ARTIST 2

Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Activity Progress Report for Year 2

JPRA-Cluster Integration

Verification of Security Properties

Cluster:

Testing and Verification

Activity Leader:

Dr. Sandro Etalle (University of Twente)
http://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 3
1.1 ARTIST2 Participants: Expertise and Roles 3
1.2 Affiliated Participants: Expertise and Roles 3
1.3 Starting Date, and Expected Ending Date 3
1.4 Baseline 3
1.5 Problem Tackled in Year2 4
1.6 Comments From Previous Review 6
1.6.1 Reviewers' Comments 6
1.6.2 How These Have Been Addressed 6

2. Summary of Activity Progress 7
2.1 Previous Work 7
2.2 Current Results 7
2.2.1 Technical Achievements / Outcomes / Difficulties encountered 7
2.2.2 Publications Resulting from these Achievements 13
2.2.3 Keynotes, Workshops, Tutorials 16

3. Future Work and Evolution 18
3.1 Problem to be Tackled over the next 18 months (Sept 2006 – Feb 2008) 18
3.2 Current and Future Milestones 19
3.3 Indicators for Integration 19
3.4 Main Funding 19
3.5 Internal reviewers 20

1. Overview of the Activity

1.1 ARTIST2 Participants: Expertise and Roles

Team Leader: Sandro Etalle – University of Twente (the Netherlands)
java card, modelling and verification.

Team Leader: Yassine Lakhnech – Verimag (France).
semantics and models for security protocols.

Team Leader: Hans Hüttel – BRICS/Aalborg Univeristy (Denmark).
process algebra and security, mobile code, modelling and verification.

Team Leader: Jean-François Raskin - Centre Fédéré de Verification (Belgium).
e-commerce, protocols, modelling and analysis.

Team Leader: Hubert Comon – LSV (France).
security protocols, logics.

Team Leader: F. Klay - FTR&D (France)
Formal methods applied to security protocols.

1.2 Affiliated Participants: Expertise and Roles

Team Leader: Michael Rusinowitch – INRIA (France).
proofs, and protocols

Team Leader: Fabio Martinelli – CNR-IIT (Italy)
foundations of security and trust; access control.

Team Leader: Boutheina Chetali – Axalto/SchlumbergerSema (France).
smart cards.

Team Leader: Andrea Bondavalli - University of Firenze (Italy)
competency.

1.3 Starting Date, and Expected Ending Date

Start date September 1st, 2004 to August 31st 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 Year2

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 three related groups of problems:

1) **The verification of more realistic protocols**. Verification tools have to be able to analyze real protocols. This raises a qualitative as well as a quantitative problem. The qualitative problem is the gap between the model of the protocol used for the verification and the real protocol under examination. The quantitative problem is due to the size of the protocol under examination.

    a. The qualitative problem translates to *bridging the gap between the formal and the computational and views of security protocols*; among the specific problems we tackled, we should mention:

        i. We investigated cryptographical aspects of security protocols: to get a more realistic account of security threats we have investigated how to lift the security results from the symbolic models to the computational models, which are generally employed by cryptographers.

        ii. We investigated how to verify protocols with algebraic properties: i.e. protocols employing operators (e.g. arithmetic) for building complex messages.

    b. The quantitative problem is *tackling industrial size protocols.* Among the specific problems we have tackled are:

        i. work on industrial cases to further validate the available tools and models.

        ii. We developed a methodology with tool support that allows certification of SmartCard applications at the highest level EAL7 of Common Criteria

iii. We investigated how to combine the advantages of model-checking based protocol verifiers with constraint-based protocol verifiers

iv. Modularity: we have started to derive combination results for addressing the verification of complex composed protocols and services;

2) **The verification of more realistic security properties.** A second, related problem is the analysis of security protocols in their real context. This raises two subproblems

a. First, *broadening the possibilities for specifying the security properties to be checked*. Present working verification tools usually refer to pre-built security notions; on the other hand, real-life security protocols require specific security properties. Therefore

i. We developed a language for the specification of security properties and a tool-supported methodology for the constraint-based verification of the specified properties.

ii. We developed new definitions of new specific security properties. We have formally defined different anonymity properties of election protocols and studied these properties on several case studies. We have also investigated protocols for electronic voting, and studied guessing attacks for password-based properties and computationally justified a definition of guessing attack based on static equivalence.

b. Secondly, adapting the attacker system (typically, the Dolev-Yao intruder) to model more realistic attack scenarios. In particular,

i. We worked on tools for the verification of security properties in the presence of unbounded attackers.

ii. We worked on understanding how sandboxing and digital signatures for handling mobile code can be described in a formal setting.

iii. We investigated extensions of the Dolev-Yao model which incorporate liveness properties.

