems Design*, 15(2):99–122, 1999.

14. D. Basin, S. Friedrich, J. Posegga, and H. Vogt. Java byte code verification by model checking. In *11th International Conference on Computer-Aided Verification (CAV'99)*, LNCS 1633, pages 491–494. Springer-Verlag, Berlin, 1999.

15. D. Basin and N. Klarlund. Automata based symbolic reasoning in hardware verification. *Formal Methods in Systems Design*, 13(3):255–288, 1998.

16. D. Basin and B. Krieg-Brückner. Formalization of the development process. In E. Astesiano, H.-J. Kreowski, and B. Krieg-Brückner, editors, *Algebraic Foundations of System Specification*, pages 521–562. Springer-Verlag, Berlin, 1998.

17. D. Basin, S. Matthews, and L. Viganò. Labelled propositional modal logics: theory and practice. *Journal of Logic and Computation*, 7(6):685–717, 1997.

18. D. Basin, S. Matthews, and L. Viganò. Labelled modal logics: quantifiers. *Journal of Logic, Language and Information*, 7(3):237–263, 1998.

19. N. Berregeb, A. Bouhoula, and M. Rusinowitch. Observational proofs with critical contexts. In E. Astesiano, editor, *Fundamental Approaches to Software Engineering - ETAPS'98*, LNCS 1382, pages 38–53. Springer-Verlag, Berlin, 1998.

20. P. Borovansky, C. Kirchner, and H. Kirchner. A functional view of rewriting and strategies for a semantics of elan. In M. Sato and Y. Toyama, editors, *Third Fuji International Symposium on Functional and Logic Programming, Kyoto*, pages 143–167. World Scientific, Singapore, 1998.

21. Common Authentication Protocol Specification Language. URL `http://www.csl.sri.com/ millen/capsl/`.

22. J. Clark and J. Jacob. A Survey of Authentication Protocol Literature: Version 1.0. Available via http://www.cs.york.ac.uk/ jac/papers/drareview.ps.gz, Nov. 1997.

23. H. Comon and F. Jacquemard. Ground reducibility is exptime-complete. In V. Pratt, editor, *Twelfth Annual IEEE Symposium on Logic in Computer Science, LICS'97*, pages 26–34. IEEE Computer Society Press.

24. H. Comon, P. Narendran, R. Nieuwenhuis, and M. Rusinowitch. Decision problems in ordered rewriting. In V. Pratt, editor, *Proceedings 13th IEEE Symposium on Logic in Computer Science*, pages 117–125. IEEE Computer Society Press, Los Alamitos, CA, 1998.

25. G. Denker and J. Millen. Capsl intermediate language. In *Formal Methods and Security Protocols*. 1999. FLOC '99 Workshop.

26. P. Ferraris and E. Giunchiglia. Planning as satisfiability in nondeterministic domains. In *Proceedings of the 17th International Joint Conference on Artificial Intelligence*. 2000.

27. H. Ganzinger, F. Jacquemard, and M. Veanes. Rigid reachability: The non-symmetric form of rigid E-unification. *International Journal of Foundations of Computer Science*, 11(1), 2000.

28. E. Giunchiglia, A. Armando, and P. Pecchiari. Structured Proof Procedures. *Annals of Mathematics and Artificial Intelligence*, 15(I):1–18, 1995.

29. E. Giunchiglia, F. Giunchiglia, R. Sebastiani, and A. Tacchella. More evaluation of decision procedures for modal logics. In A. G. Cohn, L. Schubert, and S. C. Shapiro, editors, *Sixth International Conference on Principles of Knowledge Representation and Reasoning (KR'98)*, The Morgan Kaufmann in Representation and Reasoning, pages 626–635. Morgan Kaufmann, Trento, Italy, 1998.

30. E. Giunchiglia, F. Giunchiglia, and A. Tacchella. *SAT, KSATC, DLP and TA: a comparative analysis. In P. Lambrix, A. Borgida, M. Lenzerini, R. Möller, and P. Patel-Schneider, editors, *Collected Papers from the International Description Logics Workshop (DL'99)*. CEUR, 1999.

