IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Cachan

Activity Report 2012

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.

Creation of the Project-Team: November 15, 2002 *, Updated into Team:* January 01, 2013 .

1. Members

Research Scientists
Stéphanie Delaune [Junior Researcher, HdR]
Graham Steel [Junior Researcher, Until Spring 2012, now at EPI Prosecco, Paris, HdR]

Faculty Members
David Baelde [Maître de Conférences, ENS Cachan, since Sep. 2012]
Hubert Comon-Lundh [Professor, ENS Cachan, HdR]
Jean Goubault-Larrecq [Team Leader, Professor, ENS Cachan, HdR]

Engineers
Romain Bardou [ITI engineer, Sep. 2011-June 2012, now at EPI Prosecco, Paris]
Nasr-Eddine Yousfi [ITI engineer, Dec. 2011-Nov. 2012]

PhD Students
Hedi Benzina [Digiteo grant, Nov. 2009-Dec. 2012]
Vincent Cheval [ENS Cachan student, Oct. 2009-Dec. 2012]
Rémy Chrétien [ANR JCJC VIP grant, Started Oct. 2012]
Guillaume Scerri [ERC grant ProSecure (holder: Véronique Cortier, CASSIS), Started Oct. 2011]
Robert Künnemann [Inria grant, Until Nov. 2012, now at EPI Prosecco, Paris]

Administrative Assistants
Valérie Hoareau [Nov. 2011-Jan. 2012]
Céline Halter [Feb. 2012-May 2012]
Claire Le Thomas [May 2012-Aug. 2012]
Maeva Jeannot [Sep. 2012-Nov. 2012]
Thida Iem [Since Dec. 2012]

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 the security of information systems. Originally, SECSI was organized around three main themes, and their mutual relationships:

- Automated verification of cryptographic protocols;
- Intrusion detection;
- Static analysis of programs, in order to detect security holes and vulnerabilities at the protocol level.

This has changed. Starting from 2006, SECSI concentrates on the first theme, while keeping an eye on the other two.

In a nutshell, the aim of the SECSI project is to *develop logic-based verification techniques for security properties of computer systems and networks*.

The thrust is towards more *automation* (new automata-based, or theorem-proving based verification techniques), more *properties* (not just secrecy or authentication, but e.g., coercion-resistance in electronic voting schemes), more *realism* (e.g., cryptographic soundness theorems for formal models).

The new objectives of the SECSI project are:

1. Tree-automata based methods, automated deduction, and approximate/exact cryptographic protocol verification in the Dolev-Yao model.
2. Enriching the Dolev-Yao model with algebraic theories, and associated decision problems.
3. Computational soundness of formal models (Dolev-Yao, applied pi-calculus), proofs of security in computational models.
4. Indistinguishability proofs allowing us to handle more properties, e.g. anonymity.
5. Application to new security protocols, e.g. electronic voting protocols.
6. Security in the presence of probabilistic and demonic non-deterministic choices.

The SECSI project officially terminates at the end of 2012.

The reason that the members of the project-team were given is that no permanent Inria researcher remains.

This will of course create a gap in the panel of research themes covered at Inria Saclay, and especially in computer security. Independently of Inria, the members of SECSI will remain active in the field of computer security. They will also define their new scientific project for the years to come. In time, this will be presented as an Inria project-team proposal.

2.2. Highlights of the Year

- Workshop celebrating the 15th anniversary of LSV (the lab where SECSI is hosted) and Jean Goubault-Larrecq's CNRS silver medal, ENS Cachan, February 06-07, 2012 (http://www.lsv.ens-cachan.fr/Events/LSV15Y/)
- The ANR project AVOTÉ on the formal analysis of electronic voting protocols (http://www.lsv.ens-cachan.fr/Projects/anr-avote/) has been nominated to receive a price awarded by the ANR.

3. Scientific Foundations

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.
- The Tookan tool allows one to assess the security of security tokens. These tokens are meant as safes holding secret keys, which should never be permitted to get out unencrypted. Several vulnerabilities discovered. Several interesting customers in banking (Barclays), in aeronautics (Boeing), notably.
- 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

5.1. Tookan

Participants: Graham Steel [correspondant], Romain Bardou.

See also the web page http://tookan.gforge.inria.fr/.