3) **Bridging the gap between the verification of security properties and trust management**. This is perhaps the most visionary part of this activity. Present verification technology focuses on standard security properties such as authentication, secrecy and non-repudiation. We are working towards the extension of these methodologies to cover also *trust management* properties, which will be of central interest for e.g., groups and coalitions of embedded systems. Concrete problems we have tackled in this context are:

i. We worked on the integration of security policies for embedded systems with the security protocols.

ii. We worked on the definition of new models and language for the specification of trust management properties.

iii. We worked on the modelling and verification system of state-dependent access control systems.

1.6 Comments From Previous Review

1.6.1 Reviewers' Comments

"The original report had not been accepted. The resubmitted document now contains considerable substantive material, including interesting interim results indicated in 3.1, 3.2 and 4.1 (concerning the nature of the symbolic semantic model). The provision of "A publicly available database of security protocols and their analysis .. [at] .. http://www.lsv.ens-cachan.fr/spore/." is excellent. Even the 'brief state of the art' is worthy of publication on the ARTIST2 web site, as an introduction to the subject.

page 14 of 27 However, although the 'Indicators for integration' have been updated appropriately, the 'Evolution' section has still not been updated to reflect the latest position. Nor has the statement in 3.4 on 'Milestones'.

These are relatively minor elements of the deliverable, but they should nevertheless be updated to reflect the current status of the work."

1.6.2 How These Have Been Addressed

The sections *Indicators for integration, Evolution* and *Milestones* have been rewritten in accordance to the discussion we had at the Artist 2 workshop on security held in Pisa in May 2006.

2. Summary of Activity Progress

2.1 Previous Work

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 Current Results

2.2.1 Technical Achievements / Outcomes / Difficulties encountered

Title: A logic for constraint-based protocol analysis.
The technical achievement is the design of language for specifying security properties together with a new algorithm for checking them.

Description: The outcome is 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. Main team involved: Univ. of Twente.

Difficulty: Checking temporal properties on symbolic traces is already a challenging task. In our case, the addition of constraints makes it very difficult.

Title: A non-monotonic language for the specification of Trust Management policies.
We propose RT-, a new trust management language.

Description: The outcome is new language which adds a restricted form of negation to the standard RT language, thus admitting a controlled form of non-monotonicity**.** Main team involved: Univ. of Twente.

Difficulty: Non-monotonic policies are difficult to implement and to deploy, we have tackled this problem by restricting the "degree of nonmonotonicity".

Title: A state-dependent access control system.

Description: The outcome is 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. Main team(s) involved: Centre Fédéré de Verification (actually, the team of Namur). The implementation is at: http://www.cs.bham.ac.uk/~mdr/research/projects/05-AccessControl/rw-xacml-1_6.tar.gz

Difficulty: The technical difficulties lie in the verification of state-dependent access control.

Title: Relating two standard notions of secrecy.

Description: We initiate 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. Main team involved: Verimag.

Difficulty: The active case (i.e. the one in which the intruder is active) is particularly technical and therefore challenging.

Title: The CL-Atse Protocol Analyser.

Description: We have implemented the first complete decision procedure for detecting attacks on cryptographic protocols (in the case of finite sessions) using a XOR operator. The tool is available at http://www.loria.fr/equipes/cassis/softwares/AtSe/. The system also outperforms the other ones on standard cases. Main teams involved: LORIA.

Difficulty: An important difficulty was to implement a complete and efficient unification algorithm for XOR that can be combined with free operators. This has been achieved.

Title: Design of a combination techniques for handling several equational intruder theories in protocol analysis.

