IN PARTNERSHIP WITH:
CNRS

Université de Franche-Comté

Université de Lorraine

Franche-Comté Electronique, Mécanique, Thermique et Optique-Sciences et Technologies

Activity Report 2013

Project-Team CASSIS

Combination of approaches to the security of infinite states systems

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
Nancy - Grand Est

THEME
Security and Confidentiality

Table of contents

Project-Team CASSIS

Keywords: Formal Methods, Safety, Security, Automated Theorem Proving, Cryptography, Protocols

Creation of the Project-Team: 2003 April 01.

1. Members

Research Scientists

Véronique Cortier [CNRS, Senior Researcher, HdR]
David Galindo-Chacon [CNRS, Junior Researcher]
Steve Kremer [Inria, Senior Researcher, HdR]
Christophe Ringeissen [Inria, Junior Researcher, HdR]
Michaël Rusinowitch [Team Leader, Inria, Senior Researcher, HdR]
Mathieu Turuani [Inria, Junior Researcher]

Faculty Members

Fabrice Bouquet [Univ Franche-Comté, Professor, HdR]
Frédéric Dadeau [Univ Franche-Comté, Associate Professor]
Alain Giorgetti [Univ Franche-Comté, Associate Professor]
Pierre-Cyrille Héam [Univ Franche-Comté, Professor, HdR]
Abdessamad Imine [Univ Lorraine, Associate Professor]
Olga Kouchnarenko [Deputy team leader, Univ Franche-Comté, Professor, HdR]
Laurent Vigneron [Univ Lorraine, Professor, HdR]

Engineers

Walid Belkhir [Inria, FP7 ALES FP 7 NESSOS project, until Aug 2013]
Stéphane Glondu [(50% Cassis team, 50% Caramel team)]
Minh Duc Huynh [Inria, Caisse des Dépôts et Consignations]
Franck Lebeau [Inria, Caisse des Dépôts et Consignations, until Nov 2013]
Julien Lorrain [Inria, from Oct 2013]
Ghazi Maatoug [Inria, Caisse des Dépôts et Consignations, from Feb 2013]
Thomas Sermier [Inria, OSEO Innovation, until Nov 2013]
Romain Sibre [Inria, from Nov 2013]

PhD Students

Hadrien Bride [Univ Franche-Comté, FEMTO-ST/DISC]
Kalou Cabrera [Univ Franche-Comté, project TASCCC]
Jérome Cantenot [Univ Franche-Comté, ATER]
Rémy Chrétien [ENS Cachan & LORIA, ANR Jeunes Chercheurs VIP (S. Delaune)]
Aloïs Dreyfus [Univ Franche-Comté,ATER]
Ivan Enderlin [Univ Franche-Comté, project FUI SQUASH]
Jean-Marie Gauthier [Univ Franche-Comté, Council of the Franche-Comté Region, FEMTO-ST/DISC]
Bao Thien Hoang [Univ Lorraine, project STREAMS]
Vincent Hugot [Univ Franche-Comté, DGA/Inria]
Robert Künnemann [ENS Cachan & LORIA, Inria]
Éric Le Morvan [Univ Lorraine, CNRS]
Houari Mahfoud [Univ Lorraine, Algerian grant]
Huu Hiep Nguyen [Univ Lorraine, Cordi-S, from Nov 2013]
Guillaume Scerri [ENS Cachan & LORIA, FP7 ERC ProSecure]
Elena Tushkanova [Univ Franche-Comté, ATER]
Cyrille Wiedling [Univ Lorraine, FP7 ERC ProSecure]

Post-Doctoral Fellow
Malika Izabachene [CNRS, FP7 ERC ProSecure]

Visiting Scientists
Paula Chocrón [Inria internship, 3 months, from Sep 2013]
Gemma Puig-Quer [CNRS internship, 6 months, from Sep 2013]
Gisela-Carla Rossi [Inria internship, 6 months, from Jun 2013]
Anisia Maria Magdalena Tudorescu [Inria internship, 3 months, from Mar 2013]

Administrative Assistant
Emmanuelle Deschamps [Inria]

2. Overall Objectives

2.1. Background

Cassis is a joint project between the *Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA - UMR 7503)* and *Laboratoire d'Informatique de l'Université de Franche-Comté (LIFC - FRE 2661)*.

The objective of the project is to design and develop tools to verify the safety of systems with an infinite number of states. The analysis of such systems is based on a symbolic representation of sets of states in terms of formal languages or logical formulas. Safety is obtained via automatic proof, symbolic exploration of models or test generation. These validation methods are complementary. They rely on the study of accessibility problems and their reduction to constraint solving.

An originality of the project is its focus on infinite systems, parameterized or large scale, for which each technique taken separately shows its limits. This is the case for example with protocols operating on topologies of arbitrary size (ring networks), systems handling data structures of any size (sets), or whose control is infinite (automata communicating through an unbounded buffer). Ongoing or envisioned applications concern embedded software (e.g., smart cards, automotive controllers), cryptographic protocols (IKE, SET, TLS, Kerberos) designed to ensure trust in electronic transactions, and distributed systems.

The problem of validating or verifying reactive systems is crucial because of the increasing number of security-sensitive systems. The failure of these critical systems can have dramatic consequences since they may be embedded in vehicle components, or they control power stations or telecommunication networks. Beside obvious security issues, the reliability of products whose destination is millions of end-users has a tremendous economical impact.

There are several approaches to system verification: automated deduction, reachability analysis or model-checking, and testing. These approaches have different advantages and drawbacks. Automated deduction can address practical verification, however it remains complex to handle and requires a lot of expertise and guidance from the user. Model-checking is exhaustive but must face combinatorial explosion and becomes problematic with large-size or infinite systems. Testing is fundamental for validating requirements since it allows the discovery of many errors. However, it is almost never exhaustive and therefore only leads to partial solutions. Hence we believe that these approaches should not be considered as competing but as complementary.

The goal of our project is to contribute to new combinations of these three verification techniques in a framework that would apply them in an industrial context. In particular we expect some breakthrough in the infinite-state verification domain by joint applications of deductive, model-checking and testing techniques.

2.2. Context

For verifying the security of infinite-state systems we rely on:

- different ways to express the safety, reachability or liveness properties of systems, linear-time or branching-time logics, and the application of abstraction or abstract interpretation;
- test generation techniques;
- the modeling of systems by encoding states as words, terms or trees and by representing infinite sets of states by languages. To each of these structures corresponds appropriate action families, such as transductions or rewritings.

Our goal is to apply these different approaches for ensuring the security of industrial systems by providing adequate methods and tools. In more details we aim at the following contributions (see the continuous lines in Figure 1):

1. verification of abstract models derived from existing systems;
2. test generation from the abstract model for validating the existing model;
3. cross-fertilization of the different validation techniques (deduction, model-checking, testing) by taking advantage of the complementary scopes and of their respective algorithmic contributions.

Let us mention that all these techniques comply with various development methodologies.

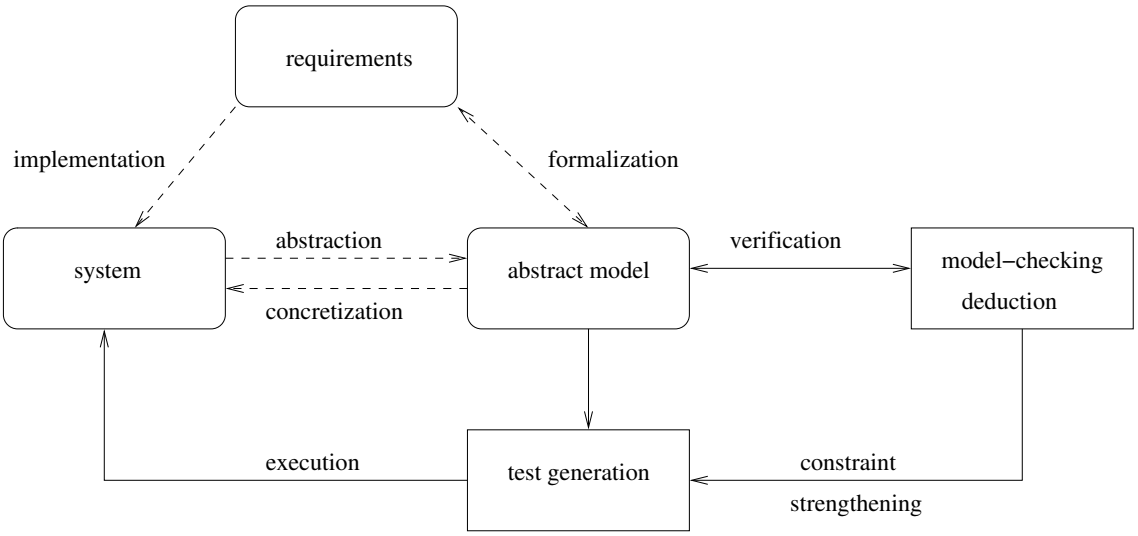

Figure 1. Software validation in Cassis.

2.3. Challenge

Verifying the safety of infinite-state systems is a challenge: nowadays algorithmic techniques only apply to very specific infinite-state systems. On the other hand the deductive approaches are good candidates to capture infinite system safety verification but are difficult to bring into operation and require a deep expertise. A solution consists of integrating several verification methods by combining, for example, theorem-proving and model-checking.

The behavior of infinite-state systems is expressed in various models by composing or iterating actions. One of the main problems with algorithmic techniques is to compute the effect of these actions on the initial state. This computation is called *reachability analysis*. The verification of safety properties as well as the automatic generation of test cases relies heavily on the accuracy of reachability analysis.

The transverse goal is to push away the limitations on the use of formal verification techniques, to ease their applications, and to let them scale-up.

1. For properties that can be checked by reachability analysis we have proposed models based on regular languages and rational transductions. We have completed them by designing algorithms for verifying a refinement relation between two models $\mathcal{S}$ and $\mathcal{T}$ [68]. This refinement relation when satisfied preserves the safety properties and therefore allows them to be inherited. We shall investigate this approach with other representations.
2. In order to generate boundary-value functional test cases, we abstract models as constrained states. These constraints are solved by a customized solver, called CLPS. The test cases are derived in two steps:
    1. partitioning of the formal model and extraction of boundary values;
    2. reachability graph exploration from constrained states in order to reach boundary values and generate state sequences (traces) as test cases with the oracle.

    After the generation phase, a concretization is used to produce the test drivers. Furthermore, the kernel of the engine allows one to perform specification animations in order to validate the model [72].
3. For the safety of infinite-state systems we have designed automated deduction tools based on term rewriting (*SPIKE*, *daTac*, *haRVey*) and an extensible and modular platform for detecting flaws and potential attacks on security protocols (*AVISPA*). The tools have been built on the modeling of systems by terms and rewrite rules. Our work with other models based on regular languages of words or trees and of transducers should complement these term rewriting models.

In order to address this challenge, we rely on complementary skills within the project. We believe that each of the three techniques will benefit from concepts and algorithms designed for the two others.

2.4. Highlights of the Year

- We have released the first version of *Belenios*, an electronic voting protocol based on a previous system, Helios. *Belenios* is an open-source voting system that offers transparent and verifiable elections. We have also signed a contract with a French company on electronic voting, Voxaly, to discuss their solution and a possible adaptation to *Belenios*' concepts.
- We have found a weakness in the biometric passports: under certain circumstances, it is possible to trace a passport holder, despite the existing security measures. Our flaw has been reported in the journals "Pour la Science" and "Journal du CNRS".

3. Research Program

3.1. Introduction

Our main goal is to design techniques and to develop tools for the verification of (safety-critical) systems, such as programs or protocols. To this end, we develop a combination of techniques based on automated deduction for program verification, constraint resolution for test generation, and reachability analysis for the verification of infinite-state systems [29].

3.2. Automated Deduction

The main goal is to prove the validity of assertions obtained from program analysis. To this end, we develop techniques and automated deduction systems based on rewriting and constraint solving. The verification of recursive data structures relies on inductive reasoning or the manipulation of equations and it also exploits some form of reasoning modulo properties of selected operators (such as associativity and/or commutativity).

Rewriting, which allows us to simplify expressions and formulae, is a key ingredient for the effectiveness of many state-of-the-art automated reasoning systems. Furthermore, a well-founded rewriting relation can be also exploited to implement reasoning by induction. This observation forms the basis of our approach to inductive reasoning, with high degree of automation and the possibility to refute false conjectures.

The constraints are the key ingredient to postpone the activity of solving complex symbolic problems until it is really necessary. They also allow us to increase the expressivity of the specification language and to refine theorem-proving strategies. As an example of this, the handling of constraints for unification problems or for the orientation of equalities in the presence of interpreted operators (e.g., commutativity and/or associativity function symbols) will possibly yield shorter automated proofs.

Finally, decision procedures are being considered as a key ingredient for the successful application of automated reasoning systems to verification problems. A decision procedure is an algorithm capable of efficiently deciding whether formulae from certain theories (such as Presburger arithmetic, lists, arrays, and their combination) are valid or not. We develop techniques to build and to combine decision procedures for the domains which are relevant to verification problems. We also perform experimental evaluation of the proposed techniques by combining propositional reasoning (implemented by means of Boolean solvers, e.g. SAT solvers) and decision procedures to get solvers for the problem of Satisfiability Modulo Theories (SMT).

