RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2014

Section Highlights of the Team

Edition: 2015-06-01

ARIC Project-Team (section vide)

CARAMEL Project-Team

6.1. Highlights of the Year

Razvan Barbulescu, ex-PhD student in the team, has received the award “Prix Le Monde de la recherche universitaire”, as one of the top-5 PhD thesis in exact science in 2014.

Emmanuel Thomé has received the “Prix Régional du Chercheur” of the Région Lorraine.

Emmanuel Thomé has received the “Prix de l’Association des Amis de l’Université de Lorraine”.
BEST PAPER AWARD :
[17] **Eurocrypt 2014**. R. BARBULESCU, P. GAUDRY, A. JOUX, E. THOMÉ.

CASCADE Project-Team (section vide)

CRYPT Team

4.1. Highlights of the Year

The team published [20] improved single-key attacks on reduced-round AES: AES is currently the most widespread block cipher standard, it is implemented in Intel processors.

The team also showed [18] how to speed-up a well-known public-key cryptanalysis technique: finding small roots of univariate polynomial congruences. This technique is used to break special cases of the RSA cryptosystem.

Phong Nguyen was Program co-Chair of the 33rd IACR Eurocrypt Conference (EUROCRYPT 2014) [22].

GALAAD2 Team (section vide)

GEOMETRICA Project-Team

6.1. Highlights of the Year

[10] was elected among the notable articles of 2013 by ACM and Computing Reviews (see http://computingreviews.com/recommend/bestof/notableitems_2013.cfm).

GRACE Project-Team

6.1. Highlights of the Year

- F. Morain and A. Guillevic (with their co-authors R. Barbulescu and P. Gaudry) broke the discrete logarithm world record for finite fields of the form $GF(p^2)$ with a prime p of 80 decimal digits. The new techniques form the preprint [31].
- D. Augot and M. Finiasz received the best paper award at FSE 2014 [17]. FSE is the most important conference devoted to symmetric cryptography. Grace contribution is to propose a mathematical construction which enables direct construction of so-called diffusion layers in block ciphers.
- A. Zeh, former Grace PhD student, received the special Prize of the Université Franco-Allemande (UFA) Jury 2014 at the French Ambassy in Berlin, on November 21st.

BEST PAPER AWARD :

[17] **21st International Workshop on Fast Software Encryption, FSE 2014**. D. AUGOT, M. FINIASZ.

LFANT Project-Team

5.1. Highlights of the Year

Aurel Page has defended his PhD thesis on *Méthodes explicites pour les groupes arithmétiques* [12] in July 2014. Nicolas Mascot has defended his PhD thesis on *Computing modular Galois representations* [11], in July 2014.

POLSYS Project-Team

6.1. Highlights of the Year

Jointly with Univ. Of Kaiserslautern (C. Eder), we have released a new open source C library for linear algebra dedicated to Gröbner bases computations (see http://www-polsys.lip6.fr/~jcf/Software/index.html). This new library opens the door to high performance applications

- The library is specialized in reducing matrices generated during Gröbner bases computations. Optimizing this reduction step is crucial for the overall computation.
- Our approach takes even more advantage of the very special structure (quasi unit-triangular sparse matrices with patterns in the data)
- We also reduce the number of operations, in a parallel friendly fashion, by changing the order of the operations in the elimination.
- We present experimental results for sequential and parallel computations on NUMA architectures. We also get good scaling up until 32 (non hyper-threaded) cores: we have speed-ups around 14 or 16.