Tookan is a security analysis tool for cryptographic devices such as smartcards, security tokens and Hardware Security Modules that support the most widely-used industry standard interface, RSA PKCS#11. Each device implements PKCS#11 in a slightly different way since the standard is quite open, but finding a subset of the standard that results in a secure device, i.e. one where cryptographic keys cannot be revealed in clear, is actually rather tricky. Tookan analyses a device by first reverse engineering the exact implementation of PKCS#11 in use, then building a logical model of this implementation for a model checker, calling a model checker to search for attacks, and in the case where an attack is found, executing it directly on the device. Tookan has been used to find at least a dozen previously unknown flaws in commercially available devices.

The first results using Tookan were published in 2010 [48] and a six-month licence was granted to Boeing to use the tool. In 2011, a contract was signed with a major UK bank. Tookan is now the subject of a CSATT transfer action resulting in the hiring of an engineer, Romain Bardou, who started on September 1st, 2011. During 2012 Bardou and Steel implemented a new version of Tookan that is intended to form the technological basis for a spin-off company to be created in 2013. As a result of the transfer of Graham Steel and Romain Bardou to team Prosecco, this project is being continued in that team.

5.2. Orchids

Participants: Jean Goubault-Larrecq [correspondant], Hedi Benzina, Nasr-Eddine Yousfi.

The ORCHIDS real-time intrusion detection system was created in 2003-04 at SECSI. After a few years where research and development around ORCHIDS was relatively quiet, several new things happened, starting from the end of 2010.

First, several companies and institutions expressed interest in ORCHIDS, among which, notably, EADS Cassidian, Thalès, Galois Inc. (USA), the French Direction Générale de l'Armement (DGA).

Second, Baptiste Gourdin was hired as a development engineer (Dec. 2010-Nov. 2011) on an Action de Développement Technologique (ADT). He improved Orchids in several ways.

Nasr-Eddine Yousfi followed up on Baptiste Gourdin, starting from December 2011, on an ITI engineer position allotted by Inria's CSATT. He mostly explored ways of writing security meta-policies for confidentiality of sensitive dat.

Orchids will be the core of a contract between Inria and DGA, to be signed in December 2012, for three years.

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 [31] propose an extension of the symbolic model, and prove it computationally sound, without this restriction on the dishonest keys.

6.2. Unconditional Soundness (Objective 2)

Participant: Hubert Comon-Lundh.

Hubert Comon-Lundh, Véronique Cortier and Guillaume Scerri [31] show how one can 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 [25], 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.

The counterpart of this nice approach is the difficulty of the automation: a tool is required for checking the consistency of a set of axioms, together with the conditions accumulated along a trace. This problem is the subject of research for the next year(s).

6.3. QRB-Domains (Objective 4)

Participant: Jean Goubault-Larrecq [correspondant].

One of the outstanding problems that remains in the denotational semantics of higher-order programming languages with probabilistic choice is the existence of a suitable, convenient category of domains for defining the denotations of types. Technically, a category of so-called continuous domains is sought after, which would be Cartesian-closed and stable by the action of the probabilistic powerdomain functor. This is not known to exist, and is part of the Jung-Tix conjecture. Jean Goubault-Larrecq found out that relaxing continuity to quasi-continuity helped gaining stability by the action of the probabilistic powerdomain functor [20]. This is an extended version of previous work published at the LICS'10 conference.

6.4. Complete WSTS

Participant: Jean Goubault-Larrecq [correspondant].

Well-structured transition systems form a large class of infinite-state transition systems on which one can decide coverability (a slightly relaxed form of reachability). These include Petri nets, lossy channel systems, and various process algebras.

With Alain Finkel, Jean Goubault-Larrecq developed a theory of *complete* well-structured transition systems, allowing one to generalize Karp and Miller's coverability tree construction for Petri nets to all well-structured transition systems. This work culminated in [19], following two conference papers (STACS'09, ICALP'09). The general theory was the topic of the invited talk [34].

6.5. 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 [16], based on P-boxes and Dempster-Shafer structures to handle imprecise probabilities. This is based on work first presented at the SCAN'11 conference.

6.6. New Attacks on RSA PKCS#1v1.5 (Objective 2)

Participants: Graham Steel [correspondant], Romain Bardou.

RSA PKCS#1v1.5 is the most commonly used standard for public key encryption, used for example in TLS/SSL. It has been known to be vulnerable to a so-called padding-oracle attack since 1998 when Bleichenbacher described the vulnerability at CRYPTO. The attack, known was the "million message attack" was not thought to present a practical threat, due in part to the large number of oracle messages required. In a paper published at CRYPTO 2012 [26] we gave original modifications showing how the attack can be completed in a median of just 15 000 messages. The results led to widespread interest, indicated by over 1400 downloads of the long version of the paper from the HAL webpage and articles in the New York Times, Boston Globe and Süddeutscher Zeitung.