3.3. Synthesizing and Solving Constraints

Applying constraint logic programming technology in the validation and verification area is currently an active way of research. It usually requires the design of specific solvers to deal with the description language's vocabulary. For instance, we are interested in applying a solver for set constraints [6] to evaluate set-oriented formal specifications. By evaluation, we mean the encoding of the formal model into a constraint system, and the ability for the solver to verify the invariant on the current constraint graph, to propagate preconditions or guards, and to apply a substitution calculus on this graph. The constraint solver is used for animating specifications and automatically generating abstract test cases.

3.4. Rewriting-based Safety Checking

Invariant checking and strenghtening is the dual of reachability analysis, and can thus be used for verifying safety properties of infinite-state systems. In fact, many infinite-state systems are just parameterized systems which become finite state systems when parameters are instantiated. Then, the challenge is to automatically discharge the maximal number of proof obligations coming from the decomposition of the invariance conditions. For parameterized systems, we are interested in a deductive approach where states are defined by first order formulae with equality, and proof obligations are checked by SMT solvers.

4. Application Domains

4.1. Verification of Security Protocols

Security protocols such as SET, TLS and Kerberos, are designed for establishing the confidence of electronic transactions. They rely on cryptographic primitives, the purpose of which is to ensure integrity of data, authentication or anonymity of participants, confidentiality of transactions, etc.

Experience has shown that the design of those protocols is often erroneous, even when assuming that cryptographic primitives are perfect, i.e., that an encoded message cannot be decrypted without the appropriate key. An intruder can intercept, analyze and modify the exchanged messages with very few computations and therefore, for example, generate important economic damage.

Analyzing cryptographic protocols is complex because the set of configurations to consider is very large, and can even be *infinite*: one has to consider any number of sessions, any size of messages, sessions interleaving, some algebraic properties of encryption or data structures.

Our objective is to automatize as much as possible the analysis of protocols starting from their specification. This consists in designing a tool that is easy to use, enables the specification of a large number of protocols thanks to a standard high-level language, and can either look for flaws in a given protocol or check whether it satisfies a given property. Such a tool is essential for verifying existing protocols, but also for helping in designing new ones. For our tool to be easy to use, it has to provide a graphical interface allowing a user to easily perform push-button verification.

Our tools for verifying security protocols are available as components of the AVISPA platform. As an extension of the AVISPA specification language, we are working on a new environment called *CASRUL* for handling more general protocols like e-business protocols for example.

4.2. Automated Boundary Testing from Formal Specifications

We have introduced a new approach for test generation from set-oriented formal specifications: the BZ-TT method. This method is based on Constraint Logic Programming (CLP) techniques. The goal is to test every operation of the system at every boundary state using all input boundary values of that operation. It has been validated in several industry case studies for smart card OS and application validation (GSM 11-11 standard [69] and Java Card Virtual Machine Transaction mechanism [71]), information system and for embedded software [80].

This test generation method can be summed up as follows: from the formal model, the system computes boundary values to create boundary states; test cases are generated by traversal of the state space with a preamble part (sequences of operations from the initial state to a boundary state), a body part (critical invocations), an identification part (observation and oracle state computation) and a post-amble part (return path to initial or boundary state). Then, an executable test script file is generated using a test pattern and a table of correspondence between abstract operations (from the model) and concrete ones. This approach differs in several main points from previous works (e.g. [76]): first, using boundary goals as test objectives avoids the complete construction of the reachability graph; second, this process is fully automated and the test engineer could just drive it at the boundary value computation level or for the path computation.

The BZ-TT method is fully supported by the BZ-Testing-Tools tool-set. This environment is a set of tools dedicated to animation and test cases generation from B, Z or State-Chart formal specifications. It is based on the CLPS constraint solver, able to simulate the execution of the specification. By execution, we mean that the solver computes a so-called constrained state by applying the pre- and post-condition of operations. A constrained state is a constraint store where state variables and also input and output variables support constraints.

One orientation of the current work is to go beyond the finiteness assumption limitations by using symbolic constraint propagation during the test generation process. Second orientation is to extend the result to object oriented specifications as UML/OCL.Third orientation is to extend the coverage of method for security aspect.

4.3. Program Debugging and Verification

Catching bugs in programs is difficult and time-consuming. The effort of debugging and proving correct even small units of code can surpass the effort of programming. Bugs inserted while “programming in the small” can have dramatic consequences for the consistency of a whole software system as shown, e.g., by viruses which can spread by exploiting buffer overflows, a bug which typically arises while coding a small portion of

code. To detect this kind of errors, many verification techniques have been put forward such as static analysis and software model checking.

Recently, in the program verification community, there seems to be a growing demand for more declarative approaches in order to make the results of the analysis readily available to the end user. To meet this requirement, a growing number of program verification tools integrate some form of theorem proving.

The goals of our research are twofold. First, we perform theoretical investigations of various combinations of propositional and first-order satisfiability checking in order to automate the theorem proving activity required to solve a large class of program analysis problems which can be encoded as first-order formulae. Second, we experimentally investigate how our techniques behave on real problems in order to make program analysis more precise and scalable. Building tools capable of providing a good balance between precision and scalability is one of the crucial challenges to transfer theorem proving technology to the industrial domains.

4.4. Verification of Web Services

Driven by rapidly changing requirements and business needs, IT systems and applications are undergoing a paradigm shift: components are replaced by services, distributed over the network, and composed and reconfigured dynamically in a demand-driven way into service-oriented architectures.Exposing services in future network infrastructures means a wide range of trust and security issues need to be adressed. Solving them is extremely hard since making the service components trustworthy is not sufficient: composing services leads to new subtle and dangerous vulnerabilities due to interference between component services and policies, the shared communication layer, and application functionality. Thus, one needs validation of both the service components and their composition into secure service architectures. In this context, there is an obvious need of applying formal methods. Our project aims at applying our proof and constraint solving techniques to reason on web services. More precisely, we focus on the composition problem in the presence of security policies.

4.5. Model-Checking of Collaborative Systems

Collaborative systems consitute a class of distributed systems where real human interactions are predominant. In these systems, users at geographically distributed sites interact by simultaneously manipulating shared objects like, text documents, XML trees, filesystems, etc. To improve data availablity, the shared objects are replicated so that the users update their local replicas and exchange their updates between them. One of the main challenges here is how to ensure the data consistency when the updates are executed in arbitrary orders at different replicas. Operational Transformation (OT) is an optimistic technique which has been proposed to overcome the consistency problem. This technique consists of an application-dependent protocol to enforce the out-of-order execution of updates even though these updates do not naturally commute. The data consistency relies crucially on the correctness of OT protocols whose proof is extremely hard. Indeed, possibly infinitely many cases should be tested. Our research work aims at applying symbolic model-checking techniques to automatically verify OT protocols. Most importantly, we are interested in finding under which conditions the model-checking problem can be reduced to a finite-state model.

5. Software and Platforms

5.1. Protocol Verification Tools

Participants: Stéphane Glondu, Pierre-Cyrille Héam, Olga Kouchnarenko, Steve Kremer, Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

5.1.1. AVISPA

Cassis has been involved in the European project AVISPA, which has resulted in the distribution of a tool for automated verification of security protocols, named *AVISPA* Tool. It is freely available on the web [1] and it is well supported. The *AVISPA* Tool compares favourably to related systems in scope, effectiveness, and performance, by (i) providing a modular and expressive formal language for specifying security protocols and properties, and (ii) integrating 4 back-ends that implement automatic analysis techniques ranging from *protocol falsification* (by finding an attack on the input protocol) to *abstraction-based verification* methods for both finite and infinite numbers of sessions.

5.1.2. CL-AtSe

We develop, as a back-end of *AVISPA*, *CL-AtSe*, a Constraint Logic based Attack Searcher for cryptographic protocols. The *CL-AtSe* approach to verification consists in a symbolic state exploration of the protocol execution, for a bounded number of sessions. This necessary restriction (for decidability, see [77]) allows *CL-AtSe* to be correct and complete. Each protocol step is represented by a constraint on the protocol state, used to check for reachability of the next state. *CL-AtSe* includes a proper handling of sets, choice points, specification of any attack states through a language for expressing e.g. secrecy, authentication, fairness, or non-abuse freeness, advanced protocol simplifications and optimizations to reduce the problem complexity, and protocol analysis modulo the algebraic properties of cryptographic operators such as XOR (exclusive or) and Exp (modular exponentiation).

CL-AtSe has been successfully used [65] to analyse France Telecom R&D, Siemens AG, IETF, or Gemalto protocols in funded projects. It is also employed by external users, e.g., from the AVISPA's community. Moreover, *CL-AtSe* achieves very good analysis times, comparable and sometimes better than state-of-the art tools in the domain (see [82] for tool details and precise benchmarks).

Cl-Atse has been enhanced in various ways. In particular, the tool fully supports Aslan semantics introduced in [63], including Horn Clauses (for intruder-independent deductions, e.g. for credential management), and LTL-based security properties. Also, bug information and correction are processed through a bugzilla server, and online analysis and orchestration are available on our team server (https://cassis.loria.fr). Cl-Atse supports negative constraints on the intruder's knowledge [66]. This extension of Cl-Atse allows us to reduce drastically the orchestrator's processing times. It has also been used to model e.g. separation of duties and non-disclosure policies. We have also extended the syntax and semantics of ASLan to better model lists of undefined length, directly inside messages. Cl-AtSe tool now supports membership predicates, deletion operators ans so on for managing these lists, and offers a first reference implementation for other tools in Avantssar. In particular, the ASLan translator has been updated by our partners.

5.1.3. Akiss

We develop the *Akiss* (Active Knowledge in Security Protocols) tool for verifying indistinguishability properties in cryptographic protocols. Indistinguishability properties are essential in formal verification of cryptographic protocols. They are needed to model anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, which can be conveniently modeled using process equivalences. *Akiss* implements a procedure to verify equivalence properties for a bounded number of sessions of cryptographic protocols. As in the applied pi-calculus, the protocol specification language is parametrized by a first-order sorted term signature and an equational theory which allows formalization of algebraic properties of cryptographic primitives. *Akiss* is able to verify trace equivalence for determinate cryptographic protocols. On determinate protocols, trace equivalence coincides with observational equivalence which can therefore be automatically verified for such processes. When protocols are not determinate *Akiss* can be used for both under- and over-approximations of trace equivalence, which proved successful on several examples. The procedure can handle a large set of cryptographic primitives, namely those that can be modeled by an optimally reducing convergent rewrite system.

[1] http://www.avispa-project.org

The underlying procedure is based on a fully abstract modelling of the traces of a bounded number of sessions of the protocols into first-order Horn clauses on which a dedicated resolution procedure is used to decide equivalence properties. Although termination of the resolution procedure has not been proved, the procedure has been effectively tested on examples, some of which are outside the scope of other existing tools, including checking anonymity in several electronic voting protocols.

Recent developments include the possibility for checking everlasting indistinguishability properties. This feature was added when analyzing everlasting privacy properties in electronic voting protocols. We are currently working on a generalization of the procedure to allow associative-commutative operators and in particular a re-design of the resolution procedure for allowing analysis of protocols that use exclusive or. Expected case studies for this development include unlinkability in RFID protocols.

The *Akiss* tool is freely available at https://github.com/ciobaca/akiss.

5.1.4. Belenios

In collaboration with the Caramel team, we develop an open-source private and verifiable electronic voting protocol, named *Belenios*. Our system is an evolution of an existing system, Helios, developed by Ben Adida, and used e.g. by UCL and the IACR association in real elections. The main differences with Helios are the following ones:

- In Helios, the ballot box publishes the encrypted ballots together with their corresponding voters. This raises a privacy issue in the sense that whether someone voted or not shall not necessarily be publicized on the web. Publishing this information is in particular forbidden by the CNIL's recommendations. Belenios no longer publishes voters' identities, still guaranteeing the correctness of the tally.
- Helios is verifiable except that one has to trust that the ballot box will not add ballots. The addition of ballots is particularly hard to detect as soon as the list of voters is not public. We have therefore introduced an additional authority that provides credentials that the ballot box can verify but not forge.

This new version has been implemented by Stéphane Glondu and has been tested in July 2013 in a mock election in the teams Cassis and Caramel.

In a first step, *Belenios* has been implemented as an extension of existing Helios system. However, the existing software development of Helios is large and its security becomes difficult to assess. We have therefore re-implemented entirely the code of the bulletin box, yielding a now independent software [2].

In Helios as well as *Belenios*, votes are encrypted using the public key of the election. To ensure privacy, the corresponding decryption key is not known to anyone. Instead, several authorities detain a share of it. For robustness reasons (and as recommended by the CNIL), it is important to be able to decrypt even if some of the authorities are missing. We have implemented the threshold decryption scheme that we have proposed [40]. This implementation is currently available only within the Helios system and we plan to integrate it to *Belenios* in the next months.

5.2. Testing Tools

Participants: Fabrice Bouquet, Frédéric Dadeau, Kalou Cabrera.

5.2.1. Hydra

Hydra is an Eclipse-like platform, based on Plug-ins architecture. Plug-ins can be of five kinds: *parser* is used to analyze source files and build an intermediate format representation of the source; *translator* is used to translate from a format to another or to a specific file; *service* denotes the application itself, i.e. the interface with the user; *library* denotes an internal service that can be used by a service, or by other libraries; *tool* encapsulates an external tool. The following services have been developed so far:

[2] http://belenios.gforge.inria.fr/

- BZPAnimator: performs the animation of a BZP model (a B-like intermediate format);
- Angluin: makes it possible to perform a machine learning algorithm (à la Angluin) in order to extract an abstraction of a system behavior;
- UML2SMT: aims at extracting first order logic formulas from the UML Diagrams and OCL code of a UML/OCL model to check them with a SMT solver.