SECRET Project-Team

6.1. Highlights of the Year

- Rafael Misoczki's PhD thesis on code-based cryptography (defended in November 2013) has been awarded by the Brazilian Society of Computer Science as the best thesis in computer security.
- *Security analysis of some primitives for authentication and authenticated encryption:* authentication is a major functionality in the vast majority of applications. It is usually implemented by a MAC (message authentication code). The main constructions for MAC are based on hash functions, and include the wide-spread HMAC construction. Gaëtan Leurent, together with Itai Dinur, has presented a new generic attack against HMAC when the underlying hash function follows the Haifa construction. This result points out that the hash function in HMAC has to be chosen very carefully and that some of the main families of hash functions may introduce unexpected weaknesses in the associated MAC. Also, the project-team is involved in a national cryptanalytic effort funded by the ANR which aims at evaluating the security of the recently proposed authenticated encryption schemes.
- *Parallel Repetition of Entangled Games:* In a two-player free game G, two cooperating but non communicating players receive inputs taken from two independent probability distributions. Each of them produces an output and they win the game if they satisfy some predicate on their inputs/outputs. The classical (resp. entangled) value of G is the maximum winning probability when the players are allowed to share classical random bits (resp. a quantum state) prior to receiving their inputs. The n-fold parallel repetition of G consists of n instances of G where the parties receive all the inputs at the same time, produce all the outputs at the same time and must win every instance of G. This work by André Chailloux in collaboration with Giannicola Scarpa establishes that the entangled value of the parallel repetition of G decreases exponentially with n, thereby generalizing to the quantum setting Raz's celebrated parallel repetition theorem which is concerned with the classical value of the game. The main tool for proving this result is the introduction of a new information-theoretic quantity: the superposed information cost.

SPECFUN Project-Team

6.1. Highlights of the Year

Two results are particularly important this year, our computer-checked proof [11] of irrationality of $\zeta(3)$ and our new algorithm [19] for the integration of multiple integrals. The former is our first success in the merger between computer algebra and formal methods, and stimulates further research in this direction around special functions and creative telescoping. The latter has made a large class of integrals possible in practice, thus allowing us to compute a challenging list of integrals related to famous Calabi–Yau various; it has also received attention by physicists.

VEGAS Project-Team (section vide)

ALF Project-Team

6.1. Highlights of the Year

André Seznec and Pierre Michaud won the 4th Championship Branch Prediction in all the 3 categories, 4KB, 32 KB and unlimited storage predictors [23], [33], thus confirming the past championships in 2011, 2006 and 2004.

ATEAMS Project-Team

5.1. Highlights of the Year

- Davy Landman, Jurgen Vinju received a Best paper award nomination, for their paper “Empirical analysis of the relationship between CC and SLOC in a large corpus of Java methods”(ICSM’14).

CAIRN Project-Team

6.1. Highlights of the Year

Our work on accuracy evaluation and optimisation for fixed point arithmetic was presented during a tutorial "Automatic Fixed-Point Conversion: a Gateway to High-Level Power Optimization" at IEEE/ACM Design Automation and Test in Europe [77].
As a proof of concept of our research on improving efficiency of dynamic reconfiguration in FPGAs [47] [48], the *eFPGA* (Figure 5) chip was designed and fabricated in 65nm CMOS technology. In the proposed and patented architecture [73] (EU patent), the configuration of the FPGA becomes independent from its placement and is moreover significantly compressed (up to $\times 10$). This notion of *Virtual Bit Stream* allows for seamless partial and dynamic reconfiguration and for task migration.

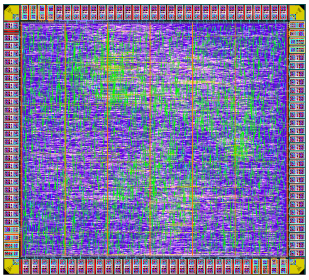

Figure 5. CAIRN*'s eFPGA chip*

CAMUS Team

6.1. Highlights of the Year

One of Philippe Clauss' early papers on Ehrhart polynomials has been celebrated, 18 years later, in a selection of papers for the International Conference on Supercomputing (ICS) 25th anniversary retrospective [13]. 35 papers have been selected among roughly 1800 papers published between 1987 and 2011. The paper is:

"Counting Solutions to Linear and Nonlinear Constraints Through Ehrhart Polynomials: Applications to Analyze and Transform Scientific Programs", by Philippe Clauss, ICS'96, which introduced Ehrhart polynomials in the field of program analysis and optimization.

Philippe Clauss wrote an additional retrospective [12] related to this research which complements the paper in the ICS special issue.