Description: This technique allows a hierarchy between the operators and has been applied to exponentiation operator with exponents ranging in an abelian group. Main teams involved: LORIA.

Difficulty: The difficulty was to find an appropriate condition on the theory so that previous disjoint combination results can be adapted.

Title: On key cycles. Recent results on interpreting symbolic security proofs in more accurate computational model rely on the assumption that no keys cycle can be produced during an execution of the protocol. Main teams involved: LORIA.

Description: We have shown that deciding the existence of key-cycle for a bounded number of sessions is NP-complete. The procedure also applies to protocols with timestamps.

Difficulty: The difficulty was to get polynomial bounds for the messages to be exchanged for building a key-cycle.

Title: Sandboxing in a distributed pi-calculus.

Description: We developed an extension of Hennessy and Riley's Dpi calculus with digital signatures and sandboxing with an associated type system that handles authentication. See http://vbn.aau.dk/fbspretrieve/4528056/article.pdf. Participants: Hans Hüttel, Morten Kühnrich.

Difficulty: Finding a suitable treatment of authentication in a type system.

Title: Recursion and replication in ping-pong protocols.

Description: Theorems that describe to which it extent it is possible to use automatic verification techniques for ping-pong protocols with recursion or replication. See http://www.brics.dk/~srba/files/HS:JAR:05.pdf. Participants: Hans Hüttel, Jíři Srba.

Difficulty: Showing that the Dolev-Yao attacker can be described within a ping-pong calculus with recursion.

Title: Preliminary integrated framework for security and trust management.

Description: 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. Main teams involved: CNR-IT.

Difficulty: The difficulty lies in combining two such different approaches.

Title: Synthesis of enforcing mechanisms for security policies

Description: 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. Main teams involved: CNR-IT.

Difficulty: the difficulties in the automatic creation of automata that enforces specific security properties.

Title: Verification of security properties of cryptographic Application Program Interfaces (API).

Description: We developed a formal specification of IBM's security API (Common Cryptographic Architecture) and a computed-aided proof of its security. Main team(s) involved: VERIMAG.

Difficulty: Arbitrary long sequences of calls and a huge number of possible primitives; algebraic properties of bitwise xor (attacks based on it are known); embedded calls of encrypting primitives; interplay between a typing and cryptography.

Tile: Computational soundness of the symbolic model for cryptographic primitives

Description: In the symbolic model, cryptographic primitives are considered as operations on abstract data type. This is not only the case for the protocol but also for the adversary trying to break the protocol. Cryptographic primitives are, however, modelled more accurately by randomized algorithms, and the security of a protocol is defined as the low probability that a probabilistic adversary with limited resources can break the protocol. Proving soundness of symbolic allows to benefit from the automated tools of the symbolic model on one hand and from the fact that the computational model is quite close to real implementations. We have proved the soundness of the symbolic model for protocols that use asymmetric and symmetric encryption, digital signature, hash functions and Diffie-Hellman exponentiation. Main team(s) involved: VERIMAG.

Difficulty: Complex reduction proofs; definition of the security properties of the cryptographic primitives.

Tile: Development methodology with tool support that allows certification of Smart Card applications at the highest level EAL7 of Common Criteria.

Description: 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). The methodology is now being transferred to TrustedLogic and integrated in their tools. This transfer is financed by a French national project. Main team(s) involved: VERIMAG.

Difficulty: Finding a suitable refinement relation, the development of verification algorithms, the implementation of the methodology

Tile: Certifying Cryptographic Protocols by Abstract Model-Checking and Proof Concretization

Description: The aim is to produce a proof of correctness independently from the tool and the abstractions used. First a proof of the abstract property is produced, and then it is automatically transformed into a proof of the concrete property and a set of proof obligations. Main team(s) involved: VERIMAG.

Difficulty: The main difficulty is to transform automatically a proof of the abstract property into a proof of the concrete property, without producing proof obligations impossible or too hard to prove.

Tile: 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. In our system, roles are programs written in simple imperative programming language and are executed by (legitimate) protocol participants. Main team(s) involved: VERIMAG.

Description: The outcome is a new specification language for cryptographic protocols which allows describing both protocols and the specific context in which they are used.

