IST-004527 ARTIST2

Network of Excellence

on Embedded Systems Design

Activity Progress Report for Year 3

JPRA-Cluster Integration

Verification of Security Properties

Clusters:

Testing and Verification

Activity Leader:

Dr. Sandro Etalle (University of Twente)
www.cs.utwente.nl/~etalle

Policy Objective (abstract)

Focus and align research in the area, with an emphasis on security for smart cards, e-commerce, and cell phones. Establish coherent links between research and industry.

Develop the basic technology needed to certify security applications at levels EAL6, and EAL7, from the Common Criteria.

Create the necessary critical mass for moving the state security technologies forward for embedded systems in Europe. This implies taking the next steps towards a ubiquitous, tight, and fluid security infrastructure for the area.

Table of Contents

1. Overview of the Activity

1.1 ARTIST Participants and Roles

Team Leader: Sandro Etalle – University of Twente (the Netherlands)
Areas of his team's expertise: java card, modelling and verification.

Team Leader: Yassine Lakhnech – Verimag (France).
Areas of his team's expertise: semantics and models for security protocols.

Team Leader: Hans Hüttel – BRICS/Aalborg Univeristy (Denmark).
Areas of his team's expertise: process algebra and security, mobile code, modelling and verification.

Team Leader: Hubert Comon – LSV (France).
Areas of his team's expertise: security protocols, logics.

Team Leader: F. Klay - FTR&D (France)
Areas of his team's expertise: Formal methods applied to security protocols

1.2 Affiliated Participants and Roles

Team Leader: Michael Rusinowitch – INRIA (France).
Areas of his team's expertise: proofs, and protocols

Team Leader: Fabio Martinelli – CNR-IIT (Italy)
Areas of his team's expertise: foundations of security and trust; access control.

Team Leader: Boutheina Chetali – Gemalto (France).
Area of his team's expertise: smart cards.

1.3 Starting Date, and Expected Ending Date

Start date September 1st, 2004 to September 30th 2008

This activity will finish after the end of the project to allow further integration activities, which might take place in September 2008.

1.4 Baseline

Ensuring data integrity, confidentiality and other security related properties such as proper authorization is a key issue for most networked embedded systems with smart cards perhaps being the most prominent example. Moreover, embedded systems are by nature difficult and costly to patch, which calls for methods for guaranteeing out-of-the-box security.

In the recent past we have witnessed major progress in the development of verification techniques for security protocols (for instance, various decidability/complexity results have been obtained and several efficient tools are now available on the web). However most of these results are only applicable to simplified, limited protocols, and to specific properties. In addition, there is a lack of well-established common methodologies, languages and tools for verifying embedded security protocols. The situation is even worse when it comes to certification (due to high costs).

Our aim is to bridge the gap between formal verification and security engineering and broaden the horizon of the verification on security protocols in such a way that it meets the requirements and the (future) expectations of industrial partners. To achieve this aim, we have outlined three concrete goals: (1) the verification of more realistic protocols, (2) the verification of more realistic properties and (3) bridging the gap with trust management. In Section 1.5 we explain in more detail the concrete problems we have tackled to achieve these goals.

The teams involved are conducting substantial research in this field as witnessed by their participation in several outstanding national and international projects in the field. The consortium brings complementary expertise ranging from development of smart cards technology to mathematical formalisms for modelling and analyzing security issues.

Collaboration exists between France Telecom, INRIA, SchlumbergerSema, and the University of Twente in the framework of the FP6 Integrated Project Inspired.

Verimag, France Telecom, LSV, LIM, Trusted Logic, and LORIA/CASSIS already cooperate in several national-level projects (FORMACRYPT, EVA, PROUVE, ROSSIGNOL). All three revolve around modelling and analysis of security protocols.

Verimag, Trusted Logic and Schlumberger cooperate in a French national project (EDEN), for developing certification technology for smart card applications.

1.5 Problem Tackled in Year 3

As mentioned above, our goal is to *broaden the horizon of the verification on security protocols* in such a way that it meets the requirements and the (future) expectations of industrial partners. To this end we have tackled two related groups of problems, which can be considered as the natural extensions of the problems tackled last year:

1) **Bridging the gap between the formal and computational views of security protocols.** In the symbolic approach cryptographic primitives and attackers are modelled using terms and deduction systems. In the computational approach attackers are PPT Turing machines and cryptographic primitives are directly modelled as algorithms. While the guarantees in the computational model are stronger, proofs are much more complex. Among the specific problems we addressed, we should mention:

    a. Computational soundness of symbolic verification of cryptographic protocols. The aim is to provide results showing that a symbolic security proof will imply security in the computational model. We have achieved several advances including soundness results for strong notions of secrecy in the presence of an active adversary and general results for several equational theories in the presence of an adaptive attacker.

    b. Verification of equivalence-based properties. Many security properties are modelled using observational equivalences, i.e. an attacker cannot distinguish two processes even if he can arbitrarily interact with them. These notions are useful for modelling strong versions of secrecy and anonymity related properties in electronic voting. The definitions of observational equivalences stem from cryptographic pi calculi but are difficult to analyse. We propose symbolic semantics for the applied pi calculus which we expect to lead to efficient algorithms for checking observational equivalences.

2) **Verification of complex combinations of systems and protocols.** In particular, we focused on

    a. **Integration of verification and trust models**. This is perhaps the most visionary part of this activity. Present trust models for security of embedded systems are always ad-hoc and focused on a specific application/domain. This year we have contributed to a new general concept of trust model by on one hand integrating various trust models with each other and on the other hand by defining the core system of a new very general framework (TULIP) for the specification and the enforcement of trust decision.

b. **The verification of voting and e-payment protocols.** This activity includes a case study provided by France Telecom, about an electronic purse protocol. The protocols we studied require considering algebraic properties which were not studied in literature before. Among the results we obtained, we have shown that these algebraic properties can be reduced to associativity and commutativity.