COMPSYS Project-Team

6.1. Highlights of the Year

For 2014, from the point of view of organization, funding, collaborations, the main points to highlight are:

- Christophe Alias and Alexandru Plesco have co-founded the XTREMLOGIC start-up in January 2014 (see Section 7.2), following the incubation of Zettice. XTREMLOGIC recently won the "concours région rhône-alpes" grant in November 2014 (40k).
- Tomofumi Yuki was hired as an Inria researcher and became a permanent member of Compsys.
- The 1988 "Array Expansion" seminal paper of Paul Feautrier has been selected for the 25th Anniversary Volume of the ACM International Conference on Supercomputing (ICS) together with 34 other papers selected from the 1800 papers published from 1987 to 2011. A short "reminescence" paper [13] was written for the occasion.
- The team was evaluated in Nov. 2014 by the HCERES (new name of AERES), as part of the LIP lab evaluation. The report has not been received yet.

From a scientific point of view, the shift, in Compsys III, towards the analysis of parallel programs and the extensions of the polyhedral model, both in terms of techniques and applications, is continuing, see the section "New Results", in particular:

- The design (by Christophe Alias and Alexandru Plesco) of a HLS compiler technology (see Section 6.2), patented by Inria [12] and transferred to XTREMLOGIC under an Inria licence (see Section 5.5).
- Two new static analyses: a more precise array bound check analysis [9] (see Section 6.3) and a more scalable termination algorithm for C programs (see Section 6.4).
- A novel equivalence-checking algorithm [7] modulo associativity/commutativity, which is a first step towards semantic program transformations (see Section 6.5).
- A groundbreaking introduction of polyhedral techniques for the analysis of parallel programs, in particular X10 (see [29] and [6]) and OpenStream (see Section 6.6).
- A seminal paper [5] introducing polynomial techniques in program analysis and compilation (see Section 6.7).
- Innovative contributions on parametric tiling [8], [3], [4] as extensions of the polyhedral model (see Sections 6.8 and 6.9).

DREAMPAL Team

5.1. Highlights of the Year

The papers [4] and [6] are published in journals (Software Testing Verification and Analisys, resp. Formal Aspects of Computing) that are among the best in their respective fields.

GCG Team

6.1. Highlights of the Year

Graduate Research Award of the OSU department in 2015 for Venmugil Elango (co-advised by Fabrice Rastello)

PAREO Project-Team (section vide)

POSTALE Team

5.1. Highlights of the Year

CovTrack: Agile multi-target multi-threaded realtime tracker We have developed and highly optimized a multi-target tracking system based on covariance tracking algorithm. The complexity of the algorithm – connected to the number of features – can be tuned to fit the processor computation power (with/without SIMD). Moreover the features can be also selected from a large set of features to adapt the algorithm to the scene and the nature of tracking (indoor/outdoor, pedestrian/car,). Some software and algorithmic transforms have been also applied to accelerate the code for scalar/SIMD processors. [20]

The Light Speed Labeling (LSL) algorithm is still the world fastest connected component labeling (CCL) algorithm. We have proposed a new benchmark that performs fair comparisons for such a data-dependent algorithm (that involves Union-Find algorithm optimization combined with memory and control flow optimization). We show that thanks to its run-based approach and its line-relative labeling, LSL is intrinsically more efficient that all State-of-the-Art pixel-based algorithms, whatever the memory management.[23]

TASC Project-Team

6.1. Highlights of the Year

In the context of the MiniZinc Challenge and in concurrency with 16 other solvers, CHOCO has won three bronze medals in three out of four categories: free search, parallel search and Open class.

AOSTE Project-Team (section vide)

CONVECS Project-Team (section vide)

HYCOMES Team

6.1. Highlights of the Year

The main advances in 2014 of the Hycomes team have been as follows:

Causality analysis of hybrid systems with ordinary differential equations (ODE) We have proposed a causality analysis, in the form of a simple type system, rejecting hybrid programs with algebraic circuits — see section 6.2 .

An index theory of DAE hybrid systems with differential algebraic equations (DAE) We have proposed a conservative extension of the notion of differentiation index to hybrid systems with differential algebraic equations — see section 6.3 .

