IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Cachan

Activity Report 2013

Project-Team SECSI

Security of information systems

IN COLLABORATION WITH: Laboratoire specification et vérification (LSV)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Programs, Verification and Proofs

Table of contents

Project-Team SECSI

Keywords: Formal Methods, Automated Theorem Proving, Cryptography, Protocols, Model-checking, Security

SECSI is a project common to Inria and the Laboratoire Spécification et Vérification (LSV), itself a common lab between CNRS (UMR 8643) and the École Normale Supérieure (ENS) de Cachan. The team was created in 2001, and became an Inria projet in December, 2002.

Creation of the Project-Team: 2002 November 15*, updated into Team:* 2013 January 01, end of the Project-Team: 2013 December 31.

1. Members

Research Scientist
Stéphanie Delaune [CNRS, Researcher, HdR]

Faculty Members
Jean Goubault-Larrecq [Team leader, ENS Cachan, Professor, HdR]
David Baelde [ENS Cachan, Maître de Conférences]
Hubert Comon-Lundh [ENS Cachan, Professor, HdR]

Engineer
Pierre-Arnaud Sentucq [Inria, granted by DGA SEREBC Bruz, from Apr 2013]

PhD Students
Lucca Hirschi [ENS Cachan, from Sep. 2013]
Rémy Chrétien [ANR JCJC VIP grant, Started Oct. 2012]
Guillaume Scerri [ERC grant ProSecure, Started Oct. 2011]

Administrative Assistant
Thida Iem [Inria]

2. Overall Objectives

2.1. Overall Objectives

SECSI is a common project between Inria Saclay and the LSV (Laboratoire Spécification et Vérification), itself a common research unit of CNRS (UMR 8643) and the ENS (École Normale Supérieure) de Cachan.

The SECSI project is a research project on verification algorithms for information system security, with two main thrusts: verification of cryptographic protocols, intrusion detection.

3. Research Program

3.1. Foundations

Computer security has become more and more pressing as a concern since the mid 1990s. There are several reasons to this: cryptography is no longer a *chasse réservée* of the military, and has become ubiquitous; and computer networks (e.g., the Internet) have grown considerably and have generated numerous opportunities for attacks and misbehaviors, notably.

The aim of the SECSI project is to *develop logic-based verification techniques for security properties of computer systems and networks*. Let us explain what this means, and what this does not mean.

First, the scope of the research at SECSI started as a rather broad subset of computer security, although the core of SECSI's activities has always been on verifying cryptographic protocols.

We took this for granted in 2006, and decided to concentrate on the latter. This already includes a vast number of concerns.

First, there is a plethora of distinct *security properties* one may wish to verify. Beyond the standard properties of secrecy (weak or strong forms), or authentication, one considers anonymity, fairness in contract-signing, and the subtle security properties involved in electronic voting such as accountability, receipt-freeness, resistance to coercion, or user verifiability. Some of these properties are trace properties, some are not, and are therefore more complex to state and verify.

Second, there are many available *models*. SECSI started with the rather simple symbolic models of security known today as Dolev-Yao models. One must then look at process algebra models (spi-calculus, applied pi-calculus), which allow for a symbolic treatment of more complex properties, especially those that are not trace properties. And one must also look at the computational models favored by cryptographers, e.g., the game-based approaches and the universal composability/simulatability approaches. They are more realistic in terms of security, but less directly amenable to automated verification. One of the features of computational models that makes them more complex is the need for computing, and bounding probabilities of certain events. This led us into contributing to the field of verification of probabilistic systems. One must also look at the relations between these models.

Third, there are many important *applications*. While SECSI started looking at the rather simple and now mundane confidentiality and authentication protocols, two important application domains have emerged: the verification of electronic voting protocols, and the verification of cryptographic APIs.

Apart from cryptographic protocols, the initial vision of the SECSI project was that computer security, being a global concern, should be taken as a whole, as far as possible. This is why one of the initial objectives of SECSI included topic in intrusion detection, again seen from the logical point of view.

One should remember the following. First, one of the key phrases in the SECSI motto is "logic-based". It is a founding theme of SECSI that logic matters in security, and opportunities are to be grabbed. Another key phrase is "verification techniques". The expertise of SECSI is not in designing protocols or security architectures. Verifying protocols, formally, is an arduous task already, and has proved to be an extremely rich area.