6.7. Deciding trace equivalence (Objectives 1, 3)

Participants: Vincent Cheval, Hubert Comon-Lundh, Stéphanie Delaune, Rémy Chrétien.

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 [44], as in similar languages based on equational logics, indistinguishability 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 does not take into account the dynamic behavior of a process, whereas trace equivalence is more general and takes into account this aspect.

6.7.1. Static equivalence.

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

Stéphanie Delaune, in collaboration with Mathieur Baudet and Véronique Cortier, has designed a generic procedure for deducibility and static equivalence that takes as input any convergent rewrite system [15]. They have shown that their algorithm covers most of the existing decision procedures for convergent theories. They also provide an efficient implementation, and compare it briefly with the tools ProVerif and KiSs. This paper is a journal version of the work presented in [47].

In [17], Ştefan Ciobâcă, Stéphanie Delaune and Steve Kremer propose a representation of deducible terms to overcome the limitation of the procedure mentionned above. This new procedure terminates on a wide range of equational theories. In particular, they obtain a new decidability result for the theory of trapdoor bit commitment encountered when studying electronic voting protocols. The algorithm has been implemented in the KiSs tool. This paper is a journal version of the work presented in [49].

In [18], Stéphanie Delaune, in collaboration with Véronique Cortier (LORIA, France), shows that existing decidability results can be easily combined for any disjoint equational theories: if the deducibility and indistinguishability relations are decidable for two disjoint theories, they are also decidable for their union. They also propose a general setting for solving deducibility and indistinguishability for an important class (called *monoidal*) of equational theories involving AC operators. This paper is a journal version of the works presented in [45], [50].

6.7.2. Trace equivalence.

When processes under study do not contain replication, trace equivalence can be reduced to the problem of deciding symbolic equivalence, an equivalence relation introduced by M. Baudet [46].

Stéphanie Delaune, Steve Kremer, and Daniel Pasaila study this symbolic equivalence problem when cryptographic primitives are modeled using a group equational theory, a special case of monoidal equational theories. The results strongly rely on the correspondance between group theories and rings. This allows them to reduce the problem under study to the problem of solving systems of equations over rings. This result was published at IJCAR'12 [33],

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 (see [42])

To deal with replication, another approach was 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 currently under submission [40].

6.8. Mobile ad-hoc networks (Objectives 1, 3)

Participants: Rémy Chrétien, Stéphanie Delaune, Graham Steel.

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.

However, existing results and tools do not apply to routing protocols. This is due in particular to the fact that all possible topologies (infinitely many) have to be considered. Véronique Cortier, Jan Degrieck, and Stéphanie Delaune propose a simple reduction result: when looking for attacks on properties such as the validity of the route, it is sufficient to consider topologies with only four nodes, resulting in a number of just five distinct topologies to consider. As an application, several routing protocols, such as the SRP applied to DSR and the SDMSR protocols, have been analysed using the ProVerif tool. This work was published at POST'12 [32].

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 is currently under submission [43].

In the context of vehicular ad-hoc networks, to improve road safety, a vehicle-to-vehicle communication platform is currently being developed by consortia of car manufacturers and legislators. In [51], Morten Dahl, Stéphanie Delaune and Graham Steel propose a framework for formal analysis of privacy in location based services such as anonymous electronic toll collection. They give a formal definition of privacy, and apply it to the VPriv scheme for vehicular services. They analyse the resulting model using the ProVerif tool, concluding that the privacy property holds only if certain conditions are met by the implementation. Their analysis includes some novel features such as the formal modelling of privacy for a protocol that relies on interactive zero-knowledge proofs of knowledge and list permutations.

6.9. Composition results (Objective 1)

Participants: Vincent Cheval, 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. Nowdays, several composition results exist for trace-based properties, but there is a lack of composition results for equivalence-based properties.

Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune study the notion of trace equivalence and we show how to establish such an equivalence relation in a modular way. They show that composition works even when the processes share secrets provided that they satisfy some reasonable conditions. Their composition result allows one to prove various equivalence-based properties in a modular way, and works in a quite general setting. In particular, they consider arbitrary cryptographic primitives and processes that use non-trivial else branches. As an example, they consider the ICAO e-passport standard, and they show how the privacy guarantees of the whole application can be derived from the privacy guarantees of its sub-protocols. This work was published at CSF'12 [22].