1.6 Comments From Year 2 Review

No particular comments related to this activity have been given.

1.6.1 Reviewers' Comments

See above.

1.6.2 How These Have Been Addressed

See above.

2. Summary of Activity Progress

2.1 *Previous Work in Year 1*

Work carried out in the first months

- We have developed a classification and studied the relation between different existing specification methods (multiset rewriting and process algebra) for security protocols.
- We used standard model-checkers for analysing various security protocols (e.g. use of muCRL, SPIN and CADP) and for addressing security treats based on real-time issues (using UPPAAL).
- We studied the expressive power of a process calculus that allows one to express arbitrarily many runs of ping-pong protocols thanks to the presence of recursive definitions. We have established a number of decidability results that indicate the limitations of automatic verification even in this simple setting. Most prominently, we show that our process calculus is Turing-powerful.
- We developed a general language for describing security protocols and their properties.
- A publicly available database of security protocols and their analysis (attacks, proofs, assumptions/properties,...) has been developed http://www.lsv.ens-cachan.fr/spore/
- a general verification method for security protocols that can handle unbounded sessions, unbounded message size and unbounded fresh nonce creations;
- a sound and complete inference system for bounded-sessions cryptographic protocols (the messages size is still unbounded), method that has been extended to take into account protocols that can use timestamps;
- A proof that the Dolev-Yao model is a sound abstraction of the complexity theoretic model for protocols that combine several cryptographic primitives.
- We consider the problem of access control for the Calculus of Mobile Resources due to Godskesen, Hildebrandt, and Sassone. We establish a type system that lets us establish security policies for processes and show that our type system satisfies the usual requirements of type preservation under reduction and safety (i.e. that well-typed processes cannot misbehave). Moreover, we present a sound type inference algorithm that will let us extract minimal security policies.
- We have worked on a protocol for an electronic purse provided by France Telecom. We specified the protocol and the common language as well as its properties and conducted a first set of validation experiments showing a potential attack.

2.2 *Previous Work in Year 2*

Short summary of the work carried out in the second year.

- We have developed a new constraint-based tool for the verification of security properties which allows one to specify the properties to check using a linear temporal language.

- We have developed a model of state dependent access control. This is useful in many applications like for example, patient health records and employee. We have developed a software tool for verifying access control systems, which can check systems against specifications of the capabilities of users.
- We have initiated a systematic investigation of situations where reachability-based secrecy entails strong secrecy. We show that in the passive case, reachability-based secrecy actually implies equivalence-based secrecy for signatures, symmetric and asymmetric encryption provided that the primitives are probabilistic. For active adversaries in the case of symmetric encryption, we provide sufficient (and rather tight) conditions on the protocol for this implication to hold.
- Sandboxing in a distributed pi-calculus. We developed an extension of Hennessy and Riley's Dpi calculus with digital signatures and sandboxing with an associated type system that handles authentication.
- A preliminary integrated framework for security and trust management. We developed a preliminary integrated framework based on process algebras and suitable inference systems for the modelling of security protocols as well as of access control and trust/reputation management policies.
- Synthesis of enforcing mechanisms for security policies. We developed a framework for the automatic synthesis of enforcing mechanisms for security policies. In particular, we modelled as process algebra operators, the security automata of Schneider as well as the edit automata of Ligatti et al.
- Verification of security properties of cryptographic Application Program Interfaces (API). We developed a formal specification of IBM's security API (Common Cryptographic Architecture) and a computed-aided proof of its security.
- Development methodology with tool support that allows certification of Smart Card applications at the highest level EAL7 of Common Criteria. A computed-aided methodology for checking the formal conformance of applications with respect to security policy. We have extended the certification methodology to take into account new features both of applications (for example we can now handle more complex data structures) and of the security policy we want to check (data flow oriented properties in addition to trace-based security properties).
- Specification language for cryptographic protocols. We developed a specification language which makes it possible to separate the roles of a protocol from the scenario which defines how instances of the roles are created
- Formalization of protocols for electronic voting. Some protocols formalization including one from France Telecom. In a simplified model we get automatic proof of some security properties (fairness and eligibility) and by-hand proof of some other properties (receipt-freeness and coercion-resistance). Main teams involved: (France Telecom, LSV, INRIA, Univ. of Birmingham)

- We have developed HERMES is a tool for the automatic verification of cryptographic protocols. The initial version of HERMES implemented a general verification method based on abstraction, which can handle unbounded sessions, for protocols described using an Alice-Bob like specification language. The second version takes as input the new specification language mentioned above. The verification capabilities of HERMES have been extended with methods that handle specified scenarios (for example, unbounded but only iterative sessions, or composition between bounded and unbounded sessions, etc.).This second version allowed us to validate the protocol for electronic purse provided by France Telecom. The HERMES tool, versions 2, is available online at http://www-verimag.imag.fr/~Liana.Bozga/home/hermes.html
- We have studied the Intruder Deduction problem for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption.

2.3 Current Results

2.3.1 Technical Achievements

Title: Common Criteria Evaluation of a Java Card commercial product (Gemalto)
A major result for the formal methods in the industry: We have successfully conducted a Common Criteria (CC) evaluation on a Java Card based commercial product. This evaluation implies that security properties, like integrity, confidentiality (applet isolation properties) have been formally proved for the product. The formal models of the design and proofs developed in this work ensure that the execution of any bytecode-verified applet on the product is safe. This is the world's first CC evaluation of a smart card product involving EAL7 components. Difficulty: formal demonstration of integrity and confidentiality.

Title: An environment for the verification of smart cards embedded C code (Gemalto)
We have developed an environment, based on Caduceus and Why tools to verify functional (e.g. correctness) and security properties (e.g. anti-tearing) of smart card software written in C (join work with LRI, (http://proval.lri.fr/index.en.html). The environment has been used to verify the security properties of a real embedded operating system (Flash Memory Manager code). Difficulty: the verification of C code is particularly challenging.