MUTANT Project-Team

6.1. Highlights of the Year

Acoustical Society of America Best Paper Award for [20].

International Computer Music Conference (ICMC) Best Presentation Award for [19].

MuTant TEDx Talk in October 2014 on *Human-Computer Musicianship* that attracted more than 12 thousand podcasts according to organisers.

MuTant in CNRS's 2nd edition of "Les Fondamentales" Science and Society event in Grenoble, in a session dedicated to Science and Music on the same Score.

MuTant Participation in the 2014 edition of *Futur en Seine* festival and showcased collaboration with Orchestre de Paris in a public event.

BEST PAPER AWARD :

[19] **International Computer Music Conference**. C. TRAPANI, J. ECHEVESTE.

PARKAS Project-Team

6.1. Highlights of the Year

The paper *ReactiveML, a reactive extension to ML* of Mandel and Pouzet has been declared to be the *most influential paper of PPDP (Principles and Practice of Declaractive Programming) 2005*. A previous version of the paper, submitted to JFLA'05, has been declared to be "une contribution marquante parmi les articles publiés aux JFLA".

SPADES Team (section vide)

TEA Project-Team

6.1. Highlights of the Year

This year's effort has been mainly devoted to the successful creation of project-team TEA and the definition of its new research perspective on Time, Events and Architectures in CPS design.

The SAE committee on the AADL adopted our recommendations to implement a timed and synchronous behavioural annex [13], [11] for standardisation [20]. The specification and reference implementation of this revised behavioral annex will be the focus of most our attention next year.

Adnan Bouakaz published and implemented more of the original results from his PhD. work on abstract affine scheduling [14], [15].

ANTIQUE Team

6.1. Highlights of the Year

Patrick and Radhia Cousot have received in 2014 the IEEE Computer Society IEEE Computer Society Harlan D. Mills award for the invention of abstract interpretation, developpment of tool support and practical application http://www.computer.org/portal/web/awards/cousots.

CELTIQUE Project-Team (section vide)

DEDUCTEAM Exploratory Action

6.1. Highlights of the Year

In the framework of the *BWare* project, Pierre Halmagrand, David Delahaye, Damien Doligez, and Olivier Hermant designed a new version of the *B* set theory using deduction modulo, in order to automatically verify a large part of the proof obligations of the benchmark of *BWare*, which consists of proof obligations coming from the modeling of industrial applications (about 13,000 proof obligations). Using this *B* set theory modulo with *Zenon Modulo*, as well as some other extensions of *Zenon*, such as typed proof search and arithmetic (implemented by Guillaume Bury), we are able to automatically verify more than 95% of the proof obligations of *BWare*, while the regular version of *Zenon* is only able to prove less than 1% of these proof obligations. This is a real breakthrough for the *BWare* project, but also for automated deduction in general, as it tends to show that deduction modulo is the way to go when reasoning modulo theories.

ESTASYS Exploratory Action

6.1. Highlights of the Year

The Plasma statistical model checker has been made available to other scientists. ESTASYS has open a new branch on verifying the security of complex systems.

GALLIUM Project-Team (section vide)

MARELLE Project-Team

6.1. Highlights of the Year

In June 2014, Yves Bertot received the ACM Software System award, as one of the main contributors to the Coq System, along with Gérard Huet, Thierry Coquand, Christine Paulin-Mohring, Bruno Barras, Jean-Christophe Filliâtre, Hugo Herbelin, Chet. Murthy, and Pierre Castéran.