Difficulty: Most specification languages are more abstract, supposedly user-friendly using the so-called Alice-Bob notation. This approach is useful to understand what a correct protocol run is supposed to look like; however, it does not describe in an unambiguous way the actions of the protocol participants. We choose to take a different approach, where the user specifies the protocol as seen by the protocol agents.

Title: Formalization of protocols for electronic voting

Outcome: some protocols formalization including one from France Telecom. In a simplified model we get automatic proof of some security properties (fairness and eligibily)and by-hand proof of some other properties (receipt-freeness and coercion-resistance). Main teams involved: (France Telecom, LSV, INRIA, Univ. of Birmingham)

Difficulty: for sophisticated properties like anonymity related properties, even specifying the properties is challenging, furthermore to take account of cryptographic primitives algebraic properties is very difficult.

Tile: HERMES: A verification tool for cryptographic primitives

Description: 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

Difficulty: Many over-abstractions are needed in order to deal with an unbounded number of sessions. These abstractions were mainly based on the notion of session and a very general scenario. Using the new specification language, the notion of session disappear and we should refine all abstractions in order to take into account the scenarios defined by the user.

Title: Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or.

Description: We show that symbolic trace reachability for well-defined protocols is decidable in presence of the exclusive or theory in combination with the homomorphism axiom. These theories allow us to model basic properties of important cryptographic operators. Involved: LSV, LIF, Marseille.

Difficulty: This active case is particularly technical. The problem amounts to solve a system of quadratic equations of a particular form over Z/2Z[h], the ring of polynomials in one indeterminate over the finite field Z/2Z.

Title: A Survey of Algebraic Properties Used in Cryptographic Protocols.

Description: A great deal of cryptographic protocols relies on algebraic properties. We give a list of some relevant algebraic properties of cryptographic operators, and for each of them, we provide examples of protocols or attacks using these properties. We also give an overview of the existing methods in formal approaches for analyzing cryptographic protocols. Persons involved: V. Cortier (LORIA), S. Delaune (LSV) and P. Lafourcade (LSV).

Difficulty: To be as exhaustive as possible.

Title: Easy Intruder Deduction Problems with Homomorphisms.

Description: We present complexity results for the verification of security protocols. We are interested in theories such as Exclusive or and Abelian groups in combination with the homomorphism axiom. We show that the intruder deduction problem is in PTIME in both cases, improving EXPTIME existing results. Persons involved: S. Delaune (LSV).

Difficulty: The difficulty was to produce the link between the resolution of the intruder deduction problem in such kind of equational theory and the solvability of linear system of equations over polynomials.

Title: Tree automata with equality constraints modulo equational theories.

Description: We present new classes of tree automata combining automata with equality test and automata modulo equational theories. This class has a good potential for application in software verification and is very useful, in the context of cryptographic protocol verification, to model the algebraic properties of the cryptographic primitives. Involved: LSV and LORIA.

Difficulty: This challenging result allows one to obtain a decision procedure for the verification of protocols in the presence of an active attacker and for a class of equational theory. As all the results of this kind, the proofs are very technical. Next steps: We plan to extend our result to more complex equational theories. In particular, those involving an AC operator.

Title: Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption

Description: The paper solves the intruder deduction problem (passive case) for a theory of Exclusive-or with commutative and distributive encryption. It is shown that this problem is in 2-EXP-Time and that even the binary case is EXP-SPACE-hard. Involved: LSV.

Difficulty: The hard part is to deal with the commutativity of the encryption operator and find a "good" normalization.

Title: ACUNh: Unification and Disunification Using Automata Theory

Description: We propose an efficient decision procedure for the (dis)unification modulo the theory of the Exclusive-or with homomorphism. The algorithm follows an automata-theoretic approach. Involved: LSV and LIF, Marseille.

Difficulty: The difficult part is to compute the set all of mgu.

Title: Guessing Attacks and the Computational Soundness of Static Equivalence.

Description: We give a computational justification of the use of a particular equational theory in the context of guessing attacks. Guessing attacks are formally modelled using static equivalence. Involved: LSV, LORIA, Microsoft research and UC Santa Cruz.