These services involve various libraries (sometimes reusing each other), and rely on several *tool* plug-ins that are: SMTProver (encapsulating Z3 solver), PrologTools (encapsulating CLPS-B solver), Grappa (encapsulating a graph library). We are currently working on transferringthe existing work on test generation from B abstract machines, JML, and statecharts using constraint solving techniques.

5.2.2. jMuHLPSL

jMuHLPSL [9] is a mutant generator tool that takes as input a verified HLPSL protocol, and computes mutants of this protocol by applying systematic mutation operators on its contents. The mutated protocol then has to be analyzed by a dedicated protocol analysis tool (here, the AVISPA tool-set). Three verdicts may then arise. The protocol can still be *safe*, after the mutation, this means that the protocol is not sensitive to the realistic "fault" represented by the considered mutation. This information can be used to inform the protocol designers of the robustness of the protocol w.r.t. potential implementation choices, etc. The protocol can also become *incoherent*, meaning that the mutation introduced a functional failure that prevents the protocol from being executed entirely (one of the participants remains blocked in a given non-final state). The protocol can finally become *unsafe* when the mutation introduces a security flaw that can be exploited by an attacker. In this case, the AVISPA tool-set is able to compute an attack-trace, that represents a test case for the implementation of the protocol. If the attack can be replayed entirely, then the protocol is not safe. If the attack can not be replayed then the implementation does not contain the error introduced in the original protocol.

The tool is written in Java, and it is freely available at: http://members.femto-st.fr/sites/femto-st.fr.frederic-dadeau/files/content/pub/jMuHLPSL.jar.

5.3. Collaborative Tools

Participant: Abdessamad Imine.

The collaborative tools allow us to manage collaborative works on shared documents using flexible access control models. These tools have been developed in order to validate and evaluate our approach on combining collaborative edition with optimistic access control.

5.3.1. P2PEdit

This prototype is implemented in Java and supports the collaborative editing of HTML pages and it is deployed on P2P JXTA platform [3]. In our prototype, a user can create a HTML page from scratch by opening a new collaboration group. Other users (peers) may join the group to participate in HTML page editing, as they may leave this group at any time. Each user can dynamically add and remove different authorizations for accessing to the shared document according the contribution and the competence of users participating in the group. Using JXTA platform, users exchange their operations in real-time in order to support WYSIWIS (What You See Is What I See) principle. Furthermore, the shared HTML document and its authorization policy are replicated at the local memory of each user. To deal with latency and dynamic access changes, an optimistic access control technique is used where enforcement of authorizations is retroactive.

5.3.2. P2PCalendar

To extend our collaboration and access control models to mobile devices, we implemented a shared calendar on iPhone OS which is decentralized and scalable (i.e. it can be used over both P2P and ad-hoc networks). This application aims to make a collaborative calendar where users can simultaneously modify events (or appointements) and control access on events. The access rights are determined by the owner of an event. The owner decides who is allowed to access the event and what privileges they have. Likewise to our previous tool, the calendar and its authorization policy are replicated at every mobile device.

[3] http://www.sun.com/software/jxta/

5.4. Other Tools

Several software tools described in previous sections are using tools that we have developed in the past. For instance BZ-TT uses the set constraints solver CLPS. Note that the development of the SMT prover haRVey has been stopped. The successor of haRVey is called veriT and is developed by David Déharbe (UFRN Natal, Brasil) and Pascal Fontaine (Veridis team). We have also developed, as a second back-end of *AVISPA*, TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols), an automata based tool dedicated to the validation of security protocols for an unbounded number of sessions.

6. New Results

6.1. Automated Deduction

We develop general techniques which allow us to re-use available tools in order to build a new generation of solvers offering a good trade-off between expressiveness, flexibility, and scalability. We focus on the careful integration of combination techniques and rewriting techniques to design decision procedures for a wide range of verification problems.

6.1.1. Building and verifying decision procedures

Participants: Alain Giorgetti, Olga Kouchnarenko, Christophe Ringeissen, Elena Tushkanova.

We have developed a methodology to build decision procedures by using superposition calculi which are at the core of equational theorem provers. In [14], we have developed automated deduction techniques to prove properties about these superposition-based decision procedures. To this aim, we have further investigated the use of schematic superposition, to check the termination and the combinability of superposition-based procedures. We have worked on the development of a framework for specifying and verifying superposition-based procedures. We have designed an implementation in Maude of the schematic superposition calculus. Thanks to this implementation we automatically derive termination of superposition for a couple of theories of interest in verification.

Until now, schematic superposition was only studied for standard superposition. In [53], [55], we introduce a schematic superposition calculus modulo a fragment of arithmetics, namely the theory of Integer Offsets. This new schematic calculus is used to prove the decidability of the satisfiability problem for some theories extending Integer Offsets. We illustrate our theoretical contribution on theories representing extensions of classical data structures, e.g., lists and records. Our Maude-based implementation has been extended to incorporate this new schematic superposition calculus modulo Integer Offsets. It enables automatic decidability proofs for theories of practical use.

6.1.2. Hierarchical combination of unification procedures

Participant: Christophe Ringeissen.

In [45], [54], a novel approach is described for the combination of unification algorithms for two equational theories which share function symbols. We are able to identify a set of restrictions and a combination method such that if the restrictions are satisfied the method produces a unification algorithm for the union of non-disjoint equational theories. Furthermore, we identify a class of theories satisfying the restrictions. The critical characteristics of the class is the hierarchical organization and the shared symbols being restricted to "inner constructors". Our approach can be applied to theories used for the analysis of protocols. The property of having an inner constructor in one side of an equality is common in the use of exponentiation in Diffie-Hellman inspired key agreement protocols. We are working on considering additional hierarchical theories. A possible candidate theory is a partial theory of Cipher Block Chaining.

6.1.3. Unification modulo equational theories of cryptographic primitives

Participant: Michaël Rusinowitch.

Some attacks exploit in a clever way the interaction between protocol rules and algebraic properties of cryptographic operators. In [74], we provide a list of such properties and attacks as well as existing formal approaches for analyzing cryptographic protocols under algebraic properties.

We have further investigated unification problems related to the Cipher Block Chaining (CBC) mode of encryption. We first model chaining in terms of a simple, convergent, rewrite system over a signature with two disjoint sorts: list and element. The 2-sorted convergent rewrite system is then extended into one that captures a block chaining encryption-decryption mode at an abstract level, (using no AC-symbols); unification modulo this extended system is shown to be decidable [15].

6.2. Security Protocol Verification

The design of cryptographic protocols is error-prone. Without a careful analysis, subtle flaws may be discovered several years after the publication of a protocol, yielding potential harmful attacks. In this context, formal methods have proved their interest for obtaining good security guarantees. Many analysis techniques have been proposed in the literature [70]. We have edited a book [62] where each chapter presents an important and now standard analysis technique. We develop new techniques for richer primitives, wider classes of protocols and higher security guarantees. In Section 6.4.3 we consider derived testing techniques for verifying protocol implementations.

6.2.1. Voting protocols

Participants: Véronique Cortier, David Galindo-Chacon, Stéphane Glondu, Malika Izabachene, Steve Kremer, Cyrille Wiedling.

Voting is a cornerstone of democracy and many voting systems have been proposed so far, from old paper ballot systems to purely electronic voting schemes. Although many works have been dedicated to standard protocols, very few address the challenging class of voting protocols. We have studied several protocols that are currently in use:

- Helios is an open-source web-based end-to-end verifiable electronic voting system, used e.g. by UCL and the IACR association in real elections. One main advantage of Helios is its verifiability, up-to the ballot box (a dishonest ballot box may add ballots). We have defined a variant of Helios, named Belenios, that prevents from ballot stuffing, even against a dishonest ballot box. Our approach consists in introducing an additional authorities that provides credentials that the ballot box can verify but not forge. This new version has been implemented by Stéphane Glondu and has been tested in a mock election in the teams Cassis and Caramel.
  We have proved computational security for both ballot secrecy and full verifiability (due to our credentials). Helios, as well as Belenios, makes use of threshold decryption, to ensure that decryption keys are distributed among several authorities, yet allowing decryption even some of the authorities are missing. We have provided a fully distributed (with no dealer) threshold cryptosystem suitable for the Helios voting system (in particular, suitable to partial decryption), and prove it secure under the Decisional Diffie-Hellman assumption [40]. Ballot privacy of Belenios then follows from ballot privacy of Helios. For full verifiability, we had first to adapt existing definitions of verifiability in the case of a corrupted ballot box and then prove verifiability of Helios [60].
- The Section 07 of CNRS (now split into Section 06 and Section 07) has proposed a voting protocol for Face-to-Face meetings to enhanced the verifiability of an election run through electronic devices. We have formally modeled this protocol and proved both ballot secrecy and verifiability [32].

Security based on cryptography relies on the fact that certain operations (such as decrypting) are computationally infeasible. However, e-voting protocols should also guarantee privacy in the future, when computers will have an increased computational power and will be able e.g. to break nowadays keys. Such privacy in the future is called *everlasting privacy* and we have proposed a definition of *practical everlasting privacy* [31]. As an illustration, we show that several variants of Helios (including Helios with Pedersen commitments) and a protocol by Moran and Naor achieve practical everlasting privacy, using the ProVerif and the AKiSs tools, which we had to adapt to cope with everlasting privacy.

We have written a popularization science paper on e-voting in Interstices[4].

6.2.2. Other families of protocols

Participants: Véronique Cortier, Steve Kremer, Robert Künnemann, Cyrille Wiedling.

Securing routing Protocols. The goal of routing protocols is to construct valid routes between distant nodes in the network. If no security is used, it is possible for an attacker to disorganize the network by maliciously interacting with the routing protocols, yielding invalid routes to be built. We have proposed a new model and an associated decision procedure to check whether a routing protocol can ensure that honest nodes only accept valid routes, even if one of the nodes of the network is compromised. This result has been obtained for a bounded number of sessions, adapting constraint solving techniques to node topologies as well as some families of recursive tests, used in routing protocols [16].

Security APIs. In some systems, it is not possible to trust the host machine on which sensitive codes are executed. In that case, security-critical fragments of a program should be executed on some tamper resistant device (TRD), such as a smartcard, USB security token or hardware security module (HSM). The exchanges between the trusted and the untrusted infrastructures are ensured by special kind of API (Application Programming Interface), that are called *security APIs*. We have designed a generic API for key-management based on key hierarchy [23], that can self-recover from corruption of arbitrary keys, provided the number of corrupted, active keys is smaller than some threshold. In [50], we propose a universally composable key management functionality and show how to achieve a secure, distributed implementation on TRDs. We are currently also working on automated verification of security APIs (and more generally protocols that require global mutable state). A tool implementation using the tamarin prover as a backend is currently in progress.

6.2.3. Automated verification of indistinguishability properties.

Participants: Rémy Chrétien, Véronique Cortier, Stéphane Glondu, Steve Kremer.

New emerging classes of protocols such as voting protocols often require to model less classical security properties, such as anonymity properties, strong versions of confidentiality and resistance to offline guessing attacks. Many of these properties can be modelled using the notion of indistinguishability by an adversary, which can be conveniently modeled using process equivalences.

Static case. The YAPA tool [17] can check static equivalence for convergent equational theories. It is proved to terminate for a wide class of equational theories that includes subterm convergent theories (e.g. encryption, signatures, pairing and hash) and layered convergent theories (e.g. blind signatures). The procedure is generic in the sense that it remains sound and complete (but may not terminate) for any convergent theory. It has been implemented in the YAPA tool[5].

Active case. We have shown that, for arbitrary equational theories, verifying indistinguishability properties such as trace equivalence in security protocols amounts to deciding the equivalence of constraint systems, i.e., checking whether they have the same set of solutions [20]. When considering the equational theory corresponding to the standard primitives, Vincent Cheval has proposed a decision procedure for checking equivalence of set constraints, which yields a procedure for checking trace equivalence [73]. We have extended this decision procedure to the case where the attacker can observe the *length* of messages [37]. This yields the discovery of a new attack on the biometric passport. This attack has been implemented and successfully tested on a small set of passports. This attack is explained in details in a webpage[6] and has obtained some press coverage.

Active case, unbounded number of sessions. Rémy Chrétien has started a PhD on deciding trace equivalence for an unbounded number of sessions. He has shown that for some classes of protocols, decidability of trace equivalence can be reduced to equivalence of deterministic pushdown automata [38]. Equivalence of deterministic pushdown automata is decidable [81] and the corresponding decision procedure is currently implemented by Géraud Senizergues. Based on his tool, we are developing a tool for automatically checking equivalence, for an unbounded number of sessions.

[4] https://interstices.info/jcms/int_68258/vote-par-internet
[5] http://www.lsv.ens-cachan.fr/~baudet/yapa/
[6] http://www.loria.fr/ glondu/epassport/attack-lengths.html

6.2.4. Securely Composing Protocols

Participants: Véronique Cortier, Steve Kremer, Éric Le Morvan.

Protocols are often built in a modular way. For example, authentication protocols may assume pre-distributed keys or may assume secure channel. However, when an authentication protocol has been proved secure assuming pre-distributed keys, there is absolutely no guarantee that it remains secure when executing a real protocol for distributing the keys. How the security of these protocols can be combined is an important issue that is studied in the PhD thesis recently started by Éric Le Morvan.