7. Partnerships and Cooperations

7.1. Regional Initiatives

- DIM Digiteo project RedPill: Malware Detection on Virtualized Architectures, Oct. 2009-Sept. 2012. Sole partner: LSV. Funds Hedi Benzina's PhD Thesis.
- DIM Digiteo project API: Automated Proofs of Indistinguishability, 2010-2013. Partners: EPI SECSI, EPI CASCADE. Oct. 2010-Sept. 2013. Funds Vincent Cheval's PhD Thesis.

7.2. National Initiatives

7.2.1. ANR

- ANR programme blanc CPP ("Confidence, Probability, and Proofs"), 2009-2012. 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 SeSur (“Sécurité et Sûreté Informatique”) project AVOTÉ, 2008-2012. Partners: Inria (Cassis, leader), LSV, Verimag and, until September 2009 France Télécom R&D.

  Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud and their security has seriously been questioned. The AVOTÉ project aims at proposing formal methods to analyze electronic voting protocols. See http://www.lsv.ens-cachan.fr/anr-avote/.

- 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/.

7.3. International Initiatives

7.3.1. Participation In 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 tageted applications are Online Social Networks, Location Based Services, and Electronic Health Record Systems.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- Myrto Arapinis, April 2012 (1 week) and in December 2012 (1 week).
- Alwen Tiu, December 2012 (1 week).

7.4.1.1. Internships

Umang MATHUR (from May 2012 until Jul 2012)

Subject: Estimating the information leakage of a recursive probabilistic program
Institution: IIT Bombay (India)

8. Dissemination

8.1. Scientific Animation

Administrative charges:

- Hubert Comon-Lundh is director of the Parisian Master of Research in Computer Science (MPRI).
- 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".
- Stéphanie Delaune is a member of the scientific committee of Inria Saclay since February 2012.
- Stéphanie Delaune is "Déléguée aux thèses" at the École Doctorale Sciences Pratiques at ENS Cachan since September 2012.
- Jean Goubault-Larrecq, 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.
- Hubert Comon-Lundh is guest editor of the Journal of Automated Reasoning (special issue, security and rewriting, Feb 2012).

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).
- 27th Annual ACM/IEEE Symposium Logic in Computer Science, Dubrovnik, Croatia, 2012 (Hubert Comon-Lundh)
- 8th International Conference on Information Security Practice and Experience ISPEC'12, Hangzhou, China (Stéphanie Delaune).
- 24th *Journées Francophones des Langages Applicatifs* JFLA'13, Aussois, France, February 2013 (David Baelde).

Selection committees:

- Hubert Comon-Lundh was president of selection committee, MCF, ENS Cachan 2012.
- Hubert Comon-Lundh was president of the selection committee for the mixed chair CNRS-Aix Marseille University, 2012.

Evaluation committees:

- Hubert Comon-Lundh, member of the jury of "Prime d'Excellence Scientifique" (National committee, professors and maîtres de conférences), 2012.
- Jean Goubault-Larrecq, AERES evaluation, LIAFA, Université Paris Diderot, December 27-28, 2012
- Jean Goubault-Larrecq, CNRS PEPS program evaluation committee, March 22, 2012

Scientific boards:

- Hubert Comon-Lundh, CNRS INSII, Oct. 2010-Oct 2014
- Jean Goubault-Larrecq, external member of the selection committee of the Formal Methods and Security Inria-DGA seminar, Rennes

Invited talks:

- Hubert Comon-Lundh *Towards unconditional soundness*. Grenoble, Jan 13, 2012, Workshop on Computer-Aided Security.
- Jean Goubault-Larrecq, *Probability and Nondeterminism in Domain Theory, Part II*, Logic and Interactions, week 4: Quantitative approaches, Marseilles, France, February 20-24.

Invitation to seminars:

- Stéphanie Delaune, Dagstuhl seminar on Analysis of security APIs, Wadern, Germany, November 25-28.
- Stéphanie Delaune, *Analysing privacy-type properties using formal methods*, CAPPRIS meeting, Paris, March 14
- Jean Goubault-Larrecq, *An Isomorphism between Powercone and Prevision Models*, McGill seminar, Bellairs Institute, Holetown, Barbados, April 01-06.