3.2. Objectives

SECSI has five objectives:

- Objective 1: symbolic verification of cryptographic protocols. Tree-automata based methods, automated deduction, and approximate/exact cryptographic protocol verification in the Dolev-Yao model. Enriching the Dolev-Yao model with algebraic theories, and associated decision problems.
- Objective 2: verification of cryptographic protocols in computational models. Computational soundness of formal models (Dolev-Yao, applied pi-calculus).
- Objective 3: security of group protocols, fair exchange, voting and other protocols. Other security properties, other security models. Security properties based on notions of indistinguishability.
- Objective 4: probabilistic transition systems. Security in the presence of probabilistic and demonic non-deterministic choices.
- Objective 5: intrusion detection, network and host protection in the large.

4. Application Domains

4.1. Application Domains

Here are a few examples of applications of research done in SECSI:

- Security of electronic voting schemes: the case of the Helios protocol, used in particular at University of Louvain-la-Neuve (2010) and at the International Association for Cryptographic Research (IACR).
- Security of the protocols involved in the TPM (Trusted Platform Module) chip, a chip present in most PC laptops today, and which is meant to act as a trusted base.
- Security of the European electronic passport—and the discovery of an attack on the French implementation of it.
- Intrusion detection with the Orchids tool: several interested partners, among which EADS Cassidian, Thales, Galois Inc. (USA), the French Direction Générale de l'Armement (DGA).

5. Software and Platforms

5.1. Orchids

Participants: Jean Goubault-Larrecq [correspondant], Pierre-Arnaud Sentucq.

The ORCHIDS real-time intrusion detection system was created in 2003-04 at SECSI. Orchids is at the core of a contract between Inria and DGA, started in April 2013, for three years.

Progress in 2013 included:

- Creation of a collection of VirtualBox virtual machines with a pre-installed instance of Orchids, for easy testing and/or installation.
- A collection of scripts, allowing one to rebuild the above cited virtual machines automatically from the sources, as a nightly build (in progress).
- A new algorithm for evaluating the worst-case thread complexity of detection by Orchids, whose first principles were laid out by Jean Goubault-Larrecq, and with two prototype implementations done by Jean-Philippe Lachance, a young L2 intern from Université Laval, Québec. The purpose is to warn users of the complexity of the tasks they delegate to Orchids, and to avert denial of service attacks on Orchids itself.

Objectives for 2014 include:

- Simplifying the Orchids installation process, which has gotten complicated over the years.
- Implementing a frontend tool incorporating the full-fledged version of the worst-case thread complexity algorithm mentioned above, plus some other checks.

6. New Results

6.1. Dishonest keys (Objective 2)

Participants: Hubert Comon-Lundh, Guillaume Scerri.

One of the main issues in the formal verification of the security protocols is the validity (and scope) of the formal model. Otherwise, it may happen that a protocol is proved and later someone finds an attack. This paradoxical situation may happen when the formal model used in the proof is too abstract.

A main stream of research therefore consists in proving full abstraction results (also called *soundness*): if the protocol is secure in the (symbolic) model, then an attack can only occur with negligible probability in a computational model. Such results have two main drawbacks: first they are very complicated, and have to be completed again and again for each combination of security primitives. Second, they require strong hypotheses on the primitives, some of which are not realistic. For instance, it is assumed that the attacker cannot forge his own keys (or that all keys come with their certificates, even for symmetric encryption keys).

Hubert Comon-Lundh, Véronique Cortier and Guillaume Scerri had proposed an extension of the symbolic model in 2012, and proved it computationally sound, without this restriction on the dishonest keys.

6.2. Deciding trace equivalence

Participants: David Baelde, Stéphanie Delaune, Rémy Chrétien, Lucca Hirschi.

Most existing results focus on trace properties like secrecy or authentication. There are however several security properties, which cannot be defined (or cannot be naturally defined) as trace properties and require the notion of indistinguishably. Typical examples are anonymity, privacy related properties or statements closer to security properties used in cryptography.

In the framework of the applied pi-calculus as in similar languages based on equational logics, indistinguishably corresponds to a relation called trace equivalence. Roughly, two processes are trace equivalent when an observer cannot see any difference between the two processes. Static equivalence applies only to observations on finite sets of messages, and do not take into account the dynamic behavior of a process whereas the notion of trace equivalence is more general and takes into account this aspect.