A related problem arises when several protocols use the same secrets, e.g. the same keys. While each protocol may be proved secure in isolation, the protocols may become insecure when executed in parallel. In [21] we study whether password protocols can be safely composed, even when a same password is reused. It seems indeed unrealistic to suppose that users do not re-use the same password for different applications. More precisely, we present a transformation which maps a password protocol that is secure for a single protocol session (a decidable problem) to a protocol that is secure for an unbounded number of sessions. Our result provides an effective strategy to design secure password protocols: (i) design a protocol intended to be secure for one protocol session; (ii) apply our transformation and obtain a protocol which is secure for an unbounded number of sessions. Our technique also applies to compose different password protocols allowing us to obtain both inter-protocol and inter-session composition.

6.2.5. Soundness of the Dolev-Yao Model

Participants: Véronique Cortier, Guillaume Scerri.

All the previous results rely on symbolic models of protocol executions in which cryptographic primitives are abstracted by symbolic expressions. This approach enables significantly simple and often automated proofs. However, the guarantees that it offers have been quite unclear compared to cryptographic models that consider issues of complexity and probability. A somewhat recent line of research consists in identifying cases where it is possible to obtain the best of both cryptographic and formal worlds: fully automated proofs and strong, clear security guarantees.

A first approach consists in proving that symbolic models (as the ones studied on the previous sections) are actually *sound* w.r.t. cryptographic models, provided the primitives satisfy some (strong) security properties. Soundness result are usually established for some set of cryptographic primitives and extending the result to encompass new primitives typically requires redoing most of the work. In [35], we propose a notion of computational soundness, amenable to modular extensions. Specifically, we prove that a deduction sound implementation of some arbitrary primitives can be extended to include all standard primitives (asymmetric ans symmetric encryption, public data-structures - e.g. pairings or list, signatures, MACs, and hashes) without repeating the original proof effort. Furthermore, our notion of soundness concerns cryptographic primitives in a way that is independent of any protocol specification language.

Such soundness results require however strong hypotheses on the implementation. For example, primitives must be tagged to avoid confusion between e.g. pairs and encryption. Gergei Bana and Hubert Comon have proposed a new framework [67] where the symbolic model now specifies what an attacker *cannot* do instead of specifying what it can do. Checking protocols security can then be reduced to checking inconsistency of some set of first order formula. During his PhD, Guillaume Scerri studies how to develop a (polynomial) decision procedure for deciding consistency of sets of formulas, for some class of formulas corresponding to security protocols [39].

6.3. Model-based Verification

We have investigated extensions of regular model-checking to new classes of rewrite relations on trees. We have studied specification and proof of modular imperative programs.

6.3.1. Verification of Linear Temporal Patterns over Finite and Infinite Traces

Participants: Pierre-Cyrille Héam, Vincent Hugot, Olga Kouchnarenko.

In the regular model-checking framework, reachability analysis can be guided by temporal logic properties, for instance to achieve the counter example guided abstraction refinement (CEGAR) objectives. A way to perform this analysis is to translate a temporal logic formula expressed on maximal rewriting words into a "rewrite proposition" – a propositional formula whose atoms are language comparisons, and then to generate semi-decision procedures based on (approximations of) the rewrite proposition. In [13] we have investigated suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation, and we have proposed a general scheme providing exact results for a fragment of LTL corresponding mainly to safety formulæ, and approximations for a larger fragment.

6.3.2. Approximations Techniques for Regular Model-Checking

Participants: Aloïs Dreyfus, Pierre-Cyrille Héam, Olga Kouchnarenko.

We address the following general problem of regular model-checking: decide whether $R^*(L) \cap L_p = \varnothing$ where R^* is the reflexive and transitive closure of a successor relation R, and L and L_p are both regular tree languages. Considering a relation R on finite words and a regular language L encoding the initial configurations of a system, the set $R^*(L)$ of accessible words is not necessarily regular. Therefore, a way to verify safety properties is to over-approximate the set of reachable words by a regular language. In [42], we develop new efficient approximation techniques based on syntactic criteria. When these syntactic over-approximations are too coarse, we propose CEGAR-like techniques to refine them using counter-examples. The approach has been successfully applied to verify mutual exclusion protocols.

6.4. Model-based Testing

Our research in Model-Based Testing (MBT) aims to extend the coverage of tests. The coverage refers to several artefacts: model, test scenario/property, and code of the program under test. The test generation uses various underlying techniques such as symbolic animation of models [75], or symbolic execution of programs by means of dedicated constraints, SMT solvers, or model-checkers.

6.4.1. Automated Test Generation from Behavioral Models

Participants: Fabrice Bouquet, Kalou Cabrera, Jérome Cantenot, Frédéric Dadeau, Jean-Marie Gauthier, Julien Lorrain.

We have developed an original model-based testing approach that takes a behavioural view (modelled in UML) of the system under test and automatically generates test cases and executable test scripts according to model coverage criteria. We continue to extend this result to SysML specifications for validating embedded systems [30]. To allow the test generation from SysML models, in [47] we study the transformation into a low level language suitable for hardware specification.

In the context of software evolution, we have worked on exploiting the evolution of requirements in order to classify test sequences, and precisely target the parts of the system impacted by this evolution. We have proposed to define the life cycle of a test via three test classes: (i) Regression, used to validate that unimpacted parts of the system did not change, (ii) Evolution, used to validate that impacted parts of the system correctly evolved, and (iii) Stagnation, used to validate that impacted parts of the system did actually evolve. The associated algorithms are under implementation in a dedicated prototype already used in the SecureChange European project.

6.4.2. Scenario-Based Verification and Validation

Participants: Fabrice Bouquet, Kalou Cabrera, Frédéric Dadeau.

Test scenarios represent an abstract test case specification that aims at guiding the model animation in order to produce relevant test cases. Contrary to the previous section, this technique is not fully automated since it requires the user to design the scenario, in addition to the model.

We have designed a scenario based testing language for UML/OCL that can be either connected to a model animation engine or to a symbolic animation engine, based on a set-theoretical constraint solver [75]. In the context of the ANR TASCCC project, we investigated the automation of test generation from Security Functional Requirements (SFR), as defined in the Common Criteria terminology. To achieve that, we worked on the definition of description patterns for security properties, to which a given set of SFRs can be related. These properties are used to automatically generate test scenarios that produce model based test cases. The traceability, ensured all along the testing process, makes it possible to provide evidences of the coverage of the SFR by the tests, required by the Common Criteria to reach the highest Evaluation Assurance Levels.

We have proposed a dedicated formalism to express test properties. translated into a finite state automaton which describes a monitor of its behaviors [36]. We have proposed dedicated property coverage criteria that can be used either to measure the property coverage of a given test suite, or to generate test cases, exercising nominal or robustness aspects of the property. This process has been fully tool-supported into an integrated software prototype[7] [41].

In the context of the SecureChange project, we have also investigatde the evolution of test scenarios. As the system evolves, the model evolves, and the associated test scenarios may also evolve. We are currently extending the test generation and management of system evolutions to ensure the preservation of the security.

6.4.3. *Mutation-based Testing of Security Protocols*

Participants: Frédéric Dadeau, Pierre-Cyrille Héam, Ghazi Maatoug, Michaël Rusinowitch.

Verification of security protocols models is an important issue. Nevertheless, the verification reasons on a model of the protocol, and does not consider its concrete implementation. While representing a safe model, the protocol may be incorrectly implemented, leading to security flaws when it is deployed. We have proposed a model-based penetration testing approach for security protocols [9]. This technique relies on the use of mutations of an original protocol, proved to be correct, for injecting realistic errors that may occur during the protocol implementation (e.g. re-use of existing keys, partial checking of received messages, incorrect formatting of sent messages, use of exponential/xor encryption, etc.). Mutations that lead to security flaws are used to build test cases, which are defined as a sequence of messages representing the behavior of the intruder. secret. We have applied our technique on protocols designed in HLPSL, and implemented a protocol mutation tool that performs the mutations. The mutants are then analyzed by the CL-Atse [82] front-end of the AVISPA toolset [64]. We have experimented our approach on a set of protocols, and we have shown the relevance of the proposed mutation operators and the efficiency of the CL-Atse tool to conclude on the vulnerability of a protocol and produce an attack trace that can be used as a test case for implementations. We applied our approach on the Paypal Express protocol, and we were able to retrieve an existing attack trace on this protocol[8]. We are now investigating the transformation of an attack trace into executable tests scripts. To achieve that, we propose to automatically generate skeletons of Java test programs that the validation engineer only has to fill in order to concretize the steps of the test. A first experience in this direction has been described in [48].

6.4.4. *Rewriting-based Mathematical Model Transformations*

Participants: Walid Belkhir, Alain Giorgetti.

Since 2011 we collaborate with the Department “Temps-Fréquence” of the FEMTO-ST institute (Franche-Comté Electronique Mécanique Thermique et Optique - Sciences et Technologies, CNRS UMR 6174) on the formalization of asymptotic methods (based on two-scale convergence).The goal is to design a software, called *MEMSALab*, for the automatic derivation of multiscale models of arrays of micro- and nanosystems. In this domain a model is a partial differential equation. Multiscale methods approximate it by another partial differential equation which can be numerically simulated in a reasonable time. The challenge consists in taking into account a wide range of geometries combining thin and periodic structures with the possibility of multiple nested scales. We have designed a transformation language facilitating the design of MEMSALab [18]. It

[7] A video of the prototype is available at: http://vimeo.com/53210102
[8] http://www.nbs-system.com/blog/faille-securite-magento-paypal.html

is proposed as a Maple™ package for rule-based programming, rewriting strategies and their combination with standard Maple™ code. We illustrate the practical interest of this language by using it to encode two examples of multiscale derivations, namely the two-scale limit of the derivative operator and the two-scale model of the stationary heat equation. A more general framework for the derivation of the multi-scale models was established in [26].

6.4.5. Code-related Test Generation and Static Analysis

Participants: Fabrice Bouquet, Frédéric Dadeau, Ivan Enderlin, Alain Giorgetti.

We have designed a new annotation language for PHP, named PRASPEL (for *PHP Realistic Annotation SPEcification Language*). This language relies on *realistic domains* which serve two purposes. First, they assign to a data a domain that is supposed to be specific w.r.t. a context in which it is employed. Second, they provide two features that are used for test generation: (i) *samplability* makes it possible to automatically generate a value that belongs to the realistic domain so as to generate test data, (ii) *predicability* makes it possible to check if the value belongs to a realistic domain. This approach is tool-supported in a dedicated framework for PHP which makes it possible to produce unit test cases using random data generators, execute the test cases on an instrumented implementation, and decide the conformance of the code w.r.t. the annotations by runtime assertion checking. This principle has been extended to generate grammar-based textual data based on various strategies, namely uniform random generation, bounded exhaustive generation and rule-coverage-based test generation. In a recent work, we have proposed a dedicated constraint solver for PHP arrays [44] aiming to avoid rejection during the generation of array structures.

6.4.6. Random Testing

Participants: Aloïs Dreyfus, Pierre-Cyrille Héam, Olga Kouchnarenko.

The random testing paradigm represents a quite simple and tractable software assessment method for various testing approaches. When performing random testing, the random sampler is supposed to be independent of tester choices or convictions: a solution is to exploit uniform random generators.

In [78] a method is proposed for drawing paths in finite graphs uniformly, and it is explained how to use these techniques for testing C programs within a control flow graph based approach. Nevertheless, as finite graphs often provide strong abstractions of the systems under test, many abstract tests generated by the approach cannot be played on the implementation. In [79], we have proposed a new approach, extending [78], to manage stack-call during the random test generation while preserving uniformity. In [61], we go further by investigating a way to biase the random testing, in order to optimize the probability to fulfil a coverage criterion. The new approaches have been implemented in a prototype and experimented on several examples. A similar approach for grammar based testing is developped in [43]: we show how to hedge the random generation of execution trees to optimize the probability of covering either all rules or all non terminal symbols.

6.5. Verification of Collaborative Systems

We investigate security problems occurring in decentralized systems. We develop general techniques to enforce read and update policies for controlling access to XML documents based on recursive DTDs (Document Type Definition). Moreover, we provide a necessary and sufficient condition for undoing safely replicated objects in order to enforce access control policies in an optimistic way.

6.5.1. Automatic Analysis of Web Services Security

Participants: Walid Belkhir, Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

Automatic composition of web services is a challenging task. Many works have considered simplified automata models that abstract away from the structure of messages exchanged by the services. For the domain of secured services (using e.g. digital signing or timestamping) we propose a novel approach to automated orchestration of services under security constraints. Given a community of services and a goal service, we reduce the problem of generating a mediator between a client and a service community to a security problem where an intruder should intercept and redirect messages from the service community and a client service till reaching a satisfying state. This orchestration specification is expressed in ASLan language, a formal language designed for modeling Web Services tied with security policies that was developed in AVANTSSAR project. The AVANTSSAR Orchestrator (presented in [28]) generates an attack trace describing the execution of a the mediator and translates it into ASLan. Then we can check with automatic tools that this ASLan specification verifies required security properties such as secrecy and authentication. If no flaw is found, we can compile the ASLan specification into a Java servlet that can be used to execute the orchestration.

In [34] we introduce an alternative approach based on *fresh-variable automata*, a natural extension of finite-state automata over infinite alphabet. In this model the transitions are labeled with constants or variables that can be refreshed in some specified states. We prove several closure properties for this class of automata and study their decision problems. We show the applicability of our model to Web services handling data from an infinite domain. We introduce a notion of simulation that enables us to reduce the Web service composition problem to the construction of a simulation of a target service by the asynchronous product of existing services, and prove that this construction is computable. We now work on synthesizing composed services that satisfy required security policies.