Title: Computationally Sound Symbolic Secrecy in the Presence of Hash Functions (LSV, LORIA, ETH Zurich)
The standard symbolic, deducibility-based notions of secrecy are in general insufficient from a cryptographic point of view, especially in presence of hash functions. We devise and motivate a more appropriate secrecy criterion which exactly captures a standard cryptographic notion of secrecy for protocols involving public-key encryption and hash functions: protocols that satisfy it are computationally secure while any violation of our criterion directly leads to an attack. Difficulty: define a new notion of symbolic security; difficulties due to hash functions in the soundness proof, which requires a new proof technique.

http://www.lsv.ens-cachan.fr/~kremer/mes_publis.php?onlykey=CKKW-fsttcs2006

Title: Symbolic Bisimulation for the Applied Pi-Calculus. (LSV, LORIA, Univ. of Birmingham) We propose a symbolic semantics for the finite applied pi calculus, which is a variant of the pi calculus with extensions for modelling cryptographic protocols. By treating inputs symbolically, our semantics avoids potentially infinite branching of execution trees due to inputs from the environment. Correctness is maintained by associating with each process a set of constraints on symbolic terms. Based on the semantics, we define a sound symbolic labelled bisimulation relation. This is an important step towards automation of observational equivalence for the finite applied pi calculus, e.g., for verification of anonymity or strong secrecy properties of protocols with a bounded number of sessions. *Difficulty*: defining a sound and complete symbolic semantics. http://www.lsv.ens-cachan.fr/~kremer/mes_publis.php?onlykey=DKR-fsttcs07

Title: Adaptive Soundness of Static Equivalence (LSV)

We define a framework to reason about implementations of equational theories in the presence of an adaptive adversary. We particularly focus on soundness of static equivalence. We illustrate our framework on several equational theories: symmetric encryption, XOR, modular exponentiation and also joint theories of encryption and modular exponentiation. This last example relies on a combination result for reusing proofs for the separate theories. Finally, we define a model for symbolic analysis of dynamic group key exchange protocols, and show its computational soundness. Difficulty: technical difficulties arise in the soundness proofs due to the fact that the adversary is adaptive.

http://www.lsv.ens-cachan.fr/~kremer/mes_publis.php?onlykey=KM-esorics07

Title: Computationally Sound Analysis of Protocols using Bilinear Pairings (LSV)

We introduce a symbolic model to analyse protocols that use a bilinear pairing between two cyclic groups. This model consists in an extension of the Abadi-Rogaway logic and we prove that the logic is still computationally sound: symbolic indistinguishability implies computational indistinguishability provided that the Bilinear Decisional Diffie-Hellman assumption is verified and that the encryption scheme is IND-CPA secure. We illustrate our results on classical protocols using bilinear pairing like Joux tripartite Diffie-Hellman protocol or the TAK-2 and TAK-3 protocols. *Difficulty*: define a sound symbolic model of bilinear pairing; extend the notion of acyclicity and well-formed terms.

http://www.lsv.ens-cachan.fr/~mazare/mes_publis.php?onlykey=Maz-wits07

Title: Associative-Commutative Deducibility Constraints (LSV, Univ. of Birmingham)

We consider deducibility constraints, which are equivalent to particular Diophantine systems, arising in the automatic verification of security protocols, in presence of associative and commutative symbols. We show that deciding such Diophantine systems is, in general, undecidable. Then, we consider a simple subclass, which we show decidable. Though the solutions of these problems are not necessarily semi-linear sets, we show that there are (computable) semi-linear sets whose minimal solutions are not too far from the minimal solutions of the system. Finally, we consider a small variant of the problem, for which there is a much simpler decision algorithm. *Difficulty*: undecidability proof of AC constraint systems; exhibit decidable subclasses of interest

http://www.lsv.ens-cachan.fr/~delaune/mes-publis.php?onlykey=BCD-stacs2007

Title: Deducibility Constraints, Equational Theory and Electronic Money (LSV, LORIA)

The starting point of this work is a case study (from France Telecom) of an electronic purse protocol. The goal was to prove that the protocol is secure or that there is an attack. Modelling the protocol requires algebraic properties of a fragment of arithmetic, typically containing modular exponentiation. The usual equational theories described in papers on security protocols are too weak: the protocol cannot even be executed in these models. We consider here an equational theory which is powerful enough for the protocol to be executed, and for which unification is still decidable. Our main result is the decidability of the so-called intruder deduction problem, i.e., security in presence of a passive attacker, taking the algebraic properties into account. Our equational theory is a combination of several equational theories over non-disjoint signatures. *Difficulty*: proving decidability in polynomial time for the intruder deduction problem; new algebraic properties.

http://www.lsv.ens-cachan.fr/~delaune/mes-publis.php?onlykey=BCD-jouannaud

Title: Logics for the applied pi-calculus (BRICKS, University of Edinburg)
Short description: We have devised a first-order epistemic logic with characterizes a version of the static equivalence introduced by Abadi and Fournet. *Difficulty:* obtaining a logic that can be used to reason about environment knowledge and that can be adapted to a particular application by defining a suitable signature and associated equational theory. http://linkinghub.elsevier.com/retrieve/pii/S1571066107001041

Title: Unification and comparison of trust models (CNR-IT).

Description: Starting from our previous work on the definition of an integrated framework based on process algebras and suitable inference systems for the modelling of security, we have encoded several trust and reputation models. We used generic structures as semiring constraints to model them. This is related to research in access and usage control models. Main teams involved: CNR-IT. *Difficulty:* The difficulty lies in combining two such different approaches.

Title: Synthesis of enforcement mechanisms for security policies (CNR-IT).

Description: In the context of our long term research on a formal framework for the automatic synthesis of enforcing mechanisms for security policies, we modelled as process algebra operators the security automata of Schneider as well as the edit automata of Ligatti et al. As main extension we were able to develop multiple controllers for systems with several untrusted components. Main teams involved: CNR-IT. *Difficulty:* the difficulties in the automatic creation of automata that enforces specific security properties.