6.2.1. Static equivalence.

As explained above, static equivalence is a cornerstone to provide decision procedures for observational equivalence.

Stéphanie Delaune, in collaboration with Mathieu Baudet and Véronique Cortier, has designed a generic procedure for deducibility and static equivalence that takes as input any convergent rewrite system [12]. They have shown that their algorithm covers most of the existing decision procedures for convergent theories. They also provide an efficient implementation. This paper is a journal version of the work presented at RTA'09.

6.2.2. Trace equivalence.

When the processes under study do not contain replication, trace equivalence can be reduced to the problem of deciding symbolic equivalence [13]. Thanks to this reduction and relying on a result first proved by M. Baudet, this yields the first decidability result of observational equivalence for a general class of equational theories (for processes without else branches and without replication). Moreover, based on another decidability result for deciding equivalence between sets of constraint systems, we get decidability of trace equivalence for processes with else branch for standard primitives.

Even though there are some implementations of the procedures described above, this does not suffice to obtain practical tools. Current prototypes suffer from a classical combinatorial explosion problem caused by the exploration of many interleavings in the behaviour of processes. David Baelde, Stéphanie Delaune, and Lucca Hirschi revisit a work due to Mödersheim et al., generalize it and adapt it for equivalence checking. They obtain an optimization in the form of a reduced symbolic semantics that eliminates redundant interleavings on the fly. This work will be published as:

- D. Baelde, S. Delaune, and L. Hirschi. A Reduced Semantics for Deciding Trace Equivalence using Constraint Systems. In *Proc. 3rd Conference on Principles of Security and Trust (POST 2014)*, Grenoble, April 2014, France.

When processes under study contain replication, the approach relying on symbolic equivalence does not work anymore. Moreover, since it is well-known that deciding reachability properties is undecidable under various restrictions, there is actually no hope to do better for equivalence-based properties. Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune provide the first results of (un)decidability for certain classes of protocols for the equivalence problem. They consider a class of protocols shown to be decidable for reachability properties, and establish a first undecidability result. Then, they restrained the class of protocols a step further by making the protocols deterministic in some sense and preventing it from disclosing secret keys. This tighter class of protocols was then shown to be decidable after reduction to an equivalence between deterministic pushdown automata. This work has been published at ICALP'13 [14].

To deal with replication, another approach has been studied by Vincent Cheval in collaboration with Bruno Blanchet. They propose an extension of the automatic protocol verifier ProVerif. ProVerif can prove observational equivalence between processes that have the same structure but differ by the messages they contain. In order to extend the class of equivalences that ProVerif handles, they extend the language of terms by defining more functions (destructors) by rewrite rules. These extensions have been implemented in ProVerif and allow one to automatically prove anonymity in the private authentication protocol by Abadi and Fournet. This work is part of Vincent Cheval's PhD thesis, and was published as:

- V. Cheval, B. Blanchet. Proving More Observational Equivalences with ProVerif. In *2nd Conference on Principles of Security and Trust (POST 2013)*. David Basin, John Mitchell, eds. Springer Verlag, Lecture Notes in Computer Science 7796, 2013.

6.3. Mobile ad-hoc networks

Participants: Rémy Chrétien, Stéphanie Delaune.

Mobile ad hoc networks consist of mobile wireless devices which autonomously organize their communication infrastructure: each node provides the function of a router and relays packets on paths to other nodes. Finding these paths in an a priori unknown and constantly changing network topology is a crucial functionality of any ad hoc network. Specific protocols, called *routing protocols*, are designed to ensure this functionality known as *route discovery*. Secured versions of routing protocols have been proposed to provide more guarantees on the resulting routes, and some of them have been designed to protect the privacy of the users.

Rémy Chrétien and Stéphanie Delaune propose a framework for analysing privacy-type properties for routing protocols. They use the notion of equivalence between traces to formalise three security properties related to privacy, namely indistinguishability, unlinkability, and anonymity. They study the relationship between these definitions and we illustrate them using two versions of the ANODR routing protocol. This work was published as:

- R. Chrétien, S. Delaune. Formal Analysis of Privacy for Routing Protocols in Mobile Ad Hoc Networks. *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. Springer 2013. Lecture Notes in Computer Science. ISBN 978-3-642-36829-5. Pages 1-20.

