IN PARTNERSHIP WITH:
CNRS

Université de Franche-Comté

Université de Lorraine

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

Activity Report 2014

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, until Jun 2014]
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 [CNRS and Univ Franche-Comté]
Stéphane Glondu [Inria, partly with Caramel Project-Team]
Minh Duc Huynh [Inria, Caisse des Dépôts et Consignations]
Julien Lorrain [Inria, from Oct 2013]
Ghazi Maatoug [Inria, Caisse des Dépôts et Consignations, until Feb 2014]
Romain Sibre [Inria, from Nov 2013]

PhD Students

Hadrien Bride [Univ Franche-Comté, FEMTO-ST/DISC]
Maxime Bride [Univ Lorraine, DGA/Inria]
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]
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]
Alexandre Vernotte [Univ Franche-Comté, FEMTO-ST/DISC]
Cyrille Wiedling [Univ Lorraine, FP7 ERC ProSecure]

Post-Doctoral Fellows

Vincent Cheval [CNRS, FP7 ERC ProSecure, from May 2014]

Catalin Dragan [CNRS, FP7 ERC ProSecure, from November 2014]

Visiting Scientists

Tushant Jha [Inria internship, 3 months, from May 2014]
Gemma Puig-Quer [CNRS internship, 6 months, from Sep 2013]
Itsaka Rakotonirina [L3 ENS Cachan, 2 months, from June 2014]
Ludovic Robin [M2 Bordeaux, 5 months, from April 2014]

Administrative Assistants

Emmanuelle Deschamps [Inria]
Delphine Hubert [Univ Lorraine]
Martine Kuhlmann [CNRS]

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 correspond 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.

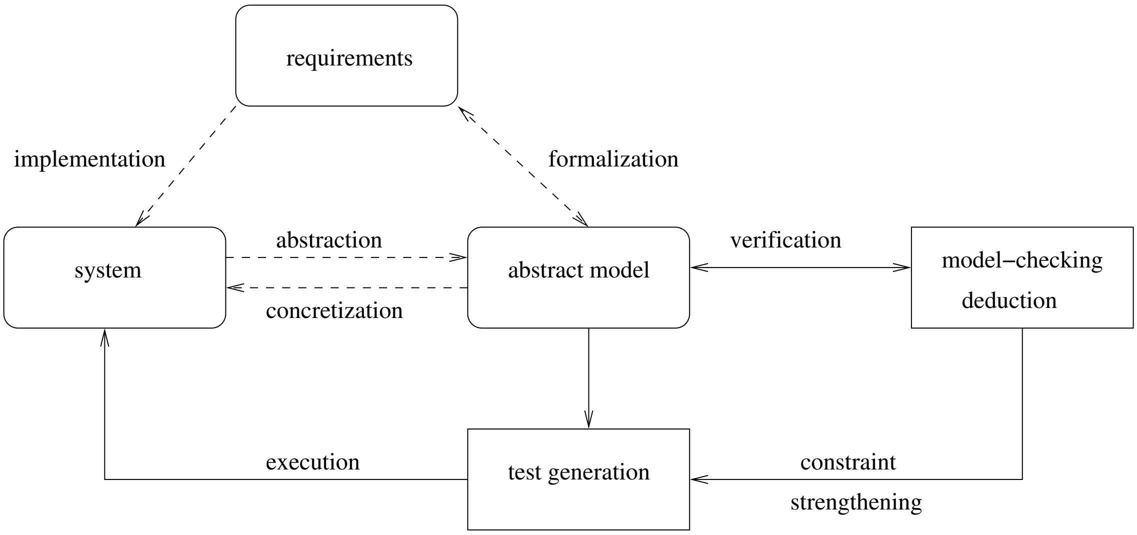

Figure 1. Software validation in Cassis.

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 $\mathcal{T}$ [74]. 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 [78].
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.

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.

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 constraintsto 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 and AVANTSSAR platforms.

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 [75] and Java Card Virtual Machine Transaction mechanism [77]), information system and for embedded software [85].

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., [81]): 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 adapt the method to 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 constitute 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. New Software and Platforms

5.1. Protocol Verification Tools

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

5.1.1. CL-AtSe

We develop *CL-AtSe*, a Constraint Logic based Attack Searcher for cryptographic protocols, initiated and continued by the European projects *AVISPA*, AVANTSSAR (for web-services) and Nessos respectively. The *CL-AtSe* approach to verification consists in a symbolic state exploration of the protocol execution for a bounded number of sessions, thus is both correct and complete. *CL-AtSe* includes a proper handling of sets, lists, 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 to analyse protocols from e.g., France Telecom R&D, Siemens AG, IETF, Gemalto, Electrum in funded projects. It is also employed by external users, e.g., from the AVISPA's community. Moreover, *CL-AtSe* achieves good analysis times, comparable and sometimes better than other state-of-the art tools.

CL-AtSe has been enhanced in various ways. It fully supports the Aslan semantics designed in the context of the AVANTSSAR project, including Horn clauses (for intruder-independent deductions, e.g., for credential management), and a large fragment of LTL-based security properties. A Bugzilla server collects bug reports, and online analysis and orchestration are available on our team server (https://cassis.loria.fr). Large models can be analysed on the TALC Cluster in Nancy with parallel processing. *CL-AtSe* also supports negative constraints on the intruder's knowledge, which reduces drastically the orchestrator's processing times and allows separation of duties and non-disclosure policies, as well as conditional security properties, like: i) an authentication to be verified iff some session key is safe; ii) relying on a leaking condition on some private data instead of an honesty predicate to trigger or block some agent's property. This was crucial for e.g., the Electrum's wallet where all clients can be dishonest but security guarantees must be preserved anyway.

5.1.2. Akiss

Akiss (Active Knowledge in Security Protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. *Akiss* implements a procedure to verify equivalence properties for a bounded number of sessions based on a fully abstract modelling of the traces of a bounded number of sessions of the protocols into first-order Horn clauses and a dedicated resolution procedure. The procedure can handle a large set of cryptographic primitives, namely those that can be modeled by an optimally reducing convergent rewrite system.

Recent developments include the possibility for checking everlasting indistinguishability properties [72]. This feature was added when analyzing everlasting privacy properties in electronic voting protocols. The tool is still under active development, including optimisations to improve efficiency, but also the addition of new features, such as the possibility to model protocols using weak secrets.

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

5.1.3. Belenios

In collaboration with the Caramel project-team, we develop an open-source private and verifiable electronic voting protocol, named *Belenios*. Our system is an evolution and a new implementation 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 a cryptographic protection against ballot stuffing and a practical threshold decryption system that allows to split the decryption key among several authorities, k out of n authorities being sufficient to decrypt. We will continue to add new cryptographic and protocol improvements to offer a secure, proved, and practical electronic voting system.

Belenios has been implemented (cf. http://belenios.gforge.inria.fr) by Stéphane Glondu and has been tested in December 2014 “in real conditions”, in a test election involving the members of Inria Nancy-Grand Est center and of the Loria lab (more than 500 potential voters) that had to elect the best pictures of the Loria.

5.1.4. SAPIC

SAPIC is a tool that translates protocols from a high-level protocol description language akin to the applied pi calculus into multiset rewrite rules, that can then be be analysed using the Tamarin Prover.

Its aim is the analysis of protocols that include states, for example Hardware Security Tokens communicating with a possibly malicious user, or protocols that rely on databases. It has been succesfully applied on several case studies including the Yubikey authentication protocol.

A recent extension, *SAPIC** extends SAPIC by a Kleene star operator (*) which allows to iterate a process a finite but arbitrary number of times. This construction is useful to specify for instance stream authentication protocols. We used it to analyse a simple version of the TESLA protocol.

The *SAPIC* tool is freely available at http://sapic.gforge.inria.fr/.

5.2. Testing Tools

Participants: Fabrice Bouquet, Frédéric Dadeau, Kalou Cabrera, Ivan Enderlin.

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:

- 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 the Z3 solver), PrologTools (encapsulating the 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 [6] 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.