31. E. Giunchiglia, F. Giunchiglia, and A. Tacchella. SAT-Based Decision Procedures for Classical Modal Logics. *Journal of Automated Reasoning*, 2000. To appear.

32. E. Giunchiglia, A. Massarotto, and R. Sebastiani. Act, and the rest will follow: Exploiting determinism in planning as satisfiability. In *Proceedings of the 15th National Conference on Artificial Intelligence (AAAI-98) and of the 10th Conference on Innovative Applications of Artificial Intelligence (IAAI-98)*, pages 948–953. AAAI Press, Menlo Park, 1998.

33. F. Jacquemard, M. Rusinowitch, and L. Vigneron. Compiling and narrowing cryptographic protocols. Technical Report 99-R-303, LORIA, Vandoeuvre les Nancy, Dec. 1999. URL: www.loria.fr/equipes/protheo/SOFTWARES/CASRUL.

34. H. Kautz and B. Selman. BLACKBOX: A new approach to the application of theorem proving to problem solving. In *Working notes of the Workshop on Planning as Combinatorial Search, held in conjunction with AIPS-98*. 1998.

35. F. Klay, M. Rusinowitch, and S. Stratulat. Analysing feature interactions with automated deduction systems. In B. Gavish, editor, *7th International Conference on Telecommunication Systems Modeling and Analysis*, pages 542–554. VIPPS, 1999.

36. G. Lowe. Casper: a compiler for the analysis of security protocols. *Journal of Computer Security*, 6(1):53–84, 1998.

37. G. Müller and K. Rannenberg. *Multilateral Security in Communications*. Addison-Wesley, 1999.

38. P. Narendran, M. Rusinowitch, and R. Verma. RPO constraint solving is in NP. In G. Gottlob, E. Grandjean, and K. Seyr, editors, *Computer Science Logic*, LNCS 1584, pages 385–398. Springer-Verlag, Berlin, 1998.

39. A. W. Roscoe. Modelling and verifying key-exchange protocols using CSP and FDR. In *8th IEEE Computer Security Foundations Workshop*, pages 98–107. 1995.

40. M. Rusinowitch, S. Stratulat, and F. Klay. Mechanical verification of an incremental abr conformance algorithm. In A. Emerson and P. Sistla, editors, *12th International Conference on Computer-Aided Verification (CAV'2000)*, LNCS. Springer-Verlag, Berlin, 2000.

41. B. Schneier. *Applied Cryptography*. John Wiley & Sons, New York, 1996.

42. W. Stallings. *Cryptography and network security*. Prentice-Hall, Englewood Cliffs, NJ, 1995.

43. L. Viganò. *Labelled Non-Classical Logics*. Kluwer Academic Publishers, Dordrecht, 2000.

44. L. Vigneron. Positive Deduction modulo Regular Theories. In H. Kleine-Büning, editor, *Proceedings of Computer Science Logic*, LNCS 1092, pages 468–485. Springer-Verlag, Berlin, 1995. URL: www.loria.fr/equipes/protheo/SOFTWARES/DATAC/.

45. L. Vigneron. Automated deduction techniques for studying rough algebras. *Fundamenta Informatica*, 33(1):85–103, 1998.

46. L. Vigneron and A. Wasilewska. Rough Sets based Proofs Visualisation. In R. N. Davé and T. Sudkamp, editors, *Proceedings of the 18th International Conference of the North American Fuzzy Information Processing Society (NAFIPS'99), invited session on Granular Computing and Rough Sets*, pages 805–808. IEEE Computer Society Press, Los Alamitos, CA, 1999.

Appendix A: Consortium Description

The consortium combines partners with complementary scientific competence. The group from the University of Freiburg has broad experience in formal methods, model-checking, and application of model-checking to security [11, 12, 13, 14, 15, 16, 17, 18, 43]. The group from the University of Genova has considerable experience on the combination of decision procedures and their application to different problem domains [4, 5, 6, 8, 7, 28, 29, 30, 31, 32, 34]. The group from INRIA has been working on theoretical foundations and system support for automated deduction for many years [10, 20, 23, 24, 27, 40, 44, 45, 46]. These groups are leaders in their respective areas and have a long history of international collaboration and strong bilateral relations. Moreover, each partner is among the leading experts on one of the three techniques upon which this project is based.