6.4. Composition results

Participant: Stéphanie Delaune.

Formal methods have proved their usefulness for analysing the security of protocols. However, protocols are often analysed in isolation, and this is well-known to be not sufficient as soon as the protocols share some keys.

Stéphanie Delaune, in collaboration with Céline Chevalier, Steve Kremer, and Mark Ryan, study whether password protocols can be safely composed, even when a same password is reused. More precisely, they present a transformation which maps a password protocol that is secure for a single protocol session (a decidable problem) to a protocol that is secure for an unbounded number of sessions. Their result provides an effective strategy to design secure password protocols: (i) design a protocol intended to be secure for one protocol session; (ii) apply their transformation and obtain a protocol which is secure for an unbounded number of sessions. Their technique also applies to compose different password protocols allowing one to obtain both inter-protocol and inter-session composition. This work was published as:

- C. Chevalier, S. Delaune, S. Kremer and M. Ryan. Composition of Password-based Protocols. *Formal Methods in System Design* 43(3), pages 369-413, 2013.

6.5. Unconditional Soundness (Objective 2)

Participants: Hubert Comon-Lundh, Guillaume Scerri.

Hubert Comon-Lundh, Véronique Cortier and Guillaume Scerri had shown in a 2012 CCS paper how one could drop one of the assumptions of computational soundness results. However, the proofs remain very complicated and there are still assumptions such as the absence of key cycles, or no dynamic corruption... that are still necessary for all these results.

Gergei Bana and Hubert Comon-Lundh investigated a completely different approach to formal security proofs in a 2012 POST paper, which does not make any such assumptions. The idea can be stated in a nutshell: whereas all existing formal models state the attacker's abilities, they propose to formally state what the attacker *cannot* do.

This makes a big difference, since the soundness need only to be proved formula by formula and only the very necessary assumptions are used for such formulas (for instance, no absence of key cycles is needed). This does not need to be proved again when a primitive is added.

Once the general setting is fixed, the question was how practical is the method. We studied the complexity of the consistency proofs in this setting and showed that we can complete such proofs in Polynomial Time for a wide class of axioms in

- H. Comon-Lundh, V. Cortier and G. Scerri. Tractable inference systems: an extension with a deducibility predicate. In CADE'13, LNAI 7898, pages 91-108. Springer, 2013

The development of a prototype implementation is under development. We expect to complete experiments on a number of protocols.

6.6. Static Analysis of Programs with Imprecise Probabilities

Participant: Jean Goubault-Larrecq [correspondant].

Static analyses allows one to obtain guarantees about the behavior of programs, without running them. Programs that handle numerical data such as feedback control loops pose a challenge in this area. This gets even harder when one considers programs that read numerical data from sensors, and write to actuators, as these data are imprecise, and are governed by probability distributions that may themselves be unknown, and only know to fall into some interval of distributions.

As part of the ANR projet blanc CPP, an efficient static analysis framework that deals with this kind of programs was proposed in 2011 by J. Goubault-Larrecq, O. Bouissou, E. Goubault, Sylvie Putot, based on P-boxes and Dempster-Shafer structures to handle imprecise probabilities.

The semantic foundations were made clearer, a new, improved algorithm was proposed, and new applications were examined in:

- A. Adjé, O. Bouissou, J. Goubault-Larrecq, E. Goubault and S. Putot. Static Analysis of Programs with Imprecise Probabilistic Inputs. In *VSTTE'13*, LNCS. Springer, 2013.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- ANR programme blanc CPP ("Confidence, Probability, and Proofs"), 2009-April 2013. Partners: LSV (scientific leader), CEA LIST (co-leader), Inria (Comète, Parsifal), Ecole Supérieure d'Electricité (L2S, SSE). External partners: Safran, Dassault Systèmes.

  In the context of proofs of safety properties for critical software, The CPP project proposes to study the joint use of probabilistic and formal (deterministic) semantics and analysis methods, in a way to improve the applicability and precision of static analysis methods on numerical programs. See http://www.lix.polytechnique.fr/~bouissou/cpp/index.php.