5.2.3. Praspel

Praspel is both a specification language, a test data generator and test execution driver for PHP programs. These latter are annotated to describe class (resp. method) contracts using invariants (resp. pre- and postconditions). Praspel contracts allow to describe data typing informations, by means of *realistic domains*. According to the contract-driven testing principles, the tool uses the contracts to both generate test data, using dedicated test generators (random for integer variables, grammar-based for strings, constraint-based for arrays), and establish the test verdict by checking the contract assertions at run-time.

The tool is open source and freely available at: http://hoa-project.net. It has been integrated into a PHP framework named Hoa, and coupled with the atoum tool (https://github.com/atoum/atoum) that can be used to execute the tests and report on their code coverage.

5.3. 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.

We have also designed tools 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.

6. New Results

6.1. Highlights of the Year

Véronique Cortier was one of the two FLoC plenary speakers during the Vienna Summer of Logic [31].

Steve Kremer and Robert Künnemann got a paper accepted at the 35th IEEE symposium on Security and Privacy [45].

The ANR project SEQUOIA has been accepted.

BEST PAPERS AWARDS :

[43] **SeTGaM: Generalized Technique for Regression Testing Based on UML/OCL Models in Software Security and Reliability (SERE)**. E. FOURNERET, J. CANTENOT, F. BOUQUET, B. LEGEARD, J. BOTELLA.

[47] **A Maximum Variance Approach for Graph Anonymization in The 7th International Symposium on Foundations & Practice of Security FPS'2014**. H. H. NGUYEN, A. IMINE, M. RUSINOWITCH.

6.2. 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.

6.2.1. Combination of Satisfiability Procedures

Participant: Christophe Ringeissen.

A satisfiability problem is often expressed in a combination of theories, and a natural approach consists in solving the problem by combining the satisfiability procedures available for the component theories. This is the purpose of the combination method introduced by Nelson and Oppen. However, in its initial presentation, the Nelson-Oppen combination method requires the theories to be signature-disjoint and stably infinite (to guarantee the existence of an infinite model). The design of a combination method for non-disjoint unions of theories is clearly a hard task but it is worth exploring simple non-disjoint combinations that appear frequently in verification. An example is the case of shared sets, where sets are represented by unary predicates. Another example is the case of bridging functions between data structures and a target theory (e.g., a fragment of arithmetic). In collaboration with Paula Chocron (U. Buenos Aires, former intern in Cassis) and Pascal Fontaine (project-team Veridis), we have investigated both cases.

The notion of gentle theory has been introduced in the last few years as one solution to go beyond the restriction of stable infiniteness, but in the case of disjoint theories. In [36], [59], we adapt the notion of gentle theory to the non-disjoint combination of theories sharing only unary predicates (plus constants and the equality). Like in the disjoint case, combining two theories, one of them being gentle, requires some minor assumptions on the other one. We show that major classes of theories, i.e., Loewenheim and Bernays-Schoenfinkel-Ramsey, satisfy the appropriate notion of gentleness introduced for this particular non-disjoint combination framework.

We have also considered particular non-disjoint unions of theories connected via bridging functions [37]. We present a combination procedure which is proved correct for the theory of absolutely free data structures. We consider the problem of adapting the combination procedure to get a satisfiability procedure for the standard interpretations of the data structure.

6.2.2. Unification Modulo Equational Theories of Cryptographic Primitives

Participants: Christophe Ringeissen, Michaël Rusinowitch.

Asymmetric unification is a new paradigm for unification modulo theories that introduces irreducibility constraints on one side of a unification problem. It has important applications in symbolic cryptographic protocol analysis, for which it is often necessary to put irreducibility constraints on portions of a state. However many facets of asymmetric unification that are of particular interest, including its behavior under combinations of disjoint theories, remain poorly understood. In [42], [63] we give a new formulation of the method for unification in the combination of disjoint equational theories developed by Baader and Schulz that both gives additional insights into the disjoint combination problem in general, and furthermore allows us to extend the method to asymmetric unification, giving the first unification method for asymmetric unification in the combination of disjoint theories.

Some attacks exploit in a clever way the interaction between protocol rules and algebraic properties of cryptographic operators. In [79], 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 [13].

6.2.3. Enumeration of Planar Proof Terms

Participant: Alain Giorgetti.

By the Curry-Howard isomorphism, simply typed lambda terms correspond to natural deduction proofs in minimal logic. Abramsky has introduced a notion of planarity for proof terms, from a graphical representation of proofs. Noam Zeilberger and Alain Giorgetti have initiated an enumerative study of normal planar lambda terms. At the MAP 2014 workshop in Paris, Noam Zeilberger conjectured that the sequence counting the number of closed normal planar lambda terms by increasing size may coincide with the one counting the number of rooted planar maps by number of edges. Zeilberger and Giorgetti started discussing this curious coincidence at the workshop and found a proof that both families are in size-preserving bijection [70]. Although the formal aspect is not emphasized in the paper, the use of formal representations of both normal planar lambda terms and rooted planar maps, of logic programming and a proof assistant software helped much in more quickly finding the bijection. Moreover the result puts a new light on the structure of proofs in minimal logic.

6.3. 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 [76]. We have edited a book [71] where each chapter presents an important and now standard analysis technique. This year, we have written a tutorial that may serve when teaching formal analysis of security protocols [26]. We develop new techniques for richer primitives, wider classes of protocols and higher security guarantees. In Section 6.5.3 we consider derived testing techniques for verifying protocol implementations.

6.3.1. Voting Protocols

Participants: Véronique Cortier, David Galindo-Chacon, Stéphane Glondu, Steve Kremer.

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.

One famous e-voting protocol is Helios, 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 authority that provides credentials that the ballot box can verify but not forge. 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 [40], [61].

This new version has been implemented by Stéphane Glondu and has been tested in an election that involved the members of the Inria Nancy-Grand Est center and the LORIA lab (about 500 people that had to chose the best LORIA pictures).

Even a basic property like ballot secrecy is difficult to define formally and several definitions co-exist. We studied all game-based privacy definitions of the literature and discovered that none of them was satisfactory: they were either limited (not fully modeling e-voting protocols), or too strong (incompatible with verifiability), or even flawed for a few of them. Based on our findings, we have proposed a new game-based privacy definition BPRIV, proved that it implies simulation-based privacy and showed that it is realized by the Helios protocol.

Existing automated analysis techniques are inadequate to deal with commonly used cryptographic primitives, such as homomorphic encryption and mix-nets, as well as some fundamental security properties, such as verifiability. In collaboration with Matteo Maffei and Fabienne Eigner (Saarland University) we propose a novel approach based on refinement type systems for the automated analysis of two fundamental properties of e-voting protocols, namely, vote privacy and verifiability. We demonstrate the effectiveness of our approach by developing the first automated analysis of Helios using an off-the-shelf type-checker.

We have presented some of our results on e-voting as plenary speaker of FLOC 2014 [31].

6.3.2. Other Families of Protocols

Participants: Véronique Cortier, Steve Kremer, 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 [15].

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 [20], that can self-recover from corruption of arbitrary keys, provided the number of corrupted, active keys is smaller than some threshold.

Security APIs, key servers and protocols that need to keep the status of transactions, require to maintain a global, non-monotonic state, e.g., in the form of a database or register. However, most existing automated verification tools do not support the analysis of such stateful security protocols - sometimes because of fundamental reasons, such as the encoding of the protocol as Horn clauses, which are inherently monotonic. A notable exception is the recent tamarin prover which allows specifying protocols as multiset rewrite (MSR) rules, a formalism expressive enough to encode states. As multiset rewriting is a “low-level” specification language with no direct support for concurrent message passing, encoding protocols correctly is a difficult and error-prone process. In [45] we propose a process calculus with constructs for manipulation of a global state by processes running in parallel. We show that this language can be translated to MSR rules whilst preserving all security properties expressible in a dedicated first-order logic for security properties. The translation has been implemented in a prototype tool which uses the tamarin prover as a backend. We apply the tool to several case studies among which a simplified fragment of PKCS#11, the Yubikey security token, and an optimistic contract signing protocol.