6.5.2. Secure Querying and Updating of XML Data

Participants: Abdessamad Imine, Houari Mahfoud, Michaël Rusinowitch.

It is increasingly common to find XML views used to enforce access control as found in many applications and commercial database systems. To overcome the overhead of view materialization and maintenance, XML views are necessarily virtual. With this comes the need for answering XML queries posed over virtual views, by rewriting them into equivalent queries on the underlying documents. A major concern here is that query rewriting for recursive XML views is still an open problem, and proposed approaches deal only with non-recursive XML views. Moreover, a small number of works have studied the access rights for updates. In [51], we present SVMAX (Secure and Valid MAnipulation of XML), the first system that supports specification and enforcement of both read and update access policies over arbitrary XML views (recursive or non). SVMAX defines general and expressive models for controlling access to XML data using significant class of XPath queries and in the presence of the update primitives of W3C XQuery Update Facility. Furthermore, SVMAX features an additional module enabling efficient validation of XML documents after primitive updates of XQuery. The wide use of W3C standards makes of SVMAX a useful system that can be easily integrated within commercial database systems as we will show. We give extensive experimental results, based on real-life DTDs, that show the efficiency and scalability of our system.

We introduce in [49] an extension of hedge automata called bidimensional context-free hedge automata, proposing a new uniform representation of vertical and horizontal computation steps in unranked ordered trees. We also extend the parameterized rewriting rules used for modeling the W3C XQuery Update Facility in previous works, by the possibility to insert a new parent node above a given node. Since the rewrite closure of hedge automata languages with these extended rewriting systems is a computable context-free hedge language we can perform some static typechecking on these XML transformations.

6.5.3. On Adding Friends Problem in Social Networks

Participants: Bao Thien Hoang, Abdessamad Imine.

Online social networks are currently experiencing a peak and they resemble real platforms of social conversion and content delivery. Indeed, they are exploited in many ways: from conducting public opinion polls about any political issue to planning big social events for a large public. To securely perform these large-scale computations, current protocols use a simple secret sharing scheme which enables users to obfuscate their

inputs. However, these protocols require a minimum number of friends, i.e. the minimum degree of the social graph should be not smaller than a given threshold. Often this condition is not satisfied by all social graphs. Yet we can reuse these graphs after some structural modifications consisting in adding new friendship relations. In this paper, we provide the first definition and theoretical analysis of the "*adding friends*" problem. We formally describe this problem that, given a graph G and parameter c, asks for the graph satisfying the threshold c that results from G with the minimum of edge-addition operations. We present algorithms for solving this problem in centralized social networks [33]. An experimental evaluation on real-world social graphs demonstrates that our protocols are accurate and inside the theoretical bounds.

6.5.4. Access Control Models for Collaborative Applications

Participants: Fabrice Bouquet, Abdessamad Imine, Michaël Rusinowitch.

The importance of collaborative systems in real-world applications has grown significantly over the recent years. The most of new applications are designed in a distributed fashion to meet collaborative work requirements. Among these applications, we focus on Real-Time Collaborative Editors (RCE) that provide computer support for modifying simultaneously shared documents, such as articles, wiki pages and programming source code by dispersed users. Although such applications are more and more used into many fields, the lack of an adequate access control concept is still limiting their full potential. In fact, controlling access in a decentralized fashion in such systems is a challenging problem, as they need dynamic access changes and low latency access to shared documents. In [19], we propose a generic access control model based on replicating the shared document and its authorization policy at the local memory of each user. We consider the propagation of authorizations and their interactions. We propose an optimistic approach to enforce access control in existing collaborative editing solutions in the sense that the access control policy can be temporarily violated. To enforce the policy, we resort to the selective undo approach in order to eliminate the effect of illegal document updates. Since, the safe undo is an open issue in collaborative applications. We investigate a theoretical study of the undo problem and propose a generic solution for selectively undoing operations. Finally, we apply our framework on a collaboration prototype and measure its performance in the distributed grid GRID'5000 to highlight the scalability of our solution.

However, verifying whether the combination of access control and coordination protocols preserves the data consistency is a hard task since it requires examining a large number of situations. In [52], we specify this access control protocol in the first-order relational logic with Alloy, and we verify that it preserves the correctness of the system on which it is deployed, namely that the access control policy is enforced identically at all participating user sites and, accordingly, the data consistency remains still maintained.

7. Bilateral Contracts and Grants with Industry

7.1. Research Result Transfer

The BZ-Testing-Tools technology has been transfered to LEIRIOS Technologies, at the end of 2004. LEIRIOS changed its name into 2007 and is now called Smartesting. The partnership between the Cassis project and the R&D department of Smartesting, located at the TEMIS Scientific and Industrial area at Besançon, will be continued through (national and international) projects or with a new transfer protocol. F. Bouquet is scientific consultant of Smartesting.

7.2. Study of the electronic voting system of Voxaly

Participants: Stéphane Glondu, Véronique Cortier.

A 4-month contract has been signed between Caramel, Cassis and Voxaly, a French company who is proposing solutions for the organization of on-line elections. During several meetings, we discussed their current solution and proposed improvements to gradually add security features that get close to the academic standards.

8. Partnerships and Cooperations

8.1. Regional Initiatives

- Franche-Comté Region project SyVAD (SysML Verification and Validation), coordinated by Fabrice Bouquet, duration: 3 years, started in September 2011. This project focuses on the SysML models for the validation and verification of the micro-systems, in particular for distributed micro airduct. The project associates several team of FEMTO-ST institute.

8.2. National Initiatives

8.2.1. ANR

- ANR PROSE *Protocoles de sécurité : modèle formel, modèle calculatoire, and implémentations — Security protocols : formal model, computational model, and implementations*, duration: 4 years, started in December 2010. The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: *(i)* the symbolic level, in which messages are terms, *(ii)* the computational level, in which messages are bitstrings, and *(iii)* the implementation level: the program itself. Partners are EPI Prosecco and EPI Cascade Paris (leader), LSV Cachan, Cassis and Verimag Grenoble.
- ANR STREAMS *Solution for Peer-to-peer Real-Time Social Web*, duration: 3 years, starting in October 2010. This project proposes to design peer-to-peer solutions that offer underlying services required by real-time social web applications and that eliminate the disadvantages of centralised architectures. There exists a tension between sharing data with friends in a social network deployed in an open peer-to-peer network and ensuring privacy. One of the most challenging issues in social applications is how to balance collaboration with access control to shared objects. This project aims at providing theoretical solutions to these challenges as well as practical experimentations. Partners are: LORIA Score team (leader), Inria project-teams Regal, Asap, Cassis, and XWiki.
- ANR FREC *Frontiers of recognizability*, duration: 4 years, starting in October 2010. The goal of this project is to be a driving force behind the extension of the algebraic theory of regular languages made possible by recent advances. Four directions will be investigated: tree languages, λ-terms, automata with counters, algebraic and topological tools. Partners are LABRI (leader), LIAFA (University Paris 7). Pierre-Cyrille Héam is a member of this project, attached to Paris 7 for administrative facilities.
- ANR OSEP *Online and offline model-based testing of SEcurity Properties*, duration: 2 years, started in November 2011 and ended in November 2013. The goal of this project was to apply online and offline model-based testing approaches for security testing of cryptographic components and software radio case studies, used as a black boxes. This approach had to be compatible with our previous offline approaches to increase the number of artefacts that can be shared. So, we developed new algorithms to allow online testing, and a dedicated tool called MBeeTle. This project was an opportunity to reuse the results of the ANR TASCCC project, and to complete these approaches with security properties expressed in TOCL. This project involved the DGA and Smartesting.

8.2.2. Competitivity Clusters

- FUI SQUASH *Software QUality ASsurance enHancement*, duration: 2 years, starting in April 2011. This project aims to industrialize and to structure software testing activities. The project will provide a methodology and tools based on open source components.
- Project "Investissement d'Avenir - Développement de l'Econimie Numérique" DAST (Dynamic Application Security Testing), duration: 2 years, starting in September 2012. The goal of this project is to generate automatically the tests to prevent vulnerabilities. We have proposed an automated model-based vulnerability testing approach, that focuses on Criss-Site Scripting vulnerabilities in web applications. It relies on a behavioral model that describes the web application and a set of security test patterns formalizing ways to detect the vulnerabilities. This partnership includes NBSystem, Smartesting (coordinator), Thales, Trusted-Labs and Inria CASSIS.

8.3. European Initiatives

8.3.1. FP7 Projects

- Nessos is a Network of Excellence on Engineering Secure Future Internet Software Services and Systems in FP7-ICT (starting in October 2010 for a period of 42 months). Nessos has 12 partners and aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. Partner Inria is involved through project-teams Arles, Triskell and Cassis. Cassis will focus on developping tools for service security verification and testing tasks.
- ProSecure (2011-2016) [9]— ERC Starting Grant Project on Provably secure systems: foundations, design, and modularity. This long-term project aims at developing provably secure systems such as security protocols. The goal is to propose foundations for a careful analysis and design of large classes of up-to-date protocols. To achieve this goal, we foresee three main tasks. First, we plan to develop general verification techniques for new classes of protocols that are of primary interest in nowadays life like e-voting protocols, routing protocols or security APIs. Second, we will consider the cryptographic part of the primitives that are used in such protocols (encryption, signatures, ...), obtaining higher security guarantees. Third, we aim at proposing modular results both for the analysis and design of protocols. Véronique Cortier is the leader of the project.

8.4. International Initiatives

8.4.1. Inria Associate Teams

BANANAS [10] *Automated design and autonomous control of hybrid solver cooperations*. In order to tackle large scale instances and intricate problem structures, sophisticated solving techniques have been developed, combined, and hybridized to provide efficient solvers. A common idea to get more efficient and robust algorithms consists in combining several resolution paradigms in order to take advantage of their respective assets. Autonomous Search is a very attractive approach for designing adaptive systems with the capability of improving its solving performance by selecting and adapting its search strategies to the problem at hand. The main goal of the project is to apply the Autonomous Search approach to hybrid solver cooperations, by automating the selection and the cooperation of solvers, by tuning the cooperation parameters, and by adapting the cooperation during solving. The international partners are Technical University Federico Santa Maria, Valparaíso (Chile) — Department of Computer Science — Carlos Castro and Eric Monfroy; University of Chile (Chile) — Center for Mathematical Modeling — Jorge Amaya. The Inria principal investigator is Christophe Ringeissen.

8.4.2. Inria International Partners

- Collaboration with Bogdan Warinschi (Bristol University) on soundness of symbolic models w.r.t. cryptographic ones.
- Collaboration with Mark Ryan's group (University of Birmingham) on the formal analysis of e-voting protocols.
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction.
- Collaboration with Hanifa Boucheneb's group (Ecole Polytechnique de Montréal) on model-checking of collaborative systems.
- Collaboration with John Mullins's group (Ecole Polytechnique de Montréal) on information hiding.

8.4.3. Participation in International Programs

French-Tunisian project on *Security Policies and Configurations of Firewalls: Compilation and Automated Verification*. We collaborate with SupCom Tunis and the Inria project-team Dahu in the context of STIC-Tunisia.

[9] http://www.loria.fr/~cortier/ProSecure.html
[10] http://www.loria.fr/~ringeiss/CHILI/bananas

French-Canadian project on *Automata for Hiding and Disclosing Information*, in the framework of the CFQCU program. We collaborate with the CRAC team at the Ecole Polytechnique de Montréal, Canada, and the MoVe team/LIP6 at the UPMC, Paris, France.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Myrto Arapinis (University of Edinburgh), one week in January 2013, two weeks in November 2013
- Florian Boehl (KIT University), one week in January 2013
- Luigi Grillo (Università di Catania), two weeks in April 2013
- Dominique Unruh (Tallin University), one week in February 2013
- Bogdan Warinschi (University of Bristol), one week in January 2013
- Paliath Narendran (SUNY Albany), one month in June-July 2013
- David Bouchard and Kim Gero (SUNY Albany), one week in September 2013
- Christoph Sprenger and Binh Nguyen (ETH Zürich) three days in April 2013

8.5.1.1. Internships

We have supervised the following internships.

Anisia Maria Magdalena Tudorescu

Subject: Integrating SMT solvers into Spike

Supervisors: Pascal Fontaine (project-team Veridis), Sorin Stratulat, and Christophe Ringeissen

Date: from Mar 2013 until May 2013

Institution: West Timisoara University (Romania)

Gisela-Carla Rossi

Subject: Formal Methods for Secure Service Composition

Supervisors: Walid Belkhir and Michaël Rusinowitch

Date: from Jun 2013 until Dec 2013

Institution: National University of Cordoba (Argentina)

Paula Chocrón

Subject: Non-disjoint combination for SMT solvers: sharing a fragment of arithmetic

Supervisors: Pascal Fontaine (project-team Veridis) and Christophe Ringeissen

Date: from Sep 2013 until Nov 2013

Institution: University of Buenos Aires (Argentina)

Gemma Puig-Quer

Subject: New protocols for private e-voting

Supervisors: David Galindo-Chacon and Véronique Cortier

Date: from Sep 2013 until Mar 2014

Institution: UPC Barcelona (Spain)

In addition, Steve Kremer has supervised the following students from the École des Mines de Nancy:

- Othmane El Omri, Analysis of a peer-to-peer E-wallet protocol (from Jul 2013 to Sep 2013)
- Pierre Lepeudry, Formalizing some combinatorial attacks in security protocols (from Sep 2013 to Jan 2014)

and Véronique Cortier and Cyrille Wiedling have supervised a group of three students from the École des Mines de Nancy on the implementation of a secure key management system on smartcards: Arnaud Kéranguéven, Hadrien Chastant, and Othmane El Omri (from Oct 2012 to June 2013).