Difficulty: The proof that that the formal definition of guessing attacks, in terms of static equivalence, is sound with respect to the computational definition is technical and non-trivial.

Title: Coercion-Resistance and Receipt-Freeness in Electronic Voting.

Description: In the context of our efforts to formally study electronic voting protocols, we have studies prominent anonymity properties of election protocols; we have given formal definitions of privacy, receipt-freeness and coercion-resistance in the applied pi calculus. Involved: LSV, Univ. of Birmingham.

Difficulty: Giving a formal definition of receipt-freeness and coercion-resistance, which reflects the intuition is tricky. In particular, for coercion resistance we defined a new simulation relation which may be of independent interest.

2.2.2 Publications Resulting from these Achievements

Corin, R.J. and Saptawijaya, A. and Etalle, S. (2006) A Logic for Constraint-based Security Protocol Analysis. In: IEEE Symposium on Security and Privacy, 21-25 May 2006, Oakland, US, pp. 155-168, IEEE Press.

Czenko, M. R. and Tran, H.M. and Doumen, J.M. and Etalle, S. and Hartel, P.H. and den Hartog, J.I. (2005) Nonmonotonic Trust Management for P2P Applications. In: 1st Int. Workshop on Security and Trust Management (STM), Milan, Italy. pp. 101-116. Elsevier Science.

Cederquist, J.G. and Corin, R.J. and Dashti, M.T. (2005) On the quest for impartiality: Design and analysis of a Fair Non-repudiation protocol. In: 7th Int. Conf. on Information and Communications Security (ICICS), Beijing, China. pp. 27-39. Springer-Verlag. ISBN 3-540-30934-9.

Cederquist, J.G. and Dashti, M.T. (2005) An Intruder Model for Verifying Termination in Security Protocols. Technical Report TR-CTIT-05-29 Centre for Telematics and Information Technology, University of Twente, Enschede. ISSN 1381-3625

Corin, R.J. and den Hartog, J.I. (2006) A Probabilistic Hoare-style logic for Game-based Cryptographic Proofs. In: ICALP 2006 track C, 9-13 Jul 2006, Venice, Italy. pp. 252-263. Springer Verlag 4052. ISBN 3-540-35907-9

Corin, R.J. (2006) Analysis Models for Security Protocols. PhD thesis, Univ. of Twente. ISBN 90-365-2279-X.

V. Cortier, M. Rusinowitch and E. Zalinescu. Relating two standard notions of secrecy. In Proc. of the 20th Int. Conference on Computer Science Logic (CSL'06), Szeged, Hungary, September 2006, volume 4207 of Lecture Notes in Computer Science, pages 303-318. Springer, 2006.

M. Turuani: The CL-Atse Protocol Analyser. RTA 2006: 277-286 Frank Pfenning (Ed.): Term Rewriting and Applications, 17th International Conference, RTA 2006, Seattle, WA, USA, August 12-14, 2006, Proceedings. Lecture Notes in Computer Science 4098 Springer 2006, ISBN 3-540-36834-5

Y. Chevalier, M. Rusinowitch: Hierarchical Combination of Intruder Theories. RTA 2006: 108-122 Frank Pfenning (Ed.): Term Rewriting and Applications, 17th International Conference,

RTA 2006, Seattle, WA, USA, August 12-14, 2006, Proceedings. Lecture Notes in Computer Science 4098 Springer 2006, ISBN 3-540-36834-5

V. Cortier and E. Zalinescu. Deciding key cycles for security protocols. In Proc. of the 13th Int. Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'06), Phnom Penh, Cambodia, November 2006. To appear in Lecture Notes in Artificial Intelligence. Springer, 2006.

D. Guelev, M. Ryan and P.-Y. Schobbens. Model-checking Access Control Policies. Seventh Information Security Conference (ISC'04). Lecture Notes in Computer Science, Springer-Verlag, 2004. 16 pages. ftp://ftp.cs.bham.ac.uk/pub/authors/M.D.Ryan/04-acl-full.pdf

H. Hüttel and J. Srba. Decidability Issues for Extended Ping-Pong Protocol. Journal of Automated Reasoning. Kluwer Academic Publishers, 2005.