Title: Enforcing usage control policies on embedded systems (CNR-IT).

Description: We extended our line of research for access control to a full usage control model. Main research efforts are on run-time enforcement of policies on Java Virtual Machines. We also made experiments and benchmarks on resource constrained virtual machine (as KVM).Main teams involved: CNR-IT. *Difficulty:* the difficulties in the automatic creation of automata that enforces specific security properties.

Title: Design of a decision procedure for analysing web services security protocols (INRIA).

We propose an algorithm that determines whether a cryptographic protocol where message are xml trees is subject to an attack, for a fixed number of sessions. *Difficulty*: The difficulty was to handle associative commutative properties of xml nodes concatenation and also to handle the nondeterminism of message replies (several answers are possible for a same query).

Title: Analysing security problems with caps. (INRIA)
In the analysis of cryptographic protocols, a treacherous set of terms is one from which an intruder can get access to what was intended to be secret, by adding on to the top of a sequence of elements of this set, a cap formed of symbols legally part of his/her knowledge. We give sufficient conditions on the rewrite system modelling the intruder's abilities, such as using encryption and decryption functions, to ensure that it is decidable if such caps exist. *Difficulty*: The result is based on a saturation procedure for which termination conditions were not obvious to derive.

Title: A Cryptographic Model for Branching Time Security Properties -- the Case of Contract Signing Protocols (INRIA)
Some cryptographic tasks, such as contract signing and other related tasks, need to ensure complex, branching time security properties. We develop a cryptographic model that deals with all of the above problems. One central feature of our model is a general definition of fair scheduling which not only formalizes fair scheduling of resilient channels but also fair scheduling of actions of honest and dishonest principals. Based on this model and the notion of fair scheduling, we provide a definition of a prominent branching time property of contract signing protocols, namely balance, and give the cryptographic proof that the Asokan-Shoup-Waidner two-party contract signing protocol is balanced. *Difficulty*: When defining Branching Time Security Properties one needs to deal with subtle problems regarding the scheduling of non-deterministic decisions, the delivery of messages sent on resilient (non-adversarial controlled) channels, fair executions (executions where no party, both honest and dishonest, is unreasonably precluded to perform its actions), and defining strategies of adversaries against all possible non-deterministic choices of parties and arbitrary delivery of messages via resilient channels. These problems are typically not addressed in cryptographic models and these models therefore do not suffice to formalize branching time properties, such as those required of contract signing protocols.

Title: Synthesizing secure protocols (INRIA)
We propose a general transformation that maps a protocol secure in an extremely weak sense (essentially in a model where no adversary is present) into a protocol that is secure against a fully active adversary which interacts with an unbounded number of protocol sessions, and has absolute control over the network. The transformation works for arbitrary protocols with any number of participants. *Difficulty*: The difficulty was to find the simplest transformation that works: Each message is tied to the session for which it is intended via digital signatures and on-the-fly generated session identifiers, and prevents replay attacks by encrypting the messages under the recipient's public key.

Title: Computationally sound typing for Non-Interference: The case of deterministic encryption (Verimag).
Type systems for secure information flow aim to prevent a program from leaking information from variables that hold secret data to variables that hold public data. In this work we present a type system to address deterministic encryption. The intuition that encrypting a secret yields a public value, that can be stored in a public variable, is faithful for probabilistic encryption but erroneous for deterministic encryption. *Difficulty:* proving the computational soundness of our type system in the concrete security framework.

Title: Generalization of DDH with applications to protocol analysis and computational soundness (Verimag & Loria).

In this work we identify the (P,Q)-DDH assumption, as an extreme, powerful generalization of the Decisional Diffie-Hellman (DDH) assumption: virtually all previously proposed generalizations of DDH are instances of the (P,Q)-DDH problem. We prove that our generalization is no harder than DDH through a concrete reduction that we show to be rather tight in most practical cases. One important consequence of our result is that it yields significantly simpler security proofs for protocols that use extensions of DDH. We exemplify in the case of several group-key exchange protocols (among other we give an elementary, direct proof for the Burmester-Desmedt protocol). *Difficulty:* use our generalization of DDH to extend the celebrated computational soundness result of Abadi and Rogaway so that it can also handle exponentiation and Diffie-Hellman-like keys. The extension that we propose crucially relies on our generalization and seems hard to achieve it through other means.

Title: Audit-Based Compliance Control (University of Twente)

While preventative policy enforcement mechanisms can provide theoretical guarantees that policy is correctly enforced, they have limitations in practice. They are inflexible when unanticipated circumstances arise, and most are either inflexible with respect to the policies they can enforce or incapable of continuing to enforce policies on data objects as they move from one system to another. In this paper we propose an approach to enforcing policies not by preventing unauthorized use, but rather by deterring it. We believe this approach is complementary to preventative policy enforcement. We call our approach APPLE for A-Posteriori PoLicy Enforcement. We introduce APPLE Core, a logical framework for using logs to verify that actions taken by the system were authorized. A trust management system is used to ensure that data objects are provided only to users operating on auditable systems who are subject to penalty should they be found in violation. This combination of audit and accountability provides a deterrence that strongly encourages trustworthy behavior, thereby allowing a high level of assurance of end-to-end policy enforcement. *Difficulty:* linking the formal framework with the observable actions.

Title: core TuLiP (Twente)

We propose CoreTuLiP - the core of a trust management language based on Logic Programming. CoreTuLiP is based on a subset of moded logic programming, but enjoys the features of TM languages such as RT; in particular clauses are issued by different authorities and stored in a distributed manner. We present a lookup and inference algorithm which we prove to be correct and complete w.r.t. the declarative semantics. CoreTuLiP enjoys uniform syntax and the well-established semantics and is expressive enough to model scenarios which are hard to deal with in RT. *Difficulty:* demonstrating correctness and completeness of the search algorithm.