6.3.3. Automated Verification of Indistinguishability Properties

Participants: Vincent Cheval, Rémy Chrétien, Véronique Cortier, 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.

Active case, unbounded number of sessions. We have studied how to reduce the search space for attacks on equivalence-based properties, for an unbounded number of sessions. Specifically, we have shown [38], [60] that if there is an attack then there is one that is well-typed. Our result holds for a large class of typing systems and a large class of *determinate* security protocols. Assuming finitely many nonces and keys, we can derive from this result that trace equivalence is decidable for an unbounded number of sessions for a class of tagged protocols, yielding one of the first decidability results for the unbounded case. As an intermediate result, we also provide a novel decision procedure in the case of a bounded number of sessions.

Active case, bounded number of sessions. We previously proposed a procedure for approximating trace equivalence in the case of a bounded number of sessions, i.e., for a replication free fragment of a cryptographic process calculus. The procedure is implemented in the *Akiss* tool. While we proved soundness and correctness for any convergent rewrite system that has the finite variant property, termination of the procedure was still an open question. We have recently shown that the procedure indeed terminates for the class of subterm convergent rewrite systems. The submission of this result is in preparation.

6.3.4. Securely Composing Protocols

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

Protocols may interact with an arbitrary attacker which yields a verification problem that has several sources of unboundedness (size of messages, number of sessions, etc.). In [14], we characterise a class of protocols for which deciding security for an unbounded number of sessions is decidable, by the means of a composition result. More precisely, we present a simple transformation which maps a protocol that is secure for a bounded number of protocol sessions (a decidable problem) to a protocol that is secure for an unbounded number of sessions. The precise number of sessions that need to be considered is a function of the security property and we show that for several classical security properties a single session is sufficient. Therefore, in many cases our result yields a design strategy for security protocols: (i) design a protocol intended to be secure for a single session; and (ii) apply our transformation to obtain a protocol which is secure for an unbounded number of sessions.

Protocols are often built in a modular way. For example, authentication protocols may assume pre-distributed keys or may assume secure channels. 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 started by Éric Le Morvan.

6.3.5. 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.

Gergei Bana and Hubert Comon have proposed a new framework [73] 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. This procedure has been extended and implemented, yielding the tool SCARY that can successfully analyse several protocols of the literature [52].

6.3.6. Advanced Cryptographic Models

Participant: David Galindo-Chacon.

A classical approach in cryptographic research consists in weakening the assumptions cryptographic primitives are built upon. The following works belong to this research line.

We generalize the decisional problem that was used to prove the security of a well-known hierarchical identity-based encryption scheme by Boneh, Boyen and Goh. We argue that our new problem is strictly harder than the original problem, and thus the security of the aforementioned cryptographic primitive is laid on even stronger foundations [24].

It is known how to transform certain canonical three-pass identification schemes into signature schemes via the Fiat-Shamir transform. Pointcheval and Stern showed that those schemes are existentially unforgeable in the random-oracle model leveraging the, at that time, novel forking lemma. Recently, a number of 5-pass identification protocols have been proposed. Extending the above technique to capture 5-pass identification schemes would allow to obtain novel unforgeable signature schemes. In this paper, we provide an extension of the forking lemma (and the Fiat-Shamir transform) in order to assess the security of what we call n-generic signature schemes. These include signature schemes that are derived from certain $(2n + 1)$-pass identification schemes. In doing so, we put forward a generic methodology for proving the security of a number of signature schemes derived from $(2n + 1)$-pass identification schemes for $n \geq 2$. As an application of this methodology, we obtain two new code-based existentially-unforgeable signature schemes, along with a security reduction. In particular, we solve an open problem in multivariate cryptography posed by Sakumoto, Shirai and Hiwatari at CRYPTO 2011 [22].

Traditionally, symbolic and computational models for cryptographic protocols do not take into account the data leaked due to the physical nature of the cryptographic computations. Recently, the research area of leakage-resilient cryptography has emerged in order to cope with this source of attacks in the computational model. We have studied a conjecture that states that an ElGamal-based public-key encryption scheme with stateful decryption resists lunch-time chosen ciphertext and leakage attacks in the only computation leaks information model. We have given a non-trivial upper bound on the amount of leakage tolerated by this conjecture. More precisely, we prove that the conjecture does not hold if more than a $(\frac{3}{8} + o(1))$ fraction of the bits are leaked at every decryption step, by showing a lunch-time attack that recovers the full secret key. The attack uses a new variant of the Hidden Number Problem, that we call Hidden Shares - Hidden Number Problem, which is of independent interest [25].

6.4. Model-based Verification

We have investigated extensions of regular model-checking to new classes of rewrite relations on terms. We have studied specification and proof of modular imperative programs, as well as of modal workflows.

6.4.1. Tree Automata with Constraints

Participants: Pierre-Cyrille Héam, Olga Kouchnarenko.

Tree automata with constraints are widely used to tackle data base algorithmic problems, particularly to analyse queries over XML documents. The model of Tree Automata with Global Constraints (TAGED) is a model introduced in 2009 for these purposes. The membership problem for TAGED is known to be NP-complete. The emptiness problem for TAGED is known to be decidable and the best known algorithm in the general case is non elementary. In collaboration with Vincent Hugot, we show that if there is at least one negative constraint, the problem is already NP-hard [64]. In the future, we plan to investigate upper bounds for the emptiness problem with a unique negative constraint. We also plan to study the complexity of the universality problem with a single constraint.

6.4.2. Random Generation of Finite Automata

Participant: Pierre-Cyrille Héam.

Developing new algorithms and heuristics raises crucial evaluation issues, as improved worst-case complexity upper-bounds do not always transcribe into clear practical gains. A suite for software performance evaluation can usually gather three types of entries: benchmarks, hard instance and random inputs, that deliver average complexity estimations, for which the catch resides in obtaining a meaningful random distribution (for instance a uniform random distribution).

In collaboration with Jean-Luc Joly, we investigate the problem of randomly and uniformly generating deterministic pushdown automata [65]. Based on a recursive counting approach, we propose a polynomial time algorithm for this purpose. The influence of the accepting condition on the generated automata is also experimentally studied.

Partially ordered automata are finite automata where simple loops have length one. They appear in several verification techniques, such as computing closures under semi-commutation relations or studying FIFO systems. In [68], we use a Markov chain based approach to randomly - and uniformly - generate deterministic partially ordered automata. The advantage of such a technique is its flexibility, allowing for instance to easily bound the number of loops. Experiments show that the mixing time seems to be polynomial, providing a tractable approach.

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

Participants: Pierre-Cyrille Héam, 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 collaboration with Vincent Hugot, 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.

6.4.4. Machine-Learning Techniques for Regular Model-Checking

Participants: Maxime Bride, Pierre-Cyrille Héam.

Using a machine-learning approach, we address the general problem of regular model-checking of computing $R^*(L)$, when L is a regular language and R a relation. Rather than developing specific algorithms to compute $R^*(L)$, it consists in using Angluin style's algorithms. In [58], we focus on the generation of examples, counter-examples and on the design of an oracle for the specific case of semi-commutation relations. Experiments are promising, particularly for the sizes of the obtained automata, which are quite smaller than with dedicated algorithms.

6.4.5. Constraint Solving for Verifying Modal Workflow Specifications

Participants: Hadrien Bride, Olga Kouchnarenko.

Workflow Petri nets are well suited for modelling and analysing discrete event systems exhibiting behaviours such as concurrency, conflict, and causal dependency between events. They represent finite or infinite-state processes, and several important verification problems, like reachability or soundness, are known to be decidable. Modal specifications introduced in [84] allow loose or partial specifications in a framework based on process algebras.

Our work in [34] focuses on the verification of modal workflow specifications using constraint solving as a computational tool. Its main contribution consists of a formal framework based on constraint systems to model executions of workflow Petri nets and their structural properties, as well as to verify their modal specifications. An implementation and promising experimental results obtained within the proposed approach constitute a practical contribution. In particular, a business process example from the IT domain enables to successfully assess the reliability of our contributions.