H. Hüttel and M. Kühnrich: Authentication and Sandboxing in a Distributed Pi-Calculus. Proceedings of 6th International Workshop on Issues in the Theory of Security (WITS '06), Vienna, 25-26 March, 2006.

R. Gorrieri, F. Martinelli and M. Petrocchi. A Formalization of Credit and Responsibility within the GNDC schema. In proc. of the 1st International Workshop on Security and Trust Management (STM'05), ENTCS, Volume 157, Issue 3, Pages 1-158.

H. Kostukanski, F. Martinelli, P. Mori and A. Vaccarelli. Fine-grained and History-based Access Control with Trust Management for Autonomic Grid Services. In proc. of ICAS'06. IEEE Press, 2006.

F. Martinelli and I. Matteucci. Through modelling to synthesis of security automata. Proc. 2nd International Workshop in Security and Trust Management (STM06). Sept. 2006. ENTCS. To appear.

H. Kostukanski, F. Martinelli, P. Mori, A. Vaccarelli and L. Bortz. A Fine-grained Access Control System for Globus Based on X.509 Certificates. In proc. of the International Symposium on GRID Computing and its Applications to Data Analysis (GADA'06), to appear in LNCS, 2006.

F. Martinelli and M. Petrocchi. On relating and integrating two trust management languages. To appear in proc. of the 2nd International Workshop on Views On Designing Complex Architectures (VODCA'06). Sept. 2006, to appear in ENTCS.

F. Martinelli and I. Matteucci. Modeling, verification and synthesis of secure. Proc. 2nd International Workshop on Views On Designing Complex Architectures (VODCA'06). Sept. 2006, ENTCS, to appear.

F. Martinelli and M. Petrocchi. A uniform approach for the modeling of security and trust on protocols and services. To appear in proc. of the First International Workshop on Computer Security (ICS06). To appear in ENTCS.

Y. Lakhnech, L. Mazaré and B. Warinschi. Soundness of Symbolic Equivalence for Modular Exponentiation. Proc. 2nd Workshop on Formal and Computational Cryptography (FCC'06), Venice, Italy, July 2006.

R. Janvier, Y. Lakhnech and L. 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.

M. Daubignard, R. Janvier, Y. Lakhnech and L. 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.

L. Bozga, Y. Lakhnech, M. Périn Pattern-based abstraction for verifying secrecy in protocols In International Journal on Software Tools for Technology Transfer (STTT) vol. 8 Feb 2006.

L. Bozga, Cristian Ene, Y. Lakhnech A symbolic decision procedure for cryptographic protocols with time stamps. Journal of Logic and Algebraic Programming , Volume 65, Issue 1, p. 1-35, 2005.

R. Janvier, Y. Lakhnech, L. Mazaré. Completing the Picture: Soundness of Formal Encryption in the Presence of Active Adversaries In The European Symposium on Programming (ESOP'05). Edinburgh (Scotland) 2005

J. Courant, J-F. Monin. Defending the bank with a proof assistant In Sixth International IFIP WG 1.7 Workshop on Issues in the Theory of Security, pages 87 - 98, Vienna, March 2006. European Joint Conferences on Theory And Practice of Software.

R. Janvier, Y. Lakhnech, M. P□érin. Certification of Cryptographic Protocols by Abstract Model-Checking and Proof Concretization Workshop on Innovative Techniques for Certification of Embedded Systems, 2006, San Jose.

M. Abadi, M. Baudet and B. Warinschi. Guessing Attacks and the Computational Soundness of Static Equivalence. In Proceedings of the 9th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'06), Vienna, Austria, March 2006, LNCS 3921, pages 398-412. Springer.

S. Delaune, S. Kremer and M. D. Ryan. Coercion-Resistance and Receipt-Freeness in Electronic Voting. In Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06), Venice, Italy, July 2006, pages 28-39. IEEE Computer Society Press.

S. Delaune, S, Kremer and M. D. Ryan. Verifying Properties of Electronic Voting Protocols. In Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE'06), Cambridge, UK, June 2006, pages 45-52.

S. Delaune, P. Lafourcade, D. Lugiez and R. Treinen. Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or. In Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) - Part II, Venice, Italy, July 2006, LNCS 4052, pages 132-141. Springer.