8.5.2. Visits to International Teams

- Olga Kouchnarenko, August 2013 (10 days), Ecole Polytechnique de Montréal (the CRAC team), Canada, visit funded by the Conseil franco-québécois de coopération universitaire" (CFQCU).

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorial board

- Information & Computation (Véronique Cortier)
- Journal of Computer Security (Véronique Cortier)

9.1.2. Conferences

- FroCoS 2013, 9th Symposium on Frontiers of Combining Systems, 18–20 September 2013, Nancy, France, (Christophe Ringeissen, conference chair)

9.1.3. Program committees

- Fabrice Bouquet: ICST 2013 (Publicity Chair), MoDeVVA 2013
- Véronique Cortier: CSF 2013 (PC Chair), CCS 2013, LICS 2013, POST 2013
- Frédéric Dadeau : CSTVA'2013 (PC Chair), QSIC'2013.
- Abdessamad Imine: AICCSA 2013 (co-chair), CIIA 2013, DEXA 2013, DEXA 2014
- Steve Kremer: ACNS 2014, POST 2014 (PC Chair), Security Track of ACM SAC 2014 (PC Chair), ESORICS 2013, ICICS 2013, ISPEC 2013, POST 2013, RV 2013
- Christophe Ringeissen: CADE-24, FroCoS 2013, UNIF 2013, UNIF 2014 (co-chair)
- Michael Rusinowitch: LATA 2013, CRISIS 2013, ESSOS DS 2013, GRSRD 2013.
- Laurent Vigneron: UNIF 2013.

9.1.4. Steering committees

- Véronique Cortier: FCS (Chair), CSF
- Steve Kremer: CSF, ETAPS, POST

9.1.5. Spring school

- Spring School on Trusted and Secure Composite Services, 27–31 May 2013, Malaga, Spain, (Abdessamad Imine, Lecturer)
- JDEV'2013 National Day for Software development, 4–6 September 2013, Ecole polytechnique (Palaiseau), France (Bouquet F., Gauthier J.-M. and Enderlin I., 5 tutorials and 1 Lecturer) - 500 participants.

- School of INRA on the Testing for Software Development, in PEPI IDL 2013 (*"Partage d'Expérience et de Pratiques en Informatique" visant l'"Ingénierie Développement Logiciel"*), 9–12 December 2013, Ecully (69) France (Bouquet F., Gauthier J.-M. and Enderlin I., 3 days of tutorials) - 30 participants.
- 13th International School on Foundations of Security Analysis and Design, 2–7 September 2013, Bertinoro, Italy (Mathieu Turuani, Tutorial).
- AFADL'2013 (*"Approches Formelles dans l'Assistance au Développement de Logiciels"*), during the GDR - GPL - CIEL - AFADL Days, 2–5 april 2013, Nancy, France (Mathieu Turuani, Tutorial) - 135 participants.

9.1.6. Working groups

- GT-Verif, Verification, GDR IM Working Group (Véronique Cortier, chair)
- IFIP WG-1.7 Foundations of Security Analysis (Véronique Cortier, vice-Chair)
- IFIP WG-1.6 - Term Rewriting (Michael Rusinowitch, Laurent Vigneron)
- MTV2, Testing Methods for Verification and Validation, GDR GPL Working Group (Frédéric Dadeau, co-chair)
- FORWAL, Formalisms and Tools for Verification and Validation, GDR GPL Working Group (Pierre-Cyrille Héam, co-chair)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence :
  - Frédéric Dadeau, Programming, 37 hours (ETD), L1, Université de Franche-Comté
  - Frédéric Dadeau, Databases, 39 hours (ETD), L1, Université de Franche-Comté
  - Frédéric Dadeau, Web Languages, 24 hours (ETD), L2, Université de Franche-Comté
  - Frédéric Dadeau, Object-Oriented Modelling and Design, 44 hours (ETD), L3, Université de Franche-Comté
  - Alain Giorgetti, Logics and Deduction, 52 hours (ETD), L2, Université de Franche-Comté, France.
  - Alain Giorgetti, Formal Methods, 81 hours (ETD), L3, Université de Franche-Comté, France
  - Olga Kouchnarenko, Formal Languages, 65 hours (ETD), L3, Université de Franche-Comté, France
  - Olga Kouchnarenko, Languages, Specification and Proof, 25 hours (ETD), L3, Université de Franche-Comté, France
  - Olga Kouchnarenko, Parsing Algorithms and XML, 30 hours (ETD), L3, Université de Franche-Comté, France
- Master :
  - Fabrice Bouquet, Artificial Intelligence (also in e-learning), 53 hours (ETD), M2, Université de Franche-Comté
  - Fabrice Bouquet, Compilation, 54 hours (ETD), M2, Université de Franche-Comté
  - Fabrice Bouquet, Testing (also in e-learning), 71 hours (ETD), M2, Université de Franche-Comté
  - Frédéric Dadeau, Testing, 13 hours (ETD), M2, Université de Franche-Comté
  - Alain Giorgetti, Program Proofs, 58 hours (ETD), M1, Université de Franche-Comté, France.

  - Alain Giorgetti, Decision Procedures, 13 hours (ETD), M2, Université de Franche-Comté, France.
  - Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.
  - Christophe Ringeissen, Decision Procedures for Software Verification, 24 hours (ETD), M2 Computer science, Lorraine University, France.
  - Laurent Vigneron, Security of information systems, 15 hours (ETD), M2 Computer science, Lorraine University, France.
  - Laurent Vigneron, Formal methods, 24 hours (ETD), M2 MIAGE, Lorraine University, France.
  - Pierre-Cyrille Héam, Calculability, 23 hours (ETD), M2 Computer science, Université de Franche-Comté, France.
  - Pierre-Cyrille Héam, Introduction to Büchi Automata, 18 hours (ETD), M2 Computer science, Université de Franche-Comté, France.
  - Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, University of Lorraine, France.
  - Olga Kouchnarenko, Specification, Verification and Validation, 12 hours (ETD), M2, Université de Franche-Comté, France.
  - Olga Kouchnarenko, Compositional approaches in verification, 18 hours (ETD), M2, Université de Franche-Comté, France.
  - Olga Kouchnarenko, Security and Components, 10,5 hours (ETD), M2, Université de Franche-Comté, France.
- Doctorat:
  - Steve Kremer, Les protocoles de sécurité : modélisation et vérification, 4,5 hours (ETD), École jeunes chercheurs en programmation (EJCP), Rennes, France

9.2.2. Supervision

- PhD :

  Kalou Cabrera Castillos, Automated Test Scenario Generation from Property Patterns and Behavioral Models, November 28, Frédéric Dadeau and Jacques Julliand

  Jérome Cantenot, Management of consistence in verication conditions in the test generation context, Université de Franche Comté, 13 November, Fabrice Ambert and Fabrice Bouquet.

  Vincent Hugot, Approximations and Constraints: Application to the Verification of Embedded Systems, Université de Franche Comté, September 27, Pierre-Cyrille Héam and Olga Kouchnarenko

  Elena Tushkanova, Specification and formal certification of (combinations of) decision procedures, Université de Franche Comté, July 19, Alain Giorgetti, Olga Kouchnarenko and Christophe Ringeissen
- PhD in progress :

  Hadrien Bride, Validation and Reconfiguration of Modal Petri Nets within Constraint Logic Programming, started in October 2013, Olga Kouchnarenko and Fabien Peureux

  Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune

  Aloïs Dreyfus, Efficient approches for systems validation, started in November 2010, Pierre-Cyrille Héam and Olga Kouchnarenko

  Ivan Enderlin, Test Data Generation for Unit Testing in PHP, started in October 2011, Fabrice Bouquet, Frédéric Dadeau and Alain Giorgetti

Jean-Marie Gauthier, Method for validation and simulation of SysML model: Applied on micro-systems, started in October 2012, Fabrice Bouquet, Fabien Peureux and Ahmed Hammad

Richard Genestier, Formal specification and verification of programs generating structured data, started in October 2012, Alain Giorgetti and Olga Kouchnarenko

Bao-Thien Hoang, Secure Collaboration in Social Networks, started in April 2011, Abdessamad Imine and Christophe Ringeissen

Jean-Luc Joly, Randomized approaches for validation and verification procedures, started in December 2011, Pierre-Cyrille Héam

Robert Künnemann, Verification of Security APIs, started in October 2010, Steve Kremer and Graham Steel

Éric Le Morvan, Secure composition of cryptographic protocols, started in October 2013, Véronique Cortier

Houari Mahfoud, Access Control Models for XML Documents, started in September 2010, Abdessamad Imine and Michaël Rusinowitch

Guillaume Scerri, Symbolic and automatic security proofs in computational models, started in September 2011, Hubert Comon-Lundh and Véronique Cortier

Cyrille Wiedling, Formal analysis of E-voting protocols, started in September 2011, Véronique Cortier

Hiep Nguyen Huu, Secure Collaboration in Mobile Social Networks, started in November 2013, Abdessamad Imine and Michaël Rusinowitch

9.2.3. Juries

Inria evaluation committee (Véronique Cortier, Michaël Rusinowitch)

Jury starting/advanced Inria positions and jury international chair Inria 2013 (Véronique Cortier)

Jury Junior Research Position Inria Nancy Grand Est (Michaël Rusinowitch)

Referee for David Cadé's PhD, December 2013: Proved Implementations of Cryptographic Protocols in the Computational Model (Véronique Cortier)

Referee for Matthijs Melissen's PhD, October 2013: Game Theory and Logic for Non-repudiation Protocols and Attack Analysis (Steve Kremer)

Referee for Jannik Dreier's PhD, November 2013: Formal Verification of Voting and Auction Protocols: From Privacy to Fairness and Verifiability (Steve Kremer)

Referee for Naipeng Dong's PhD, November 2013: Enforced Privacy: from Practice to Theory (Michaël Rusinowitch)

Referee for Mohamed Iguernelala's PhD, June 2013: Renforcement du Noyau d'un Démonstrateur SMT (Michaël Rusinowitch)

Referee for Sarah Nait Bahloul's PhD, December 2013: Inférence de règles de contrôle d'accès pour assurer la confidentialité des données au niveau des vues matérialisées (Michaël Rusinowitch)

Referee for Robert Guduvan's PhD, April 2013, A model driven Development of tests for avionics embedded systems (Fabrice Bouquet)

Referee for Taha Triki's PhD, October 2013, Filtering and reduction techniques combinational tests (Fabrice Bouquet)

Examiner for Florent Pompigne's PhD, December 2013, Nancy: Modélisation logique de la langue et Grammaires Catégorielles Abstraites (Laurent Vigneron).

Examiner for Asma Tafat's PhD, September 2013, Orsay: Preuves par raffinement de programmes avec pointeurs. (Alain Giorgetti).

Commitee chair for Lilia Ziand Khodja's PhD, May 2013, Besançon: Résolution de systèmes linéaires et non linéaires creux sur grappes de GPU's (Pierre-Cyrille Héam).

9.3. Popularization

Invited conference of Véronique Cortier at the conference "Sciences et Société", Nancy, January 17th, 2013.

"Vote par internet", popularization science paper on e-voting. In Interstices, January 2013. Véronique Cortier and Steve Kremer.

Fête de la Science 2013: Science popularization action during one week on a workshop "a cryptographic treasure hunting". Véronique Cortier, David Galindo, Stéphane Glondu, Steve Kremer, Éric Le Morvan, Cyrille Wiedling.

Video gaming month at the "Fabrikà Science", University of Franche-Comté, December 2013. Popularization of computer science using the topic of video games. Frédéric Dadeau.