The coordinator, Prof. Basin from the University of Freiburg, has participated in a number of national projects in Germany (funded by the German Science Foundation DFG, the German Federal Ministry of Education and Research BMBF, and the Max-Planck-Gesellschaft) and has lead three international projects funded by the German Academic Exchange Society DAAD (with Great Britain, France, and Italy). In addition, he has coordinated a number of projects with German industry.

Initial case studies will be undertaken during the assessment, which, if successful (according to the criteria given below) will lead to the proposal of a RTD project with industrial partners. Enclosed to the proposal are statements from potential industrial partners (namely Deutsch Telekom, France Télécom, and GEMPLUS) who are interested in applying the tools or results from our research to their development of secure electronic commerce systems.

A.1 ALUFR – University of Freiburg, Institute for Software Engineering

The Albert-Ludwigs-Universität Freiburg is one of the oldest universities in Germany with a long history of collaboration with other universities and research institutes in Europe. Currently the university has 120 active EU-projects, including projects with every country in the Union. The University has central infrastructure for, and considerable experience with, the administration of EU-projects.

The Institute for Software Engineering at the Albert-Ludwigs-Universität Freiburg was founded in 1997 by Prof. Dr. David Basin and currently consists of 15 members. Research in the institute is focused around two overlapping themes: (1) formal methods for the design and analysis of safety or mission critical systems, and (2) design and analysis of multi-laterally secure systems and their commercial application.

In the last 3 years the institute has been involved in several national projects including a BMBF-funded VIROR project, where the institute has developed multimedial educational material on computer security, and a DFG project that supports research on formal methods for reasoning about secure systems. Internationally, the institute has been supported by two DAAD grants with France (Procope) and Italy (Vigoni), supporting collaborative work on formal methods for secure systems.

The Freiburg group has worked on several projects with German industry related to the proposed project. The institute has had projects in 1998 and 1999 funded by Deutsche Telekom, where they have developed formal methods for reasoning about security properties of mobile code, in particular Java byte-code. This year, the German company "Interac-

tive Objects GmbH" has started funding a PhD student in the group to investigate formal methods for secure electronic commerce: this project concerns developing verification and test methodologies for validating software architectural descriptions and protocols used by Interactive Objects in their e-commerce applications. The institute is also partner of the IST Working Group "Computer-Assisted Reasoning Based on Type Theory (TYPES)", due to start in 2000.

People Involved

Prof. Dr. David Basin   received his bachelors in Mathematics at Reed College in 1984 and his Ph.D. in Computer Science from Cornell University in 1989. His appointments include a two-year post-doctoral position at the University of Edinburgh and five years as a project leader at the Max-Planck-Institut für Informatik in Saarbrücken (Germany), where he received his Habilitation in 1996. Currently he is head of the Institute for Software Engineering at the University of Freiburg, where he has been a full professor since 1997. His research focuses on methods for the specification, verification, and construction of security and mission critical systems, as well as computer support for these activities. His past work includes foundational work on logics for verification, the development of system support for formal methods, and applications. He has published more than 20 journal papers and 40 papers in international conferences on deduction, formal methods and systems design, e.g. [11, 12, 13, 14, 15, 16, 17, 18]. In the last three years his teaching and research has focused on computer security. In particular, he has worked together with Deutsche Telekom on the development of methods for automatically analyzing security properties of Java byte-code and is the developer of a new on-the-fly model-checking approach to analyzing security protocols. Along with Dr. Viganò he has co-organized several classes and seminars on security and formal methods for secure system development. He has organized or been a member of the program committee of 15 international conferences and workshops, and is currently organizing a "Dagstuhl Seminar" on security protocols.

Dr. Luca Viganò   received his Masters in Electronic Engineering from the University of Genova in 1994 and his Ph.D. in Computer Science from the University of Saarbrücken in 1997. His appointments include a research position at the Max-Planck-Institut für Informatik in Saarbrücken (1994-1997). Since October 1997 he is an assistant professor at the Institute for Software Engineering at the University of Freiburg. His research focuses on methods for the specification, verification, and construction of secure systems. His work includes foundational work on the theory and applications of non-classical and security logics, of proof development systems, and of logical frameworks. On these topics he has co-organized several classes and seminars, and has published a book and 20 papers in international journals and conferences, e.g. [17, 18, 43].