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 Computability*, 45h., 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, 4h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Stéphanie Delaune, *Cryptography, Cryptographic Protocols and Quantum Cryptography*, Part 2/3, 4h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Jean Goubault-Larrecq, *Advanced Complexity*, 42h., M1, MPRI course 1-17, 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 *Computational Soundness*, 12h., M2, MPRI course 2-30, France, Jan-Feb 2012
- Hubert Comon-Lundh *Formal proofs of security*, 24h, M2, MPRI course 2-30, France Oct-Dec 2012 (48h)
- 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
- Jean Goubault-Larrecq, rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 18h., ENS Cachan, France

8.2.2. Supervision

PhD :

- Vincent Cheval, *Automatic verification of cryptographic protocols: privacy-type properties*, ENS Cachan, Dec. 03, 2012 [12], supervised by Stéphanie Delaune and Hubert Comon-Lundh
- Hedi Benzina, *Enforcing virtualized systems security*, ENS Cachan, Dec. 17, 2012 [11], supervised by Jean Goubault-Larrecq

PhD in progress :

- Rémy Chrétien, *Trace equivalence for an unbounded number of sessions*, Started Oct. 2012, supervised by Stéphanie Delaune
- Robert Künnemann, *Secure APIs and Simulation-Based Security*, Started Oct. 2010, supervised by Steve Kremer and Graham Steel; Graham and Robert are now at EPI Prosecco
- Gavin Keighren, *A Type System for Security APIs*, since 2007 (to submit March 2013), advisors Graham Steel and David Aspinall (University of Edinburgh). Graham is now at EPI Prosecco.
- Guillaume Scerri, *Preuves abstraites de protocoles cryptographiques concrets*, Started Oct. 2011, supervised by Hubert Comon-Lundh

Masters:

- Rémy Chrétien, *Trace equivalence of protocols for an unbounded number of sessions*, 2012, advisors Stéphanie Delaune and Véronique Cortier
- Apoorvaa Deshpande, *Automated verification of equivalence properties modulo AC*, 2012, advisors Stéphanie Delaune and Steve Kremer

8.2.3. Juries

- PhD:
  - Hubert Comon-Lundh, president of the jury: Jeremy Planul, *Typage, compilation, et cryptographie pour la programmation répartie securisée*, Ecole Polytechnique, Feb 08, 2012.
  - Hubert Comon-Lundh, member of the jury: Vincent Cheval, *Preuves automatiques d'indistinguabilité*, ENS Cachan, Dec 03, 2012.
  - Jean Goubault-Larrecq, member of the jury: Gabriel Kerneis, *Continuation-Passing C: Program Transformations for Compiling Concurrency in an Imperative Language*, Université Paris Diderot, November 09, 2012.
  - Jean Goubault-Larrecq, member of the jury: Hedi Benzina, *Enforcing virtualized systems security*, ENS Cachan, December 17, 2012
- HdR:
  - Hubert Comon-Lundh, reviewer of the habilitation and member of the jury: Karthikeyan Bhargavan, *Towards the Automated Verification of Cryptographic Protocol Implementations*, Ecole Normale Supérieure, May 04, 2012.
  - Hubert Comon-Lundh, reviewer of the habilitation and member of the jury: Pascal Lafourcade *Cryptographic Primitives, Voting protocols, and Wireless Sensor Networks*, Université Joseph Fourier, Grenoble, Nov. 06, 2012.
  - Hubert Comon-Lundh, president of the jury: Jérôme Leroux, *Machines à compteur et arithmétique de Presburger*, Université Bordeaux I, Bordeaux, Dec 06, 2012.
  - Jean Goubault-Larrecq, member of the jury: Laurent Doyen, *Games and Automata: From Boolean to Quantitative Verification*, ENS Cachan, March 13, 2012

8.3. Popularization

- Hubert Comon-Lundh , *Le vote électronique*, Institut des Hautes études en Sciences et Technologies (IHEST), Jan 20, 2012
- Stéphanie Delaune, member of the scientific mediation committee at Inria Saclay. (“Mediation” is the new name for popularization.)
- Jean Goubault-Larrecq, *Sécurité informatique*, talk and discussion with the public at the “débat citoyen” organized by Inria, Alan Turing building, Inria Saclay, November 19, 2012
- Jean Goubault-Larrecq, breakfast with the press, organized by CNRS, on computer security, November 29, 2012
- Stéphanie Delaune gave two popularization talks, *Ces protocoles qui nous protègent*, at *Journée Régionale de l’APMEP - Haute-Normandie*, Rouen, April 18, and at *Journée de rentrée de l’ENS Cachan*, Cachan, September 7.
- Stéphanie Delaune was interviewed by a journalist in charge of a special issue on cryptography for the magazine “Cahiers Sciences et Vie”.
- Rémy Chrétien, *Le vote électronique*, article for the ANAJ-IHEDN Cybersecurity newsletter, to be published.