- ANR VERSO program ProSe ("Proofs of Security"), 2010-2014. Partners: Inria (Cascade, leader; Cassis), LSV, Verimag.

  The goal of the ProSe project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the *symbolic* level, in which messages are terms; the *computational* level, in which messages are bitstrings; and the *implementation* level: the program itself. This project is a continuation of the FormaCrypt project. See https://crypto.di.ens.fr/projects:prose:main.

- ANR JCJC project VIP, 2012-2015. Awarded to Stéphanie Delaune.

  The aim of this project is to formally analyze modern applications in which privacy plays an important role. Many applications having an important societal impact are concerned by privacy, e.g. electronic voting, electronic auction protocols, RFID tags, safety critical application in vehicular ad hoc networks, routing protocols in mobile ad hoc networks, etc. Moreover, each application comes with its own specificities. E.g. e-voting protocols often rely on complex cryptographic primitives, some routing protocols rely on recursive tests, and so on. In mobile ad hoc networks, taking into account mobility issues is also an important challenge.

  Because security protocols are notoriously difficult to design and analyse, formal verification techniques are extremely important. However, nearly all studies focus on trace-based security properties, and thus to not allow one to analyse privacy-type properties that play an important role in many modern applications. Moreover, the envisioned applications have some specificities that prevent them to be modelled in an accurate way with existing verification tools.

  The goal of this project is to design verification algorithms to analyse privacy-type properties on several applications having an important societal impact. The project is accompanied by an effort in case studies and application domains which will allow at the end of the project an assessment of the pragmatic potential both in terms of modelling and effective analysis. More details are available on the web page of the project: http://www.lsv.ens-cachan.fr/Projects/anr-vip/.

- Inria-DGA contract, on evaluation of the Orchids tool. This is a 3-year contract, starting in April 2013, on the evaluation and improvement of the Orchids intrusion detection tool. The actual contents of the contract is not public.

7.2. International Initiatives

7.2.1. Inria International Partners

7.2.1.1. Informal International Partners

- Mark D. Ryan, U. Birmingham
- Alwen Tiu, Australian National University
- Achim Jung, U. Birmingham
- Frédéric Mynard, Georgia Southern University
- Roberto Segala, U. Verona
- Dominique Unruh, U. Tallinn

7.2.2. Participation In other International Programs

- Inria Project Lab CAPPRIS (Collaborative Action on the Protection of Privacy Rights in the Information Society). Member: Stéphanie Delaune.

  The goal of CAPPRIS is to provide solutions to enhance the privacy protection in the Information Society. The targeted applications are Online Social Networks, Location Based Services, and Electronic Health Record Systems.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

- Dominique Unruh, Tallinn, 1 month, January 2013.
- Mark Ryan, Birmingham, 2 weeks, July 2013.
- Achim Jung, Birmingham, 1 month, April-May 2013.

7.3.1.1. Internships

Stéphanie Delaune et David Baelde co-supervised the following master student:

- Lucca Hirschi, ENS Lyon, "Réduction d'ordre partiel pour les propriétés d'équivalence", 2013.

Jean Goubault-Larrecq supervised the following L2 student:

- Jean-Philippe Lachance, U. Laval, Québec, "Evaluation automatique de la complexité de détection des signatures Orchids", 2013.

8. Dissemination

8.1. Scientific Animation

Administrative charges:

- Hubert Comon-Lundh is member of the "comité de pilotage", labex Digicosme.
- Hubert Comon-Lundh is member of the "commission formation", labex Digicosme.
- Hubert Comon-Lundh is member of the "Jury prix de these Gilles Kahn/SIF".
- Hubert Comon-Lundh is member of the jury "appel à projets Digiteo"
- Hubert Comon-Lundh is member of the Master MPRI studies committee and director of the MPRI until sept. 2013.
- Stéphanie Delaune has been a member of the scientific committee of Inria Saclay since February 2012.
- Stéphanie Delaune has been "Déléguée aux thèses" at the École Doctorale Sciences Pratiques at ENS Cachan since September 2012.
- Jean Goubault-Larrecq is in charge of computer science questions, common Ecole Polytechnique-ENS Paris, Lyon, Cachan-ESPCI entrance competitive exam, starting September 2012.

Editorial boards:

- Hubert Comon-Lundh is associate editor of the ACM Transactions on Computational Logic.