6.4.6. 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 [17]. It is proposed as a Maple$^{\text{TM}}$ package for rule-based programming, rewriting strategies and their combination with standard Maple$^{\text{TM}}$ 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 [29].

6.5. 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 [55]. The test generation uses various underlying techniques such as symbolic animation of models [80], or symbolic execution of programs by means of dedicated constraints, SMT solvers, or model-checkers.

6.5.1. Automated Test Generation from Behavioral Models

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

We have developed an original model-based testing approach that takes a behavioral view (modelled in UML) of the system under test and automatically generates test cases and executable test scripts according to model coverage criteria [18]. We continue to extend this result to SysML specifications for validating embedded systems. We apply this method on smartSurface [44].

In the context of the FSN DAST project on Dynamic Application Security Testing, we investigated the use of a model-based testing approach for vulnerability testing in web applications. We designed a process based on two artefacts. First, a generic UML model, that is used to represent the web application entities (pages, forms, etc.), coupled with OCL constraints that describe the business logics of the application. Second, a set of test purposes, that will look for specific vulnerabilities (cross-site scripting, SQL injections, etc.). We have implemented a research prototype and applied it on several case studies. It has shown its effectiveness to detect vulnerabilities on already deployed web applications [50].

6.5.2. 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 proposed a dedicated formalism to express test properties. A test property is first translated into a finite state automaton which describes a monitor of its behaviors. We have also 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 [41]. This process has been fully tool-supported into an integrated software prototype[1]. This process has been designed during the ANR TASCCC project (2009-2012) and was continued during the ANR ASTRID OSEP project (2012-2013). The industrialization of this approach, and its integration within commercial test generation tools has started with the ANR ASTRID Maturation MBT_Sec project (2014-2015).

In the context of the SecureChange project, we have also investigated 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 [43].

6.5.3. Mutation-based Testing of Security Protocols

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

We have proposed a model-based penetration testing approach for security protocols [41]. 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. We have applied our technique on protocols designed in HLPSL, and implemented the protocol mutation tool jMuHLPSL that performs the mutations. The mutants are then analyzed by *CL-AtSe*. 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* 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[2]. We also investigated the transformation of an attack trace into executable tests scripts. To achieve that, we have proposed 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. Experimentations on these principles have been described in [53].

6.5.4. Code and Contract-based Test Generation and Static Analysis

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

[1] A video of the prototype is available at: http://vimeo.com/53210102

[2] http://www.nbs-system.com/blog/faille-securite-magento-paypal.html

With the CEA we have developed a test generation technique based on C code and formal specifications, to facilitate deductive verification, in a new tool named StaDy [67], [49], [51]. The tool integrates the concolic test generator PathCrawler within the static analysis platform Frama-C. StaDy is able to handle the ANSI C Specification Language (ACSL) of the framework and other Frama-C plug-ins are able to reuse results from the test generator. This tool is designed to be the foundation stone of modular static and dynamic analysis combinations in the Frama-C platform.

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 aiming to avoid rejection during the generation of array structures. Finally, we have proposed dedicated specification coverage criteria to drive the test generation process. These coverage criteria focus on the selection of a subset of a method's contract, or the selection of specific predicates or realistic domains inside the contract. The whole approach has been implemented into a dedicated framework [62] integrated with state-of-the-practice test execution environments, such as atoum.

6.5.5. *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 [82] 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 [83], we have proposed a new approach, extending [82], to manage stack-call during the random test generation while preserving uniformity. In [23], 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.

6.6. 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.

6.6.1. *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 [56]) generates an attack trace describing the execution of 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 [16] we develop our alternative approach based on *parametrized 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. The existence of a service orchestrator solving a service composition problem can alternatively be reduced to the satisfiability of formula in parametrized propositional dynamic logic, and the latter was shown decidable in [33].

We now work on synthesizing composed services that satisfy required security policies.

6.6.2. 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 [11], 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. We give extensive experimental results, based on real-life DTDs, that show the efficiency and scalability of our system.

6.6.3. Secure Computation in Social Networks

Participants: Bao Thien Hoang, Abdessamad Imine, Huu Hiep Nguyen, Michaël Rusinowitch.

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 publish social graph data for achieving in-depth studies. To securely perform these large-scale computations, we need the design of reliable protocols to ensure the data privacy. To address the polling problem in social networks (where the privacy of exchanged information and user reputation are very critical), we provide a simple decentralized polling protocol that relies on the current state of social graphs. More explicitly, we define one family of social graphs that satisfy what we call the m-broadcasting property (where m is less than or equal to a minimum node degree). We show their structures enable low communication cost and constitute necessary and sufficient condition to ensure vote privacy and limit the impact of dishonest users on the accuracy of the polling output. To securely publish social graph data, we focus on the problem of anonymizing a deterministic graph by converting it into an uncertain form [48], [47]. We first analyze drawbacks in a recent uncertainty-based anonymization scheme and then propose Maximum Variance, a novel approach that gains better tradeoff between privacy and utility. Towards a fair comparison between the anonymization schemes on graphs, the second contribution of our work is to describe a quantifying framework for graph anonymization by assessing privacy and utility scores of typical schemes in a unified space.

6.6.4. Safe and Secure Protocols for Collaborative Applications

Participants: Abdessamad Imine, Michaël Rusinowitch.

The Operational Transformation (OT) approach, used in many collaborative editors, allows a group of users to concurrently update replicas of a shared object and exchange their updates in any order. The basic idea is to transform any received update operation before its execution on a replica of the object. Designing transformation functions for achieving convergence of object replicas is a critical and challenging issue. In this work, we investigate the existence of transformation functions [27]. From the theoretical point of view, two properties, named TP1 and TP2, are necessary and sufficient to ensure convergence. Using controller synthesis technique, we show that there are some transformation functions, which satisfy TP1 for the basic signatures of insert and delete operations. But, there is no transformation function, which satisfies both TP1 and TP2. Consequently, a transformation function which satisfies both TP1 and TP2 must necessarily have additional parameters in the signatures of some update operations. Accordingly, we provide a new transformation function and show formally that it ensures convergence.

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 use 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. To validate our approach, we implement an optimistic access control on the top of 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 [30], 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. F. Bouquet is scientific consultant of Smartesting.

7.2. Electronic Voting Systems

Participant: Véronique Cortier.

A collaboration agreement has been signed between Loria and Scytl, a Spanish company who is proposing solutions for the organization of on-line elections, including legally binding elections, in several countries. We have a collaboration with David Galindo (who joined Scytl in July 2014) on defining security properties for e-voting (privacy as well as verifiability properties) and designing e-voting schemes that meet all these properties. Further contracts may cover the analysis of the solutions developed at Scytl.

7.3. Analysis of Electrum Bitcoin Wallet

Participants: Michaël Rusinowitch, Mathieu Turuani.

Electrum has signed a 2-month contract with Cassis for verifying its electronic bitcoin wallet. The protocol model has been specified in Aslan language and covers then registration of new users, the confirmation phase, and the usage of the wallet by the clients. Many optimisations techniques had to be used to limit state explosion, and *CL-AtSe* has been extended to cover a class of security properties with negative constraints that appear in this model, and might be useful for other protocol analysis. *CL-AtSe* has been applied to several scenarios to verify the security properties, and a few modifications were suggested to Electrum designer.

8. Partnerships and Cooperations

8.1. Regional Initiatives

- The 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 micro-systems, in particular for a distributed micro airduct. Several teams of the FEMTO-ST institute work together on micro-systems specification, simulation and validation.

8.2. National Initiatives

8.2.1. ANR

- ANR PROSE *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 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 SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, starting in October 2014. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalence. The increasing use of observational equivalence as a modeling tool shows the need for new tools and techniques that are able to analyze such equivalence properties. The aims of this project are *(i)* to investigate which process equivalences-among the plethora of existing ones-are appropriate for a given security property, system assumptions and attacker capabilities; *(ii)* to advance the state-of-the-art of automated verification for process equivalences, allowing for instance support for more cryptographic primitives, relevant for case studies; *(iii)* to study protocols that use low-entropy secrets expressed using process equivalences; *(iv)* to apply these results to case studies from electronic voting.