MEXICO Project-Team

6.1. Highlights of the Year

6.1.1. Active Diagnosis for Probabilistic Systems

Diagnosis fits well with probabilistic systems since it is natural to model the uncertainty about the behaviour of a partially observed system by distributions. We had previously revisited the active diagnosis (which aims at controlling the system to make it diagnosable) in discrete event systems designing optimal decision and synthesis procedures [7]. This year, we have considered active diagnosis for probabilistic discrete event systems, obtaining again optimal procedures [26]. Furthermore we have refined the notion of active diagnosis by introducing the *safe active diagnosis* which ensures that after the control is applied, there is a positive probability that a fault never occurs. Interestingly this problem is undecidable but for finite memory controller we have shown that the problem becomes again decidable and we have designed optimal decision and synthesis procedures. Our approach has raised an issue that has not be observed by previous researchers: while in discrete event system, most variants of diagnosis are in fact equivalent, this is no more the case for probabilistic systems. So in [26], we have undertaken the task of classifying the different versions obtaining a complete landscape of the notions both in terms of relations and complexity. Furthermore we have proposed a new notion of diagnosis, the *prediagnosis* that combines the advantages of diagnosis and prediction.

6.1.2. Weighted automata and weighted logics

Weighted automata are a conservative quantitative extension of finite automata that enjoys applications, e.g., in language processing and speech recognition. Their expressive power, however, appears to be limited, especially when they are applied to more general structures than words, such as graphs. To address this drawback, we have introduced weighted pebble walking automata, which allow to navigate freely in the graph and may use pebbles to mark some positions.

In [20], we have shown with examples from natural language modeling and quantitative model-checking that weighted expressions and automata with pebbles are more expressive and allow much more natural and intuitive specifications than classical ones. We have extended Kleene-Schu ¨tzenberger theorem showing that weighted expressions and automata with pebbles have the same expressive power. We focussed on an efficient translation from expressions to automata. We also proved that the evaluation problem for weighted automata can be done very efficiently if the number of reusable pebbles is low.

In [18], we have studied the expressive power of these automata on words. We have proved that two-way pebble weighted automata, one-way pebble weighted automata, and our weighted logic with transitive closure are expressively equivalent. We also gave new logical characterizations of standard recognizable series.

In [30], we addressed the more general case of graphs such as nested words, trees, pictures, Mazurkiewicz traces, ... We established that weighted pebble walking automata have the same expressive power as weighted first order logic with transitive closure logic, lifting a similar result by Engelfriet and Hoogeboom from the Boolean case to a quantitative setting.

6.1.3. Verification of concurrent recursive programs

Distributed systems form a crucially important but particularly challenging domain. Designing correct distributed systems is demanding, and verifying its correctness is even more so. The main cause of difficulty here is concurrency and interaction (or communication) between various distributed components. Hence it is important to provide a framework that makes easy the design of systems as well as their analysis. There are two schools of thought on reasoning about distributed systems: one following the interleaving based semantics, and one following the visual partial-order/graph based semantics. In [23], we compare these two approaches and argue in favour of the latter. An introductory treatment of the split-width technique is also provided.

In [34], we develop a general technique based on split-width for the verification of networks of multi-threaded recursive programs communicating via reliable FIFO channels. We extend the approach of [6] to this setting. Split-width offers an intuitive visual technique to decompose our behaviour graphs such as MSCs and nested words. The decomposition is mainly a divide-and-conquer technique which naturally results in a tree decomposition. Every behaviour can now be interpreted over its decomposition tree. Properties over the behaviour naturally transfer into properties over the decomposition tree. This allows us to use tree-automata techniques to obtain decision procedures for a range of problems such as reachability, model checking against logical formalisms etc. In this way, we obtain simple, uniform and optimal decision procedures for various verification problems parametrised by split-width. Furthermore, the simple visual mechanism of split-width is as powerful as yardstick graph measures such as tree-width or clique-width. Hence it captures any class of distributed behaviours with a decidable MSO theory.

Multi-threaded recursive programs communicating via channels are turing powerful, hence their verification has focussed on under-approximation techniques. Any error detected in the under-approximation implies an error in the system. However the successful verification of the under-approximation is not as useful if the system exhibits unverified behaviours. In [24], we study controllers that observe/restrict the system so that it stays within the verified under-approximation. We identify some important properties that a good controller should satisfy. We consider an extensive under-approximation class, construct a distributed controller with the desired properties and also establish the decidability of verification problems for this class.