Title: timed analysis of security protocols (Twente)

We propose a method for engineering security protocols that are aware of timing aspects. We study a simplified version of the well-known Needham Schroeder protocol and the complete Yahalom protocol, where timing information allows the study of different attack scenarios. We model check the protocols using UPPAAL. Further, a taxonomy is obtained by studying and categorising protocols from the well known Clark Jacob library and the Security Protocol Open Repository (SPORE) library. Finally, we present some new challenges and threats that arise when considering time in the analysis, by providing a novel protocol that uses time challenges and exposing a timing attack over an implementation of an existing security protocol. *Difficulty:* demonstrating effectiveness of the approach in modelling time-based attacks.

2.3.2 Individual Publications Resulting from these Achievements

University of Twente

Bhargavan, K. and Corin, R.J. and Fournet, C. (2007) Crypto-Verifying Protocol Implementations in ML. In: 3rd Workshop on Formal and Computational Cryptography, FCC 2007, 4-5 Jul 2007, Venice, Italy..

Bhargavan, K. and Corin, R.J. and Fournet, C. and Gordon, A.D. (2007) Secure Sessions for Web Services. ACM Transactions on Information and System Security (TISSEC), 10 (2). article 8. ISSN 1094-9224

Corin, R.J. (2007) Computational Soundness of Formal Encryption in Coq. In: 3rd Workshop on Formal and Computational Cryptography, FCC 2007, 4-5 Jul 2007, Venice, Italy. INRIA.

Corin, R.J. and Denielou, P.M. and Fournet, C. and Bhargavan, K. and Leifer, J. (2007) Secure Implementations for Typed Session Abstractions. In: 20th IEEE Computer Security Foundations Symposium, 6-8 July, Venice, Italy. pp. 170-186. IEEE Computer Society. ISBN 0-7695-2819-8

Cederquist, J.G. and Corin, R.J. and Dekker, M.A.C. and Etalle, S. and den Hartog, J.I. and Lenzini, G. (2007) *Audit-based compliance control.* International Journal of Information Security, 6 (2-3). pp. 133-151.

Corin, R.J. and Etalle, S. and Hartel, P.H. and Mader, A.H. (2007) *Timed Analysis of Security Protocols.* Journal of Computer Security. To appear.

Dekker, M.A.C. and Cederquist, J.G. and Crampton, J. and Etalle, S. (2007) *Extended Privilege Inheritance in RBAC.* In: Proceedings of the 2nd ACM symposium on Information, computer and communications security, ASIACCS 2007. pp. 383-385.

Dekker, M.A.C. and Etalle, S. and den Hartog, J.I. (2007) *Privacy Policies.* In: Security Privacy and Trust in Modern Data Management. Springer Verlag, Berlin, pp. 383-397.

Delzanno, G. and Etalle, S. and Gabbrielli, M. (2007) *Introduction to the Special Issue on Specification Analysis and Verification of Reactive Systems.* Theory and Practice of Logic Programming, 6 (3). pp. 225-226.

Etalle, S. and Winsborough, W.H. (2007) *A Posteriori Compliance Control.* In: 12th ACM Symposium on Access Control Models and Technologies (SACMAT), 20-22 June 2007, Nice, France. pp. 11-20. ACM Press.

Chong, C.N. and Corin, R.J. and Doumen, J.M. and Etalle, S. and Hartel, P.H. and Law, Y.W. and Tokmakoff, A. (2006) *LicenseScript: A Logical Language for Digital Rights Management.* Annals of telecommunications special issue on Network and Information systems security, 61 (3-4). pp. 284-331.

Dekker, M.A.C. and Etalle, S. (2006) *Audit-Based Access Control for Electronic Health Records.* In: Proceedings of the Second International Workshop on Views on Designing Complex Architectures (VODCA), 16-17 Sept 2006, Bertinoro, Italy. pp. 221-236. Elsevier Electronic Notes in Theoretical Computer Science 168. Elsevier.

CNR

Fabio Martinelli, Paolo Mori: Enhancing Java Security with History Based Access Control. FOSAD 2007: 135-159

Fabio Martinelli, Marinella Petrocchi: On Relating and Integrating Two Trust Management Frameworks. Electr. Notes Theor. Comput. Sci. 168: 191-205 (2007), Elsevier Science.

Fabio Martinelli, Ilaria Matteucci: An Approach for the Specification, Verification and Synthesis of Secure Systems. Electr. Notes Theor. Comput. Sci. 168: 29-43 (2007), Elsevier Science.

Fabio Martinelli, Paolo Mori. A Model for Usage Control for GRID. International Workshop on Security, Trust and Privacy for GRID. To appear. IEEE digital library.

Maurizio Colombo, Fabio Martinelli, Paolo Mori, marinella Petrocchi, Anna Vaccarelli, Extending Globus Authorization with Role-based Trust Management. EUROCAST 2007. Pages to appear LNCS 4739. Springer.

Maurizio Colombo, Fabio martinelli, Paolo Mori, Marinella Petrocchi, Anna Vaccarelli. Fine Grained Access Control with Trust and Reputation Management for Globus.To appear in Proc. of GADA 2007.

BRICKS

Hans Hüttel, Michael D. Pedersen: A Logical Characterisation of Static Equivalence. Electr. Notes Theor. Comput. Sci. 173: 139-157 (2007), Elsevier Science.

Gemalto

B. Chetali. How the Common Criteria requirements could be used for the development of secure software, 7th International Common Criteria Conference (ICCC'06), Lanzarrote, Spain, September 2006 (http://www.7iccc.es).

LSV

S. Kremer and L. Mazare. Adaptive Soundness of Static Equivalence. In Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS'07), Dresden, Germany, September 2007, LNCS 4734. Springer. To appear.

S. Kremer and L. Mazare. Adaptive Soundness of Static Equivalence. In Proceedings of the 3rd Workshop on Formal and Computational Cryptography (FCC'07), Venice, Italy, July 2007.