8.2.2. Fondation MAIF

Project *Protection de l'information personnelle sur les réseaux sociaux*, duration: 3 years, started in October 2014. The goal of the project is to lay the foundation for a risk verification environment on privacy in social networks. Given social relations, this environment will rely on the study of metrics to characterize the security level for a user. Next, by combining symbolic and statistical techniques, it is a question to synthesize a model of risk behavior as a rule base. Finally, a verifier à la model-checking will be developed to assess the security level of user. Partners are Cassis (leader), Orpailleur and Fondation Maif.

8.2.3. *Competitivity Clusters*

- Project "Investissement d'Avenir - Développement de l'Economie 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 focusses on developping tools for service security verification and testing tasks.
- ProSecure (2011-2016) [3]— 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 (2012-2014) [4] — *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 defining game-based privacy for e-voting protocols.
- Collaboration with Myrto Arapinis (University of Edinburgh) on simplification results for the formal analysis of e-voting protocols.

[3] http://www.loria.fr/~cortier/ProSecure.html

[4] http://www.loria.fr/~ringeiss/CHILI/bananas

- Collaboration with Matteo Maffei (CISPA, Germany) on type systems for e-voting systems.
- 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-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), March, December 2014
- David Bernhard (Bristol University), March 2014
- Fabienne Eigner (University of Saarbruecken), February, May 2014
- Joshua Guttman (MITRE), January 2014
- Olivier Pereira (University of Louvain-la-Neuve), March 2014
- Nicolas Pouillard (DemTech, University of Copenhagen), February 2014

8.5.1.1. Internships

Tushant Jha

Subject: Synthesis of Secure Services Composition

Supervisor: Michaël Rusinowitch

Date: from May 2014 until July 2014

Institution: IIIT Hyderabad

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)

Itsaka Rakotonirina

Subject: Automated verification of security protocols with loops

Supervisor: Steve Kremer

Date: from June 2014 until July 2014

Institution: ENS Cachan

Ludovic Robin

Subject: Analysis of security protocols using weak secrets

Supervisor: Steve Kremer

Date: from April 2014 until September 2014

Institution: U. Bordeaux

9. Dissemination

9.1. Promoting Scientific Activities

The CNIL (Commission Nationale Informatique et Liberté) has official recommendations in terms of electronic voting [5]. These recommendations influence the design of e-voting systems that are deployed in France. However, some of the recommendations seem a bit outdated and dedicated to particular classes of systems. Even more importantly, the CNIL recommendations focus on vote privacy but do not say much about verifiability. Véronique Cortier, David Galindo, and Stéphane Glondu have formulated new recommendations, submitted to the CNIL. They have met some CNIL members to discuss how to integrate some of the propositions to the new version of the CNIL recommendations that should appear in 2015.

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Véronique Cortier: FMS 2014, 5th Workshop on Formal Methods for Security.
Christophe Ringeissen: UNIF 2014, 28th International Workshop on Unification.

9.1.2. Scientific Events Selection

9.1.2.1. Program Committee Chair

- Steve Kremer: Post 2014, ACM SEC@SAC 2014, GRSRD'15

9.1.2.2. Program Committee Member

- Véronique Cortier: ACNS 2014, CCS 2014, Esorics 2014, FCC-FCS 2014, FoSSaCs 2014, Icalp 2014, Movep 2014, Concur 2015, LICS 2015, POST 2015.
- Christophe Ringeissen: CADE-25, FroCoS 2015.
- Frédéric Dadeau : CSTVA 2014, NFM 2014, QSIC 2014.
- Abdessamad Imine : AICCSA 2014, DEXA 2014, DEXA 2015, ICEIS 2015, DASFAA 2015
- Steve Kremer : ACNS 2014, ICFEM 2014, AsiaCCS 2015, ESORICS 2015, FCS 2015, TGC 2015.
- Michaël Rusinowitch: LATA 2014, CRISIS 2014, STP 2014, GRSRD 2014, TGC 2015, POST 2016.
- Fabrice Bouquet : ICST 2014, MoDeVVa 2014, AMOST 2015

9.1.3. Journal

9.1.3.1. Editorial Board Member

- Véronique Cortier: Information & Computation, Journal of Computer Security.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Summer School:

  Fabrice Bouquet, Test techniques and validation for Software, ENVOL 2014, Organized by: CNRS, INRA, VetAgro-Sup and Inria, November 18-21, 2014 (https://www.projet-plume.org/envol-2014)

  Steve Kremer, Formal Modeling and Automated Analysis of Security Protocols, 14th International School on Foundations of Security Analysis and Design (FOSAD'14)

[5] http://www.cnil.fr/documentation/deliberations/deliberation/accessible/non/delib/249/

- Master:

  Fabrice Bouquet, Functional Testing, 18 hours, M2 Computer science, Franche-Comté University, France.

  Fabrice Bouquet, Artificial Intelligence, 42 hours, M1 Computer science, Franche-Comté University, France.

  Frédéric Dadeau, Structural testing, 9 hours (ETD), M2 Computer science, Franche-Comté University, France.

  Alain Giorgetti, Program Proofs, 58 hours, M1 Computer science, Franche-Comté University, France.

  Alain Giorgetti, Decision Procedures, 13 hours, M2 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Specification, Verification and Validation, 12 hours (ETD), M2 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Security and Components, 10,5 hours (ETD), M2 Computer science, Franche-Comté University, France.

  Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.

  Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, 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, 22.5 hours (ETD), M2 Computer science, Lorraine University, France.

  Laurent Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Lorraine University, France.

- Licence:

  Alain Giorgetti, Logics and Deduction, 52 hours, L2 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Formal Languages, 65 hours (ETD), L3 Computer science, Franche-Comté University, France.

- E-Learning:

  Fabrice Bouquet, Artificial Intelligence, 78 (ETD), M1 Computer science, Franche-Comté University, France.

  Fabrice Bouquet, Specification Validation and Test, 39 (ETD), M2 Computer science, Franche-Comté University, France.

  Alain Giorgetti, Formal Methods, 81 hours, L3 computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Languages, Specification and Proof, 25 hours (ETD), L3 Computer science, Franche-Comté University, France.

  Olga Kouchnarenko, Compositional approaches in verification, 18 hours (ETD), M2 Computer science, Franche-Comté University, France.

9.2.2. Supervision

- PhD (defended in 2014):

  Robert Künnemann, Verification of Security APIs, January 7, Steve Kremer and Graham Steel

Houari Mahfoud, Access Control Models for XML Documents, February 18, Abdessamad Imine and Michaël Rusinowitch

Cyrille Wiedling, Formal analysis of E-voting protocols, November 21, Véronique Cortier

Ivan Enderlin, Test Data Generation for Unit Testing in PHP, July 16, Fabrice Bouquet, Frédéric Dadeau and Alain Giorgetti

Aloïs Dreyfus, Contribution to the efficient model-based verification and testing, October 22, Pierre-Cyrille Héam and Olga Kouchnarenko

Bin Yang, Contribution to a kernel of a symbolic asymptotic modeling software, December 16, Michel Lenczner and Alain Giorgetti

- 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

  Maxime Bride, Automated Synthesis and Verification of Security Services, started in October 2014, Michaël Rusinowitch

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

  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

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

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

  Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, Steve Kremer

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

9.2.3. Juries

Inria evaluation committee (Véronique Cortier, Steve Kremer, Michaël Rusinowitch)

Vice-president of the Jury Junior Research Position Inria Nancy Grand Est (Véronique Cortier)

Jury Junior Research Position Inria Paris-Rocquencourt (Véronique Cortier)

Preselection Jury for Inria Advanced and Starting Research Positions (Michaël Rusinowitch)

Member of the ANR scientific evaluation committee, challenges 7 and 9 (Olga Kouchnarenko)