6.1.4. Regulation in Systems Biology

6.1.4.1. Rare events in Signalling Cascades

The visit in 2013 of Professor Monika Heiner from Cottbus University has led to a fruitful collaboration related to statistical model checking of rare events in signalling cascades (a regulatory biological system) [25]. This work has received one of the five top paper awards of the conference. In addition, we have improved the statistical methods used in our tool Cosmos.

6.1.4.2. Characterization of Reachable Attractors Using Petri Net Unfoldings

Attractors of network dynamics represent the long-term behaviours of the modelled system. Their characterization is therefore crucial for understanding the response and differentiation capabilities of a dynamical biological system. In the scope of qualitative models of interaction networks, the computation of attractors reachable from a given state of the network faces combinatorial issues due to the state space explosion.

In [33], we have presented a new algorithm that exploits the concurrency between transitions of parallel acting components in order to reduce the search space. The algorithm relies on Petri net unfoldings that can be used to compute a compact representation of the dynamics. We have illustrated the applicability of the algorithm with Petri net models of cell signalling and regulation networks, boolean and multi-valued. The proposed approach aims at being complementary to existing methods for deriving the attractors of Boolean models, while being generic since it applies to any safe Petri net.

PARSIFAL Project-Team

6.1. Highlights of the Year

Dale Miller's 1994 LICS paper titled "A Multiple-Conclusion Meta-Logic" [67] was a co-recipient of the LICS Test of Time Award.

PI.R2 Project-Team

5.1. Highlights of the Year

We successfully organised the thematic trimester Semantics of Proofs and Certified Mathematics (IHP, April-July 2014). The trimester attracted over two hundred participants altogether (with about 60 “resident” participants staying a month or more), hosted 5 special workshops, as well as other related regevents such as Types, MAP (Mathematics, Algorithms, and Proofs). It was the first thematic trimester in the history of IHP to feature computer science prominently. There was a kick-off day on April 22, with talks of Georges Gonthier, Thomas Hales, Xavier Leroy, and Vladimir Voevodsky, with the presence of some science journalists. During the trimester, the Bourbaki Seminar devoted an afternoon (June 21) to these themes, with talks of Thomas Hales and Thierry Coquand.

Shortly before, Coq has received the Software System Award 2013 from the Association for Computing Machinery (ACM). Hugo Herbelin is one of the recipients of this prize.

SUMO Project-Team

6.1. Highlights of the Year

We started our first industrial collaboration "Project P22" with Alstom Transport, in the context of a common laboratory between Inria and Alstom. The project started in March 2014 and tackles robustness issues and regulation in urban train systems. The second phase of the project will start in march 2015, for a duration of three years. Most of the researchers of Sumo are involved in this project.

TEMPO Team

6.1. Highlights of the Year

The project was created.

TOCCATA Project-Team

6.1. Highlights of the Year

- The ACM Software System Award 2013 was given, during a ceremony in June 2014 in San Francisco, to the Coq proof assistant (http://awards.acm.org/software_system/). The prestigious ACM price was previously awarded to the LLVM compiler infrastructure (2012) and to the Eclipse IDE (2011). Among the 9 recipients of the 2013 award are Christine Paulin and Jean-Christophe Filliâtre, from the Toccata team.
- The *Concours Castor informatique* (http://castor-informatique.fr/) had an even larger success than in the previous years. In November 2014, more than 228,000 teenagers from over 1500 schools participated and solved the interactive tasks of the contest. Arthur Charguéraud and Sylvie Boldo, from the Toccata team, significantly contributed to the prepation of the tasks and to the organization of the contest.

VERIDIS Project-Team

6.1. Highlights of the Year

The veriT solver (section 5.1) participated in the SMT competition 2014, part of the Vienna Summer Of Logic Olympic Games, and received the gold medal for the SMT category.

CARTE Project-Team

6.1. Highlights of the Year

Our team made remarkable progress into the understanding of complexity of higher-order functionals. While a robust class of computable functionals exists at any finite type built from $\mathbb{N}$ and $\rightarrow$ (the Kleene-Kreisel functionals), no satisfying complexity classes had been defined so far, except the class BFF of Basic Feasible Functionals. However that class is not a complexity class in the usual sense and does not offer the possibility to define space complexity or non-deterministic time complexity. In his PhD Hugo Férée has developed a non-trivial notion of size for higher-order functionals using game semantics and he has defined a notion of polynomial-time computable functional including BFF but behaving more satisfactorily in several ways. A paper in preparation will gather these results.