F. Jacquemard, M. Rusinowitch and L. Vigneron. Tree automata with equality constraints modulo equational theories. In Proceedings of the 3rd International Joint Conference on Automated Reasoning (IJCAR'06), Seattle, Washington, USA, August 2006, LNAI 4130, pages 557-571. Springer-Verlag.

P. Lafourcade. Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption. In Proceedings of the 1st International Workshop on Security and Rewriting Techniques (SecReT'06), Venice, Italy, July 2006.

P. Lafourcade, D. Lugiez and R. Treinen. ACUNh: Unification and Disunification Using Automata Theory. In Proceedings of the 20th International Workshop on Unification (UNIF'06), Seattle, August 2006.

S. Delaune. Easy Intruder Deduction Problems with Homomorphisms. Information Processing Letters 97(6), pages 213-218, 2006.

V. Cortier, S. Delaune and P. Lafourcade. A Survey of Algebraic Properties Used in Cryptographic Protocols. Journal of Computer Security. 14(1), pages 1-43, 2006.

S. Delaune, S. Kremer and M. D. Ryan. Receipt-Freeness: Formal Definition and Fault Attacks (Extended Abstract). In Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005), Milan, Italy, September 2005.

2.2.3 Keynotes, Workshops, Tutorials

Keynote: On the use of formal models for proving cryptographic security notions. Special Session on Formal Approaches to Security.

Cork, Ireland, August 2006.

Veronique Cortier. Information-MFCSIT'06 conference,

Keynote: When reachability-based secrecy implies equivalence-based secrecy in security protocols.

Pisa, Italy, May 18th 2006.

Veronique Cortier. Artist 2 Workshop on Specification and Verification of Secure Embedded Systems.

Keynote: Deciding Protocol Insecurity with Rewriting Techniques.

S. Servolo, Venice – Italy, July 15, 2006

M. Rusinowitch. 1st International Workshop on Security and Rewriting Techniques.

Tutorial: Security protocols.

LORIA, Nancy, France July 3-7, 2006

M. Rusinowitch International School on Rewriting.

Tutuorial: Formal Verification of Cryptographic Protocols

Bordeaux, France, June 19-23, 2006.

Steve Kremer. MOdelling and VErifying parallel Processes (MOVEP'06)

http://movep.labri.fr/

Workshop: 4th International Workshop on Formal Aspects in Security and Trust.

Hamilton, Ontario, Canada, August 26-27 2006.

The workshop is co-located with Formal Methods 2006. Fabio Martinelli is a co-organizer of the event that fosters the research in security and trust management. The workshop received near 50 submissions and accepted 16 full papers. The papers will be published in LNCS. A special issue on a journal is also planned.

Workshop : Specification and Verification of Secure Embedded Systems

Pisa, Italy- May 18, 2005,

The workshop was co-located with iTrust2006, and was organized by Bruno Bouyssounouse, Sandro Etalle, Steve Kremer, Yassine Lakhnech, Fabio Martinelli and Marinella Petrocchi. The program included invited talks, regular talks and plenty of time for discussion. The workshop focused on the formal specification and verification of security properties, and in particular on the specification and formal verification of security protocols. Topics included: formal definition and verification of security properties, formal analysis and design of cryptographic protocols, modelling information flow, formal techniques for (mobile) code security, security in real-time/probabilistic systems. language-based security, and theory and application of policy languages and trust management. One of the goals of this open workshop was to bring together the part of the European community working on security.

Workshop: 2nd Workshop on Formal and Computational Cryptography (FCC 2006)

Venice, Italy - July 9, 2006.

http://www.lsv.ens-cachan.fr/FCC2006/ and http://hal.inria.fr/FCC2006

The workshop was co-located with ICALP'06 and was organized by Véronique Cortier and Steve Kremer. The workshop focuses on the relation between the symbolic (Dolev-Yao) model and the computational (complexity-theoretic) model. The workshop included 9 presentations followed by stimulating, technical discussions. With about 50 participants the workshop was the largest ICALP'06 affiliated workshop.