Examiner for Guillaume Laville PhD, Besançon, June 27, 2014, *Exécution efficace de systèmes multi-agents sur GPU* (Fabrice Bouquet)

Reviewer for Maxime Fonda PhD, Bourges, May 21, 2014, *Protection obligatoire des serveurs d'application web : application aux processus métiers* (Fabrice Bouquet)

Examiner for Yufang Dan PhD, CITI Lyon (France), Security and self-healability enforcement of dynamic components in a service-oriented system, May 14, 2014 (Frédéric Dadeau)

Examiner for Xiaoping Che PhD, Telecom SudParis (France), Cross-Fertilizing Formal Approaches for Protocol Conformance and Performance Testing, June 26, 2014 (Frédéric Dadeau)

Examiner for Kaim Hossem PhD, LIG Grenoble (France), *Inférence automatique de modèles d'applications web et protocoles pour la détection de vulnérabilités*, December 15, 2014 (Frédéric Dadeau)

Reviewer for Valérie Murat PhD, Rennes, June 26th 2014, Tree automata extensions for the infinite states systems verification (Pierre-Cyrille Héam)

Examiner for Rafik Kheddam PhD, Valence (France), Safety software approaches for RFID systems, April 9, 2014 (Pierre-Cyrille Héam)

Examiner for Sven DeFelice PhD, Marne-la-Vallée, Codeterministic automata and acyclic automata: analysis of algorithm and random generation, July 1, 2014 (Pierre-Cyrille Héam)

Examiner for Maguy Medlej PhD, Besançon, June 30, 2014, Data Management in Periodic Wireless Sensor Networks (Olga Kouchnarenko)

Reviewer for Hikmat Farhat PhD, Toulouse, September 25, 2014, Composition of Services Behavior via Orchestrator Synthesis (Olga Kouchnarenko)

Examiner for Evelyne Contejean HDR, Orsay, June 13, 2014, Facets of Deduction (Michaël Rusinowitch)

Examiner for Myriam Paiola PhD, Paris, May 28, 2014, Verification of Security Protocols with Lists (Michaël Rusinowitch)

Examiner for Joshua Amavi PhD, Orléans, November 28, 2014, *Comparaison et évolution de schémas XML* (Michaël Rusinowitch)

Examiner for Lakhdar Akroun PhD, Clermont-Ferrand, December 8, 2014, Decidability and complexity of simulation preorder for data-centric web services (Michaël Rusinowitch)

Reviewer for Abdelkader Kersani PhD, Grenoble, October 30, 2014, *Preuves par induction dans le calcul de superposition* (Laurent Vigneron)

9.3. Popularization

Presentation of security protocols to high school teachers in Computer Science (April 17th, 2014, Véronique Cortier).

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, W. ARSAC, T. AVANESOV, M. BARLETTA, A. CALVI, A. CAPPAI, R. CARBONE, Y. CHEVALIER, L. COMPAGNA, J. CUÉLLAR, G. ERZSE, S. FRAU, M. MINEA, S. MÖDERSHEIM, D. VON OHEIMB, G. PELLEGRINO, S. E. PONTA, M. ROCCHETTO, M. RUSINOWITCH, M. T. DASHTI, M. TURUANI, L. VIGANÒ. *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, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings", Lecture Notes in Computer Science, Springer, 2012, vol. 7214, pp. 267–282

[3] 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

[4] R. CHADHA, S. CIOBACA, S. KREMER. *Automated Verification of Equivalence Properties of Cryptographic Protocols*, in "Programming Languages and Systems - 21st European Symposium on Programming, ESOP 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings", H. SEIDL (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7211, pp. 108–127

[5] V. CORTIER, B. SMYTH. *Attacking and fixing Helios: An analysis of ballot secrecy*, in "Journal of Computer Security", 2013, vol. 21, n^o 1, pp. 89–148

[6] 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

[7] 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

[8] 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

[9] A. DREYFUS. *Contribution to the efficient model-based verification andtesting*, Université de Franche-Comté, October 2014, https://hal.inria.fr/tel-01090759

[10] I. ENDERLIN. *Automated Unit Test Generation with Praspel, a Specification Language for PHP*, Université de Franche-Comté, July 2014, https://hal.inria.fr/tel-01093355

[11] H. MAHFOUD. *Efficient Access Control to XML Data: Querying and Updating Problems*, Université de Lorraine, February 2014, https://tel.archives-ouvertes.fr/tel-01093661

[12] C. WIEDLING. *Formal Verification of Advanced Families of Security Protocols: E-Voting and APIs*, Université de Lorraine, November 2014, https://tel.archives-ouvertes.fr/tel-01107718

Articles in International Peer-Reviewed Journals

[13] 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, vol. 10, n^o 1:5, pp. 1-26 [*DOI :* 10.2168/LMCS-10(1:5)2014], https://hal.archives-ouvertes.fr/hal-00854841

[14] M. Arapinis, S. Delaune, S. Kremer. *Dynamic Tags for Security Protocols*, in "Logical Methods in Computer Science (LMCS)", June 2014, vol. 10, n^{o} 2, 50 p. [*DOI :* 10.2168/LMCS-10(2:11)2014], https://hal.inria.fr/hal-01090766

[15] M. Arnaud, V. Cortier, S. Delaune. *Modeling and Verifying Ad Hoc Routing Protocols*, in "Information and Computation", 2014, vol. 238, 38 p. , forthcoming, https://hal.inria.fr/hal-00881009

[16] W. Belkhir, Y. Chevalier, M. Rusinowitch. *Parametrized automata simulation and application to service composition*, in "Journal of Symbolic Computation", September 2014, 21 p. , https://hal.inria.fr/hal-01089128

[17] W. Belkhir, A. Giorgetti, M. Lenczner. *A Symbolic Transformation Language and its Application to a Multiscale Method*, in "Journal of Symbolic Computation", November 2014, vol. 65, pp. 49 - 78, https://hal.inria.fr/hal-00917323

[18] J. Cantenot, F. Ambert, F. Bouquet. *Test generation with SMT solvers in Model Based Testing*, in "Journal of Software Testing, Verification, and Reliability", 2014, vol. 24, n^{o} 7, 33 p. [*DOI :* 10.1002/stvr.1537], https://hal.inria.fr/hal-01093461

[19] A. Cherif, A. Imine, M. Rusinowitch. *Practical access control management for distributed collaborative editors*, in "Pervasive and Mobile Computing", December 2014, pp. 62-86, https://hal.archives-ouvertes.fr/hal-01094068

[20] V. Cortier, G. Steel. *A Generic Security API for Symmetric Key Management on Cryptographic Devices*, in "Information and Computation", 2014, vol. 238, 25 p. , https://hal.inria.fr/hal-00881072

[21] F. Dadeau, P.-C. Héam, R. Kheddam, G. Maatoug, M. Rusinowitch. *Model-based mutation testing from security protocols in HLPSL*, in "Journal of Software Testing, Verification, and Reliability", April 2014, 30 p. [*DOI :* 10.1002/stvr.1531], https://hal.inria.fr/hal-01090881

[22] Ö. Dagdelen, D. Galindo, P. Véron, S. M. El Yousfi Alaoui, P.-L. Cayrel. *Extended security arguments for signature schemes*, in "Designs, Codes and Cryptography", September 2014, 23 p. [*DOI :* 10.1007/s10623-014-0009-7], https://hal.inria.fr/hal-01091185

[23] A. Dreyfus, P.-C. Héam, O. Kouchnarenko, C. Masson. *A random testing approach using pushdown automata*, in "Journal of Software Testing, Verification, and Reliability", 2014, vol. 24, pp. 656 - 683 [*DOI :* 10.1002/stvr.1526], https://hal.inria.fr/hal-01088712

[24] D. Galindo. *Compact hierarchical identity-based encryption based on a harder decisional problem*, in "International Journal of Computer Mathematics", April 2014 [*DOI :* 10.1080/00207160.2014.912278], https://hal.inria.fr/hal-01011299