S. Bursuc, H. Comon-Lundh and S. Delaune. Associative-Commutative Deducibility Constraints. In Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07), Aachen, Germany, February 2007, LNCS 4393, pages 634-645. Springer.

L. Mazare. Computationally Sound Analysis of Protocols using Bilinear Pairings. In Preliminary Proceedings of the 7th International Workshop on Issues in the Theory of Security (WITS'07), Braga, Portugal, March 2007, pages 6-21.

Verimag

Judicaël Courant, Cristian Ene and Yassine Lakhnech Computationally sound typing for Non-Interference: The case of deterministic encryption. Proc FSTTCS 2007.

Marion Daubignard, Romain Janvier, Yassine Lakhnech and Laurent Mazaré. Game-based Criterion Partition Applied to Computational Soundness of Adaptive Security. International Workshop on Formal Aspects in Security and Trust (FAST'06), Hamilton, Canada, August 2006.

Romain Janvier, Yassine Lakhnech and Laurent Mazaré. Relating the Symbolic and Computational Models of Security Protocols Using Hashes.Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'06), Seattle, US, August 2006.

Yassine Lakhnech, Laurent Mazaré and Bogdan Warinschi. Soundness of Symbolic Equivalence for Modular Exponentiation. The 2nd Workshop on Formal and Computational Cryptography (FCC'06), Venice, Italy, July 2006.

INRIA

Tarek Abbes, Adel Bouhoula, Michaël Rusinowitch: A Traffic Classification Algorithm for Intrusion Detection. AINA Workshops (1) 2007: 188-193

Yannick Chevalier, Denis Lugiez, Michaël Rusinowitch: Towards an Automatic Analysis of Web Service Security. FroCos 2007: 133-147

Siva Anantharaman, Paliath Narendran, Michaël Rusinowitch: Intruders with Caps. RTA 2007: 20-35

Abdessamad Imine, Michaël Rusinowitch: Applying a Theorem Prover to the Verification of Optimistic Replication Algorithms. Rewriting, Computation and Proof 2007: 213-234

Véronique Cortier, Bogdan Warinschi, Eugen Zalinescu: Synthesizing Secure Protocols. ESORICS 2007: 406-421

Véronique Cortier, Ralf Küsters, Bogdan Warinschi: A Cryptographic Model for Branching Time Security Properties - The Case of Contract Signing Protocols. ESORICS 2007: 422-437

Véronique Cortier, Gavin Keighren, Graham Steel: Automatic Analysis of the Security of XOR-Based Key Management Schemes. TACAS 2007: 538-552

Véronique Cortier, Heinrich Hördegen, Bogdan Warinschi: Explicit Randomness is not Necessary when Modeling Probabilistic Encryption. Electr. Notes Theor. Comput. Sci. 186: 49-65 (2007)

2.3.3 Interaction and Building Excellence between Partners

Interaction and integration has been achieved by working at the same topics and by sharing experiences at conferences and workshops we specifically organized to promote the exchange of ideas. The common topics we have focused on are (1) bridging the computational and symbolic view in the verification of security protocols and (2) verification of complex combinations of systems and protocols. As it appears from the list of publications, these two areas attracted most of our academic contributions. In particular, area (1) sees notable contribution of Verimag, BRICS, LSV, Inria and Twente, while area (2) sees contribution of Twente, LSV, Inria, FTR&D, CNR-IT and Gemalto. Notice that there is a sensible overlap between the two groups working on each topics. Concerning the interaction, this has been realized in practice in a number of different ways. In particular, we should mention the organization of focused high level meetings both for the exchange of ideas (the Artist2 security meeting in Trento, the 3rd international workshop on Formal and Computational Cryptography and the Itrust-PST joint conferences – in addition there is a Dagstuhl workshop being organized for the fall of 2007) and for the dissemination (the Artist-FOSAD summer school on security, which is the most prominent summer school on the field of security).

In addition to this there are a number of other actions/initiatives we should mention.

- We have had a major role in the organization of STM 2006, the second international workshop on security and trust management.
- LSV has hosted visits from several researchers in security: S.P. Suresh (2 weeks, June 2007), Mark Ryan (1 month, April 2007), Adel Bouhoula (1 month, July 2007)
- There are regular visits between LORIA and LSV which resulted in joint publications.
- A French national project on e-voting has been started by VERIMAG, LORIA, LSV and FT R&D.
- A French national project on Computer-Aided Security setup by VERIMAG and INRIA
- An international master programme "Cryptography, Security and Coding" setup in Grenoble with the participation of some companies (Gemalto, CEA-LETI...)
- Twente and INRIA now participate together in a the project POSEIDON, for the specification and the enforcement of privacy policies.

2.3.4 Joint Publications Resulting from these Achievements

M. Arnaud, V. Cortier, S. Delaune: Combining Algorithms for Deciding Knowledge in Security Protocols. FroCos 2007: 103-117

V. Cortier, S. Kremer, R. Kuesters and B. Warinschi. Computationally Sound Symbolic Secrecy in the Presence of Hash Functions. In Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06), Kolkata, India, December 2006, LNCS 4337, pages 176-187. Springer.

S. Delaune, S. Kremer and M. D. Ryan. Symbolic Bisimulation for the Applied Pi-Calculus. In Proceedings of the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'07), New Delhi, India, December 2007, LNCS. Springer. To appear.

S. Delaune, S. Kremer and M. D. Ryan. Symbolic bisimulation for the applied pi calculus. In Proceedings of the 5th International Workshop on Security Issues in Concurrency (SecCo'07), Lisbon, Portugal, September 2007, ENTCS. Elsevier Science Publishers. (Preliminary version)

S. Bursuc, H. Comon-Lundh and S. Delaune. Deducibility Constraints, Equational Theory and Electronic Money. In Rewriting, Computation and Proof - Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of his 60th Birthday, Cachan, France, June 2007, LNCS 4600, pages 196-212. Springer.