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, p. 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, p. 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^{o} 1, p. 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, p. 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^{o} 4, p. 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, p. 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, p. 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, p. 286-290 [*DOI :* 10.1007/11513988_28], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/OG-cav05.pdf.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] H. BENZINA. *Enforcing virtualized systems security*, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012.

[12] V. CHEVAL. *Automatic verification of cryptographic protocols: privacy-type properties*, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012.

Articles in International Peer-Reviewed Journals

[13] A. ADJÉ, S. GAUBERT, É. GOUBAULT. *Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis*, in "Logical Methods in Computer Science", January 2012, vol. 8, n^{o} 1:1 [*DOI :* 10.2168/LMCS-8(1:01)2012], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/AGG-lmcs12.pdf.

[14] D. BAELDE. *Least and greatest fixed points in linear logic*, in "ACM Transactions on Computational Logic", January 2012, vol. 13, n^{o} 1 [*DOI :* 10.1145/2071368.2071370], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/baelde12tocl.pdf.

[15] M. BAUDET, V. CORTIER, S. DELAUNE. *YAPA: A generic tool for computing intruder knowledge*, in "ACM Transactions on Computational Logic", 2012, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-tocl12.pdf.

[16] O. BOUISSOU, É. GOUBAULT, J. GOUBAULT-LARRECQ, S. PUTOT. *A Generalization of P-boxes to Affine Arithmetic, and Applications to Static Analysis of Programs*, in "Computing", March 2012, vol. 94, n^{o} 2-4, p. 189-201 [*DOI :* 10.1007/s00607-011-0182-8], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BGGLP-comp11.pdf.

[17] Ş. CIOBÂCĂ, S. DELAUNE, S. KREMER. *Computing knowledge in security protocols under convergent equational theories*, in "Journal of Automated Reasoning", February 2012, vol. 48, n° 2, p. 219-262 [*DOI :* 10.1007/s10817-010-9197-7], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDK-jar10.pdf.

[18] V. CORTIER, S. DELAUNE. *Decidability and combination results for two notions of knowledge in security protocols*, in "Journal of Automated Reasoning", April 2012, vol. 48, n° 4, p. 441-487 [*DOI :* 10.1007/s10817-010-9208-8], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-jar10.pdf.

[19] A. FINKEL, J. GOUBAULT-LARRECQ. *Forward Analysis for WSTS, Part II: Complete WSTS*, in "Logical Methods in Computer Science", September 2012, vol. 8, n° 3:28 [*DOI :* 10.2168/LMCS-8(3:28)2012], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/FG-lmcs12.pdf.

[20] J. GOUBAULT-LARRECQ. *QRB-Domains and the Probabilistic Powerdomain*, in "Logical Methods in Computer Science", 2012, vol. 8, n° 1:14 [*DOI :* 10.2168/LMCS-8(1:14)2012], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/JGL-lmcs12.pdf.

[21] S. KREMER, A. MERCIER, R. TREINEN. *Reducing Equational Theories for the Decision of Static Equivalence*, in "Journal of Automated Reasoning", February 2012, vol. 2, n° 48, p. 197-217 [*DOI :* 10.1007/s10817-010-9203-0], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KMT-jar10.pdf.

International Conferences with Proceedings

[22] M. ARAPINIS, V. CHEVAL, S. DELAUNE. *Verifying privacy-type properties in a modular way*, in "Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF'12)", Cambridge Massachusetts, USA, IEEE Computer Society Press, June 2012, p. 95-109 [*DOI :* 10.1109/CSF.2012.16], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-csf12.pdf.

[23] D. BAELDE, P. COURTIEU, D. GROSS-AMBLARD, CH. PAULIN-MOHRING. *Towards Provably Robust Watermarking*, in "Third International Conference on Interactive Theorem Proving (ITP'12)", Princeton, NJ, USA, L. BERINGER, A. P. FELTY (editors), Lecture Notes in Computer Science, Springer, August 2012, vol. 7406, p. 201-216 [*DOI :* 10.1007/978-3-642-32347-8_14], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/baelde12itp.pdf.

[24] D. BAELDE, G. NADATHUR. *Combining Deduction Modulo and Logics of Fixed-Point Definitions*, in "Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science (LICS'12)", Dubrovnik, Croatia, IEEE Computer Society Press, June 2012, p. 105-114 [*DOI :* 10.1109/LICS.2012.22], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/baelde12lics.pdf.

[25] 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)", Tallinn, Estonia, P. DEGANO, J. D. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, March 2012, vol. 7215, p. 189-208 [*DOI :* 10.1007/978-3-642-28641-4_11], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BC-post12.pdf.