3. Future Work and Evolution

3.1 Problem to be Tackled over the next 18 months (Sept 2006 – Feb 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. As mentioned in section 1.5, this goal is made concrete in a threefold challenge:

1) The verification of more realistic protocols.

2) The verification of more realistic security properties.

3) Bridging the gap between the verification of security properties and trust management.

Concerning challenge (1), there are various problems we intend to tackle. First the verification of *group protocols:* nowadays, protocols often involve groups (whose size is not defined a priori) of participants. Typical examples of such protocols are group-key exchange protocols. Verifying such protocols is a major challenge, because the number of participants is a parameter. Moreover, new security properties emerge due to the fact that members can dynamically enter or leave a group. We wish to define a framework for defining and analysing such protocols and their related properties. Another problem we intend to tackle in challenge (1) is to lift the analysis of protocol properties to services properties: security protocols are often used in conjunction with other applications (e.g. access control) and may manipulate complex data (e.g. XML), in order to compose a service. We plan to address these service verification problems. Next to this topic, the problem of the verification of security properties should be broadened to include authentication protocols for mobile ad-hoc networks in the applied pi-calculus. Finally, we intend to develop a tool for the automatic verification of cryptographic APIs

Concerning challenge (2) Most automatically verifiable properties are reachability properties, such as secrecy and authentication. Anonymity properties and stronger versions of secrecy can be modelled elegantly using equivalence relations, such as observational equivalence in the applied pi calculus. We wish to define symbolic semantics of the applied pi calculus in terms of constraint systems and a corresponding symbolic observational equivalence relation. This should lead to new decidability and complexity results, as well as algorithms, for deciding this equivalence in the case of a bounded number of sessions and particular equational theories. A major advantage of equivalence based properties is that they are compositional. Within the same challenge, we are going to assess the usability of type inference algorithms for checking security properties: we intend to find and analyze a type inference algorithm for correspondence assertions in the spi-calculus and generalizing it to the applied pi-calculus. Further up in the goal line, we aim at implementing a tool that uses type inference for the analysis of cryptographic protocols.

Concerning challenge (3), we plan to define a complete and uniform framework for the specification of security protocols and trust management systems in complex, dynamic and open scenarios. The framework will be both supported by modelling and analysis tools as well as by effective implementations. A second problem that will be addressed in the coming months is the integration of rule-based and reputation based trust management systems.

The ongoing work on the individual tools will be continued. However, emphasis will also be made on evaluation of the tools through case studies in order to identify the most stable and mature versions with respect to integration.

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.

Year 3: develop compositional proof techniques for verifying services security properties, and for verifying group protocols.

Year 4: design monitoring procedures for ensuring trust in services execution**.**

3.3 *Indicators for Integration*

A critical issue concerning the development of verification tools and their acceptance by non-expert users is the choice of the specification language. This issue is even more delicate for cryptographic protocols because of the semantic subtleties of these programs. Indeed, these 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 (see for instance the proceedings of AsiaCrypt 2005) 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 made available a new tool for the Constraint Logic based Model-Checking of Security Protocols (CL-Atse). The tool is available at http://www.loria.fr/equipes/cassis/softwares/AtSe/. The system refers to the AVISPA intermediate format, which allows to interchange the specification with other verification tools. A second constraint based tool for the verification of security protocols in which the properties to be verified can be specified in a somewhat standard language (a dialect of LTL) is now at the stage of prototype.

The collaboration between Verimag, LSV and LORIA has been strengthened. There are common publications in preparation. Moreover, Laurent Mazaré (Verimag) has received a postdoctoral position at LSV starting from October 2006. There are two national projects involving LSV and Verimag dedicated to the verification of cryptographic protocols. Verimag and Trusted Logic are collaborating on the integration of the certification tools and methodology into Trusted Logic's commercial suite tool.

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.

- 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
- EDEN: Develop a methodology with tool support for the devlopement of application cetified at the highest assurance level of the Common Criteria.Partners: Axalto, 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.

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 Account: Accountability in Electronic Commerce Protocols http://dies.cs.utwente.nl/research/#account
- 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.

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.

3.5 *Internal reviewers*

We are thankful to the internal reviewers for their useful comments: Bruno Bouyssounouse, Pieter Hartel, Fabio Martinelli.