Participation to program committes of conferences:

- 16th International Conference on Foundations of Software Science and Computation Structures FoSSaCS'13, Rome, Italy, March 2013 (Jean Goubault-Larrecq).
- 24th International Conference on Automated Deduction (CADE), Lake Placid, New York, USA, 2013 (Stéphanie Delaune)
- 26th IEEE Computer Security Foundations Symposium (CSF), Tulane University, New Orleans LA, USA, 2013 (Stéphanie Delaune)
- 24th International Conference on Rewriting Techniques and Applications (RTA), Eindhoven, The Netherlands, 2013 (Stéphanie Delaune)
- 20th Workshop on Logic, Language, Information and Computation (WoLLIC), Darmstadt, Germany, 2013 (Stéphanie Delaune)
- Worshop *Formal and Computational Cryptography (FCC)*, president of the program commitee. June 30, 2013, New Orleans (Hubert Comon-Lundh).
- Workshop on *Logical Frameworks and Meta-Languages: Theory and Practice* LFMTP'13, Boston, U.S.A., September 2013 (David Baelde).
- Workshop on *Fixed Points in Computer Science* FICS'13, Torino, Italy, September 2013 (David Baelde).
- 24th Journées Francophones des Langages Applicatifs JFLA'13, Aussois, France, February 2013 (David Baelde).

Organization of conferences:

- Workshop on *Fixed Points in Computer Science* FICS'13, Torino, Italy, September 2013 (David Baelde).
- 25th Journées Francophones des Langages Applicatifs JFLA'14, Fréjus, France, January 2014 (David Baelde).

Selection committees:

- Hubert Comon-Lundh was president of the "Maitre de Conférences" selection committee, ENS Paris, 2013.
- Hubert Comon-Lundh was member of the selection committee of "Maitre de conférences" selection committee, Univ. Paris-Diderot, 2013.
- Hubert Comon-Lundh was member of the Inria Paris-Rocquencourt junior researche selection committee, 2013.
- Jean Goubault-Larrecq was member of the Inria Saclay-Ile-de-France junior researcher selection committee, 2013.

Scientific boards:

- Hubert Comon-Lundh, CNRS INSII, Oct. 2010-Oct 2014
- Hubert Comon-Lundh, scientific committee, labex CPU.
- Hubert Comon-Lundh, scientific committee, LIPN.
- Jean Goubault-Larrecq, external member of the selection committee of the Formal Methods and Security Inria-DGA seminar, Rennes
- Jean Goubault-Larrecq, external member of the selection committee of the Formal Methods and Security Inria-DGA seminar, Rennes
- Jean Goubault-Larrecq, member of the scientific committee of the Labex "Fondation Sciences Mathématiques de Paris".
- Jean Goubault-Larrecq, member of the scientific committe of the "Ecole de Printemps d'Informatique Théorique" (EPIT).

Invited talks:

- Hubert Comon-Lundh, *LICS: Logic in Computer Security*, invited tutorial, IEEE Symp. Logic in Computer Science, New Orleans, July 2013.
- Jean Goubault-Larrecq, *A few Pearls in the Theory of Quasi-Metric Spaces*, semi-plenary talk, Summer Topology Conference, North Bay, Ontario, Canada, July 23-26, 2013.
- Jean Goubault-Larrecq, *A Simple Proof of the Schröder-Simpson Theorem*, session on Asymmetric Topology, Summer Topology Conference, North Bay, Ontario, Canada, July 23-26, 2013.
- Jean Goubault-Larrecq, *A Constructive Proof of the Topological Kruskal Theorem*, Mathematical Foundations of Computer Science (MFCS), IST Austria, near Vienna, Austria, August 26-30, 2013.
- Jean Goubault-Larrecq, *Is Mathematical Rigor Needed in Intrusion Detection?*, Foundations and Practice of Security (FPS), La Rochelle, France, October 21, 2013.