Emmanuel Bresson, Yassine Lakhnech, Laurent Mazaré and Bogdan Warinschi. A generalization of DDH with applications to protocol analysis and computational soundness Proc CRYPTO 2007.

Bhargavan, K. and Corin, R.J. and Fournet, C. (2007) Crypto-Verifying Protocol Implementations in ML. In: 3rd Workshop on Formal and Computational Cryptography, FCC 2007, 4-5 Jul 2007, Venice, Italy..

Bhargavan, K. and Corin, R.J. and Fournet, C. and Gordon, A.D. (2007) Secure Sessions for Web Services. ACM Transactions on Information and System Security (TISSEC), 10 (2). article 8. ISSN 1094-9224

Corin, R.J. and Denielou, P.M. and Fournet, C. and Bhargavan, K. and Leifer, J. (2007) Secure Implementations for Typed Session Abstractions. In: 20th IEEE Computer Security Foundations Symposium, 6-8 July, Venice, Italy. pp. 170-186. IEEE Computer Society. ISBN 0-7695-2819-8

Michael Backes and Yassine Lackhnech. Proceedings of the 3rd workshops on Formal and Computational Cryptography.

(With Contributions of F. Martinelli and S. Etalle) Foundations of Security Analysis and Design IV, FOSAD 2006/2007 Tutorial Lectures. Lecture Notes in Computer Science 4677 Springer 2007, ISBN 978-3-540-74809-0

2.3.5 Keynotes, Workshops, Tutorials

Workshop: 3rd workshop on Formal and Computational Cryptography.
Venice, Italy, July 5th 2007.

Cryptographic protocols are small distributed programs that add security services, like confidentiality or authentication, to network communication. Since the 1980s, two approaches have been developed for analyzing security protocols. One of the approaches relies on a computational model that considers issues of complexity and probability. The other approach relies on a symbolic model of protocol executions in which cryptographic primitives are black boxes.
The workshop focuses on the relation between the symbolic (Dolev-Yao) model and the computational (complexity-theoretic) model. Recent results have shown that in some cases the symbolic analysis is sound with respect to the computational model. Recent results have shown that in some cases the symbolic analysis is sound with respect to the computational model. A more direct approach which is also investigated considers symbolic proofs in the computational model. The workshop seeks results in any of these areas, and more generally, in the area of system and program verification for security and cryptography.

http://www-verimag.imag.fr/~lakhnech/FCC/

Summer School: Fosad-Artist FOSAD International School on Foundations of Security Analysis and Design.
Bertinoro, Italy, 10-16 September 2006.

The *International School on Foundations of Security Analysis and Design* (FOSAD) has been one of the foremost events established with the goal of disseminating knowledge in this critical area. The main aim of the FOSAD school is to offer a good spectrum of current research in foundations of security - ranging from programming languages to analysis of protocols, from cryptographic algorithms to access control policies and trust management - that can be of help for graduate students and young researchers from academia or industry that intend to approach the field..

http://www.sti.uniurb.it/events/fosad/

Workshop: Artist workshop on the verification of security properties of embedded systems.
Trento, Italy, February 22nd 2007.

In this workshop we have brought together the members of the activity “verification of security properties” of the ARTIST 2 project. Goal of the workshop was to foster cooperation, exchange ideas, plan new actions and outline future research directions for the NoE.

http://wwwhome.cs.utwente.nl/~etalle/meeting_artist/program_day_2.txt

Workshop: 2nd International Workshop on Security and Trust Management. *Hamburg, Germany, September 20th 2006.*

Main goals of the workshop were to investigate the foundations and applications of security and trust in ICT, and ro study the deep interplay between trust management and common security issues such as confidentiality, integrity and availability. STM 2006 has also provideda platform for presenting and discussing emerging ideas and trends.

http://www.hec.unil.ch/STM06/index.htm

Conference: IFIPTM 2007: Joint iTrust and PST Conferences on Privacy, Trust Management and Security
Moncton, Canada – July 30th – August 2nd 2007.

In 2007, the iTrust and PST conferences joined together with IFIP as IFIPTM 2007 to provide a truly global platform for the reporting of research, development, policy and practice in the interdependent areas of Privacy, Security, and Trust. The annual iTrust international conference has provided a forum with a multidisciplinary perspective: economic, legal, psychology, philosophy, sociology as well as information technology, is built on the work of the iTrust working group (http://www.itrust.uoc.gr), and has had four highly successful conferences in Europe to date.

http://www.unb.ca/pstnet/itrust-pst2007/

Keynote: S. Kremer. Formal analysis of an electronic voting protocol in the applied pi calculus. Workshop on the security of electronic voting (VETO'07)
Paris, France, April 26-27, 2007

http://www.lepolytechnicien.org/veto-07/

Keynote: Fabio Martinelli: Modelling, verification and synthesis of secure systems. 2nd International Workshop on Views On Designing Complex Architectures (VODCA'06).
Bertinoro, Italy, September 16-17 2006

Panel: S. Kremer. Information hiding: state-of-the-art and emerging Trends.
5th International Workshop on Security Issues in Concurrency (SecCo'07)
Lisbon, Portugal, September 3, 2007

http://www.dsi.uniroma1.it/~gorla/SecCo07/

Tutorial: Introduction to Trust Management
FOSAD 2006 6th International School of Foundations of Security Analysis and Design
Bertinoro, Italy, September 10-16 2006.

3. Future Work and Evolution

3.1 Problem to be Tackled over the next 12 months (Sept 2007 – Aug 2008)

As mentioned above, our goal is to *broaden the horizon of the verification on security protocols* in such a way that it meets the requirements and the (future) expectations of industrial partners. Two concrete problems we are going to tackle in the next year are

1) Start bringing into practice the results obtained in bridging the gap between the formal and computational views of security protocols by designing new practical tools. In the past years we have worked at bridging the gap between the formal and computational view of security protocol. As we have argued this bridge is needed to ensure that the verification of security protocols gives reasonable guarantees that a protocol that has been determined correct in the assumption that cryptography is perfect does not turn out to be flawed because of the interplay between the algebraic properties of the underlying cryptographic system and the protocol itself. Next year we are going to focus on bringing theory into practice by developing usable tools for the verification of security protocols with take into consideration the results obtained so far.