Expertise: On-the-fly Model-Checking

The Freiburg group has developed a model-checker for security protocols that offers a number of advantages over conventional model-checking approaches [12]. In this work, a protocol and an attacker model give rise to an infinite state space that formalizes the interleaving semantics of the protocol. The group has developed specialized data structures and algorithms that are

then used to represent and compute with the infinite state-space associated with a protocol. The key idea is that the state-space is constructed in a lazy, "on-the-fly" way, i.e. in a demand-driven fashion, where heuristics can be easily integrated with state-space construction.

A.2 UNIGE – Università di Genova, Dipartimento di Informatica Sistemistica e Telematica

Research in the MRG Lab at DIST (Department of Information, Computers and Systems Science) at the University of Genova is focused on the design of automated reasoning tools and their effective use in a variety of application areas such as program verification and synthesis, planning, and validation of safety or security critical systems.

The laboratory has been involved in several national projects including a project on the design of a SAT-based model-checking tool and its application to the validation of safety critical systems. Internationally, the laboratory has been supported by two grants with Germany (University of Freiburg and University of Saarbrücken), a grant with France (INRIA Lorraine), and a grant with the UK (University of Edinburgh). The laboratory is also partner of the EU-funded Research Training Network "CALCULEMUS: Systems for Integrated Computation and Deduction" due to start in July 2000.

The laboratory will benefit of the administrative support from DIST, which has a long record of international projects (more than 70 EU-funded projects since 1984).

People Involved

Dr. Alessandro Armando received his master degree in Electronic Engineering in 1988 and his Ph.D. from the University of Genova in 1994. His appointments include a postdoctoral research position at the University of Edinburgh (1994-1995) and one at LORIA-INRIA (1998-1999). Since 1995 he is an assistant professor at the University of Genova. His research focuses on the integration of automated reasoning tools [3, 4, 5, 6, 8, 28] and their applications in a variety of problem domains ranging from the verification and synthesis of programs [2, 9] to the automation of temporal reasoning [1]. He is scientific representative for DIST of the EU-funded Research Training Network CALCULEMUS and member of the board of trustees of the CALCULEMUS Interest Group. He is the author of more than 40 research works in international journals and conferences. He is guest editor of a Special Issue of the Journal of Symbolic Computation on Integrated Symbolic Computation and Automated Deduction. He has been program committee member of a number of international workshops and conferences.

Prof. Dr. Enrico Giunchiglia received his master degree in Electronic Engineering in 1989 and his Ph.D. from the University of Genova in 1993. His appointments include a postdoctoral research position at the University of Texas (1993-1994). Since 1997 he is an associate professor at the University of Genova. His research focuses on methods for the integration of automated reasoning tools [3, 28] and related applications in planning and reasoning about actions [26, 32, 34]. He is scientific representative for DIST in several national research projects. He is the author of more than 60 research works in international journals and conferences. He has been program committee member of a number of major international conferences.

Expertise: SAT-based State-Exploration

The Genova group has a long history of research on SAT-based state exploration [28, 29, 30, 31] as well as in the combination and integration of automated reasoning tools [3, 4, 5, 6, 8]. In previous works, the group has shown how it is possible to define different encodings and/or search heuristics for verifying properties of domains specified in different formalisms [26, 32, 34]. Some of the proposed encodings and search heuristics led to improvements in the overall performances of the system of several orders of magnitude.

A.3 INRIA Lorraine, Protheo Group

INRIA (National Institute for Research in Computer Science and Control) is a French public-sector scientific and technological institute. The research carried out at INRIA brings together experts from the fields of computer science and applied mathematics. INRIA gathers in its premises around 2,100 people including 1,600 scientists, many of which belong to partner organizations (CNRS, industrial labs, universities) and work on common projects.

LORIA, the Lorraine Laboratory for Research into Information technology and its Applications, is a combined research unit common to the following organizations: CNRS, INRIA and the Universities of Nancy. With more than 150 researchers and around a hundred post-graduates, LORIA carries out its research along two themes: theories and techniques of software production, and human/machine communication and artificial intelligence.