Invitation to seminars:

- Hubert Comon-Lundh, *Towards Unconditonal Soundness*, IRISA, Rennes, Feb 1, 2013.
- Hubert Comon-Lundh, *Computationally Sound Automated Proofs of Security*, LRI, Orsay, March 15, 2013.
- Jean Goubault-Larrecq, *Orchids, ou: de l'importance de la sémantique*, séminaire DGA Innosciences, DGA, Bagneux, June 25, 2013.
- Jean Goubault-Larrecq, *Full Abstraction for Non-Deterministic and Probabilistic Extensions of PCF*, Pierre-Louis Curien Festschrift, Venice, Italy, September 9-11, 2013.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence :

- Rémy Chrétien, *Initiation à l'informatique* (TP), 39h., L1, Université Paris 7, Paris, France
- Hubert Comon-Lundh *Logic and Computability*, 42h., L3, ENS Cachan, France
- Jean Goubault-Larrecq, *Programming*, 42h., L3, ENS Cachan, France
- Jean Goubault-Larrecq, *Logic and Computer Science* (a.k.a., the lambda-calculus), 36h., L3, ENS Cachan and ENS Paris, France
- Jean Goubault-Larrecq, Internship reviews, 4h., L3, ENS Cachan, France
- David Baelde, *Logic and Computer Science*, 24h., L3, ENS Cachan, France
- David Baelde, *Logic II*, 22.5h., L3, ENS Cachan, France
- David Baelde, *Programming II*, 22.5h., L3, ENS Cachan, France
- David Baelde, Internship reviews, 3h., L3, ENS Cachan, France

Master :

- Jean Goubault-Larrecq, *Cryptography, Cryptographic Protocols and Quantum Cryptography*, Part 1/3, 3h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Stéphanie Delaune, *Cryptography, Cryptographic Protocols and Quantum Cryptography*, Part 2/3, 3h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Jean Goubault-Larrecq, *Advanced Complexity*, 42h., M1, MPRI course 1-17, France
- David Baelde, *Software Engineering Project*, 30h., M1, ENS Cachan, France
- Jean Goubault-Larrecq, Internship reviews, 4h., M1, ENS Cachan, France
- Hubert Comon-Lundh, Internship reviews, 32h, M2 MPRI
- Jean Goubault-Larrecq, Internship reviews, 16h., M2, MPRI, France
- Hubert Comon-Lundh *Preparation option info agreg: logique*, 24h, préparation à l'agrégation de Mathématiques, Jan-May 2012, ENS Cachan, France
- Hubert Comon-Lundh, rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 18h., ENS Cachan, France
- Hubert Comon-Lundh, *Tree Automata*, M1, MPRI, 22h
- Jean Goubault-Larrecq, rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 18h., ENS Cachan, France

8.2.2. Supervision

PhD in progress :

- Rémy Chrétien, *Trace equivalence for an unbounded number of sessions*, Started Oct. 2012, supervised by Stéphanie Delaune and Véronique Cortier
- Lucca Hirschi, *Reduction techniques for equivalence-based properties*, Started Sep. 2013, supervised by David Baelde and Stéphanie Delaune
- Guillaume Scerri, *Preuves abstraites de protocoles cryptographiques concrets*, Started Oct. 2011, supervised by Hubert Comon-Lundh

8.2.3. Juries

- PhD:

  - Jean Goubault-Larrecq, member of the jury: Rémi Bonnet, *Decidability and Undecidability in Vector Addition Systems with one (or more !) Zero-Tests*, ENS Cachan, January 22, 2013.
  - Jean Goubault-Larrecq, president of the jury: Song Fu, *On Pushdown Systems Model Checking: Application to Malware Detection and Software Model-Checking*, U. Paris Diderot, April 12, 2013.
  - Jean Goubault-Larrecq, president of the jury: Alexis Goyet, *The $\lambda\overline{\lambda}$-calculus, A Dual Calculus for Unconstrained Strategies*, U. Paris Diderot, December 11, 2013.
  - Jean Goubault-Larrecq, member of the jury: David Cadé, *Imple´mentations de protocoles cryptographiques prouve´es dans le mode`le calculatoire*, U. Paris Diderot, December 16, 2014.
  - Jean Goubault-Larrecq, member of the mid-term evaluation jury: Pablo Rauzy, SupTelecom Paris Tech, December 4, 2013.
- HdR:
  - Hubert Comon-Lundh, president of the jury: Jérôme Leroux. *Presburger Counter Machines*, Bordeaux, Dec.6, 2012.
  - Jean Goubault-Larrecq, reviewer and member of the jury: Michele Pagani, *Some Advances in Linear Logic*, U. Paris Nord Villetaneuse, December 5, 2013.
  - Jean Goubault-Larrecq, reviewer and member of the jury: Michele Pagani, *Some Advances in Linear Logic*, U. Paris Nord Villetaneuse, December 5, 2013.