2) Lay the basis for a new trust management framework which generalizes present approaches, and is *not* application specific. We set a first step by integrating other TM frameworks and by defining a new language to express and resolve trust management policies. The next problem to be tackled is that of laying the basis for a completely new TM framework which is flexible enough to describe and implement both classic rule-based TM system and *reputation systems.*

3.2 Current and Future Milestones

(achieved) Year1: Define a reference model for security protocols

(achieved) Year2: prototypes capable of performing automatic analysis of security protocols. This has been achieved also by defining a constraint-based tool for the automatic verification of security protocols in which the user can specify arbitrary properties to be checked.

(achieved) Year 3: *develop compositional proof techniques for verifying services security properties, and for verifying group protocols. This milestone has been partially achieved. We have developed techniques for verifying service security and group protocols (see publications), but these techniques do not exploit compositional proof techniques. Indeed, it turns out that non-compositional techniques are more suitable to tackle the complexity these problems pose.*

Year 4:

- **Design new practical verification tools which take advantage of the results we obtained in bridging the gap between the computational and the symbolic view of security protocols.**
- **design high level protocols for modelling and enforcing trust in services execution.**

3.3 Indicators for Integration

A critical issue concerning the development of verification tools is their flexibility and expressiveness. While old-fashioned tools were suitable to check the correctness of standard authentication and confidentiality protocols, new services and application such as web-based applications, electronic money and trust-dependent systems rely on complex protocols which cannot be reduced to the classical black-box cryptography and Dolev-Yao adversary. In addition, these systems are not only concurrent but they are run in presence of an active adversary that tries to break the protocol and they use cryptographic primitives whose semantics is defined by means of probabilistic Turing machines and probabilistic games. For instance, the behaviour of a protocol critically depends on the power that is given to the adversary. This for instance determines whether a static corruption model is considered or a dynamic one, what is the effect of a corruption: does it leak only long-lived keys or also the whole state , etc.…

It is well-known that protocols proved correct in one model are not correct in another model. Thus, we consider that an important outcome of the integration work could be an agreed on common specification language for describing security protocols and their properties including notions of “trust”.

We have started new collaborative projects on e-voting, privacy protection and computer-aided security, which will help fostering cooperation and provide the essential funding to guarantee progress.

The collaboration between Verimag, LSV, LORIA and the University of Twente has been strengthened. We have organized a number of joint workshops and we are organizing (October 2007) a Dagstuhl seminar on the topic of verification of security protocols where various Artist2 participants have a prominent role. Clearly, there are numerous common publications. Moreover, Laurent Mazaré (Verimag) has received a postdoctoral position at LSV starting from October 2006. There are various national projects involving LSV and Verimag dedicated to the verification of cryptographic protocols. Stéphanie Delaune was a post-doc at LORIA (January until October 2007) after her PhD at LSV. Verimag and Trusted Logic are collaborating on the integration of the certification tools and methodology into Trusted Logic's commercial suite tool.

The collaboration between the University of Twente and CNR-IIT has been vital in the organization of the STM 2006 and of the IFIPTM 2007 conferences (see conference list).

3.4 Main Funding

FP5 Roadmap project RESET

French National Programmes

IST-2000-26410 AVISS (Automated Verification of Infinite State Systems)

Various French national projects:

- FormaCrypt (http://www.di.ens.fr/~blanchet/formacrypt/index.html), in which both LSV and LORIA participate.
- EDEN: Develop a methodology with tool support for the development of application certified at the highest assurance level of the Common Criteria. Partners: Gemalto, Trusted Logic (project co-ordinator), CEA-LIST, CEA-LETI and \Verimag
- POTESTAT: http://www-lsr.imag.fr/POTESTAT/. Partners: Landes IRISA, Vertecs IRISA, LSR-IMAG, Verimag.

- POSE http://www.rntl-pose.info/ Partners : Gemalto, INRIA/CASSIS, Leirios Technologie (coordinator), etc.
- Avote, Partners: LSV, LORIA and Verimag participate.

Terminated French projects

- PROUVE: http://www.lsv.ens-cachan.fr/prouve/ Partners: CRIL Technology Systèmes Avancés, France Telecom R&D, LSV ENS Cachan, LORIA Nancy, Verimag.
- ROSSIGNOL: http://www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html Partners: LIF Marseille, INRIA Futurs (LIX and LSV ENS Cachan) and Verimag

Various national funds and centres, such as:

- the Centre for Embedded Systems,
- CISS (http://ciss.auc.dk/),
- BRICS (http://www.brics.dk/),

SECURE: Secure Environments for Collaboration among Ubiquitous Roaming Entities IST Project: IST-2001-32486 (http://www.dsg.cs.tcd.ie/dynamic/?category_id=-30)

FP6 IP project Inspired: Integrated Secure Platform for Interactive Personal Devices

Various Dutch national projects:

- NL NWO project BRICKS: Basic Research in Informatics for Creating the Knowledge Society http://www.bsik-bricks.nl/
- NL IOP project PAW: Privacy in an Ambient World http://www.cs.ru.nl/~jhh/paw/.
- NL Freeband project I-share http://www.freeband.nl/project.cfm?id=520&language=en.
- NL STW project PEARL http://www.pearl-project.org/
- NL STW project S-mobile http://dies.cs.utwente.nl/research/#S-Mobile

EU-FET SENSORIA: Software Engineering for Service-Oriented Overlay Computers.

EU-FET BIONETS: Bio-Inspired Networks.

EU-IST S3MS: Secure software and services for mobile systems.

EU-IST GRID-Trust: Security and Trust for GRID systems.

4. Internal Reviewers for this Deliverable

Prof. Dr. Pieter Hartel, University of Twente.