[26] R. BARDOU, R. FOCARDI, Y. KAWAMOTO, L. SIMIONATO, G. STEEL, J.-K. TSAY. *Efficient Padding Oracle Attacks on Cryptographic Hardware*, in "Proceedings of the 32nd Annual International Cryptology Conference (CRYPTO'12)", Santa Barbara, CA, USA, R. SAFAVI-NAINI, R. CANETTI (editors), Lecture Notes in Computer Science, Springer, August 2012, vol. 7417, p. 608-625 [*DOI :* 10.1007/978-3-642-32009-5_36], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BFKSST-crypto12.pdf.

[27] H. BENZINA. *A Network Policy Model for Virtualized Systems*, in "Proceedings of the 17th IEEE Symposium on Computers and Communications (ISCC'12)", Nevşehir, Turkey, IEEE Computer Society Press, July 2012, p. 680-683 [*DOI :* 10.1109/ISCC.2012.6249376], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/benzina-iscc12.pdf.

[28] H. BENZINA. *Towards Designing Secure Virtualized Systems*, in "Proceedings of the 2nd International Conference on Digital Information and Communication Technology and its Application (DICTAP'12)", Bangkok, Thailand, IEEE Computer Society Press, May 2012, p. 250-255 [*DOI :* 10.1109/DICTAP.2012.6215385], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/HB-dictap12.pdf.

[29] R. CHADHA, Ş. CIOBÂCĂ, S. KREMER. *Automated verification of equivalence properties of cryptographic protocols*, in "Programming Languages and Systems - Proceedings of the 22nd European Symposium on Programming (ESOP'12)", Tallinn, Estonia, H. SEIDL (editor), Lecture Notes in Computer Science, Springer, March 2012, vol. 7211, p. 108-127 [*DOI :* 10.1007/978-3-642-28869-2_6], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCK-esop12.pdf.

[30] R. CHADHA, P. MADHUSUDAN, M. VISWANATHAN. *Reachability under Contextual Locking*, in "Proceedings of the 18th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'12)", Tallinn, Estonia, C. FLANAGAN, B. KÖNIG (editors), Lecture Notes in Computer Science, Springer, March 2012, vol. 7214, p. 437-450 [*DOI :* 10.1007/978-3-642-28756-5_30], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CMV-tacas12.pdf.

[31] H. COMON-LUNDH, V. CORTIER, G. SCERRI. *Security proof with dishonest keys*, in "Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)", Tallinn, Estonia, P. DEGANO, J. D. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, March 2012, vol. 7215, p. 149-168 [*DOI :* 10.1007/978-3-642-28641-4_9], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CCS-post12.pdf.

[32] V. CORTIER, J. DEGRIECK, S. DELAUNE. *Analysing routing protocols: four nodes topologies are sufficient*, in "Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)", Tallinn, Estonia, P. DEGANO, J. D. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, March 2012, vol. 7215, p. 30-50 [*DOI :* 10.1007/978-3-642-28641-4_3], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CDD-post12.pdf.

[33] S. DELAUNE, S. KREMER, D. PASAILĂ. *Security protocols, constraint systems, and group theories*, in "Proceedings of the 6th International Joint Conference on Automated Reasoning (IJCAR'12)", Manchester, UK, B. GRAMLICH, D. MILLER, U. SATTLER (editors), Lecture Notes in Artificial Intelligence, Springer-Verlag, June 2012, vol. 7364, p. 164-178 [*DOI :* 10.1007/978-3-642-31365-3_15], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKP-ijcar12.pdf.

[34] A. FINKEL, J. GOUBAULT-LARRECQ. *The Theory of WSTS: The Case of Complete WSTS*, in "Proceedings of the 33rd International Conference on Applications and Theory of Petri Nets (ICATPN'12)", Hamburg, Germany, S. HADDAD, L. POMELLO (editors), Lecture Notes in Computer Science, Springer, June 2012, vol. 7347, p. 3-31 [*DOI :* 10.1007/978-3-642-31131-4_2], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/FGL-atpn12.pdf.

[35] M. IZABACHÈNE, B. LIBERT. *Divisible E-Cash in the Standard Model*, in "Proceedings of the 5th International Conference on Pairing-Based Cryptography (PAIRING'12)", Cologne, Germany, M. ABDALLA, T. LANGE (editors), Lecture Notes in Computer Science, Springer, May 2012, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/IL-pairing12.pdf.