10. Bibliography

Major publications by the team in recent years

[1] M. ABADI, V. CORTIER. *Deciding knowledge in security protocols under equational theories*, in "Theoretical Computer Science", November 2006, vol. 387, n^{o} 1-2, pp. 2-32

[2] A. ARMANDO, D. BASIN, Y. BOICHUT, Y. CHEVALIER, L. COMPAGNA, J. CUELLAR, P. HANKES DRIELSMA, P.-C. HÉAM, O. KOUCHNARENKO, J. MANTOVANI, S. MÖDERSHEIM, D. VON OHEIMB, M. RUSINOWITCH, J. SANTOS SANTIAGO, M. TURUANI, L. VIGANO, L. VIGNERON. *The AVISPA Tool for the automated validation of internet security protocols and applications*, in "17th International Conference on Computer Aided Verification, CAV'2005", Edinburgh, Scotland, Lecture Notes in Computer Science, Springer, 2005, vol. 3576, pp. 281-285

[3] A. ARMANDO, S. RANISE, M. RUSINOWITCH. *A Rewriting Approach to Satisfiability Procedures*, in "Journal of Information and Computation — Special Issue on Rewriting Techniques and Applications (RTA'01)", June 2003, vol. 183, n^{o} 2, pp. 140–164

[4] M. BAUDET, V. CORTIER, S. KREMER. *Computationally Sound Implementations of Equational Theories against Passive Adversaries*, in "Information and Computation", April 2009, vol. 207, n^{o} 4, pp. 496-520

[5] Y. BOICHUT, R. COURBIS, P.-C. HÉAM, O. KOUCHNARENKO. *Finer is better: Abstraction Refinement for Rewriting Approximations*, in "19th International Conference on Rewriting Techniques and Applications - RTA'2008", Hagenberg, Austria, A. VORONKOV (editor), Lecture Notes in Computer Science, Springer, 2008, vol. 5117, pp. 48-62

[6] F. BOUQUET, B. LEGEARD, F. PEUREUX. *CLPS-B: A Constraint Solver to Animate a B Specification*, in "International Journal of Software Tools for Technology Transfer, STTT", August 2004, vol. 6, n^{o} 2, pp. 143–157

[7] Y. CHEVALIER, R. KUESTERS, M. RUSINOWITCH, M. TURUANI. *Complexity results for security protocols with Diffie-Hellman exponentiation and commuting public key encryption*, in "ACM Transactions on Computational Logic (TOCL)", 2008, vol. 9, Article 24

[8] Y. CHEVALIER, L. VIGNERON. *Strategy for Verifying Security Protocols with Unbounded Message Size*, in "Journal of Automated Software Engineering", April 2004, vol. 11, n^{o} 2, pp. 141–166

[9] F. DADEAU, P.-C. HÉAM, R. KHEDDAM. *Mutation-Based Test Generation from Security Protocols in HLPSL*, in "4th International Conference on Software Testing Verification and Validation (ICST'2011)", Berlin, Germany, M. HARMAN, B. KOREL (editors), IEEE Computer Society Press, March 2011 [*DOI :* 10.1109/ICST.2011.42], http://hal.inria.fr/inria-00559850/en

[10] A. GIORGETTI, J. GROSLAMBERT, J. JULLIAND, O. KOUCHNARENKO. *Verification of Class Liveness Properties with Java Modelling Language*, in "IET Software", 2008, vol. 2, n^{o} 6, pp. 500-514

[11] E. NICOLINI, C. RINGEISSEN, M. RUSINOWITCH. *Combinable Extensions of Abelian Groups*, in "Proc. of 22nd International Conference on Automated Deduction, CADE-22", Montreal, Canada, R. SCHMIDT (editor), Lecture Notes in Artificial Intelligence, Springer, 2009, vol. 5663, pp. 51–66

Publications of the year

Doctoral Dissertations and Habilitation Theses

[12] K. CABRERA CASTILLOS. , *Generation automatique de scenarios de tests a` partir de proprietes temporelles et de mode`les comportementaux*, Université de Franche-Comté, November 2013, http://hal.inria.fr/tel-00924485

[13] V. HUGOT. , *Tree Automata, Approximations, and Constraints for Verification. Tree (Not-Quite) Regular Model-Checking*, Université de Franche-Comté, September 2013, co-directeur: Pierre-Cyrille Héam, http://hal.inria.fr/tel-00909608

[14] E. TUSHKANOVA. , *Calculs schématiques pour l'analyse de procédures de décision*, Université de Franche-Comté, July 2013, http://hal.inria.fr/tel-00910929

Articles in International Peer-Reviewed Journals

[15] S. ANANTHARAMAN, C. BOUCHARD, P. NARENDRAN, M. RUSINOWITCH. *Unification modulo a 2-sorted Equational theory for Cipher-Decipher Block Chaining*, in "Logical Methods in Computer Science", 2014, (To appear), http://hal.inria.fr/hal-00854841

[16] M. ARNAUD, V. CORTIER, S. DELAUNE. *Modeling and Verifying Ad Hoc Routing Protocols*, in "Information and Computation", 2013, To appear, http://hal.inria.fr/hal-00881009

[17] M. BAUDET, V. CORTIER, S. DELAUNE. *YAPA: A generic tool for computing intruder knowledge*, in "ACM Transactions on Computational Logic", 2013, vol. 14, n^{o} 1 [*DOI :* 10.1145/2422085.2422089], http://hal.inria.fr/hal-00732901

[18] W. BELKHIR, A. GIORGETTI, L. MICHEL. *A Symbolic Transformation Language and its Application to a Multiscale Method*, in "Journal of Symbolic Computation", December 2013, http://hal.inria.fr/hal-00917323

[19] A. CHERIF, A. IMINE, M. RUSINOWITCH. *Practical access control management for distributed collaborative editors*, in "Pervasive and Mobile Computing", September 2013 [*DOI :* 10.1016/J.PMCJ.2013.09.004], http://hal.inria.fr/hal-00915315

[20] V. CHEVAL, V. CORTIER, S. DELAUNE. *Deciding equivalence-based properties using constraint solving*, in "Theoretical Computer Science", 2013, vol. 492, pp. 1-39 [*DOI :* 10.1016/J.TCS.2013.04.016], http://hal.inria.fr/hal-00881060

[21] C. CHEVALIER, S. DELAUNE, S. KREMER, M. D. RYAN. *Composition of Password-based Protocols*, in "Formal Methods in System Design", 2013 [*DOI :* 10.1007/S10703-013-0184-6], http://hal.inria.fr/hal-00878640

[22] V. CORTIER, B. SMYTH. *Attacking and fixing Helios: An analysis of ballot secrecy*, in "Journal of Computer Security", 2013, vol. 21, n° 1, pp. 89-148 [*DOI :* 10.3233/JCS-2012-0458], http://hal.inria.fr/hal-00732899

[23] V. CORTIER, G. STEEL. *A Generic Security API for Symmetric Key Management on Cryptographic Devices*, in "Information and Computation", 2013, To appear, http://hal.inria.fr/hal-00881072

[24] D. GALINDO. *A note on an IND-CCA2 secure Paillier-based cryptosystem*, in "Information Processing Letters", November 2013, vol. 113, n° 22-24, pp. 913-914 [*DOI :* 10.1016/J.IPL.2013.09.008], http://hal.inria.fr/hal-00909726

[25] D. GALINDO, S. VIVEK. *Limits of a conjecture on a leakage-resilient cryptosystem*, in "Information Processing Letters", April 2014, vol. 114, n° 4, pp. 192-196 [*DOI :* 10.1016/J.IPL.2013.11.014], http://hal.inria.fr/hal-00933429

[26] B. YANG, W. BELKHIR, M. LENCZNER. *Computer-Aided Derivation of Multi-scale Models: A Rewriting Framework*, in "International Journal for Multiscale Computational Engineering", December 2013, 26 pages, http://hal.inria.fr/hal-00916568

Invited Conferences

[27] F. JACQUEMARD, M. RUSINOWITCH. *Unranked tree rewriting and effective closures of languages*, in "Meeting of the IFIP WG 1.6 on Term Rewriting", Eindhoven, Netherlands, Jürgen Giesl, June 2013, http://hal.inria.fr/hal-00852379

[28] M. RUSINOWITCH. *Automated verification of security protocols and application to services*, in "Verification and Evaluation of Computer and Communication Systems", Florence, Italy, H. BOUCHENEB, F. FLAMMINI (editors), Alessandro Fantechi, University of Florence, Italy, November 2013, http://hal.inria.fr/hal-00915323

[29] L. VIGNERON. *Déduction automatique appliquée à l'analyse et la vérification de systèmes infinis*, in "Approches Formelles dans l'Assistance au Développement de Logiciels", Nancy, France, J. SOUQUIÈRES, V. WIELS (editors), April 2013, http://hal.inria.fr/hal-00916581

International Conferences with Proceedings

[30] F. AMBERT, F. BOUQUET, J. LASALLE, B. LEGEARD, F. PEUREUX. *Applying a Def-Use Approach on Signal Exchange to Implement SysML Model-Based Testing*, in "ECMFA'13, 9-th European Conference on Modelling Foundations and Applications", Montpellier, France, Lecture Notes in Computer Science, Springer, 2013, vol. 7949, pp. 134–151 [*DOI :* 10.1007/978-3-642-39013-5_10], http://hal.inria.fr/hal-00913694

[31] M. ARAPINIS, V. CORTIER, S. KREMER, M. D. RYAN. *Practical Everlasting Privacy*, in "2nd Conferences on Principles of Security and Trust (POST'13)", Rome, Italy, D. BASIN, J. MITCHELL (editors), Lecture

Notes in Computer Science, Springer, 2013, vol. 7796, pp. 21-40 [*DOI :* 10.1007/978-3-642-36830-1_2], http://hal.inria.fr/hal-00878630

[32] M. ARNAUD, V. CORTIER, C. WIEDLING. *Analysis of an electronic Boardroom Voting System*, in "VoteID'13 - 4th International Conference on e-Voting and Identity - 2013", Guildford, United Kingdom, J. HEATHER, S. SCHNEIDER, V. TEAGUE (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7985, pp. 109-126 [*DOI :* 10.1007/978-3-642-39185-9_7], http://hal.inria.fr/hal-00881011

[33] H. BAO THIEN, A. IMINE. *On Constrained Adding Friends in Social Networks*, in "SocInfo - The 5th International Conference on Social Informatics - 2013", Kyoto, Japan, A. JATOWT, E.-P. LIM, Y. DING, A. MIURA, T. TEZUKA, G. DIAS, K. TANAKA, A. J. FLANAGIN, B. T. DAI (editors), Lecture Notes in Computer Science, Springer, November 2013, vol. 8238, pp. 467-477 [*DOI :* 10.1007/978-3-319-03260-3_40], http://hal.inria.fr/hal-00916037

[34] W. BELKHIR, Y. CHEVALIER, M. RUSINOWITCH. *Fresh-Variable Automata for Service Composition*, in "SYNASC 2013 -15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing", Timisoara, Romania, IEEE, September 2013, 28 pages. 4 Figures, http://hal.inria.fr/hal-00914778

[35] F. BOEHL, V. CORTIER, B. WARINSCHI. *Deduction Soundness: Prove One, Get Five for Free*, in "CCS '13 - Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security - 2013", Berlin, Germany, ACM, 2013, pp. 1261-1272 [*DOI :* 10.1145/2508859.2516711], http://hal.inria.fr/hal-00881023

[36] K. CABRERA CASTILLOS, F. DADEAU, J. JULLIAND, S. TAHA, B. KANSO. *A Compositional Automata-based Semantics for Property Patterns*, in "iFM'2013 - 10th International Conference on integrated Formal Methods", Turku, Finland, E. JOHNSEN, L. PETRE (editors), Lecture Notes in Computer Science, Springer, June 2013, vol. 7940, pp. 316-330 [*DOI :* 10.1007/978-3-642-38613-8_22], http://hal.inria.fr/hal-00912628

[37] V. CHEVAL, V. CORTIER, A. PLET. *Lengths may break privacy – or how to check for equivalences with length*, in "CAV'13 - 25th International Conference on Computer Aided Verification - 2013", Saint Petersbourg, Russian Federation, N. SHARYGINA, H. VEITH (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8044, pp. 708-723 [*DOI :* 10.1007/978-3-642-39799-8_50], http://hal.inria.fr/hal-00881065

[38] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. *From security protocols to pushdown automata*, in "ICALP'2013 - 40th International Colloquium on Automata, Languages and Programming - 2013", Riga, Lithuania, F. V. FOMIN, R. FREIVALDS, M. KWIATKOWSKA, D. PELEG (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7966, pp. 137-149 [*DOI :* 10.1007/978-3-642-39212-2_15], http://hal.inria.fr/hal-00881066

[39] H. COMON-LUNDH, V. CORTIER, G. SCERRI. *Tractable inference systems: an extension with a deducibility predicate*, in "CADE'24 - 24th International Conference on Automated Deduction - 2013", Lake Placid, United States, M. P. BONACINA (editor), Lecture Notes in Computer Science, Springer, 2013, vol. 7898, pp. 91-108 [*DOI :* 10.1007/978-3-642-38574-2_6], http://hal.inria.fr/hal-00881068

[40] V. CORTIER, D. GALINDO, S. GLONDU, M. IZABACHÈNE. *Distributed ElGamal à la Pedersen - Application to Helios*, in "WPES 2013 - Proceedings of the 12th ACM workshop on privacy in the electronic society - 2013", Berlin, Germany, ACM, 2013, pp. 131-142 [*DOI :* 10.1145/2517840.2517852], http://hal.inria.fr/hal-00881076

[41] F. DADEAU, K. CABRERA CASTILLOS, Y. LEDRU, T. TRIKI, G. VEGA, J. BOTELLA, S. TAHA. *Test Generation and Evaluation from High-Level Properties for Common Criteria Evaluations – The TASCCC Testing Tool*, in "ICST'2013 - IEEE Sixth International Conference on Software Testing, Verification and Validation", Luxembourg, Luxembourg, B. BAUDRY, A. ORSO (editors), Yves Le Traon, March 2013, pp. 431-438 [*DOI :* 10.1109/ICST.2013.60], http://hal.inria.fr/hal-00912639

[42] A. DREYFUS, P.-C. HEAM, O. KOUCHNARENKO. *Enhancing Approximations for Regular Reachability Analysis*, in "CIAA 2013 - 18th International Conference on Implementation and Application of Automata - 2013", Halifax, Canada, S. KONSTANTINIDIS (editor), Lecture Notes in Computer Science, Springer, July 2013, vol. 7982, pp. 331-339 [*DOI :* 10.1007/978-3-642-39274-0_29], http://hal.inria.fr/hal-00909204