This FET Open project at LORIA–INRIA Lorraine will be based on the Protheo group that includes 20 researchers among which are 11 permanent members (full-time researchers from INRIA and CNRS and professors from Nancy's Universities). The Protheo group is well-known for more than a decade of research on term rewriting systems, constraint solving and automated deduction. This research aims at designing tools for system specification and verification. The group is working on a logical framework for constructing deduction systems, on automated proofs by induction and equational proof techniques involving constraints and rewrite rules. The group has developed several widely distributed software packages, including SPIKE (an induction based theorem-prover), ELAN [20] (an environment for prototyping constraint resolution tools and deduction systems), and daTac [44] (a first-order theorem-prover for associative-commutative theories).

The Protheo group has been recently involved in the Esprit project Basic Research CCL and Working Group CoFI, in the COMPULOG network of excellence and in the ERCIM Working Groups, and collaborates with numerous foreign institutes. The group has industrial collaborations on formal verification with CNET-France Télécom and on constraint solving with GIHP-Champagne.

People Involved

Dr. Florent Jacquemard received his Ph.D. in Computer Science from the University of Paris 11 in November 1996. His appointments include postdoctoral research positions at SRI International (USA) and Max-Planck-Institut für Informatik (Saarbrücken, Germany). Since October 1998 he is a researcher at INRIA. His main research area is tree automata and their application to automated deduction and formal methods for verification. He is working on deductive and inductive automated theorem-proving with constraints, term rewriting, symbolic constraints solving, the complexity of decision problems in these settings, software

and protocols specification and verification, tree automata and monadic second order logics. He is coauthor of a book on tree automata techniques and applications, has published extensively in international journals and conferences (e.g. [23, 27]), and is a member of the executive board of the French chapter of the European Association of Theoretical Computer Science (EATCS).

Dr. Michaël Rusinowitch   received a Thèse d'État in Computer Science in 1987 at the University Henri Poincaré in Nancy. Since 1994 he is Directeur de Recherche at INRIA. His research is mainly concerned with theorem-proving, term-rewriting, and their application to software verification. He contributed to the development of automated deduction with constraints (e.g. [24, 38]) and to new proof methods based on induction and rewriting (e.g. [19]) that have been applied successfully to the detection of feature interaction [35] in telecommunication services and to the verification of reactive systems. He is currently collaborating with a team at CNET France-Télécom on the mechanical verification of ATM protocols [40]. Dr. Rusinowitch has been responsible in 1998/99 for an INRIA Cooperative Research Action on the Validation of Infinite State Systems. He has published his works in international conferences and journals, and is the author of a book on automated deduction. He has been a member of program committees for several international conferences and co-chairman of the conference on Rewriting Techniques and Applications.

Dr. Laurent Vigneron   is an assistant professor at the University Nancy 2 since 1997, and works at LORIA. He received his Ph.D. from University Henri Poincaré in Nancy in 1994. He held a postdoctoral research position at the University of Stony Brook (NY) in 1995. He is secretary of the IFIP Working Group 1.6 on rewriting. His research focuses on methods for automated deduction, theorem-proving, and verification, and has developed new techniques for deduction in first-order logic with built-in theories and with constraints, such as ordering and unification constraints. He has developed a system named daTac [44], implementing some of his results, which has been successfully used for proving difficult theorems and studying algebras [45, 46]. His current work is on automatic verification of cryptographic protocols.

Expertise: Theorem-Proving with Constraints

In a previous work [33], the group has shown how to automatically translate standard descriptions of security protocols into logic programs. This both defines an operational semantics for protocol executions and permits one to simulate protocol execution by exploiting the built-ins of the first-order prover daTac that was developed in the same group [44]. Flaws can be detected by deriving an inconsistency in the theory associated with the protocol. During this work the group has developed a prototype translator CASRUL [33] whose target language can serve as a basis for the common declarative format to be used by the project partners. Furthermore, the group plans to develop theorem-proving strategies that are well-adapted both to the high-level syntax used in this project and to the theorem-provers that are being developed, and to analyze fragments of e-commerce protocols where freshness and timeliness requirements are important.

Appendix B: Contract Preparation Forms