8.3. Popularization

- Stéphanie Delaune, member of the scientific mediation committee at Inria Saclay. (“Mediation” is the new name for popularization.)
- Rémy Chrétien and Stéphanie Delaune, *La protection des informations sensibles*, article in *Pour La Science*, Nov. 2013.

9. Bibliography

Major publications by the team in recent years

[1] M. BAUDET, V. CORTIER, S. KREMER. *Computationally Sound Implementations of Equational Theories against Passive Adversaries*, in "Information and Computation", April 2009, vol. 207, n^{o} 4, pp. 496-520 [*DOI :* 10.1016/J.IC.2008.12.005], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCK-ic09.pdf

[2] M. BORTOLOZZO, M. CENTENARO, R. FOCARDI, G. STEEL. *Attacking and Fixing PKCS#11 Security Tokens*, in "Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10)", Chicago, Illinois, USA, ACM Press, October 2010, pp. 260-269 [*DOI :* 10.1145/1866307.1866337], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCFS-ccs10.pdf

[3] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *Trace Equivalence Decision: Negative Tests and Non-determinism*, in "Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)", Chicago, Illinois, USA, ACM Press, October 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCD-ccs11.pdf

[4] H. COMON-LUNDH, V. CORTIER. *Tree Automata with One Memory, Set Constraints and Cryptographic Protocols*, in "Theoretical Computer Science", February 2005, vol. 331, n° 1, pp. 143-214 [*DOI :* 10.1016/J.TCS.2004.09.036], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/ComonCortierTCS1.ps

[5] H. COMON-LUNDH, V. CORTIER. *Computational soundness of observational equivalence*, in "Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS'08)", Alexandria, Virginia, USA, ACM Press, October 2008, pp. 109-118, http://dx.doi.org/10.1145/1455770.1455786

[6] S. DELAUNE, S. KREMER, M. D. RYAN. *Verifying Privacy-type Properties of Electronic Voting Protocols*, in "Journal of Computer Security", July 2009, vol. 17, n° 4, pp. 435-487, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-jcs08.pdf

[7] S. DELAUNE, S. KREMER, G. STEEL. *Formal Analysis of PKCS#11 and Proprietary Extensions*, in "Journal of Computer Security", 2009, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKS-jcs09.pdf

[8] J. GOUBAULT-LARRECQ. *On Noetherian Spaces*, in "Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science (LICS'07)", Wrocław, Poland, IEEE Computer Society Press, July 2007, pp. 453-462 [*DOI :* 10.1109/LICS.2007.34], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-lics07.pdf

[9] J. GOUBAULT-LARRECQ, F. PARRENNES. *Cryptographic Protocol Analysis on Real C Code*, in "Proceedings of the 6th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05)", Paris, France, R. COUSOT (editor), Lecture Notes in Computer Science, Springer, January 2005, vol. 3385, pp. 363-379 [*DOI :* 10.1007/B105073], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GouPar-VMCAI2005.pdf

[10] J. OLIVAIN, J. GOUBAULT-LARRECQ. *The Orchids Intrusion Detection Tool*, in "Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05)", Edinburgh, Scotland, UK, K. ETESSAMI, S. RAJAMANI (editors), Lecture Notes in Computer Science, Springer, July 2005, vol. 3576, pp. 286-290 [*DOI :* 10.1007/11513988_28], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/OG-cav05.pdf

Publications of the year

Articles in International Peer-Reviewed Journals

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

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

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

International Conferences with Proceedings

[14] R. CHRÉTIEN, V. CORTIER, S. DELAUNE. *From security protocols to pushdown automata*, in "ICALP'2013 - 40th International Colloquium on Automata, Languages and Programming - 2013", Riga, Lithuania, F. V.

FOMIN, R. FREIVALDS, M. KWIATKOWSKA, D. PELEG (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7966, pp. 137-149 [*DOI :* 10.1007/978-3-642-39212-2_15], http://hal.inria.fr/hal-00881066

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

Research Reports

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