[36] R. KÜNNEMANN, G. STEEL. *YubiSecure? Formal Security Analysis Results for the Yubikey and YubiHSM*, in "Preliminary Proceedings of the 8th Workshop on Security and Trust Management (STM'12)", Pisa, Italy, A. JØSANG, P. SAMARATI (editors), September 2012, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/KS-stm12.pdf.

Scientific Books (or Scientific Book chapters)

[37] J. GOUBAULT-LARRECQ. *Non-Hausdorff Topology and Domain Theory—Selected Topics in Point-Set Topology*, Cambridge University Press, 2012, To appear.

Research Reports

[38] A. ADJÉ, J. GOUBAULT-LARRECQ. *Concrete Semantics of Programs with Non-Deterministic and Random Inputs*, Computing Research Repository, October 2012, n^{o} cs.LO/1210.2605, 19 pages, http://arxiv.org/abs/1210.2605.

[39] R. CHADHA, M. UMMELS. *The complexity of quantitative information flow in recursive programs*, Laboratoire Spécification et Vérification, ENS Cachan, France, July 2012, n^{o} LSV-12-15, 24 pages, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2012-15.pdf.

[40] V. CHEVAL, B. BLANCHET. *Proving More Observational Equivalences with ProVerif*, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2012, n^{o} LSV-12-19, 34 pages, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2012-19.pdf.

[41] V. CHEVAL, V. CORTIER, S. DELAUNE. *Deciding equivalence-based properties using constraint solving*, Laboratoire Spécification et Vérification, ENS Cachan, France, August 2012, n^{o} LSV-12-17, 53 pages, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2012-17.pdf.

[42] R. CHRÉTIEN. *Trace equivalence of protocols for an unbounded number of sessions*, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012, n^{o} LSV-12-22, 30 pages, http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2012-22.pdf.

[43] R. CHRÉTIEN, S. DELAUNE. *Formal analysis of privacy for routing protocols in mobile ad hoc networks*, Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012, n^{o} LSV-12-21, 25 pages, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/rr-lsv-2012-21.pdf.

References in notes

[44] M. ABADI, C. FOURNET. *Mobile Values, New Names, and Secure Communication*, in "Proc. 28th ACM Symposium on Principles of Programming Languages (POPL'01)", ACM Press, 2001, p. 104–15.

[45] M. ARNAUD, V. CORTIER, S. DELAUNE. *Combining algorithms for deciding knowledge in security protocols*, in "Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)", Liverpool, UK, F. WOLTER (editor), Lecture Notes in Artificial Intelligence, Springer, September 2007, vol. 4720, p. 103-117 [*DOI :* 10.1007/978-3-540-74621-8_7], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/ACD-frocos07.pdf.

[46] M. BAUDET. *Deciding Security of Protocols against Off-line Guessing Attacks*, in "Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)", Alexandria, Virginia, USA, ACM

Press, November 2005, p. 16-25 [*DOI :* 10.1145/1102125], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Baudet_CCS05revised.pdf.

[47] M. BAUDET, V. CORTIER, S. DELAUNE. *YAPA: A generic tool for computing intruder knowledge*, in "Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09)", Brasília, Brazil, R. TREINEN (editor), Lecture Notes in Computer Science, Springer, June-July 2009, vol. 5595, p. 148-163, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCD-rta09.pdf.

[48] 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, p. 260-269 [*DOI :* 10.1145/1866307.1866337], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCFS-ccs10.pdf.

[49] Ş. CIOBÂCĂ, S. DELAUNE, S. KREMER. *Computing knowledge in security protocols under convergent equational theories*, in "Proceedings of the 22nd International Conference on Automated Deduction (CADE'09)", Montreal, Canada, R. SCHMIDT (editor), Lecture Notes in Artificial Intelligence, Springer, August 2009, p. 355-370.

[50] V. CORTIER, S. DELAUNE. *Deciding Knowledge in Security Protocols for Monoidal Equational Theories*, in "Proceedings of the 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07)", Yerevan, Armenia, N. DERSHOWITZ, A. VORONKOV (editors), Lecture Notes in Artificial Intelligence, Springer, October 2007, vol. 4790, p. 196-210 [*DOI :* 10.1007/978-3-540-75560-9_16], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CD-lpar07.pdf.

[51] M. DAHL, S. DELAUNE, G. STEEL. *Formal Analysis of Privacy for Anonymous Location Based Services*, in "Proceedings of the Workshop on Theory of Security and Applications (TOSCA'11)", Saarbrücken, Germany, March-April 2011, To appear, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DDS-tosca11.pdf.