[25] D. Galindo, S. Vivek. *Limits of a conjecture on a leakage-resilient cryptosystem*, in "Information Processing Letters", April 2014, vol. 114, n^{o} 4, pp. 192-196 [*DOI :* 10.1016/j.ipl.2013.11.014], https://hal.inria.fr/hal-00933429

[26] S. Kremer, V. Cortier. *Formal Models and Techniques for Analyzing Security Protocols: A Tutorial*, in "Foundations and Trends in Programming Languages", September 2014, vol. 1, n^{o} 3, 117 p. [*DOI :* 10.1561/2500000001], https://hal.inria.fr/hal-01090874

[27] A. Randolph, H. Boucheneb, A. Imine, A. Quintero. *On Synthesizing a Consistent Operational Transformation Approach*, in "IEEE Transactions on Computers", February 2015, 1 p. , https://hal.archives-ouvertes.fr/hal-01094030

[28] E. Tushkanova, A. Giorgetti, C. Ringeissen, O. Kouchnarenko. *A rule-based system for automatic decidability and combinability*, in "Science of Computer Programming", March 2015, vol. 99, pp. 3-23 [*DOI :* 10.1016/j.scico.2014.02.005], https://hal.inria.fr/hal-01102883

[29] B. Yang, W. Belkhir, M. Lenczner. *Computer-Aided Derivation of Multi-scale Models: A Rewriting Framework*, in "International Journal for Multiscale Computational Engineering", January 2014, vol. 12, n^{o} 2, pp. 91–114, https://hal.inria.fr/hal-00916568

Articles in National Peer-Reviewed Journals

[30] A. Randolph, A. Imine, H. Boucheneb, A. Quintero. *Spécification et Analyse d'un Protocole de Contrôle d'Accès Optimiste pour Éditeurs Collaboratifs Répartis*, in "ISI (Ingénierie des Systèmes d'information)", January 2015, 1 p. , https://hal.archives-ouvertes.fr/hal-01093982

Invited Conferences

[31] V. Cortier. *Electronic Voting: How Logic Can Help*, in "12th International Joint Conference on Automated Reasoning (IJCAR 2014)", Vienne, Austria, July 2014, https://hal.inria.fr/hal-01080294

[32] M. Rusinowitch. *Automated Verification of Security Protocols and Services* , in "Third International Seminar on Program Verification, Automated Debugging and Symbolic Computation", Vienna, Austria, Tudor Jebelean; Wei Li ; Dongming Wang, July 2014, https://hal.inria.fr/hal-01090000

International Conferences with Proceedings

[33] W. Belkhir, G. Rossi, M. Rusinowitch. *A Parametrized Propositional Dynamic Logic with Application to Service Synthesis*, in "Advances in Modal Logic", Groningen, Netherlands, Advances in Modal Logic, August 2014, vol. 10, pp. 34-53, https://hal.inria.fr/hal-01087829

[34] H. Bride, O. Kouchnarenko, F. Peureux. *Verifying Modal Workflow Specifications Using Constraint Solving*, in "IFM - The 11th International Conference on Integrated Formal Methods", Bertinoro, Italy, LNCS, September 2014, n^{o} 8739, pp. 171 - 186 [*DOI :* 10.1007/978-3-319-10181-1_11], https://hal.inria.fr/hal-01091283

[35] V. Cheval, V. Cortier. *Timing attacks in security protocols: symbolic framework and proof techniques*, in "4th Conference on Principles of Security and Trust (POST 2015)", Londres, United Kingdom, April 2015, https://hal.inria.fr/hal-01103618

[36] P. Chocron, P. Fontaine, C. Ringeissen. *A Gentle Non-Disjoint Combination of Satisfiability Procedures*, in "Automated Reasoning - 7th International Joint Conference, IJCAR 2014, Held as Part of the Vienna Summer of Logic", Vienna, Austria, Lecture Notes in Computer Science, Springer, July 2014, vol. 8562, pp. 122-136 [*DOI :* 10.1007/978-3-319-08587-6_9], https://hal.inria.fr/hal-01087162

[37] P. Chocron, P. Fontaine, C. Ringeissen. *Satisfiability Modulo Non-Disjoint Combinations of Theories Connected via Bridging Functions*, in "Workshop on Automated Deduction: Decidability, Complexity, Tractability, ADDCT 2014. Held as Part of the Vienna Summer of Logic, affiliated with IJCAR 2014 and RTA

2014", Vienna, Austria, Silvio Ghilardi, Ulrike Sattler, Viorica Sofronie-Stokkermans, July 2014, https://hal.inria.fr/hal-01087218

[38] R. Chrétien, V. Cortier, S. Delaune. *Typing messages for free in security protocols: the case of equivalence properties*, in "25th International Conference on Concurrency Theory (CONCUR'14)", Rome, Italy, September 2014, https://hal.inria.fr/hal-01080293

[39] V. Cortier, F. Eigner, S. Kremer, M. Maffei, C. Wiedling. *Type-Based Verification of Electronic Voting Protocols*, in "4th Conference on Principles of Security and Trust (POST)", London, United Kingdom, Springer, 2015, https://hal.inria.fr/hal-01103545

[40] V. Cortier, D. Galindo, S. Glondu, M. Izabachène. *Election Verifiability for Helios under Weaker Trust Assumptions*, in "Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS'14)", Wroclaw, Poland, September 2014, https://hal.inria.fr/hal-01080292

[41] F. Dadeau, K. Cabrera Castillos, J. Julliand. *Coverage Criteria for Model-Based Testing using Property Patterns*, in "MBT 2014, 9th Workshop on Model-Based Testing, Satellite workshop of ETAPS 2014", Grenoble, France, A. K. Petrenko, B.-H. Schlingloff (editors), EPTCS, Electronic Proceedings in Theoretical Computer Science, April 2014, vol. 141, 15 p. [*DOI :* 10.4204/EPTCS.141.3], https://hal.inria.fr/hal-01089687

[42] S. Erbatur, D. Kapur, A. Marshall, C. Meadows, P. Narendran, C. Ringeissen. *On Asymmetric Unification and the Combination Problem in Disjoint Theories*, in "Foundations of Software Science and Computation Structures - 17th International Conference, FOSSACS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS", Grenoble, France, Lecture Notes in Computer Science, Springer, April 2014, n^{o} 8412, 15 p. [*DOI :* 10.1007/978-3-642-54830-7_18], https://hal.inria.fr/hal-01087065

[43] *Best Paper*
E. Fourneret, J. Cantenot, F. Bouquet, B. Legeard, J. Botella. *SeTGaM: Generalized Technique for Regression Testing Based on UML/OCL Models*, in "Software Security and Reliability (SERE)", San Francisco, CA, France, Software Security and Reliability (SERE), 2014 Eighth International Conference on, June 2014, 19 p. , Best paper Award of the conference [*DOI :* 10.1109/SERE.2014.28], https://hal.inria.fr/hal-01093493.

[44] A. Hammad, F. Bouquet, J.-M. Gauthier, D. Gendreau. *Modeling and simulation of modular complex system: Application to air-jet conveyor*, in "Advanced Intelligent Mechatronics (AIM)", Besançon, France, AIM 2014, IEEE/ASME Int. Conf. on Advanced Intelligent Mechatronics, IEEE, July 2014, 6 p. [*DOI :* 10.1109/AIM.2014.6878244], https://hal.inria.fr/hal-01093474

[45] S. Kremer, R. Künnemann. *Automated Analysis of Security Protocols with Global State*, in "35th IEEE Symposium on Security and Privacy (S&P'14)", San Jose, United States, I. C. Society (editor), 2014, pp. 163–178 [*DOI :* 10.1109/SP.2014.18], https://hal.inria.fr/hal-01091241

[46] A. Lanoix, O. Kouchnarenko. *Component Substitution through Dynamic Reconfigurations*, in "11th International Workshop on Formal Engineering approaches to Software Components and Architectures, Satellite event of ETAPS", Grenoble, France, April 2014, 14 p. , https://hal.archives-ouvertes.fr/hal-00935129

[47] *Best Paper*
H. H. Nguyen, A. Imine, M. Rusinowitch. *A Maximum Variance Approach for Graph Anonymization*, in "The 7th International Symposium on Foundations & Practice of Security FPS'2014", Montreal, Canada, November 2014, Best Paper Award, https://hal.inria.fr/hal-01092442.