CASSIS Project-Team

6.1. Highlights of the Year

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

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

The ANR project SEQUOIA has been accepted.

BEST PAPERS AWARDS :

[43] **Software Security and Reliability (SERE)**. E. FOURNERET, J. CANTENOT, F. BOUQUET, B. LEGEARD, J. BOTELLA.

[47] **The 7th International Symposium on Foundations & Practice of Security FPS'2014**. H. H. NGUYEN, A. IMINE, M. RUSINOWITCH.

COMETE Project-Team

6.1. Highlights of the Year

- Prix de thèse de l'Ecole Polytechnique 2014 for the thesis "The Epistemic View of Concurrency Theory" by Sophia Knight (Defended 20 September, 2013).
- Catuscia Palamidessi has been invited keynote speaker at the joint conferences CONCUR 2014 and TGC 2014. Rome, September 2014.

DICE Team (section vide)

PRIVATICS Project-Team

5.1. Highlights of the Year

Vincent Roca was awarded the 3rd Applied Research price of the Fédération des Industries Electriques, Electroniques et Communications (FIEEC), for his transfer activities to the Expway French SME, Lyon, October 8th, 2014.

The team got two major contributions:

- *A Case Study: Privacy Preserving Release of Spatio-temporal Density in Paris* was published by Gergely Acs and Castelluccia at KDD 2014.
- *Censorship in the Wild: Analyzing Internet Filtering in Syria* was published by Chaabane Abdelberi, Mathieu Cunche,and Mohamed Ali Kaafar at IMC 2014.

PROSECCO Project-Team

6.1. Highlights of the Year

This year, we published 17 articles in international peer-reviewed journals and conferences, including papers in prestigious conferences such as POPL (2 papers) and all the top conferences in computer security: IEEE S&P Oakland (2 papers), CRYPTO, ACM CCS, NDSS, and Financial Cryptography. Our papers in these top venues (discussed later in New Results) serve as highlights of our research during the year. In addition to these papers, we published 1 PhD thesis and several technical reports.

We released updates to miTLS, ProVerif, CryptoVerif, and started working on a brand-new version of F*. We discovered serious vulnerabilities in a number of TLS libraries, web browsers, and web servers, resulting in 6 published CVEs, and over a dozen software updates based on our recommendations in widely used software such as Firefox, Chrome, Internet Explorer, Safari, OpenSSL, Java, and Mono.

We organized a winter school "The Joint EasyCrypt-F*-CryptoVerif School 2014" which attracted industrial researchers, academics, and students from around the world. Over 75 students learned to use cryptographic verification tools from instructors at Inria, IMDEA, and Microsoft Research. Two of the tools: CryptoVerif and F* are being developed in collaboration with Inria.

If we were to choose one research theme as our highlight of the year, it would be our activities surrounding Transport Layer Security (TLS):

- At CRYPTO 2014, we published a detailed cryptographic proof of the TLS handshake as implemented in miTLS
- At NDSS 2014, we published a study in the use of X.509 certificates in TLS servers on the web
- At IEEE S&P (Oakland), we published a new attack on the TLS protocol called the *triple handshake*, which affected all TLS libraries and mainstream TLS applications such as web browsers.
- To prevent our attack, we proposed patches to major software libraries as part of responsible disclosure. Our research directly led to security updates for all major web browsers and TLS implementations.
- We also proposed a long-term countermeasure for our attack, the TLS Session Hash extension, which we published as an internet draft and presented at the IETF. This draft is on its way to being a published standard and is already implemented in all major TLS libraries.
- We participated in the design of next version (1.3) of the TLS protocol. We hosted an interim TLS working group meeting in Paris. Our proposals such as the session hash construction are now an integral part of the new design, and we continue consulting on the design and implementation of TLS.