[43] A. DREYFUS, P.-C. HEAM, O. KOUCHNARENKO. *Random Grammar-based Testing for Covering All Non-Terminals*, in "2013 IEEE Sixth International Conference on Software Testing, Verification and Validation - CSTVA Workshop", Luxembourg, Luxembourg, IEEE, March 2013, http://hal.inria.fr/hal-00909225

[44] I. ENDERLIN, A. GIORGETTI, F. BOUQUET. *A Constraint Solver for PHP Arrays*, in "ICSTW - Sixth International IEEE Conference on Software Testing, Verification and Validation Workshops - 2013", Luxembourg, Luxembourg, IEEE, 2013, pp. 218-223 [*DOI :* 10.1109/ICSTW.2013.80], http://hal.inria.fr/hal-00909202

[45] S. ERBATUR, D. KAPUR, A. MARSHALL, P. NARENDRAN, C. RINGEISSEN. *Hierarchical Combination*, in "CADE-24 - 24th International Conference on Automated Deduction - 2013", Lake Placid, United States, M. P. BONACINA (editor), Lecture Notes in Computer Science, Springer, June 2013, vol. 7898, pp. 249-266 [*DOI :* 10.1007/978-3-642-38574-2_17], http://hal.inria.fr/hal-00878649

[46] D. GALINDO, S. VIVEK. *A Leakage-Resilient Pairing-Based Variant of the Schnorr Signature Scheme*, in "14th IMA International Conference, IMACC 2013", Oxford, United Kingdom, M. STAM (editor), LNCS, Springer, December 2013, vol. 8308, http://hal.inria.fr/hal-00909745

[47] J.-M. GAUTHIER, F. BOUQUET, A. HAMMAD, F. PEUREUX. *Verification and Validation of Meta-Model Based Transformation from SysML to VHDL-AMS*, in "MODELSWARD 2013, 1st Int. Conf. on Model-Driven Engineering and Software Development", Barcelona, Spain, 2013, pp. 123–128, http://hal.inria.fr/hal-00913739

[48] H. GHABRI, G. MAATOUG, M. RUSINOWITCH. *Compiling symbolic attacks to protocol implementation tests*, in "Fourth International Symposium on Symbolic Computation in Software Science", Tunis, Tunisia, EPTCS, Adel Bouhoula and Tetsuo Ida and Fairouz Kamareddine, October 2013, vol. 122 [*DOI :* 10.4204/EPTCS.122.4], http://hal.inria.fr/hal-00915320

[49] F. JACQUEMARD, M. RUSINOWITCH. *Rewrite Closure and CF Hedge Automata*, in "7th International Conference on Language and Automata Theory and Application", Bilbao, Spain, Lecture Notes in Computer Science, Springer, 2013, http://hal.inria.fr/hal-00767719

[50] S. KREMER, R. KÜNNEMANN, G. STEEL. *Universally Composable Key-Management*, in "18th European Symposium on Research in Computer Security (ESORICS'13)", Egham, United Kingdom, J. CRAMPTON, S. JAJODIA (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8134 [*DOI :* 10.1007/978-3-642-40203-6_19], http://hal.inria.fr/hal-00878632

[51] H. MAHFOUD, A. IMINE, M. RUSINOWITCH. *SVMAX: a system for secure and valid manipulation of XML data*, in "IDEAS'13 Proceedings of the 17th International Database Engineering & Applications Symposium",

Barcelone, Spain, B. C. DESAI, J.-L. LARRIBA-PEY, J. BERNARDINO (editors), ACM, October 2013 [*DOI :* 10.1145/2513591.2513657], http://hal.inria.fr/hal-00915318

[52] A. RANDOLPH, A. IMINE, H. BOUCHENEB, Q. ALEJANDRO. *Specification and Verification Using Alloy of Optimistic Access Control for Distributed Collaborative Editors*, in "18th International Workshop on Formal Methods for Industrial Critical Systems", Madrid, Spain, C. PECHEUR, M. DIERKES (editors), Lecture Notes in Computer Science, Springer, September 2013, vol. 8187, pp. 184-198 [*DOI :* 10.1007/978-3-642-41010-9_13], http://hal.inria.fr/hal-00917001

[53] E. TUSHKANOVA, C. RINGEISSEN, A. GIORGETTI, O. KOUCHNARENKO. *Automatic Decidability: A Schematic Calculus for Theories with Counting Operators*, in "RTA - 24th International Conference on Rewriting Techniques and Applications - 2013", Eindhoven, Netherlands, LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, June 2013, vol. 21, pp. 303-318 [*DOI :* 10.4230/LIPICS.RTA.2013.303], http://hal.inria.fr/hal-00878657

Conferences without Proceedings

[54] S. ERBATUR, D. KAPUR, A. MARSHALL, P. NARENDRAN, C. RINGEISSEN. *Hierarchical Combination of Unification Algorithms*, in "The 27th International Workshop on Unification (UNIF 2013)", Eindhoven, Netherlands, June 2013, http://hal.inria.fr/hal-00920509

[55] E. TUSHKANOVA, C. RINGEISSEN, A. GIORGETTI, O. KOUCHNARENKO. *Automatic Decidability for Theories with Counting Operators*, in "Automated Deduction: Decidability, Complexity, Tractability (workshop ADDCT)", Lake Placid, United States, June 2013, http://hal.inria.fr/hal-00920496

Books or Proceedings Editing

[56] P. FONTAINE, C. RINGEISSEN, R. SCHMIDT (editors). , *Frontiers of Combining Systems*, Lecture Notes in Artificial Intelligence, Springer, September 2013, vol. 8152, 359 p. , http://hal.inria.fr/hal-00868424

Research Reports

[57] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. , *From security protocols to pushdown automata*, Inria, April 2013, n^{o} RR-8290, http://hal.inria.fr/hal-00817230

Scientific Popularization

[58] A. IMINE, M. RUSINOWITCH. *Secure Collaboration for Smartphones*, in "ERCIM News", April 2013, n^{o} 93, http://hal.inria.fr/hal-00915317

Other Publications

[59] W. BELKHIR, Y. CHEVALIER, M. RUSINOWITCH. , *Guarded Variable Automata over Infinite Alphabets*, 2013, 29 pages p. , arXiv admin note: text overlap with arXiv:1302.4205, http://hal.inria.fr/hal-00914779

[60] V. CORTIER, D. GALINDO, S. GLONDU, M. IZABACHÈNE. , *A generic construction for voting correctness at minimum cost - Application to Helios*, 2013, Cryptology ePrint Archive, Report 2013/177, http://hal.inria.fr/hal-00881079

[61] A. DREYFUS, P.-C. HEAM, O. KOUCHNARENKO, C. MASSON. , *A Random Testing Approach Using Pushdown Automata*, December 2013, submitted (minor revision required), http://hal.inria.fr/hal-00912392

References in notes

[62] S. KREMER, V. CORTIER (editors). , *Formal Models and Techniques for Analyzing Security Protocols*, Cryptology and Information Security Series, IOS Press, 2011, vol. 5, 312 p. , http://hal.inria.fr/inria-00636787/en

[63] A. ARMANDO, W. ARSAC, T. AVANESOV, M. BARLETTA, A. CALVI, A. CAPPAI, R. CARBONE, Y. CHEVALIER, L. COMPAGNA, J. CUELLAR, G. ERZSE, S. FRAU, M. MINEA, S. MÖDERSHEIM, D. VON OHEIMB, G. PELLEGRINO, S. ELISA PONTA, M. ROCCHETTO, M. RUSINOWITCH, M. TORABI DASHTI, M. TURUANI, L. VIGANO. *The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures*, in "Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012", Tallinn, Estonie, C. FLANAGAN, B. KONIG (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7214, pp. 267-282 [*DOI :* 10.1007/978-3-642-28756-5_19], http://hal.inria.fr/hal-00759725

[64] A. ARMANDO, D. BASIN, Y. BOICHUT, Y. CHEVALIER, L. COMPAGNA, J. CUELLAR, P. HANKES DRIELSMA, P.-C. HÉAM, O. KOUCHNARENKO, J. MANTOVANI, S. MÖDERSHEIM, D. VON OHEIMB, M. RUSINOWITCH, J. SANTOS SANTIAGO, L. VIGANO, M. TURUANI, L. VIGNERON. *The AVISPA Tool for the automated validation of internet security protocols and applications*, in "17th International Conference on Computer Aided Verification - CAV 2005", Lecture Notes in Computer Science, Springer, 2005, vol. 3576, pp. 281-285

[65] C. ARORA, M. TURUANI. *Validating Integrity for the Ephemerizer's Protocol with CL-Atse*, in "Formal to Practical Security: Papers Issued from the 2005-2008 French-Japanese Collaboration", Lecture Notes in Computer Science, Springer, 2009, vol. 5458, pp. 21–32

[66] T. AVANESOV, Y. CHEVALIER, M. RUSINOWITCH, M. TURUANI. *Towards the Orchestration of Secured Services under Non-disclosure Policies.*, in "6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012", St. Petersburg, Russie, Fédération De, I. V. KOTENKO, V. A. SKORMIN (editors), Lecture Notes in Computer Science, Springer, October 2012, vol. 7531, pp. 130-145 [*DOI :* 10.1007/978-3-642-33704-8_12], http://hal.inria.fr/hal-00755947

[67] G. BANA, H. COMON-LUNDH. *Towards Unconditional Soundness: Computationally Complete Symbolic Attacker*, in "Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)", Lecture Notes in Computer Science, Springer, 2012, vol. 7215, pp. 189-208

[68] F. BELLEGARDE, C. DARLOT, J. JULLIAND, O. KOUCHNARENKO. *Reformulation: a Way to Combine Dynamic Properties and Refinement*, in "International Symposium Formal Methods Europe (FME 2001)", LNCS, Springer-Verlag, 2001, vol. 2021

[69] E. BERNARD, B. LEGEARD, X. LUCK, F. PEUREUX. *Generation of Test Sequences from Formal Specifications: GSM 11-11 Standard Case-Study*, in "International Journal on Software Practice and Experience", 2004, vol. 34, n^{o} 10, pp. 915–948

[70] Y. BOICHUT, P.-C. HÉAM, O. KOUCHNARENKO. *Vérifier automatiquement les protocoles de sécurité*, in "Techniques de l'ingénieur", October 2007, pp. RE95-1–RE95-8

[71] F. BOUQUET, B. LEGEARD. *Reification of Executable Test Scripts in Formal Specification-Based Test Generation: The Java Card Transaction Mechanism Case Study*, in "Formal Methods, FME 2003", Springer-Verlag, September 2003, vol. 2805, pp. 778–795

[72] F. BOUQUET, B. LEGEARD, F. PEUREUX. *CLPS-B - A Constraint Solver for B*, in "International Conference on Tools and Algorithms for Construction and Analysis of Systems, TACAS2002", Grenoble, France, Lecture Notes in Computer Science, Springer, April 2002, vol. 2280, pp. 188–204

[73] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *Trace Equivalence Decision: Negative Tests and Non-determinism*, in "Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)", Chicago, Illinois, USA, Y. CHEN, G. DANEZIS, V. SHMATIKOV (editors), ACM Press, October 2011, pp. 321-330 [*DOI :* 10.1145/2046707.2046744], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCD-ccs11.pdf

[74] V. CORTIER, S. DELAUNE, P. LAFOURCADE. *A Survey of Algebraic Properties Used in Cryptographic Protocols*, in "Journal of Computer Security", 2006, vol. 14, n° 1, pp. 1–43

[75] F. DADEAU, K. CABRERA CASTILLOS, R. TISSOT. *Scenario-Based Testing using Symbolic Animation of B Models*, in "Software Testing, Verification and Reliability", March 2012, vol. 6, n° 22, pp. 407-434, http://hal.inria.fr/hal-00760020

[76] J. DICK, A. FAIVRE. *Automating the Generation and Sequencing of Test Cases from Model-Based Specifications*, in "FME'93: Industrial-Strength Formal Methods", Lecture Notes in Computer Science, Springer-Verlag, April 1993, vol. 670, pp. 268–284

[77] S. EVEN, O. GOLDREICH. *On the Security of Multi-Party Ping-Pong Protocols*, in "IEEE Symposium on Foundations of Computer Science", 1983, pp. 34-39, http://citeseer.ist.psu.edu/46982.html

[78] M.-C. GAUDEL, A. DENISE, S.-D. GOURAUD, R. LASSAIGNE, J. OUDINET, S. PEYRONNET. *Coverage-biased Random Exploration of Models*, in "Electr. Notes Theor. Comput. Sci.", 2008, vol. 220, n° 1, pp. 3-14

[79] P.-C. HÉAM, C. MASSON. *A Random Testing Approach Using Pushdown Automata*, in "Tests and Proofs", Zurich, Switzerland, Lecture Notes in Computer Science, Springer, 2011, vol. 6706, http://hal.inria.fr/hal-00641750/en

[80] B. LEGEARD, F. BOUQUET, N. PICKAERT. , *Industrialiser le test fonctionnel*, Management des systèmes d'information, Dunod, 2009, 266 p. , http://hal.inria.fr/inria-00430538/en/

[81] G. SÉNIZERGUES. *The Equivalence Problem for Deterministic Pushdown Automata is Decidable*, in "24th International Colloquium on Automata, Languages and Programming (ICALP'97)", Lecture Notes in Computer Science, Springer, 1997, pp. 671-681

[82] M. TURUANI. *The CL-AtSe Protocol Analyser*, in "Term Rewriting and Applications - Proc. of RTA", Seattle, WA, USA, Lecture Notes in Computer Science, 2006, vol. 4098, pp. 277–286