[48] H. H. Nguyen, A. Imine, M. Rusinowitch. *Enforcing Privacy in Decentralized Mobile Social Networks*, in "ESSoS Doctoral Symposium 2014", Munich, Germany, February 2014, https://hal.inria.fr/hal-01092447

[49] G. Petiot, N. Kosmatov, A. Giorgetti, J. Julliand. *How Test Generation Helps Software Specification and Deductive Verification in Frama-C*, in "Tests and Proofs", York, United Kingdom, M. Seidl, N. Tillmann (editors), Lecture Notes in Computer Science, Springer, July 2014, vol. 8570, pp. 204 - 211 [*DOI :* 10.1007/978-3-319-09099-3_16], https://hal.inria.fr/hal-01108553

[50] A. Vernotte, F. Dadeau, F. Lebeau, B. Legeard, F. Peureux, F. Piat. *Efficient Detection of Multi-step Cross-Site Scripting Vulnerabilities*, in "ICISS - 10th International Conference on Information Systems Security", Hyderabad, India, Springer, December 2014, vol. LNCS 8880, https://hal.inria.fr/hal-01089702

National Conferences with Proceedings

[51] R. Genestier, A. Giorgetti, G. Petiot. *Gagnez sur tous les tableaux*, in "Vingt-sixièmes Journées Francophones des Langages Applicatifs (JFLA 2015)", Le Val d'Ajol, France, D. Baelde, J. Alglave (editors), January 2015, https://hal.inria.fr/hal-01099135

Conferences without Proceedings

[52] H. Comon-Lundh, V. Cortier, G. Scerri. *A tool for automating the computationally complete symbolic attacker (Extended Abstract)*, in "Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC'14)", Vienne, Austria, July 2014, https://hal.inria.fr/hal-01080296

[53] G. Maatoug, F. Dadeau, M. Rusinowitch. *Model-Based Vulnerability Testing of Payment Protocol Implementations*, in "HotSpot'14 - 2nd Workshop on Hot Issues in Security Principles and Trust, affiliated with ETAPS 2014", Grenoble, France, April 2014, https://hal.inria.fr/hal-01089682

[54] H. H. Nguyen, I. Abdessamad, M. Rusinowitch. *Anonymizing Social Graphs via Uncertainty Semantics*, in "ASIACCS 2015 - 10th ACM Symposium on Information, Computer and Communications Security", Singapour, April 2015, https://hal.inria.fr/hal-01108437

Scientific Books (or Scientific Book chapters)

[55] F. Bouquet, F. Peureux, F. Ambert. *Model-Based Testing for Functional and Security Test Generation*, in "Foundations of Security Analysis and Design VII", A. Aldini, J. Lopez, F. Martinelli (editors), LNCS, Springer International Publishing, 2014, vol. 8604, 33 p. [*DOI :* 10.1007/978-3-319-10082-1_1], https://hal.inria.fr/hal-01093442

[56] J. A. Martin, F. Martinelli, I. Matteucci, E. Pimentel, M. Turuani. *On the Synthesis of Secure Services Composition*, in "Engineering Secure Future Internet Services and Systems", M. Heisel, W. Joosen, J. Lopez, F. Martinelli (editors), Lecture Notes in Computer Science, Springer, June 2014, vol. LNCS 8431, n^{o} 8431, 392 p. , https://hal.inria.fr/hal-01094964

Books or Proceedings Editing

[57] M. ABADI, S. KREMER (editors). *Principles of Security and Trust*, Lecture Notes in Computer Science, SpringerFrance, 2014, vol. 8414 [*DOI :* 10.1007/978-3-642-54792-8], https://hal.inria.fr/hal-01090879

Research Reports

[58] M. BRIDE, P.-C. HÉAM, I. JACQUES. *Computing Semicommutation Closures: a Machine Learning Approach*, FEMTO-ST, December 2014, https://hal.inria.fr/hal-01087740

[59] P. CHOCRON, P. FONTAINE, C. RINGEISSEN. *A Gentle Non-Disjoint Combination of Satisfiability Procedures (Extended Version)*, April 2014, n^o RR-8529, https://hal.inria.fr/hal-00985135

[60] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. *Typing messages for free in security protocols: the case of equivalence properties*, June 2014, n^o RR-8546, 46 p. , https://hal.inria.fr/hal-01007580

[61] V. CORTIER, D. GALINDO, S. GLONDU, M. IZABACHÈNE. *Election Verifiability for Helios under Weaker Trust Assumptions*, June 2014, n^o RR-8555, 20 p. , https://hal.inria.fr/hal-01011294

[62] I. ENDERLIN, F. BOUQUET, F. DADEAU, A. GIORGETTI. *Praspel: Contract-Driven Testing for PHP using Realistic Domains*, September 2014, n^o RR-8592, 39 p. , https://hal.inria.fr/hal-01061900

[63] S. ERBATUR, D. KAPUR, A. MARSHALL, C. MEADOWS, P. NARENDRAN, C. RINGEISSEN. *Asymmetric Unification and the Combination Problem in Disjoint Theories*, February 2014, n^o RR-8476, https://hal.inria.fr/hal-00947088

[64] P.-C. HÉAM, V. HUGOT, O. KOUCHNARENKO. *The Emptiness Problem for Tree Automata with at Least One Disequality Constraint is NP-hard*, FEMTO-ST, December 2014, https://hal.inria.fr/hal-01089711

[65] P.-C. HÉAM, J.-L. JOLY. *Random Generation and Enumeration of Accessible Determinisitic Real-time Pushdown Automata*, FEMTO-ST, September 2014, https://hal.inria.fr/hal-01087748

[66] S. KREMER, R. KÜNNEMANN. *Automated analysis of security protocols with global state*, arXiv, March 2014, 56 p. , https://hal.inria.fr/hal-00955869

[67] G. PETIOT, N. KOSMATOV, A. GIORGETTI, J. JULLIAND. *StaDy: Deep Integration of Static and Dynamic Analysis in Frama-C*, May 2014, https://hal.inria.fr/hal-00992159

Other Publications

[68] P.-C. HÉAM, J.-L. JOLY. *On the Uniform Random Generation of Determinisitic Partially Ordered Automata using Monte Carlo Techniques*, December 2014, https://hal.inria.fr/hal-01087751

[69] O. KOUCHNARENKO, J.-F. WEBER. *Decentralised Evaluation of Temporal Patterns over Component-based Systems at Runtime*, 2014, Long version of the paper accepted for FACS 2014 - The 11th International Symposium on Formal Aspects of Component Software, https://hal.archives-ouvertes.fr/hal-01044639

[70] N. ZEILBERGER, A. GIORGETTI. *A correspondence between rooted planar maps and normal planar lambda terms*, August 2014, https://hal.inria.fr/hal-01057269

References in notes

[71] 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

[72] M. Arapinis, V. Cortier, S. Kremer, M. Ryan. *Practical Everlasting Privacy*, in "Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings", D. A. Basin, J. C. Mitchell (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7796, pp. 21–40

[73] 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

[74] 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

[75] 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

[76] 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

[77] 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

[78] 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

[79] V. Cortier, S. Delaune, P. Lafourcade. *A Survey of Algebraic Properties Used in Cryptographic Protocols*, in "Journal of Computer Security", 2006, vol. 14, n^{o} 1, pp. 1–43

[80] 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^{o} 22, pp. 407-434, http://hal.inria.fr/hal-00760020

[81] 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

[82] 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^{o} 1, pp. 3-14

[83] 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

[84] K. G. LARSEN, B. THOMSEN. *A modal process logic*, in "Proc. of the 3rd Annual Symp. on Logic in Computer Science (LICS'88)", IEEE, July 1988, pp. 203–210

[85] 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/